Nuclear Science and Technology Symposium - NST2016
Helsinki, Finland, 2-3 November 2016

Reliability Analysis of Digital I&C in Nuclear Power Plants

Jan-Erik Holmberg
Risk Pilot Ab
Metallimiehenkuja 10, 02150 Espoo, Finland
jan-erik.holmberg@riskpilot.fi

Markus Porthin, Tero Tyrväinen
VTT Technical Research Centre of Finland Ltd
P.O.Box 1000, 02044 VTT, Finland
Markus.Porthin@vtt.fi, Tero.Tyrvainen@vtt.fi

ABSTRACT

Digital protection and control systems are appearing as upgrades in older nuclear power plants (NPPs) and are commonplace in new NPPs. To assess the risk of NPP operation and to determine the risk impact of digital system upgrades on NPPs, digital I&C systems must be included in the probabilistic risk analyses. Due to the many unique attributes of these systems, several challenges exist in systems analysis, modelling and in data collection. This paper summarises earlier and recent R&D activities in this field.

1 INTRODUCTION

Digital protection and control systems are appearing as upgrades in older nuclear power plants (NPPs) and are commonplace in new NPPs. To assess the risk of NPP operation and to determine the risk impact of digital system upgrades on NPPs, quantifiable reliability models are needed along with data for digital systems that are compatible with existing probabilistic risk analyses (PRAs). Due to the many unique attributes of these systems (e.g., complex dependencies, software), several challenges exist in systems analysis, modelling and in data collection. This paper summarises earlier and recent Finnish R&D activities in this field.

2 EARLIER R&D WORK

2.1 1990's

Research on reliability of computer-based systems was initiated in the Finnish national research programs on nuclear safety. In the Programmable automation systems in nuclear power plants (OHA) -project (1995–1998), e.g., the statistical testing methods and operational profiles and diversity requirements were studied and a reference model for safety case processes was developed for computer-based systems [1].

Acquisition, development and testing of new and more cost-effective reliability and safety assessment methods for the computer-based systems was the main objectives of the Programmable automation system safety integrity assessment (PASSI) -project (1999–2002). The emphasis of PASSI was on the application of Bayesian inference in reliability assessment and an experimental case study was performed in the project. [2]

2.2 Euratom FP5 projects

Several European projects have dealt with the key technologies enabling efficient I&C modernisation at NPPs. One of the key projects was the Euratom FP5 project CEMSIS (Cost-Effective Modernisation of Systems Important to Safety) that produced guidance on a proposed approach to safety justification of SIS (System Important for Safety), on requirements engineering for SIS and on qualification strategy for COTS (Commercial Off-The-Shelf) or pre-existing software products [3].

In parallel with CEMSIS, the BE-SECBS (Benchmark Exercise on Safety Evaluation of Computer Based Systems) project provided a comparative evaluation of assessment methodologies for safety critical computer based systems that are in use in the nuclear industry [4]. One of these methodologies was aimed at quantitative software reliability estimation.

The work done in CEMSIS and BE-SECBS have been later continued in the FP7 project HARMONICS (see ch. 4.4).

3 STATE-OF-THE PRACTICE

A summary of experiences of modelling digital systems in OECD/NEA CSNI member countries can be found in [5]. There is a general consensus that protection systems shall be included in PRA, while control systems can be treated in a limited manner. The system architecture and the mode of operation of protection systems versus control systems are different, which creates a different basis for the reliability analysis.

Digital I&C systems include unique features, such as complex dynamic interactions and the usage of software, that can be difficult to take into account with traditional PRA methods such as with the event tree-fault tree approach. Dynamic methodologies provide a more accurate representation of probabilistic system evolution in time. However, the dynamic models are on a trial stage.

There is an on-going debate on how to treat software reliability in the quantification of reliability of systems important to safety. It is mostly agreed that software could and should be treated probabilistically but the question is to agree on a feasible approach.

Software reliability estimation methods described in academic literature are not applied in real industrial PRAs for NPPs. Software failures are either omitted in PRA or modelled in a very simple way as common cause failure (CCF) related to the application software of the operating system (platform). It is difficult to find any basis for the numbers used except the reference to a standard statement that 1E-4 per demand is a limit to reliability claims, which limit is then categorically used as a screening value for software CCF.

The engineering judgement approaches used in PRA can be divided into the following categories depending on the argumentation and evidence they use: screening out approach, screening value approach, expert judgement approach, operating experience approach. The reliability model used for software failures is practically always the simple "probability of failure per demand" (pfd).

4 RECENT R&D ACTIVTIES

4.1 DIGREL failure modes taxonomy

In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRISK) to set up a task group to coordinate an activity in this field. One of the recommendations was to develop a taxonomy of failure modes of digital components for the purposes of PRA, resulting in a follow-up task group called DIGREL [5].

The WGRISK/DIGREL failure modes taxonomy [6] is based on a hierarchical definition of five levels of abstraction for a nuclear power plant safety automation: 1) system level, 2) division level, 3) I&C unit level, 4) I&C unit module level, 5) basic component level. This structure corresponds to a typical reactor protection system architecture.

The main feature of the taxonomy is to describe the failure propagation using a failure model. The failure model and the taxonomy consist of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect. The purpose of the taxonomy is to support PRA, and therefore it focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

4.2 DIGREL Nordic guidelines

In a parallel Nordic DIGREL activity (2010–2014), the goal was to develop guidelines for analysing and modelling digital I&C systems. The failure modes taxonomy [6] is one part of the guidelines. In addition, the modelling issue has been studied by developing a fictive, simplified PRA model representing a four-redundant distributed protection system. The Nordic project also included a development of an approach to model and quantify software faults, which have been implemented in the example model [7].

4.3 DIGREL example model

The purpose of the example model is to support evaluation of design and PRA modelling alternatives. The architecture of the safety I&C is presented in Figure 1. The protection system is divided into two subsystems, called RPS-A and RPS-B. The two subsystems enable diversification of safety functions the whole path from sensors to actuators. The four divisions (1 to 4) are identical.

The example I&C architecture has been implemented in a PRA-model representing a fictive boiling water reactor (BWR), which has four-redundant safety systems. The example PRA considers the main modules of the I&C unit, i.e.,

hardware and software modules necessary for the performance of several actuation signals.

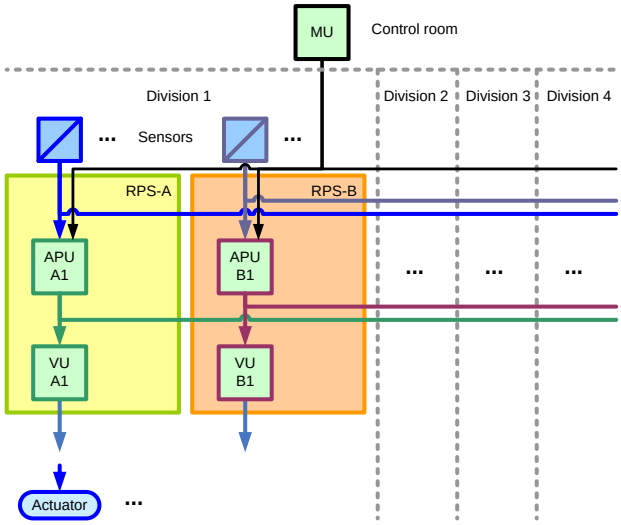

Figure 1: Architecture of the example reactor protection system. APU = Acquisition and processing unit, VU = Voting unit, MU = Processor unit for operator.

The example PRA model has been designed in a dynamic manner to allow major changes of the modelling of different digital I&C aspects. The model changes are mainly performed by the use of boundary condition sets in the consequence analysis cases. The modelling aspects that have been addressed in this project are:

- Relative importance of digital I&C modules and hardware failure modes.
- System level vs. I&C unit level vs. module level modelling.
- Importance of the default value modelling.
- Importance of handling detected faulty input signals in voting logic.
- Common cause failure parameter importance.
- Relative importance of digital I&C units and software failure modes.

4.4 Euratom FP7 project HARMONICS

The objective of the HARMONICS (Harmonised Assessment of Reliability of Modern Nuclear I&C Software) project (2011–15) was to ensure that the nuclear industry has well founded and up-to-date methods and data for assessing software of computer-based safety systems [8]. The project addressed three key issues: software verification & validation (V&V), software safety justification, and quantitative evaluation of software reliability. The focus was on the independent confidence building for software of I&C systems implementing Category A functions, which is the highest safety category in NPPs.

Regarding software reliability, the developed framework integrates quantitative software reliability claims in the overall software and system safety justification. HARMONICS investigated the nature and justification for any reliability claim limit. It also proposed practical approaches to estimate the values needed for PRA: probabilities of failure on demand, conditional CCF probabilities, and possibly frequencies of spurious actuations that lead to initiating events. It proposed a more analytical approach that takes into consideration all the information obtained by V&V and organised by the software safety justification. This approach can be based on the identification of failure modes of interest (as outlined in [6]), of the failure mechanisms that could lead to these modes, and on the effectiveness of the measures taken to prevent given mechanisms. It also considers the implication of I&C architectures and implementation technologies in the system safety justification.

4.5 DIGREL software reliability quantification approach

In the DIGREL project, a practical approach for software reliability analysis for PRA purposes has been developed [9], following the failure modes taxonomy for software modules [6] and the HARMONICS framework, which combines probability estimates with available evidence [8].

The approach to handle software failures is based on the postulation of software faults in different software modules and the consideration of a limited but representative number of end effects for the software module failures. A software failure can cause either a fatal failure crashing the processor or an application function specific non-fatal failure causing a functional failure of a specific application function.

System software is a generic module (not plant-specific) and its failure rate could be estimated from operating experience. Application software modules implementing the I&C functions are plant-specific and it can be hard to collect sufficient statistical evidence for them. In DIGREL, indirect evidence such as complexity of the module and V&V category (i.e. safety class) are used as input to the reliability estimates. There are also other important software modules which could fail, but from the failure effect and CCF risk point of view system software and application software cover the relevant and representative cases.

4.6 MODIG

The NKS-project MODIG (MODelling of DIGital I&C), started 2015, aims to get a consensus approach for a reliability analysis of digital I&C, improved integration of probabilistic and deterministic approaches in the licensing of digital I&C, improved failure data collection including software failure probability quantification, and a practical application of PRA [10].

In 2015, a survey of the defence-in-depth (DiD) framework and PRA's role in it was made. Also approaches to analyse spurious actuations, e.g., caused by I&C failures, were discussed. The software reliability quantification proposed in DIGREL has been further developed.

5 CONCLUSIONS

Digital I&C reactor systems form the functional core in a modern NPP. A failure in the hardware or software has a potential to propagate and affect the overall safety of the station. The design of the system needs to meet the deterministic criteria and due to the complexity of the system the use of PRA technique could be very relevant to demonstrate the DiD concept. The digital I&C systems should also be included in the PRA evaluation, as it has a potential to significantly affect the overall plant reliability. Experience from DIGREL, HARMONICS and MODIG projects demonstrates the importance of international collaboration in a challenging licensing area where a consensus has not yet been achieved.

ACKNOWLEDGEMENTS

DIGREL and MODIG projects have been financed by NKS (Nordic nuclear safety research), SAFIR (the Finnish Research Programs on Nuclear Power Plant Safety) and the Nordic PSA Group. HARMONICS was co-funded by the European Commission, the UK C&I Nuclear Industry Forum and the consortium organisations VTT, EDF, ISTeC, Adelard LLP and SSM.

REFERENCES

[1] P. Haapanen, J. Korhonen, U. Pulkkinen, "Licensing process for safety-critical software-based systems", STUK-YTO-TR 171, STUK, Helsinki, 2000.

[2] P. Haapanen, A. Helminen, U. Pulkkinen , "Quantitative reliability assessment in the safety case of computer-based automation systems", STUK-YTO-TR 202, STUK, Helsinki, 2004.

[3] CEMSIS, "Cost Effective Modernisation of Systems Important to Safety", Work Package 0. Final Public Synthesis Report (first issue), 2004. http://www.cemsis.org/

[4] V. Kopustinskas, C. Kirchsteiger, B. Soubies, F. Daumas, J. Gassino, J.C. Péron, P. Régnier, J. Märtz, M. Baleanu, H. Miedl, M. Kersken, U. Pulkkinen, M. Koskela, P. Haapanen, M.L. Järvinen, H,W. Bock, W, Dreves, "Benchmark Exercise of Safety Evaluation of Computer Based Systems (BE-SECBS Project)", In Proc. of FISA-2003 conference, Luxembourg, November 10–13, 2003.

[5] OECD/NEA/CSNI, "Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants", NEA/CSNI/R(2009)18, Paris, 2009.

[6] OECD/NEA/CSNI, "Failure modes taxonomy for reliability assessment of digital I&C systems for PRA", NEA/CSNI/R(2014)16, Paris, 2015.

[7] S. Authén, S., J.-E. Holmberg, T. Tyrväinen, L. Zamani, "Guidelines for reliability analysis of digital systems in PSA context – Final Report", NKS-330, Nordic nuclear safety research (NKS), Roskilde, 2015.

[8] N. Thuy, J. Valkonen, S. Guerra, R. Bloomfield, J. Märtz, A. Lindner, "HARMONICS Final Public Report", D5.7, Euratom, 2015.

[9] O. Bäckström, J.-E. Holmberg, M. Jockenhövel-Barttfeld, M. Porthin, A. Taurines, T. Tyrväinen, "Software reliability analysis for PSA: failure mode and data analysis", NKS-341, Nordic nuclear safety research (NKS), Roskilde, 2015.

[10] S. Authen, O. Bäckström, J.-E. Holmberg, M. Porthin, T. Tyrväinen, "Modelling of DIgital I&C, MODIG — Interim report 2015". NKS-361, Nordic nuclear safety research (NKS), Roskilde, 2016.