HARMONICS

Euratom FP7 project HARMONICS — Harmonised Assessment of Reliability of MOdern Nuclear I&C Software

Newsletter January 2013

Objectives

The overall objective of the EU FP7 project HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) 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. HARMONICS will focus on the independent confidence building for software of I&C systems implementing Category A functions. The duration of the project is 2011-2014. The public website is http://harmonics.vtt.fi/.

Project achievements during 1st period (January 2011–June 2012)

WP1 Needs, practices, and experiences in Europe and China

Kick-off workshop has been organised with the Chinese parallel project RAVONSICS (Reliability and V&V of Nuclear Safety I&C Software). End users' needs analysis was carried out based on a questionnaire and discussions at the end user workshop.

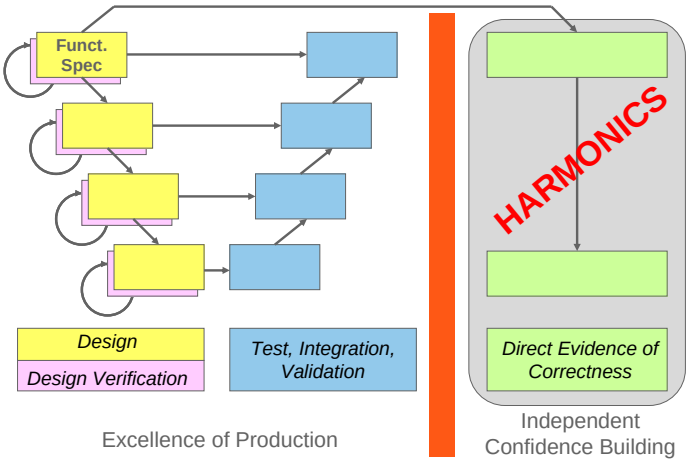
HARMONICS-RAVONSICS kick-off meeting participants, April 2011 in Shanghai, China

WP2 Methods

The objective of WP2 is to develop the technical approaches of the project to safety justification and to quantification of software reliability. These approaches will exploit both direct (e.g. product-based) and indirect (e.g. process-based) evidence of software reliability and present this within a consistent and overarching justification framework. WP2 will also propose innovative verification methods and tools to provide evidence to justify high reliability claims. The first phase of WP2 was for the partners to develop technical working papers summarizing their respective research and experience and how it might be extended within the project. The topics addressed included:

- Model checking of safety properties
- Architecture modelling
- Statistical testing
- Diversity
- Process modelling
- Software reliability models.

A draft structure for the Safety Justification framework has been proposed and extensive discussion have been had on combining rule-based, risk informed and goal based approaches.



WP3 Case studies

The different case studies that will be performed by the HARMONICS partners within the framework of the project have been identified. The case studies serve several main objectives:

- Help WP2 develop its methods and tools.
- Confirm that these methods and tools can be applied with success to real-case systems and software.
- Provide an illustrative public example that could be used to show-case and disseminate the results of the project.

HARMONICS

The case studies form a set of inter-related studies, all deriving from a single fictitious but realistic project. This project features a microprocessor-based I&C system, but to provide an adequate level of diversity, one function of that microprocessor-based system is also implemented in an FPGA-based system. In the microprocessor-based I&C system, several key software components have been identified and are subject to specific analyses:

- The Operating System.
- The pre-developed Function Blocks.
- A Single-Task Application Function (a Diesel Load Sequencing function).
- The Multi-Task, Distributed Application Function (a Safety Injection function).
- The complete Application Software of a Protection System.
- A Public Application Function (a Stepwise Shutdown function).

WP4 Assessment of results from the case studies

The objective of the WP4 is to assess the results of the approaches tested on case studies to support the utilities in licensing their software of I&C systems. During the 1st period, a list of criteria for the evaluation of methods was prepared.

Forthcoming actions 2nd period (July 2012–December 2013)

During the second project period, HARMONICS will focus on the finalisation of the method development work and the performance of the case studies.

End user and advisory group

End user and advisory group has been constituted with interested stakeholders (utilities, regulatory bodies, suppliers) to review and give feedback on the project work. First workshop was organised in April 2012 in Helsinki. The plan is to organise the final workshop in May-June 2014.

HARMONICS End user group meeting, April 2012 in Helsinki, Finland

Publications

The following publications can be loaded from the HARMONICS web site (http://harmonics.vtt.fi/publications.htm):

- Project presentation
- HARMONICS End User workshop April 2012 notes
- HARMONICS End User workshop April 2012 presentations
- HARMONICS paper in TOPSAFE2012 in Helsinki in April 2012: J.-E. Holmberg, S. Guerra, N. Thuy, J. Märtz, B. Liwång, Harmonised assessment of reliability of modern I&C software — EU FP7 project HARMONICS

The HARMONICS work has been also presented in the following international conferences:

- J.-E. Holmberg, P. Bishop, S. Guerra, N. Thuy, Safety case framework to provide justifiable reliability numbers for software systems, PSAM11/ESREL2012, Helsinki, June 25-29, 2012, IAPSAM
- J.-E. Holmberg, S. Guerra, N. Thuy, J. Märtz, B. Liwång, HARMONICS — EU FP7 project on the reliability assessment of modern nuclear I&C software, NPIC & HMIT 2012, San Diego, July 2012, American Nuclear Society
- P. Bishop, R. Bloomfield, S. Guerra, N. Thuy, Safety justification frameworks: integrating rule-based, goal-based and risk informed approaches, NPIC & HMIT 2012, San Diego, July 2012, American Nuclear Society

HARMONICS Consortium

- VTT Technical Research Centre of Finland, www.vtt.fi
- Électricité de France (EDF), www.edf.fr
- Institute for Safety Technology (ISTeC), www.istec.grs.de
- Adelard LLP, www.adelard.com
- Strålsäkerhetsmyndigheten (SSM), www.stralsakerhetsmyndigheten.se

Project Coordinator

Dr. Jan-Erik Holmberg , VTT Technical Research Centre of Finland, P.O. Box 1000, FI-02044 VTT, Finland, e-mail: jan-erik.holmberg(at)vtt.fi, phone +358-20-722 6450