HARMONICS — EU FP7 Project on the Reliability and Safety Assessment of Modern Nuclear I&C Software

Janne VALKONEN[1], Sofia GUERRA[2], Robin BLOOMFIELD[2], Nguyen THUY[3], Josef MÄRTZ[4], Bo LIWÅNG[5], and Jari HÄMÄLÄINEN[1]

1. VTT Technical Research Centre of Finland, Espoo, Finland (janne.valkonen@vtt.fi, jari.hamalainen@vtt.fi)
2. Adelard LLP, London, United Kingdom, (aslg@adelard.com, reb@adelard.com)
3. EDF R&D, Chatou, France, (n.thuy@edf.fr)
4. ISTec GmbH, Garching b. München, Germany, (josef.maertz@istec.grs.de)
5. Strålsäkerhetsmyndigheten, Stockholm, Sweden, (bo.liwang@ssm.se)

Abstract: The reliability of computer-based systems implementing safety functions is a critical issue for the modernization and construction of nuclear power plants, in particular because software can usually not be proven to be entirely free of defects. The differences in regulation and safety justification principles between different countries restrict efficient co-operation and hinder the emergence of widely accepted best practices. This paper gives an introduction to an EU FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software, 2011-2014) which has an overall objective to ensure that the nuclear industry has well founded and up-to-date methods and data for assessing software of computer-based safety systems.

Keywords: Software reliability, safety justification, verification and validation

1 Introduction

The reliability and safety of computer-based systems that implement safety functions are critical issues for the construction and modernisation of nuclear power plants. This is in particular due to the fact that software can usually not be proven to be free of defects, and that postulated residual defects could be suspected of leading to common cause failure that could defeat redundancy and defence-in-depth. Unfortunately, the differences in current safety justification principles and methods between different countries restrict co-operation and hinder the emergence of widely accepted best practices. They also prevent cost sharing and reduction, and unnecessarily increase licensing uncertainties, thus creating a difficult operating environment for utilities, vendors and regulatory bodies.

Given the experience with nuclear-related and software-based systems worldwide, there is now the possibility of using empirical reliability data in a way that has not been feasible before. In addition, advances in computer power and testing techniques means that simulated experience and statistical testing are becoming more practicable as forms of evidence. This evidence could have an important role in the assurance of nuclear I&C systems. Advances have also been made, and practical experience gained, in several other domains, such as the formal verification of software, defensive measures to tolerate postulated residual software faults, and safety justification frameworks.

The overall objective of the HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software, 2011–2014) project is to ensure that the nuclear industry has well founded and up-to-date methods and data for assessing software of computer-based safety systems. It takes advantage of the aforementioned advances to propose systematic and consistent, yet realistic and practical approaches for software verification, software safety justification and quantification of software failure rates.

2 HARMONICS project structure

The project is organised in four technical work-packages (WP):

- WP1 establishes the current state-of-the-art and needs regarding software verification, safety justification and quantification of failure rates.
- WP2 develops innovative methods and tools for these three topics.

- WP3 applies the methods and tools (proposed by WP2) to case studies.
- WP4 assesses the effectiveness of the proposed methods and tools, based on the results of the case studies.

The project consortium has five partners: VTT Technical Research Centre of Finland (coordinator), Électricité de France (EDF), Institute for Safety Technology (ISTec) from Germany, Adelard LLP from UK and The Swedish Radiation Safety Authority (SSM). Consortium partners represent different stakeholders in the nuclear I&C field. Five EU countries together ensure that a large overview of national policies and practices regarding safety issues and licensing are considered in the project. In addition, a large “End User and Advisory Group” consisting of utilities, regulatory bodies, suppliers, and technical support organizations has been constituted to review and give feedback on the project work. Thus, the project should foster an international consensus based on a sound scientific and technical approach, and provide a good basis for harmonisation. Two End User Workshops have been organised, in April 2012 in Helsinki and in April 2014 in Paris. The public website of the project is http://harmonics.vtt.fi.

3 State-of-the art in V&V and reliability assessment of software in nuclear industry

The state of the art of nuclear I&C systems is well described in the major nuclear industry standards (i.e. IAEA NS-G-1.1 [1] and 1.3 [2], IEC 61513 [3], IEC 60880 [4], IEC 62138 [5]) and the supporting corporate and regulatory guidance. These standards represent an international consensus, but their application provides considerable configuration and interpretation. This is particularly true for systems and devices not originally developed to nuclear industry standards, which is an increasing issue as the nuclear industry does not dominate the supply chain.

Several European projects have dealt with the key technologies enabling effective I&C modernisation of NPPs, namely with I&C systems, networks and instrumentation, hardware components design technologies, and software and safety. One of the key projects was CEMSIS (Cost-Effective Modernisation of Systems Important to Safety) that produced guidance on a proposed approach to safety justification of SIS (System Important for Safety), on requirements engineering for SIS and on qualification strategy for COTS (Commercial Off-The-Shelf) or pre-existing software products [6]. Another preceding project, BE-SECBS (Benchmark Exercise on Safety Evaluation of Computer Based Systems), provided a comparative evaluation of assessment methodologies for safety critical computer based systems that are in use in the nuclear industry [7]. One of the methodologies was aimed at quantitative software reliability estimation. Since CEMSIS and BE-SECBS, several bi-lateral and national projects have utilized and developed the results further.

When developing safety justifications of I&C systems, one has to recognise the different regulatory and licensing approaches used by the different countries. The regulatory guidance (e.g., in YVL in Finland [8], [9], the SAPs in the UK [10], SKIFS in Sweden [11]) provides compelling advice and is further backed up by the "Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations" [12] on areas of consensus and challenge.

HARMONICS addresses the difficult issue of justifying claims about I&C software contribution to the reliability of protection function, claims that are likely to be dominated by CCF contribution. This is still a difficult area because there is no international or scientific consensus. In addressing the issue, the project also has to consider the broader set of claims that need to be made about the software systems.

4 HARMONICS methods and tools

HARMONICS mainly focuses on the independent confidence building for software of I&C systems implementing the highest safety class, i.e., category A functions. In the framework of the project, the term ‘software’ is interpreted in a broad sense to include not only ‘classical’ software to be executed in a microprocessor, but also HDL (hardware description language) designs (usually for FPGAs, Field Programmable Gate Arrays) and digital systems architectures.

The development of methods and tools in HARMONICS can be divided into the following key issues: 1) development of software verification methods and tools, 2) evaluation of justification frameworks for software-based systems, 3) development of approaches to the quantification of software failure rates.

4.1 Software verification

In software verification, the main objective is to provide direct evidence of software correctness. Formal verification has many benefits including the fact it can provide a high level of assurance that a claimed property is satisfied. The safety properties to be verified can be classified into:

- A functional property: the outputs computed by the software program satisfy specified functional and timing requirements.
- An integrity property: the software program is free from given types of faults, usually so-called intrinsic faults. Intrinsic faults are faults that can be recognised as such without knowing the functional and timing requirements specified for the software program.
- A structural property, which states how the software program is structured or how it functions internally.
- An equivalence property, which states that a given software program or software representation is equivalent to another one for a given functional, integrity or structural property.

One of the formal methods to be demonstrated in HARMONICS is model checking, which is a computer-aided verification method developed to formally verify the correct functioning of a system design model [13], [17]. In model checking, all possible system behaviours, i.e. system responses to all possible input sequences, are examined. In HARMONICS, model checking has been applied to verify the correctness of functional logic diagrams with respect to system requirements.

The use of software statistical testing (SST) provides the potential to demonstrate estimated system reliability. Reference [12] discusses the use of SST and it recommends its use for justifying software based systems when there is no access to the source code. In the UK, the regulator has encouraged that SST should be performed and it has been employed to demonstrate reliability of safety-related programmable systems. In Finland, quantitative reliability assessment of I&C systems is mandatory in the highest safety category [8], [9].

Many reliability arguments may rely on specific behaviour of design features. For example, cyclic behaviour and transparency to plant conditions may be essential elements in the justification that the operating system of a safety I&C platform will not be a significant cause of failure when a demand condition occurs, and thus will also not be a significant source of common cause failure (CCF).

Complexity analysis is a means to direct assessment to the real critical parts of the digital I&C system where intrinsic investigation is needed due to the complexity of the corresponding digital I&C software. Complexity analysis can be applied to the assessment of the functional logic diagrams to identify complex-intensive parts of the digital I&C system and can thus support to direct the investigation activities into the real critical parts of the system. Besides, complexity analysis can provide indirect evidence for the reliability quantification.

4.2 Safety justification framework

One widely used approach to justifying an I&C system and its software is to provide evidence that they have been designed and verified following a well-structured development process and applying the requirements and recommendations of rigorous standards. This type of justification approach can be called the rule-based approach, as it relies on the application of pre-defined rules. The rule-based approach works well in stable environments where best practice is deemed to imply adequate safety. However, it does not always provide direct evidence that the I&C system and its software achieve the behaviour or the properties required to the desired level of reliability. In addition, there might be cases where one finds no suitable set of applicable rules that can confer the desired level of confidence in a given property or that can be demonstrated to have been met. To overcome these difficulties, a more goal-oriented justification approach may be applied, where the justification explicitly demonstrates that the desired behaviour, property or reliability has been achieved.

This type of approach can be called the goal-based approach.

Lastly, particularly for safety systems, one also needs to justify that the I&C system and its software will not have unacceptable behaviour, that the postulated hazards have been addressed, and that the risks incurred by the remaining vulnerabilities have been reduced to an acceptable level. This type of approach can be called the risk-informed approach.

One important aim of HARMONICS is to improve safety justifications by integrating these three approaches (rule-based, goal-based, and risk informed) to get a coherent process for justifying software-based I&C systems (see Fig. 1). The justification framework is further discussed in [14].

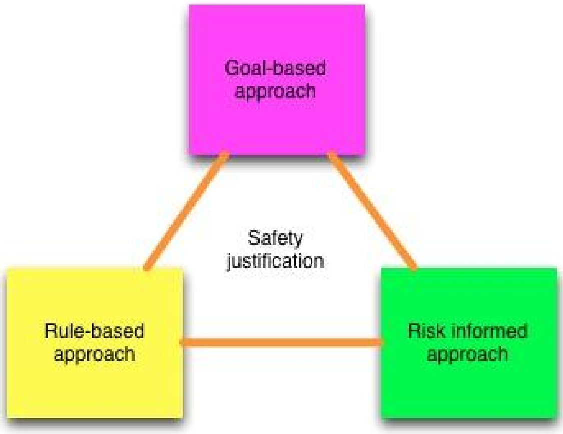


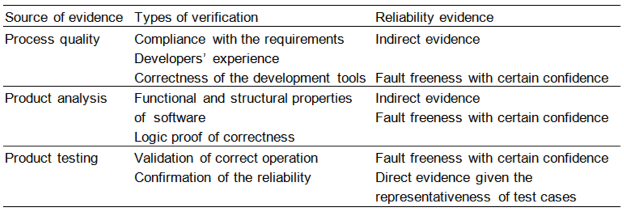
Fig. 1 Integrated safety justification strategy.

4.3 Quantification

HARMONICS tackles the problem of software reliability assessment using analytical approaches that, for example, take into consideration all the information obtained by V&V. One of the possible ways of organising the various pieces of evidence in a probabilistic format is to use Bayes belief network (BBN). Bayes network is a general model for probabilistic inference so that the conditional dependences between the random variables are presented in a directed acyclic graph [15]. In this context, the random variables are reliability claims related to the software and various pieces of evidence available for reliability assessment.

One key issue is how different pieces of evidence from software V&V are interpreted in a probability model context and how their interrelationships are assessed. This can be combined with other analytical approaches that model the development process and use development fault data to estimate the number of residual faults. This information can then be used to estimate worst case bounds on the software reliability. The justification of the reliability estimated will be based on the concept of a structured safety case [16].

Fig. 2 lists various sources of evidence available for the independent confidence building. Indirect evidence needs to be measured by some rating scale which needs to be interpreted in terms of reliability. Fault freeness evidence can be used to exclude certain software fault modes. From the reliability point of view there may remain doubt on the correctness of the evidence, which can be expressed as a probability. Direct evidence is in principle the optimal case, but in reality the confidence on the representativeness of the data may need to be included in the assessment.



Source of evidence	Types of verification	Reliability evidence
Process quality	Compliance with the requirements Developers' experience Correctness of the development tools	Indirect evidence Fault freeness with certain confidence
Product analysis	Functional and structural properties of software Logic proof of correctness	Indirect evidence Fault freeness with certain confidence
Product testing	Validation of correct operation Confirmation of the reliability	Fault freeness with certain confidence Direct evidence given the representativeness of test cases

Fig. 2 Types of evidence for software reliability estimation.

5 Case studies

The methods and tools proposed in the project have been applied in case studies that serve several objectives:

- Help develop methods and tools.
- Confirm that the methods and tools can be applied with success to real systems and software.
- Provide an illustrative public example that could be used to demonstrate and disseminate the results of the project.

The case studies address the following topics:

- Confidence in requirements specifications,
- Formal verification,
- Safety justification framework,
- Reliability quantification,
- Model checking, and
- Complexity analysis.

The evaluation of the case studies and the proposed approaches for safety justification was performed in several phases. The first evaluation step was taken while different verification methods were developed. It summarized the first impressions and already existing experiences of the applicability of the methods. The second step of the evaluation was the analysis of the results of the case studies where the approaches were utilized on practical level to understand and demonstrate how they should be used, for what kinds of problems they can be utilized, who should use them, in what project or development phase they should be used and how much effort the utilization takes. Finally, the third evaluation step was the evaluation done by the HARMONICS end user group in the 2nd End User Workshop.

The evaluations and end users' recommendations will be taken into account while developing a public case study which aims at summarizing the main results of the project. It should be finished by the end of 2014 when the HARMONICS project ends.

Acknowledgements

HARMONICS is co-funded by the European Commission, the UK C&I Nuclear Industry Forum (CINIF) and the consortium organisations: VTT Technical Research Centre of Finland, Électricité de France (EDF), Institute for Safety Technology (ISTec) from Germany, Adelard LLP from UK and Strålsäkerhetsmyndigheten (SSM) from Sweden. The authors also acknowledge the contributions of the other HARMONICS project members.

References

[1] "Software for Computer Based Systems Important to Safety in Nuclear Power Plants," IAEA Safety Guide No. NS-G-1.1, International Atomic Energy Agency, Vienna, 2000.

[2] "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," IAEA Safety Guide No. NS-G-1.3, International Atomic Energy Agency, Vienna, 2002.

[3] "Nuclear power plants. Instrumentation and control important to safety. General requirements for systems," IEC 61513:2011, International Electrotechnical Commission, Geneva, 2011.

[4] "Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions," IEC 60880:2006, International Electrotechnical Commission, Geneva, 2006.

[5] "Nuclear power plants. Instrumentation and control important for safety. Software aspects for computer-based systems performing category B or C functions," IEC 62138. International Electrotechnical Commission, Geneva, 2004.

[6] "CEMSIS. Cost Effective Modernisation of Systems Important to Safety. Work Package 0. Final Public Synthesis Report (first issue)," http://www.cemsis.org/, 2004.

[7] V. Kopustinskas, C. Kirchsteiger, B. Soubies, F. Daumas, J. Gassino, J.C. Péron, P. Régnier, J. Märtz, M. Baleanu, H. Miedl, M. Kersken, U. Pulkkinen, M. Koskela, P. Haapanen, M.L. Järvinen, H.W. Bock, W. Dreves, "Benchmark Exercise of Safety Evaluation of Computer Based Systems (BE-SECBS Project)," Proc. of FISA-2003 conference, Luxembourg, November 10-13, 2003.

[8] "Safety design of a NPP", Guide YVL B.1, Radiation and Nuclear Safety Authority, Helsinki, 2013.

[9] "Electrical and I&C equipment of a nuclear facility", Guide YVL E.7, Radiation and Nuclear Safety Authority, Helsinki, 2013.

[10] "Safety Assessment Principles for Nuclear Facilities – 2006 Edition," Health and Safety Executive, Office for Nuclear Regulation, Revision 1, 2008.

[11] "The Swedish Nuclear Power Inspectorate's Regulations concerning the Design and Construction of Nuclear Power Reactors," The Swedish Nuclear Power Inspectorate Regulatory Code, SKIFS 2004:2, 2004.

[12] "Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations, Revision 2013, BEL V, Belgium, BfS, Germany, CSN, Spain, ISTec, Germany, ONR, United Kingdom, SSM, Sweden, STUK, Finland

[13] E. M. Clarke, Jr., O. Grumberg, D. A. Peled, Model Checking, The MIT Press, 1999.

[14] S. Guerra, N. Thuy, “Safety Justification Frameworks: Integrating Rule-Based, Goal-Based, and Risk-Informed Approaches,” Proc. of 8th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT), July 22-26, 2012, San Diego, CA.

[15] J. Pearl, “Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference,” Representation and Reasoning Series (2nd printing ed.). San Francisco, California: Morgan Kaufmann, 2007.

[16] J.-E. Holmberg, P. Bishop, S. Guerra, N. Thuy, “Safety case framework to provide justifiable reliability numbers for software systems,” Proc. of 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012.

[17] J. Lahtinen, J. Valkonen, K. Björkman, J. Frits, I. Niemelä, K. Heljanko, “Model checking of safety-critical software in the nuclear engineering domain”, Reliability Engineering & System Safety 105(104–113)2012.