Probabilistic Risk Assessments of Digital I&C in Nuclear Power Plant

Li Shi(a), Robert Enzinna(b), Steve Yang(c), Scot Blodgett(d)

a) I&C Electrical System, Altran Solutions Corp. b) Risk & Reliability Engineering,

AREVA NP. c) I&C V&V, AREVA NP. d) I&C Electrical System, Altran Solutions Corp

Key issues associated with the characteristics of the digital system are discussed in this paper. These issues are: Understanding the failure modes of the digital compo-nents, the fault coverage of the digital systems (e.g., the portion of the failure rate that are selfmonitored and non self-monitored), the treatment of software (SW) reliability/common cause failure(CCF), the hardware failure data and planning ahead for integra-tion with the overall plant PRA. The modeling techniques corresponding to each of the issues above are discussed and summarized in this paper. These approaches are re-alistic and conservative. It also shows that by relying upon good engineering judgment and simplified modeling techniques, the NPP risk importance of a digital I&C system can be estimated with relative low cost. The discussed and summarized methods are suitable for estimating the probabilistic risk of digital instrumentation and control (I&C) systems in nuclear power plants (NPP) for design certification (DC) and combined operating license (COL) applications at both new plants and operating plants.

A Generic Failure Modes and Effects Analysis (FMEA) Approach for Reliability Modeling of Digital Instrumen-tation and Control (I&C) Systems

Tsong-Lun Chu, Meng Yue, Gerardo Martinez-Guridi, John Lehner

Brookhaven National Laboratory, Upton, NY, USA

In this paper, a systematic failure modes and effects analysis (FMEA) approach is proposed for creating reliability models for digital instrumentation and control systems. The FMEA approach is at the level of detail where data are available or at least poten-tially available, i.e., at a level of generic components. The proposed FMEA approach envisions a digital system as consisting of modules, each comprising common generic components, such as an analog/digital converter or a multiplexer. The failure modes of a generic component are defined in terms of their impact on the signal(s) carried by the component, and used to evaluate their impact on the module’s input and output signals based on the component’s interconnection in the module, that, in turn, determines the status of the entire system. This approach was applied to a digital feedwater control system (DFWCS), consisting of several modules that perform different functions. An automated FMEA tool was created based on the source code of the software and used to propagate failures through the system to determine the system status. The pro-posed approach is considered a generic one that can support the reliability modeling of any digital system, and can provide a practical solution to addressing the complexity of digital systems with the aid from the automated tool. It should be noted that the implementation of the FMEA approach described in this paper did not involve detailed analysis of software; instead, two generic software failure modes were included as placeholders in the DFWCS example.

International Experience with Modeling Digital Systems in PSAs

Tsong-Lun Chu(a), Gerardo Martinez-Gurdi(a), Alan Kuritzky(b), and Abdal-lah Amri(c)

a) Brookhaven National Laboratory, Upton, NY, USA. b) U.S. Nuclear Regulatory

Commission Washington, DC, USA. c) Nuclear Energy Agency, Paris, France

This paper summarizes the discussions and recommendations from an international technical meeting focused on current experiences with reliability modeling and quanti-fication of digital systems in the context of probabilistic safety assessments of nuclear power plants. The meeting was organized by the Working Group on Risk Assessment of the Committee on the Safety of Nuclear Installations of the Nuclear Energy Agency of the Organization for Economic Co-operation and Development, and was held in Paris, France during October 2008.

Sensitive Incorporation of Ageing Effects into the PSA Model

Emil Stefanov(a,b) and Gueorgui Petkov(b,a)

a) Kozloduy Nuclear Power Plant, Kozloduy, Bulgaria. b) Technical University of Sofia, Bulgaria

The paper presents the results of a case study on sensitive incorporation of ageing effects into the PSA model of the Russian PWR - WWER-1000. The possible impact of age-related degradation on the component unreliability, safety system unavailability and on the plant risk profile is demonstrated. The discussion on the sensitive use of PSA to evaluate the structures, systems and components ageing effects on the overall plant safety is provided using the WWER-1000 large LOCA PSA model as an example. Based on the comparison of generic and specific ageing reliability databases used in case study some practical insights, recommendations and limitations for sensitive incorporation of the ageing effects into the PSA model are also discussed. The set of “virtual” reliability data was prepared on the basis of the results of case study and available generic data sources. The data includes time-dependent reliability models for certain mechanical, electrical and instrumentation & control components of the high pressure injection system, accumulator’s injection system and low pressure injection & residual heat removal system. The study was carried out within the framework of the EC-JRC Ageing PSA Network Task 7.