EUROPEAN COMMISSION
Community research

HARMONICS

(Contract Number: 269851)

DELIVERABLE (D-N°: 5.7)

Final Public Report

Author(s):

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

REVISIONS

IND REV	STATUS DATE	PARAGRAPH	SCOPE OF THE REVISION
1.0	11/01/2015		Final version.

List of contents

1 Introduction

This document constitutes deliverable D5.7 of the HARMONICS project.

Section 2 presents the objectives and scope of the project. Section 3 presents the project work programme and the work actually performed. Section 4 presents and overview of the project results and deliverables.

2 HARMONICS Objectives & Scope

The demand of cost-effectively and reliably produced CO2 free energy is increasing. Dependence on fossil fuels and concerns over climate change are coinciding to make the case for increasing use of safe and reliable nuclear power. This means, in the near future, the construction of new nuclear power units, and the upgrade for lifetime extension of many existing units.

The reliability and safety of the computer-based systems that implement safety functions are critical issues. This is in particular due to the fact that software can usually not be proven to be completely 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 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. Relevance of I&C issues is addressed in the Strategic Research Agenda (SRA) of the EC Sustainable Nuclear Energy Technology Platform (SNETP 2009).

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 formal verification techniques means that simulated experience and formal verification 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 defensive measures to tolerate postulated residual software faults, and safety justification frameworks.

2.1 Objectives

The overall objective of the HARMONICS 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 of Gen-II and Gen-III NPPs. It has taken advantage of the aforementioned advances to propose systematic and consistent, yet realistic and practical approaches for software assessment. These approaches address critical phases of the software and system lifecycles, from requirements specification to verification and validation.

In addition to the core project team, a larger “end user group” has been constituted with other interested stakeholders (utilities, regulatory bodies, suppliers) to review and give feedback on the project work. Thus, the project has fostered an international consensus based on a sound scientific and technical approach, and hopefully provides a good basis for harmonisation.

2.2 Scope

The project addresses three key issues: software verification & validation (V&V)[1], software safety justification, and quantitative evaluation of software reliability. The term “software reliability” is used throughout this document as a shortcut for “software-related aspects of system reliability”. The focus has been mainly on I&C systems performing category A functions (as defined by IEC 61226) which is the highest safety category in NPP. To support research activities on these three main issues, the project has investigated and developed theories, techniques and tools as necessary. In addition, the feasibility of the developed approaches has been experimented and demonstrated with selected case examples provided by the project participants and the end user group.

Regarding software V&V, the project has analysed the state of the art, proposed innovative techniques and tools, and provided practical guidelines for applying some of these techniques and tools. V&V may be used to ascertain the effective implementation of fault avoidance measures, such as compliance to complexity limits, to design and coding rules, to specified development processes and methods. V&V may also be used for fault detection (for their subsequent removal), by applying techniques such as simulation and testing, formal verification, inspection. Lastly, V&V may be used to ascertain the effective implementation of design measures taken to guarantee that certain types of postulated residual software faults will not lead to failures or common cause failures.

Regarding software safety justification, the HARMONICS project has built on current practices and on results of previous Euratom FP6 research projects, namely CEMSIS (Cost-Effective Modernisation of Systems Important to Safety) and BE-SECBS (Benchmark Exercise on Safety Evaluation of Computer Based Systems). In particular, it proposes a framework integrated into the overall system safety justification, and based on the complementarity and integration of the rule-based, the goal-based and the risk-informed approaches. In particular, the project has analysed the domain of applicability and acceptability of each approach, and provides practical guidelines based in particular on the information gathered with the proposed V&V techniques.

Regarding software reliability, the framework integrates quantitative software reliability claims in the overall software and system safety justification. In particular, the project has

[1] Validation = Test and evaluation of the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements. (IEC 60880)
Verification = Confirmation by examination and provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity. (IEC 60880)

investigated the nature and justification for any reliability claim limit. It also proposes practical approaches to estimate the values needed for Probabilistic Safety Assessments (PSA): probabilities of failure on demand, conditional probabilities of common cause failures (so-called beta-factors), and possibly frequencies of spurious actuations that lead to initiating events. To this end, the project has analysed the current state of the art, which is usually based on holistic approaches (e.g., conformance to international standards, collection and analysis of operating experience, statistical testing and corresponding trade-offs between realism and scale of tests). It also proposes a more analytical approach that takes into consideration all the information obtained by V&V and organised by the software safety justification. This approach can be based on the identification of failure modes of interest, of the failure mechanisms that could lead to these modes, and on the effectiveness of the measures taken to prevent given mechanisms. It will also consider the implication of I&C architectures (levels of defence and diversity) and implementation technologies in the system safety justification.

3 Work programme & work performed

The overall strategy to reach the objectives is based on the following steps of activities:

- Clarification of needs, practices and experiences. Exchange of information between EU and China. Specification of the scope, target and objectives of the approach to be developed in the next step. This activity shall facilitate the co-operation between EU and China partners.
- Development of common approaches to the assessment and justification of the reliability of safety software. The project will take advantage of the experience from the recent licensing processes and research projects (including EU FP5 projects BE-SECBS and CEMSIS). The approach will be based on the Claim-Argument-Evidence approach.
- Test of the approaches in case studies.
- Assessment of results from the case studies. Critical assessment applicability of approaches and lessons learnt.
- Dissemination of results. An important part of the whole project is to get feedback from a large group of advisories and end users. The advisory and end user group will include utilities, regulators and vendors from EU and China. Advisory and end users workshops will be arranged. Contacts with international organisations like IAEA, OECD/NEA will be utilised.

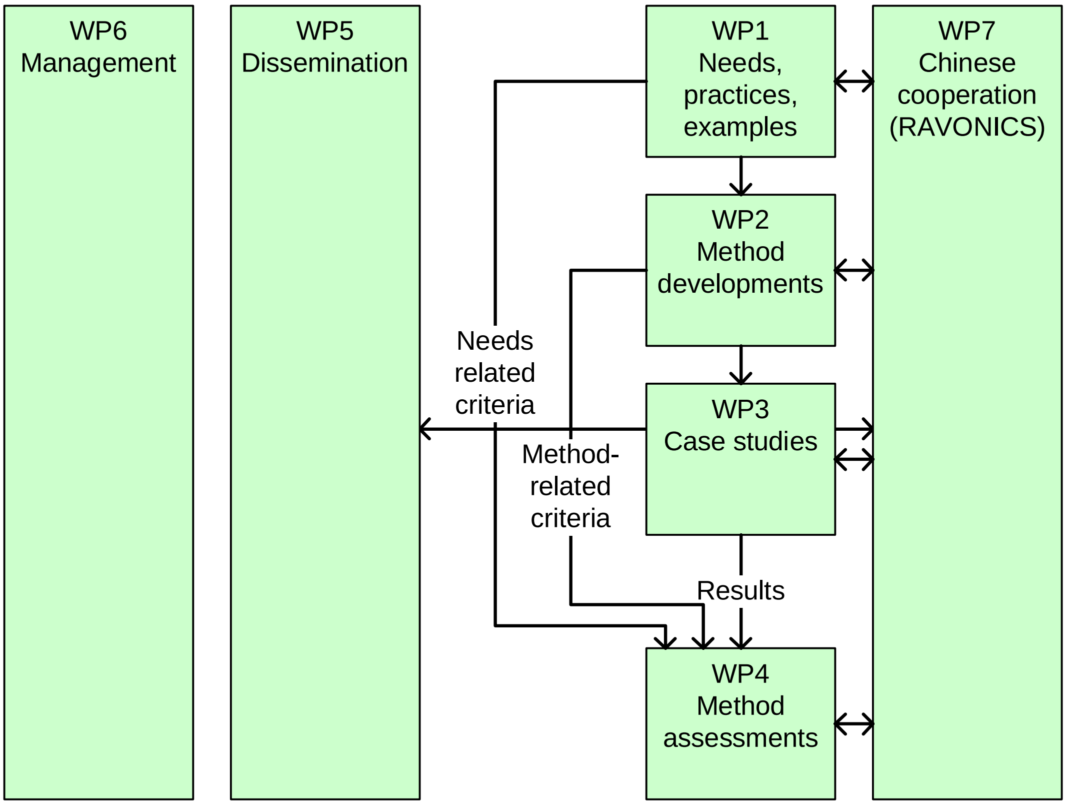

Figure 1. Logical dependencies diagram.

The research activities were carried out by two parallel projects (the EU project HARMONICS and the corresponding Chinese project RAVONICS). For various reasons, RAVONSICS has been unable to start in due time, and cooperation between the two projects has been limited.

3.1 WP1 - Needs, practices, experiences

The objectives of the WP1 were:

- To reduce the technical gaps between Chinese and European participants on safety-critical software reliability assessment and V&V.
- To establish a common base for the project by exchanging information, knowledge, and experiences
- To clarify the needs of China and Europe for safety-critical software reliability and V&V.

A kick-off workshop was organized in Shanghai, China at the beginning of the project. After that, HARMONICS prepared a needs analysis questionnaire that was sent to over 70 nuclear I&C experts in Europe representing utilities, regulators, vendors, research organizations and TSOs. A needs analysis report was issued based on the answers received, and also on the discussions in the first End User workshop organized in Helsinki, Finland. The results of the analysis served as a basis to determine priorities for WP2.

3.2 WP2 - Methods development

Work on methods development focused on the following topics:

- Confidence in functional and timing requirements specification: experience in the nuclear industry and in other safety critical industries has shown that flaws in functional and timing requirements could result in undesirable behaviours that are detected late in the development process, or worse, during operation.
- Complexity and structural analysis of functional diagrams: the purpose here was to identify the diagrams of higher complexity than average and their relationships with the other diagrams, in order to help determine an appropriate verification and validation approach.
- Formal software verification: an approach to the formal verification of the complete software of a class 1 digital I&C system (implementing Category A functions) has been developed
- Safety justification framework, which provides:
  - A set of principles.
  - A strategy based on understanding the behaviour of the system and its interactions
  - An approach to developing, communicating and challenging the understanding based on claims, argument and evidence (CAE).
  - Guidance on the underlying concepts of CAE and an extension of them into generic “blocks” that provide the basis for domain and problem specific templates.
  - A high level process for deploying the framework and detailed guidance on specific issues.
- Formal software verification: an approach to the formal verification of the complete software of a class 1 digital I&C system (implementing Category A functions) has been developed and expressed in the format of the Safety justification framework.
- Quantification of software reliability: the approach developed provides justifiable reliability numbers for software of computer-based safety systems in nuclear power plants. These numbers may be used to represent the software-related aspects of the computer-based systems in probabilistic safety assessments (PSA).
- Stepwise Shutdown System: development of a simple case study that can serve as the basis for the public case study.

3.3 WP3 - Case studies

5 case studies were made to help develop the methods and to confirm their applicability:

- A Backup Power Supply (BPS) case study has been made to develop the proposed approach for improving confidence in functional and timing requirements.

- The complexity and structural analysis was test cased on a complete, real-life application (not of Category A).
- Formal software verification and the safety justification framework have been test cased on the complete software of a class 1 digital I&C system.
- A case study was developed to illustrate how the Claims-Argument-Evidence (CAE) structuring approach and the research on reliability can be used to provide a template and discussion of the issues that need to be addressed in justifying software reliability, using a combination of techniques (including statistical testing).
- Stepwise Shutdown System: development of a simple case study that serves as the basis for the public case study.

3.4 WP4 - Methods assessment

WP4 had two main objectives:

- To assess the results of the approaches and methods developed by WP2, based on the case studies of WP3.
- To present recommendations to improve the proposed approaches to safety justification.

The evaluation was performed in several steps during the project. The first step was made when different verification methods were reported in D2.1 Verification methods. The report contains the first impressions and already existing experiences of the applicability of the methods.

The second step was the analysis of the results of the case studies where the developed approaches were utilized in 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 phase they should be used and how much effort the utilization takes.

The third step was the evaluation done by the HARMONICS End User Group. The methods and the case studies were presented at the second HARMONICS End User Workshop, and each participant filled in an evaluation form. In addition to individual evaluations and feedback, several working groups consisting of the end users (workshop participants) were formed to discuss the topic and finally present questions, ideas, feedback, open issues and conclusions on the approaches.

The criteria that the end users used for the evaluation of the proposed approaches for safety justification can be divided in two categories: the evaluation of the case study itself and the evaluation of the methods and tools. The criteria are summarized below.

Case studies:

- How the case study represents the problems and challenges of the respondent?

- Does the case study illustrate the proposed method and its usage?
- Is the case study extensive enough?
- Is the case study too complex to understand and digest?

Method and tools:

- Are the presented methods and tools useful in the context of the respondent?
- Are the presented methods and tools applicable in real projects?
- What kind of improvement they would bring to the current practice?
- What kind of drivers for, or barriers to adoption of the presented methods and tools there are?

In addition to the predefined questions of the evaluation form, the end users were also asked to make suggestions and remarks to widen the perspective and to cover issues not addressed by the evaluation form.

Working in groups and discussing with other experts clarified the overall understanding on the current utilization of the safety justification approaches in the European organizations. Despite the positive development on the adoption of the presented approaches and methods during the last few years, there are still several topics that need more explanation, education and development to bring them to standard practice in European organizations.

3.5 WP5 - Dissemination

The objective of the WP5 was to inform all potential end users of the results of the project, and to promote the use of the methods and tools proposed. The dissemination actions can be divided into three main categories:

- Communication actions, where the project results are presented in professional journals, conferences, lectures, curriculum in colleges, etc. A Dissemination Plan was developed to identify and maintain a list of communication actions throughout the duration of the project. (For more information on these communication actions, see D5.6 Journal articles, conference papers, other publications.)
- The development of a Public Case Study. This action involved all project participants. Its objective was to document the complete approach proposed by the project in a report (D5.4 Public Case Study) not be restricted by any NDA.
- Organisation of End Users Workshops to inform the end user community. One has been organised early in the project, and another at the end of the project. (For more information on these workshops, see D5.3 End User Workshop 1 Proceedings and D5.5 End User Workshop 2 Proceedings.)

4 Results

4.1 Interactions with stakeholders

The interactions with stakeholders are formalised in four HARMONICS deliverables: D1.2, D5.3, D5.5 and D4.2.

4.1.1 D1.2: Needs analysis report

Deliverable D1.2 gives a summary of the answers of the questionnaire sent to the identified end users in the beginning of the project to clarify the current practices and needs of European organizations for safety-critical software reliability and V&V. When appropriate, a reference to the "Common position of seven European nuclear regulators and authorised technical support organisations, ver. 2010" is made as a point of comparison. The synthesis of the answers also reflects the summary of a similar type of questionnaire from the previous Euratom FP6 project CEMSIS. This deliverable is not public. Its table of contents is as follows:

4.1.2 D5.3: End User Workshop 1 proceedings

This deliverable is public and can be downloaded from the HARMONICS website. Its table of contents is as follows:

4.1.3 D5.5: End User Workshop 2 proceedings

This deliverable is public and can be downloaded from the HARMONICS website. Its table of contents is as follows:

4.1.4 D4.2: Recommendations to improve the proposed approach to safety justification

This deliverable presents the recommendations to improve the proposed approaches to safety justification received from the project's end user group consisting of various representatives of licensees, utilities and nuclear regulators. It is not public. Its table of contents is as follows:

4.2 Summary of scientific deliverables

The technical results are formalised in five HARMONICS deliverables: D2.1, D2.2, D2.3, D3.2, and D5.4.

4.2.1 D2.1: Verification methods

In order to understand some of the motivation and application of the deliverable, an introduction to the overall approach to safety justification is provided in Section Error! Reference source not found.. The details of the approach– the safety justification framework– is the subject of deliverable, D2.2. Section Error! Reference source not found. summarises the technical aspects of the Verification Methods, which are described in more detail in the Annexes, and Section 5 presents some conclusions and discusses future work.

Most of the substantive technical work is described in the Annexes. Annex 1 addresses the High-Level Functional & Timing I&C System Requirements that form the basis for assessing whether the system behaves as required. Annexes 2 and 3 on Formal Analysis and Annex 4 on Statistical Testing provide details of these two approaches, which provide direct evidence of how the product behaves. Annex 5 on Complexity Analysis describes an approach that provides some information on structural properties of the software.

This deliverable is not public. Its table of contents is as follows:

Annex 2 Formal Verification

A2.1 Introduction
A2.2 Background
A2.3 Description of the Method
A2.4 Comments
A2.5 Roles in Safety Justification Triangle

Annex 3 Formal verification – Model Checking

A3.1 Introduction
A3.2 Background and scope
A3.3 Description of model checking
A3.4 Role of model checking in safety justification
A3.5 Issues

Annex 4 Statistical Testing

A4.1 Introduction
A4.2 Background to statistical testing
A4.3 Method
A4.4 Roles in safety justification triangle
A4.5 Summary and conclusions
A4.6 Addendum: Dealing with non-determinism

Annex 5 Complexity analysis

A5.1 Introduction
A5.2 Background to Complexity Analysis
A5.3 Complexity Analysis / Method
A5.4 Complexity Analysis in Safety Justification
A5.5 Benefits and Limitations
A5.6 Process and Application

4.2.2 D2.2: Safety justification framework

This deliverable defines a framework for justifying the use of software in systems implementing Category A nuclear functions. The framework provides

- A set of principles.
- A strategy based on understanding the behaviour of the system and its interactions.
- An approach to developing, communicating and challenging the understanding based on claims, argument and evidence (CAE).
- Guidance on the underlying concepts of CAE and an extension of them into generic "blocks" that provide the basis for domain and problem specific templates.
- A high level process for deploying the framework and detailed guidance on specific issues.

Additional deliverables contain more guidance on the techniques deployed in the framework (D2.1 on verification techniques and D2.3 on software reliability). In addition, there are supporting case studies in D3.2 and a public domain case study in D5.4.

This deliverable is not public. Its table of contents is as follows:

4.2.3 D2.3: Quantification of software reliability

This deliverable describes the approach developed in HARMONICS to provide justifiable reliability numbers for software of computer-based safety systems in nuclear power plants. These numbers may be used to represent the software-related aspects of the computer-based systems in probabilistic safety assessments (PSA).

This deliverable is not public. Its table of contents is as follows:

4.2.4 D2.4: Complexity and structural analysis

The overall objective of complexity analysis of the complete application software of a digital I&C system is the identification of complex Function Diagrams (FDs), according to various complexity measurements. The overall objective of structural analysis is the identification of manageable subparts of the complete application software, based on the dependencies between FDs.

Moreover, complexity analysis and its extension to structural analysis support the identification of meaningful and manageable subsets for V&V of the application specific I&C-software.

This deliverable is not public. Its table of contents is as follows:

4.2.5 D3.2: Case studies

The case studies that were implemented are described in detail in five Appendixes (A to E):

- Appendix A addresses the verification that I&C functional and timing requirements are adequate and complete. The case study is the I&C system of a Backup Electric Power Supply system.
- Appendix B addresses the issue of software complexity analysis. The case study is the complete software of a typical reactor protection system.
- Appendix C addresses the formal software verification of the complete software of a typical reactor protection system. The case presents a formal verification strategy in a Claim-Argument-Evidence structure as suggested by WP2.2 on Safety Justification Framework. Thus, the case study is also an illustration of the results of WP2.2. A number of the formal verification tools necessary to provide evidence have been developed during the HARMONICS project or were pre-existing. However, not all necessary tools are available yet, and further work still needs to be done.
- Appendix D addresses the issue of failure rate assessment for software, based on statistical testing.
- Appendix E illustrates all the HARMONICS results on a simple system, the Stepwise Shutdown System.

This deliverable is not public. Its table of contents is as follows:

Appendix D: Justification of a Reliability Quantification Claim

Appendix F: Stepwise Shutdown System

4.2.6 D5.4: Public case study

This deliverable presents the main results of the project in the framework of a public case study that can be freely disseminated. Section 2 presents the main HARMONICS principles. Section 3 provides an overview of the public case study. Section 4 presents an application of complexity and structural analysis. Section 5 showcases the validation of functional and timing requirements specification. Section 6 showcases the formal verification of the software implementation and presents an application of the claim-argument-evidence (CAE) based safety justification framework. Section 7 showcases the quantification of the probability of failure on demand, based on statistical testing.

The deliverable is public and can be downloaded from the HARMONICS website. Its table of contents is as follows:

4.3 Dissemination of HARMONICS results (papers, conferences, IAEA, etc.)

The abstracts of the presentations mentioned hereafter can be found in D5.6. – Journal Articles, Conference Papers, Other Publications, which is a public report that can be freely downloaded from the HARMONICS website.

4.3.1 14th International Workshop on Nuclear Safety and Simulation

This workshop was held October 23-24 2012 in Harbin (China). It is organised by the Harbin Engineering University, one of the members of RAVONSICS. Two presentations were made on behalf of HARMONICS:

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

4.3.2 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

4.3.3 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.

In 2012, 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

4.3.4 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

4.3.5 EHPG meeting in 2013

The Enlarged Halden Programme Group meeting was held 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

4.3.6 FISA 2013 - 8th European conference on Euratom research and training in reactor systems

HARMONICS was presented at this 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.

4.3.7 NUGENIA Forum 2013

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

4.3.8 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

4.3.9 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. Several members of the HARMONICS project are part of the expert team that is drafting the report. 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).

As usual, the finalisation of the report 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.

5 Conclusion

Harmonics has focused on justifying the software of systems implementing Category A nuclear safety functions. As part of this we have proposed a safety justification framework provides that is based on set of core principles. Table 1 outlines how the Harmonics principles have been addressed in the project.

Principle	*Contribution of Harmonics*
1. Effective understanding of the hazards and their control should be demonstrated.	The development of high-level requirements about system and plant behaviour explicitly addressed in the framework (and supporting case studies in D3.2) and supported by the formal analysis techniques in D2.1. Complexity and structural analysis provides an understanding of the overall software structure and the role of the different parts of the software.D2.4 The approach to take is addressed by property and vulnerability aspects of the strategy triangle in D2.2. The systematic use of CAE can promote and record understanding of the system and its justification D2.2
2. Intended and unintended behaviour of the technology should be understood.	Supported by the formal analysis techniques of D2.1. Addressed by property and vulnerability aspects of the strategy triangle and the CAE blocks instantiated with relevant claims, can raise the issues to be addressed (D2.2) Complexity and structural analysis provides an understanding of the overall software structure and any unintended dependencies can be identified (D2.4) CCF analysis and the techniques described in D2.3 can provide a means for modelling the risks from unintended interactions.
3. Multiple and complex interactions between technical systems and also human systems to create adverse consequences should be recognised.	Formal analysis provides a technique for this (but interaction with human systems outside scope of Harmonics). Statistical testing can reveal unexpected behaviour that might be significant although not the main goal of the testing.

Principle	*Contribution of Harmonics*
4. Active challenge should be part of decision making throughout the organisation. Needs of all stakeholders to understand and challenge the case should be taken into account in its structure and presentation.	The justification framework (D2.2) provides a basis for implementing or reinforcing effective challenge throughout the organisation. It does not include organisational aspects as such. The use of CAE templates provides a structured way for guidance to challenge their use. The use of explicit claims and arguments makes the justification more transparent and should facilitate challenge. (D2.2 and D5.4) The underlying process for using the framework includes a challenge and response cycle. (D2.2) The use of the analysis techniques and formal analysis (D2.1, D2.4) provide powerful methods for confidence building and challenge.
5. Lessons learned from internal and external sources should be incorporated.	Addressed by vulnerability part of triangle and in the use of CAE templates and guidance that incorporate lessons learned (D2.2). Addressed by compliance with standards as they are considered to contain "experience" (but not elaborated in Harmonics as a requirement for compliance for systems performing Cat A functions is assumed).
6. Justification should be logical, coherent, traceable, accessible, repeatable with a rigour commensurate with the degree of trust required of the system.	The use of CAE supports a logical, coherent, traceable and accessible approach (D2.2). Templates support repeatability, and the introduction of blocks and templates provides a graduated approach to increasing rigour in a case as does the use of strong formal analysis techniques and statistical testing (D2.2, D3.2, D5.4).

Table 1: Description of the Harmonics principles and the contribution of the project

Additional Harmonics deliverables contain more guidance on the techniques deployed in the framework (D2.1 on verification techniques and D2.3 on software reliability). In addition, there are supporting case studies in progress and a public domain case study will be delivered later in 2014. While the framework is focused on systems implementing Cat A nuclear safety functions, there are many aspects

It should be born in mind that these results are the products of research and, while some aspects are mature, the combined approach needs experimentation and validation. There are some aspects that are immature and need more reviewing and trialling.

For further information, contact HARMONICS participants. Contact information can be found at http://harmonics.vtt.fi/publications.htm.