Forum 2013

NUGENIA
NUclear GENeration II & III Association

HARMONICS (2011−2014)

Harmonised Assessment of Reliability of Modern Nuclear I&C software

OBJECTIVES

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. The overall objective of HARMONICS 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.

SCIENTIFIC APPROACH

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

- WP1 has established the current state-of-the-art and needs
- WP2 develops innovative methods and tools for the topics: 1) software verification, 2) safety justification, 3) quantification of software failure rates.
- WP3 will apply the methods and tools to case studies.
- WP4 will assess the effectiveness of the methods and tools.

HARMONICS will focus on the independent confidence building for software of I&C systems implementing Category A functions.

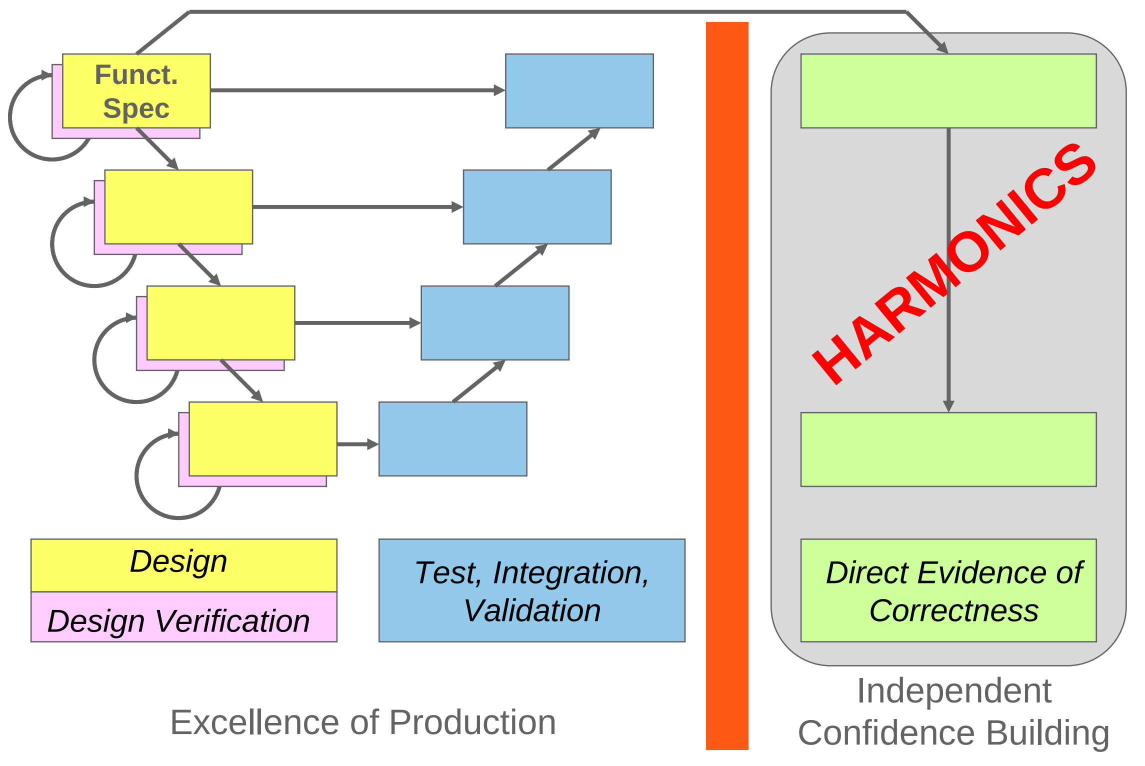
Work on case studies will parallel work in methods development. Different types of case studies will be needed to cover the different types of software that can be found in systems implementing Category A functions (platform software, application software, HDL designs). Each type of software may be the object of specific verification methods. For failure rates quantification and justification frameworks, system level case studies will be used.

SCIENTIFIC HIGHLIGHTS

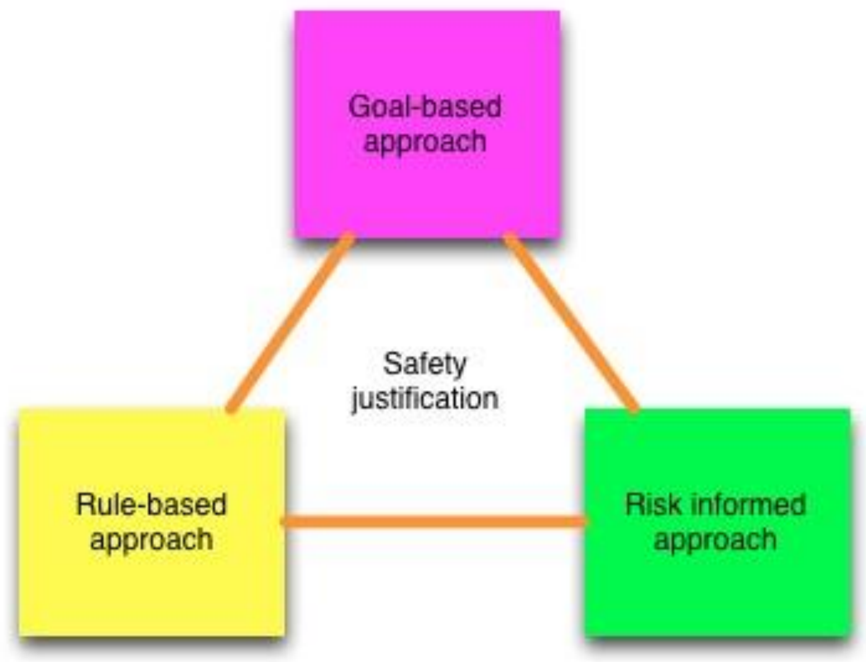
Regarding software verification, the main objective is to provide direct evidence of software correctness. Verification approaches are to be investigated: formal verification, statistical testing, logic coverage testing and complexity analysis. Formal verification will address different types of safety properties of software, such as:

- functional properties
- integrity properties
- structural properties
- 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.


Funct. Spec
HARMONICS
Design
Design Verification
Test, Integration, Validation
Direct Evidence of Correctness
Excellence of Production
Independent Confidence Building

HARMONICS perspective on verification



Integrated safety justification strategy

A second objective of safety justification 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
HARMONICS tackles the problem of software reliability assessment using an analytical approach that takes into consideration all the information obtained by V&V. One of the ways of organising the various pieces of evidence in a probabilistic format is to use Bayes belief network.

IMPACT

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 introducing more consistent and uniform requirements for licensing of digital I&C systems that will make the licensing process more transparent and cost efficient.
HARMONICS will increase commonality in nuclear I&C within and between EU countries and the rapidly growing nuclear market of China via the Chinese parallel project RAVONSICS. Sharing the effort and knowledge within a strong network of European NPP utilities, technical support organisations and regulators will cut R&D costs, contribute to the progress of best practices in verification and validation procedures. The tools and methods for V&V 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.
By developing the adjustable approach in co-operation, HARMONICS and the parallel Chinese project RAVONICS facilitate the harmonization of software licensing practices within the EU member states and China. The whole nuclear sector will benefit from this and there will arise opportunities of cost savings for utilities, regulators and system suppliers.

PARTNERS & CONTACTS

VTT Technical Research Centre of Finland, Électricité de France (EDF), Institute for Safety Technology (ISTeC) from Germany, Adelard LLP from UK, Strålsäkerhetsmyndigheten (SSM) from Sweden
Coordinator: jan-erik.holmberg@vtt.fi
Website: http://harmonics.vtt.fi

VTT EDF R&D ADELARD ISTec Institut für Sicherheitstechnologie (ISTec) GmbH Strål säkerhets myndigheten Swedish Radiation Safety Authority

secretariat@nugenia.org
www.nugenia.org

NUGENIA is mandated by SNETP to coordinate nuclear Generation II & III R&D. - This poster was prepared and is owned by NUGENIA Association.

Conception HELIOSERVICE 01 64 70 50 20