WGRISK Task “Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA”

NKS/DIGREL seminar, 14.9.2010

Jan-Erik Holmberg

VTT Technical Research Centre of Finland

OECD NEA WGRISK

OECD = Organisation for Economic Co-operation and Development

NEA = Nuclear Energy Agency

CSNI = Committee on the Safety of Nuclear Installations

WGRISK = Working Group on Risk Assessment

http://www.nea.fr/html/nsd/csni/wgrisk.html

- The main mission is to advance the understanding and utilisation of PSA in ensuring the continued safety of nuclear installations in member countries

Objectives of the WGRISK task

- To develop technically sound and feasible failure modes taxonomy for reliability assessment of digital I&C systems for PSA
- To provide best practice guidelines on the use of taxonomy in modelling, data collection and quantification of digital I&C reliability

Scope

- The activity focuses on failure modes taxonomy and its application to modelling, data collection and impacts on quantification

- The following items will be considered (but not limited to):
  - Protection systems and control systems
  - Hardware and software
  - Development, operation and maintenance
  - Failure detection and recovery means

Justification

- Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new NPPs
- A need to quantitatively assess the reliability of the digital systems in a justifiable manner
- Due to the many unique attributes of digital systems, a number of modeling and data collection challenges exist, and consensus has not yet been reached
- One of the recommendations of the DICREL task group was to develop a taxonomy of hardware and software failure modes of digital components.
- An activity focused on development of a common taxonomy of failure modes is an important first step towards standardised digital I&C reliability assessment techniques for PSA
- Needs from PSA will guide the work
- The taxonomy will be the basis of future modelling and quantification efforts
- Helps define a structure for data collection
- The results can be directly used in the review of PSA studies
- Will take advantage from recent and ongoing PSA application and R&D activities carried out in the member countries in this field

Relation to other projects

- OECD/NEA Computer-based Systems Important to Safety (COMPSIS) Project
- OECD/NEA International Common-cause Failure Data Exchange (ICDE) Project
- Multinational Design Evaluation Program (MDEP) Issue-Specific Digital I&C Working Group (DICWG)
- IAEA NE-ICT activities (Network of Excellence for Supporting the Use of I&C Technologies for the Safe and Effective Operation of NPPs)
- Nordic NKS project on "Development of guidelines for reliability analysis of digital systems in PSA context“
- ...

Lead organization(s)

- Responsible for planning and organisation of working meetings and preparation of the guidelines
  - VTT, Finland (leader)
  - Risk Pilot, Sweden
  - IRSN, France
  - EDF, France
  - AREVA, France
  - GRS, Germany
  - KAERI, Korea
  - Ohio State University, USA
  - NRC, USA
  - NRI, Czech
  - JNES, Japan
  - MTA SZTAKI, Hungary
  - ENEL, Italy
  - OECD/NEA, secretariat
  - OECD/COMPSIS project

Milestones (deliverables vs. time)

- Nomination and organisation of the task group (Summer 2010)
- First planning meeting of the task group: planning of the 1st workshop, design of the questionnaire/call for workshop (Fall 2010)
- 1st Working meeting (Spring 2011): collection of taxonomies, identification of commonalities and differences between taxonomies, identification of needs for and uses of common taxonomy, planning of the preparation of the guidelines
- Development of the guidelines by the task group:
  - first draft of the taxonomy sent for commenting (Fall 2011)
  - second draft Spring 2012
  - final draft before the 2nd working meeting (Fall 2012)
- 2nd Working meeting (late 2012/early 2013): presentation of the guidelines, endorsement, planning of future activities
- Report to the CSNI (2013)

Participants (individuals and organizations)

- Experts from countries with known experience in the topic will be invited to the workshops (which are open to every organisation.) and to contribute to the project work

- Representatives from all the WGRISK member countries are invited to take part in the work
- Participation of those countries with experience in modeling digital systems will be strongly encouraged

Generic I&C system as a reference

- In order to facilitate the collection, analysis and definition of the taxonomies, it would be helpful to have a reference I&C system (automation design)
- It may be easier to create a fictive the example system than to consider real automation solution
- It should cover all conceivable features of safety I&C at an NPP
- It should thus cover the system architecture (communicating processors, sensors, actuators, priority logic, bus, ...)