Safety Demonstration and Justification of Digital Instrumentation and Control Systems for Nuclear Power Plants

Peter Karpati, Vikash Katta, Christian Raspotnig, Sunil Nair

Institute for Energy Technology/OECD Halden Reactor Project,
Software Engineering Department

Overview

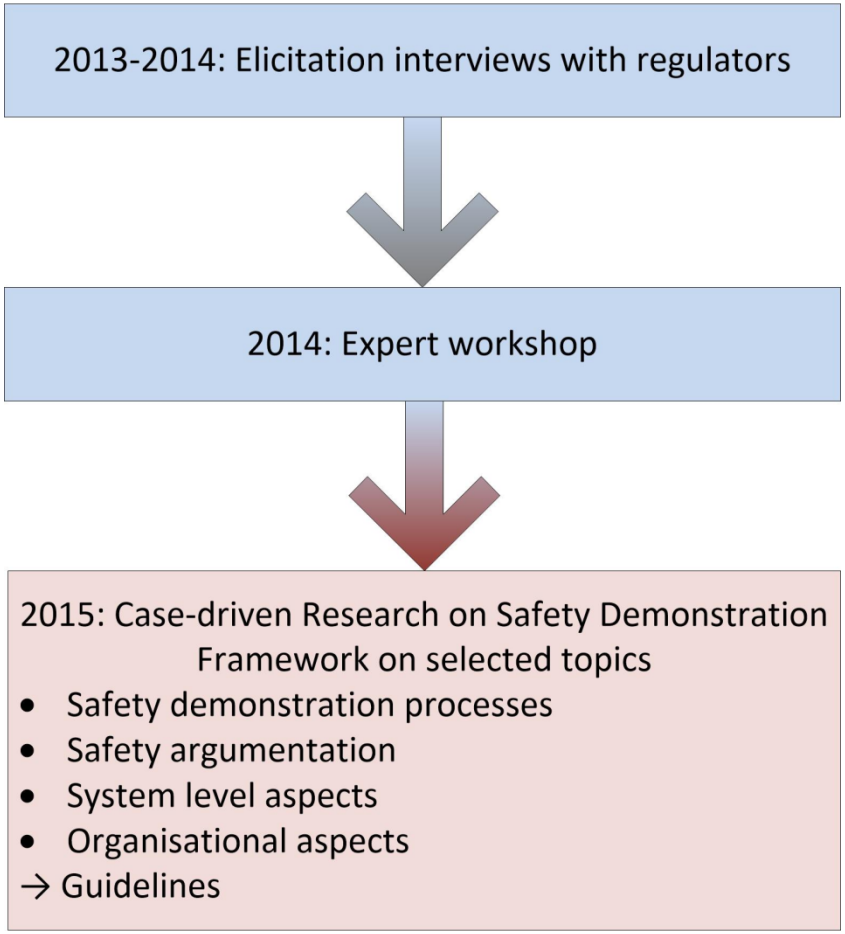
1. Introduction
2. Interviews with nuclear regulators
3. Expert workshop
4. Case studies on submittals *(ongoing)*

1. Introduction – IFE & HRP

- Independent foundation established in 1948
- Norway's second largest research institute
- Research with international nuclear industry
  - Transferring experiences to Nordic industry (e.g. oil and gas, transportation)
- Hosting the *OECD Halden Reactor Project (HRP)*
  - International collaborative research for Safe and Reliable Operation of Nuclear Power Plants (NPPs)
  - Established in 1958, affiliated to OECD NEA in Paris
  - Three year program periods
    - Current period: 2015-2017, 3-year budget about 70 mill. USD
  - 19 member-countries and more than 100 organisations
    - Regulators, utilities, suppliers and research institutes

Safety Demonstration Framework project in HRP

- Objective: understanding and answering challenges in safety demonstration for DI&C in NPPs
- Plan: exploring related theoretical means; apply them to specific challenges using concrete cases
- Expected results: empirical knowledge summarized in guidelines



2. Interviews with nuclear regulators

Objectives

- To learn about the safety demonstration and licensing practice of Digital Instrumentation and Control systems (DI&C) within the nuclear field in different countries
- To identify the challenges

Participants

- Representatives from nuclear safety authorities or relevant support organizations – referred commonly as Regulators

Elicitations conducted in a six month period more than a year ago

Interviews – cont.

Organized as a semi-structured interview

- 2 interviewers and 1 or 2 interviewees
- Conducted over one or two full days
- Interviewees were given a list of prepared elicitation aspects and questions in advance
- Interviewees were asked to prioritize the elicitation aspects in advance and were also encouraged to propose their own aspects to the list

Elicitation aspects and questions

- 16 different elicitation aspects of interest prepared
- 45 questions prepared for the elicitation aspects altogether
- Many more additional questions on the fly

Elicitation aspects

- Background related aspects, e.g. country specific regulatory environment
- Core aspects
  - Safety demonstration as part of safety licensing
  - Activities
  - Content
  - Structure
  - Techniques and methods
  - Documentation
- Additional relevant aspects, e.g. related costs, tools used, cross acceptance

Results

- Interviews were noted down and audio recorded, transcribed, summarized and anonymized
- Information from summaries was sorted according to the elicitation aspects
- Based on that, a high level comparison of practises was performed considering
  - commonalities and
  - differences,

  and exemplified by information from the summaries
- Documented in a technical report (HWR-1112)

General observations on regulatory practises

Differences

- The time when the regulations were written – modernization of regulations underway or planned in many countries
- Mix of the goal-setting (product focused) and prescriptive (process focused) approaches with difference in the emphasis
- Type of actual licensing requests – whether new plants are built or requests only for modernizations and smaller changes

Commonalities

- Risk and responsibility remains with the Licensee by law
- Licensee is expected to be confident in its own arrangements to achieve adequate safety
- Regulators are involved in research activities

General observations - cont.

Main difference in philosophy, e.g. whether structured safety demonstration was produced by the Licensee (e.g. safety case)

- One Regulator does not need it, prefers to not be influenced
- Safety case does not fit the current regulations structure in another country but the Regulator is interested in it
- Another Regulator expressed a neutral standpoint
- Some other Regulators would welcome it
- One Regulator requires it

Two main commonalities

- To achieve confidence in licence applications, Regulators need evidence and reasoning
- Safety demonstration documentation is often not well organized

Examples of regulatory challenges

- Achieving common understanding and clear communication between parties
  - Requirements and terminology (e.g. independence)
  - Between organizations (regulator and licensee), inside organization (management and engineers)
- Receiving a safety demonstration plan
  - Safety demonstration is often an after-thought in the project
  - E.g. produced after the design has been completed
- Correctness and completeness of requirements
  - Checking their completeness, achieving confidence that they are suitable and correct
  - Traceability between the higher level and the lower level requirements is a demanding necessity

Examples – cont.

- Safety demonstration structure and elements
  - Explicit and well-defined arguments are often wished for but rarely received
  - Claims might lack a basis of evidence, e.g. because the underlying assumptions are not validated
  - Evaluating correctness, completeness, and consistency of the decomposition of a claim into sub-claims might be missing or unclear
  - Demonstration structures presented might be difficult to comprehend, e.g. because too many technical details are included at a high-level of the argument
  - Confusion of what a claim, argument and evidence

Examples – cont.

- Complexity of systems and size of documentation can be overwhelming
  - Number and length of documentation increase as systems' complexity increases
  - Regulator has limited number of engineers to analyse the safety while the I&C systems are usually the results of a large number of engineering years
- Assessing independence, separation, diversity and other type of architectural issues
  - Increasing dependencies and the interactions across multiple safety classifications (between non-safety critical and safety critical systems)
  - Architecture description might be not sufficient to perform analysis

3. Expert workshop

- Primary objective was to discuss challenges of safety demonstration of DI&C systems, especially the main challenges identified through the interviews with regulators

- Secondary objective was to elicit suggestions for future research activities on safety demonstration that could be performed within the HRP

Topics

Topic 1: How to achieve a common understanding between stakeholders of elementary safety principles

Topic 2: How to express the safety demonstration

Topic 3: How to build confidence

Topic 4: How to handle documentation overload

Topic 5: How to design DI&C systems for safety demonstration

Topic 6: How to harmonize safety demonstration with the development process

Results

- Consensus: all topics represented valid challenges
- The main challenge, pointed out by several workshop participants, is how to convincingly express and argue safety
  - Keywords: complete, correct, consistent, and transparent.
- Several requirements were identified for a suitable safety demonstration framework
- The proposal was to direct future HRP research towards the development of a reasoning framework for safety demonstration, and investigate the applicability of this framework on an existing submittal
- Documented in a technical report (HWR-1113)

4. Case studies on submittals

- Main objective: defining a safety demonstration reasoning framework for DI&C in NPPs
- Step-by-step experience building
  - Starting with a manageable case
    - Public part of a submittal
    - Restricted focus (Protection System, independence dimension)
  - Apply a generic reasoning structure
    - Toulmin's model of argumentation
  - Discuss the findings with experts
  - Develop a reasoning framework for safety demonstration
    - Whether and how to utilise existing approaches

First step

- Go through the publicly availabe part of an existing submittal with focus on DI&C
- Identify information on independence
  - Independence between redundant divisions
  - Independence between safety and non-safety I&C systems
- Structure the safety demonstration, clarify the details of the safety reasoning, identify implicit information
- Investigate whether there is enough information to come to conclusions on independence or there are gaps
  - Missing, unclear, incorrect or non-verifiable information
  - Deficits in suggested pieces of claims, evidence and reasoning

Applying a structured approach for reviewing assurance arguments

Step 1: *Argument comprehension* (ongoing work)

- Understanding the argument by identifying essential elements (key claims, strategies, assumptions, context and evidence) and links of the argument. Representing the argument in a structured form is suggested.

Step 2: *Well-formedness checks*

- Identifying structural errors in the argument

Step 3: *Expressive sufficiency checks*

- Checking whether the arguments are sufficiently expressed

Step 4: *Argument criticism and defeat*

- Investigating the overall sufficiency of the argument and identifying possible causes of argument defeat

So far…

Pilot case study (submittal)

- No explicit reasoning structure
- Often implicit claims, reasoning and evidence
- Difficult to get an overview of interdependences and how independence is achieved and argued

Current activity

- Revisiting the first version of the submittal using the previous 4 step approach
- Thorough analysis to explore reasoning structure and elements
- Recording observations and improvement suggestions

Future work

- Method-independent reasoning framework for safety demonstration
- Try it on different submittals and develop it according to the findings
- Aim: help to achieve common understanding of safety demonstration needs between parties e.g. by showing better ways of presenting information about justification;
- *No judgement of submittals*

Related project – NKS PLANS

- Nordic Nuclear Safety Research (NKS) funded for 2015; 2 more years planned
- Partners: IFE, Solvina, SSM, VTT
- Objectives
  - Improve guidance on safety demonstration planning for Digital I&C systems in NPPs
    - Base: Safety Demonstration Plan Guide (ELFORSK rapport 13:86), developed by Solvina AB
    - Guide for how to plan for and perform demonstration of safety in modernization and new build projects including digital I&C systems within NPPs
  - Establishing a Nordic network of competence on nuclear Digital I&C safety demonstration

Thank you

The discussion sessions

Each discussion session was conducted in the following format:

- 50-minutes group discussion on selected topics
  - Starting with 5-minute individual reflection upon the topic
  - Followed by 2 minutes for each participant for presenting his or her viewpoints on the topic
  - Finally, an open discussion within the group on the topic
- 30-minutes plenary discussion with all three groups present