EUROPEAN COMMISSION

Community research

HARMONICS

(Contract Number: 269851)

DELIVERABLE (D-N°: 5.6)

Journal Articles, Conference Papers, Other Publications

Author(s): Nguyen Thuy, EDF
Janne Valkonen, VTT
Bo Liwång, SSM
Robin Bloomfield, ADELARD
Josef Märtz, ISTec
Arndt Lindner, ISTec

Reporting period: 11/07/12 - 11/01/15

Date of issue of this report: 11/01/2015

Start date of project: 12/01/2011 Duration: 48 Months

EURATOM

DISTRIBUTION LIST

Name	Number of copies	Comments
European Commission/ Georges van Goethem	1	
HARMONICS partners:		
VTT/Jari Hämäläinen	1	
EDF/Nguyen Thuy	1	
Adelard/ Sofia Guerra	1	
ISTec/ Arndt Lindner	1	
SSM/Bo Liwång	1	

Project co-funded by the European Commission under the Seventh Euratom Framework Programme for Nuclear Research &Training Activities (2007-2011)		
Dissemination Level		
PU	Public	X
RE	Restricted to a group specified by the partners of the [HARMONICS]	
CO	Confidential, only for partners of the [HARMONICS] project	

REVIEW

	Name	Date	Signature
Authors	Nguyen Thuy, EDF Janne Valkonen, VTT Robin Bloomfield, ADELARD Josef Märtz, ISTec Arndt Lindner, ISTec Bo Liwång, SSM	31/12/2014	
Reviewed by	Sofia Guerra, ADELARD	11/01/2015	
Approved by	Jari Hämäläinen, VTT	11/01/2015	

REVISIONS

IND REV	STATUS DATE	PARAGRAPH	SCOPE OF THE REVISION
1.0	11/01/15		Final version.

List of contents

1 Introduction

This document constitutes deliverable D5.6 of the HARMONICS project. It presents the main actions performed to disseminate the results of the projects.

Section 2 presents the communications made at scientific and industry conferences and workshops. Since the rights on the full papers and presentation slides have often been transferred to the conferences or workshops, only the abstracts are presented here.

Section 3 presents the on-going development of an IAEA report on the Dependability Assessment of Software for Safety I&C Systems at NPPs.

The two End Users Workshops organised by the project are reported in deliverables D5.3 and D5.5 and are not addressed here.

2 Communication actions

2.1 14th International Workshop on Nuclear Safety and Simulation

This workshop was held October 23-24 2012 in Harbin (China). Two HARMONICS presentations were made:

- Keynote lecture: Overcoming Regulatory Differences Regarding Digital I&C
- Software reliability analysis in probabilistic risk analysis

2.1.1 Overcoming Regulatory Differences Regarding Digital I&C - Abstract

For many reasons, modern I&C architectures and upgrades of obsolete I&C systems rely in a very large part on digital systems. In the past, a plant (and its I&C design) was usually presented to only one regulatory body. With globalisation, this is no longer true: plant designers now present their designs in multiple countries. Unfortunately, due to lack of regulatory harmonisation, designs accepted by one country have been rejected by another. This is problematic for several reasons. Firstly, this raises doubts in the general public: who is right? Is it really safe? Secondly, this increases the regulatory uncertainty, leading to increased costs and delays.

Regarding digital I&C, there are many reasons for such disharmony. In particular, because of complexity, it is in general impossible to fully guarantee that a digital design (including software) is free of design errors. And because of the deterministic nature of software, digital systems are suspected of common-cause failure that could defeat redundancy and defence-in-depth. International regulatory bodies have made several attempts at harmonisation. Past efforts have led to limited results. Current efforts (like the Multinational Design Evaluation Programme) might be more fruitful, but progress is slow and unlikely to provide practical solutions either.

To complement regulatory efforts, the industry needs to do its part. It should work together to propose overall I&C architectures principles that are acceptable to all (or to most) regulatory bodies. If no reasonable architecture can be found, it should highlight the regulatory differences that are the most troublesome. These should be the priority targets of regulatory harmonisation efforts.

Concerning the licensing of individual I&C systems, efforts might be focused on ensuring that the same design is acceptable in all or most countries. That a given country has specific requirements regarding verification and validation (not directly affecting the design) is a lesser ill. At that level, the world is divided into two sides: the first applies the IEC standards, the second applies the IEEE standards. The two sets of standards are difficult to compare and harmonise. Though "dual logo" standards have been proposed, very few have reached the final publication stage, in large part due to rivalry between the two sides. Therefore, novel approaches need to be proposed where no side would appear to be a winner or a loser.

Last but not least, research may play a significant role. For example, the HARMONICS project specifically aims at providing innovative software verification and justification methods that could support regulatory, industry and standards efforts.

2.1.2 Software reliability analysis in probabilistic risk analysis – Abstract

To assess the risk of nuclear power plant operation and to determine the risk impact of digital systems, there is a need to quantitatively assess the reliability of the digital systems in a justifiable manner. The Probabilistic Risk Analysis (PRA) is a tool which can reveal shortcomings of the NPP design in general and PRA analysts have not had sufficient guiding principles in modelling particular digital components malfunctions.

Currently digital I&C systems are mostly analysed simply and conventionally in PRA. The software reliability estimates are engineering judgments – often lacking a proper justification. The use of probabilities for software reliability is based on some common understanding rather than a proper reference. The backgrounds for this figure is however not clear, as what it really means.

This paper gives an overview of the state-of-the-art in software reliability analysis in PRA. It also presents interim results of two on-going international research activities: 1) The EU Euratom FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software and 2) the task group DIGREL of the OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) on the taxonomy of failure modes of digital components.

HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) tackles the problem of software reliability quantification using analytical and Bayesian approaches that take into consideration all the information available, in particular evidence obtained by verification and validation (V&V). Key to these approaches 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 approaches that model the development process and use development fault data to estimate the number of residual faults.

The aim of DIGREL is to develop a best practice guidelines on failure modes taxonomy for the reliability assessment of digital I&C systems for PRA. In the OECD/NEA DIGREL task, the taxonomy will be developed jointly by PRA and I&C experts. An activity focused on the development of a common taxonomy of failure modes is seen as an important step towards standardised digital I&C reliability assessment techniques in PRA. The needs of PRA guide the work, meaning, e.g., that I&C system and its failures are studied from their functional significance point of view. The taxonomy will be the basis of future modelling and quantification efforts. It will also help define a structure for data collection and to review PRA studies.

Keywords: Software reliability, probabilistic risk analysis, Bayesian belief network

2.2 ANS NPIC-HMIT 2012

This conference of the ANS (American Nuclear Society) addressing NPIC (Nuclear Plant Instrumentation & Control) and HMIT (Human-Machine Interface Technologies) was held July 22-26, 2012 in San Diego (USA). Two presentations were made on behalf of HARMONICS:

- HARMONICS — EU FP7 Project on the reliability assessment of modern nuclear I&C software
- Safety Justification Frameworks: Integrating rule-based, goal-based and risk-informed approaches

2.2.1 HARMONICS — EU FP7 Project on the reliability assessment of modern nuclear I&C software - 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.

2.2.2 Safety Justification Frameworks: Integrating rule-based, goal-based and risk-informed approaches – Abstract

The reliability and safety of the digital I&C systems that implement safety functions are critical issues. In particular, software defects could result in common cause failures that defeat redundancy and defence-in-depth mechanisms. Unfortunately, the differences in current safety justification principles and methods for digital I&C restrict international co-operation and hinder the emergence of widely accepted best practices. These differences 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 European project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) is seeking to develop a more harmonised approach to the justification of software-based I&C systems important to safety.

This paper outlines the justification framework we intend to develop in HARMONICS. It will integrate three strategies commonly used in safety justifications of I&C system and its software: rule-based—evidence of compliance to accepted standards; goal-based—evidence that the intended behaviour and other claimed properties has been achieved; and risk-informed—evidence that unintended behaviour is unlikely. The paper will present general forms of safety case that can be adapted to a variety of specific topics.

Key Words: Safety justification, I&C systems, Software

2.3 PSAM 11 and ESREL 2012

This conference on Probabilistic Safety Assessment brings together experts from various industries, research organisations, regulatory authorities and universities. It offers a platform for contacts between different fields from nuclear, process and chemical industries, off-shore and marine, space and aviation, IT and telecommunications, bio and medical technology, civil engineering and financial management. The multi-disciplinary conference is aimed to ensure the cross-fertilization of methods, technologies and ideas.

It was held June 25-29, 2012 in Helsinki (Finland). One presentation was made on behalf of HARMONICS:

- Safety case framework to provide justifiable reliability numbers for software systems

2.3.1 Safety case framework to provide justifiable reliability numbers for software systems - 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 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.

Very high reliability figures cannot be formally justified for a piece of software. Failure probabilities lower than 1E-4 are rarely claimed or justified even in a highly diversified software system, and there is not an accepted approach for the use of quantitative evaluation for software reliability between the different countries. The situation is even more difficult concerning figures for software CCF. The current state of the art for the quantification of software reliability relies mostly on holistic approaches, such as conformance to appropriate safety standards such as IEC 61508, or statistical testing.

The EU Euratom FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) 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. Key to this 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 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.

2.4 TopSafe 2012

TopSafe is a conference that provides a forum for addressing the current status and future perspectives with regards to safety at nuclear installations worldwide. It is directed at a broad range of experts in the area of nuclear safety, including professionals from the different disciplines involved in the safety of nuclear power plants, fuel cycle installations and research reactors. It is aimed at professionals coming from the research organisations, universities, vendors, operators, regulatory bodies as well as policy makers. Top level representatives of the Countries that are constructing new nuclear power plants are invited. Regulators of all individual Countries with nuclear programme are expected to contribute the Conference.

In 2012, the conference was held April 22-26 in Helsinki (Finland). One presentation was made on behalf of HARMONICS:

- Harmonised Assessment of Reliability of Modern Nuclear I&C Software — EU FP7 project HARMONICS.

2.4.1 Harmonised Assessment of Reliability of Modern Nuclear I&C Software — EU FP7 project HARMONICS – 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.

2.5 EHPG meeting in 2013

The Enlarged Halden Programme Group meeting was held on March 10-15, 2013 in Norway. Two presentations were made on behalf of HARMONICS:

- HARMONICS — EU FP7 Project on the reliability assessment of modern nuclear I&C software
- Design, implementation and V&V of a stepwise shutdown system – A case study in HARMONICS EU FP7 project.

2.5.1 HARMONICS — EU FP7 Project on the reliability assessment of modern nuclear I&C software - Abstract

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 mainly 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:

- Development of software verification methods and tools.
- Evaluation of justification frameworks for software-based systems.

- Development of approaches to the quantification of software failure rates.

Regarding software verification, the main objective is to provide direct evidence of software correctness. Three main verification approaches are to be investigated: formal verification, statistical testing, and logic coverage testing. Formal verification will address different types of safety properties, such as functional, integrity, structural and equivalence properties.
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 can be combined to justify a claim.

For the software quantification, an analytical approach is promoted to systematically define and identify critical software fault modes, which require further attention. One of the approaches to be investigated is based on the identification of failure mechanisms and the evaluation of the effectiveness of the defences provided, either as design measures or as verification measures. For software reliability quantification, Bayesian belief network based on various pieces evidence from V&V is proposed.

Different types of 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, possibly HDL designs). Each type of software may be the object of specific verification methods. For failure rates quantification and justification frameworks, system level case studies will be used.

HARMONICS has started in January 2011 will end in 2014. A collaboration project in China, called RAVONSICS (Reliability and V&V of Nuclear Safety I&C Software), has started in 2012. The paper will present the interim results of the project.

2.5.2 Design, implementation and V&V of a stepwise shutdown system – A case study in HARMONICS EU FP7 project - Abstract

The FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) aims to ensure that the nuclear industry has well-founded and up-to-date methods and tools for assessing software of computer-based safety systems. One part of the project is to develop case studies that are used to confirm that the available methods and tools can be applied with success to real systems and software.

This paper presents the work in progress to develop software for a safety function called stepwise shutdown system and to assess its safety and reliability with selected verification and validation (V&V) methods. Based on the experiences gained with the case study, the lessons learned will be written to improve the V&V methods and give guidance on their applicability and usage in the licensing processes.

The development of the case starts with writing the functional requirements specification for the system. Based on the requirements, the functionality is designed by using standard function block diagrams. The design is implemented with C++ code and also with FPGA (Field-Programmable Gate Array) technology to have two independent versions to compare and to test the different implementation technologies.

Along the design and implementation phases, various V&V activities will be performed. A software verification and validation plan will be written following the international nuclear standards, e.g., IEEE Std 1012–2004. The requirements will be verified, the design will be reviewed and verified through model checking, the implemented code will be reviewed and tested.
Finally, the direct and indirect elements of the safety justification will be collected. Conclusions will be drawn based on the coverage of the evidence and the applicability of the methods utilized in the case study.

2.6 FISA 2013 – 8th European conference on Euratom research and training in reactor systems

HARMONICS was presented at FISA 2013 conference, which was held October 14-17, 2013, in Vilnius (Lithuania). It was Co-organised by the European Commission and the Lithuanian Presidency of the EU.

2.7 NUGENIA Forum 2013

HARMONICS was also presented at the 2013 NUGENIA Forum, which was held March 18-20, in Budapest (Hungary).

2.8 ISOFIC 2014

The International Symposium on Future I&C for Nuclear Power Plants/International Symposium on Symbiotic Nuclear Power Systems (ISOFIC/ISSNP) was held August 24-28, 2014 in Jeju (Republic of Korea). Its objective is to promote academic exchanges of the topics of mainly instrumentation and control (I&C), human machine interface (HMI) technologies, and symbiosis of technology in nuclear industries. One presentation was made on behalf of HARMONICS:

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

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

3 IAEA Report on Dependability Assessment of Software for Safety I&C Systems at NPPs

The IAEA has started in May 2014 the development of a technical report on the Dependability Assessment of Software for Safety I&C Systems at NPPs. The development of IAEA reports is performed in the framework of Consultancy Meetings and Technical Meetings.

In Consultancy Meetings, the expert team debates on the contents of the report and writes draft proposals. Several members of the HARMONICS project are members of the expert team. Major results from the HARMONICS project have been proposed to the team and have been accepted (approaches to improve confidence in functional requirements, role of formal software verification, safety justification framework).

In Technical Meetings, the expert team presents the draft and main concepts to delegates from IAEA Member States, and collects their feedback. The draft proposal has been well-received, including in particular the HARMONICS results.

To this date (December 2014), there had been:

- One Consultancy Meeting, May 12-15, 2014 in Vienna (Austria).
- One Technical Meeting, September 23-26, 2014 in Daejeon (Republic of Korea).

As is usual with the development of such reports, finalisation is not expected before the end of the HARMONICS project. However, the HARMONICS members who are part of the drafting team will carry on until the report is published.

3.1 Table of contents of the Draft Report (September 2014)

Note. This table of contents reflects the current state of the draft report, and is not necessarily the final one.