HARMONICS Second End-User Workshop
April 2^{ND}-3^{RD}, 2014 - Chatou, FRANCE

The reliability and safety of the digital systems that implement safety functions are critical issues. This is in particular due to the fact that software can usually not be proven to be completely defect-free, and that postulated residual defects might lead to common-cause failure that could defeat redundancy and defence-in-depth. Unfortunately, the differences in current safety justification principles and methods restrict co-operation and hinder the emergence of widely accepted best practices. They also prevent cost sharing and reduction, and unnecessarily increase licensing uncertainties, thus creating a very difficult operating environment for utilities, vendors and regulatory bodies.

HARMONICS – Harmonised Assessment of Reliability of MOdern Nuclear I&C Software – is a four-year Euratom FP7 project that started in January 2011. The overall objective of the 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 aims at proposing improved yet realistic and practical approaches for software verification, software safety justification and quantification of software failure rates for I&C systems and software implementing category A functions. For further information, see the HARMONICS webpage: http://harmonics.vtt.fi.

The objective of this second workshop is to present HARMONICS results to potential end-users (licensees, regulatory bodies or their technical supports, system designers). It is also an opportunity for workshop participants to discuss the issues and to give feedback.

During the workshop, the project results will be presented through five topics, each illustrated by concrete case studies:

- Verification of functional requirements specification
- Software complexity analysis
- Formal software verification
- Safety justification framework
- Quantification of software failure rates

A simple I&C system (a Stepwise Shutdown System) will also be presented: it will be the basis of a public case study that will illustrate all HARMONICS results.

Verification of I&C functional requirements specification

I&C functional requirements specification (including timing) is the first, and one of the most critical, step of the I&C system and software lifecycle. Errors or lackings are likely to be revealed only late in the development cycle. In the worst cases, they could be revealed by system failure during operation.

In the approach proposed by HARMONICS, the I&C functional requirements are verified in the context of the plant environment of the I&C system (including human operators). Verification can be based on simulation and / or formal verification, as will be illustrated with the case study.

Software complexity analysis

Size is a significant issue for software verification, including for safety I&C software. It often needs to focus on the most critical parts of the software. Complexity analysis is a means to identify such parts. The complexity analysis proposed by HARMONICS mainly aims at the application specific software that is generated automatically on the basis of Functional Diagrams. As a case study, HARMONICS has performed:

- Complexity analysis of the complete set of functional diagrams of a full scale application software.
- Tracing of incoming and outgoing signals for each functional diagram.

Formal software verification

Formal verification aims at ensuring on a rigorous and exhaustive basis that a given item has a desired property. One such property is full compliance with the specified I&C functional requirements. However, a direct formal verification of such a property for the complete software of a real-life reactor protection system is still out of reach. Instead, HARMONICS proposes a divide-and-conquer approach where this big problem is decomposed into smaller, more tractable steps. Although not all individual steps have been fully resolved yet, the workshop will present the progress made and the road map still ahead.

Safety justification framework

Harmonics is developing a Safety Justification Framework. The framework provides

- A set of principles and a strategy based on understanding the behaviour of the system and its interactions
- An approach to developing, communicating and challenging the understanding based on claims, argument and evidence (CAE)
- Guidance on the underlying concepts of CAE and an extension of them into generic "blocks" that provide the basis for domain and problem specific templates (or composite blocks)
- A high level process for deploying the framework

Additional Harmonics deliverables contain, or will contain, more guidance on the techniques deployed in the framework (e.g. verification techniques and software reliability). In addition, there are supporting case studies in progress and a public domain case study will be delivered later in 2014.

Quantification of software failure rates

The reliability and safety of computer-based systems that implement safety functions are critical issues for the construction and modernisation of nuclear power plants. Given the experience with nuclear-related and software-based systems worldwide, there is now the possibility of using empirical reliability data in a way that has not been feasible before. In addition, advances in computer power and testing techniques means that simulated experience and statistical testing are becoming more practicable as forms of evidence. This evidence could have an important role in the assurance of nuclear I&C systems. Advances have also been made, and practical experience gained, in several other domains, such as the formal verification of software, defensive measures to tolerate postulated residual software faults, and safety justification frameworks.

In Harmonics we are investigating a variety of approaches to provide justifiable reliability numbers for software of computer-based safety systems in nuclear power plants that recognise the important role of epistemic doubts in our knowledge of the plant behaviour and uncertainty in our assumptions.

Public case study: Stepwise Shutdown System

In order to be representative of the real needs, most of the HARMONICS case studies are based on real life problems. These however are subject to non-disclosure-agreements (NDAs) and cannot be made public. The objective of the public case study is to illustrate all the HARMONICS results with a simple, easy to understand example not subject to NDA. It will be presented during the workshop so that participants can express feedback on which aspects need be highlighted or clarified.