PROJECT PERIODIC REPORT

Grant Agreement number: 269851

Project acronym: HARMONICS

Project title: Harmonised Assessment of Reliability of MOdern Nuclear I&C Software

Funding Scheme: Collaborative project

Date of latest version of Annex I against which the assessment will be made:

Periodic report: **1st** ☐ **2nd** ☐ **3rd** X **4th** ☐

Period covered: **from** 12/1/2014 **to** 11/1/2015

Name, title and organisation of the scientific representative of the project's coordinator:

Jari Hämäläinen, D.Sc.(Tech.), Senior Principal Scientist, VTT Technical Research Centre of Finland

Tel: +358 20 722 6467

Fax: +358 20 722 6027

E-mail: jari.hamalainen@vtt.fi

Project website address: http://harmonics.vtt.fi

1 Publishable summary

Objectives

The overall objective of the HARMONICS project was 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 took 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. The approach took into account a co-operation project in China and also took into consideration the different views, practices, and requirements of the participating countries.

Consortium partners represented different stakeholders in the nuclear I&C field. Four EU countries and China were represented in order to ensure a large overview of national policies and practices regarding safety issues and licensing. A larger "End user and advisory group" with other interested stakeholders (utilities, regulatory bodies, suppliers) to reviewed and gave feedback on the project work in two End Used Workshops. Thus, the project should have fostered an international consensus based on a sound scientific and technical approach, and provided a good basis for harmonisation.

Project structure

The project was organised into 7 work packages (WP):

- WP1 establishes the current state-of-the-art and needs regarding software verification, safety justification and quantification of failure rates.
- WP2 develops innovative methods and tools for these three topics.
- WP3 applies the methods and tools proposed by WP2 to case studies.
- WP4 assesses the effectiveness of the methods and tools proposed by WP2 with respect to needs identified by WP1, based on the results of the case studies of WP3.
- WP5 is in charge of disseminating the results of the project.
- WP6 is in charge of the management of the project.
- WP7 coordinates the activities with a parallel Chinese project RAVONSICS (Reliability And Verification Of Nuclear Safety I&C Systems).

Project scope

HARMONICS focused on the independent confidence building for software of I&C systems implementing Category A functions. Research work benefited from recent licensing projects, for new builds and also for I&C upgrades. In the framework of the project, the term 'software' is interpreted in a broad sense, to include not only 'classical' software to be executed in a microprocessor, but also HDL (Hardware Description Language) designs (usually for FPGAs, Field Programmable Gate Arrays) and digital systems architectures.

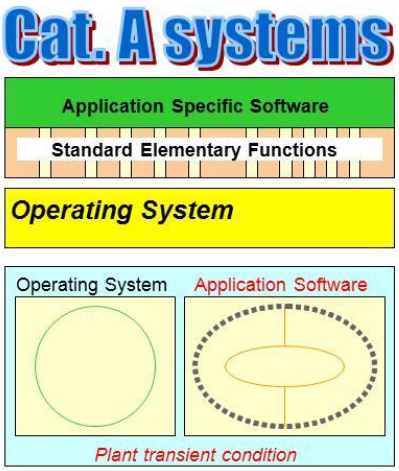

Figure 1. HARMONICS scope.

Methods and tools

HARMONICS addressed 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 was to provide direct evidence of software correctness. Three main verification approaches dealt with were: formal verification, statistical testing, and logic coverage testing. Formal verification addressed different types of safety properties, such as:

- 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, in particular for fault tolerance, defence against common-cause failure or failure rate quantification).
- Equivalence properties (in order to verify that translation tools such as compilers, synthesisers or place & route tools have not introduced discrepancies with the source code).

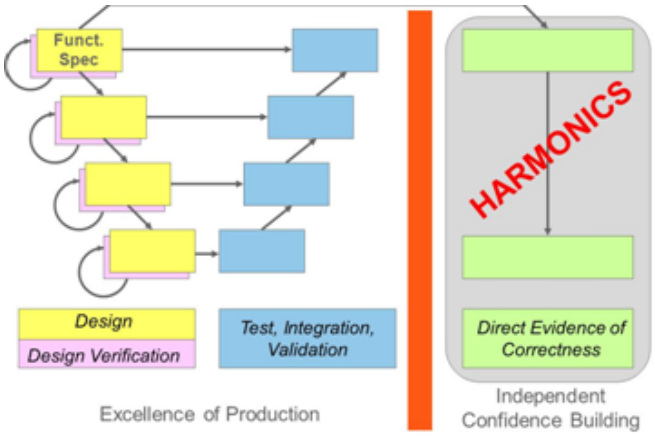

Figure 2. HARMONICS perspective on verification.

Regarding ***justification frameworks***, HARMONICS analysed 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 was to determine how different types of evidence (formal verification, dynamic and static analysis, operational experience, statistical testing, development processes, quality controls) could be combined to justify a claim.

For ***software failure rate quantification***, one of the approaches 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. Other approaches were also considered, such as fault modelling (estimation of the number of residual faults), components reliability estimation, and overall architecture effects.

Case studies

Work on case studies paralleled the methods development. Different types of case studies were needed to cover the different types of software that can be found in systems implementing Category A functions (platform software, application software, HDL designs). Specific verification methods may be applied to each type of software. System level case studies were carried out for failure rates quantification and justification frameworks evaluation.

Dissemination

HARMONICS organised two public events (1st End User Workshop was organised in April 2012 and the 2nd End User Workshop will take place in April 2014) to inform the community. A public case study was developed to present the HARMONICS methods. Information was forwarded to and communication established with various work groups influential in the development and assessment of computer-based systems important to the safety of nuclear power plants, such as IAEA, IEC, NEA, MDEP (Multinational Design Evaluation Program), and WENRA (Western European Nuclear Regulator's Association). Papers presenting the methods and the results of the case studies were submitted to conferences and journals influential in the nuclear or software community.

Progress of the project in January 2011-January 2015
The main activities of HARMONICS have concerned:

- The organisation of the project: kick-off meeting, kick-off workshop with a Chinese parallel project RAVONSICS (23-25 March 2011, China), initial project management duties
- Planning of the methods and case studies
- HARMONICS 1st End User Workshop (17-18 April 2012, Finland)
- End users' needs analysis based on a questionnaire and discussions at the End User Workshop
- The deployment of formal methods, statistical testing and complexity analysis in the assessment of software-based systems
- Development of analytical approach to quantification of the software reliability
- Analysis of the selected case studies by using HARMONICS approach and methods
- Evaluation criteria on methods to safety justification
- Development of a public case study
- HARMONICS 2nd End User Workshop (2-3 April 2014, France)
- Coordination of activities with RAVONSICS
- Presentation of HARMONICS approach and results in conferences and workshops.

Results and their potential impact and use
New concepts and technologies such as digital I&C platforms, i.e. software-based systems, have to be employed in nuclear power plants. Common approaches to safety aspects at the European level are needed as cost-cutting measures in the deregulated electricity market will put pressure on utilities. Projects related to nuclear power are typically large and include several international actors having expertise from several different areas. Large scale cost savings as well as improved safety and reliability are hard to achieve on a national level but agreeing on policies internationally has stronger impact.

HARMONICS dealt with essential questions of technical development. The participating organisations represented utilities, technical support organisations, research institutes and regulators, which guaranteed a cross-fertilisation between the various views of safety justification of digital I&C. The views presented will render deeper understanding of the shared problems, which will be further enhanced by the different approaches planned in the project.

HARMONICS will facilitate achieving better efficiency in plant operation and higher level of safety by supporting the use of new digital I&C technologies and methods. Harmonised practices help introduce more consistent and uniform requirements for licensing of digital I&C systems, which will make the licensing process more transparent and cost efficient.

HARMONICS will also increase commonality in nuclear I&C within and between EU countries and also in the rapidly growing nuclear market of China via the Chinese parallel project RAVONSICS. The representatives of RAVONSICS participated in both HARMONICS End User Workshops. Sharing the effort and knowledge within a strong network of European NPP utilities, technical support organisations and regulators will cut R&D costs and contribute to the progress of best practices in verification and validation procedures. The tools and methods for verification and validation of computer-based I&C solutions is a disorganised area. Validating new approaches through case studies focusing on digital I&C technologies is therefore one of the key issues within HARMONICS. The results will increase motivation of manufacturers to promote corresponding digital I&C technologies and solutions on the market.

By developing the adjustable approach in co-operation, HARMONICS and the parallel Chinese project RAVONICS facilitate the harmonisation of software licensing practices within the EU member states and China. The whole nuclear sector will benefit from harmonisation.

Website address: http://harmonics.vtt.fi

Project type: Collaborative Projects, Small or medium-scale focused (CP-FP)

Project start date: 12/01/2011
Duration: 48 months

Total budget: EUR 1,577,237
EC contribution: EUR 999,458

EC project officer:
Georges VAN GOETHEM Dr Ir
Innovation in nuclear fission and Education & training
European Commission
Directorate-General for Research
Directorate Energy (Euratom)
Unit J.2 – Fission
CDMA 1/47
B-1049 Brussels
Email: Georges.Van-Goethem@ec.europa.eu

Coordinator:
Dr. Jari Hämäläinen
VTT Technical Research Centre of Finland
P.O. Box 1000
FI-02044 VTT
Finland
Telephone +358 20 722 6467
Fax +358 20 722 6027
E-mail: jari.hamalainen@vtt.fi

Partners:

Partner number	Partner full name	Short name	Country code
1	VTT Technical Research Centre of Finland	VTT	FI
2	Électricité de France	EDF	FR
3	Institute for Safety Technology	ISTec	DE
4	Adelard LLP	Adelard	UK
5	Swedish Radiation Safety Authority	SSM	SE