International Experience with Modeling Digital Systems in PSAs

Tsong-Lun Chu [a*], Gerardo Martinez-Gurdi [a], Alan Kuritzky [b], and Abdallah Amri [c]

[a]Brookhaven National Laboratory, Upton, NY, USA
[b]U.S. Nuclear Regulatory Commission Washington, DC, USA
[c]Nuclear Energy Agency, Paris, France

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

Keywords: PSA, PRA, Digital I&C Systems, Reliability Modeling and Quantification

1. INTRODUCTION

Digital protection and control systems are appearing as upgrades in older nuclear power plants (NPPs) and are commonplace in new NPPs. To assess the risk of NPP operation and/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 modeling and in data collection. The Committee on the Safety of Nuclear Installations (CSNI) of the Nuclear Energy Agency (NEA) of the Organization 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 sharing and discussing current experiences with reliability modeling and quantification of these systems in the context of PSAs of NPPs. The results of the work performed under this activity are documented in an NEA/CSNI report [1].

2. 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 modeling and evaluating the reliability of these systems.

3. APPROACH

The principal mechanism for the discussion of experiences with reliability modeling and quantification of digital I&C systems in the context of PSAs of NPPs was a technical meeting that was held in Paris,

[*] Contact author e-mail address: chu@bnl.gov
[†] The terms probabilistic safety assessment (PSA) and probabilistic risk assessment (PRA) are synonymous and are used interchangeably in this report.

France, during October 21-24, 2008. The TG prepared and distributed a list of technical areas associated with DIC system reliability modeling 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 organizations, 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 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 at the annual meeting and subsequent post-meeting member comments were used to develop a final set of recommendations [1].

4. SUMMARY OF TECHNICAL DISCUSSIONS

As mentioned above, a document describing technical areas for discussion and associated questions on different aspects of probabilistic modeling of a digital system was provided to all participants in advance of the technical meeting. This section summarizes some of the key points made during the discussions of these technical areas.

4.1 Development of Probabilistic Models of Digital Systems

There was consensus that it is meaningful to model failures of digital components, including software, in a probabilistic way. The hardware components of a digital system can be modeled probabilistically because they are subject to failure mechanisms similar to those of analog components, such as wear and tear, and thus can fail randomly. Software “failures” can be considered to be random, since although the way a fault is introduced into the software is not necessarily random, the occurrence of the particular context that would cause the fault to manifest into a digital system failure is random.

All representatives from countries with operating NPPs indicated that models of some DIC systems have been developed, though there is wide variability in the scope of the models in terms of modeling hardware and software failures. The models can be classified into three types: (1) models that 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) models where software failures are included as separate events; and (3) models where only hardware failures are considered (i.e., software failures are omitted).

There are no specific standards or guidance for modeling 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 modeling and quantifying DIC systems. The International Electrotechnical Commission (IEC) 61508 [2] and IEC 60880 [3] are standards related to digital systems; however, regulatory bodies have not endorsed them. Recently, the U.S. Nuclear Regulatory Commission (NRC) staff developed a draft Interim Staff Guide (ISG) on reviewing the PRAs of new reactors’ DIC systems [4]. Further, Brookhaven National Laboratory (BNL) (U.S.) advanced a set of desirable characteristics for a probabilistic model of a digital system, documented in NUREG/CR-6962 [5]. It was an input to the NRC staff’s ISG.

4.2 Methods Used for Modeling

Most participating organizations used traditional fault trees to model DIC systems. However, the French representatives (from the Institut de Radioprotection et de Sûreté Nucléaire [IRSN], Électricité de France [EdF], and AREVA) described one similar approach using a logical equivalent to a fault tree. They employ a "compact model" [6], 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 organizational factors. Other modeling approaches have also been applied. For example, the NRC sponsored several organizations to apply other methods to the case study of a digital feedwater control system (DFWCS). ASCA (U.S.) used the dynamic flowgraph methodology (DFM) [7,8], BNL employed a traditional Markov modeling approach [5,9], and The Ohio State University (OSU) (U.S.) developed a Markov/Cell-to-Cell Mapping Technique (CCMT) [7,8].

4.3 Level of Detail of Models

The level of detail varies substantially between the models described by the participants. 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.

4.4 Methods for Identifying Failure Modes

Most organizations use failure modes and effects analysis (FMEA) with different levels of detail for hardware failures. The three exceptions are: (1) the Canadian Nuclear Safety Commission (CNSC) representative stated that identifying failure modes is not a major issue in modeling DIC systems of CANDU reactors in view of the level of detail at which they are modeled; (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 Taiwan 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 Korea Atomic Energy Research Institute (KAERI) representatives that carries out an FMEA specifically for software, (2) the identification of failure modes of software by the OECD Halden Reactor

Project, and (3) the two generic software failure modes used as placeholders in the BNL model of the DFWCS [9].

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 recognized as requiring additional research.

4.5 Modeling of Dependencies

The dependencies arising from the use of digital systems may be grouped into the following categories:

- Dependencies related to communication
- Dependencies related to support systems
- Dependencies related to sharing of hardware
- Dependencies related to fault-tolerance features
- Dependencies related to dynamic interactions
- Dependencies related to common-cause failures (CCFs)

All organizations considered CCFs. Most organizations accounted for dependencies due to communication, support systems, and sharing of hardware. Some groups modeled dependencies due to fault-tolerance features, but only OSU and ASCA included dynamic interactions. In general, the participants considered that the current methods for identifying and modeling dependencies are adequate, though some areas are thought to need more research (e.g., dependencies due to fault-tolerance features and dynamic interactions).

4.6 Treatment of Dynamic Interactions

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. In general, most participants considered that it is currently still unclear whether modeling these interactions and their timing accurately offers substantial advantages. Some organizations are researching this topic. The representatives from many organizations 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 modeling the former, but will probably not be needed for the latter.

4.7 Failure Data

The participants discussed the difficulties in obtaining raw failure data; such information is scarce and sometimes unavailable. Some organizations 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

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

Geseffschaft für Anlagen and Reaktorsicherheit (GRS) (Germany) mainly used reliability data provided by the manufacturer which were validated with limited operating experience from an NPP. BNL mainly used raw failure data from the PRISM database [10], 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 organizations 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) [11]
- Data from other industries

The Japan Nuclear Energy Safety Organization (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 modeled, (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 [10] for the other components of the DFWCS.

The participants agreed that 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.

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.

4.8 Modeling of Software Failures

All organizations agreed that the impact of software failures should be accounted for in DIC system reliability models. Most accomplish this objective by explicitly including events representing these failures in the reliability model. Some organizations 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 CCFs that usually are the dominant contributors compared with individual failures; accordingly, some organizations include only CCF events in their models.

- Digital systems are used for control and protection functions. Further, some are classified as safety-related, while others are non-safety-related. 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 can potentially introduce some failure modes that were not considered for analog systems.

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

4.9 Treatment of Uncertainties

Most participants 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 [9].

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

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

4.10 Modeling of Human Errors Associated With Digital Systems

While the introduction of digital systems provides benefits to an 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 an 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.

JNES and KAERI pointed out that they are applying current human reliability analysis (HRA) methods for analog systems to digital systems. CNSC and the Technical Research Centre of Finland (VTT) also consider that the current methods can be used for these systems. However, KAERI is developing an HRA method for a digitalized main-control room.

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.

In addition:

- The Institute of Nuclear Energy Research (INER) (Taiwan) 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.

- The Electric Power Research Institute (EPRI) (U.S.) indicated that a computerized HSI can introduce additional failure modes that are not typical of analog systems.

- The Idaho National Laboratory (INL) (U.S.) pointed out that the new interface with DIC systems involves cognitive processes that fundamentally differ from those associated with analog systems.

5. CONCLUDING REMARKS

The October 2008 WGRisk technical meeting provided a useful forum for the participants to share and discuss their respective experiences with modeling and quantifying DIC systems. It was recognized 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 modeling digital systems. In particular, those organizations that developed DIC reliability models at a higher level of detail were less concerned about some of the modeling challenges associated with a more detailed level of modeling. 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 organizations 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 CCF parameters, which often dominate the results.

Summarizing the activities during the technical meeting, the participants recognized that several difficult technical challenges remain to be solved in the fields of modeling 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. The different ideas that were suggested at the technical meeting were further discussed at the WGRisk annual meeting in March 2009, resulting in the final set of recommendations provided below.

6. RECOMMENDATIONS

The recommendations from this WGRisk activity [1] are grouped into the following three categories: method development, data collection and analysis, and international cooperation. They are summarized 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 modeling (including CCF), quantification of software reliability, assessing the effect of failures of components of a DIC system on the system, reliability modeling 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

Acknowledgements

The results presented in this paper are due to the collective effort of the task group "Digital I&C Reliability" of OECD/NEA Working Group on Risk Assessment (WGRisk) and the participants to the Technical meeting held in Paris, France, during October 21-24, 2008.

References

[1] Organization for Economic Co-operation and Development, "Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants," NEA/CSNI/R(2009)18, December 17, 2009.

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

[3] 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.

[4] United States Nuclear Regulatory Commission, "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments," Interim Staff Guidance, DI&C-ISG-03, Revision 0, August 11, 2008 (Accession Number: ML080570048).

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

[6] J.-P. Coulomb, and H. Chardonnal, "Simplified Modelling of the Instrumentation and Control in PSA," Proceedings of ICONE 5: 5th International Conference on Nuclear Engineering, Nice, France, May 26-30, 1997.

[7] 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 Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, October 2007.

[8] T. Aldemir, S. Guarro, J. Kirschenbaum, D. Mandelli, L.A. Mangan, P. Bucci, M. Yau, B. Johnson, C. Elks, E. Ekici, M.P. Stovsky, D.W. Miller, X. Sun, S.A. Arndt, Q. Nguyen and J. Dion, “A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems,” NUREG/CR-6985, February 2009.

[9] T.L. Chu, M. Yue, G. Martinez-Guridi, K. Mernick, J. Lehner, and A. Kuritzky, “Modeling Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods,” NUREG/CR-6997, August 2009.

[10] Reliability Analysis Center (RAC), “PRISM User’s Manual, Version 1.4,” Prepared by Reliability Analysis Center Under Contract to Defense Supply Center Columbus.

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