EUROPEAN COMMISSION

European Research Area

PROJECT PRESENTATION (PP)

Harmonised Assessment of Reliability of MOdern Nuclear I&C Software HARMONICS

Contract (grant agreement) number: 269851

Author(s):
Jan-Erik Holmberg, VTT
Nguyen Thuy, EDF
Sofia Guerra, Adelard
Josef Märtz, ISTec
Bo Liwång, SSM

Date of issue of this report: 30/06/2011

EURATOM

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. 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. The approach will be the result of a close co-operation between the EU and China and will take into consideration the different views, practices, and requirements of the participating countries.

Consortium partners represent all the stakeholders in the nuclear I&C field. Four EU countries and China are 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" will be constituted with other interested stakeholders (utilities, regulatory bodies, suppliers) to review and give feedback on the project work. Thus, the project should foster an international consensus based on a sound scientific and technical approach, and provide a good basis for harmonisation.

Project structure

The project is organised into 7 work-packages (WP):

- WP1 will establish the current state-of-the-art and needs regarding software verification, safety justification and quantification of failure rates.
- WP2 will develop innovative methods and tools for these three topics.
- WP3 will apply the methods and tools proposed by WP2 to case studies.
- WP4 will assess the effectiveness of the methods and tools proposed by WP2 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 will ensure the coordination with the sister Chinese project RAVONSICS (Reliability And Verification Of Nuclear Safety I&C Systems).

Project scope

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. 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.

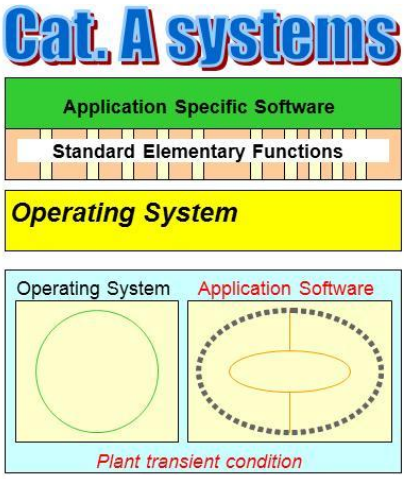

Figure 1. HARMONICS scope.

Methods and tools

HARMONICS 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 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).

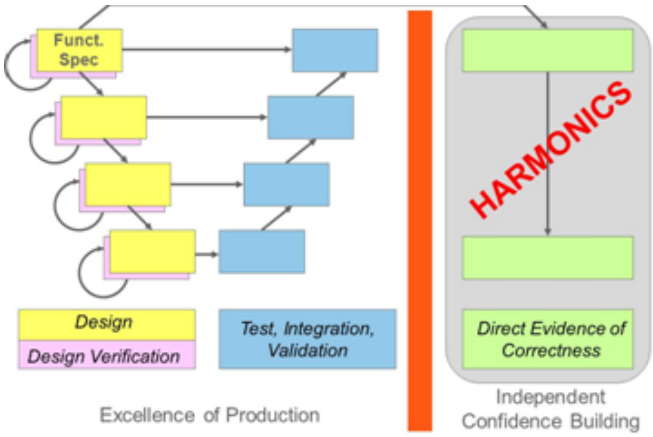

Figure 2. HARMONICS perspective on verification.

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

For quantification, 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. Other approaches are also to be considered, such as fault modelling (estimating the number of residual faults), estimating components reliability, and overall architecture effects.

Case studies

Work on case studies will parallel work in methods development. 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.

Dissemination

HARMONICS will organise two public events (interim seminar in Spring 2012 and final seminar in 2014) to inform the community. RAVONSICS will arrange similar seminars in China. A public case study will be developed to present the HARMONICS methods to the widest audience possible. Information will be 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 will be submitted to journals and conferences influential in the nuclear or software community.

Project information

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. Jan-Erik Holmberg
VTT Technical Research Centre of Finland
P.O. Box 1000
FI-02044 VTT
Finland
Telephone +358-20-722 6450
Fax +358-20-722 6027
E-mail: jan-erik.holmberg@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