HARMONICS — EU FP7 PROJECT ON THE RELIABILITY ASSESSMENT OF MODERN NUCLEAR I&C SOFTWARE

Jan-Erik Holmberg
VTT
P.O.Box 1000, FI-02044 VTT, Finland
jan-erik.holmberg@vtt.fi

Sofia Guerra
Adelard LLP
10 Northampton Square, EC1V 0HB, London, United Kingdom
aslg@adelard.com

Nguyen Thuy
EDF R&D
6, Quai Watier, 78401 Chatou, FRANCE
n.thuy@edf.fr

Josef Märtz
ISTec GmBH
Boltzmannstrasse 14, 85748 Garching, GERMANY
josef.maertz@istec.grs.de

Bo Liwång
Strålsäkerhetsmyndigheten
Solna strandväg 96, SE-171 16 Stockholm, SWEDEN
bo.liwang@ssm.se

ABSTRACT

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 due to the fact that software can usually not be proven to be defect-free, and that postulated residual defects could be suspected of leading to common cause failure that could defeat redundancy and defence-in-depth. The differences in current safety justification principles and methods between different countries restrict co-operation and hinder the emergence of widely accepted best practices. 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. Advances in computer power and testing techniques means that simulated experience and statistical testing are becoming more practicable as forms of evidence. Advances have also been made in several other domains, such as software formal verification, defensive measures to tolerate postulated residual software faults, and safety justification frameworks. The overall objective of the EU FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) 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 will take 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. HARMONICS will focus on the independent confidence building for software of I&C systems implementing Category A functions.

Key Words: Software reliability, verification and validation, safety case, nuclear power plant

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 defect-free, 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 very 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 will take 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.

HARMONICS plans to collaborate with a parallel Chinese R&D project RAVONSICS (Reliability And V&v Of Nuclear Safety I&C Software), being part of the recently initiated co-operation between Euratom and Chinese Atomic Energy Agency (CAEA). RAVONSICS will have similar objectives, scope and structure. At the moment of writing this paper, the coordination agreement between the EU and the Chinese project, however, has not yet been signed. The aim of the collaboration is to take into consideration the different views, practices, and requirements of the participating countries in Europe and China.

2 HARMONICS PROJECT STRUCTURE

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

- WP1 will establish the current state-of-the-art and needs regarding 1) software verification, 2) safety justification and 3) quantification of failure rates.
- WP2 will develop innovative methods and tools for these three topics.
- WP3 will apply the methods and tools proposed by WP2 to case studies.
- WP4 will assess the effectiveness of the methods and tools proposed by WP2, based on the results of the case studies of WP3.

The project consortium has five partners: 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. Consortium partners represent different stakeholders in the nuclear I&C field. Five EU countries together with collaboration with China ensure that a large overview of national policies and practices regarding safety issues and licensing are considered by the project.

A larger "End user and advisory group" has been constituted with other interested stakeholders (utilities, regulatory bodies, suppliers) 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. HARMONICS will organise two public events (interim seminar in April 2012 and final seminar in 2014) to inform the community. The public website address 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 these methodologies was aimed at quantitative software reliability estimation. Since these two projects, several bi-lateral and national projects have been taking these 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], the SAPs in the UK [9], SKIFS in Sweden [10]) provides compelling advice and is further backed up by the "Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations" [11] 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 this issue, the project will also have to consider the broader set of claims that need to be made about the software systems.

4 HARMONICS METHODS AND TOOLS

HARMONICS focuses on the independent confidence building for software of I&C systems implementing the highest safety class, i.e., category A functions (Figure 1). Research work will benefit from recent licensing projects, for new builds and also for I&C upgrades. 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.

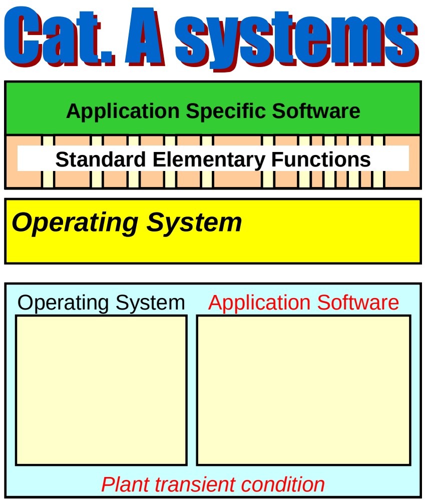
Cat. A systems
Application Specific Software
Standard Elementary Functions
Operating System
Operating System
Application Software
Plant transient condition

Figure 1. Scope of HARMONICS.

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 (Figure 2). Two main verification approaches considered in HARMONICS are formal verification and statistical testing.

Formal verification has many benefits including, that fact it can provide a high level of assurance that a claimed property is satisfied. Currently, methods exist that allow functional properties to be formally verified, but only for software of single processor systems. HARMONICS will investigate the use of alternative methods to able to verify complex electronic designs, which are typically concurrent and asynchronous. For example, one objective will be to provide rigorous evidence that the application software of a distributed system meets its functional and timing requirements.

The safety properties to be verified can be classified into:

- Functional properties (i.e., ability to meet functional and timing requirements).
- Integrity properties (i.e., freedom from certain types of faults, in particular intrinsic faults detectable without knowledge of functional and timing requirements).

- Structural properties (i.e., properties related to claimed design measures, such as fault tolerance, defence against common-cause failure or failure rate quantification).
- Equivalence properties (to verify that translation tools such as compilers, synthesisers or place & route tools have not introduced discrepancies with the source code).

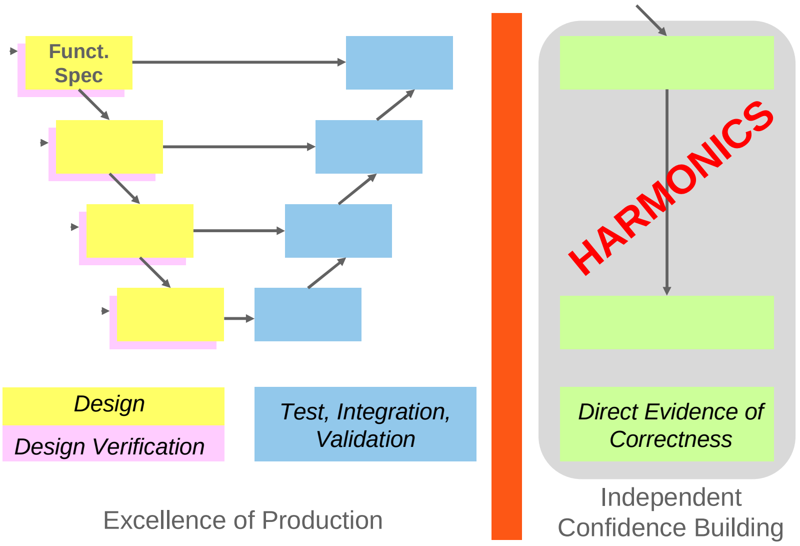
Funct. Spec
HARMONICS
Design
Design Verification
Test, Integration, Validation
Direct Evidence of Correctness
Excellence of Production
Independent Confidence Building

Figure 2. HARMONICS perspective on verification.

The use of software statistical testing (SST) provides the potential to demonstrate estimated system reliability. Reference [11] 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].

The most important practical limitation is the very high number of tests necessary to demonstrate that a system is highly reliable. It can require prohibitively long execution times if all the tests are to be performed on the final system. One technical limit is the fact that not all postulated failure mechanisms are well covered by statistical testing. For example, failures triggered by long elapsed times are very unlikely to occur during statistical tests, which need to be executed rapidly one after the other. HARMONICS will:

- Identify the possible failure mechanisms not well covered by statistical tests; these mechanisms will then be addressed by other approaches, like static analysis and formal verification.
- Investigate the justification of the reduction of the number of tests necessary for a given reliability claim, for example through a complementary use of statistical testing and analysis of known design features.
- Investigate the justification of the use of simulation, (and in particular of high performance simulation on massively parallel supercomputers) for statistical testing.

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). Also, as noted previously, particular design features could be relied upon to increase the efficiency of statistical testing. HARMONICS will:

- Investigate approaches to systematically classify the software failure and software CCF mechanisms that can lead to failure modes of interest.
- Identify design features that can preclude particular classes of failure mechanisms.
- Propose practical means to verify, and provide evidence of the correct implementation of these behaviour and features.
- Describe how such evidence can be incorporated into the claims, e.g., for failure propagation, tolerance to residual software faults, defence against software CCF, and optimisation of tests.

4.2 Justification framework

Regarding justification frameworks, HARMONICS will investigate different approaches (goal-based, rule-based, and risk-informed approaches) to justify systems and software performing category A functions. The project will, consider strengths and weaknesses of the different approaches, their applicability domains, and how they can complement one another. A second objective will be to determine how different types of evidence (e.g., formal verification, dynamic and static analysis, operational experience, statistical testing, development processes, quality controls) can be combined to justify a claim. The justification framework is further discussed in [12].

4.3 Quantification

HARMONICS will tackle 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 [13]. 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 in the HARMONICS approach is how different pieces of evidence 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 [14].

The process models developed in BE-SECBS [7] and UK CINIF projects will be developed further to provide support for judgments about the reliability. The exact form of the safety case based on these approaches is depending on the application and on negotiation by the parties involved, but must generally conform to a given framework.

The aim is to develop approaches so that evidence of reliability from statistical testing and other quantitative software reliability methodologies can be included in the safety justification for I&C system. This would complement the other verification and analysis activities, including the analysis of operational experience. It would need to address technical questions concerning:

- The role of statistical testing in the overall safety justification, e.g., would it be more convincing to assess the sources of doubt in the other part of the case rather than attempt a stand-alone justification.

- The role of testing given the low numerical targets required. The extent to which high performance simulation can go beyond current claim limits for software (typically 10^{-4}) and additional assumptions needed to achieve this. The integration of assumption doubt into the claimed reliability will draw on current research into confidence.
- The role of particular software behaviour and design features that can limit or even preclude specific failure mechanisms.
- The nature of the arguments that will be used to demonstrate reliability of the system (direct measurement, inference form component reliability, arguments of fault freeness with certain confidence).
- The role of operational experience in providing confirmation of reliability and an indication of possible vulnerabilities in the components used. This will necessitate both pragmatic advice on data collection, the development of safety justification approaches to use the data and specialised models to infer reliability estimates from the evidence.

5 CASE STUDIES

Work on case studies will be performed in parallel with the development of the methods. Different case studies will be needed to cover the different types of software that can be found in systems implementing category A functions (platform software, application software, HDL designs). Different verification methods will be used for the different types of software systems. System level case studies will also be used, mainly to illustrate the quantification of failure rates and the justification framework.

A public case study will also be developed to present the HARMONICS methods to a wider audience, as most of the other case studies have a restricted distribution due to confidentiality conditions.

For the time being, the following types of case studies are considered:

- Diesel Load Sequencer from requirements specification, formal verification and statistical testing point of view.
- Simulation-based statistical testing.
- Formal verification of an operating system software.
- Application software from the requirements specification, formal verification and reliability assessment point of view.
- Safety justification of a comprehensive digital I&C-system.

6 ACKNOWLEDGMENTS

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.

7 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 ftp://ftp.cordis.europa.eu/pub/fp5-euratom/docs/fisa2003_2-8_be-secbs_en.pdf (2003).
8. "Instrumentation systems and components at nuclear facilities," Guide YVL 5.5, Radiation and Nuclear Safety Authority, Helsinki http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL5-5 (2002).
9. "Safety Assessment Principles for Nuclear Facilities – 2006 Edition," Health and Safety Executive, Office for Nuclear Regulation, Revision 1, http://www.hse.gov.uk/nuclear/saps/ (2008).
10. "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).
11. "Licensing of safety critical software for nuclear reactors. Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations, BEL V, Belgium, BfS, Germany, CSN, Spain, ISTec, Germany, NII, United Kingdom, SSM, Sweden, STUK, Finland," Revision 2010. http://www.hse.gov.uk/nuclear/software.pdf (2010).
12. 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 (2012).
13. J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Representation and Reasoning Series (2nd printing ed.). San Francisco, California: Morgan Kaufmann (2007).
14. 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* (2012).