EUROPEAN COMMISSION

Community research

HARMONICS

(Contract Number: 269851)

DELIVERABLE (D-N°:5.3)

1st HARMONICS Workshop Proceedings
Helsinki, April 16-17, 2012

Author(s): Nguyen Thuy, EDF

Reporting period: e.g. 12/01/11 – 11/07/12

Date of issue of this report: 20/06/12

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/Jan-Erik Holmberg	1	
EDF/Nguyen Thuy	1	
Adelard/ Sofia Guerra	1	
ISTec/Josef Märtz	1	
SSM/Bo Liwång	1	
Workshop participants	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	20 /06/12	
Reviewed by	Robin Bloomfield, Adelard	5/7/12	
Approved by	Jan-Erik Holmberg, VTT	5/7/12	

REVISIONS

IND REV	STATUS DATE	PARAGRAPH	SCOPE OF THE REVISION
1.0	15/06/12	All	Approved version

List of contents

1 Introduction

This document constitutes deliverable D5.3 of the HARMONICS project. It collects all the material presented during the 1st HARMONICS workshop held in Helsinki, April 16th and 17th, 2012. It also summarises the discussions and suggestions made by the participants.

Section 2 provides a definition for acronyms used. Section 3 presents the workshop objectives. Section 4 lists the participants to the workshop. Section 5 recalls the agenda of the workshop. Section 6 summarises the presentations and Section 7 workshop discussions. Workshop conclusions are given in Section 8. Presentations are in Appendix 1.

2 Glossary

BBN	Bayesian Belief Network
CAE	Claim-Argument-Evidence
CCF	Common-Cause Failure
CEMSIS	Cost-Effective Modernisation of Systems Important to Safety
CINIF	Control & Instrumentation Nuclear Industry Forum
EDF	Electricité de France
EC	European Commission
ENEF	European Nuclear Energy Forum
ENSREG	European Nuclear Safety Regulators Group
EU	European Union
EUG	End User Group
FPGA	Field Programmable Gate Array
HARMONICS	Harmonised Assessment of the Reliability of MOdern Nuclear I&C Software
I&C	Instrumentation & Control
IEC	International Electrotechnical Commission
IGD-TP	Implementing Geological Disposal of Radioactive waste
ISO	International Standards Organisation
MELODI	Multidisciplinary European Low Dose Initiative
NRSC	Nuclear & Radiation Safety Centre
OE	Operational Experience
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
RAVONSICS	Reliability And V&V of Nuclear Safety I&C Software
SIL	Safety Integrity Level
SJF	Safety Justification Framework
SNE-TP	Sustainable Nuclear Energy Technology Platform
SSM	Swedish Radiation Safety Authority
US NRC	United States Nuclear Regulatory Commission
V&V	Verification & Validation
VTT	Technical Research Centre of Finland

3 Workshop Objectives

Nuclear I&C standards development and harmonisation have been on-going for over 25 years, but different countries still have different requirements for category A digital I&C systems. The workshop discussed the challenges with V&V, reliability assessment and safety justification with the industry and regulators, in order to foster an international consensus based on a sound scientific and technical approach.

4 Participants

Title	*First name*	*Last name*	*Company / Organization*	*Country*
Prof	Robin	Bloomfield	Adelard LLP	UK
Mr	Ruidong	Dai	State Nuclear Power Automation System Engineering Company	China
Mr	Ian	Donnellan	EDF Energy	UK
Dr	Sofia	Guerra	Adelard LLP	UK
Mr	Juha	Halminen	Teollisuuden Voima Oyj	Finland
Mr	Karl	Hamar	Hungarian Atomic Energy Authority	Hungary
Mr	Hannu	Harju	VTT	Finland
Mr	Atte	Helminen	TVO	Finland
Mr	Jan-Erik	Holmberg	VTT	Finland
Mr	Jari	Hämäläinen	VTT	Finland
Mr	Kalle	Jänkälä	Fortum Power and Heat Oy	Finland
Dr	Sébastien	Labbé	EDF Research & Development	France
Mr	Bo	Liwång	Swedish Radiation Safety Authority	Sweden
Mr	Sami	Matinaho	Fortum Power and Heat Oy	Finland
Mr	Josef	Märtz	ISTec	Germany
Mr	Thuy	Nguyen	EDF	France
Mr	Emil	Ohlson	Forsmarks Kraftgrupp AB	Sweden
Mr	Rainer	Poppenborg	Horizon Nuclear Power	UK
Ms	Wietske	Postma	NRG	Netherlands
Mr	Jim	Thomson	Invensys	UK
Mr	Janne	Valkonen	VTT	Finland
Mr	Peter	Wyman	Horizon Nuclear Power	UK
Mr	Martti	Välisuo	Fortum	Finland
Mr	Georges	Van Goethem	European Commission	Belgium

5 Workshop Agenda

Tuesday April 17th, 2012

Welcome address
Introduction of each participant
Introduction to the HARMONICS project

- Background & Objectives
- Overall organisation
- Role of the End User Group (EUG)

Introduction to the RAVONSICS project
Overall presentation of the research tasks in WP1-WP4
WP1 (Users Needs) & WP4 (Evaluation)

- Presentation and results
- Preparation of the group discussion

Break

- Discussion in groups
- Presentation of groups conclusions
- Round table discussion

Wednesday April 18th, 2012

Summary of Tuesday's discussions
Welcome address by Euratom
RAVONSICS technical presentation
Break
WP2 (Methods) & WP3 (Case Studies)

- Introduction
- Safety justification framework
  - Global Example: Application to an overall I&C architecture
  - Detailed example: Application to a specific I&C function

Lunch

Common Regulatory Positions
WP2 and WP3, Continued - Challenging issues

- Software architecture and complexity analysis
- Statistical testing
- Quantification of software failure probabilities

Break
Round table comments from members of EUG
Project responses
Workshop conclusions

6 List of Presentations

The following presentations were made during the workshop (the corresponding presentation slides are provided in Appendix 1):

- HARMONICS - Overview (J.-E. Holmberg)
- RAVONSICS - Brief Introduction (Dai Ruidong)
- HARMONICS - Overall WP1-WP4 Presentation (N. Thuy)
- HARMONICS WP1 - Needs, Practices, Experiences (J. Valkonen)
- HARMONICS WP4 - Assessment Criteria (H. Harju)
- Group Discussion
- Round Table Discussion
- Summary of Day 1, April 17th, 2012 (J.-E. Holmberg)
- The EU Framework Programme for Research and Innovation 2014–2020 (G. van Goethem)
- RAVONSICS - Introduction (Dai Rui dong)
- HARMONICS WP2 Methods - Safety Justification Framework (R. Bloomfield, S. Guerra)
- HARMONICS WP2 Methods - Quantification of Failure Probabilities (N. Thuy)
- Some Comments from a Regulator (B. Liwång)
- HARMONICS WP2 Methods - Improving Functional Requirements Specification (N. Thuy)
- HARMONICS WP2 Methods - Statistical testing (N. Thuy)
- HARMONICS WP2 Methods - Structure and Complexity of Digital I&C (J. Märtz)

7 Summary of Discussions

7.1 HARMONICS - Overview

A question was raised on US involvement, or rather lack of it. The main answer is that this is being handled outside of the HARMONICS project. In particular:

- HARMONICS is a research project that aims at informing the regulatory projects.
- Several HARMONICS members do have scientific and technical discussions with non-European regulators, in particular with US NRC.
- Also, as was shown by the different I&C requirements and architectures for the EPR reactors in Finland, France and the UK, harmonization in Europe is far from being achieved.

7.2 RAVONSICS - Brief Introduction

Participation of RAVONSICS members to the workshop has been hampered by the Chinese government's more stringent requirements for visas. Internal meetings, research investigations and case studies have started. One point highlighted was the strong interest of RAVONSICS in the FPGA technology.

One question was raised regarding the participation of the Chinese Safety Authority, the NRSC, as it no longer appears in the list of RAVONSICS partners. The answer was that they may join the project later.

7.3 HARMONICS - Overall WP1-WP4 Presentation

No significant questions were raised during the presentation.

7.4 HARMONICS WP1 - Needs, Practices, Experiences

Regarding the Questionnaire, it was noted that there were no vendors responses. Invensys offered to see if they could respond.

7.5 HARMONICS WP4 - Assessment Criteria

No significant questions were raised during the presentation.

7.6 Group Discussion

The Group Discussion was organised into four separate groups. Each group had 30 min to discuss the topic(s) of their choice, with HARMONICS members acting as moderators. Then, each group had 5 min to present their conclusions. Six discussion topics were proposed:

- Software reliability quantification
- Operating experience
- Verification and validation
- Statistical testing
- Harmonisation
- Other key topics in digital I&C systems

7.6.1 Group **A**

Topic: software reliability quantification
Conclusions:

- Is quantification of software reliability useful? The group concluded that Yes, but it is difficult to estimate. In particular, one needs to be careful about what reliability we are talking about: different failure modes might have different reliability.
- Is it mandatory? Yes, for PRA. For licensing, it is useful, but not necessarily mandatory. PRA also helps defines reliability requirements for software.
- How to do it? There is no good answer. One needs to be comfortable with the approach. It depends on authority and how everybody will be happy with approach. It is difficult to get information from vendors to support reliability estimation.

7.6.2 Group **B**

Topic: software reliability quantification
Conclusions:

- Software failure rate is not significant to CCF.
- It is an estimate only – no accurate figure.
- We need to trust functional specification as well as implementation.

- We also need to consider reliability now and in the future (during lifetime of the I&C system).

Topic: operating experience
Conclusions:

- OE is useful but not enough. There is the need to consider incentives and cost sharing/barriers for the collection and use of OE.
- There are large differences between vendors on the quality of documentation, what information they have, standards they use, how up to speed with nuclear requirements they are.

7.6.3 Group C

Topic: software reliability
Conclusions:

- There are significant difficulties with software reliability estimation, in particular due to differences in regulatory requirements.
- There is also a lack of guidance on how to apply standards and how to make use of quantification, lack of guidance on quantification methods, and lack of trust on numbers.
- However, contribution of software to system unreliability is small.
- When numerical reliability estimation is required, numbers are often too optimistic or too conservative. How can we make them realistic?

Topic: Operating experience
Conclusions:

- There are challenges to generalise across applications for some components. It is useful for smart devices.

7.6.4 Group D

Topic: harmonisation
Conclusions:

- Is harmonisation about standards or acceptability of standards?
- Vendors choose which standards to use. They might need to meet the highest common denominator.
- If we think about Claims Argument Evidence (CAE), there are also issues of harmonisation for each of the components of CAE.
- Some consequences of lack of harmonisation include: use of analogue devices, reverse engineering, use of FPGAs.
- One possible solution for functional complexity is to map complex functions into testable components.
- There was discussing about different approaches taken by different sectors.

7.7 Round table discussion

During the round table discussion, Karl Hamar made two points:

- Licensing Category A is easier than licensing Category B for a number of reasons, including simpler functions, simple properties, more rigid implementation, good compilers use, simpler numerical calculations.
- Hungary is considering introducing SIL-based standards and in some cases using them instead of nuclear standards (specially for Category B and Category C) to reduce costs.

7.8 Summary of Day 1

Jan-Erik Holmberg, the project coordinator, summarised the discussions as follows:

- Should the project address harmonisation with US requirements and standards (IEEE)?
- Category A systems easier to assess than Category B
- No universally applicable solutions to software reliability quantification – struggle between too optimistic and too pessimistic estimates
- Operating experience is useful but not enough
- Assessment of the functional complexity is considered important
- The interest in FPGAs is increasing
- We can take into account what other industries are doing.

7.9 The EU Framework Programme for Research and Innovation 2014-2020

Horizon 2020: 80 billion € research and innovation funding programme (2014 -2020)

Three main points:

1. Excellent science
2. Industrial leadership
3. Social challenges – proposed funding of "Secure, clean and efficient energy" is 5,8 billion €.

EURATOM

- The EC is in charge of promoting and facilitating nuclear research activities in the MSs and to complement them through a Community Research & Training programme
- To encourage the implementation of the (national) research programmes, the EC can:
  - bring financial support to research contracts,
  - provide to MSs, people or enterprises, facilities, equipments or expert assistance,
  - stimulate joint funding (from MSs, people, enterprises)
- The general objective of the Euratom Programme is to improve nuclear safety, security and radiation protection, and to contribute to the long-term decarbonisation of the energy system in a safe, efficient and secure way.

The role of the Technological Platforms

- Safety authorities (High level group ENSREG - European Nuclear Safety Regulators Group)
- Stakeholders (European Nuclear Energy Forum ENEF)
- Research / Innovation (Technology Platforms:
  - SNE-TP = Sustainable Nuclear Energy Technology Platform
  - IGD-TP = Implementing Geological Disposal of Radioactive waste
  - MELODI = Multidisciplinary European Low Dose Initiative

Georges van Goethem emphasised direct contacts to persons of appropriate platforms.

The European Commission will put more and more funding on learning "Erasmus for all", 17 billion Euros during 2014–2020. It also wants to continue cooperation with the non-European partners.
Nuclear is a common concern, if something happens it concerns everyone.

7.10 RAVONSICS - Introduction

Q: HARMONICS deals with Category A software, what about RAVONSICS?
A: Only Category A.

Q: How to cooperate with HARMONICS?
A: Exchanging deliverables.
Q: But exchanging deliverables is not cooperation, cooperation means also working together.

Q: Internal meetings of RAVONSICS?
A: There are only proposals; I will give them to HARMONICS.

Q: Why do you work with statistical testing? Do you think it is beneficial? Is it required from regulator?
A: It is not required by regulator. The answers of the questionnaire are quite diversified.

Q: RAVONSICS had a kick off in February, what are the next steps?
A:

- Signature of CA is in 25th February
- Discussion of CooA is on-going.
- Discussion for clarifying research contents is on-going.

Q: How about next RAVONSICS meetings?
A: We have not fixed schedule. We will organize a meeting when we need one.

Q: What is the role of standards in China, are they mandatory or just guidelines?

A: There are so many different standards at the moment. Most of the Chinese standards are translated from IEEE or IEC. The Chinese government wants to harmonize the technical aspects.

Q: You talked about case studies, are you going to do case studies on systems provided by Chinese vendors or foreign vendors?
A: Chinese providers, but I do not have detailed information.

Q: The focus of RAVONSICS is in FPGA and also in software. What type of systems are you going to investigate?
A: We have something proposed by Westinghouse.

Q: Chinese consortium has totally 6 partners. Have they agreed on the technical content?
A: We have organized an internal working meeting.

Q: Do all the Chinese partners have the same expectations? Do they share that view?
A: All Chinese partners have common expectations. They need that kind of technology for confidence building.

7.11 HARMONICS WP2 Methods - Safety Justification Framework

Q: Is my specification correct? Does my system apply specification? I should know how I assess safety in the end.
A: Develop CAE structure. Change arguments feasibility. Reduce importance to compliance with standards.
Harmonizing – Templates everyone uses

Q: How to sell the idea to Americans? Are standards needed? Is safety case enough? How it is in practice?
A: All American stakeholders are in NPIC-HMIT conference where HARMONICS has a presentation. We have to go through all channels, we don't have direct access.
In practice, product must be seen at once, directly, not step by step.
Lot of safety issues were not covered using some specific standards.

7.12 HARMONICS WP2 Methods - Quantification of Failure Probabilities

Q: You cannot know all failure modes of processors!
A: We don't need to – only failure modes of functions.
Q: You cannot prove that beta is not 1.
A: We shall see. If you always assume worst cases, you end up with architectures that are stupid.

Quantification ultimately relies on informed judgement. Convincing that a reasoning is appropriate requires negotiation

7.13 Comments from a Regulator

Q: Who should create the safety justification?
A: In Sweden, no organization can handle all the aspects. The overall strategy of safety justification should be under responsibility of the utility, but support and close cooperation with the supplier is needed (e.g. competence in modern I&C)

Q: What's new compared to CEMSIS?
A: SJF is more mature, but what remains problematic is the amount and scope of documentation.

Q: What would be a possible follow-up project, what are the next big steps?
A: There will be some remaining safety justification problems, due to the fact that plants are increasingly complex. Also, what should be documented and where, during development, in order to properly feed the subsequent licensing phase?

Q: What should be the regulatory involvement in safety categorization?
A:

- This is an important issue, due to the increasing number of systems (post Fukushima)
- There is a need for international consensus on I&C principles and understanding of diversity (cf. the three different European EPR I&C designs).
- Sources of differences are the unclear definition of diversity, national requirements, diverging interpretations of international standards.

Q: Would it have helped if ASN had been part of WENRA?
A: They didn't participate in the 2010 report (reasons unknown, only rumours).

Q: Diversity solutions for Category A functions: How high should the requirements be?
A: Diverse solutions should be licensed and reviewed. The principle in Sweden is that the backup system is of Category B, but the quality should be equal.

7.14 HARMONICS WP2 Methods - Improving Functional Requirements Specification

The discussion emphasized the need for another format than functional diagrams. This format should be more concise and easier to understand, in order to minimise risks that "oracles" have the same errors than the systems under test.

7.15 HARMONICS WP2 Methods - Statistical Testing

The objective is to address the known weaknesses of the method, and to investigate the complementary use of statistical testing and formal verification.

Q: How test cases are created? How to select the operational profiles? Is that mature?

A: This is not really a software issue, and therefore, it is not directly addressed by HARMONICS. However, with simulation-based statistical testing, the issue could become less relevant: brute force may be used.

7.16 HARMONICS WP2 Methods - Structure & Complexity of Digital I&C

Q: How is the complexity of function blocks handled?
A: Two levels: Evaluation of function blocks and their usage (how often called?)

Comment: Complexity evaluation provides an objective input for the application of BBNs.

8 Conclusion: Round Table Comments from the EUG

The workshop concluded with a round table discussion where all participants who were not members of the HARMONICS project could provide their personal opinion (not necessarily the view of their organisation), in particular on the following questions:

- What are the major needs we should focus on?
  - What should be achieved in 2-3 years?
  - What should be achieved in 4-10 years?
- What solutions/methods/technologies should be explored or applied in HARMONICS?
- How would you like to interact with HARMONICS?
  - Get reports, review of the work done, workshops, provide cases, ...

TVO

- Interesting project, can be useful one day for refurbishment.
- Expectations: practical tools in the years to come.
- Time for group discussions was too short.
- HARMONICS is more handling licensing issues
- Lack of Practical case studies
- Focus on independent assessment, gaps assessment (dvp % standards)
- Operational experience: generic, not solid.
- What would be a good classification (operational profiles, failures)?
- Complexity analysis: good idea, provides guidance where to focus

Invensys

- Encouragement to engage America if possible at all: this would be highly desirable.

EDF Energy

- This project is highly linked to CINIF research.
- Are other countries regulators assessing what's going on?
- Perspectives after the project (EC presentation).

Horizon

- The results could be applicable to conventional safety sectors as well.
- Valuable area: statistical assessment.

- Great contribution can be expected.
- Future workshops: more guidance to the end users prior to the event, so that they can prepare appropriately.

EC

- A bigger impact on regulatory process is desirable.
- Technology: common safety justification framework (quantification data for PSA)
- Possible follow-up project on overall I&C architectures.
- Non-nuclear sectors: a European project with process industry and avionics to be considered.
- Education and Training: next generation who will implement the results
- Vendors are not represented in the consortium.
- The project is extremely interesting / challenging
- To improve: raise the visibility at the European level (e.g. platform for Gen 2 and 3 research activities)

HAEA

- V&V methods, harmonization and safety justification: what is necessary?
- Harmonized standards are needed.
- Formal verification is important from a regulatory standpoint.
- Results should be understandable (public opinion).
- Temptation to set limits to complexity measurements to limit the complexity itself.
- Operational experience: data collection mechanisms
- Quantification: in the beginning, PSA data came from the holy bible (reactor vessel rupture: 10-7 per year), then interpreted as generic data. One needs to make a clear distinction between generic and specific data (specific preferred is possible)

Fortum

- Guidance ==> easier to move towards digital systems (too complicated)
- Appreciate SJF presentation (Rule based, goal based)
- Real case studies (more if possible)
- Complexity analysis = one way of moving forward
- Involvement from US: Europe and Chine is already a challenge
- More vendors would be appreciated
- Future activities: workshop (discuss things, make new friends, interaction is as valuable as information coming from the slides)
- Encourage quantification efforts. Data needed for PRA
- PRA is used in decision making, data should be realistic
- Operational experience: How can changes affect the reliability
- Framework (goal-based risk-informed) is interesting

NRG

- Most interesting = SJF (guidance) and quantification