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

J.-E. HOLMBERG
VTT
P.O.Box 1000, FI-02044 VTT, FINLAND

S. GUERRA
Adelard LLP
10 Northampton Square, EC1V 0HB, London, UNITED KINGDOM

N. THUY
EDF R&D
6, Quai Watier, 78401 Chatou, FRANCE

J. MÄRTZ
ISTec GmBH
Boltzmannstrasse 14, 85748 Garching, GERMANY

B. Liwång
SSM
Solna strandväg 96, SE-171 16 Stockholm, SWEDEN

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. 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. 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. HARMONICS will focus on the independent confidence building for software of I&C systems implementing Category A functions. Research work will benefit from recent licensing projects, for new builds and also for I&C upgrades. HARMONICS will address three 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. HARMONICS started in January 2011 will end in 2014. A collaboration project in China is in preparation.

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.

Several European projects have dealt with the key technologies enabling efficient I&C modernisation at 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 [1]. 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 [2]. One of these methodologies was aimed at quantitative software reliability estimation.

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.

2. HARMONICS project structure

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

- WP1 will establish the current state-of-the-art and needs regarding software verification, safety justification and 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 all the stakeholders in the nuclear I&C field. HARMONICS will collaborate with a parallel Chinese R&D project RAVONSICS (Reliability And V&v Of Nuclear Safety I&C Software). At the moment of writing this paper, the coordination agreement between the EU and the Chinese project, however, has not yet been signed.

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. HARMONICS methods and tools (WP2)

HARMONICS focuses on the independent confidence building for software of I&C systems implementing the highest safety class, i.e., category A functions. 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 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.

3.1 Software verification

In software verification, the main objective is to provide direct evidence of software correctness. Three main verification approaches considered in HARMONICS are formal verification, statistical testing, and logic coverage testing.

Formal verification can provide a very high level of assurance that a claimed property is indeed satisfied. Currently, methods and means exist that allow functional properties to be formally verified, but only for software of single processor systems. HARMONICS will investigate the use of methods and means developed for formal verification of complex electronic designs, which are typically concurrent and asynchronous. The 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).

The use of software statistical testing (SST) provides the potential to demonstrate estimated system reliability. Reference [3] 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.

The most important practical limitation is the very high number of tests necessary. 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. These mechanisms will then need to be addressed by other approaches, like static analysis, complexity measurement and formal verification.

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.

3.2 Justification framework

Regarding justification frameworks, HARMONICS will investigate different approaches (goal-based, rule-based, and risk-informed approaches) to justify category A systems and software, to identify their strengths and weaknesses, applicability domains, and how they can complement one another. A second objective will be to determine how different types of evidence (formal verification, dynamic and static analysis, operational experience, statistical testing, development processes, quality controls) can be combined to justify a claim.

The exact form of the safety case based on these approaches depends on the application and on negotiation by the parties involved, but the application specific subjects must conform to the general form of a safety case.

The risk-informed approach will enhance the following subjects in justifying safety:

- Explicit consideration of a broader set of potential challenges to safety.
- Prioritisation of these challenges based on risk significance, operating experience, and engineering judgment.
- Identification and quantification sources of uncertainty in the V&V, tests and analysis.
- Analysis of software failure mechanism.

The progress beyond the state of the art will also involve characterising the justification of the quality of development process and providing explicit links to the reliability case.

3.3 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 and organised by a Bayes network model. 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. In this context, the random variables are reliability claims related to the software and various pieces of evidence available for reliability assessment.

Key issue 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 follow the concept of a structured safety case, which is a solution to get a coherent process for the quantitative reliability assessment of software-based systems.

4. Case studies (WP3)

Work on case studies will parallel the methods development. Different types of case studies will be needed to cover the types of software that can be found in systems implementing category A functions (platform software, application software, HDL designs). Each type of software will be the object of specific verification methods. For failure rates quantification and justification frameworks, system level case studies will be used. A public case study will be developed to present the HARMONICS methods to the widest audience possible.

5. Evaluation of methods and case studies (WP4)

In HARMONICS, the main idea to use case studies is to gain a deep understanding of the approaches, methods and tools, and to test whether the results of the research and development work can be recommended in licensing I&C systems and software in nuclear power plants. The objective of the WP4 is to assess the results of the approaches tested on case studies to support the utilities in licensing their software of I&C systems. Independent persons (project partners and volunteer end users) not involved in the case studies will evaluate the developed methods (WP2) based on the results from the case studies (WP3).

6. Conclusions

The overall objective of the HARMONICS 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 recent advances in computer power and testing techniques as well as operating experience collection, to propose systematic and consistent, yet realistic and practical approaches for software verification, software safety justification and quantification of software failure rates. 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.

7. References

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

2. Kopustinskas, V., Kirchsteiger, C., Soubies, B., Daumas, F., Gassino, J., Péron, J.C., Régnier, P., Märtz, J., Baleanu, M., Miedl, H., Kersken, M., Pulkkinen, U., Koskela, M., Haapanen, P., Järvinen, M.L., Bock, H.W., Dreves, W., Benchmark Exercise of Safety Evaluation of Computer Based Systems (BE-SECBS Project). In 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

3. 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