Bibliographic Data Sheet **NKS-230**

Title	Guidelines for reliability analysis of digital systems in PSA context — Phase 1 Status Report
Author(s)	Stefan Authen 1, Kim Björkman 2, Jan-Erik Holmberg 2, Josefin Larsson 1
Affiliation(s)	1 Risk Pilot, Sweden and 2 VTT, Finland
ISBN	978-87-7893-301-0
Date	December 2010
Project	NKS-R / DIGREL
No. of pages	29
No. of tables	9
No. of illustrations	2
No. of references	55

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, quantitative reliability models are needed for digital systems. Due to the many unique attributes of these systems, challenges exist in systems analysis, modeling and in data collection.

Currently there is no consensus on reliability analysis approaches. Traditional methods have clearly limitations, but more dynamic approaches are still in trial stage and can be difficult to apply in full scale probabilistic safety assessments (PSA). The number of PSA:s worldwide including reliability models of digital I&C systems are few.

A comparison of Nordic experiences and a literature review on main international references have been performed in this pre-study project. The study shows a wide range of approaches, and also indicates that no state-of-the-art currently exists. The study shows areas where the different PSA:s agree and gives the basis for development of a common taxonomy for reliability analysis of digital systems.

It is still an open matter whether software reliability needs to be explicitly modelled in the PSA. The most important issue concerning software reliability is proper descriptions of the impact that software-based systems has on the dependence between the safety functions and the structure of accident sequences. In general the conventional fault tree approach seems to be sufficient for modelling reactor protection system kind of functions.

The following focus areas have been identified for further activities:

1. Common taxonomy of hardware and software failure modes of digital components for common use
2. Guidelines regarding level of detail in system analysis and screening of components, failure modes and dependencies
3. Approach for modelling of CCF between components (including software).

Key words

Digital I&C system, probabilistic safety assessment, reliability, nuclear power plant safety

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org