Unclassified **NEA/CSNI/R(2009)18**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

17-Dec-2009

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2009)18
Unclassified

RECOMMENDATIONS ON ASSESSING DIGITAL SYSTEM RELIABILITY IN PROBABILISTIC RISK ASSESSMENTS OF NUCLEAR POWER PLANTS

JT03276315

English text only

FOREWORD

As stated in the mandate of CSNI's Working Group on Risk Assessment (WGRisk), the working group supports improved uses of Probabilistic Safety Assessment (PSA) in risk informed regulation and safety management through the analysis of results and the development of perspectives regarding potentially important risk contributors and associated risk-reduction strategies. WGRisk's activities address the PSA methods, tools, and data needed to provide this information.

Digital Protection and Control systems are appearing as upgrades in older plants and are commonplace in new nuclear power plants. In order to assess the risk of nuclear power plant operation and/or to determine the risk impact of digital system upgrades, there is a need for quantifiable reliability models and data for digital systems that are compatible with existing plant PSAs. Due to the many unique attributes of digital systems (e.g., software, dynamic interactions, and internal state-transitions), a number of modelling and data collection challenges exist. Many countries have some experience with modelling digital systems, and CSNI members would benefit from sharing this experience.

The working group's past efforts in this area include the following: (1) In 2001, the group performed a survey of member countries regarding their experience, activities and plans for safety assessment of programmable systems, as well as the use of PSA on such systems. (2) In 2006, a WGRisk technical note [NEA/SEN/SIN/WGRISK(2007)1] indicated that there were no universally accepted methods for the modeling of digital system risk and reliability. However, there are some countries that are using risk insights to support regulatory reviews of digital systems and are performing some level of PSA modeling. The present task was requested in June 2007 by the CSNI Bureau in order to provide recommendations to the CSNI on methods and information sources for quantitative evaluation of digital system reliability in PSA.

This report presents the results of this work and the basis for its main recommendations to promote method development (e.g., methods for quantifying software reliability, approaches for assessing the impact of failure modes of digital components), data collection and analysis (e.g., failure data, including common cause failures, that can be used for PSA purposes), and international cooperation (e.g., sharing of approaches, methods, probabilistic data and insights gained from relevant projects among NEA members, benchmark studies of the same systems to share and compare methods, data, results and insights).

In addition to the individuals and organisations listed at the end of the report, whose inputs were invaluable to the task, the Working Group would like to thank Alan Kuritzky (US NRC), Tsong-Lun Chun (BNL) and Gerardo Martinez-Guridi (BNL) for preparing the report, and A. Amri and A. Huerta of the NEA Secretariat for their support throughout this work.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

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/or 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 safety assessments (PSAs). Due to the many unique attributes of these systems (e.g., software), several challenges exist in modelling and in data collection. The Committee on the Safety of Nuclear Installations (CSNI) of the Nuclear Energy Agency (NEA) of the Organisation for Economic Co-operation and Development (OECD) considered that an international cooperative effort, focused on an exchange of information and perspectives, would greatly facilitate addressing these challenges. Accordingly, during its June 2007 meeting, the CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group (TG) to coordinate an activity on digital instrumentation and control (I&C) system risk. The focus of this WGRisk activity is on current experiences with reliability modelling and quantification of these systems in the context of PSAs of NPPs.

Objective of the Work

The objectives of this activity were to make recommendations regarding current methods and information sources used for quantitative evaluation of the reliability of digital I&C (DIC) systems for PSAs of NPPs, and identify, where appropriate, the near- and long-term developments that would be needed to improve modelling and evaluating the reliability of these systems.

Approach

The principal mechanism for the discussion of experiences with reliability modelling and quantification of digital I&C systems in the context of PSAs of NPPs was a technical meeting that was held in Paris, France, during October 21-24, 2008. The TG prepared and distributed a list of fifteen technical areas associated with DIC system reliability modelling and quantification to the participants prior to the technical meeting. The participants were invited to consider this list as a tool to understand the level of technical detail to be discussed at the meeting. Presentations were made at the meeting by representatives from research institutions, regulators, industry organisations, and academicians. The presentations either addressed the entire process for developing and quantifying reliability models of DIC systems, or some particular aspects of the related methods or data. In addition, group discussions were held to address the fifteen technical areas, and identify areas of research and development that would enhance the state of the art.

At the WGRisk annual meeting in Paris, France, on March 25-27, 2009, the results of the technical meeting and a summary set of TG recommendations were discussed. In general, the WGRisk membership was supportive of the TG recommendations. The results of the WGRisk discussion and subsequent post-meeting member comments have been used to develop the final set of recommendations presented in this report.

Results and their Significance

The October 2008 technical meeting provided a useful forum for the participants to share and discuss their respective experiences with modelling and quantifying DIC systems. It was recognised that although many studies have been performed in various countries, the models of DIC systems developed so far have a wide variation in terms of scope and level of detail, and there was a spectrum of opinions on what is an acceptable method for modelling digital systems. In particular, those organisations that developed digital I & C reliability models at a higher level of detail were less concerned about some of the modelling challenges associated with a more detailed level of modelling. At the same time, the participants believed that the contribution of software failures to the reliability of a DIC system should be accounted for in the models. Some organisations have attempted to quantify software failure probability in limited applications. Some others have included software failures in reliability models as simple common-cause-failure events and quantified them using expert judgment. In addition, the participants agreed that probabilistic data are scarce, so there is an urgent need to address this shortcoming. This is particularly important in the case of common cause failure (CCF) parameters, which often dominate the results.

Near the end of the technical meeting, each organisation identified the near- and long-term developments that it believed were most needed in order to enhance the capability for developing and quantifying reliability models of DIC systems.

Summarising the activities during the technical meeting, the participants recognised that several difficult technical challenges remain to be solved in the fields of modelling and evaluating the reliability of DIC systems, presented their progress on these fields, and reached general consensus on the need to continue the research and development activities to address these challenges. The different ideas that were suggested at the technical meeting were further discussed at the WGRisk annual meeting in March 2009, as described previously.

Recommendations

The recommendations from this task are grouped into the following three categories: Method development, data collection and analysis, and international cooperation. They are summarised below.

Method Development

- Develop a taxonomy of hardware and software failure modes of digital components for common use
- Develop methods for quantifying software reliability
- Develop approaches for assessing the impact of failure modes of digital components
- Develop methods for estimating the effect of fault-tolerant features of a digital system on the reliability of the system's components
- Address human-system interfaces unique to digital systems and associated human reliability analysis
- Evaluate the need and approaches for addressing dynamic interactions

Data Collection and Analysis

- Collect hardware failure data, including common cause failures, that can be used for PRA purposes
- Use operating experience for identifying software failure modes to be included in reliability models

International Cooperation

- Share approaches, methods, probabilistic data, results, and insights gained from relevant projects among NEA members
- Jointly develop methods on software modelling (including CCF), quantification of software reliability, assessing the effect of failures of components of a DIC system on the system, reliability modelling of a DIC system, and human reliability analysis
- Perform benchmark studies of the same systems to share and compare methods, data, results, and insights
- Publish technical documents, such as "CSNI Technical Opinion Papers," and papers in journals and conferences.

ACRONYMS

ABWR	Advanced Boiling Water Reactor
AL	Assurance Level
ASN	Autorité de Sûreté Nucléaire (French Nuclear Regulatory Agency)
ATM	Air Traffic Management
BBN	Bayesian Belief Network
BDMP	Boolean logic Driven Markov Process
BNL	Brookhaven National Laboratory
CANDU	Canada Deuterium Uranium
CCF	Common Cause Failure
CCMT	Cell-to-Cell Mapping Technique
CDF	Core Damage Frequency
CNRA	Committee on Nuclear Regulatory Activities
CNSC	Canadian Nuclear Safety Commission
COMPSIS	COMPuter-based Systems Important to Safety
CSNI	Committee on the Safety of Nuclear Installations
CSRM	Context-based Software Risk Model
CTMC	Continuous-Time Markov Chains
DFM	Dynamic Flowgraph Method
DFWCS	Digital Feedwater Control System
DIC	Digital Instrumentation and Control
DoD	United States Department of Defense
DSPS	Digital Safety Protection System
EDF	Électricité de France
EPRI	United States Electric Power Research Institute
ESARR4	Eurocontrol Safety Regulatory Requirement 4
ESFAS	Engineered Safety Features Actuation System
ET/FT	Event Tree/Fault Tree
FI	Fault Injection
FMEA	Failure Modes and Effects Analysis
GRS	Geseffschaft für Anlagen and Reaktorsicherheit
HAZOP	Hazard and Operability
HEP	Human Error Probability
HRA	Human Reliability Analysis
HRP	Halden Reactor Project
HSI	Human-System Interface
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
ISG	Interim Staff Guide
JNES	Japan Nuclear Energy Safety Organisation
KAERI	Korea Atomic Energy Research Institute
MCR	Main Control Room
NASA	United States National Aeronautics and Space Administration

NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NRC	United States Nuclear Regulatory Commission
NSR	Non-Safety Related
OECD	Organisation for Economic Co-operation and Development
OSU	The Ohio State University
PBM	Program Behaviour Model
PRA	Probabilistic Risk Assessment
PRG	Programme Review Group
PSA	Probabilistic Safety Assessment
PWR	Pressuriser Water Reactor
R&D	Research and Development
RAC	Reliability Analysis Center, United States
RPS	Reactor Protection System
SR	Safety Related
TG	Task Group
U.S.	United States
V&V	Verification and Validation
VTT	Technical Research Centre of Finland
WG	Working Group
WGRisk	Working Group on Risk Assessment

1. INTRODUCTION

1.1 Background and Justification of the Project

Digital instrumentation and control (I&C) systems that are commonplace in new nuclear power plants (NPPs) now are appearing as upgrades in older plants. To assess the risk of NPP operation and/or 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 plant probabilistic risk assessment (PRAs)[1]. Due to the many unique attributes of these systems (e.g., software), several challenges exist in modelling and data collection. The CSNI considered that an international cooperative effort, focused on an exchange of information and perspectives, would greatly facilitate addressing these challenges. Many countries have some experience with modelling digital systems that would be useful to share and discuss. Accordingly, WGRisk took the lead in establishing the information requirements to qualify new technology for existing reactors, specifically including digital I&C (DIC) systems. This WGRisk project particularly relates to three CSNI safety issues: the technical basis for risk-informed regulation, providing an international safety perspective, and new technology for existing reactors.

During its June 2007 meeting, the CSNI directed WGRisk to set up a task group (TG) to coordinate this project. The CSNI approved the WGRisk proposal which had the U.S. Nuclear Regulatory Commission (NRC) as the lead organisation of the TG, supported by Brookhaven National Laboratory (BNL, U.S.). As described in the proposal, the TG's focus was on current experiences with reliability modelling and the quantification of digital systems in the context of PRA. As their main mechanism for coordinating the international collaboration, the TG organised a technical meeting in Paris, France, during October 21-24, 2008. The results of the technical meeting and a summary set of TG recommendations were then discussed at the WGRisk annual meeting in Paris, France, during March 25-27, 2009. This report documents the exchange of information and discussions during the October 2008 technical meeting, and the recommendations on methods and data that resulted from the WGRisk membership discussions during the annual meeting and subsequent, post-meeting member comments. Regulatory organisations, practitioners of risk analysis, and those responsible for plant safety management are expected to be the main users of the report.

Before the technical meeting in Paris, the TG held a planning meeting during October 30-31, 2007 in Rockville, Maryland (U.S.), with the objective of laying out the framework and expectations for the technical meeting. Experts from countries with experience in the topic were invited to participate in the planning meeting; representatives from all the WGRisk member countries were invited to participate in the technical meeting. The participation of those countries with experience in modelling digital systems was strongly encouraged. In addition, several well-known experts in this topic area were individually invited to attend the technical meeting. Representatives of over 20 organisations from 11 countries attended the technical meeting.

1.2 Objective and Scope

This WGRisk project, and the technical meeting, had two objectives:

[1] The terms probabilistic safety assessment (PSA) and probabilistic risk assessment (PRA) are synonymous and are used interchangeably in this report.

1. Make recommendations about current methods and information sources used to quantitatively evaluate the reliability of digital systems for PRA.
2. Identify, where appropriate, the near- and long-term developments that would be needed to improve reliability assessments.

The scope of this project is Level-1 PSA (internal events) for operating reactors and those reactors that will be constructed in the next 5 years.

1.3 Organisation of the Report

During the first day and a half of the technical meeting, there were several presentations by participants, mostly on modelling and evaluating the reliability of DIC systems. Section 2.1 summarises the presentations. The dedicated WGRisk digital website contains the complete presentations.

The participants during the earlier planning meeting had grouped different aspects of probabilistic modelling of a digital system into fifteen general technical areas or topics. Subsequently, the NRC/BNL team further revised and refined them, each with some specific questions. A document describing the areas and associated questions was sent to all countries that are members of WGRisk, together with the invitation to the technical meeting. The document served as useful guidance for organising the discussions during the technical meeting. Section 2.2 summarises the discussions in these areas. In addition, eleven organisations sent written responses to the questions (see Appendix B).

Chapter 3 provides concluding remarks based on the discussions during the technical meeting and identifies some potential areas of research in modelling and quantifying the reliability of DIC systems. Chapter 4 provides recommendations that came out of the WGRisk annual meeting and subsequent post-meeting member comments. Chapter 5 lists the references. Appendix A presents the names and contact information of the participants in the technical meeting.

2. TECHNICAL MEETING SUMMARY

The first day and a half of the meeting involved participant presentations. Most of these presentations addressed modelling and evaluating the reliability of DIC systems. Section 2.1 summarises the presentations. The dedicated WGRisk digital website contains the complete presentations.

A document describing 15 technical areas and associated questions on different aspects of probabilistic modelling of a digital system was sent to all countries that are members of WGRisk, together with the invitation to the technical meeting. These topics were discussed during the remainder of the meeting. In addition, 11 organisations sent written responses to the questions (see Appendix B). Section 2.2 summarises the discussions and written responses on these areas.

The following summaries provide a record of the discussions that occurred during the meeting. Due to time constraints, many of the concepts introduced or practices described by the participants were not discussed by the group, and therefore no judgment is provided as to the relative advantages or disadvantages of these concepts or practices. In the discussions below, the terms probabilistic safety assessment (PSA) and probabilistic risk assessment (PRA) are used interchangeably.

2.1 Presentations by Participants

During the first day and a half of the meeting, there were several presentations mostly on modelling and evaluating the reliability of DIC systems. Each presentation lasted for about 25 minutes, followed by a ten-minute question period. This section summarises the presentations in the order that they were given.

Dr. Abdallah Amri (NEA) opened the meeting by welcoming the participants, and then gave an inclusive overview of the OECD, the NEA, the CSNI, and WGRisk. This information is summarised in Chapter 1.

Mr. Alan Kuritzky (NRC, U.S.) next outlined the background and objectives of this technical meeting. This information also appears in Chapter 1.

Mr. Taeyong Sung (Canadian Nuclear Safety Commission [CNSC]) mainly focused on the types of digital instrumentation and control (DIC) systems used in Canada Deuterium Uranium (CANDU) reactors. He briefly described the probabilistic analysis of these systems, indicating that the system failure models include both the contribution to the failure of the associated mitigating function and to the occurrence of an initiating event. Models were developed for a shutdown system (a dedicated system for a reactor trip for a design-basis event) and a dual-control computer (a control system comprised of two identical computers). He highlighted the following issues in modelling these systems in a PSA:

- Scarcity of failure data
- Modelling of software
- Modelling of fault-tolerance mechanisms (including automatic test mechanism)
- Dependency between initiating event and mitigating function

Mr. Sung also introduced a CANDU plant level I&C design concept that reduces vulnerability to dependent failures.

Dr. Jan-Erik Holmberg (Technical Research Centre of Finland [VTT]) made the following main points in his talk:

1. The reliability models of I&C systems in current Finnish PSAs use the traditional methods of reliability analysis: failure modes and effects analysis (FMEA), fault-tree modelling, and generic data with expert judgments.

2. Quantitative reliability assessment of software-based systems is achievable only by a combination of evidence from several sources. The VTT approach is based on the Bayesian Belief Network (BBN) method. He briefly illustrated this approach with their study of a motor-protection relay. In assessing the reliability of a software-based product, the vendor's contribution is vital because they have a comprehensive knowledge about the product.

3. "Model checking" is a set of methods for analyzing whether a system's model fulfils the system's specifications by examining all the possible behaviours of the system. "Model checking" verifies the existence/non-existence of a property of a system; for instance, single-failure tolerance can be examined. However, the model of "model checking" is not a probability model.

4. Two potential approaches to the reliability analysis of distributed control systems were identified: Markov modelling and the dynamic flowgraph method (DFM). Their efficacy was tested for modelling a feedwater system of a nuclear power plant (NPP). There is a need to develop methods and tools for dynamic reliability analysis.

Mr. Richard Quatrain (Électricité de France [EDF] Research and Development [R&D]) discussed the way EDF currently represents I&C in a PSA using the "compact model." According to Mr. Quatrain, the goal of this model is to represent simply the contribution to the failure of the protective action of the components implemented in the control channels. The model divides an I&C channel into four parts: sensors part, logic part specific to a given protection channel and its processing logic, logic part common to all channels and specific to a programmable controller, and actuation part. The final value of the unavailability assigned to the I&C automatic devices is considered to essentially come from systematic failures (mainly residual errors), and their importance can only be evaluated from a qualitative judgment based on the devices' quality. This judgment is independent of the modelling options. Standard unavailability values for a single protection channel are assigned according to the channel's classification level. The model offers several benefits: use of encompassing values, agreement among Areva/Siemens/EDF experts, and acceptance by the French nuclear regulatory agency (Autorité de Sûreté Nucléaire [ASN]). Further, it is a flexible, simplified model, compatible with the Boolean structures of a PSA model, and it is convenient for carrying out sensitivity studies. These operational features enabled EDF to represent the I&C contribution in all of its PSA models. Mr. Quatrain mentioned the following limitations of the model: (1) it cannot properly evaluate I&C improvements because it lacks details of the relevant aspects of the system, such as internal architecture, types of common-cause failure (CCF), software reliability, and related human errors; and (2) it cannot model relevant items, such as spurious actuations, I&C failure due to human errors, and specific requests from ASN.

Mr. Nguyen Thuy (EDF R&D, France) offered the following four reasons for extending the compact model: (1) the need to compare various design options (such as digital vs. non-digital equipment, and data-communication architectures), (2) more demanding overall safety targets (the current compact model could overestimate the contribution from digital equipment and thus skew safety assessments and design decisions), (3) the increased functional capability of the digital equipment (ignoring its positive effects could also lead to poor decisions), and (4) operating experience can now provide information on the relative importance of the various failure mechanisms (viz., software played a minor role in common-cause failures of safety-classified digital systems). He then briefly described EdF's research project aimed at

developing modelling approaches that evaluate more accurately the full impact of digital equipment and systems on plant safety and availability. The project involves four types of modelling: plant-level, digital equipment, hardware dependability, and human factors. Mr. Thuy pointed out three types of failure mechanisms of digital equipment: (1) random hardware failures, (2) systematic failures (specification errors, design errors, and installation errors), and (3) human factors (operation and maintenance of digital equipment). He stated that systematic failures can happen in a digital system without any component failing. The failure may be, for example, due to the way components interact with one another. Each may operate as designed, but the system may fail because their interactions do not match. Systematic failures are triggered by operating conditions. Mr. Thuy also described certain aspects of the CCF of digital equipment and of software failures, and defensive measures to reduce their probability of occurrence.

Dr. Jan Stiller and Mr. Ewgenij Piljugin (GRS, Germany) presented responses to the questions in the 15 technical areas that were provided to the participants in advance of the meeting. Their responses appear in the next subsection, "Discussion on the 15 Technical Areas," and in Appendix B.

Dr. Enrico Zio (Politecnico di Milano, Italy) presented computational methods for modelling and post-processing dynamic failure scenarios of digital I&C in NPPs. He pointed out that the development of a dynamic reliability model of a system must address the following issues in an integrated manner:

- The modelling of the stochastic failure behaviour of the system hardware components;
- The modelling of the dynamics of evolution of the physical processes associated with the system operation;
- The modelling of the software components of the system;
- The modelling of the human operator acting upon the system;
- The representation and propagation of the uncertainties associated to the modelling and quantification of the hardware/software/human/process behaviours and their interactions.

He addressed the computational challenges related to the generation of dynamic accident sequences and to their post-processing and summarised work done on the development and application of efficient computational methods of:

- Monte Carlo simulation, by Subset Sampling and Line Sampling, for modelling the stochastic failure behaviour of the system hardware components;
- Locally recurrent neural networks for modelling of the dynamics of evolution of the physical processes associated with the system operation;
- Post-processing of dynamic sequence scenarios by fuzzy clustering.

Advanced Monte Carlo simulation techniques and empirical modelling by recurrent neural networks were shown to offer the capabilities for reducing the computational burden associated to accident sequence generation; fuzzy clustering was shown to be a promising approach for the preliminary post-processing of the generated dynamic accident sequences, aimed at grouping them into distinct classes depending on the failure/success end state.

Dr. Zio pointed out that implementing the computational methods of the kind presented is expected to bring significant benefits to dynamic reliability analyses of digital I&C systems.

Mr. Keisuke Kondo (Japan Nuclear Energy Safety Organisation [JNES]) presented the approach to probabilistic modelling of digital systems in Japan. A digital safety protection system (DSPS) was installed in four operating advanced boiling-water reactors (ABWRs), and will be set up in two other units currently under construction. Three Japanese pressurised water reactor (PWR) units also will have DSPS.

A probabilistic model of a DSPS was developed and used for the PSA of an ABWR. The Japanese PWR model is underway, based on the model of an RPS of a typical PWR in Europe. Mr. Kondo related that: (1) The probabilistic model of the DSPS for ABWRs consists of both hardware and software parts, (2) the hardware part includes common-cause failure events and self-diagnosis functions for digital components, and (3) the software part was developed based on the bug-per-lines assumption and debugging rates through verification and validation (V&V) process, and treated as common-cause failure events.

Dr. Hyun Gook Kang (Korea Atomic Energy Research Institute [KAERI]) pointed out that there is no widely accepted PSA method for digital technology. Based on research at KAERI, he identified the following 12 factors of a PSA that are associated with the characteristics of digital I&C systems:

- Modelling the multi-tasking of digital systems
- Estimating the probability of software failure
- Estimating the effect of software diversity and verification & validation (V&V) efforts
- Estimating the coverage of fault-tolerant features
- Modelling CCF in hardware
- Modelling the interactions between hardware and software
- Identifying the failure modes of digital systems
- Ascertaining environmental effects
- Investigating digital-system-induced initiating events, including human errors
- Evaluating the effect of automated periodic testing
- Modelling network communication failure and protocol errors
- Estimating the human error probabilities affected by digitalised information system

He grouped the issues in modelling and quantifying DIC systems into four main categories, as follows:

1. Hardware-module level. The main issues are the unavailability of data, modelling of in-module fault tolerance, and the complexity of the DIC system's structure.
2. Software level. The main problem is estimating the probability of failure of software.
3. System level. The main difficulties center on risk concentration and dependency, diversity and CCF, fault coverage of self monitoring, effectiveness of automated periodic system testing, and network communication failures.
4. Safety-function level. The main questions concern human-system interactions, plant-condition dependency, and coverage of the test inputs before and after installation.

KAERI performed a risk study on a safety-related digital engineered safety features actuation system (ESFAS) of a Korean NPP, including sensitivity studies of two factors of human actions related to DIC systems: 1) the degree of dependence between some human actions, and 2) the human error probabilities (HEPs). According to Dr. Kang, digital component failures could have a large effect on the core damage frequency (CDF) (i.e., comprising up to 10% of the CDF) depending on the assumptions regarding the HEPs and the level of dependence between human actions.

Dr. Man Cheol Kim (KAERI) noted four important parameters in DIC PSA: software reliability, fault coverage, human reliability, and common-cause failures. His presentation addressed the first three. He began by briefly describing three approaches for quantifying software reliability, viz., software-reliability-growth model, Bayesian Belief Network (BBN)-based approach, and test-based approach. To quantify fault coverage, he proposed using fault injection (FI), and mentioned two requirements for an environment for FI for the PSA of a digital I&C system: simulation of a permanent fault and accessibility to the system's memory. He also detailed the quantitative results of fault coverage.

Finally, Dr. Kim discussed the need for a specific method of human reliability analysis (HRA) to use for digital-based advanced main control rooms (MCRs). He discussed two research findings on formulating such a method: (1) performance of simple tasks is faster in the digitalised MCR than in an analog-based conventional MCR, and (2) performance is comparable in both types of MCR for complex tasks composed of several steps. Dr. Kim noted that the second result may reflect insufficient training or the unfamiliarity of operators in a digitalised MCR.

Dr. Bjorn Axel Gran (OECD Halden Reactor Project [in Norway]) initially discussed research related to air traffic management (ATM) particularly that associated with DIC systems. Specifically, he described the Eurocontrol Safety Regulatory Requirement 4 (ESARR4) involving risk assessment and mitigation in ATM. Within this context, the safety process validates the processes carried out by the engineering and development teams to ensure that the software meets the safety requirements. Assurance levels (ALs) describe the extent of evidence required for this validation. After identifying the appropriate ALs for each software module, evidence must be obtained via testing, field experience, analyses, and assessing the code itself. For the hardware, safety calculations are carried out using hardware failure rates and beta-factors. On the other hand, as systems become more integrated and more complex, there is an increased need for methods that assess that: (1) various applications are adequately isolated, (2) failures do not propagate between applications, and (3) applications address the potential existence of common-cause failures and their effects. An approach being exercised to address this need is employing a full-scope simulator of a BWR plant. The basic idea here is to simulate the functionality of the application being evaluated, focusing on how to assess systems and applications for the potential existence of common-cause failures and their effects. This approach will support the comparison of different architectures or designs.

Mr. Bruce Hallbert (Idaho National Laboratory, U.S.) described research on DIC to support light-water-reactor sustainability. He briefly described four technical projects on advanced instrumentation and controls (I&C) technology: (1) centralised on-line monitoring for critical structures, systems, and components; (2) new I&C and human system interface capabilities and architecture; (3) life-cycle nondestructive examination information assessment; and (4) maintaining the licensing and design basis.

Dr. Swu Yih (Ching Yun University of Chinese Taipei) focused on the mathematical analysis of the software reliability assessment process. He divided his presentation into four parts:

1. Motivation for this analysis. Dr. Yih pointed out that the issue of software reliability assessment is controversial, citing several examples of publications by researchers and government organisations questioning the meaningfulness of some concepts, such as software reliability and failure rate of software. To address this controversy, he proposed applying mathematical analysis.

2. Principles of this analysis. Since software reliability assessment is controversial, first there is a need for a mathematical model of the software to analyse mathematically the process of software reliability assessment. Dr. Yih defined computability as the discipline for studying the mathematical model of software, and provided some background material. Based on the research on computability, he mentioned that the most interesting questions about software, such as whether a program will ever divide by zero, are "undecidable." An undecidable problem is a decision problem (a problem with a yes/no answer) for which there is no algorithm for finding a solution. Hence, when undertaking research on the reliability of software, it is crucial to establish whether a problem falls into this category to avoid investing resources on a project that is unlikely to be successful.

3. Preliminary Results. Dr. Yih proposed a Program Behaviour Model (PBM) for studying a program's failure behaviour. This model contains a procedure for assessing software reliability based on comparing the software's output with that generated by an "Oracle function." The PBM

can define software reliability, but the value may not always be measurable. A set of sufficient or necessary conditions must be met for measuring software reliability.

4. Conclusions and recommendations. Dr. Yih presented several conclusions and recommendations; those appearing most relevant to modelling and evaluating the reliability of a DIC system are:

   a) The concept of software failure probability is meaningful.

   b) The value of this probability is measurable only if the PBM meets certain sufficient or necessary conditions.

   c) A risk model should be developed for investigating potential failure scenarios caused by software faults, and sensitivity studies undertaken to identify vulnerable points (especially in the human-computer interface design).

   d) The impacts to safety margin should be studied in scenarios wherein software failure is not recognised and handled by the operators in time.

Mr. Alan Kuritzky (NRC, U.S.) outlined the status of NRC-sponsored research on the PRA of DIC systems. He noted that presently there are no consensus methods for quantifying the reliability of digital systems. NRC is conducting research to support the development of regulatory guidance for assessing risk evaluations involving digital systems, and including digital-system models into nuclear power plant PRAs. NRC is investigating several potential methods for modelling digital-system reliability:

1. Traditional methods: Event tree/fault tree (ET/FT) methods and Markov models.
2. Dynamic methods: Markov models coupled with the cell-to-cell mapping technique (CCMT) and DFM.

Mr. Kuritzky explained that for the purpose of the NRC's research, dynamic methods are defined as those that explicitly attempt to model the interactions between an NPP DIC system and the NPP physical processes, and the timing of these interactions. He described the capabilities and limitations of both the traditional and dynamic methods, and the status of related projects. NRC work on traditional methods identified the following possible areas of additional research:

- Identifying the failure modes of components of digital systems
- Determining the effects of single-component failure modes, and combinations of component failure modes on the system
- Establishing a failure parameter database
- Quantifying the contribution of software failures for use in a PRA model
- Treating uncertainties in models of DIC systems
- Performing human reliability analysis associated with digital systems and human-system interfaces

Dr. Tsong-Lun Chu (Brookhaven National Laboratory [BNL], U.S.) described recent and current research being performed by BNL for the NRC on development and application of an approach for modelling digital systems. The objective of this research is to determine the capabilities and limitations of using traditional reliability modelling methods to develop and quantify the models of digital-system reliability, with the goal of supporting the development of regulatory guidance for assessing risk evaluations of digital systems, and including digital system models into NPP PRAs. A proposed approach was demonstrated for modelling digital systems and implemented for analyzing a digital feedwater control system (DFWCS). The approach included development of a simulation model based upon the DFWCS software as a means of

automatically identifying sequences of component failures that lead to system failure. A Markov model of the system was then developed as a quantification method. Dr. Chu stated that the research revealed that:

1. The model realistically represents the system using an FMEA for generic components of a digital module.
2. The method is applicable to any digital system.
3. The order in which failure modes occur is relevant because of fault-tolerant features that automatically reconfigure the system.
4. Simulation of some component failure modes (individually or in combination) revealed unexpected responses from the DFWCS.
5. State explosion (an issue with Markov models of complex systems) can be addressed by truncation based on convergence of the system failure probability.
6. A potential weakness of the method is omitting a thermal hydraulic model of the plant, but this does not appear to be too limiting.

Dr. Chu also identified a number of limitations in the current state-of-the-art for modelling digital systems, which are candidates for further research, including:

1. Incompleteness of components and their failure modes.
2. Lack of a commonly accepted philosophical basis for modelling software failure rates and probabilities, and methods for quantifying them.
3. Weakness in estimating failure parameters, i.e., failure rates, failure mode distributions, and CCF factors.

Mr. Gerardo Martinez-Guridi (BNL, U.S.) indicated that no commonly accepted method exists for quantitative software reliability, and then proceeded to describe preliminary work performed by BNL for the NRC on modelling of software failures in an NPP PRA. He provided some considerations in probabilistic modelling of software failures, and described some of the causes of software failure. He stated that a software failure occurs when (1) the software contains a fault (i.e., an error introduced during stages of the software life cycle), and (2) an error forcing context (EFC) (i.e., a set of conditions that trigger a fault) happens. Mr. Martinez-Guridi concluded that software failures can be considered as random due to the randomness of the EFCs that trigger software faults, and that the random nature of the software failure can be modelled in terms of a failure rate and/or failure probability.

Mr. Martinez-Guridi presented a conceptual model of the causes of software failures, and the propagation of these failures in a complex engineered system, such as an NPP. He also stated that a review of actual software failures in domestic and foreign nuclear industries, and other industries, supports the concepts presented.

Dr. Tunc Aldemir (The Ohio State University [OSU], U.S.) discussed the Markov/CCMT methodology and its application to the PRA modelling of digital instrumentation and control systems. His discussion focused on the following main points:

1. The need for dynamic methodologies. Dr. Aldemir pointed out that the stochastic description of the behaviour of digital I&C systems often requires considering the statistical dependencies between failure events that arise from:
   a) Type I Interactions, defined as interactions between physical-process variables (e.g., temperature, pressure) and the I&C system that monitors and manages the process.
   b) Type II Interactions, defined as interactions within the I&C system itself due to the presence of software/firmware (e.g., multi-tasking and multiplexing).

2. A brief account of the system that was studied, viz., the DFWCS of a pressuriser water reactor (PWR).

3. A description of the Markov/CCMT methodology. This methodology involves two steps: deterministic modelling and probabilistic modelling. The two types of interactions are analysed separately for each step. The system analysis merges the information for Type I and II interactions.

4. Conclusions. Dr. Aldemir concluded that:

   a) Markov/CCMT methodology can be used to analyse elaborate communication systems.
   b) It can account for coupling among components through Type I and II interactions.
   c) It is possible to couple Markov/CCMT with existing PRAs.

The presentation "Risk Modelling of Digital I&C and Software-Intensive Systems" was given by Dr. Aldemir because the author, Dr. Sergio Guarro (ASCA Inc., [U.S.]), was unavailable.[2] The following main points were presented:

1. Background. The initial part of the presentation gave some background on the NRC-sponsored research that was described by Mr. Kuritzky (see above). One important point made was that the distinction between "traditional methods" and "dynamic methods" is less clear than may appear at face value.

2. Applying DFM to the DFWCS of a typical PWR. The first step identifies the relevant events involving DFWCS functions from the event-tree models in the plant's PRA. The DFM model represents the causality flow of the DFWCS, while the DFM analysis determines the prime implicants and associated probabilities for the top events of interest of the DFWCS.

3. Integrating the results into the plant's PRA model. Since DFM top events and prime implicants logically are consistent and equivalent to binary ET / FT events and cutsets, the results straightforwardly are integrated into the traditional PRA framework. NUREG-1150-style ETs were re-quantified with results from the DFM to generate new risk-scenario probabilities. The same process is applicable when traditional PRA events of interest are events from ETs or FTs.

4. Comparing the results from DFM and Markov/CCMT analyses. The OSU team conducted a parallel DFWCS modelling and analysis effort using the Markov/CCMT dynamic method (see above presentation by Dr. Aldemir). The qualitative and quantitative results obtained from the DFM and Markov/CCMT analyses exhibited close agreement in both qualitative and quantitative content.

5. Closing observations. The dynamic methods project successfully demonstrated the applicability of dynamic PRA modelling and analysis methods for digital I&C systems and the results obtained also successfully demonstrated the ability to integrate dynamic method results into traditional PRA models and frameworks. The scope of project left the following questions open to investigation:

   a) Model coverage of software design and specification errors,
   b) Quantification of software faults,
   c) Coordination of DIC risk modelling with validation and verification and test processes, and
   d) The validity / transferability of findings from parallel research efforts, such as those being undertaken by the U.S. National Aeronautics and Space Administration (NASA).

Dr. Carol Smidts (OSU, U.S.) discussed extending the methodology proposed by OSU and ASCA (see presentations by Drs. Aldemir and Guarro), which included work by the University of Virginia, by

[2] Dr. Guarro joined the meeting the day after this presentation.

integrating related research results, lessons learned, and insights from NASA, the Department of Defense (DoD), and other NRC research. She pointed out six limitations of the existing methodology and proposed approaches for addressing the following four:

a) It does not consider software implementation faults. This limitation can be addressed by post-development review of software artifacts and identification of residual implementation faults.

b) It does not consider permanent hardware faults. This limitation can be addressed by applying a method that uses fault injection coupled with a fault injection profile. This profile is a four-element-tuple <p, i, f, t>, where p is the probability that device i is affected by fault f at time t.

c) It does not consider non-uniform distribution of hardware faults and fault types. The method for considering permanent hardware faults (described in bullet b) also addresses this limitation.

d) It does not consider a representative/exhaustive/systematically defined operational (input) profile. This limitation can be addressed by using a representative, exhaustive operational profile. Dr. Smidts stated that representativeness ensures statistical accuracy and exhaustiveness helps account for requirements faults. The operational profile should be based on operational data, FMEA, data extracted from current PRAs, generic databases, and thermal hydraulic simulations.

Dr. Smidts noted that the remaining two limitations are the unclear degree to which requirements or design faults are considered, and the failure to consider CCF.

Mr. Prince Kalia (NASA Goddard Space Flight Center, U.S.) described the application of the Context-based Software Risk Model (CSRM) concept in NASA's space systems. He mentioned that all robotic mission functions and most critical functions of manned missions are computer-and software-dependent, and that software has been the cause of, or a critical contributor to, several space-mission failures in the last decade. He also noted that software V&V methods currently used are effective at catching specifications-to-code implementation errors, but are not intended to address design and specification errors.

Mr. Kalia stated that the CSRM framework, documented in the NASA PRA Procedures Guide, addresses both design-driven and implementation-driven failures in software-intensive systems, and enables the integration of functional models of digital I&C and software-related risk into traditional PRA frameworks. "Context-based" means that the CSRM analysis partitions the potential failure domain of a system into "bins" that group together scenarios triggered by similar initiating conditions. The CSRM risk model seeks to identify, as far as possible, the conditions to which the SW was designed to respond, and the types of conditions for which it may not have been expressly designed or tested. The PRA risk models can be quantified by combining hardware quantifications with software risk estimates obtained via risk-informed testing.

Mr. Kalia then described an application of the CSRM framework to the Miniature Autonomous Extravehicular Robotic Camera (Mini-AERCam) system. Event trees and DFM were employed to study this system. His example showed how the CSRM analysis identifies software entry conditions for which the software may need to be tested, although they do not correspond to normal states of the system and may not be otherwise identified and tested. Testing served to "demonstrate" a risk contribution from software within certain scenarios. Mr. Kalia also stated that NASA was pursuing a larger application of the CSRM framework in support of the NASA Constellation Project. The initial project mission to be modelled was selected, and the analysis of the software specifications/design of the mission and the

development of CSRM models of this software are underway. Two software components initially were chosen for modelling. One objective of the current work is the demonstration of the scalability of the CSRM approach to full-size space system applications.

Dr. Marc Bouissou (EDF R&D, France) presented the Boolean logic Driven Markov Process (BDMP). He began by pointing out the main advantages and disadvantages of fault trees (FTs) and continuous-time Markov chains (CTMCs). FTs provide hierarchical models that can be solved to obtain minimal cutsets, but their quantification requires the independence of basic events because they are static models. CTMCs have the ability to account for complex dependencies and have a "perfect" mathematical framework. However, most of their quantification methods do not yield qualitative results, they require a higher-level (i.e., more concise) representation, validating a complex model is very difficult, and combinatorial explosion is an issue. Dr. Bouissou stated that BDMP combines the best features of FTs and CTMCs:

1. Simple dependencies replace the total independence of leaves of a fault tree.
2. Each leaf has two modes: Required, and not required.
3. Transitions between these two modes define instantaneous states wherein on-demand failures can be triggered.
4. Any "triggered Markov process" can be associated with a leaf.
5. A BDMP allows the efficient determination of "minimal sequences," i.e., generalization of minimal cutsets for dynamic systems.
6. Combinatorial explosion is lowered by giving a "structure" to the Markov graph equivalent to the BDMP.
7. BDMPs are supported fully by efficient computerized tools.

2.2 Discussion on the 15 Technical Areas

As mentioned previously, a document describing 15 technical areas and associated questions on different aspects of probabilistic modelling of a digital system was provided to all participants in advance of the technical meeting. Each technical area has one or more questions associated with it. Below, the description of each technical area is presented, followed by its associated questions and a summary of the pertinent discussions. Appendix B contains the written responses to the complete set of questions from the 11 organisations that provided them.

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in NPPs. In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant PSAs. Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

There was consensus that it is meaningful to model failures of digital components, including software, in a probabilistic way because these components fail randomly. These components fail randomly because, although the way a fault is introduced into a digital system is not necessarily random, the occurrence of the particular context that would cause the fault to become a failure is random. A fault is a condition of a digital component that will cause the component to fail when the specific context that causes the fault to become a failure happens. In addition, the hardware components of a digital system may fail randomly because they are subject to failure mechanisms similar to those of analog components, such as wear and tear.

b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

All representatives from countries with operating nuclear power plants (NPPs) indicated that models of some DIC systems have been developed. There was great variation in the type of DIC system modelled, and the objective, scope, and level of detail of the models. Some of these differences are discussed in the answers to subsequent questions.

c) *For what purpose have these models been developed?*

The main goal of most studies was to develop a model of a DIC system able to be integrated into an existing PSA. Often, this goal was pursued to meet the requirements of a regulatory body, as for example, the regulatory certification of designs of new nuclear power plants, such as Westinghouse AP1000. After integrating a model of a DIC system into an existing PSA, the PSA then can be used for supporting risk-informed decisions.

The representative from CNSC stated that their model of a DIC system was developed for evaluating the system unavailability, with the objective of meeting regulatory requirements or a licensee's internal program. In addition, several organisations formulated models to carry out research on modelling and quantifying the reliability of DIC systems.

d) *What are the standards or guidance that you have used for developing or reviewing these models?*

There are no specific standards or guidance for modelling digital systems that a particular regulatory body has approved or endorsed. Some studies used generic guidance for PRA that does not provide specific information on modelling and quantifying DIC systems.

The International Electrotechnical Commission (IEC) 61508 [IEC 2000] and IEC 60880 [IEC 2006] are standards related to digital systems; however, regulatory bodies have not endorsed them.

Recently, the NRC staff developed a draft Interim Staff Guide (ISG) on reviewing the PRAs of new reactors' DIC systems. Further, BNL (U.S.) advanced a set of desirable characteristics for a probabilistic model of a digital system, documented in NUREG/CR-6962 [BNL, 2008]. It was an input to the NRC staff's ISG.

e) *What is the scope of the models, e.g., do they include hardware and software failures?*

There is wide variability in the scope of the models in terms of modelling hardware and software failures. The models can be classified into three types: (1) most models combine hardware and software failures, e.g., a software failure is lumped together into a single event with the failure of an associated hardware component, such as a processor; (2) in some cases, software failures are modelled as separate events; and (3) in a few cases, hardware failures are considered, but software failures are omitted.

f) Have the models been integrated into a PSA model of an entire NPP?

The models of DIC systems were integrated into a PSA model of an entire NPP, with two exceptions: (1) the models developed by VTT (Finland), and (2) the model of a digital system developed by BNL (U.S.). In the case of the BNL model, integration with a plant PSA model was not included in the project scope.

g) Can you make available at the technical meeting any publications documenting your work in this area?

Publications that the organisations shared are available from the dedicated WGRisk digital website. In addition, some responses to the questionnaire on these 15 technical topics, in Appendix B, contain additional references to publications.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

Most organisations used the traditional ET/FT method. Specifically, they used FTs to model DIC systems.

The French representatives (from IRSN, EdF, and AREVA) described one similar approach using a logical equivalent to a FT. They employ a "compact model," the function of which is to generate a simplified representation of the contribution of I&C channels to the failure of a protective function. They found that the probability of this failure is dominated by "systematic failures," which may be related to software failures or organisational factors.

The NRC (U.S.) sponsored several organisations to apply other methods to the case study of a digital feedwater control system (DFWCS). ASCA used the dynamic flowgraph methodology (DFM), BNL employed a traditional Markov modelling approach, and The Ohio State University (OSU) developed a Markov/Cell-to-Cell Mapping Technique (CCMT).

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

Since most organisations used traditional FTs or logical variations of them to model a DIC system, they were integrated or can be directly integrated with the PSA of the entire NPP. The presentations by ASCA and OSU on their dynamic modelling methods briefly describe the process of incorporating their models into a PSA. The case study by BNL did not include such integration in its scope.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Most organisations only develop models of digital protection systems. As described in the response to question 2(a), the U.S. organisations sponsored by the NRC (ASCA, BNL, and OSU) generated models for the case study of a digital feedwater control system. The representatives

from OSU consider that their methods are applicable to protection systems. VTT considers that their method is applicable to control and protection systems.

The representatives from GRS and the written response from the U.S. nuclear industry indicate that they do not model control systems because the relevant probabilistic parameters, such as the frequency of an initiating event, are estimated from operating data.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

The level of detail varies substantially between the models described by the participants. The reasons for choosing the level of detail are listed and described in the response to question 3(c).

b) Why was this level of detail used?

Please see the response to question 3(c).

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

The level of detail chosen for the models was based on one or more of the following:

- The objective of the model. The level of detail strongly depends on the goal(s) of the model. If the intent of the model is to assess a specific feature of a digital system, then the level of detail would have to be sufficient to evaluate this feature, such that its risk contribution can be assessed. On the other hand, if the objective is to include in the PSA the risk contribution from a DIC system that is known to have a small contribution to risk and no important dependencies with other systems, the system may be included in the PSA of the entire NPP with a model that is not detailed.

- The availability of failure data. The process of refining a system in a typical PRA from failures of major components into failures of basic components is considered acceptable provided that it stops at the level of the latter for which probabilistic data are available. Accordingly, in general there is a close relationship between the level of detail of the system's logic model and its associated data.

- The level at which events in the fault tree do not have dependencies. In prescribing a model of a DIC system, the level of detail chosen must properly account for the inter- and intra-system dependencies. In this way, the basic events of the model do not have dependencies between them.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HAZOP) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

   a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

      Most organisations use FMEA with different levels of detail for hardware failures. The three exceptions are: (1) the CNSC representative stated that identifying failure modes is not a major issue in modelling DIC systems of CANDU reactors in view of the level of detail at which they are modelled; (2) the representatives from IRSN, EdF, and AREVA stated that for the compact model they do not identify failure modes of components of a digital system, but only consider "failure" of parts of an I&C channel causing "failure" of the channel; and (3) the approach described by the representatives from Chinese Taipei does not identify individual failure modes and effects, but uses a conservative assumption to attempt to bound all possible effects of component failures.

      Usually, failure modes of software are not identified. Three exceptions are: (1) the approach discussed by the KAERI representatives that carries out an FMEA specifically for software, (2) the identification of failure modes of software by the Halden Reactor Project, and (3) the two types of software failure modes considered in the BNL model of the DFWCS: viz., the software continues running but generates erroneous results, and the software stops running. These two types are generic failure modes applicable to any software.

      There is no specific guidance for identifying failure modes and for carrying out an FMEA of a digital system. Identification of hardware and software failure modes is an area recognised as requiring additional research.

   b) *Do you consider operating experience in identifying failure modes?*

      The participants agreed that operating experience should be taken into account. However, a concern mentioned was that PRA analysts do not always have access to full operating experience.

      An exception is the course described by representatives from Chinese Taipei wherein operating experience is not considered because they use the conservative assumption mentioned in the discussion on question 4(a).

c) *How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?*

The participants responded that they use the results of the FMEA for this purpose. The vendor or manufacturer of a digital product usually undertakes an FMEA on which the PRA analysts rely. The CNSC representative also suggested carrying out a Hazard and Operability study (HAZOP), in addition to FMEA, for protection systems. He also pointed out that the former is more appropriate than the latter for control systems.

The BNL representatives stated that in order to identify the relevant features of a digital system that potentially contribute to its unreliability, and to facilitate the model's quantification, it is necessary to model the system at a fairly detailed level. At this level of detail, it is often difficult to determine the effect on the system from individual component failures, and virtually impossible for combinations of failures. Hence, BNL developed a method and associated computerized tool to determine the effect of a failure mode of a component or a combination of failure modes on the digital system. The simulation model, implemented in the tool, assesses the system's response to postulated individual or combinations of failure modes of components, thus identifying those that fail the system.

The OSU representatives indicated that FMEA was used in their study to evaluate the immediate effects of a failure mode of a digital system component. The effect of a failure mode on the capability of the digital system to accomplish its function was propagated either through Markov/CCMT or DFM.

d) *How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?*

Please see the response to question 4(c).

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

- Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

- Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

- Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

- Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

- Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

- Dependencies related to common-cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a reactor protection system (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

The following table summarises the dependencies modelled by several participants. The dependencies identified in bold font in the table were identified by the organisation as risk-significant contributors to their PRA models.

Organisation	Comm.	Support	Sharing	Fault-Tolerance	Dynamic	CCF
VTT	X	**X**	X			**X**
IRSN, EDF, and AREVA	X	X	X	X		X
GRS	X	**X**	**X**			X
JNES						**X**
KAERI	X			X		**X**
HRP						**X**
INER	**X**	X	X	X		**X**
BNL	X	X	X	X		X
EPRI*		X	X			X
OSU	X	X	X	X	**X**	X

*Electric Power Research Institute (U.S.)

All organisations considered CCFs. The representatives from GRS stated that only the CCF of hardware was considered, but that there are no operating-experience data regarding CCFs. Most organisations account for dependencies due to communication, support systems, and sharing of hardware. Some groups modelled dependencies due to fault-tolerance features, but only OSU included dynamic interactions.

KAERI staff pointed out an additional relevant dependency, i.e., that between a digitalised information system (such as an alarm system) and human operators.

b) Did you find any of these dependencies to be risk significant?

As mentioned above, the dependencies identified in bold font in the previous table were identified by the organisation as risk-significant contributors to their PRA models. Several organisations noted that the CCFs of components of digital systems are risk significant. Some organisations found few other important dependencies, as the table shows.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

In general, the participants considered that the current methods are appropriate, though some areas are thought to deserve more research. The representative from CNSC mentioned that the methods are not adequate for identifying some dependencies, especially for hardware failures.

The VTT representative opined that methods are not necessarily adequate, and that dependencies due to fault-tolerance features and dynamic interactions may be important. The representatives from GRS stated that there are no methods available to them for including these two dependencies, and that new ones will have to be proposed. The representatives from IRSN, EdF, and AREVA noted that they consider their current methods are adequate, but they intend to improve them for an EPR unit since its overall DIC architecture is different than in current plants, and the target for core damage frequency is more demanding. KAERI's representatives considered that methods are adequate, but probabilistic data do not suffice to quantify the models.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

   a) Do you consider it necessary to accurately model these interactions and their timing?

   The participants seemingly had a somewhat different interpretation of the meaning of the term "dynamic method." In general, most considered that it is currently still unclear whether modelling these interactions and their timing accurately offers substantial advantages. Some organisations are researching this topic.

   The representatives from many organisations drew an important distinction between control systems (such as a feedwater control system) and protection systems (such as a reactor protection system). They thought that dynamic methods might turn out to be useful for modelling the former, but will probably not be needed for the latter.

   b) Have any dynamic methods been used in your country for modelling digital systems?

   The representatives from OSU and ASCA have applied dynamic methods for modelling and evaluating the DFWCS of a NPP. The VTT representative mentioned that DFM was tested for modelling a feedwater system of a NPP. The representatives from GRS indicated that some German research institutions have employed these methods; a current project at GRS is assessing the potential advantages and difficulties of using them for DIC systems.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

   The participants discussed the difficulties in obtaining raw failure data; such information is scarce and sometimes unavailable. Some organisations managed to obtain raw data from one or more of the following sources, even though some rarely are available:

   Generic-and plant-specific data from operating experience
   Plant-maintenance documentation
   Licensee-event reports

GRS mainly used reliability data provided by the manufacturer which were validated with limited operating experience from a NPP.

BNL mainly used raw failure data from the PRISM database [RAC PRISM], published by the U.S. Reliability Analysis Center (RAC). BNL also broke down the failure rates of components into their constituent failure modes mainly by using information in another RAC publication on failure modes and mechanisms.

Other organisations obtained data in the form of failure rates or probabilities directly from one or more of the following sources, despite some limitations:

Vendor's or manufacturer's data
The "military handbook" (MIL-HDBK-217F) [DoD 1984]
Data from other industries

JNES used probabilistic data from reports published by the NRC and the International Atomic Energy Agency (IAEA).

ASCA and OSU used three sources of data: (1) failure data from the operating experience of the DFWCS they modelled, (2) data for fault coverage of a microprocessor of the DFWCS obtained by the method of fault injection, and (3) failure rate data from the PRISM commercial database [RAC PRISM] for the other components of the DFWCS.

b) *What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?*

Digital-specific CCF parameters are lacking. To evaluate their models, the participants used different approaches, such as expert judgment and the parameters of non-digital components.

c) *What method did you use for processing these raw data into failure parameters, such as failure rates?*

The organisations that gathered raw data used standard methods of reliability parameter estimation, i.e., classical and Bayesian methods.

d) *What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?*

There was consensus among the participants on the lack of data for quantifying probabilistic parameters of software failures, such as the probability of a software failure and CCF of software.

For practical purposes, all participants agreed that now there is no commonly accepted method for assessing probabilistic parameters of software failures, though some PRAs or case studies employ some values of probabilities of software failure, as discussed next. The CNSC representative said that the probabilistic model uses a value that is allocated for the probability of software failure, or this probability is estimated via expert judgment. In one case study, HRP used values for these probabilities that are associated with software assurance levels. JNES's approach takes into account the failure rate of software "bugs" per command line of the software code. KAERI assumed some failure parameters for software for the purpose of a sensitivity study.

IRSN, EdF, and AREVA combine the contributions of hardware and software failures into the parts of the Compact Model. They base their evaluation of the probability of failure of each part on the detailed analysis of the design and features of a digital system, on expert judgment, and on values for similar systems from standards published by the International Electrotechnical Commission (IEC).

One representative from EdF noted that there would be very large uncertainties associated with any estimated failure probability/rate for software. This representative stated that since precise failure probabilities/rates are not needed in most cases, it would be preferable to use qualitative approaches (e.g., justifying a target value based on the use of a standard or other highly controlled process).

Some organisations are exploring methods for assessing probabilistic parameters of software failures. ASCA is developing a framework for the Context-based Software Risk Model (CSRM).KAERI's presentation described their studies on two main methods for this assessment: test-based- and Bayesian Belief Network (BBN)-based approaches. VTT has been exploring the use of the latter.

A topic related to CCF of software is that if redundant channels (or trains) of a system use the same or similar software, then complete dependence between them is often assumed. In other words, failure of the software of the channels is presumed to fail all channels. This assumption is somewhat conservative because the channels would have to receive the same input to cause them all to fail, viz., a condition that may not always be satisfied. However, using this assumption may be a practical way of simplifying the analysis.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) How do you account for the impact of software failures on system reliability?

All organisations agreed that the impact of software failures should be accounted for. Most accomplish this objective by explicitly including events representing these failures in the reliability model. Some organisations combine the contributions of hardware and software failures of a physical entity of a DIC system, such as a channel, into a single element of the model. However, the GRS representatives pointed out that software failures currently are not included in the German PSAs due to lack of methods for appropriately carrying out this task. Hence, they considered that the reliability model should account for the contribution of these failures, and that methods should be developed and data gathered for this purpose.

Other relevant comments during the discussion of this topic include the following:

- There is consensus that software failures can cause common-cause failures (CCFs) that usually are the dominant contributors compared with individual failures; accordingly, some organisations include only CCF events in their models.

- Digital systems are used for control and protection functions. Further, some are classified as safety-related (SR), while others are non-safety-related (NSR). Hence, the quality of the

development process for producing the software for each type of system will correspond to its purpose. Software generated under a high-quality process is expected to be more reliable than other software. Therefore, different methods for quantifying software reliability might be applied for different types of software.

- The failure of software potentially can impact the occurrence of initiating events and the performance of mitigating systems.

- Software potentially might introduce some failure modes that were not considered for analog systems.

- In some cases, software carries out multiple functions, so it is complicated. Accordingly, the software and its associated system may be more susceptible to failure than analog components that usually only execute one function. An important example of the effect of the failures of software would be an increase in the number of occurrences of spurious actuations of its associated system.

- The positive and negative effects of the features of a digital system, including its software, should be included in the system's reliability model. However, there are limitations in the models available for representing these effects, especially for modelling the positive effects. Further research in these areas is advisable.

- There are large uncertainties in evaluating the reliability of software. Hence, quantitatively evaluating this reliability is difficult, and further research is recommended.

b) *How realistic is your approach for accounting for this impact?*

Most organisations that include software failures in their models consider that their approaches are realistic or conservative, though many participants are not comfortable with the state-of-the-art in this area. Some organisations are currently pursuing research in the area of software failure modelling. In particular, the CNSC representative suggested that more research is required to establish the level of realism.

BNL indicated in their response to the questionnaire that the approach on modelling software failures used in their study of a DFWCS should not be considered realistic, because of the following issues: (1) level of detail at which software failures should be modelled, (2) completeness of software failure modes, and (3) lack of failure rates of software failures. Accordingly, the NRC is sponsoring BNL to investigate the topic of quantitative software reliability.

c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

Most organisations consider that software failures should be explicitly included in the reliability model. An exception is EDF's "compact model" that combines the software and hardware failures into the "blocks" of the model. Further, the response from EPRI indicates that sometimes a software failure can be included together with a related hardware failure, so that no separate event is needed to represent the former. The representatives from GRS pointed out that software failures currently are not included in the German PSAs, due to lack of methods to do so. However, they believed that these failures should be covered, although it is unclear whether they should be modelled separately or an integrated probabilistic model of hardware and software-related failures should be used.

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

Participants did not reach consensus about what these interactions are, and hence, drew no conclusions on if and how they should be modelled.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into: (1) those that are associated with the data used to quantify the models (parameter uncertainty), (2) those that are related to the models employed (model uncertainty), and (3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

The representatives from VTT, IRSN, EdF, AREVA, GRS, JNES, HRP, INER, and OSU stated that they addressed the uncertainty associated with the parameters of the basic elements of the probabilistic model. In addition, BNL pointed out that they propagated parameter uncertainty through the probabilistic model using a limited number of samples.

KAERI undertook basic sensitivity studies to quantify the modelling uncertainty for some models or methods used in the PRA. HRP considered this kind of uncertainty by applying simplifications to a reliability model and observing their effects, thus discovering some errors. BNL addressed modelling uncertainty by documenting the main assumptions made in formulating its model.

Regarding the completeness uncertainty, BNL recognised that the failure modes of both software and hardware may not be complete, and more research is needed. OSU discussed the completeness uncertainty in fault injection because the faults injected may not represent all the conditions that may be experienced during actual operation.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: (1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. (2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

JNES and KAERI pointed out that they are applying current human reliability analysis (HRA) methods for analog systems to digital systems. CNSC and VTT also consider that the current methods can be used for these systems.

GRS stated that introducing new computer-based interfaces significantly changes NPP operation and this fact should be considered in the HRA. GRS is conducting research in this area.

KAERI is developing a HRA method for a digitalised main-control room.

INER has carried out some investigations on potential human errors caused by a DIC system.

HRP devotes a large effort to research on human reliability and human factors.

EPRI indicated that a computerized human-system interface can introduce additional failure modes that are not typical of analog systems.

INL pointed out that the new interface with DIC systems involves cognitive processes that fundamentally differ from those associated with analog systems.

b) Are there any available data associated with the probability of this kind of error?

There is consensus among the participants that failure data related to human errors associated with digital systems does not have a firm technical basis, such as data from operating experience.

KAERI and INER now are collecting such data as part of research projects. VTT indicated that event reports might be useful in estimating the probabilities of these errors.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?

Most organisations are carrying out R&D activities on developing methods and tools for modelling and quantifying reliability models of DIC systems. Some of these activities are briefly described in the summaries of the responses to other questions in this section, and in the summaries of the presentations by the participants.

R&D activities mentioned by participants, but which are not described elsewhere in this report, include the following:

EdF R&D is conducting a research project on PSA called SPINOSA. The objective of the project is to develop modelling approaches to accurately evaluate the full impact of digital equipment and systems on plant safety and availability. This project seeks to integrate the following disciplines: PSA, software and digital design, electronics, and human factors.

HRP is carrying out research on the following topics: dependability of software-based systems, addressing strengths and weaknesses of different methods for probabilistic modelling of DIC systems, and collecting data for the project "COMPuter-based Systems Important to Safety (COMPSIS)."

KAERI is working on quantifying software failure probability, fault coverage of DIC systems with fault-tolerant mechanisms, and the validity of automated periodic test. These topics were identified based on the results of previous research. They are planning to establish a standard framework for probabilistic modelling of DIC systems within 4 years.

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

Please see the discussion on recommendations for further R&D work in the next chapter.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

Several organisations stated that they have used risk information related to digital systems for decision-making. The representative from CNSC mentioned that they employed the reliability evaluation of a digital shutdown system to determine test intervals of equipment because meeting a system reliability target is a regulatory requirement in Canada; a risk-informed approach was used for plant and system design of new NPPs. The representative from VTT indicated that a PSA is used for various applications, and that the DIC systems are part of the PSA. Further, these systems are assigned reliability targets from the points of view of plant safety and availability, and that compliance with these targets must be demonstrated. The representative from JNES pointed out that this kind of information was used in evaluating the effectiveness of accident management measures of ABWRs and the latest PWR. KAERI employed this type of information for modifying the design of a safety-critical DIC system. BNL stated that U.S. vendors included models of some DIC systems in the PSAs of advanced NPPs, and that these PSAs were required for the design certification of these plants.

b) What decision making do you foresee that would use risk information related to digital systems?

Several organisations proposed some uses of risk information related to digital systems for decision-making. CNSC's representative stated that risk information will figure increasingly in the design process of new NPPs. The representatives from VTT and KAERI mentioned the analyses of design changes of DIC systems, and regulatory applications, such as acceptance of these systems and their upgrades. The representative from JNES also suggested evaluating the adequacy of the design of these systems, assessing their test and maintenance interval, and judging compliance with a safety goal.

The representatives from BNL pointed out that the U.S. nuclear industry is considering replacing safety-related and non-safety-related analog systems with digital ones. Possibly, some submittals from licensees to the NRC requesting approval of these changes will use risk information. It also might be used in other licensing applications, e.g., in submittals for changes to Technical Specifications.

EPRI proposed to use risk information for determining the value of diversity in the performance of defense-in-depth and diversity evaluations.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

Many participants responded positively to this question. The BNL representatives pointed out that developing an inventory and categorising digital systems is one subject being considered in NRC's new 5-year research plan.

b) *If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?*

The CNSC representative proposed to categorise systems according to the importance of the system and the purpose of the model of the system. Similarly, the representatives from VTT and KAERI suggested categorising systems according to the importance of their functions; the INER representative mentioned using the results and insights from the PRA for this purpose. The EPRI response to the questionnaire stated that categorisation should be carried out by separating non-safety-related (NSR) process-control systems from SR protection systems, as failure modes and modelling techniques applicable to one will not necessarily be relevant to the other. The EPRI response also indicated that categorisation should consider the specific application (use) of the system.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

Some organisations provided some relevant topics that are more detailed aspects of the topics discussed under the previous questions. Hence, they are not described here; readers are referred to Appendix B that contains the responses from the organisations to these 15 topics.

15. From the topics above, which do you consider most important to address, and why?

The following table summarises the topics that participants considered most important.

Organisation	Identification of Failure Modes	Dependencies	Coverage by Fault-Tolerant Features	Failure Data	Software Failures	Human Reliability Related to DIC Systems
CNSC			X			
IRSN, EdF, AREVA						X
GRS		X		X	X	
JNES				X		X
KAERI			X		X	X
INER	X				X	
BNL	X			X	X	
OSU		X				X

Most organisations selected software failures and human reliability related to DIC systems as the most important topics. Failure data also were considered as important. The other three topics in the table were deemed important by one or two organisations.

The following "higher-level questions" were regarded more important by VTT than those presented in the above table: Integrated safety analysis methods, communication of results, and handling of reliability requirements.

3. CONCLUDING REMARKS ABOUT TECHNICAL MEETING

During the WGRisk technical meeting, the participants presented their research and discussed various topics on reliability modelling of digital instrumentation and control (DIC) systems, including their ideas on what additional research should be performed. In addition, some participants provided written responses to the list of topics distributed prior to the meeting. It became obvious that different organisations have developed reliability models of digital systems with very different scopes and levels of detail. The participants agree that the current methods for modelling digital systems need to be improved. Sections 3.1 and 3.2 summarise the discussions during the meeting and the areas of research that the participants identified as having potential to enhance the state of the art, respectively.

3.1 Summary of Discussions

The focus of the WGRisk activity on digital instrumentation and control (DIC) systems is on current experiences with reliability modelling and quantification of these systems in the context of PSAs of NPPs. The principal mechanism for the discussion of these experiences is the technical meeting described in this report. The objectives of this meeting were to make recommendations regarding current methods and information sources used for quantitative evaluation of the reliability of DIC systems for PSAs of NPPs, and identify, where appropriate, the near- and long-term developments that would be needed to improve modelling and evaluating the reliability of these systems.

Presentations were made at the meeting by research institutions, international regulators, industry organisations, and academicians. The presentations either addressed the entire process for developing and quantifying reliability models of DIC systems, or some particular aspects of the associated methods or data.

The meeting provided a useful forum for the participants to share and discuss their respective experiences with modelling and quantifying DIC systems. Group discussions addressed the fifteen technical areas that were distributed to the participants prior to the technical meeting, i.e., the principal topics associated with DIC system reliability modelling and quantification. It was recognised that although many studies have been performed in various countries, the models of DIC systems developed so far have a wide variation in terms of scope and level of detail, and there was a spectrum of opinions on what is an acceptable method for modelling digital systems. In particular, those organisations that developed digital I&C reliability models at a higher level of detail were less concerned about some of the modelling challenges associated with a more detailed level of modelling. In general, the participants believed that the contribution of software failures to the reliability of a DIC system should be accounted for in the models. However, this is probably the most vexing issue associated with probabilistic modelling of DIC systems. It was generally agreed that software may fail differently than hardware. Many participants considered it impractical to obtain and/or use software failure data. Some organisations have attempted to quantify software failure probability in limited applications. Some others have included software failures in reliability models as simple common-cause-failure events and quantified them using expert judgment. The participants agreed that probabilistic data are scarce, so there is an urgent need to address this shortcoming. Summarising, the participants recognised that several difficult technical challenges remain to be solved in the fields of modelling and evaluating the reliability of DIC systems, presented their progress in these fields, and reached general consensus on the need to continue the research and development activities to address these challenges.

Near the end of the technical meeting, each organisation identified the near- and long-term developments that it believed were most needed to enhance the capability for developing and quantifying reliability models of DIC systems. Several ideas were promulgated, such as collecting more digital I&C (hardware components and possibly software) failure data and an international collaborative effort to obtain additional failure data, though a concern was raised regarding the amount of data that would be available, especially considering the pace of technological change. Some of the other proposed ideas include further work on (1) evaluating fault-tolerance mechanisms, (2) dynamic modelling, (3) developing a complete digital system operational profile, (4) identifying digital component failure modes (including developing a taxonomy), and (5) developing methods for addressing software failures. Several participants suggested an international benchmark exercise, where different methods would be applied to the same system (or systems). This exercise potentially would shed additional light on the strengths and limitations of current approaches, methods, and probabilistic data.

3.2 Proposed Areas of Research

This section gives a summary of the areas of research that the technical meeting participants identified as having potential to enhance the state of the art. These areas of research were grouped into the following three categories: Method development (Section 3.2.1), data collection and analysis (Section 3.2.2), and international cooperation (Section 3.2.3).

3.2.1 Method Development

Modelling of software failures

Software is the most unique feature of digital systems and its contribution to system unavailability should be included in reliability models of the systems. Most participants include failure rates or probabilities in their models, and agree that it is a reasonable way to include the contribution of software failures in a reliability model. The participants recognize the difficulties in doing so, and a few research ideas were suggested and described below.

All participants agree that software reliability should be quantified and think it is important to develop methods for quantifying software reliability.

It was pointed out that typically digital systems have several redundant channels that use the same software that may be subject to CCF. Several participants pointed out that software CCF is an important contributor to system failure and suggested to develop approaches for accounting for this contribution.

Two participants pointed out that some experts question the meaningfulness and usefulness of modelling software failures in terms of failure rates and probabilities, and suggested to perform research on the theoretical, i.e., philosophical and mathematical, basis for doing so.

One participant suggested that quantification of software reliability can be carried out using testing, taking into account the context of the software.

Another participant suggested that in modelling and quantifying software failures, it is important to consider failures due to incorrect requirements. Hence, it would be helpful to conduct research to understand the issues associated with this kind of failure, so that they can be accounted for in the models.

Coverage estimates

Digital systems have fault tolerant features, e.g., watchdog timers and test and backup computers, that can potentially detect failures and initiate mitigation actions to prevent the failures from developing into more

serious incidents. This is one of the benefits of digital systems. Five participants pointed out that in order to properly capture the benefits of such features, it is necessary to develop methods and/or data for modelling them. An important issue of the modelling is estimating the fraction of failures that a particular feature is capable of detecting, i.e., its coverage. The estimation should take into consideration the detailed designs of such features, and possibly make use of fault injection experiments.

Human reliability analysis

Digital upgrades at current NPPs and the designs of new reactors introduce new human- system interfaces that are significantly different from those of existing plants. Most participants agree that it may be useful to perform HRA method research to address these new interfaces in support of PSAs for both existing plants and new reactors. In particular, one participant emphasised that special consideration should be given to the maintenance of the digital equipment. Another participant suggested developing or evaluating HRA methods in the context of the new main control rooms (MCRs) that use these systems. The representatives from two organisations indicated that it may be useful to develop and use a simulator of these MCRs for this purpose.

Dynamic methods

Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. It was generally agreed there are currently no clear indications that the use of dynamic methods in modelling software-based protection systems offers considerable improvements. However, several participants indicated that such methods might be warranted when modelling software-based control systems. Several organisations are carrying out research projects in this area and some pointed out that the benefits of the research include evaluating the added value of dynamic methods and helping to identify weaknesses of a system. One organisation considers that a study to apply dynamic methods in a full-scale PSA is needed to demonstrate their ability to improve modelling, but considers the research to have a low priority.

Identification of software and hardware failure modes

Typically, it is necessary to identify all the failure modes of the components of a system to develop a reliability model of that system. However, for digital systems, there are no commonly accepted lists of failure modes of digital components. This is due to insufficient operating experience with the new technology and the fact that digital system failure modes can be defined at different levels of detail. Two participants pointed out that the failure modes of components that are currently used may not be complete, and organisations may have different interpretations of the meaning of a failure mode. Hence, it may be desirable to carry out research to identify failure modes in a more comprehensive way. One suggestion was to develop a list of agreed-upon failure modes that all organisations would use. This would have several benefits, such as a more comprehensive list of failure modes, and it would allow a straightforward way to compare models developed by different organisations.

Impacts of FMs

The effects on a digital system of an individual component failure mode are hard to predict because of the complexity of (1) the digital system, i.e., complex interconnections between the system's components; and (2) the internal logic of each component, usually implemented in software. It is even more difficult to assess the failure effects of combinations of failure modes of multiple components. It was pointed out that it is important to determine the effect of an individual failure mode of a component and of combinations of failure modes on the associated system, i.e., propagation of the effects from component level to system

level. Research on this topic would be beneficial to make the probabilistic models of DIC systems more realistic.

In addition to the above research ideas, the following suggestions on method development were made:

1. Investigate dependencies introduced by digital systems, e.g., communication. Dependencies introduced by digital systems between initiating events and/or one or several mitigation systems could be an important risk contributor.
2. Research the treatment of uncertainties. Since the current models of DIC systems have significant parameter, model, and completeness uncertainties, addressing uncertainty is a relevant area of investigation.
3. Establish reliability targets or limiting values based on the design of a DIC system. For example, if the system meets specified design requirements, then its reliability is at least a certain value.
4. In the long term, develop tools and standards on modelling digital systems.

3.2.2 Data Collection and Analysis

Most participants consider existing models of digital systems suffer from scarcity of hardware failure data. There is an urgent need to collect applicable data. This is particularly important in the case of CCF parameters, which often dominate the results. On the other hand, there was a spectrum of opinions on the specifics of the data needed, in large part because different levels of detail of modelling were performed by the participants. Possible sources of data that can be used include operating experience at nuclear and non-nuclear facilities and vendor data. One participant proposed a possible approach by creating a clearinghouse for collecting the data that guarantees the anonymity of the sources of the data. This would overcome proprietary or confidential issues. This idea is similar to that of the COMPSIS (Computer-based Systems Important to Safety) project of the CSNI discussed under International Cooperation, below.

In the case of software failure data, due to the uniqueness of software failures, it is not practical to use operating experience as the only source for estimating software failure rates or probabilities. Operating experience can possibly be used to identify software failure modes to be included in reliability models. Methods for quantifying software reliability remain to be developed.

3.2.3 International Cooperation

The following main areas of international cooperative research on digital system modelling were suggested:

- Sharing approaches, methods, probabilistic data, results, and insights gained from relevant projects among NEA members
- Jointly developing methods on software modelling, quantification of software reliability, assessing the effect of failures of components of a DIC system on the system, reliability modelling of a DIC system, and HRA
- Performing benchmark studies of the same systems to share and compare methods, data, results, and insights
- Enhancing COMPSIS to address PSA needs or creating a new system to obtain probabilistic data
- Publishing technical documents, such as “CSNI Technical Opinion Papers,” and papers in journals and conferences.

These areas are briefly discussed below.

Given the difficult technical challenges that remain to be solved in the fields of modelling and evaluating the reliability of DIC systems, it is advisable that the organisations participating in the workshop, as well as other organisations in countries that are members of NEA, continue their research and development activities in these fields.

It is also advisable to establish a means for sharing the approaches, methods, probabilistic data, results, and insights gained from relevant projects of each organisation with the other member countries of NEA. For example, the dedicated WGRisk DIC website (or a similar website) may be used as an exchange mechanism for this purpose.

Furthermore, organisations of countries that are members of NEA can jointly carry out research on particularly important but challenging technical fields, such as methods for software modelling, quantification of software reliability, assessing the effect of failures of components of a DIC system on the system, reliability modelling of a DIC system, and HRA. In addition, some digital systems can be jointly selected for performing benchmark studies of common systems to share and compare methods, probabilistic data, results, and insights.

Currently, the COMPSIS project allows sharing of operating experience among the member countries to obtain insights and lessons learned resulting from events related to DIC systems. However, it is not specifically designed to address PSA needs. While the coding guidelines and design of the database recently have been changed such that in principle the estimation of reliability parameters is facilitated, there are several obstacles and principle limitations. These include the heterogeneousness of the populations and the large variability in pedigree of data collected in different countries, as well as difficulties in determining the number of operating hours or demands of the populations from which the failure data were collected. Since probabilistic data are necessary for quantifying models of DIC systems, enhancing COMPSIS to address PSA needs or creating a new system for obtaining these data would be beneficial.

The CSNI publishes documents on nuclear safety. In particular, it publishes “CSNI Technical Opinion Papers” which focus on specific areas of nuclear safety, such as PSA-based event analysis. It is proposed that some of these papers could be prepared on some of the areas identified in this chapter by some of the participants (or other relevant experts from the NEA member countries) having expertise in each specific area. In this way, more specific insights and recommendations are expected to be obtained that would benefit all the NEA member countries, and possibly other members of the nuclear safety community.

4 RECOMMENDATIONS

The results of the October 2008 technical meeting and a summary set of TG recommendations were discussed as part of the WGRisk annual meeting on March 25-27, 2009. During this meeting the WGRisk membership was, in general, supportive of the recommendations. The following recommendations reflect the results of the group discussion during this meeting and subsequent, post-meeting comments.

Method Development

- Develop a taxonomy of hardware and software failure modes of digital components for common use
- Develop methods for quantifying software reliability
- Develop approaches for assessing the impact of failure modes of digital components
- Develop methods for estimating the effect of fault-tolerant features of a digital system on the reliability of the system's components
- Address human-system interfaces unique to digital systems and associated human reliability analysis
- Evaluate the need and approaches for addressing dynamic interactions

Data Collection and Analysis

- Collect hardware failure data, including common cause failures, that can be used for PRA purposes
- Use operating experience for identifying software failure modes to be included in reliability models

International Cooperation

- Sharing approaches, methods, probabilistic data, results, and insights gained from relevant projects among NEA members
- Jointly developing methods on software modelling (including CCF), quantification of software reliability, assessing the effect of failures of components of a DIC system on the system, reliability modelling of a DIC system, and HRA
- Performing benchmark studies of the same systems to share and compare methods, data, results, and insights
- Publishing technical documents, such as "CSNI Technical Opinion Papers," and papers in journals and conferences

5 REFERENCES

1. Chu, T.L., Martinez-Guridi, Yue, M., Lehner, J., and Samanta, P., "Traditional Probabilistic Risk Assessment Methods for Digital Systems," NUREG/CR-6962, October 2008.

2. Department of Defense, AProcedures for Performing a Failure Mode, Effects, and Criticality Analysis, Military,@ Standard 1629A, Notice 2, November 1984.

3. International Electrotechnical Commission, "Function Safety of Electrical/Electronic/ Programmable Safety-Related Systems," Parts 1-7, IEC 61508, 2000.

4. International Electrotechnical Commission, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions," IEC 60880, 2nd Edition, 2006.

5. Reliability Analysis Center (RAC), "PRISM User's Manual, Version 1.4," Prepared by Reliability Analysis Center Under Contract to Defense Supply Center Columbus.

APPENDIX A

LIST OF PARTICIPANTS

CANADA

Mr. Taeyong SUNG
Specialist
CNSC
280 Slater Street
Ottawa, Ontario

Tel: +1 613 943 0015
Fax: +1 613 995 5086
Eml: taeyong.sung@cnsc-ccsn.gc.ca

CHINESE TAIPEI

Dr. Chun-Chang CHAO
Institute of Nuclear Energy Research
P.O. Box 3-3, Lung Tan, Tao Yuan, 325
Taiwan, R.O.C.

Tel: +886 3 471 1400 Ext 6008
Fax: +886 3 471 1404
Eml: chuncchao@iner.gov.tw

Mr. Ching-Hui WU
Assistant Researcher
Institute of Nuclear Energy Research
P.O.Box 3-3, Lung Tan, Tao Yuan, 325
Taiwan, R.O.C.

Tel: +886 3 471 1400 Ext.6059
Fax: +886 3 471 1404
Eml: chwu2@iner.gov.tw

Dr. Swu YIH
Ching Yun University
229 Jiansing Rd
Jhong Li City
Taiwan, R.O.C

Tel: +886 3 458 1196 Ext. 7713
Fax: +886 3 250 3013
Eml: swuyih@cyu.edu.tw

FINLAND

Dr. Jan-Erik HOLMBERG
Senior Research Scientist
VTT
P.O. Box 1000
FIN-02044 VTT

Tel: +358 20 722 6450
Fax: +358 20 722 6752
Eml: jan-erik.holmberg@vtt.fi

FRANCE

Dr. Marc BOUISSOU
Electricité de France (EdF) R&D
MRI Dept
1 avenue du Général de Gaulle
92141 Clamart

Tel: +33 1 47 65 55 07
Eml: marc.bouissou@edf.fr

Mr. Hervé BRUNELIERE
AREVA
Tour AREVA
Place de la Coupole, La Défense

Tel: +33 1 34 96 75 89
Eml: herve.bruneliere@areva.com

Mr. Gilles DELEUZE
EdF
1 avenue du Général de Gaulle
92141 Clamart
Tel: +33 1 47 65 46 30
Eml: gilles.deleuze@edf.fr

Mr. Jean-Luc DOUTRE
EdF
EDF CNEN
Tel: +33 1 41 48 93 68
Fax: +33 4 72 82 7155
Eml: jean-luc.doutre@edf.fr

Mr. Gabriel GEORGESCU
Reliability and Safety Engineer
IRSN/RSD
Systems and Risk Protection Assessment Department
B.P. N°17
92262 Fontenay-aux-Roses Cedex
Tel: +33 1 58 35 81 08
Fax: +33 1 58 35 91 71
Eml: gabriel.georgescu@irsn.fr

Mr. Franck JOUANET
EdF
1 avenue du Général de Gaulle
92141 Clamart
Tel: +33 1 47 65 39 88
Eml: franck.jouanet@edf.fr

Dr. Jeanne-Marie LANORE
Scientific Advisor - IRSN/DSR
B.P. N°17
92262 Fontenay-aux-Roses Cedex
Tel: +33 1 58 35 76 48
Fax: +33 1 42 53 91 54
Eml: jeanne-marie.lanore@irsn.fr

Mr. Richard QUATRAIN
EdF
1 avenue du Général de Gaulle
92141 Clamart
Tel: +33 1 47 65 59 67
Eml: richard.quatrain@edf.fr

Mr. Pascal REGNIER
IRSN
Deputy Manager I&C Section
B.P. 17
92262 Fontenay-aux-Roses Cedex
Tel: +33 1 58 35 81 84
Fax: +33 1 58 35 91 71
Eml: pascal.regnier@irsn.fr

Mr. Nguyen THUY
EdF
Tel: +33 1 30 87 72 49
Eml: n.thuy@edf.fr Fax:

GERMANY

Mr. Ewgenij PILJUGIN
Gesellschaft für Anlagen-und
Reaktorsicherheit (GRS) mbH
Forschungsinstitute
85748 Garching
Tel: +49 89 04 470
Fax: +49 89 04 10470
Eml: Ewgenij.Piljugin@grs.de

Dr. Jan STILLER
Gesellschaft für Anlagen-und
Reaktorsicherheit (GRS) mbH
Schwertnergasse 1
50667 Köln

Tel: +49 221 2068 932
Fax: +49 221 2068 709
Eml: Jan.Stiller@grs.de

HUNGARY

Mr. Tibor KISS
Assessment Section
NPP Paks
P.O. Box 71
7031 PAKS

Tel: +36 75 508 978
Fax: +36 11 551 332
Eml: kisst@npp.hu

ITALY

Dr. Enrico ZIO
Energy Department
Polytechnic of Milan
Via Ponzio 34/3
20133 Milano

Tel: +39 02 2399 6340
Fax: +39 02 2399 6309
Eml: enrico.zio@polimi.it

JAPAN

Mr. Keisuke KONDO
JNES
Kamiya-cho MT Bldg., 4-3-20
Toranomon, Minato-Ku
Tokyo 105-0001

Tel: +81 3 4511 1553
Fax: +81 3 4511 1598
Eml: kondo-keiske@jnes.go.jp

KOREA (REPUBLIC OF)

Dr. Hyun Gook KANG
Korea Atomic Energy Research Institute (KAERI)
150, Daedok-daeto, Yuseong-gu
Daejeon

Tel: +82 42 868 8884
Fax: +82 42 868 8256
Eml: hgkang@kaeri.re.kr

Dr. Man Cheol KIM
Korea Atomic Energy Research Institute (KAERI)
150, Daedok-daeto, Yuseong-gu
Daejeon

Tel: +82 42 868 2200
Fax: +82 42 868 8256
Eml: charleskim@kaeri.re.kr

UNITED STATES OF AMERICA

Dr. Tunc ALDEMIR
Department of Mechanical Engineering
The Ohio State University
427 Scott Laboratory
201 West 19th Avenue
Columbus, OH 43210

Tel: +1 614 292 4627
Eml: aldemir.1@osu.edu

Dr. Tsong-Lun CHU
Brookaven National Laboratory
Building 130
P.O Box 5000
Upton, NY 11973-5000
Tel: +1 613 344 2389
Fax: +1 613 344 5730
Eml: chu@bnl.gov

Dr. Sergio GUARRO
ASCA, Inc.
1720 South Catalina Ave., Suite 220
Redondo Beach, CA 90277
Tel: +1 310 316 6249
Fax: +1 310 316 6972
Eml: sergio.guarro@ascainc.com

Mr. Bruce P. HALLBERT
Idaho National Laboratory
PO Box 1625
Mail Stop 3605
Idaho Falls, ID 83415-3605
Tel: +1 208 526 9867
Fax: +1 208 526-2777
Eml: bruce.hallbert@inl.gov

Mr. Prince KALIA
NASA-GSFC, S&MA-B6/W119
8800 Greenbelt Rd
Greenbelt, MD 20771
Tel: +1 301 286 7685
Fax: +1 301 286 1701
Eml: prince.m.kalia@nasa.gov

Mr. Alan KURITZKY
U.S. Nuclear Regulatory Commission
Mail Stop CSB-4-C07M
Washington, DC 20555
Tel: +1 301 251 7587
Fax: +1 301 251 7435
Eml: alan.kuritzky@nrc.gov

Mr. G. MARTINEZ-GURIDI
Brookhaven National Laboratory
Building 130
P.O. Box 5000
Upton, NY 11973-5000
Tel: +1 613 344 7907
Fax: +1 613 344 5730
Eml: martinez@bnl.gov

Dr. Carol SMIDTS
Department of Mechanical Engineering
The Ohio State University
418 Scott Laboratory
201 West 19th Avenue
Columbus, OH 43210
Tel: +1 614 292 6727
Eml: Smidts.1@osu.edu

Dr. Ronaldo H. SZILARD
Director, Nuclear Science and Engineering
Idaho National Laboratory
2525 Freemont Ave
P.O. Box 1625, MS 3860
Idaho Falls, ID 83415-3860
Tel: +1 208 526 8376
Fax: +1 208 526 2930
Eml: Ronaldo.Szilard@inl.gov

INTERNATIONAL ORGANISATIONS

OECD/Halden Reactor Project, Institutt for Energiteknik, Halden

Dr. Bjorn Axel GRAN
Institutt for Energiteknikk
OECD - Halden Reactor Project
Os Allé 13
P.O. Box 173
N-1751 Halden
Norway

Tel: +47 69 21 2395
Fax: +47 69 21 24 40
Eml: bjorn.axel.gran@hrp.no

OECD Nuclear Energy Agency, Issy-les-Moulineaux

Dr. Abdallah AMRI
OECD-NEA/Nuclear Safety Division
Le Seine St-Germain
12 bd des Ile
F-92130 Issy-les-Moulineaux
France

Tel: +33 1 45 24 10 54
Fax: +33 1 45 24 11 29
Eml: abdallah.amri@oecd.org

APPENDIX B

Compilation of Received Responses to the 15 Technical Areas

CNSC RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Yes, the digital component important to safety should be modelled in a probabilistic way. CNSC regulations and industry standard require licensees perform quantitative analysis of digital I&C system.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      CANDU reactors have used digital I&C system for the safety function as well as the safety related control function for decades and licensees have developed probabilistic models of them.

   c) *For what purpose have these models been developed?*

      The probabilistic model has been developed i) for evaluating a system unavailability in accordance with the CNSC regulation or licensees' internal program and/or ii) for integrating to plant level probabilistic safety assessment.

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      There is no detailed standard or guidance to develop or review the probabilistic model of digital I&C system.

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      Most of the probabilistic models include not only hardware but also software. However some models include only the hardware failure.

f) Have the models been integrated into a PSA model of an entire NPP?

As indicated in c, the probabilistic models are integrated into PSA model in two ways *i) a mitigating system and ii) initiating events.*

g) Can you make available at the technical meeting any publications documenting your work in this area?

All documents are proprietary of licensees.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

All models use traditional fault tree method for the probabilistic model of Digital I&C system.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

No, there is no issue to integrate the digital I&C model with the PSA because the plant level PSA also uses ET/FT approach.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Same fault tree approach is using for continuous control system and protection system, but different failure modes are used.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

The level of detail varies licensee by licensee, but the level is not detailed than card or board level.

b) Why was this level of detail used?

The availability of failure data is main reason to define level of detail; most of vendors usually provide the reliability estimation data in board level or even whole equipment level.

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

The level of detail should be determined by two major considerations;

- The objective of model: It is believed that the objective of model is most critical factor to determine the level of detail associate with the importance of the system to plant risk. When the model is used for system level risk-informed approach, the level of detail should have appropriate level of detail.

- The modelling requirement: However, the level of detail is sufficient to meet the adequacy of PSA requirements, for instance the system model has to have sufficient level of detail to model inter/intra system dependencies.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?

There is no clear systematic approach employed to identify the failure modes. However considered the fault tree approach and the level of detail applied, the failure mode identification is not a major issue in digital I&C modelling in existing CANDU reactors.

b) Do you consider operating experience in identifying failure modes?

Operating experience is very important, but more careful treatment is required due to the unique aspects of digital I&C system. Most observed failures of protection system are safe failures, therefore the model can not use directly the experience data.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

It depends on the level of detail and specific system design features, but the bottom line is all applicable failure modes have to be captured in the model. Two different responsibility and approaches are expected;

- For system level: PSA analyst is responsible to indentify the failure mode and effect, but
- For component or equipment level: manufacture is responsible to do with the clear definition of system (equipment) function by system designer.

And

- For protection system: any systematic approach for instance, FMECA or HAZOP
- For control system: HAZOP seems to be more appropriate

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

Same answer of c.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

- Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

- Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

- Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

- Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

- Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

- Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

While CANDU probabilistic model in PSA includes all dependencies which are able to be modelled in system model explicitly (A, B, C, D), it did not include a residual dependency (CCF)

(F) traditionally. Even though industries start to model the CCF in the PSA model, the methodology and ways to model varies.

b) Did you find any of these dependencies to be risk significant?

The contribution of digital I&C system is not risk significant due to the unique CANDU I&C architecture with defense in depth concept.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Present method in dependency modelling is considered not sufficient to identify the residual dependencies especially for hardware failures.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

It is believed that the protection system dose not required to model the dynamic interaction because the accident sequence model somewhat take into account the dynamic effects. For instance a reactor trip model credits a redundant trip parameter after failure occurs in a primary trip parameter. However the dynamic effect is more relevant to the continuous control system. It seems to be an applicable issue same as the conventional analog I&C system model has.

b) Have any dynamic methods been used in your country for modelling digital systems?

No, there is no dynamic approach in probabilistic modelling directly. Even though the dynamic method is used to generator failure data of a certain component / equipment, it is integrated into PSA in static way.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

Vendor data is usually used for hardware failure data, but it is believed to be conservative. The probabilistic model uses reliability allocation value or/and expert judgment for software failures.

b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

There is no CCF modelling yet. One licensee estimate CCF parameters using UPM (Unified Partial Method (ISBN-085 356 4337)), which is developed in UK to model dependant failure.

c) *What method did you use for processing these raw data into failure parameters, such as failure rates?*

Industry uses Bayesian approach to integrate operating experience.

d) *What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?*

The probabilistic model uses reliability allocation value or/and expert judgment for software failures.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) *How do you account for the impact of software failures on system reliability?*

Probabilistic model explicitly includes the software failures. The failure is treated as a dependent failure in redundant components.

b) *How realistic is your approach for accounting for this impact?*

More R&D result is necessary to determine it.

c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

It is believed that the reliability evaluation should explicitly model the software failure quantitatively.

d) *Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?*

There is no interaction between software and hardware in the model.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) *How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?*

Uncertainty is not clearly addressed in the model.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

    a) *What methods are used in your country for modelling human errors associated with digital systems?*

       There is no special approach to model the human error associated with the digital I&C system. The human error issues seem to be more relevant to the digitalised control room rather that the safety class protection system.

    b) *Are there any available data associated with the probability of this kind of error?*

       There in no available data for human errors associated with digital I&C system.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

    a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

       There is no active R&D in reliability modelling of digital systems in CNSC.

    b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

       A research project is planned for evaluating the coverage of fault tolerance mechanism.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

    a) *Has risk information related to digital systems already been used for decision making in your country?*

       The reliability evaluation of the digital shutdown system has been used to determine test interval of equipment because system reliability target is a regulatory requirement in Canada. New reactor design also uses risk informed approach for plant and system design.

    b) *What decision making do you foresee that would use risk information related to digital systems?*

       New reactor design will use more risk information during design process.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

    a) Do you consider that this kind of categorisation is feasible and practical?

    The categorisation is a common approach in PSA. A screening approach for HRA and CCF may be good examples of the categorisation approach.

    b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

    It is believed that the major factors of categorisation are the importance of the system and purpose of model.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

    - Fault tolerance coverage
    - Reliability and effectiveness (coverage) of online test device
    - Dependency modelling of software failure

15. From the topics above, which do you consider most important to address, and why?

    The coverage estimation of fault tolerance or test devices (mechanisms) is considered most important, because these features are most advantageous aspect of digital I&C systems and most of digital I&C system must have the features and the coverage will be a critical factor to determine the reliability of the D I&C system.

VTT RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Yes. They should be accounted as a part of the whole system design, and their failure probabilities should be modelled as the probability that the system enters a state where the failure emerges.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      In research projects, the following approaches have been tried out specifically for digital systems. 1) Bayesian belief network (BBN), 2) Dynamic flowgraph method (DFM)

   c) *For what purpose have these models been developed?*

      BBN: Estimation of the reliability of software based components
      DFM: Modelling and estimation of the reliability of distributed control systems

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      BBN: BBN literature, expert judgement literature
      DFM: DFM literature

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      Both

   f) *Have the models been integrated into a PSA model of an entire NPP?*

      No

g) Can you make available at the technical meeting any publications documenting your work in this area?

BBN reports and papers are publicly available. DFM work is in progress

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

Responses below are from the present PSA praxis point of view.

a) What modelling method or methods have been used in your country for modelling digital systems?

FT

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

No difference

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Same

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

It varies. Sometimes the whole control system is a black box, but sometimes analysis and modelling is broken down to processing unit and module level.

b) Why was this level of detail used?

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

As for all systems, the system reliability model should represent all relevant functional dependencies from the safety tasks point of view. For many purposes, the system/software architecture level is sufficient, because of time constraints and because testing and inspection can guarantee to an adequate

degree that individual digital/software components meet their specifications. On the other hand, available reliability data determines level of details of the model.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

   a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

      FMEA

   b) *Do you consider operating experience in identifying failure modes?*

      Implicitly yes, and some checks may be done. However, failure modes should be standardized, and the question is to use operating experience to review the standardized failure modes. Operating experience is also valuable for determining effects of a failure mode.

   c) *How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?*

      It's a matter of IC expert to assist here. Effects should be defined from the safety tasks point of view.

   d) *How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?*

      Can be difficult, but principally it happens in the same way as for a single failure mode.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

   A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

At least A, B, C and F should be included. D and E are more difficult to capture at least in traditional fault tree/event tree models.

b) Did you find any of these dependencies to be risk significant?

B and F

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Not necessarily. D and E may be important. In addition it can be difficult to define effects of failure modes, e.g. effect of smoke for I&C systems.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

It is a research problem to find the appropriate level of accuracy of the model.

b) Have any dynamic methods been used in your country for modelling digital systems?

In research purposes. On the other hand, dynamic methods have been used for level 2 PSA (STUK PSA tool).

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) *What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?*

      Raw data are available only in rare cases. For older components, there may be data in the plant's maintenance systems. For new components, it is dependent on vendor/manufacturer's willingness to provide data.

   b) *What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?*

      Principally same answer as for question a), but for CCF there is hardly any raw data.

   c) *What method did you use for processing these raw data into failure parameters, such as failure rates?*

      In case raw data is available, standard reliability parameter estimation methods are used (Bayesian, frequentist).

   d) *What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?*

      See c.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) *How do you account for the impact of software failures on system reliability?*

      As failure modes of a computer-based system

   b) *How realistic is your approach for accounting for this impact?*

      It is realistic if failure modes are realistic

   c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

      To model failure modes and effects of computer-based systems is essential. To explicitly evaluate failure causes is not necessary in a reliability analysis, unless there is a need to improve software reliability.

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

Not necessarily. Functions and failure modes are addressed.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

Same way as for other components and systems. Parametric uncertainties are mainly addressed by assessing uncertainty distributions for the parameters. All uncertainties are addressed qualitatively in a qualitative uncertainty analysis. Sensitivity studies may be performed, e.g., to study the importance of CCF assumptions or importance of reliability parameter estimates used.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

Normally, human errors are not explicitly addressed, or the approach is not different from other types of systems.

b) Are there any available data associated with the probability of this kind of error?

Presumably no for the estimation of probabilities. Event reports might be used in estimating the probabilities.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

Development of methods and tools for reliability modelling of digital control systems

b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

Development of methods for the estimation of failure probabilities. They are needed already.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) *Has risk information related to digital systems already been used for decision making in your country?*

Yes. 1) Assessment of reliability of digital systems is part of PSA, and PSA is used for various applications. 2) Digital systems have typically reliability targets (plant safety and availability point of view), and the compliance with the reliability targets must be shown.

b) *What decision making do you foresee that would use risk information related to digital systems?*

Licensing related, selection between design alternatives.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) *Do you consider that this kind of categorisation is feasible and practical?*

Categorisation from the (functional) safety importance point of view is practical.

b) *If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?*

By means of a systems analysis (which systems/failure events are important, which are not)

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

Integrated safety analysis methods, communication of results, handling of reliability requirements

15. From the topics above, which do you consider most important to address, and why?

See 14. They are higher level questions.

FRENCH (IRSN-EDF-AREVA) RESPONSES

List of Representatives Contributing to the Reply

IRSN : Gabriel Georgescu, Jeanne-Marie Lanore
EdF : Jean-Luc Doutre, Richard Quatrain, Gilles Deleuze, Nguyen Thuy
AREVA: Herve Bruneliere

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?

   A preliminary list of definitions could be useful: the terms digital systems, digital components, are used and could be understood in different ways by the respondents.

   From our point of view and understanding of the terms, a probabilistic representation of the effects of programmed equipments at the level of a PSA is possible. If we define digital components as subsystems like boards or electronic digital components, we consider that modelling at that level may not be useful for PSA.

   b) Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?

   Yes. EdF developed the Compact Model on the basis on a detailed study, the C03 project, during the 90s, when full digitalised system was introduced in NPP of the version N4. The goal is a representation of the contribution of the components implemented in the control channels to the failure of the protective action

   c) For what purpose have these models been developed?

   They have been developed to represent the effect of digital I&C on safety in the context of a PSA, as much accurately (in qualitative and quantitative terms) as possible

d) What are the standards or guidance that you have used for developing or reviewing these models?

At the time of the development of the compact model as part of the CO3 project, there were no standards on this issue.

e) What is the scope of the models, e.g., do they include hardware and software failures?

We do not speak in terms of hardware or software failures, but in terms of random and systematic failures. Random failures are mostly caused by material (i.e. hardware) failures. Software failures are a very limiting concept that does not necessarily cover the main causes of systematic failures that may be physical, organisational….

f) Have the models been integrated into a PSA model of an entire NPP?

Yes. The compact model enabled EDF to introduce I&C contribution in all of its PSA models, for its existing NPP series (900MW, 1300MW, N4) or coming soon EPR.

g) Can you make available at the technical meeting any publications documenting your work in this area?

The compact model and the plans in EdF for its extension have been presented during the Paris meeting, October 2008. Documentation is available: the compact model is presented in annex A of the IEC 61838 document and in publications.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

The CO3 relied on Markovian models and Petri nets. The compact model is an adaptation of FT formalism.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

No. The compact model introduces I&C failures as fault trees which are easily integrated into the complete model. The level of details avoids huge disproportionate I&C new branches.

c) Control systems versus protection systems?

We do not model the digital systems in detail and how failures can occur. At present time, the continuous control systems are not represented according the compact model, but new questions raised by new EPR NPP (like représentation of some regulations) might lead to extensions.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as

their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

The compact model represents a protection channel in four parts: sensors part, logic part specific to a given protection channel and its processing logic, logic part common to all channels and specific to a programmable controller, and actuation part. Therefore a simple protection channel is then represented with 4 basic events. A more complex one can have some more elements (like various sensors), or be a logic combination of elementary channels.

b) Why was this level of detail used?

It was considered as sufficient for a significant model, given the design and architecture of protection chains in NPP. But, after the very detailed (and costly) representation of I&C in our previous project, the motto was "the simpler, the better". So the idea was to have the most macroscopic modelling, but flexible enough to capture any dependency of channels sharing some material or software parts. For example, there is no point in distinguishing sensors and their associated boards, since failures of each of them will lead to the same channel failures. But we have to model sensor part and logic part in two different basic events, since the sensor part can be the input of several different, and may be diversified, channels.

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

That decision is design and safety level dependent. Of course, the "keep it simple" principle of the compact model has the huge benefit of being operational, and give a rough, but extensive view of I&C contribution among the whole model. One aspect also, that is important, and could be neglected, is to keep interpretation of PSA results (namely minimal cut sets) simple and intuitive. I&C events do scare PSA analysts, who are more confident with pump and valve failures. So it is really important for I&C basic event to be highly clear, in terms of what main feature of what digital system failed.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-

level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?

The final value of the unavailability assigned to the I&C automatic devices essentially comes from systematic failures. The evaluation of their importance is derived from a qualitative assessment based on the quality of these automatic devices. This assessment is independent from the modelling options.

b) Do you consider operating experience in identifying failure modes?

Operating experience is used for hardware (boards, sensors) failures. An annual report is made to gather and analyse failures of protection and operating digital systems of all NPP series.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

Operating experience interpretation is based on expertise of I&C specialists.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

The compact model describes I&C failures in macroscopic events ("loss of pressure measure"). Then combination of elementary component failures can be related to a single basic event, and to justify compact model parameters, the relation between elementary components failures and compact model basic events must be clarified. After that, combination of I&C events (or others) which lead to function losses are handled by the PSA itself.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

The goal is to represent all these types of dependencies, as they are all part of our independence analyses, CCF assessment and/or reliability assessment.

The table summarises the failures represented in the compact model.

Part of Compact Model	System Components	Failures
acquisition	sensors	measuring cell and boards failures
	analogical/digital conversion module	
	transmission of the data to the logic part	
specific logic	redundant boards computing the function	independent and CCF hardware failures
		errors in software specifically developped for the channel
		human errors in operating or in input of the parameters
		functional design errors
		specification errors
common logic	final voters	hardware or software failure of shared components
	input/output boards	design error of I&C (sizing)
	data buses	software error in operating system or in shared functions
	components present on all boards	all CCF due to the use of the same technology
actuation	ESF boards, relays	boards failures

b) Did you find any of these dependencies to be risk significant?

The final value of the unavailability assigned to the I&C automatic devices essentially comes from systematic failures that may be software-related, physical, organisational. The relative importance of the various possible dependencies is specific to each technology, design and organisation.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Yes, we consider that the methods applied for the N4 series is adequate for this series, considering the overall digital I&C architecture and the core damage frequency target. We intend to improve on the methods for the Flamanville EPR unit since the overall digital I&C architecture is different and the core damage frequency target more demanding.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

   a) Do you consider it necessary to accurately model these interactions and their timing?

   The necessity of such models has to be considered after first PSA using non dynamic models. It is not sure there is a need of such models for safety systems, as the design rules used for nuclear protection systems try as much as possible to avoid complex dynamic behaviour.

   b) Have any dynamic methods been used in your country for modelling digital systems?

   Markov based methods have been the most widely used as a support for French PSA.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

   Usual reliability estimates are calculated for hardware according operational experience. For new plants, we use vendor data, but challenge the assumptions.

   b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

   Common cause coefficients (beta factors) are extrapolated from other systems observations. There is currently no international agreement of beta factors estimates for programmed systems. Generic parameters (like a β value of 5% for two components) are generally used, and supposed conservative.

   c) What method did you use for processing these raw data into failure parameters, such as failure rates?

   Usual reliability estimates are calculated for hardware according operational experience. Raw failure rates might have to be interpreted, to distinguish "don't care" failures, failures leading to a signal emission, failures that will block a signal. Other important parameters are ratios of detected (by self testing, or by other system components) or not detected failures. Experts might be interviewed to evaluate ratios.

   d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

   We based our estimates for probabilistic parameters for systematic failures on the detailed analysis of the design and features of the digital systems concerned, on expert judgment, and on generally accepted values for similar systems (international standards).

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) *How do you account for the impact of software failures on system reliability?*

      We analyse in detail the design of digital systems, and in particular the defensive measures taken to prevent specific systematic failure and common cause failure mechanisms. We also analyse in detail aspects such as data communications, diversity, and independence. Based on these analyses, we use expert judgment to determine the probabilities of failure on demand and beta-factors.

   b) *How realistic is your approach for accounting for this impact?*

      There is currently no generally recognised approach for accounting the impact of systematic failures of highly reliable digital systems. We consider our qualitative approach as realistic enough, since it is based on detailed knowledge of digital design and on verifiable evidence and reasoning

   c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

      Software failures are not explicitly modelized. The PSA is interested by functions, considering software and hardware as a whole.

   d) *Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?*

      What we represent in PSA are functions and possibly systems, i.e. digital systems. Digital systems always behave as the result of interactions between hardware and software. They are not analysed or modelled at the level of the PSA, neither using probabilistic models.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

   a) *How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?*

      Data uncertainties have been addressed. I&C basic events are introduced in the PSA model as “fail to start” failure, with a log-normal distribution. Most of the time:

      - Specific logic and common logic values are considered as full expert judgements, and have then an error factor set to 10.
      - For more simple concepts, like sensor parts, or actuation boards, with a straightforward way to estimate average unavailibility from operating experience, error factor is set to 3.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

At present time, three kinds of human/digital system interactions are considered, but all of them are only implicit in the model:

- Human error when entering a safety threshold. After a question by the French Safety Authority, the CO3 project addressed the issue of evaluating the probability of entering a wrong parameter. The operating experience of the 1300MW series was analysed, and also the process of entering a threshold with a HRA point of view. Both methods lead to consider an error probability around 3 10-5 by threshold. This risk is then included, in an implicit way, in the "specific logic" of the compact model, which has a default proposed value of 10-4 for class A digital systems.

- Human error because HSI will fail in carrying operator signal. In EDF, the MERMOS approach evaluates the Human error probability by analysing scenarios and contexts that could lead to a human failure. Among the elements defining the context, failures of HSI might be relevant. Failure parameters, which were transmitted to the French Safety Authority, are used to evaluate probabilities of scenarios. I&C values are in range of compact model values for level 1 I&C. That is, for example, 10-3 for the failure of carrying a specific order, or 10-4 for the failure of the whole HSI. Then the MERMOS method adds up all scenarios probabilities, and the role of HSI becomes implicit.

- Human error when correct information is not available because of HSI and compromise diagnosis. Then again, inclusive values are used, but I&C gets implicit in the final Human error estimation.

A question of the French Safety Authority about dependencies between operator actions and automatic safety functions might lead to explicit this contribution of I&C in human errors.

b) Are there any available data associated with the probability of this kind of error?

There are currently no data available for this topic in France, but, as said before, a few arbitrary probability values that fix an order of magnitude when applying MERMOS HRA method. Future work is planned within the SPINOSA project about this subject.

As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?

In the field of PSA, the main project is the SPINOSA project, leaded by EDF R&D.

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

Additional R&D is needed in other domains than nuclear industry, and for the development of modelling methods.

11. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

There is no position of France about this subject

b) What decision making do you foresee that would use risk information related to digital systems?

There is no position of France about this subject

12. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

Yes.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

We are currently working on the subject, as part of SPINOSA.

13. What other aspects of probabilistic modelling of digital systems do you consider relevant?

It is important that digital systems are not represented in PRA only through their failures: their benefits must also be represented. Human factors aspects of digital technology also need to be further investigated, in terms of benefits and failures.

14. From the topics above, which do you consider most important to address, and why?

The presentation of the SPINOSA project done during the Paris meeting summarises the research planning for 2009-2001 in the domain in France.

GRS RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      We consider it to be meaningful to model failures of digital components in a probabilistic way. We do not see any fundamental difference between software based digital I&C and conventional equipment regarding the principal applicability of stochastic models.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Yes.

   c) *For what purpose have these models been developed?*

      A fault tree model of a software based digital I&C system designed for emergencies (fourth level of defense) was developed by GRS to include this system in the plant PSA (see answer to 2 b).

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      In Germany no special guidelines exist for the modelling of software based digital I&C. The general German PSA guidelines (Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Bundesanzeiger Nr. 207a, 2005) were applied.

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      In a recent PSA study software based I&C equipment was modelled. However, only hardware failures were considered. No reliability data for software specific failures was available. The failures of the digital hardware components, e.g. CPU, computer backplane, digital I/O modules and communication modules were considered in the fault tree model of the safety relevant I&C functions.

f) Have the models been integrated into a PSA model of an entire NPP?

The fault tree model of the hardware of the digital I&C was an integral part of the PSA model of the plant.

g) Can you make available at the technical meeting any publications documenting your work in this area?

The report on the PSA study mentioned above is not publicly available.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

In the recent PSA the fault tree method was applied to software based digital I&C equipment. Only hardware failures were considered.

Currently, there are no special methods available for the consideration of failures related to software (software failure or synergetic failure).

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

The method applied to the hardware of software based digital I&C was identical to the method applied to conventional I&C. A system implementing several I&C functions was modelled. This system is designed for emergencies (fourth level of defense). The technical report describing the work in detail is not publicly available.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Control systems were not modelled. The probability of these systems to initiate an event is directly estimated from operating experience.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.]

What level of detail was modelled in your country?

As stipulated in the German PSA guideline, the fault tree has to have such a level of detail, that basic events do not have any common functional dependencies. The basic events comprise all events that occur on component level and can be described by reliability parameters. Generally, these parameters have a statistical basis.

a) *Why was this level of detail used?*

See the response to question 3a.

b) *Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?*

The **possibility to estimate reliability parameters** from operation experience is an important criterion when choosing an appropriate level of detail.

The level of detail should only be raised as far as necessary (not too detailed).

To determine an appropriate level of detail, an extensive FMEA of the entire I&C system including software is necessary.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

The FMEA is the most important source for the identification of failure modes. Operating experience (generic and plant-specific) is an additional source. In the recent PSA both sources were used. GRS has started to look into the development of a method for collecting and assessing operating experience with respect to software-related failures.

b) *Do you consider operating experience in identifying failure modes?*

See response to question 4a.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

In most cases GRS uses the top-down-approach to develop a fault tree which represents the relevant effects of single and multiple failures of I&C components. Failure modes of the I&C components are determined by an FMEA taking into account relevant operating experience. The bottom-up-approach is only employed for relatively simple systems in special cases, e.g. to model the effects of spurious actuations due to fire or external events.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

See answer to question 4d.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

In the recent PSA the following sources of dependencies were considered:

- communication,
- support systems,
- sharing of hardware.

For dependencies related to CCF (only hardware considered) no reliability data was available.

No methods are available for including:

- dependencies related to dynamic interactions,
- dependencies related to fault-tolerance features.

b) Did you find any of these dependencies to be risk significant?

No detailed analysis of the effects of the dependencies was carried out.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

We regard the methods adequate for the sources of dependencies that were considered.

For systems having additional sources of dependencies, new methods would have to be developed.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

In our view it is still unclear whether methods which explicitly model the dynamic interaction of the plant system with the plant's physical processes (dynamic PSA) have substantial benefits.

There are indications that at least for some aspects (e.g. man-machine interaction) this might be the case.

An extensive study to apply dynamic PSA methods in a full-scale PSA is needed to demonstrate their ability to improve modelling.

Currently, dynamic PSA modelling methods for software-based digital I&C also still need to be developed.

b) Have any dynamic methods been used in your country for modelling digital systems?

In research projects at different German research institutions dynamic methods have been applied, e.g. for the reliability analysis of computer networks.

A current project at GRS aims at systematically assessing possible advantages and difficulties (e.g. estimation of model parameters) applying dynamic models to software based digital I&C systems. From this research new concept of modelling digital I&C systems might be expected.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

   According to the German PSA guideline, plant-specific data shall be used when possible. Plant maintenance documentation is the main data source. When plant-specific operating experience is not sufficient (e.g. for CCF), additional data sources are used:

   - German licensee event reports,
   - international events (very limited).

   For software based digital I&C equipment generic data was used. It was partly validated with a limited amount of operating experience.

   In human factor analysis (THERP/ASEP) and very few special cases other sources of reliability estimates are used.

   For software based digital I&C, to our knowledge no specific method to collect operational data of software failures has been established in Germany. GRS recently started to develop such a method.

   b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

   See response to question 7a.

   c) What method did you use for processing these raw data into failure parameters, such as failure rates?

   Bayesian statistical methods are applied to estimate reliability parameters from operating experience. These methods take the statistical estimation uncertainty into account.

   d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

   Software related failures have not been modelled.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) How do you account for the impact of software failures on system reliability?

   It is GRS opinion that failures of digital I&C related to software (software failures, synergetic failures) shall be included in PSA. We currently have no method in place to accomplish this.

Until now, software related failures have not been considered in German PSA. Currently, there are no software based RTS and ESFAS systems present in German NPP.

a) Since the appropriate level of detail is still to be determined, it is not clear whether software failures will be modelled separately or in combination with hardware failures.

These topics are under investigation in a current GRS research project.

b) How realistic is your approach for accounting for this impact?

See answer to question 8 a.

c) Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?

See answer to question 8 a.

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

See answer to question 8 a.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

b) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

The statistical uncertainties related to limited operating experience of technical components are treated by Bayesian statistical methods.

The question of a systematic consideration of the additional sources of uncertainty, i.e.

- modelling assumptions and
- completeness,

is still a topic of basic research.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the

system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) *What methods are used in your country for modelling human errors associated with digital systems?*

The introduction of new computer-based interfaces results in a significant change of NNP operation.

According to our opinion, this topic has not always been given enough emphasis in the past.

The effects of the new interfaces should be considered in human factor analyses.

Different approaches to accomplish this are under development at GRS.

b) *Are there any available data associated with the probability of this kind of error?*

Presently, only limited human reliability data regarding the new computer-based interfaces is available.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

There are different research projects sponsored by the German Ministry of Economy (BMWi), e.g.:

- GRS research activities,
- VeNuS project.

b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

According to GRS opinion the adequate modelling of software related failures and the estimation of reliability parameters of software based I&C equipment using plant operating experience are the most urgent research topics and additional research efforts are needed to advance them.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) *Has risk information related to digital systems already been used for decision making in your country?*

German regulations regarding safety and safety-related functions are based on deterministic criteria. This is also true for the new rules explicitly covering software based digital I&C which are currently under development.

To our knowledge, risk information regarding software based I&C systems has not been used for decision making.

b) What decision making do you foresee that would use risk information related to digital systems?

See answer to question 12 a.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

Considering the present state of the development of PSA methods for software based I&C, in our view a pre-categorisation would currently not be useful.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

In our opinion the topics given in appendix 1 (i.e., the fifteen topics provided before the technical meeting) cover the main problems in modelling software based digital I&C.

It should be emphasised, however, that the reliability of software based I&C systems are influenced e.g. by:

- hardware and software modifications,
- software corrections and upgrades and
- other maintenance activities.

We conjecture that these activities have substantial influence on the system reliability. Failures related to these causes should be included by using appropriate operating experience.

15. From the topics above, which do you consider most important to address, and why?

According to GRS opinion the first priority is to develop and apply methods to appropriately account for software related failures (software failures/synergetic failures).

The development of methods to analyse operating experience data and to estimate reliability parameters from the data has to go hand in hand with the development of the modelling approaches themselves.

Models whose parameters cannot (for theoretical or practical reasons) be derived from operating experience are not useful.

JNES RESPONSES

31 October 2008
Keisuke Kondo, JNES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      JNES considers that it is meaningful to model the digital instrumentation and control (I&C) system with probabilistic way to understand the level of reliability of it and check the adequacy of design.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      It has been developed for nuclear power plants.

   c) *For what purpose have these models been developed?*

      Models have been developed to evaluate the unavailability of digital I&C system due to component failures including software common cause failures (CCF).

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      There is a guideline for reviewing digital I&C system design adequacy but any specific standards or guidance for PSA modelling of digital I&C system, except for the generic Level 1 PSA modelling standards, does not exist.

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

JNES's PSA models include both hardware and software failure for ABWR (advanced BWR). The digital I&C systems are installed in Japanese ABWR. However, Industry's PSA models for PWR include only hardware failure.

f) Have the models been integrated into a PSA model of an entire NPP?

The models have been integrated into a PSA model of an entire NPP.

g) Can you make available at the technical meeting any publications documenting your work in this area?

There are several reports written in Japanese for ABWR and it may take some time to translate into English. There is no open publication for PWR.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

Fault Tree method has been used to evaluate the unavailability of digital I&C system and Event Tree method has been used to evaluate the overall plant risk (i.e. core damage frequency: CDF). These methods are the same as used in the ordinary PSA.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

There's no difference from the model for PSA of the rest of the plant.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

To evaluate the CDF, JNES models protection system only. JNES does not model continuous control system.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

To the level expressing fundamental functions such as Parallel I/O, Multiplexer, Digital Trip Modules, etc for ABWR.

b) Why was this level of detail used?

The level for minimum functional unit for counting common cause failure is necessary to model the digital I&C system.

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

JNES does not have detailed design information of the target digital safety protection system. Therefore, the current level is a limit in modelling the system.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?

JNES uses failure mode information from the IEEE std-500, 1984 and other limited international technical meetings for digital I&C system.

b) Do you consider operating experience in identifying failure modes?

JNES thinks it necessary to consider operating experience, however, only a few failure experiences in Japan are available, so that not useful enough to estimate the failure mode of them using operating experience at this present.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

Independent failure of any hardware basic events in one train of reactor protection system (RPS) should fail the function of the entire train.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

Dependent failure of the same basic events of hardware in different channels should fail the whole channels of the system. For software, JNES assumes if it fails in any part of single train of RPS or ESFAS, the whole associated system of will lose its function.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

   A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

   B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

   C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

   D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

   E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

   F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

      a) What types of dependencies do you include in your digital system reliability model?

      JNES includes common cause failures between hardware equipments of same type among different channels and software among different channels.

      b) Did you find any of these dependencies to be risk significant?

      Yes, software common cause failure (CCF) is risk dominant.

      c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

      JNES believes that accumulation of more operating experience of digital I&C system for verification and validation (V&V) of modelling would be necessary to make it more adequate.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

   a) Do you consider it necessary to accurately model these interactions and their timing?

   JNES can't judge the necessity of it at the moment.

   b) Have any dynamic methods been used in your country for modelling digital systems?

   No, as far as respondent knows on Japanese nuclear industry.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

   JNES used open literature of NRC and IAEA and did not directly use raw failure data.

   b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

   JNES cited CCF data used in the NRC's final safety evaluation report for ABWR and general CCF data, like WASH-1400, just the same as generic internal PSA.

   c) What method did you use for processing these raw data into failure parameters, such as failure rates?

   As mentioned above (a), JNES did not directly process raw failure data.

   d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

   For the hardware part of digital I&C, JNES did not use any method for assessing probabilistic parameters, but for the software part of it, JNES took the failure rate of software bugs per command line into account.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) How do you account for the impact of software failures on system reliability?

   JNES makes assumption that if any bug in software is found, associated digital RPS or ESFAS will lose its function at all. A part of bugs in software is assumed to be removed during pre-install test. The effect of pre-install test is also modelled in JNES's PSA model.

b) How realistic is your approach for accounting for this impact?

JNES considers that software failure will cause loss of all redundant units in the RPS or ESFAS in high likelihood, so the assumption that if any bug in software is found, the associated system lose its function at all is seemed highly conservative.

c) Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?

There is no reliability evaluations in digital I&C system that JNES does not feel the need to explicitly model software failures at this moment.

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

JNES don't address interactions between software and hardware. JNES handles them separately.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

JNES addresses the uncertainty of hardware and software failure rate with error factor. The probabilistic density function (pdf) of failure (hard and software) is assumed to be as log-normal distribution.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

JNES considers human error for recovery of hardware failure of the digital I&C protection system components based on the time-reliability correlation curves of the NUREG/CR-1278 as well as manual scram after failure of automatic scram just as conventional internal PSA.

b) Are there any available data associated with the probability of this kind of error?

There is no available data in Japan at this moment.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?

No specific activities, except for collecting plant components' failure data, are ongoing.

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

Refining the existing software failure rate evaluation model as well as CCF and human error probability (HEP) will be required, but time frame is not fixed.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

Risk information related digital system was used in evaluation of effectiveness of the Accident Management (AM) measures of ABWR and the latest PWR.

b) What decision making do you foresee that would use risk information related to digital systems?

Decision making with risk information may be foreseeable in the field of evaluating the adequacy of design, the test and maintenance interval of digital I&C and judging compliance to the safety goal.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

It may be feasible and practical; however, establishing basic PSA model to embed in the current internal PSA model is the first priority. It's not practical to consider that aspect in current situation.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

N.A.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

No idea comes to mind at the present situation.

15. From the topics above, which do you consider most important to address, and why?

Update the digital I&C system failure data as well as HEP data is important. Even though JNES could build a new PSA model for digital safety protection system, it is not useful without the operating experiences.

KAERI RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Yes

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Yes. DPPS/DESFAS (KHNP model developed by W/H, KAERI model), ESF-CCS (KAERI model), PCS (KOPEC model for Shin Kori 1&2, KAERI model, very simple)

   c) *For what purpose have these models been developed?*

      All KAERI model: research purpose (determining important factor and plant risk effect analysis)

      DPPS/DESFAS KHNP model: supplementary for regulatory body

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      KHNP model: NEI guide 00.02 for peer review

      KAERI model: no standard applied (for research purpose)

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      KHNP model: only hardware

      KAERI model: hardware and software (S/W failure considered as a part of processor failure)

f) Have the models been integrated into a PSA model of an entire NPP?

KHNP model: No → Yes

KAERI model: Yes

g) Can you make available at the technical meeting any publications documenting your work in this area?

Yes (Paper reprints, distributable files such as RPS risk analysis paper, ESF-CCS design issue paper)

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

ET/FT approach + supplementary analysis

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

The way of software failure probability calculation is different with the failure probability calculation of hardware. But, it is integrated to the ET/FT models. It is reflected in processors' failure events.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Continuous control systems are not modelled in PSA except several safety-critical components control which is modelled very simply (eg. failure of controllers + I/O failures).

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

Dangerous failures of modules are basic events.

b) Why was this level of detail used?

Data availability (handbook, vendor data) and dependency consideration

c) *Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?*

If we apply black box module data directly, we will have too conservative results since some components in the module do not play the role in safety-critical function.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

Designers and developers performed a very detailed FMEA even to the element (such as CPU, RAM) level in the modules of a digitalised system. For the SW, separate FMEA was performed. But the results of these detailed level FMEA were not proper to use directly in PSA since failure modes in digital system is not straight forward. So conservatively, all failures of critical components are assumed to be dangerous in KAERI's model and recoverable failures with installed mechanism are modelled in fault trees explicitly.

b) *Do you consider operating experience in identifying failure modes?*

We do not have enough failure data in nuclear safety critical system, but the experience of other industries must be referable. We don't reflect them yet.

c) *How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?*

Same answer with (a).

d) *How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?*

Combinations of failures are considered in FT models explicitly.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

   A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

   B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

   C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

   D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

   E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

   F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

      a) What types of dependencies do you include in your digital system reliability model?

      Monitoring functions (among processor modules, and between watchdog timers and processor modules) are considered. Hardware CCF is considered. SW is treated as a part of Hardware CCF if identical software is installed in more than one processor modules. Dependencies which are arisen by sharing data bus and backplane are not considered since their failures are fail-safe. Network communication failures in ESF-CCS are considered as an independent failure of hardware network modules or their CCF. Protocol errors seem to be treated in the similar way with software errors. And CCFs are modelled by using simplified modelling method.

      On the other hand, dependency between digitalised information system (such as alarm system) and human operator is considered based on condition-based HRA. Dependencies among operator's recovery actions are considered also.

      b) Did you find any of these dependencies to be risk significant?

      Of course. For example, the CCF of output modules is dominant. and the software failure can be treated as a part of the CCF of processor modules. Human error probabilities are important also.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

For the model, yes. But detailed data for quantification are not enough.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

Human operators are affected by plant's physical processes. Therefore, the interactions must be considered. We do.

But, in the case of safety-critical systems, the function of safety-critical digital systems itself does not change. The timing of interactions may affect the function of safety-critical digital systems. But, the considering timing factors does not seem to be cost-effective for safety-critical systems at this moment. It is notable that safety-critical systems such as RPS are on-demand actuation systems.

For control systems, on the other hand, the plant dynamics and timing factors should be considered. From the viewpoint of initiating event, control systems are important also.

b) Have any dynamic methods been used in your country for modelling digital systems?

No, not yet.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

Vendor data (usually calculated based on MIL-HDBK-217F in consideration of in-module fault tolerance mechanisms). KAERI is trying to get the experience data, but for the safety systems, it is not successful till now.

b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

Utility applied beta factor method. KAERI usually apply alpha factor method for CCF but for digital I&C we do not have enough raw data for estimating parameters. We use generic values for alpha factors.

c) What method did you use for processing these raw data into failure parameters, such as failure rates?

N/A

d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

Utility does not model software failure in PRA. For KAERI, at present, assumed data is applied for the purpose of a sensitivity study. The software test results and BBN models for assessing the V/V activities are under consideration.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) How do you account for the impact of software failures on system reliability?

As a part of programmable module failures

b) How realistic is your approach for accounting for this impact?

Acceptable for practical use

c) Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?

No. Software should be considered always

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

No.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

Primitive sensitivity study to see the effect of model or method change and to see the range of risk variance

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

    a) *What methods are used in your country for modelling human errors associated with digital systems?*

    HRA methods such as THERP and ASEP. Currently, the HRA method for digitalised MCR is under development.

    Condition-based HRA was developed to accommodate the human operator's dependency on the signal availability which is closely related to the I&C system

    Experiments for comparing a fully digitalised MCR with the case of conventional MCR using mockup and plant operators→ data collection phase

    b) *Are there any available data associated with the probability of this kind of error?*

    Data is under collection now.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

    a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

    R&D activities such as quantification of S/W failure probability, fault coverage of digital systems with fault tolerant mechanisms, the validity of automated periodic test, and the development of a HRA method for digitalised MCR are performed under the mid-and-long-term nuclear R&D program in KAERI and they are still under research. These topics are developed based on the result of risk effect analysis. We are going to establish the standard framework for Digital I&C system PSA within 4 years.

    And we would like to propose an international R&D cooperation by comparing the results with each other which are generated based on various methods developed by participants. Target system must be the same (if possible, one for protection function, and the other for control function).

    b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

    Identification of failure modes and collection of field experienced failure data is additionally required. But we cannot fix the time frame since the data availability is limited.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

    a) Has risk information related to digital systems already been used for decision making in your country?

    Yes. (already applied to modify the design of safety-critical digital system)

    b) What decision making do you foresee that would use risk information related to digital systems?

    Design change and regulation (acceptance of digital systems in NPPs and upgrades)

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

    a) Do you consider that this kind of categorisation is feasible and practical?

    Yes.

    b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

    The categorisation should be performed based on the importance of system function.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

    Two presentations from KAERI will be delivered on this topic.

15. From the topics above, which do you consider most important to address, and why?

    Factors are closely correlated, but human errors, software failures, and fault coverage are dominating the risk from digital I&C systems.

HRP RESPONSES

Response from Bjørn Axel Gran on behalf of Halden Reactor Project (HRP)
No answers should be interpreted as a Norwegian opinion

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Response: Yes, and we have performed research on it within HRP and gained experiences through consultant work within Air Traffic Management (ATM).

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Response: research within HRP have been done e.g. on the use of BBN, approaches to address dependent failures, and on how to assess logic diagrams. Applied/gained experience within ATM on an approach to assess fulfillment of safety goals on the basis of failure modes through a FTA.

   c) *For what purpose have these models been developed?*

      Response: research for the HRP and consultant work within ATM

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      Response: ICE61508, IEC60880, international publications

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      Response: research within HRP has focused on sw. Within ATM the applied approach includes both hw and sw.

f) Have the models been integrated into a PSA model of an entire NPP?

Response: No

g) Can you make available at the technical meeting any publications documenting your work in this area?

Response: A number of reports from HWR are available for the members of the Halden Project. Among these is a lessons learned report covering the research 94-2005. Experiences from ATM were published at ESREL 2005 and in this meeting.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

Response: see presentation. Within ATM: FMEA for hw. and sw., FTA for linking failure modes to safety objectives. Assessment of sw failure modes through an approach for sw assurance levels and the identification of independent barriers.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

Response: Not Applicable

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

Response: Not Applicable

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

Response: In general Not Applicable. In ATM depending on vulnerabilities/failure modes. If diversity exists: high level, if required p=0 on a low level.

b) Why was this level of detail used?

Response: see above

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

Response: see above

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

Response: in ATM FMEA on the sequence level through expert judgment and assessment of the code.

b) *Do you consider operating experience in identifying failure modes?*

Response: within ATM, yes on the identification of mitigations/possible detection mechanisms.

c) *How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?*

Response: through a FTA, linking failure modes to safety goals.

d) *How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?*

Response: through a FTA, linking failure modes to safety goals.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

Response: within ATM performed a CCF according to BS5760, addressing more life cycle phases

b) Did you find any of these dependencies to be risk significant?

Response: within ATM yes.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Response: within ATM yes

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

Response: no consensus. In ATM addressed ad-hoc, e.g. by addressing sw. failure modes in sequence

b) Have any dynamic methods been used in your country for modelling digital systems?

Response: no specific research performed.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

   a) *What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?*

      Response: within HRP we lack availability to data. Within ATM: vendor data

   b) *What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?*

      Response: within ATM: Beta factors by expert judgment

   c) *What method did you use for processing these raw data into failure parameters, such as failure rates?*

      Response: within ATM: conservative approach

   d) *What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?*

      Response: within ATM: values associated with sw assurance levels

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) *How do you account for the impact of software failures on system reliability?*

      Response: see Q7

   b) *How realistic is your approach for accounting for this impact?*

   c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

      Response: Within ATM: yes, when having enough independent barriers covering all the possible sw. failure modes for that part/module/item.

   d) *Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?*

      Response: so far not addressed

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

   a) *How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?*

      Response: HRP: applied BBN, and done research on the choice of prior distributions. Within ATM: uncertainty in data addressed through sensitivity assessments. ad 2) and 3): applied simplifications and discovered the effects of errors in the models

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

   a) *What methods are used in your country for modelling human errors associated with digital systems?*

      Response: within HRP there is a large research effort on Human Reliability and Human Factors related to e.g. data collection from experiments of HAMMLAB. Some scenarios address error masking without saying the cause of the error which could be digital.

   b) *Are there any available data associated with the probability of this kind of error?*

      Response: the HRP could be asked to look into it, but the priorities are set by the members of the Halden Project.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

   a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

      Response: Research on Software Systems Dependability as one chapter within the Halden Reactor Project

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

Response: NA.

b) What decision making do you foresee that would use risk information related to digital systems?

Response: NA.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

Response: NA.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

Response: Within HRP we have not focused to much on development of new methods, more on addressing strengths/weaknesses/aspects of different methods. We want to move towards doing experimental research, using e.g. a simulator for the plant.

COMPSIS will not provide any data in order to be applied as probabilistic data, but should be an important knowledge database with respect to categories of experienced failures, lessons learned reports, and exchange of knowledge about the failures.

15. From the topics above, which do you consider most important to address, and why?

INER RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      ANS: Through the international cooperation of data collection, it is possible to obtain meaningful failure rates of digital components.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      ANS: Digital systems have been modelled in the PSA of Lungmen nuclear power plant which is now under construction. Other example is the aircraft reliability analysis of air force. For three operating nuclear power plants, part of the control systems was digitalised. The qualitative analysis showed that the upgraded control system may be not risk significant. So there is no detailed modelling in the associate PSA models.

   c) *For what purpose have these models been developed?*

      ANS: The model for Lungmen nuclear power plant was developed to estimate the CDF and LERF required by the Atomic Energy Council of Taiwan and also for the risk-informed applications in the future. The model developed by the air force is used to estimate the reliability of the aircraft.

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      ANS: There is no specific guidance or standard to review the model of digital systems for nuclear power plants. The standard used by US air force was also adopted in Taiwan to review the reliability model for the military aircraft.

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      ANS: No specific software failure was modelled in the PSA of Lungmen nuclear power plant or in the reliability model of military aircraft. Both hardware failure and software failure were lumped as a failure rate of digital I&C module which contained hardware device and software package.

f) Have the models been integrated into a PSA model of an entire NPP?

ANS: Yes! The model has been integrated into Level 1 Lungmen PSA.

g) Can you make available at the technical meeting any publications documenting your work in this area?

ANS: The Lungmen PSA is now a proprietary material of Taipower Company and may be released after the commercial power operation.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

ANS: The event tree/fault tree approach was used in Lungmen PSA.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

ANS: The Lungmen nuclear power plant is the first plant using digital control system. The model of digital system in the PSA was focused on the signal transmission to actuate a single component or to lineup a system. Series of fault trees were developed as external transfer when demanded by component or system.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

ANS: Only demand failures were modelled in Lungmen PSA. No continuous control was modelled. Regarding the reactor protection system, a basic event was used as the failure of control rod insertion.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

ANS: In Lungmen PSA, the digital control system was divided into several modules by its major function during signal transmission. The boundary of each module was selected to minimise the dependency between modules.

b) Why was this level of detail used?

ANS: For the most cases in nuclear power plant, there may be more than one signal source to actuate a component or to lineup a system. Different signal sources may use more than one common module during signal transmission such as the analog-digital converter or network. A proper selection of module boundary can minimise the dependency analysis when quantifying the event tree sequence.

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

ANS: The level of detail when modelling digital systems is a trade-off between the size of digital system fault trees and the complexity of the accident sequence dependency analysis. The boundary of module should be extended to the extreme by considering the function dependency between modules. This would minimise the size of the digital system fault trees and also eliminate the accident sequence dependency analysis.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?

ANS: No specific method was used to identify the failure modes of digital systems. A conservative assumption was made to simplify the model and to focus the analysis on identifying the weak point of all possible plant responses after reactor trip. In the digital system fault trees, the failure of any module will interrupt the signal transmission that pass the failed module and the failure cannot recovered within the entire mission time.

b) Do you consider operating experience in identifying failure modes?

ANS: It is not necessary to consider the operating experience when such conservative assumption was used in the fault tree analysis.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

ANS: N/A

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

ANS: N/A

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

ANS: All dependency mentioned above except the dynamic interactions were modelled in the digital system fault trees.

b) Did you find any of these dependencies to be risk significant?

ANS: When reviewing the cutest of the plant core damage sequence, it was found that the common cause failure of network to be risk significant. It won't be surprise for a fully digitalised plant since most of the automatic signals and manual control signals from main control room need network to communicate. When all networks failed, the main control room will loss all indication of plant status and only very few controls that using hardwire are available in the main control room. The operating crew has to evacuate to remote shutdown panel according to the operating procedure when network crashed.

c) *Do you consider that the methods you used for identifying and modelling dependencies are adequate?*

ANS: It is adequate to measure the importance of each module and also to identify the weak point of all possible plant responses after reactor trip.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) *Do you consider it necessary to accurately model these interactions and their timing?*

ANS: It is necessary to model those interactions and timing only any of them was considered to be important to the risk.

b) *Have any dynamic methods been used in your country for modelling digital systems?*

ANS: No dynamic method was used when modelling digital systems.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) *What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?*

ANS: Data available from other industries are used as raw data to estimate the failure rates.

b) *What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?*

ANS: A conservative common cause beta factor was assumed for similar modules.

c) *What method did you use for processing these raw data into failure parameters, such as failure rates?*

ANS: The raw failure data were calculated by considering the mean time between failures, the average self test interval and the conservative reliability of maintenance.

d) *What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?*

ANS: Equations from reliability handbook were used to calculate the failure rates.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

   a) How do you account for the impact of software failures on system reliability?

   ANS: Software failures are treated as common cause failure of related modules.

   b) How realistic is your approach for accounting for this impact?

   ANS: The assumed common cause failure beta factor may not reflect the actual contribution of software failure to the CDF or LERF. The common cause failures that were identified to be important by the importance analysis need further sensitivity studies to account for the impact to CDF or LERF.

   c) Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?

   ANS: N/A

   d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

   ANS: No interactions between software and hardware were addressed in Lungmen PSA.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

   a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

   ANS: Only parameter uncertainties were addressed in Lungmen PSA. A conservative error factor was assigned to all basic events of digital systems.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of

occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) *What methods are used in your country for modelling human errors associated with digital systems?*

ANS: In Lungmen nuclear power plant, a special team was organized to find out the potential human errors caused by digital control system. A questionnaire designed by the special team was sent to all operators and the answers from all operators were summarised. Then individual interview with all operators was performed. And finally, a serious of exercise on the simulator was performed to observe the response of operating crew to different plant status. All data were collected and analysed by specialists from regulatory body, plant manager, vendor and research institute.

b) *Are there any available data associated with the probability of this kind of error?*

ANS: No data associate with HEP is available now.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

ANS: Most of the ongoing activities are focused on the qualitative safety analysis of Lungmen nuclear power plant to meet the regulatory requirements.

b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

ANS: The work for data collection should be initiated as soon as possible.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) *Has risk information related to digital systems already been used for decision making in your country?*

ANS: There is no such application in Taiwan's nuclear power plants.

b) *What decision making do you foresee that would use risk information related to digital systems?*

ANS: The results of importance analysis.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) *Do you consider that this kind of categorisation is feasible and practical?*

ANS: Yes, it has to be done to focus the resources on the most important issues of specific digital system design which will integrate to plant operation.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

ANS: It can be categorised by the use of the results and insights of the results.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

ANS: N/A

15. From the topics above, which do you consider most important to address, and why?

ANS: The software failure and the other new failure modes induced by digital system should be the most important issues to address. Those failure modes are new for PSA people and need to be addressed in PSA for those failures could negate the defense-in-depth features.

BNL RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Yes, we consider that it is meaningful to model failures of digital components in a probabilistic way because these components fail in a random way.

      Regarding software failures, we did some preliminary work on developing a basis for modelling them probabilistically based on occurrence of triggering events.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Yes, for example, some probabilistic models of digital systems have been developed in the US for new reactor design certifications and certification of digital designs, such as the Tricon design.

      BNL developed a probabilistic model of a digital feedwater control system (DFWCS).

      Many of our responses to the questions below are based on insights obtained while studying this system and building the model.

   c) *For what purpose have these models been developed?*

      Regulatory certification of designs of new nuclear power plants, such as Westinghouse AP1000.

      Research on the capabilities and limitations of "traditional" and dynamic probabilistic methods.

      Supporting information for digital systems developed by the US industry, such as Triconex.

d) What are the standards or guidance that you have used for developing or reviewing these models?

There are no NRC-endorsed standards/methods for modelling digital systems. Hence, no standards or guidance in the US have been used for developing or reviewing models of digital systems.

ANSI/ISA 84.1 and IEC 61508 are standards related to digital systems, and the former was used by Triconex in modelling Tricon. However, they have not been endorsed by NRC.

Recently, NRC staff developed a draft Interim Staff Guide (ISG) on reviewing PRAs of new reactor I&C systems.

BNL recently developed a set of desirable characteristics for a probabilistic model of a digital system. It was an input to the NRC staff's ISG.

e) What is the scope of the models, e.g., do they include hardware and software failures?

The scope varies substantially between the different models.

All models include hardware failures of the components of a digital system.

Several models do not include software failures of the components of a digital system.

Some models include a "top-level" treatment of software failures.

The BNL model of the DFWCS includes hardware failures and high-level software failures.

f) Have the models been integrated into a PSA model of an entire NPP?

The models developed for the regulatory certification of designs of new nuclear power plants are the main example of integration into a PSA model of an entire NPP.

g) Can you make available at the technical meeting any publications documenting your work in this area?

The most recent report from BNL, "Traditional Probabilistic Risk Assessment Methods for Digital Systems," NUREG/CR-6962, is available in the section of the NEA's web site for the WGRisk digital I&C reliability activity. The advanced reactor PRAs are available on the NRC website. The Tricon study is proprietary.

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) What modelling method or methods have been used in your country for modelling digital systems?

The ET/FT method has been primarily used. As part of NRC-sponsored work, Markov methods and the dynamic flowgraph method (DFM) have been used in proof-of-concept studies.

b) Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?

All overall PSAs of NPPs in the US use the ET/FT method.

The models of digital systems prepared for the regulatory certification of designs of new nuclear power plants use the ET/FT method, so the integration is straightforward.

The BNL model of DFWCS is a Markov model, so its integration with the entire PRA is not straightforward. We consider that it is possible to implement this integration; however, no attempt has been made to do so.

c) If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?

So far the analysts in the US appear to apply the same approach and methods for modelling continuous control systems and protection systems.

However, the potential differences in modelling these two types of digital systems have not been studied in detail in the US.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) What level of detail was modelled in your country?

The level of detail varies substantially between the different models.

BNL used the level of detail of the microprocessors for hardware failures. This is the deepest level of the models that we are aware of.

High-level software failures are also included as placeholders, without detailed analysis and quantification because this topic was beyond the scope of the study.

b) Why was this level of detail used?

The level of detail used by BNL was considered necessary to capture the features of the digital system that contribute to the unreliability of the system. It is also the level at which some failure data are available publicly.

c) *Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?*

We consider that a reliability model of a digital system should be developed to a level of detail that captures the design features affecting the system's reliability, provides the output needed for risk evaluations, and for which probabilistic data are available.

The BNL model of DFWCS captures important design features/components of the system; in particular, the normal behaviour of the software is included by using a simulation tool.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

The models of digital systems developed by separate organisations in the US appear to use different sources of failure modes of hardware components.

There is a potential lack of completeness of identification of failure modes of hardware components.

Failure modes of software components are usually not identified.

Two types of software failure modes are considered in the BNL model of the DFWCS: software continues running but generates erroneous results, and software stops running. They are generic failure modes that are applicable to any software. It is recognised that in general identification software failure modes is an area requiring additional research.

b) *Do you consider operating experience in identifying failure modes?*

BNL carried out a review of operating experience related to the example digital system studied. However, the review did not reveal additional failure modes.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

BNL developed a method and associated computerized tool to determine the effect of a failure mode of a component on the digital system. The method uses a simulation model to assess the response of the system to postulated combinations of failure modes of components, thus identifying those combinations that fail the system.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

BNL used the method and associated computerized tool mentioned above.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

BNL's study of the DFWCS included all these dependencies, except for the dynamic interactions.

b) Did you find any of these dependencies to be risk significant?

Dependencies are more important to those systems that have more redundancy, because the dependencies tend to defeat the benefits of redundancy. The DFWCS provides some redundancy by having main and backup CPUs. However, they share several controllers which have many single failures of the system that are dominant contributors to system failure probability. Hence, this redundancy is adversely affected by such sharing.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Yes, we consider that all the relevant dependencies of the DFWCS were identified and modelled as appropriate, except for dynamic interactions.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

BNL's study of a DFWCS did not model these interactions, but it analysed all the other dependencies mentioned in point 5, above. Since this study did not address these interactions, no general conclusion was reached about the need to model them.

Regarding the interactions between the DFWCS and the plant's physical processes, we think it might be covered by conservatively including in-the-range drifting signals as failure modes of the system.

b) Have any dynamic methods been used in your country for modelling digital systems?

Yes, the USNRC sponsored the application of two dynamic methods to the DFWCS.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

Raw failure data from the PRISM database were used as input data for the Hierarchical Bayesian Method (HBM) (see answer to question 7c, below).

The Reliability Analysis Center also has a publication of failure modes and mechanisms which was used as an important source of failure mode distributions, i.e., breaking down of failure rates into their constituent failure modes.

Failure rate estimates of some components of the DFWCS could not be assessed using the HBM analysis, and were obtained from other sources of reliability data.

b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

Due to the lack of digital-specific CCF parameters and because developing a database for CCF parameters of digital components was beyond the scope of BNL's study of a DFWCS, it was decided to use the generic beta factor suggested in a report by the Electric Power Research Institute (EPRI) related to advanced reactors. This report does not specifically address digital components and suggests using a generic CCF parameter.

c) What method did you use for processing these raw data into failure parameters, such as failure rates?

The Hierarchical Bayesian Method (HBM) was used by categorising and grouping raw data.

d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

Due to the lack of consensus on software reliability methods, modelling software failures was beyond the scope of BNL's study of a DFWCS.

However, some top-level software failures were considered. An arbitrarily selected small failure rate was used for these failures in the model quantification, such that the contribution of software failure did not mask the contribution from other modelled failures.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) How do you account for the impact of software failures on system reliability?

Due to the lack of consensus on software reliability methods, modelling software failures was beyond the scope of BNL's study of a DFWCS. However, some top-level software failures were considered.

In addition, software faults may manifest themselves through the use of the simulation tool. Some of them were identified in BNL's study. Others may be identified by carrying out a more detailed study of the system using the tool.

b) How realistic is your approach for accounting for this impact?

BNL's approach on modelling software failures used in the study of a DFWCS is not considered realistic, because of the following issues: 1) the level of detail at which software failures should be modelled, 2) completeness of software failure modes, and 3) lack of failure rates of software failures. BNL is currently starting a project to address quantitative software reliability.

c) Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?

For the example system studied by BNL, i.e., a DFWCS, it was considered necessary to explicitly model software failures because they are a potentially significant contributor to system reliability.

d) Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?

BNL developed an approach, i.e., use of a simulation tool of the system, for accounting for the effect of the normal behaviour of the software of the components of the DFWCS on the hardware components. The combinations of failure modes of the hardware components that fail the system are identified using this approach. The probabilistic model was built using these combinations.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

BNL's study of a DFWCS recognised the main sources of parameter, model, and completeness uncertainty.

Parameter uncertainty was propagated through the probabilistic model, taking into account the state-of-knowledge correlation, using a limited number of samples.

Modelling uncertainty was addressed by documenting the main assumptions made in developing the model. Due to limitations in the state-of-the-art for evaluating the reliability of digital systems and lack of detailed design information, no sensitivity calculations were performed to evaluate the effects of alternative assumptions.

Regarding completeness uncertainty, it was recognised that the failure modes of both software and hardware may not be complete and additional research is needed.

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

Currently the same methods that are used for analog systems are being applied to digital systems.

b) Are there any available data associated with the probability of this kind of error?

There does not appear to be available data at this time.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?

BNL is currently starting a project to address quantitative software reliability methods.

As part of updating its 5-year digital I&C research plan, the NRC is considering research that may support addressing some of these challenges, such as including investigation of failure modes, categorisation of digital systems, and study of operating experience.

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

BNL identified the following areas for potential additional research, and believes that they should be addressed in the near-term:

1. Approaches for identifying failure modes of the components of digital systems, and determining the effects of their combinations on the system.

2. Methods and parameter data for modelling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures.

3. Better data for hardware failures of digital components.

4. Better data for CCFs of digital components.

5. Software reliability methods for quantifying the likelihood of failures of both application and support software.

6. Methods for modelling software CCF across system boundaries (e.g., due to common support software).

7. Methods for addressing modelling uncertainties in modelling digital systems.

8. Methods for human-reliability analysis associated with digital systems.

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

Risk information related to digital systems has not been explicitly used yet for decision making in the US. The industry has developed a simplified approach for making risk-informed decisions regarding digital systems. However, the approach has not been accepted by the NRC.

b) What decision making do you foresee that would use risk information related to digital systems?

The nuclear industry in the US is currently considering replacing safety and non-safety analog systems with digital systems. There is a possibility that some of the submittals from licensees to the NRC requesting approval of these changes will use risk information. Risk information may also be used in other licensing applications, e.g., in submittals related to changes to Technical Specifications.

The designs of new reactors incorporate digital systems, so decisions related to the licensing review of these designs are expected to use risk information.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

a) Do you consider that this kind of categorisation is feasible and practical?

Development of an inventory and categorisation of digital systems is one of the subjects being considered in NRC's new 5-year research plan.

BNL has not previously worked on the subject of categorisation; therefore, we do not have a response to this question at this time.

b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

Not applicable.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

We consider that the areas requiring additional research mentioned in our response to question 11b are important to address.

15. From the topics above, which do you consider most important to address, and why?

All topics are relevant to evaluating the reliability of digital systems. The following topics are the most important to address because they are known to potentially have a significant impact on this reliability:

1. Software reliability methods for quantifying the likelihood of failures of both application and support software.

2. Better data for hardware failures of digital components, including CCFs.

3. Approaches for identifying failure modes of components of digital systems.

EPRI RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Response: Yes, it is meaningful to model failures of digital components in a probabilistic way recognizing that the software failures themselves are deterministic (that is, given the same input, software will produce the same output each time it is executed). What is probabilistic are the plant conditions that may be encountered that may also trigger any software errors that could exist that would result in the components being controlled by the digital system responding in a manner that is adverse to safety. As input to PRA, the probability of software failure is the probability of a software error combined with the probability of plant conditions that will result in the error manifesting itself in an adverse way.

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Response: Yes, by reactor vendors for new plants, current plants in support of digital upgrades Electric Power Research Institute (EPRI) in support of development of risk insights regarding the value of defense-in-depth and diversity in digital systems and the United States Department of Energy (US DOE) in the design an operation of digital systems in research reactors.

   c) *For what purpose have these models been developed?*

      Response: Generating risk insights associated with digital systems to influence the design, making decisions about functional diversity and how and when to use backups, determining the value of defense-in-depth and diversity, and review and comment on regulatory guidance. Specific examples of these applications include, ensuring that the controls for manual backups such as feed and bleed are diverse from the potential CCFs that can contribute to the loss of all feedwater, modifying the dependencies of selected components on remote processors to address communication failures, evaluating the benefits and risks of automated diverse actuation systems

(DAS), providing automatic backups (not DAS) for the most sensitive I&C failures such as loss of level control during mid-loop.

d) *What are the standards or guidance that you have used for developing or reviewing these models?*

Response: Hardware portions of the system are modelled using traditional techniques for the development of event tree and fault tree logic model, along the line of the PRA Procedures Guide, NUREG-0492, Nuclear Energy Institute's (NEI) PRA Peer Review Guideline (NEI 00-02), ASME Std RA-S-2002, Regulatory Guide 1.200. Also, numerous plant specific PRAs include detailed modelling of analog I&C systems that can be used as a basis for developing models of the digital I&C hardware. Other than vendor in-house guidance, only limited generic guidance is available on the modelling of the software portion of digital I&C systems. An NEI white paper on digital I&C modelling describes current methods (ML0723350195) most closely describes current methods. The effects of software and hardware failures are modelled together in an integrated manner. An NRC guideline on digital I&C modelling for new reactors most closely describes current review methods (DI&C-ISG-03 Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments-ML080570048). Several draft NUREGs on modelling digital I&C in PRA using current and advanced methods are available.

e) *What is the scope of the models, e.g., do they include hardware and software failures?*

Response: Detailed models by the reactor vendors and the DOE couple the software and hardware (e.g., the software is linked to its associated processor). Models developed for the purpose of developing regulatory insights focus on software CCF linked to the hardware that it controls (e,g., the software CCF is linked to the failure modes of the pumps and valves it controls).

f) *Have the models been integrated into a PSA model of an entire NPP?*

Response: Yes, by the reactor vendors and DOE.

g) *Can you make available at the technical meeting any publications documenting your work in this area?*

Response: The following US nuclear industry documents are available through the USNRC ADAMS website:

"Defense In-Depth and Diversity Assessments for Digital Upgrades, Applying Risk-Informed and Deterministic Methods." ML050540262

"Modelling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessments" ML0723350195

"Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions"

"U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience" I&C System Operating Experience Revision 0, June 13, 2008. ML081690011

"Common-Cause Failure Applicability"

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

   a) *What modelling method or methods have been used in your country for modelling digital systems?*

      Response: Standard event tree/fault tree techniques for safety systems, as they are simple on/off type actuation systems and not dynamic in nature.

   b) *Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP?*

      Response: No, given the models use standard fault tree/event tree methods and are not dynamic.

      If so, how do you integrate the model of the digital system with the PSA?

      Response: As basic events incorporated in the fault trees associated with the hardware in the system (e.g., the processor) or the components that they actuate (e.g., the pumps and valves and associated failure modes).

      Some very early work has just begun on the methods and process could be used to integrate current methods for PRA modelling (Event tree/fault tree approach) with the results of dynamic models such as Markov modelling.

   c) *If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?*

      Response: Continuous control system modelling is typically a generation related application and not found in many safety applications. Where it exists (e.g. feedwater control), it is typically a contributor to an initiating event (e.g., loss of feedwater) and can be estimated from operating data. Post reactor trip, such control systems are typically overridden by single element control or manual operation. Most modelling of digital systems has been performed for protection system purposes, which are typically not dynamic. Other dynamic systems such as turbine and generator digital systems can result in a failure of turbine stop and control valves to fully close but this function is not safety related and is backed up by a safety related system, the main steam isolation valves (MSIVs). Many failure modes of these non safety systems can be postulated but in general the results are un complicated turbine trips that, as in the case of feedwater, can be represented by operating data.

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) *What level of detail was modelled in your country?*

Response: The level of detail varies depending on the application and the sensitivity of the results to the digital system. Some models go to the level of rack-mounted module as this is the level at which data collection is expected to occur.

- For generating risk insights regarding regulation, modules or supercomponents were used to model the effect of software CCF on the components they actuate.

- For assessing the impact of the digital system on plant design, hardware was modelled and potential software effects added associated with the hardware.

b) *Why was this level of detail used?*

Response:

- In the assessment of regulatory requirements, the impact of the software on risk was shown to be small and insensitive to wide ranges of failure probabilities and software related failure modes. Limited detail was all that was necessary.

- In the assessment of the impact of the digital system on plant design, sufficient detail was assumed to be needed to assess the impact of common hardware and software effects across multiple redundant systems.

c) *Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?*

Response: I&C systems typically do not dominate the accident sequence results of PRA, whether analog or digital. This is a result of the defense-in-depth and diversity built into the I&C with respect to the overall integrated plant design. This existing defense-in-depth and diversity is defined by the mechanical and electrical systems that the I&C systems control. As long as the defense-in-depth and diversity in the mechanical and electrical systems is reflected in the I&C controlling these systems, then the I&C would not be expected to dominate the risk in the accident sequences in which these mechanical and electrical systems are credited.

The level of detail needed in modelling digital systems is dependent on the application. However, where the I&C reflects the defense-in-depth and diversity of the mechanical and electrical systems it controls, the level of modelling detail needed is likely limited, particularly if looking only at the overall PRA results. If the I&C system design does not support the defense-in-depth and diversity of the mechanical and electrical systems it controls (e.g., a common digital element is shared between diverse mechanical or electrical trains of equipment), then detailed digital I&C modelling may need to be considered to reflect the effects of common elements between redundant components.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the

component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) *Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?*

   Response: Identification of failure modes for digital system components begins with the extensive failure modes and effects analyses typically performed by the vendor in design of the digital system. Such failure modes may consider:

   - Hardware failures
   - Module I/O failures and removal
   - Module initialisation failures
   - Optical/electrical interface failures
   - Power supply failures
   - Communications failures (inside and between modules)
   - Data highway loss or corruption
   - Spurious actuation of I/O module
   - Channel spurious energisation
   - Hardware/software failures leading to loss of multiple processors.

   The PRA analyst must interface with the designer and I&C personnel in order to assure the completeness of the failure modes for the digital system under study and an understanding of the effects of these failure modes..

b) *Do you consider operating experience in identifying failure modes?*

   Response: In the US the vendors typically have access to operating experience with their systems in other industries or countries. Such operating experience is used when available through the vendor.

c) *How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?*

   Response: In designing the digital system, the vendors consider various failure modes of digital components and the causes of those failure modes. Where they could result in loss of a division or system function, the designs are modified to eliminate those failure modes from the design (e.g., software hang due to infinite loop) or assure the system responds in a safe manner (e.g., no output or delayed signal).

It should be recognised that the digital I&C, by itself, is not capable of accomplishing the front line safety functions modelled in the PRA. Rather, the I&C must be examined in terms of the functions performed by the mechanical and electrical systems it actuates or controls. Therefore, the failure modes of a digital system must be translated to the failure modes of the mechanical and electrical equipment to which it is connected. The failure modes of the mechanical and electrical equipment are well understood and are modelled in detail in the PRA. Where the effects of digital I&C failure modes on the mechanical and electrical equipment in the PRA are uncertain, bounding assumptions can be made in the modelling of the digital I&C in the PRA that potential digital I&C failures lead to the failure modes of the mechanical and electrical equipment. Given these bounding assumptions, if the digital I&C does not dominate the results of the PRA, then the modelling of specific I&C failure modes and a precise translation of their effects on the plant systems and equipment credited in performing the safety functions in the PRA is not critical.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

Response: As noted in the response to 'a' above, the vendor performs a detailed failure modes and effects analysis. Incorporating the effects of relevant failure modes from this analysis on the mechanical and electrical equipment included in the PRA accounts for the effects of a number of combinations of digital failures. In addition, for safety related I&C systems, the vendors perform a defense-in-depth and diversity (D3) evaluation. This D3 evaluation is a useful input to the PRA in that it breaks up the safety related systems, identifies those blocks containing common software an, therefore, potential candidates for common cause modelling.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

C. Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

D. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

E. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

F. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

Response: The level of detail needed in the modelling of digital I&C in PRA is dependent on the application and the sensitivity of overall plant risk to the digital I&C. Consideration is given to a number of dependencies with incorporation of only those that may be significant in the models.

For the initial modelling of the digital I&C in the PRA and its overall effect on risk, consideration has been given to CCF, shared hardware between redundant trains of equipment, and support system dependencies. For safety-related systems in particular, the rules of separation and independence between redundant channels and between SR and NSR are recognised (e.g., there is not one network like in your office that connects the whole plant).

For evaluation of regulatory proposals, detailed design of the digital I&C system was not always available. In this situation, there was a focus on the potential for introducing CCF and shared support systems.

b) Did you find any of these dependencies to be risk significant?

Response: Where the defense-in-depth and diversity in the I&C reflected that in the mechanical and electrical systems actuated or controlled by the I&C, these dependencies were not found to be risk significant. As hardware and software dependencies were introduced between redundant, diverse systems modelled in the PRA, the I&C could be made to increase in risk significance.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Response: Yes, for the purpose of integrating digital I&C in existing PRAs in assessing the overall risk significance of the I&C and for specific applications for the purpose of assessing the value of existing and additional defense-in-depth and diversity.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

Response: The need to consider the effects of interactions between plant systems and the plant's physical processes or the timing of these interactions is application specific. Some of the referenced literature is primarily concerned with process control systems, which are not a big

contributor to NPP PRAs. Dynamic interactions are not applicable to protection systems. Furthermore, the success criteria in PRA is sufficiently broad that such interactions do not play a significant role (e.g., a steam generator level between the steam lines and the tube sheet is sufficient for the success of the heat sink as opposed to maintaining it over the narrow range required for power operation). Therefore, for most applications of PRA, considerations of dynamic methods are not necessary (Technical Specifications, configuration risk management, significance determination, in-service inspection and testing, etc.).

b) *Have any dynamic methods been used in your country for modelling digital systems?*

Response: US National Laboratories are considering dynamic methods. Reactor vendors and US utilities are not yet considering applications which would require such methods.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) *What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?*

Response: There are two types of failure rates associated with digital I&C for which data is necessary in quantification of the PRA, initiating event frequencies and mitigating system failure probabilities.

Initiating event frequencies: I&C that contribute to plant trips in the US are generally associated with balance of plant systems (e.g., turbine and feed water control systems). Several sources of initiating event data are available regarding these balances of plant systems – the North American Reliability Council Generating Availability Data System (NERC-GADS) and Licensee Event Reports (LERs). NERC-GADS provides data regarding the number of plant trips as a function of time as well as an estimate of the operating hours for the industry as a whole by system and includes sufficient detail to estimate what portion of those trips were I&C related. An LER is generated by licensees for each plant trip. Review of each LER is necessary to determine whether the trip was I&C related. Information not necessarily available in either data source is whether the I&C is digital or analog.

Failure probabilities: Given the experience in the US nuclear industry with digital safety systems, there is limited raw data from which to develop failure probabilities Some raw data is available for portions of plant protection systems that are digital and have been in service for as much as 20 years. However, access to plant specific records is necessary to determine in service and demand information useful in generating failure probabilities for these systems. Consideration is being given to collecting such data where available in the US. However, this data is not readily available and while this operating experience has been useful to vendors for improving their designs and eliminating failure causes, its use for failure rate generation may be questionable because of significant advancement of the digital technology over the last 20 years. Therefore, there are generally three sources of data from which to derive digital system failure probabilities in the US - vendors with operating experience at foreign utilities or in other industries, expert opinion based on a review of the design characteristics of the digital system design and conformance to standards that indicate the likelihood of failure of digital systems complying with the standard.

b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

Response: See 'a' above.

c) What method did you use for processing these raw data into failure parameters, such as failure rates?

Response: See 'a' above.

For initiating event frequencies,, it is not necessary to break out the digital I&C portion of the frequency from those caused by mechanical failures unless the digital system shares common elements with mitigating systems. In that case, classical or Bayesian statistics can be used to develop an unique frequency for the digital system contribution to plant trips. Given that the precise date associated with the transition to digital controls is not available from the referenced generic data sources, an estimate of when this occurred must be made.

For failure probabilities, vendor information, expert opinion or conformance with standards have been used as noted above.

d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

Response: See 'a' and 'c' above.

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) How do you account for the impact of software failures on system reliability?

Response: Among the principal benefits of some of the software in a digital system is to assure the reliability of the system, quite likely making it greater than that for analog counterparts. The ability to incorporate features such as data validation, fault tolerance, self testing of digital system components can permit greater assurance of the system performing its function when called upon. This also the principle reason for the wide spread transition to digital technology in many industries. In the US, these design features are treated superficially, if at all, in PRAs and is an area for further improvements in modelling.

Given that it does not exist in comparable analog systems, software can add new failure modes and behaviours to the I&C system. These failure modes ultimately may manifest themselves as failures of components they control to perform their functions or to operate in an unexpected manner when not called upon. These potentially negative effects are the focus of software modelling in PRA at this time. Software is incorporated in PRA models as an event representing a failure mode associated with the hardware in which it exists (e.g., a processor) or in terms of the effects in has on the components that the digital system controls (e.g., pumps and valves and their associated failure modes). Shared digital system components and software are linked as dependencies for redundant components. Common software is included in the models for redundant components as CCF events.

b) *How realistic is your approach for accounting for this impact?*

Response: Sometimes overly conservative modelling of software CCF, as is sometimes the case with strictly deterministic methods (such as not accounting for defenses and other measures that ensure separation and independence), leads to unrealistic results and a masking of the I&C features that are important, such as functional diversity.

As noted above, consideration of defensive design measures is treated superficially, if at all, in PRAs and is an area for further improvements in modelling. With improved modelling, the value of such design features can be estimated and suggestions made with respect to the design of the digital system itself for reliability purposes.

With respect to the failure modes of the digital system, the effects on the components that the digital system controls are considered explicitly and in some cases in a bounding manner even if the digital system itself is not modelled in detail. Improvements in modelling techniques could make modelling more realistic through removal of conservative approaches to modelling the effects of the digital I&C.

c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

Response: The need to model software failures in the PRA and the level of detail required is dependent on the application. In some applications, the software may not need to be modelled explicitly at all. For example, process control systems for normal plant control that affect only initiating event frequency can be quantified based on operating experience. Applications in which the software is not common to diverse systems also may not need to consider explicit modelling of the software. In these cases, the software is effectively a subcomponent of the equipment in which it is included and can be considered among the other subcomponents not modelled explicitly but leading to the failure modes already modelled for those components (including both random and CCF failure modes).

d) *Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?*

Response: The software and its associated hardware are modelled in an integrated fashion in PRAs at this time. If the software can cause a failure mode of the hardware that is not currently included in the PRA then that failure mode can be added to the model. Applications have not been encountered as yet which require unique modelling of interactions between the software and the hardware that are not typical of the failure modes already included in PRAs.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?

Response: The effect of uncertainties on the results of risk evaluations involving digital systems depends on the application and how sensitive the decisions being made are to the contribution to risk from the digital system. Recent risk evaluations involving digital systems have addressed each of the three sources of uncertainty as follows:

Parametric uncertainty – Typically addressed through the performance of sensitivity studies, particularly if failure rates for the digital system are developed using expert judgment or through use of probabilities derived from generic sources such as consensus standards. Such sensitivity studies generally derive how much variation in the failure rates is needed to influence the decision under consideration as opposed to attempting to estimate an upper and lower bound. When distributions are assumed, broadening the error factors by several orders of magnitude can be performed to assess the effect on the decision being made.

Model uncertainty – Remembering that the I&C must be examined in terms of the functions performed by the mechanical and electrical systems it actuates or controls, consideration of potential digital failure modes that may occur other than those modelled in the PRA can be addressed as a part of the translation of the digital system failure modes to those associated with the components that they actuate or control. If not already assumed as a part of the application, assuming that digital system failures always lead to the specific failure modes of the mechanical and electrical equipment that are included in the PRA can bound modelling uncertainty for the failure modes of the digital system.

Completeness uncertainty – Completeness uncertainty is a reflection of scope limitations and the focus of a completeness evaluation is necessarily application specific. When considering alternatives in resolving a safety issue, assuring that all accident sequences that could be affected by each alternative are considered, not just those that are the subject of the issue being addressed (e.g., a digital system modification directed at LOCAs could also have an effect on transients or external events. Both positive and negative effects of the design change should be identified and quantified).

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) What methods are used in your country for modelling human errors associated with digital systems?

Response: The consensus within the US is that the overall net effect of transition to digital technologies will likely be an improvement in operator response to accidents and transient conditions resulting from a better interface associated with the digital HSI as compared to current

analog indications and controls, greater access to operator informational needs associated with plant conditions and the status of safety functions, fewer actions needed on the part of the operators to control mitigating system or division operation, computerized procedures and a higher reliability of the HSI due to measures such as fault tolerance and self testing. Nevertheless, additional failure modes can be introduced associated with the HSI that are not typical of analog systems.

Pre-initiator operator actions: As noted above, pre-initiator errors are not exclusive to digital systems. Current PRAs already incorporate failure to restore from maintenance and miscalibration. These failure modes are expected to be retained as a part of the digital I&C modelling. Also, CCF of instrumentation and control systems are normally included in PRA models and would be upgraded with incorporation of digital I&C models. Whether these are more likely than that for analog systems remains to be determined.

Post-initiator operator actions: Given that emergency procedures will remain symptom oriented, operator actions required post trip are similar whether I&C used by the operators are analog or digital. Digital I&C and computerized procedures are expected to facilitate the implementation of emergency procedures. Therefore, the approach to developing human error probabilities using digital instrumentation and controls is expected to be similar to that currently used for analog control rooms. Where additional human error probabilities may need to be generated is in the event the normal HSI is subject to digital CCF. In this instance, use of diverse backup HSI (required in current regulatory guidance) will need to be considered in development of human error probabilities.

Whether it affects pre or post-initiator operator actions, the analyst must understand what configuration control measures are used? In addition, for new US plants, The HSI design is required to consider the PRA identified risk-important human actions in the HSI design (task analysis, V&V, etc).

b) *Are there any available data associated with the probability of this kind of error?*

Response: The timing of accidents and transients is not expected to change as a result of the use of digital I&C. The response of the operators is expected to improve given the implementation of digital controls leaving the overall time needed to implement actions in accordance with EOPs dictated by the response of the mechanical and electrical systems being actuated by the operators. Where there is a difference in the manner in which operators respond to an accident or transient given digital displays and controls is when digital failures are postulated to affect the normal HSI. Procedures and training are currently under development in the US for this situation and no formal data is available at this time.

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

Response: The US nuclear industry is performing research in the areas of identifying defensive measures used by designers to limit the potential for digital failures and CCF, identifying what constitutes adequate diversity in mitigating postulated digital CCF, reviewing operating experience to determine the characteristics of digital failures that are known to have occurred, identify what has been done to prevent recurrence and establish design measures that have

prevented the occurrence of such failures. In addition, the industry is applying PRA in the evaluation of the risks associated with digital I&C. Such evaluations include a determination of the value of defense-in-depth and diversity given a plant wide digital upgrade and quantification of the benefits and risks of proposed diverse actuation systems.

As mentioned previously, methods are being investigated that would allow combinations of the traditional approach to PRA methods (event tree/fault tree) to be combined with other dynamic methods such as Markov modelling. This research is in the very early planning stages.

b) What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?

Response: The following are several areas for further work in the modelling and quantification of digital I&C in PRA. To influence the licensing of new plants and the design digital upgrades of current plants, the research would need to be complete over the next year or two.

- Review operating experience to determine of failure modes of digital systems that have occurred and identify design measures that have been effective in preventing them.

- Review operating experience to obtain estimates of demands and operating hours to support development of empirical data regarding the failure probability of digital system designs with reference to specific design features.

- Develop techniques for assessing the quantitative benefits of design measures directed at limiting the potential for digital failures including CCF (e.g., data validation, fault tolerance, self testing, etc.) Part of this will involve estimating the "fault coverage" parameter for different types of digital components and their failure modes by the fault tolerant/self testing circuits.

- Establish a methodology for estimating the failure probability of digital I&C, including software, given the absence or presence of specific design features (e.g., cyclic behaviour, data validation, etc.)

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

a) Has risk information related to digital systems already been used for decision making in your country?

Response: Yes, the vendors of advanced reactors are modelling digital I&C in PRA and making recommendations regarding the design of the systems to address risk. Existing plants are modelling digital I&C in PRA for similar purposes. EPRI is modelling digital I&C in PRA to develop risk insights regarding new regulatory guidance directed at addressing digital CCF.

b) What decision making do you foresee that would use risk information related to digital systems?

Response: Determining the value of diversity in the performance of defense-in-depth and diversity evaluations.

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

    a) *Do you consider that this kind of categorisation is feasible and practical?*

       Response: One important categorisation step is the need to separate NSR process control systems from SR protection systems as failure modes and modelling techniques applicable to each will not necessarily be relevant to the other.

       Following that is a need to classify methods by application as the level of detail in modelling digital I&C in PRA and quality of data needed will depend on the use to which the PRA is put. The greater the sensitivity of the results of the PRA to the digital I&C and the influence the I&C has on the decision being made, the greater the level of detail and the quality of the data needs to be.

    b) *If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?*

       Response: Overall PRA results and risk-informed decisions that are not greatly influenced by the effects of the digital I&C failure modes or failure rates are applications for which detailed modelling and precise data are not critical.

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

15. From the topics above, which do you consider most important to address, and why?

OSU (DR. TUNC ALDEMIR) RESPONSES

1. Digital protection and control systems are appearing as upgrades in older plants, and are commonplace in new nuclear power plants (NPPs). In order to assess the risk of NPP operation and/or to determine the risk impact of digital systems, there is a need for reliability models and failure data for these systems that are compatible with existing plant probabilistic safety assessments (PSAs). Once the models and data are obtained, system unreliability and some risk metrics of a NPP, such as core damage frequency (CDF), can be quantified.

   However, at present there are no consensus methods and failure data for quantifying the reliability of digital systems. Due to the many unique features of these systems (e.g., software), a number of modelling and data collection challenges exist. Addressing these challenges would be greatly facilitated through an international cooperative effort, focused on an exchange of information and experiences on modelling these systems. Many countries have this kind of experience, and it would be useful to share and discuss it.

   a) *Do you consider that it is meaningful to model failures of digital components in a probabilistic way? If not, how should they be accounted for in evaluating the risk of a digital system?*

      Yes

   b) *Have probabilistic models of digital systems been developed in your country (nuclear or relevant non-nuclear)?*

      Yes

   c) *For what purpose have these models been developed?*

      To investigate the potential impacts of digital upgrade of nuclear power reactor I&C systems

   d) *What are the standards or guidance that you have used for developing or reviewing these models?*

      Capability to model the statistical dependency between failure events that may arise from hardware/software/firmware/process interaction.

   e) *What is the scope of the models, e.g., do they include hardware and software failures?*

      They include both hardware and software failures, but as software embedded in hardware due to failure data availability.

   f) *Have the models been integrated into a PSA model of an entire NPP?*

      Yes.

g) *Can you make available at the technical meeting any publications documenting your work in this area?*

T. ALDEMIR, D. W. MILLER, M. STOVSKY, J. KIRSCHENBAUM, P. BUCCI, A. W. FENTIMAN, and L. M. MANGAN, Current State of Reliability Modelling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, U. S. Nuclear Regulatory Commission, Washington, D.C. (2006)

T. ALDEMIR, M. P. STOVSKY, J. KIRSCHENBAUM, D. MANDELLI, P. BUCCI, L. A. MANGAN, D. W. MILLER, X. SUN, E. EKICI, S. GUARRO, M. YAU, B. W. JOHNSON, C. ELKS, and S. A. ARNDT, Dynamic Reliability Modelling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942, U.S. Nuclear Regulatory Commission, Washington, D.C. (2007)

2. PSAs of NPPs have been and are typically developed using the event tree/fault tree (ET/FT) approach. Other methods, such as the Markov method, have also been used for this purpose. It may be possible to develop a probabilistic model of digital systems using one of these methods.

a) *What modelling method or methods have been used in your country for modelling digital systems?*

Dynamic flow graph methodology and Markov/cell-to-cell mapping technique. For description of the methods as well as their application please see NUREG/CR-6942 cited in Item 1.g above

b) *Is the method used for modelling digital systems in your country different from the method employed for the PSA of the rest of the NPP? If so, how do you integrate the model of the digital system with the PSA?*

Yes. For the description of the integration process see NUREG/CR-6942 cited in Item 1.g above

c) *If you model digital systems, do you use the same or different methods for modelling continuous control systems versus protection systems?*

Same methods

3. In its most basic form, a probabilistic model of a system (analog or digital) is a combination of a "logic model" and probabilistic data. The logic model describes the relationship of relevant failures of the components of the system leading to some undesired event, such as the failure of the system to respond adequately to a demand. The data are some parameters of the failures modelled, such as their failure rates. In general, a system's logic model is established by breaking down the failures of its major components into the individual failures of minor components. For example, a digital system may be decomposed into "modules," which consist of a microprocessor and its associated components. An example of a component is an analog-digital converter. Thus, the logic model can be developed by expressing the failures of modules (or large components) in terms of failures of their components. This refinement from failures of major components into failures of basic components is continued to a level of detail that the analyst considers appropriate.

a) *What level of detail was modelled in your country?*

Modules or macro-component level

b) *Why was this level of detail used?*

Failure data availability as well as computational limitations

c) Do you have any insights or recommendations on the level of detail that is appropriate for modelling digital systems?

If modelled at the macro-component level, the macro-components should be defined in such a way that all statistical dependencies of macro-component constituents on other system components are contained within the macro-component.

4. There is a relationship between failure cause, failure mechanism, failure mode, and failure effect. Using an analogy from a common component, a valve, a failure cause may be inappropriate maintenance of the valve, an associated failure mechanism is that due to corrosion the components of the valve are stuck in their current position, the related failure mode is that the "valve fails to open" (if the valve is normally closed), and the resulting failure effect is that the water that is required to pass through the valve is blocked. This example valve may have other failures causes, mechanisms, modes, and effects. A reliability model of a system is mainly concerned with the component's failure modes (how it fails) and failure effects (the consequences of the failure modes). In a probabilistic model, the effects of failure modes of components on the digital system and on the overall NPP are accounted for. To this end, it is first necessary to identify the failure modes of the components of the digital system. Typical methods for identifying failure modes of the components of analog systems are the failure modes and effects analysis (FMEA) and the Hazard and Operability (HazOp) analysis. Usually, the FMEA is carried out by successively analyzing the system at deeper levels. In other words, the system is first analysed at a top-level, i.e., the entire system. Then the failure modes at lower levels of the system, such as its "modules," are postulated and evaluated. Subsequently, the failure modes of the components of each module are analysed. As mentioned above, this refinement is continued to the level of detail considered adequate for the objective of the model.

a) Identifying the failure modes of the components of a digital system is necessary for modelling them in the PSA. What methods, tools and/or guidance do you use for this identification?

FMEA, experiments and operational experience

b) Do you consider operating experience in identifying failure modes?

Yes, but not only operating experience.

c) How do you determine the effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function?

FMEA to evaluate the immediate effects. The effect of a failure mode of a digital system component on the capability of the digital system to accomplish its function is propagated either through Markov/CCMT or DFM.

d) How do you determine the effect of a combination of failure modes of digital components on the capability of the digital system to accomplish its function?

Please see Item 4.c above.

5. An important requirement of a PSA model is that all types of dependencies are correctly included in the logic model. This is particularly important for digital systems, whose unique features can result in different types of dependencies. The dependencies arising from the use of digital systems may be grouped into the following categories:

A. Dependencies related to communication. Components of digital systems communicate through buses, hardwired connections, and networks. A network may be used for the communication

between the components of one digital system and the components of another. A network also may connect a digital system with the components controlled by the system.

B. Dependencies related to support systems. Digital systems depend on AC or DC power, and may also depend on Heating, Ventilation, and Air Conditioning (HVAC) for room cooling.

Dependencies related to sharing of hardware. Some hardware components may be shared by other components or systems; either within the system or across the boundaries of systems. For example, voters may receive signals from several channels within a system, and sensors may send signals to several systems.

C. Dependencies related to fault-tolerance features. Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they are expected to have a positive effect on the system=s reliability. However, these features may also have a negative impact on the reliability of digital systems if they are not designed properly or fail to operate appropriately.

D. Dependencies related to dynamic interactions. These dependencies are addressed in Topic 6, below.

E. Dependencies related to common cause failures (CCFs). In many cases, a digital system is implemented using several redundant channels. Furthermore, redundancy sometimes is used within a channel to enhance reliability. This high level of redundancy is typically used when a digital system is significant to the safety of a NPP, such as a Reactor Protection System (RPS). Such redundancy at the channel level and within each channel usually employs identical components. Hence, CCFs may occur at each level. CCF events represent dependent failures that otherwise are not explicitly modelled, e.g., manufacturing defects and design errors.

a) What types of dependencies do you include in your digital system reliability model?

All of the above.

b) Did you find any of these dependencies to be risk significant?

Dependencies related to dynamic interactions in so much as to changing the demand rate on a safety system.

c) Do you consider that the methods you used for identifying and modelling dependencies are adequate?

Yes.

6. Some probabilistic dynamic methods have been proposed in the literature that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and (2) the timing of these interactions, i.e., the timing of the progress of accident sequences. However, the PSA community has not reached a consensus about the need for explicitly including these interactions in the PSA model.

a) Do you consider it necessary to accurately model these interactions and their timing?

We have observed that the interactions and their timing can affect the demand rate on a safety system. However, it is not clear at this point in time whether they can significantly affect the core damage frequency due to the limited number of initiating events and systems considered.

b) Have any dynamic methods been used in your country for modelling digital systems?

Yes. Please see NUREG/CR-6942.

7. A digital system is usually comprised of hardware and software. The probabilistic model of this kind of system may explicitly include the failures of both to be able to capture all the relevant contributors to system unreliability and to risk metrics of a NPP, such as CDF. To quantify the system unreliability and the CDF, it is necessary to have probabilistic data, such as a failure rate, for each hardware failure and software failure included in the system model.

a) What information sources did you use for obtaining raw failure data, such as number of failures in a given period, of hardware components of digital systems?

Fault injection (please see NUREG/CR-6942).

b) What information sources did you use for obtaining raw failure data of common cause failures of hardware components of digital systems?

Common cause data were unavailable.

c) What method did you use for processing these raw data into failure parameters, such as failure rates?

Please see NUREG/CR-6942

d) What method or approach did you use for assessing probabilistic parameters, such as failure rates, of software failures?

Please see NUREG/CR-6942

8. The most unique characteristic of a digital system distinguishing it from an analog system is that it contains software. While software gives great capabilities and flexibility to a digital system, software failures have caused system failures and have resulted in serious events in many industries. Accordingly, it is advisable to include software failures in the probabilistic model of a digital system because they have the potential to be significant to the reliability of the system. On the other hand, there does not appear to be consensus in the PSA community on how to include them.

a) How do you account for the impact of software failures on system reliability?

By quantifying coverage through fault injection. Please see NUREG/CR-6942

b) How realistic is your approach for accounting for this impact?

In principle the technique used is capable of considering software failures. However, the limitations in the application described in NUREG/CR-6942 are the following:

- Requirements and design faults were not considered.
- Software implementation faults were not considered.
- Permanent hardware faults were not considered.
- Possible non-uniform distribution of hardware faults and fault types was not considered.
- Fault-injection testing was not carried out according to a representative operational (input) profile.

c) *Are there reliability evaluations involving digital systems where you did not feel the need to explicitly model software failures? If so, why was it not necessary to model them?*

None

d) *Do you address interactions between software and hardware? If so, how do you account for such interactions in the probabilistic model?*

Please see Items 8.a and 8.b above.

9. Reliability models of digital systems are complex and consist of many elements. Since probabilities cannot be measured directly, there can be no direct verification of either the models or their results. In addition, these models involve varying degrees of approximation. Therefore, the associated uncertainty in the results may be significant and must be addressed. It is helpful and convenient to categorise uncertainties into 1) those that are associated with the data used to quantify the models (parameter uncertainty), 2) those that are related to the models employed (model uncertainty), and 3) those that are due to the incompleteness of the model (completeness uncertainty). For digital systems, parameter uncertainty is due to the scarcity of failure data of digital components, model uncertainty arises from the assumptions made in developing and selecting the probabilistic models, and completeness uncertainty is due to the possibility that some relevant elements of the model were not included.

a) *How have the three types of uncertainty been addressed when developing and assessing reliability models of digital systems?*

Please see NUREG/CR-6942

10. While the introduction of digital systems provides benefits to a NPP, it may introduce new failure causes and failure modes, e.g., the new human-system interfaces (HSIs) may cause new human errors. Two types of human errors associated with digital I&C systems are: 1) Once a digital system has been installed and is operational in a NPP, it may be upgraded to fix some identified problems, to enhance its functionality, or for another reason. An upgrade may introduce new errors into the system. This type of failure also may happen when upgrading an analog system. However, it may have a higher probability of occurring when upgrading digital systems due to their greater complexity and use of software. 2) If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use. It is advisable that both types of human errors be accounted for in the probabilistic model, as well as other types of human errors related to digital systems, as applicable.

a) *What methods are used in your country for modelling human errors associated with digital systems?*

b) *Are there any available data associated with the probability of this kind of error?*

11. As described in the previous points, reliability modelling of digital systems presents several technical challenges.

a) *What, if any, research and development (R&D) activities are currently ongoing in your country to address any of these challenges?*

b) *What additional R&D activities are needed to improve digital system reliability assessments, and in what time frame are they needed?*

12. Information and insights obtained by developing and quantifying digital system models may be used for risk-informed decision making.

    a) Has risk information related to digital systems already been used for decision making in your country?

    b) What decision making do you foresee that would use risk information related to digital systems?

13. It may be possible to allocate different types of digital systems (or risk-informed decisions involving digital systems) into different categories of reliability modelling. Each category of modelling would have different modelling requirements, e.g., level of detail or quality of data.

    a) Do you consider that this kind of categorisation is feasible and practical?

    b) If the answer to the previous question is affirmative, do you have any thoughts on how such categorisation could be accomplished?

14. What other aspects of probabilistic modelling of digital systems do you consider relevant?

    The questions above cover all the aspects.

15. From the topics above, which do you consider most important to address, and why?

    Dependencies and human machine interface.