# DETERMINATION OF THE OPTIMAL SURVEILLANCE TEST INTERVAL FOR SHUTDOWN SYSTEM NUMBER 1

Sungwhan Cho[1)] and Jin Jiang[2)]
Department of Electrical and Computer Engineering, The University of Western Ontario
London, Ontario, Canada, N6A 5B9
Phone 1-519-661-2111 ext 81271[1)], 88320[2)], Fax 1-519-850-2436
E-mails: scho25@uwo.ca [1)] jjiang@eng.uwo.ca [2)]

**Keywords:** Surveillance Test Interval, SDS1, Markov Process, Core Damage Probability

## Abstract

Two probabilistic models focusing on the channel surveillance tests of the shutdown system number 1 (SDS1) in a CANDU nuclear power plant are proposed in this paper. The first one is a state transition model which is used to study the effect of surveillance test intervals on the unavailability and the probability of spurious trips. The second model is developed to examine the effect of the test interval on the core damage probability caused by both spurious trips and unavailable channels in the SDS1. The calculated core damage probabilities have clearly shown that there is an optimal test interval to provide the minimal probability of core damage. Therefore, the results are of significant importance in practice.

## 1 INTRODUCTION

One of the unique properties of any safety shutdown system (SDS) is that the system usually remains dormant, until it is called upon in an emergency. To ensure their availability, surveillance tests are often carried out to reveal latent failures. In case of nuclear power plants, such regular tests are enforced by regulatory bodies. For example, in Canadian nuclear power plants, the Canadian Nuclear Safety Commission (CNSC) has set the availability target for such systems to have a reliability level of $10^{-3}$ years/year [1][2]. To show compliance, the safety systems are tested regularly. The interval between two consequent tests, known as the surveillance test interval (STI) needs to be determined.

It is important to note that shorter and more frequent tests do not always translate into higher availability because the test itself will reduce the robustness of the 2-out-of-3 decisionmaking process, and could trigger the shutdown system by mistake to actually reduce the availability. In practice, to meet CNSC demand on availability in the presence of uncertainties in the data, higher failure rates are often assumed in calculating the test interval, which usually result in more conservative (shorter) test intervals. Since too frequent testing can be an economic burden to the operational personnel, may even lead to unnecessary reactor shutdown, and can contribute to shortening lifetimes of some system components. Therefore, it is highly desirable to determine the 'optimal' test interval to meet the availability specification under the given failure rates of the related system components.

To increase the immunity of the safety system against common-mode failures and to allow on line test, most of the shutdown systems in a nuclear power plant are designed with multi channel signal paths followed by a voting process. However, during the on-line test of a channel,, the multi-channel voting logic becomes degraded status to spurious operation. Such spurious operations not only cause unnecessary economical loss, but also increase the probability of core damage frequency (CDF) by stressing the plant electrical distribution system which is required for removal of decay heat during the plant shutdown. Therefore, it is very important to determine the desirable test interval.

In the process of determining the STIs, the target reliability should be established based on the 1) frequency of demand; 2) consequence of failures; and 3) risk [3]. The minimum requirements are often set in the regulatory document, for example, in CANDU NPPs, these values are provided in [1][2]. After the numerical goals are specified, the modeling techniques should be used for quantitative analysis, and industry standards and guideline [3][4][5][6][7][8][9] should be followed.

One of the important considerations in designing the routine tests is to ensure that the combined unavailability of the primary and the backup protection system for a process failure listed in the regulatory documents [1][2] is within the unavailability target of $10^{-3}$ years /year. The unavailability allocation for components in SDS1 is listed in Table 1. The allocated unavailability depends on the reliability of the components and the failure rates of the routine test. The unavailability for the detectors, the multiple channels, and the shutoff rods are designed to achieve the target unavailability by assigning the proper test frequency for each component.

The formulas for calculating the unavailability of the SDS1 are also listed in Table 1 with the target primary and backup trip channel unavailability. These formulas can be derived and found in many reliability engineering books [10][11].

Table 1: Routine Test Design for the SDS1

| Components | Trip Parameter Sensors(2/3) | | Channel Logic (2/3) | | Shutoff Rods (26/28) |
|---|---|---|---|---|---|
| | Primary | Backup | Primary | Backup | |
| Unavailability Allocation | $3\times10^{-4}$ | $3\times10^{-4}$ | $0.5\times10^{-4}$ | $0.5\times10^{-4}$ | $1\times10^{-4}$ |
| Failure Rate | $\lambda_{S1}$ | $\lambda_{S2}$ | $\lambda_{C1}$ | $\lambda_{C2}$ | $\lambda_R$ |
| Test Frequency | $\tau_{S1}$ | $\tau_{S2}$ | $\tau_{C1}$ | $\tau_{C2}$ | $\tau_R$ |
| One Component Unavailability | $\frac{\lambda_{S1}\tau_{S1}}{2} \equiv p_{S1}$ | $\frac{\lambda_{S2}\tau_{S2}}{2} \equiv p_{S2}$ | $\frac{\lambda_{C1}\tau_{C1}}{2} \equiv p_{C1}$ | $\frac{\lambda_{C2}\tau_{C2}}{2} \equiv p_{C2}$ | $\frac{\lambda_R\tau_R}{2} \equiv p_R$ |
| M out of N Component Unavailability | $\sum_{k=2}^{3} P(E_k)$ | $\sum_{k=2}^{3} P(E_k)$ | $\sum_{k=2}^{3} P(E_k)$ | $\sum_{k=2}^{3} P(E_k)$ | $\sum_{k=3}^{28} P(E_k)$ |
| | $P(E_k) = \frac{n!}{(n-k)!k!}(1-p)^{n-k} p^k$, $k=0,1,2\ldots n$ | | | | |

Various efforts have been made to analyze the reliability of shutdown systems through the selection of optimal surveillance test intervals. Some of the results are available in the literature [12][13][14]. Even though these studies share the similar view that the STI is closely related to spurious reactor trips and such trips also have the potential risk leading to core damages, however, few studies can be found for determining the STI of shutdown systems in CANDU NPP that considers the core damage probability (CDP) as the STI changes.

The objective of this paper is to develop analytical techniques which can quantify the effect of STI on the spurious trip probability ($P_{SP}$) and the unavailability of the trip channel ($U_{CH}$) in the SDSs. The results can be directly used to determine the optimal STI for SDSs in CANDU NPPs. Two scenarios leading to core damage from the surveillance test have been considered in this paper. The first one is related to unavailable SDSs due to a process failure and the second is through the spurious reactor trip which challenges the class IV power in CANDU electrical distribution system.

# 2 MODELS FOR DETERMINING THE OPTIMAL STI FOR SDS1

Selection of STIs in SDSs involves the properties of sensors, channel logics, and shutoff rods. This paper focuses only on the channel logic test. Two models are developed. One is a state transition model which is capable of handling multiple states as shown in the industry standards and the studies [15][16][17][18][19][20]. The model relates the variation of STI to the unavailability of trip channel ($U_{CH}$) and the spurious trip probability ($P_{SP}$). The other model calculates the core damage probabilities as a function of the spurious trip probability ($P_{SP}$) and the unavailability of trip channel ($U_{CH}$).

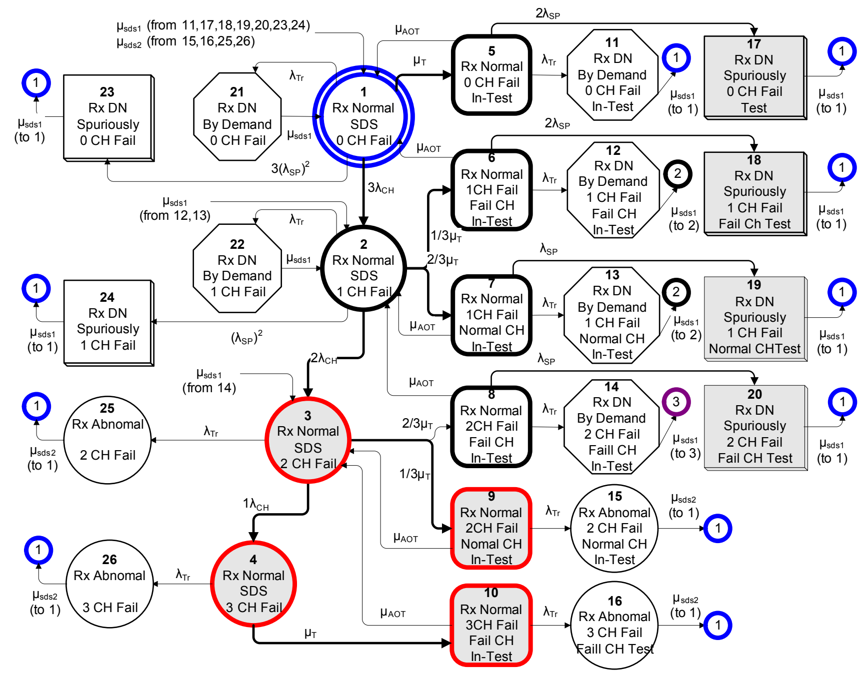


Fig. 1: State Transition Diagram of the STI Model for SDS1

## 2.1 *State Transition Model of the STI for SDS1*

The state transition diagram as illustrated in Fig. 1 reflects all the events that can change the states of the reactor and the trip channels of the SDS1. Other state transitions, such as the marginal shutoff rod tests, the detector calibrations, have not included in this diagram for simplicity. The full state space involved 26 variables. The interested readers can refer to [21] for detail.

Let $P = [P_1 \ \ P_2 \ \ ...... \ \ P_{26}]$ represents the steady state solution vector of the 26 states and $V$ represents the state transition matrix, and then the steady state expression of the model can be written as $PV = V$ as in Ref. [10]. By solving this equation, the unavailability of the trip channel can be obtained by

$$U_{CH} = P_3 + P_4 + P_9 + P_{10} \tag{2-1}$$

The probability of reactor abnormal condition is

$$P_{ABN} = P_{15} + P_{16} + P_{25} + P_{26} \tag{2-2}$$

Similarly, the spurious trip probability can also be obtained as

$$P_{SP} = P_{17} + P_{18} + P_{19} + P_{20} \tag{2-3}$$

## *2.2 Loss of Class IV Power Supply on a Plant Trip*

A simplified power distribution scheme showing only Class IV power in a CANDU NPP is illustrated in Fig. 2. Once spurious reactor trip signals are registered, the SDS1 will trip the reactor and the turbine generator trip follows. Consequently, the unit service transformer (UST) will lose its power and the "*13.8kV parallel bus transfer*" from the system service transformer (SST) will automatically be initiated. If the transfer fails and the power from the SST fails, the loss of Class IV power event occurs. The reliability of Class IV power depends on the reliability of 13.8kV Odd bus only once the plant is tripped. The fault tree for the unavailability of the Class IV power on a plant trip is shown in Fig. 3. As shown, the top event, i.e. the 5314-BUA loss of power, occurs if the bus itself fails or the grid supplying power to the plant fails.

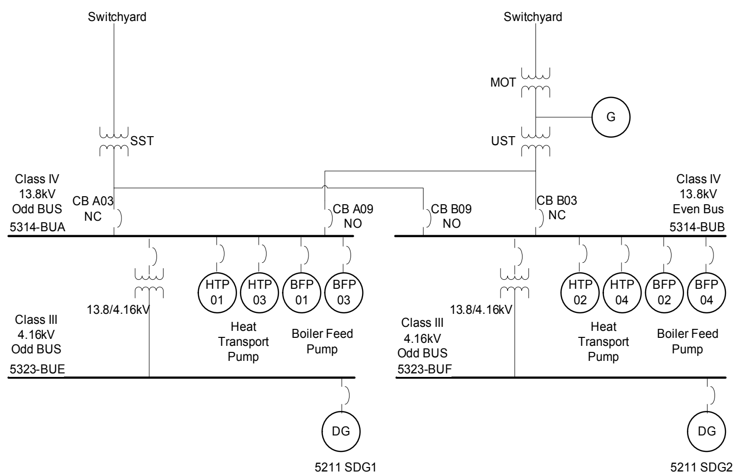


Fig. 2: Power Distribution System in CANDU

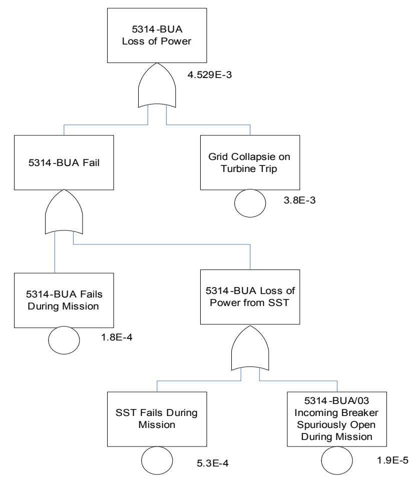


Fig. 3: 13.8kV Odd Bus Fault Tree

The data from the operating experience can be used to estimate the probability of grid disturbance on the plant trip. Table 2 shows the probability of grid disturbance on plant trip reported by Martinez et al. [22]. In this analysis, the probability of loss of Class IV on a spurious trip ($CP_{LOCL4}$) is chosen as $4.529\times10^{-3}$. Failure of Class IV is a major event, as it may lead to rapid increase in fuel temperature, which can cause failure in the fuel channel and fuel damage. The conditional core damage probability (CCDP) on a loss of Class IV power ($CCDP_{LOCL4}$) can be derived based on CANDU probabilistic safety assessment (PSA) results, which is estimated to be the initiating event frequency (IEF) of $6.6\times10^{-2}$/year and the resulting core damage frequency (CDF) $7.29\times10^{-6}$/year. Then the CCDP for loss of Class IV power ($CCDP_{LOCL4}$) can be calculated to be $1.104\times10^{-4}$ as shown in Table 3.

Table 2: Probability of Loss of Offsite Power (LOOP) for Different Reactor Types

| Type | Number of Trip-LOOP Events | Number of Trips | Grid Disturbance, Failure During Bus Transfer |
|---|---|---|---|
| BWR | 3 | 813 | $3.7\times10^{-3}$ |
| PWR | 7 | 1804 | $3.9\times10^{-3}$ |
| Total | 10 | 2617 | $3.8\times10^{-3}$ |

Table 3: Conditional Core Damage Probability for a Loss of Class IV Event

| IE | I.E.F | CDF | $CCDP_{LOCL4}$ | Reference |
|---|---|---|---|---|
| Loss of Class IV | $6.6\times10^{-2}$/year | $7.29\times10^{-6}$/year | $1.104\times10^{-4}$ | CANDU PSA |

### *2.3 CDP Model of SDS1*

By quantifying the system modeled in Fig. 1 using a time homogeneous Markov process technique as a function of STI, the effect of STI on the spurious trip probability ($P_{\mathrm{SP}}$) and the unavailability of the trip channel ($U_{\mathrm{CH}}$) can be numerically derived. However, the spurious trip probability ($P_{\mathrm{SP}}$) and the unavailability of the trip channel ($U_{\mathrm{CH}}$) do not have the same level of importance as far as the plant safety is concerned so that they cannot be compared directly with each other. The question that CDP calculation tries to answer is 'How many routine tests will provide the most benefit to the plant safety in a given SDS1 system?'

The core damage may occur after a spurious reactor trip if the loss of Class IV power event and the subsequent mitigating system failures also occur at the same time. The CDP caused by a spurious reactor trip during a routine test can be calculated by

$$CDP_{SP} = P_{SP} \times CP_{LOCL4} \times CCDP_{LOCL4} \tag{2-4}$$

where $CDP_{SP}$ is the core damage probability due to the spurious reactor trip, $P_{SP}$ is the probability of the spurious reactor trip during the test, $CP_{LOCL4}$ is the conditional probability of loss of Class IV event given that a reactor is tripped, and $CCDP_{LOCL4}$ is the conditional core damage frequency given a loss of Class IV event.

The core damage may follow a process failure when the failure occurs at the states 3, 4, 9, and 10 at which more than two undetected channel failures exist as shown in Fig. 1. Although the backup trip parameters of SDS1 and the redundant Shutdown System 2 (SDS2) trip parameters are designed for the situations where the primary SDS1 trip parameter is unavailable, the probability of failure in these backup and redundant trip parameters exist at the same time. The CDP due to unavailable channel can be derived as

$$CDP_{UC} = P_{ABN} \times P_{BCU} \times P_{SDS2} \tag{2-5}$$

where $CDP_{UC}$ is the core damage probability for the unavailable channel, $P_{ABN}$ is the probability of reactor abnormal condition challenged by a process failure during the undetected SDS1 channel failure mode. $P_{BCU}$ is the probability of unavailable backup SDS1 trip parameter, and $P_{SDS2}$ is the failure probability of the SDS2.

## 3 ANALYSIS OF THE RESULTS

Ten trip parameters are used in the SDS1 to cope with the possible process failures listed in R-8 [1]. All the trip parameters are under different schedules for the surveillance tests. The analysis results under a high neutron power (HNP) trip channel are presented herein as an illustrative example.

The calculated results of the spurious trip probability ($P_{\mathrm{SP}}$), the unavailability of trip channel ($U_{\mathrm{CH}}$), and the probability of reactor abnormal condition ($P_{ABN}$) are plotted with respect to the test frequency ($\mu_T$) in Fig. 4. The probabilities are obtained by varying the test frequency ($\mu_T$) from 1 test/year to 312 tests/year. The test duration is assumed to be one hour ($\mu_{AOT}$). As it can be seen from Fig. 4, the unavailability of the trip channel ($U_{\mathrm{CH}}$) decreases while the spurious trip probability ($P_{\mathrm{SP}}$) increases as the test frequency ($\mu_T$) increases. The results also show that the unavailability of the trip channel ($U_{\mathrm{CH}}$) is $4.93\times10^{-5}$ at the test frequency of 72 tests/year. It can be assumed that more than 72 tests/year is required to satisfy the unavailability allocation for the channel logic of $5\times10^{-5}$ as shown in Table 1. The probability of reactor abnormal condition ($P_{ABN}$) decreases as the test frequency increases.

The core damage probabilities for unavailable channel ($CDP_{UC}$) are illustrated in Fig. 5 as a function of the test frequency ($\mu_T$). The CDP profiles are drawn with the assumption of the failure probability of SDS1 backup trip parameters for $4.5\times10^{-4}$, $2.25\times10^{-4}$, and $1.125\times10^{-4}$ respectively and the SDS2 failure probability of $1.0\times10^{-3}$. The results show that the CDP decreases with the increased test frequency and the increased reliability of the system based on the backup trip parameters.

The core damage probabilities caused by the spurious reactor trip ($CDP_{SP}$) are shown in Fig. 6 as a function of the test frequency ($\mu_T$). Three cases of test duration ($\mu_{AOT}$) are also considered. The results show that the CDPs increases with the increased test frequency and the increased test duration ($\mu_{AOT}$).

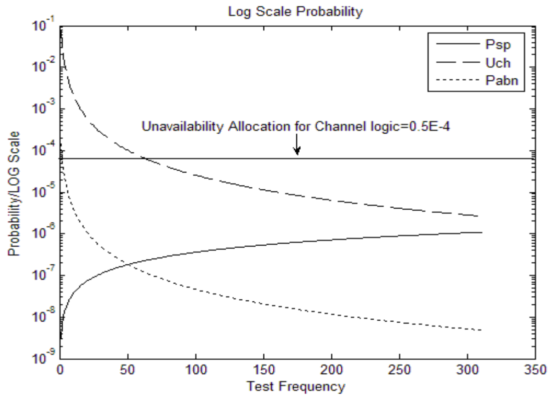


Fig. 4 : $P_{SP}$, $U_{CH}$, $P_{ABN}$

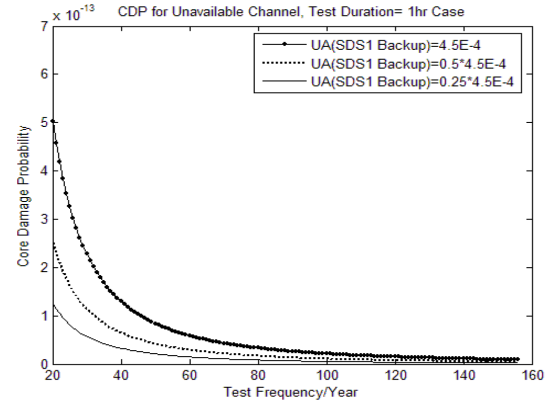


Fig. 5: $CDP_{UC}$

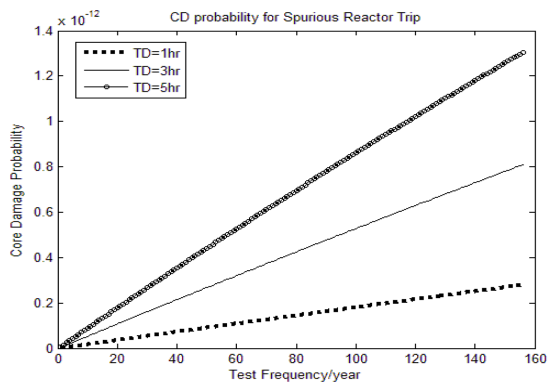


Fig. 6: $CDP_{SP}$

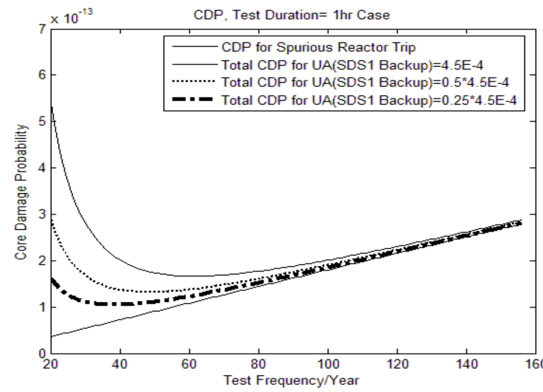


Fig. 7: Total CDP for TD=1hr

The total CDPs of the core damage probability for unavailable channel ($CDP_{UC}$) and the core damage probability caused by a spurious reactor trip ($CDP_{SP}$) for different test duration are shown in Fig. 7, Fig. 8 and Fig. 9, respectively. Each figure contains three cases of CDPs for different failure probability in backup trip of SDS1 ($P_{BCU}$). For the sensitivity study of SDS1, different cases for SDS1 backup trip unavailability are calculated. Based on the unavailability allocation design for SDS1 components shown in Table 1, the unavailability of the basic backup trip function of SDS1 is assumed to be $4.5\times10^{-4}$, which is the summation of the unavailability of backup trip parameter sensors, channel logic, and shutoff rods. For test duration 1 hour and the assumption of the basic backup trip parameter unavailability of SDS1 of $4.5\times10^{-4}$, 61 tests/year provides the lowest total CDP.

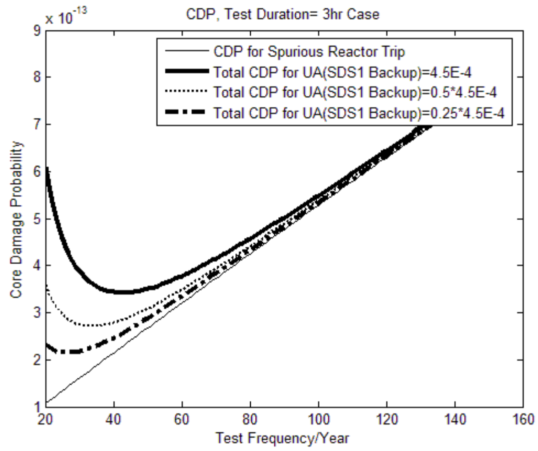


Fig. 8: Total CDP for TD=3hr

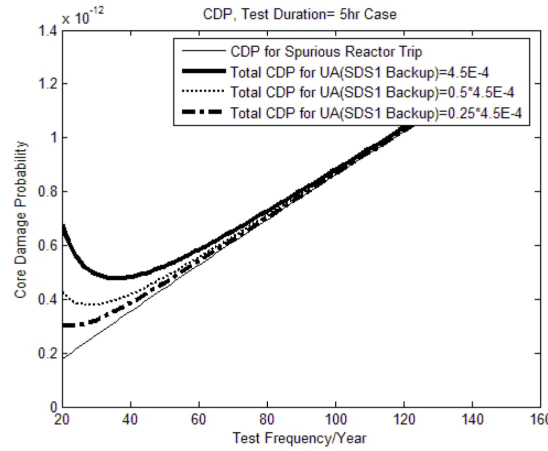


Fig. 9: Total CDP for TD=5hr

## 4 CONCLUSIONS

The relationships between the surveillance test interval and the core damage probability caused by spurious trips have been developed with the consideration of the loss of Class IV power failure. The effect of the surveillance test interval on the core damage probability has been studied based on two developed models. They are: 1) the state transition model for quantification of the effect of the surveillance test interval on the unavailability and the spurious trip probability; and 2) the core damage probability model for quantification of the effect of the surveillance test interval on the core damage probability. Through analysis studies, the optimal surveillance test interval which gives the lowest core damage probability can be determined.

The results of the core damage probability for a HNP channel clearly show that reduction of the surveillance test interval does not always bring reduced risk in terms of the core damage probability. It can be concluded that there exists an optimal value for the surveillance test interval at which the probability of core damage is minimized. The core damage probabilities, the main outcome of the models proposed in this paper can provide the necessary input parameters for more detailed probabilistic safety assessment studies.

## ACKNOWLEDGMENT

The authors would like to acknowledge the financial support from NSERC and UNENE as well as the technical supports from the UNENE industrial partners for the work reported in this paper.

## REFERENCES

[1] CNSC, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants," CNSC Regulatory Document R-8, February 1991.

[2] CNSC, "The use of two shutdown systems in reactors," CNSC Regulatory Document R-10, 1977.

[3] American National Standard, IEEE Guide for General Principle of Reliability Analysis of Nuclear Power Generation Station Safety Systems, ANSI/IEEE Std 352-1987.

[4] CAN/CSA-N285.4-94 (R1999), Periodic Inspection of CANDU Nuclear Power Plant Components.

[5] CAN/CSA-N290.1-80 (R2002), Requirements for the Shutdown Systems of CANDU Nuclear Power Plants.

[6] American National Standard, IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, ANSI/IEEE Std 338-1987.

[7] American National Standard, IEEE Standard Application of the Single-Failure Criteria to Nuclear Power Generating Station Safety Systems, ANSI/IEEE Std 379-1988.

[8] American National Standard, IEEE Guide for Safety Systems for Nuclear Power Generating Stations, ANSI/IEEE Std 352-1987.

[9] American National Standard, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, ANSI/IEEE Std 603-1998.

[10] R. Billinton, R. N. Allan, "Reliability Evaluation of Engineering System," Plenum Press, 1983.

[11] M. Rausand, A. Hoyland, "System Reliability Theory Models, Statistical Methods, and Applications-Second Edition", Wiley-Interscience, 2004.

[12] Y. D. Lukic, "Nuclear Power Plant Core-Protection-Calculator Reliability Analysis," Proceedings annual reliability and maintainability symposium, pp. 116-120, 1996.

[13] H.P.Chou, Y.H.Wang, Y.S. Wei, and T.J. Lin, "Evaluation of Surveillance Test Interval from Risk Viewpoint," IEEE transactions on nuclear science, Vol. 45, No. 3, pp. 1009-1013, June 1998.

[14] I. A. Papazoglow, "Risk-Informed Assessment of the Technical Specifications of PWR RPS instrumentation," Nuclear Technology, Vol. 130, pp. 329-350, June 2000.

[15] D. Dyer, "Unification of Reliability/ Availability/ Repairability Models for Markov Systems," IEEE Transactions on reliability, Vol. 38, No. 2, pp. 246-252, June 1989.

[16] P.M. Anderson, S.K. Agarwal, "An Improved Model for Protective-System Reliability," IEEE transactions on reliability, Vol, 41, No. 3, pp. 422-426, September 1992.

[17] P.M. Anderson, G.M. Chintaluri, S.M. Magbuhat, R.F. Ghajar, "An Improved Reliability Model for Redundant Protective Systems- Markov Models," IEEE transactions on Power Systems, Vol, 12, No. 2, pp. 573-578, May 1997.

[18] R. Billington, T.S. Sidhu "Determination of the Optimum Routine Test and Self-Checking Intervals in Protective Relaying Using a Reliability Model," IEEE transactions on Power Systems, Vol, 17, No. 3, pp. 663-669, August 2002.

[19] A. Birolini, "Reliability Engineering- Theory and Practice, Fourth Edition," Springer, 2003.

[20] W.E. Boyce, R.C. Diprima, "Elementary Differential Equations and Boundary Value Problems, Sixth Edition," John Wiley & Sons Inc., 1997.

[21] S. W. Cho, "Design and Analysis of Surveillance Test Intervals for Safety Systems," MESc. Thesis, The University of Western Ontario, June 2006.

[22] M. Guridi et al., Brookhaven National Laboratory, "LOCA with Delayed Loss of Off-Site Power.", Nuclear Technology, vol. 131, page 297-318, April 2000.