Journal of NUCLEAR SCIENCE and TECHNOLOGY, Vol. 41, No. 3, p. 323–330 (March 2004)

ORIGINAL PAPER

Probabilistic Safety Assessment for Instrumentation and Control Systems in Nuclear Power Plants: An Overview

Lixuan LU and Jin JIANG*

Department of Electrical and Computer Engineering, University of Western Ontario, London, ON, N6A 5B9, Canada

(Received July 18, 2003 and accepted in revised form December 3, 2003)

Deregulation in the electricity market has resulted in a number of challenges in the nuclear power industry. Nuclear power plants must find innovative ways to remain competitive by reducing operating costs without jeopardizing safety. Instrumentation and Control (I&C) systems not only play important roles in plant operation, but also in reducing the cost of power generation while maintaining and/or enhancing safety. Therefore, it is extremely important that I&C systems are managed efficiently and economically. With the increasing use of digital technologies, new methods are needed to solve problems associated with various aspects of digital I&C systems. Probabilistic Safety Assessment (PSA) has proved to be an effective method for safety analysis and risk-based decisions, even though challenges are still present. This paper provides an overview of PSA applications in three areas of digital I&C systems in nuclear power plants. These areas are Graded Quality Assurance, Surveillance Testing, and Instrumentation and Control System Design. In addition, PSA application in the regulation of nuclear power plants that adopt digital I&C systems is also investigated.

KEYWORDS: probabilistic safety assessment, instrumentation and control systems, graded quality assurance, risk-informed regulation, nuclear power plants, power system deregulation, common cause failures

I. Introduction

It is expected that over the next decade there will be an accelerating trend for governments worldwide to privatize major portions of their countries' electricity supply industry through deregulation.[1)] Philipson defines deregulation as ''a re-structuring of the rules and economic incentives that governments set up to control and drive the electric power industry''.[2)] Before deregulation, all levels of the electric power sector including generation, transmission, distribution, and even retail sales reside within a single company. This type of company fulfills all functions itself, and is referred to as being vertically integrated. After deregulation, a vertically integrated utility no longer exists. It is dismantled into separate companies according to their major business functions. Power generators now have to compete with each other to generate electricity and auction it on the electricity market. They must operate more efficiently and more economically to remain competitive. Nuclear power sectors have to compete with other power sources such as fossil-fuel, hydroelectric power, windmills, and distributed power generations. Deregulation forces Nuclear Power Plants (NPPs) to manage their operations more efficiently and effectively while making sure that safety levels are not jeopardized.

''Instrumentation and Control (I&C) systems play an important role in reducing the cost of producing electricity while maintaining or enhancing safety''[3)] in NPPs. Therefore, more attention should be paid to I&C systems, particularly in a deregulated environment. Furthermore, advanced digital I&C systems are being introduced to replace obsolete analog systems thus creating even more challenges for NPPs. Questions such as: how to allocate resources for digital I&C systems, how to design optimal testing and maintenance procedures, how to design reliable and cost-effective I&C systems, and how to make regulation decisions for NPPs with digital I&C systems need to be answered in the deregulation process.

Probabilistic Safety Assessment (PSA), which was initially introduced in the nuclear industry to facilitate regulation, is a suitable method to handle operational issues such as surveillance testing and maintenance. PSA is an analytical tool used to identify potential system failures and to determine the likelihood and consequences of their occurrence.[4)] PSA techniques are used in the nuclear industry to assess the relative effects of contributing events on system reliability and plant risk. Consequently, resources are allocated to the most risk-significant segments of the system and unnecessary expenditures are reduced. The problems confronted by I&C systems can be handled more efficiently if PSA results are considered. Therefore, the introduction of the ''risk'' concept and PSA methodology into I&C systems deserves further investigation.

PSA is applied in various aspects of I&C systems. An important area of PSA application is risk-informed regulation. Traditionally, the regulation of NPPs is based on a deterministic approach,[5)] where one considers a set of arbitrary accidents and determines how these challenges should be handled. Thus, only a predefined set of factors is considered. The deterministic approach also lacks an explicit definition for ''safety'' and there are potential inconsistencies in the judgment of relative safety. Consequently, the probabilistic approach for reactor safety regulation is proposed.[6–9)] A

*Corresponding author, Tel. +1-519-661-2111ext.88320, Fax. +1-519-850-2436, E-mail: jjiang@uwo.ca

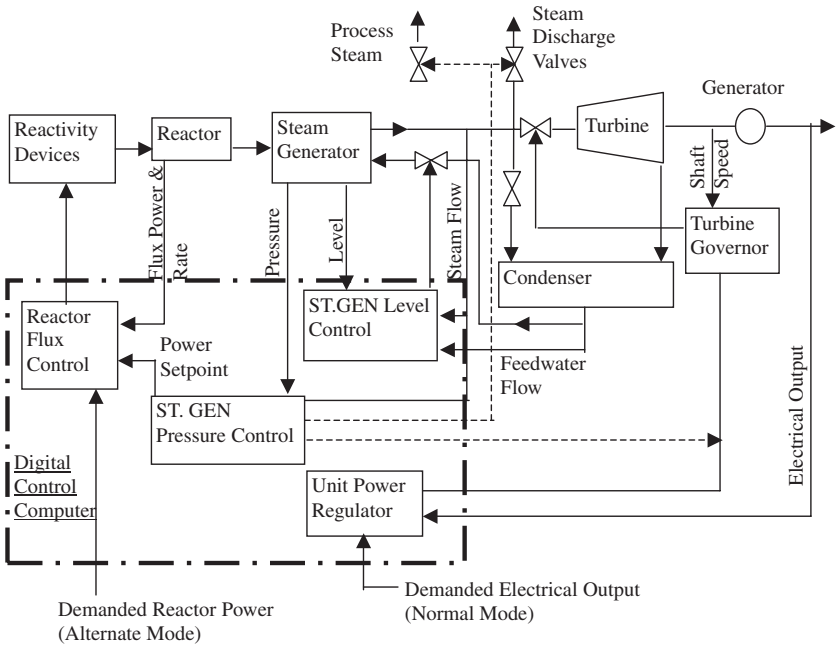

Fig. 1 Block diagram of overall plant control

probabilistic approach makes a comprehensive evaluation of all accident scenarios, extracts relevant factors, and ranks their relative importance according to marginal risk contributions. Therefore, the regulation of NPPs can be improved by allowing designer/operator to focus on important issues. Based on this information, the use of risk-informed regulation is advocated, thus allowing for the allocation of resources to components or systems according to their safety contributions in the plant. Risk-informed regulation is extremely important for I&C systems since they consume a large portion of the resources in NPPs.

This paper provides an overview of PSA for I&C systems in NPPs. It reviews current practice and recent results on this subject with reference to the experience of the nuclear industry and governments around the world. This will put research in PSA for I&C systems in perspective and also stress the importance of this subject. Chapter II introduces the basic notion of I&C systems and challenges faced by digital I&C systems. Chapter III examines existing techniques for performing PSA in NPPs and risk importance measures found in PSA studies. The methodologies to apply PSA in various aspects of I&C systems in NPPs and PSA's potential advantages and challenges are discussed in Chap. IV. One of the important applications of PSA is for regulation purposes and relevant regulations and industry standards are discussed in Chap. V.

II. I&C Systems in Nuclear Power Plants

1. Introduction

I&C systems in NPPs "cover a broad range of systems including instrument, control, safety, protection, information, human-machine interface, diagnosis, and other related systems".[3] NPPs rely heavily on I&C systems to provide monitoring, control, and protection both during the normal system operation and under contingencies.

Canadian Deuterium–Uranium (CANDU) reactor based NPPs can be used as an example. The main systems in the overall plant control are shown in **Fig. 1**.[10] The control computer is illustrated in a separate box highlighted by dotted lines. The primary control systems consist of a unit power regulator, a steam generator pressure controller and a reactor flux controller. Instrumentation systems are used to measure the reactor neutron flux over the full operating range of the reactor. The instrumentation systems for the reactor power measurement in a CANDU6 design are summarized in **Table 1**.[10] Proportional counters, ion chambers and self-powered in-core flux detectors are used to provide continuous measurement.

2. Transition from Analog to Digital in I&C Technologies

Analog and rudimentary digital I&C technologies were adopted when NPPs were designed and constructed decades ago. At present, many of the original I&C systems are approaching or have exceeded their designed lifecycle. As a result, the failure rate of these systems increases gradually, leading to increased maintenance costs and decreased availability of spare parts. Obsolescence has become a major issue for the nuclear industry and in the mid-nineties, NPPs throughout the world began to adopt digital technologies to modernize their I&C systems.[11–14]

3. Advantages of Digital Technologies

Digital systems generally have higher data handling and storage capacities.[15] Therefore, digital technologies are expected to improve system performance, reduce maintenance costs, enhance safety and increase competitiveness. The annual report (1993–1994) from the World Technology Evaluation Center (http : //www.wtec.org/loyola/

Table 1 Reactor power measurement systems

Neutron Flux Instrumentation System	Application			
	Flux Mapping	Flux Regulation	Safety Systems	
			SDS-1	SDS-2
Proportional Counters	N/A	3 BF_3 Counters (in-core) for 10^{-14} to 10^{-9} of full power 3 BF_3 Counters (ex-core) for 10^{-10} to 10^{-6} of full power		N/A
Ion Chambers	N/A	3 at one side of calandria (for bulk flux between 10^{-6} and 0.15 of full power)	3 at one side of calandria (ex-core)	3 at opposite side of calandria (ex-core)
Flux Detectors	102 in-core vanadium detectors	28 in-core platinum detectors	34 in-core platinum detectors	23 in-core platinum detectors

ar93_94/icss.htm) reports that Canadian CANDU plants adopted very advanced digital I&C systems at the time. The Darlington plant which began operation in 1990 relies entirely on digital systems for its control functions and over 70% for its plant protection systems. The Canadian NPPs designer Atomic Energy of Canada, Ltd. (AECL) and electrical power utilities have demonstrated over the years that digital I&C systems are effective in monitoring and controlling CANDU NPPs and in providing sufficient safety margins to protect both the plant and the public. As a result, the percentage of digital I&C systems has grown gradually as shown in **Fig. 2**.

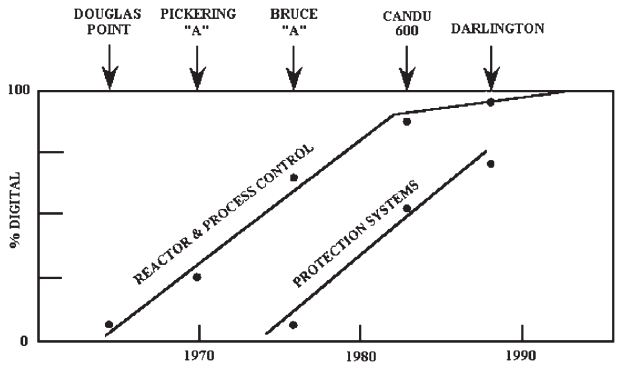

Fig. 2 Trend towards digital control and protection in CANDU Pressurized Heavy Water Reactor Nuclear Steam Supply Systems (PHWR NSSS) (Source: Atomic Energy of Canada, Ltd.)

4. Challenges in Using Digital Technologies

There are some challenges associated with introducing digital technologies. These include:

(1) uncertainties inherent in the introduction of new technologies;
(2) Common Cause Failures (CCFs) in software, configuration management, and their effects on safety margins; and
(3) lack of consensus on issues underlying the evaluation and adoption of digital I&C technologies.

The nuclear power industry has put a great deal of effort into resolving the digital system licensing issues[15] that arise from these challenges. However, the performance of digital I&C systems can still be improved. PSA ''allows one to account for, apart from the performance of system hardware, the aspects like human factor and uncertainty modeling''.[16] It can also be used to quantify CCFs. Therefore, the insights revealed from PSA analysis could be useful in various aspects of I&C systems.

III. Probabilistic Safety Assessment

1. Introduction

PSA is an analytical tool used to assess the safety of safety-critical facilities under various events. The theoretical aspects of PSA are documented in several books.[17–20] PSA typically involves fault tree analysis, often in combination with other methods such as event trees, reliability block diagrams, and Markov models.[21] PSA attempts to answer the following three basic questions:

(1) What are the initiating events (undesirable starting events) that lead to adverse consequence(s)?
(2) What and how severe are the adverse consequences that a NPP may be eventually subjected to as a result of the occurrence of the initiating events? and
(3) What is the probability or frequency of these undesirable consequences occurring?

2. Risk Importance Measures

The most important information from a PSA analysis is the ''risk importance measure''. ''A risk importance measure gives an indication of the contribution of a certain component to the total risk.''[22] It ranks the components according to their importance to safety in order to help make reliable and cost effective choices with respect to (re)design or maintenance efforts. The most frequently used risk importance measures are given in **Table 2**.[22]

In Table 2, the following definitions are used:

$R(x_i=1)$: The increased risk level without basic event x_i or with the failed basic event x_i

$R(x_i=0)$: The decreased risk level with the basic event optimized or assumed to be perfectly reliable

R(base): The present risk level

x_i(base): Unavailability of a component i.

3. PSA Worldwide

PSA studies have been carried out in many NPPs around the world. Ontario Hydro, Atomic Energy of Canada Ltd. (AECL), and Atomic Energy Control Board (AECB) (now

Table 2 Risk importance measures

MEASURES	ABBREVIATIONS	PRINCIPLES
Risk Reduction	RR	$R(base)\text{-}R(x_i = 0)$
Fussell-Vesely	FV	$\frac{R(base)\text{-}R(x_i = 0)}{R(base)}$
Risk Reduction Worth	RRW	$\frac{R(base)}{R(x_i = 0)}$
Criticality Importance	CI	$\frac{R(x_i = 1)\text{-}R(x_i = 0)}{R(base)} \times x_i(base)$
Risk Achievement	RA	$R(x_i = 1)\text{-}R(base)$
Risk Achievement Worth	RAW	$\frac{R(x_i = 1)}{R(base)}$
Partial Derivative	PD	$\frac{R(x_i + \partial x_i)\text{-}R(x_i)}{\partial x_i}$
Birnbaum Importance	BI	$R(x_i = 1)\text{-}R(x_i = 0)$

Canadian Nuclear Safety Commission (CNSC)) in Canada have performed PSA studies on a number of NPPs.[23] These studies have been used for design verification and improvement, as support for license applications, and to assess potential public risks from operation of nuclear facilities.

The first large-scale probabilistic assessment of reactor safety in the U.S., the Landmark Reactor Safety Study (RSS), was published in 1975. Subsequently, the US Nuclear Regulatory Commission (NRC) and nuclear industry began to perform PSAs for different reactor designs. Individual Plant Examinations (IPEs) were requested by NRC in 1988 for each operating reactor and seventy-five IPEs were submitted to the NRC within three years. NRC and the nuclear industry then began to focus on the use of the risk information in regulating decisions.[24]

The International Atomic Energy Agency (IAEA) in Europe actively promoted the use of PSA to complement the deterministic defense-in-depth concept. An important aspect of the work by IAEA was to reach international consensus on the possibilities and limitations of the use of PSA methods. It identified approximately 100 safety issues for the first generation plants in Europe in 1996. Even though deterministic criteria were sufficient to identify some high priority items, it was concluded that for long term operation, the use of PSA might allow for cost effective improvements.[25]

The Australian government commissioned an independent assessment of the safety of its NPPs based on PSA techniques in 1996. The PSA was completed in early 1998 and the results were presented to the Australian Nuclear Science and Technology Organization (ANSTO).[26]

4. Future of PSA

The theoretical aspects of PSA have already reached maturity. The future of PSA lies in the scope of its applications. Configuration management, aging management, maintenance, operating procedures, and operational safety system test programs are all potential areas of application for PSA. I&C systems are natural candidates for PSA application.

IV. PSA for I&C Systems in Nuclear Power Plants

PSA was firstly adopted in the nuclear industry to make regulation decisions. As PSA methodology became more mature, it proved to be a promising candidate for making operational decisions. Various operational issues associated with I&C systems that are discussed in this section can better be dealt with if PSA results are considered, even though some challenges still remain.

1. Potential Difficulties when Applying PSA in I&C Systems

As the use of digital computers in I&C systems increases, there are several potential issues when applying PSA in I&C systems. For example,

(1) The nature of software failures
(2) The time dependency of unavailability and accident sequences
(3) The lack of adequate statistical data on system and equipment failure
(4) The incomplete independence of various systems and operator errors.

There have been some R&D efforts that address the first two issues. Garrett[21] describes a ''context-based'' approach to software risk assessment that explicitly recognizes the fact that the behavior of software is not probabilistic. However, Kang[27] presents a different idea which proves that when the software is utilized for a specific application, it fails randomly because of the randomness of the input sequences. This is based on the ''error crystals in software'' concept, which is the most common justification why a software failure is random. Living PSA which allows the safety of systems being analyzed in a real-time environment has been studied[28–32] in regard to the time dependency of unavailability and accident sequences. More research can be undertaken to address the last two issues.

2. PSA Applications in I&C Systems

Despite some difficulties, there have been some applications of PSA in I&C systems that demonstrate that PSA is a promising candidate to solve various problems associated with digital I&C systems. PSA used for Graded Quality Assurance (GQA), surveillance testing strategies, and I&C system design is discussed in more detail below. PSA for regulation will be elaborated on in section V. Readers who are interested in PSA applications for availability analysis, hazard analysis, and reliability evaluation of I&C systems are referred to Refs. 33–37).

(1) Graded Quality Assurance (GQA) for Digital I&C Systems

The purpose of applying GQA is to ''preferentially allocate resources based on the safety significance''[38] thus improving the safety and operation efficiency for both regulators and licensees. A recently proposed Bayesian approach[39] is promising in supporting the GQA practice for digital I&C systems.

A Quality Assurance (QA) model consists of elements that represent software development staff, software QA staff, development activities, QA activities and documents generated. Each element is represented as a node and is connected based on its causal relation with other elements. Each node is further designated by two to five states representing its status. In reality, the relation among QA process elements is not static. In order to represent the probabilistic behavior of the QA process, a technique based on the Bayesian Belief Network (BBN) can be applied. BBN is a modeling technique that represents systems that exhibit probabilistic behavior. The QA process model is then used to generate complete QA process scenarios. The process of failure scenario generation is shown in **Fig. 3**.

The number of occurrences of final outcomes of the model will be used to draw the risk profile graph. This graph is helpful in identifying potential areas of unnecessary conservatism.[39]

(2) Surveillance Testing Strategies

IEEE STD 338 ''Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems'' provides design and operational criteria for performing periodic testing as part of the surveillance program for NPP safety systems. (This standard can be found from IEEE website: http : //ieeexplore.ieee.org.) All systems and equipment receive equal consideration according to these criteria regardless of their functions or risk levels. The IEEE STD 338 revision was performed by considering ''lessons learned'' from the implementation of risk-informed approaches in other standards and regulatory activities. An I&C component testing approach proposed by Schinzel[40] is summarized as follows with abbreviations defined in Table 2:

(a) All electrical and I&C components are grouped into one of four categories according to risk levels.
   High Safety Significance (HSS):
      RAW$\geqq$100.0, or
      FV$\geqq$0.01, or
      FV$\geqq$0.005 and RAW$\geqq$2.0;
   Medium Safety Significance (MSS):
      FV$\geqq$0.005 and RAW$<$2.0, or
      FV$<$0.005 and RAW$>$2.0;
   Low Safety Significance (LSS):
      FV$<$0.005 and RAW$<$2.0;
   Not Risk Significant (NRS):
      The remaining components belong to NRS.
(b) Other conventional and deterministic factors remain a part of the categorization decision.
(c) The resulting grouping is verified or validated.
(d) HSS and MSS are combined and classified as safety significant. LSS and NRS are considered as not safety significant.
(e) Testing intervals are applied to safety significant components based on the mean time between failures, reasonable margins, and satisfying any established availability goals.
(f) For components classified as NRS, limited testing may be imposed.

A methodology was developed in Canada that can be applied to optimize the costs associated with testing dormant components.[41] The methodology is based on system unavailability models. The test optimization methodology is based on the basic optimization theory where the objective of the optimization is to reduce the cost (imposed by periodic testing) or to minimize the system unavailability. The identification of system limitations (represented by optimization constraints) goes hand-in-hand with the choice of optimization goals. The methodology is a practical tool that can be utilized to optimize the test programs at NPPs. As periodic inspection and testing constitutes a significant portion of a plant's resources, there are some benefits in applying Test Interval (TI) optimization to reduce overall costs associated with this activity while meeting the safety/reliability requirements or to minimize the overall system unavailability for a given cost level.

(3) I&C Systems Design

Some effort has been made to use probabilistic analysis when making design decisions for I&C systems. Kang[27] presented a case study that examines the fault tree analysis framework for the safety of digital systems. The case study was performed for the digital based reactor protection sys-

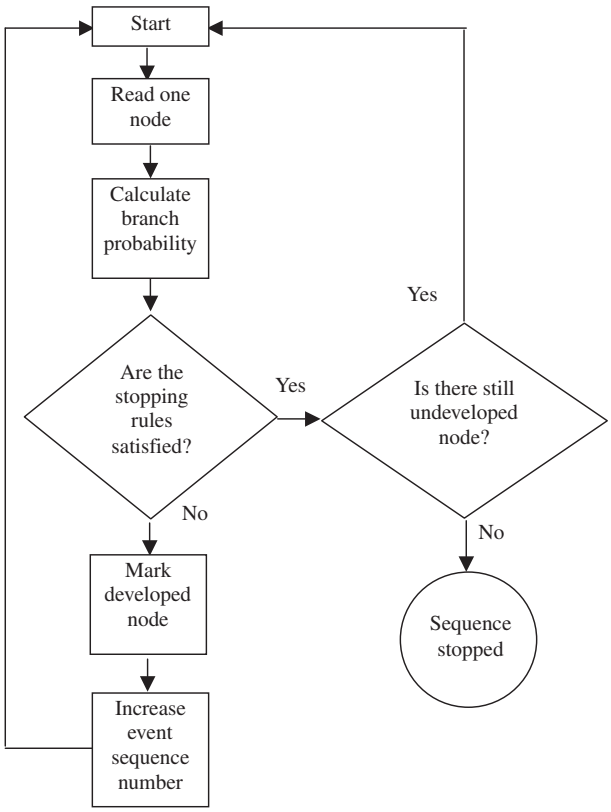

Fig. 3 Scenario generation process

tems in NPPs. It demonstrated that some factors can affect system safety. These factors include the Common Cause Failures (CCFs), the coverage of fault tolerant mechanisms, and software failure probability. Therefore, designers should exercise caution in minimizing the effect of CCFs and must consider the economical aspects such as development and maintenance costs. Designers can make more informed decisions from alternative choices based on the qualitative and quantitative results from PSA analysis.

Another case study was performed by Kubik for Big Rock Point Plant in the United States.[4] The investigation was undertaken to determine whether PSA methods would be useful in assigning priorities to environmental qualification requirements for instrumentation. The first step was to rank the importance of the equipment that was explicitly addressed in the plant PSA. The ranking provided insight into what systems and instrument groupings are important. Based on this information, engineers can make more accurate decisions about proposed plant modifications.

V. Risk-Informed Regulation

1. Applicability of Risk-Informed Regulation for I&C Systems

As Yih (2000) stated:[42] ''Regulation process has been considered as the major bottleneck for digital I&C projects of nuclear plants''. The variability and uncertainties associated with various aspects of I&C projects have always been major concerns. Risk-informed regulation may be preferable for the purpose of maximizing efficiency of the project resource allocation under these conditions. The situation can be represented as an optimization problem and can be solved using nonlinear programming techniques. The goal is to select an optimal set of activities that consumes the least amount of resources while achieving the maximal benefit.

The object function L can be represented as:

$$L = p_1a_1 + p_2a_2 + \cdots + p_na_n + \lambda(R(a_1, a_2, \ldots, a_n) - R_0), \tag{1}$$

where $a_1, a_2, \ldots, a_n$ are the candidate activities that can be used to improve the safety, λ is the Lagrange multiplier, R_0 is the achievable risk goal,

$$R = R(a_1, a_2, \ldots, a_n). \tag{2}$$

represents the risk level achieved when the activities $a_1, a_2, \ldots, a_n$ are selected and executed;

$$C = C(p_1a_1, p_2a_2, \ldots, p_na_n) = \sum_{i=1}^{n} p_ia_i, \tag{3}$$

where C is the cost of performing activities $a_1, a_2, \ldots, a_n$; p_i is the price paid for the activity a_i.

The necessary conditions for an optimal solution to L can be derived as:

$$\frac{\partial L}{\partial a_1} = \frac{\partial C}{\partial a_1} + \lambda \frac{\partial R}{\partial a_1} = 0 \tag{4}$$

$$\frac{\partial L}{\partial a_2} = \frac{\partial C}{\partial a_2} + \lambda \frac{\partial R}{\partial a_2} = 0 \tag{5}$$

$$\cdots$$

$$\frac{\partial L}{\partial a_n} = \frac{\partial C}{\partial a_n} + \lambda \frac{\partial R}{\partial a_n} = 0 \tag{6}$$

$$\frac{\partial L}{\partial \lambda} = (R(a_1, a_2, \ldots, a_n) - R_0) = 0. \tag{7}$$

From Eq. (4), the optimal resource allocation for the activity a_1 occurs at the point when

$$\frac{\partial C}{\partial a_1} = -\lambda \frac{\partial R}{\partial a_1}. \tag{8}$$

The same results can be derived for the activities: $a_2, \ldots, a_n$. The overall optimal resource allocation condition can be summarized as:

$$\sum_{i=1}^{n} \frac{\partial C}{\partial a_i} = -\lambda \sum_{i=1}^{n} \frac{\partial R}{\partial a_i}. \tag{9}$$

From Eqs. (8) and (9), one can obtain

$$\left[\frac{\partial C}{\partial a_i} \Big/ \sum_{i=1}^{n} \frac{\partial C}{\partial a_i}\right]\left[\frac{\partial R}{\partial a_i} \Big/ \sum_{i=1}^{n} \frac{\partial R}{\partial a_i}\right]^{-1} = 1. \tag{10}$$

It can be concluded that the overall optimal resource allocation occurs at the point where the relative change in the marginal cost over the relative change in the marginal risk equals unity. Characteristics of software development and the QA process for digital I&C systems meet these conditions. It is therefore possible for risk-informed regulation to be applied to digital I&C regulation for more efficient resource utilization.

2. Experience from Several Countries

Several countries around the world have used PSA for NPP regulation. Nuclear power in Canada is regulated by the Canadian Nuclear Safety Commission (CNSC) (formally the Atomic Energy Control Board (AECB)). Canadian NPP safety regulations and licensing practice in existence since the 1950s have evolved over the past few decades. The AECB issued a draft regulatory guide in 1998 entitled Safety Analysis of CANDU Nuclear Power Plants (C-6 Revision 1) that can be found from the CNSC website http : //www.nuclearsafety.gc.ca/eng/licensees/pdf/c006r1%5Fe.pdf. This guide requires that licensees perform PSA for any newly constructed plants.[18]

The Nuclear Regulatory Commission (NRC) in the U.S. has a long history in the development and application of PSA. The Reactor Safety Study (RSS) made it evident that the probabilistic methodology had a large potential to improve the regulation of NPPs. However, general acceptance of this methodology was obscured by political issues.[19] The Three Mile Island incident in 1979 provided some indirect validation of RSS. The risk-informed approach to reactor safety and regulation has been increasingly accepted since that incident. The NRC issued a policy statement in 1995 on the use of PSA methods in regulatory activities.[43] This policy statement has been implemented in a series of Regulatory Guides shown in Refs. 33) and 44–47).

The approach to NPP safety in France has long been based on conventional deterministic techniques and well known defense in-depth principles. In addition to this approach

two standardized nuclear power plant designs (900 and 1,300 MW) were studied and assessed using PSA methods.[48,49] A Non-Full-Power PSA was performed[50] as a follow-up study to these two PSAs. A PSA has also been carried out for the European Pressurized Water Reactor (EPR).[51]

The Nuclear Safety Bureau (NSB) in Australia regulates the safety of nuclear plants operated by the Australian Nuclear Science and Technology Organization (ANSTO). The safety assessment policy treats risk from accidents both deterministically and probabilistically. A PSA is considered to be complementary to a deterministic assessment, and PSA analysis results are key supporting documents in a safety assessment.

VI. Conclusions

An overview of applying PSA to I&C systems in NPPs is presented in this paper. The importance of I&C systems in NPPs in a deregulated electricity market is emphasized and the challenges introduced by digital technologies are presented. It is clear that PSA plays an important role in managing various aspects of I&C systems. The basic concepts and methodology of PSA are introduced. The challenges in applying PSA for I&C systems are pointed out. Despite these challenges, the theoretical analysis and industry experience have demonstrated that PSA is a promising tool with a lot to offer. PSA application in allocating resources for I&C systems, determining the surveillance testing strategies, and designing I&C systems are discussed. Risk-informed regulation is also considered.

Acknowledgments

The authors would like to express their gratitude to the editor and reviewers for their constructive comments.

References

1) J. D. Shiffer, "Issues for nuclear plants in a deregulated electricity supply industry," *Nucl. Energy*, **38**[4], 259 (1999).
2) L. Philipson, H. L. Willis, *Understanding Electric Utilities and De-regulation*, M. Dekker, New York, 173 (1999).
3) J. Naser, R. Torok, S. Ramesh, "Modernizing and maintaining instrumentation and control systems to increase the competitiveness of nuclear power plants in a deregulated environment," *The Third American Nuclear Society International Topical Meeting on NPIC&HMIT*, Washington, D.C., Nov. 13–17, 2000, (2000).
4) R. N. Kubik, *Probabilistic Risk Assessment in the Design of Instrument and Control Systems*, IAEA-SM-265, 687 (1999).
5) K. Christian, "On the use of probabilistic and deterministic methods in risk analysis," *J. Loss Prevention Process Ind.*, **12**, 399 (1999).
6) K. N. Fleming, *Regulatory Enhancements Through Application of Probabilistic Safety Assessment Technology and Insights*, Atomic Energy Control Board, Microfiche, Toronto, Ont., (1999).
7) F. R. Farmer, "Sitting criteria—A new approach," *Symp. on the Containment and Sitting of Nuclear Power Reactors*, International Atomic Energy Agency, Vienna, Austria, (1967).
8) I. B. Wall, "Probabilistic assessment of risk for reactor design and sitting," *Trans. Am. Nucl. Soc.*, **12**, 1 (1969).
9) H. J. Otway, R.C. Erdmann, "Reactor sitting and design from a risk viewpoint," *Nucl. Eng. Des.*, **3**, 365 (1970).
10) R. M. Lepp, L. M. Watkins, *Control and Instrumentation Systems for the 600 MWe CANDU PHW Nuclear Power Plants*, AECL-7519, Atomic Energy of Canada Limited, Chalk River Nuclear Laboratories, Ontario, (1982).
11) R. P. Ornellas, R. S. Gross, "Strategies for instrumentation and control upgrades," *Nuclear Science Symp. and Medical Imaging Conf., IEEE Conference Record*, Vol. 3, Oct. 30–Nov. 5, 1994, 1047 (1994).
12) R. T. Fink, J. O. Betlack, R. C. Torok, "Application of guidelines on digital I&C; upgrades," *Nuclear Science Symp. and Medical Imaging Conf., IEEE Conference Record*, Vol. 3, Oct. 30–Nov. 5, 1994, 1063, (1994).
13) R. C. Carruth, W. G. Sotos, "Design concepts for the reactor protection and control process instrumentation digital upgrade project at the Donald C. Cook nuclear plant units 1 and 2," *IEEE Trans. Nucl. Sci.*, **43**[3], 1899 (1996).
14) B. Gan, J. H. Brendlen, "Nuclear power plant digital instrumentation and control modifications," *Nuclear Science Symp. and Medical Imaging Conf., IEEE Conference Record*, Vol. 2, Oct. 25–31, 1992, 730, (1992).
15) National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, National Academy Press, Washington, D.C., (1997).
16) P. V. Varde, D. Y. Lee, J. B. Han, "Reliability modeling of digital safety systems of nuclear power plant," *11th Int. Conf. on Nuclear Engineering*, Japan, April 20–23, 2003, (2003).
17) H. Kumamoto, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, IEEE Press, New York, 2nd ed., (1996).
18) R. R. Fullwood, *Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications*, Pergamon Press, Toronto, (1988).
19) M. G. Stewart, *Probabilistic Risk Assessment of Engineering Systems*, Chapman & Hall, London, UK, (1997).
20) N. J. Bahr, *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor & Francis, Washington D.C., (1997).
21) C. J. Garrett, G. E. Apostolakis, "Context in the risk assessment of digital systems," *Risk Anal.*, **19**[1], 23 (1999).
22) M. Borst, H. Schoonakker, "An overview of PSA importance measures," *Reliab. Eng. Syst. Saf.*, **72**, 241 (2001).
23) Y. Zeng, P. Webster, P. Hessel, "Probabilistic safety assessment in Canada," *Reliab. Eng. Syst. Saf.*, **62**, 33 (1998).
24) I. B. Wall, J. J. Haugh, *et al.*, "Recent application of PSA for managing nuclear power plant safety," *Prog. Nucl. Energy*, **39**, 367 (2001).
25) L. Lederman, F. Niehaus, B. Tomic, "Probabilistic safety assessment past, present and future: An IAEA perspective," *Nucl. Eng. Des.*, **160**, 273 (1996).
26) R. F. Cameron, A. Willers, "Use of risk assessment in the nuclear industry with specific reference to the Australian situation," *Reliab. Eng. Syst. Saf.*, **74**, 275 (2001).
27) H. G. Kang, T. Sung, "An analysis of safety-critical digital systems for risk-informed design," *Reliab. Eng. Syst. Saf.*, **78**, 307 (2002).
28) R. I. Freeman, G. R. Moir, "What is living PSA?," *Nucl. Energy*, **32**[6], 355 (1993).
29) P. Kafka, "Living PSA-risk monitoring—Current use and developments," *Nucl. Eng. Des.*, **175**[3], 197 (1997).

30) L. J. Perryman, N. A. S. Foster, *et al.*, ''Real time risk assessment of operational events,'' *Nucl. Eng. Des.*, **160**[1–2], 203 (1996).
31) K. Gotz, T. Richter, ''Optimization of power plant operation—Application of plant specific PSA,'' *Nucl. Eng.*, **43**[3], 71 (2002).
32) M. V. Bonaca, *Living Probabilistic Safety Assessment for Nuclear Power Plant Management*, OECD Nuclear Energy Agency. (1992).
33) C. J. Garrett, G. E. Apostolakis, ''Automated hazard analysis of digital systems,'' *Reliab. Eng. Syst. Saf.*, **77**, 1 (2002).
34) H. D. Fischer, ''Conservative availability analyses including dependent failures in redundant I&C-systems with recurrent tests,'' *Nucl. Eng. Des.*, **222**, 79 (2003).
35) J. J. Lisboa, ''Defense-in-depth concept for nuclear power plant normal plant control systems using probability analysis,'' *IEEE Trans. Nucl. Sci.*, **36**[1], 1284 (1989).
36) S. K. Khobare, S. V. Shrikhande, *et al.*, ''Reliability analysis of microcomputer circuit modules and computer based control systems important to safety of nuclear power plants,'' *Reliab. Eng. Syst. Saf.*, **59**, 253 (1998).
37) M. Čepin, ''Optimization of safety equipment outages improves safety,'' *Reliab. Eng. Syst. Saf.*, **77**, 71 (2002).
38) NRC, *An Approach for Plant-specific, Risk-informed Decision Making: Graded Quality Assurance*. NRC, Regulatory Guide 1.176, (1998).
39) S. Yih, C. F. Fan, ''A GQA resource allocation approach for digital I&C project,'' *Int. Topical Meeting on Probabilistic Safety Assessment*, Detroit, MI, Oct. 6–9, 2002, 196 (2002).
40) G. E. Schinzel, T. J. Riccio, *et al.*, ''Considerations for adopting risk informed techniques for electrical surveillance testing (future revision of IEEE 338),'' *Int. Topical Meeting on Probabilistic Safety Assessment*, Detroit, MI, Oct. 6–9, 2002, 618 (2002).
41) R. Parmar, B. Hryciw, ''Optimization of test intervals for dormant components,'' *Int. Topical Meeting on Probabilistic Safety Assessment*, Detroit, MI, Oct. 6–9, 2002, 603 (2002).
42) S. Yih, D. S. Lee, *et al.*, ''The applicability of applying risk informed performance based approach to digital I&C regulation,'' *The Third American Nuclear Society Int. Topical Meeting on NPIC&HMIT*, Washington, D.C., Nov. 13–17, 2000, (2000).
43) *Use of PRA Methods in Nuclear Regulatory Activities; Policy Statement*, Federal Register 60, 42622, (1995).
44) NRC, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, NRC Regulatory Guide 1.174, (1998).
45) NRC, *An Approach for Plant-Specific, Risk-Informed, Decision Making: Technical Specifications*, NRC Regulatory Guide 1.177, (1998).
46) NRC, *An Approach for Plant-Specific, Risk-Informed, Decision Making: Inservice Testing*, NRC Regulatory Guide 1.175, (1998).
47) NRC, *An Approach for Plant-Specific, Risk-Informed, Decision Making: Inservice Inspection of Piping*, NRC (for trial use) Regulatory Guide 1.178, (1998).
48) IPSN, *EPS 900 A Probabilistic Safety Assessment of Standard French 900 MWe Pressurized Water Reactor Main Report*, April, (1990).
49) EDF, *EPS 1300 Probabilistic Safety Assessment of Reactor Unit 3 in the Paluel Nuclear Center (1330 MWe)*, EDF Overall, May 31, 1990, (1990).
50) IPSN, *PSA for Reactor Shut-Down States*, IPSN, (1995).
51) Nuclear Engineering International, *EPR Project Status Report*. (1997).