Third International Conference on
Radiation Sciences and Applications
12 – 16 November 2012/ Hurghada, Egypt

Safety Analysis for Power Reactor Protection System

E. A. Eisawy and Hany Sallam

ABSTRACT

The main function of a Reactor Protection System (RPS) is to safely shutdown the reactor and prevents the release of radioactive materials. The purpose of this paper is to present a technique and its application for used in the analysis of safety system of the Nuclear Power Plant (NPP). A more advanced technique has been presented to accurately study such problems as the plant availability assessments and Technical Specifications evaluations that are becoming increasingly important. The paper provides the Markov model for the Reactor Protection System of the NPP and presents results of model evaluations for two testing policies in technical specifications. The quantification of the Markov model provides the probability values that the system will occupy each of the possible states as a function of time.

1. INTRODUCTION

The RPS is composed of systems that are designed to immediately terminate the nuclear reaction. While the reactor is operating, the nuclear reaction continues to produce heat and radiation. By breaking the chain reaction, the source of heat can be eliminated, and other systems can then be used to continue to remove decay heat from the core.

Safety is one of the most important concerns in the design and operation of NPPs. Quantitative safety analysis is mainly performed in the framework of probabilistic safety assessment (PSA) [(1)]. The analysis framework of the safety of digital systems in the context of the PSA was examined [(2)]. It quantitatively presents the results of a case study of the safety of digital systems. The case study was performed for the Digital Reactor Protection System (DRPS) of NPPs. From the viewpoint of PSA [(3)], there are some important unresolved issues in digital systems' safety analysis which are complex and correlated.

An analysis was performed of the safety-related performance of the RPS at U.S. Westinghouse commercial reactors. RPS operational data were collected from licensee Event Reports [(4)]. The analysis focused on the ability of

the RPS to automatically shut down the reactor given a plant upset condition requiring a reactor trip while the plant is at full power. A strategy and relating activities of a Software Safety Analysis (SSA) are presented by Function Blocks (FBs) [5].

An in-depth review of the U.S nuclear operating experience with the first generation of DRPS was summarized [6]. Based upon this review of digital system operating experience, a series of risk assessment calculations were performed to evaluate the safety significance of the observed failure events. The methodological difficulties met in the safety qualification of the RPS are pointed out [7]. If any unrecognized failure happens in the RPS, then the RPS can not shut down the reactor on demand. This case will not satisfy the reactor safety requirement, because the undetected failure may disturb the proper RPS operation [8]. As a result, the quantitative safety of a number power plant is defined as the probability that the system operates correctly or fails in a safe manner [9].

In this paper a Markov model approach is employed to simulate all the RPS states and the stochastic behavior of the system as a function of time. The model calculates the probabilities of various plant damage states the sum of which provides the probability of core damage. The paper also presents some results of its applications to the RPS of a NPP.

2. SYSTEM DEFINITION

Before any analysis, it is necessary to define the system being analyzed. The RPS continuously monitors the selected plant safety parameters to assure that the plant safe status is constantly maintained. The RPS automatically initiates reactor protective action whenever the monitored plant parameter reaches a predetermined set point level [8] .

Generally, it is most efficient to consider the system as a collection of replaceable modules or units. The RPS consists of four redundant channels (A, B, C and D) as shown in Figure 1 to satisfy single failure criteria.

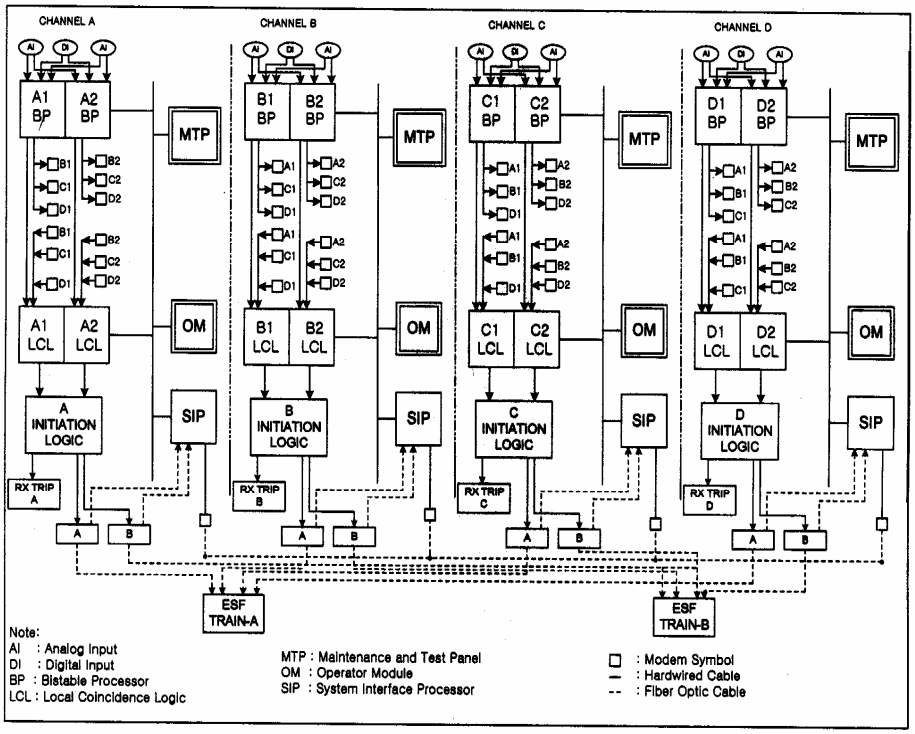

Fig. (1): RPS block diagram

3. MARKOV MODEL

This section describes briefly the Markov model developed for the electrical portion of the RPS (Fig.1). There are four channels and two logic trains. Each functional channel is considered as a super component composed of several basic components in series.

The Markov model describes the system behavior by using the pre-defined system states and the transitions between them [10]. There are some problems, however, in implementing the Markov model. One of them is to build and solve the transition probability matrix, since it is very complex and time-consuming work.

The channel is represented by a five-state component: State 1: is the operating state; State 2: is the failed state; State 3: is the tripped state; State 4: is the bypass state related to state 1; State 5: is the bypass state related to state 2. Whenever the allowable bypass time is small compared to the mean time of channel failure, the two test states (4 and 5) can be omitted by assuming that the transitions in and out of states 4 and 5 occur instantaneously at the time of testing and with the following probabilities as shown in Figure 2.

In this study, exponentially distributed times to test completion were used. This assumption is not, however, a requirement of the model. Any distribution of testing times can be used.

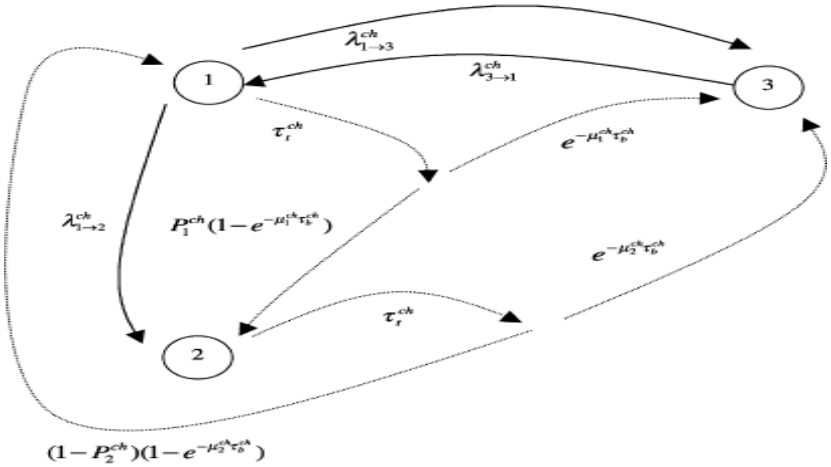

Fig. (2): State transition diagram for channel (Equivalent Markovian Model)

Where:

$1/\mu_1$: Mean duration of test given that analog channel is operable.
$1/\mu_2$: Mean duration of test given that analog channel is failed.
P_1 : Human error probability of failing a channel or a logic train following a test
P_2 : Probability of failing to detect a failure
λ_S : Spurious Scram transition rate.
$1/\mu_*$: Mean time to repair a failed channel.
λ : Failure rate.
τ : Allowable Bypass Time (ABT).
λ_T : Transition rate fallowing a test which takes place every T hours.
T : Testing period.
CH : Channel.

The Six components (4 channels and 2 logic trains) form a system that can be in 729 states. After the system states are generated, the system states have been grouped. The major grouping involves states that imply a spurious scram. If two channels are in the trip state or if one logic train is in the trip state a spurious scram signal is generated because of the 2-out-of-4 and 1-out-of-2 logic, respectively. The scram signal will cause a reactor shutdown that will result in a successful shutdown or in a core damaged state depending on the availability of the decay heat removal function.

The 729 system states can be further grouped into the following nine

groups: 1) RPS Available with No Tripped Channel, 2) RPS Available with One Tripped Channel, 3) RPS Unavailable, 4) Real Scram with No Core Damage, 5) Real Scram with Core Damage, 6) Spurious Scram with No Core Damage, 7) Spurious Scram with Core Damage, 8) ATWS with No Core Damage and 9) ATWS with Core Damage.

The system transitions are graphically depicted, in summary form, in the state transition diagram in Figure 4. If the system is in a state of group 1 it can transit to a state in group 3 if a component fails. The system transits from a state of group 1 to a state of group 2 if an analog channel trips. Transitions from groups 2 and 3 back to group 1 occur whenever a component is repaired. Similar transitions (involving failures and repairs of components) can occur between groups 2 and 3.

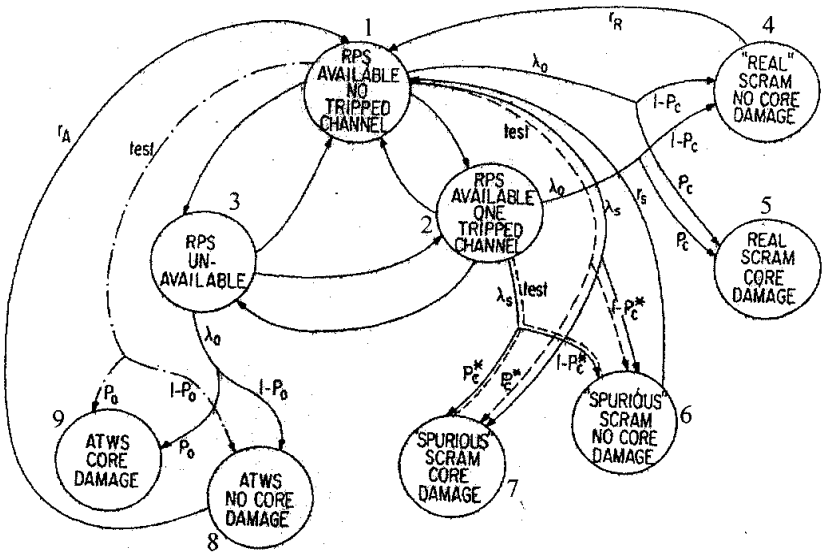

Fig. 3 Generalized state diagram

4. RESULTS OF THE ANALYSIS

A key factor in making a system analysis is the selection of applicable part failure rates. The Markov model described before was quantified using the data given in [10,11] and Table 1. The quantification of the model provides numerical values for two attributes of interest in the evaluation of the Technical Specifications (TS) policies:

1-The Probability of Core Damage per year of reactor operation (CDP)

2-The Average Reactor Downtime per year of reactor operation (ARD)

The quantification of the Markov model provides the probabilities that the system will occupy each of the possible states as a function of time.

Table (1): Data for the model parameters

Parameter	Data
μ_1^{TR}	1 h^{-1}
μ_2^{TR}	1/7 h^{-1}
μ_1^{CH}	1 h^{-1}
μ_2^{CH}	1/7 h^{-1}
λ_o	9.71y^{-1}
$r_s = r_R$	25.6 h
P_c	1.43 (-5)/d
	1.60(-6)/d
P_c^*	5.21(-7)/d
P_o	6.0(-2)/d

Where:

TR : Logic train

r_s : Transition rate from a safe shutdown state following a spurious scram to the operating state

r_R : Transition rate from a safe shutdown state following a real scram to the operating state

λ_o : Frequency of transients

P_c : Conditional probability of core damage given a real scram

P_c^* : Conditional probability of core damage given a spurious scram

P_o : Conditional probability of core damage given an ATWS

5. COMPARISON OF TWO TECHNICAL SPECIFICATION POLICIES

The above two attributes were calculated for two specific TS testing policies summarized in Table 2. A TS policy consists of the period of testing of channels, the period of testing logic trains, the allowable bypass time for channel test and the allowable bypass time for a logic train test. The values of the parameters for the two TS policies are given in the table. In summary, policy 2 extends both the testing periods and the allowable bypass time.

Table (2): Testing schedules

Policy	T^{CH} (Days)	T^{TR} (Days)	τ_0 (Hours)	τ_1 (Hours)
1	30	60	1	1
2	90	180	6	4

Where:

T^{CH}, T^{TR} : Test intervals for channels and logic trains, respectively.

τ_o : Allowable bypass time for an analog channel test.

τ_1 : Allowable bypass time for a logic train test.

The core damage probability as a function of time for policy 1 is given in Figure 4. This core damage probability [$F_{CD}(t)$] consists of three contributors:

1-Probability of core damage as a result of real scram and the subsequent failure of the decay heat removal safety functions [$F_R(t)$].

2-Probability of core damage as a result of a spurious scram and subsequent failure of the decay heat removal safety function [$F_s(t)$].

3-Probability of core damage as a result of an ATWS and subsequent failure to mitigate it [$F_A(t)$].

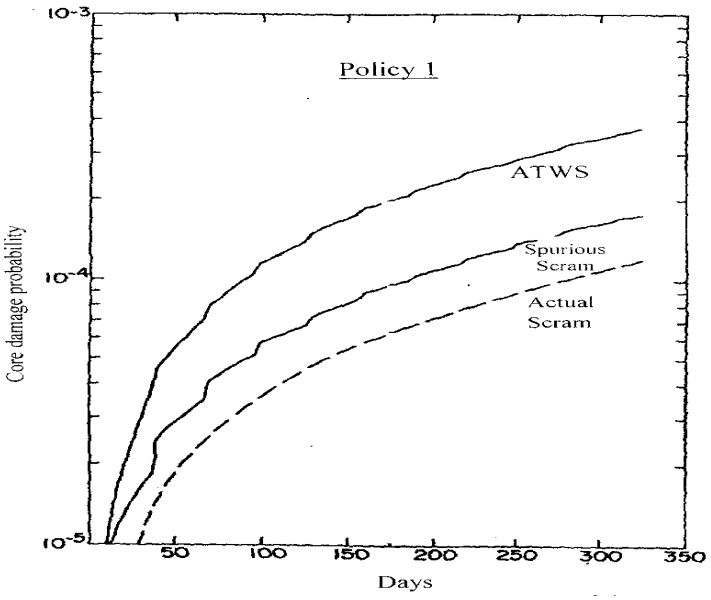

Fig. (4): Probability of core damage as a function of time

The core damage probability as a function of time for policy 2 is given in Figure 5 along with that for policy 1. The probability of core damage as a result of a real scram [$F_R(t)$] is practically the same for the two policies. Policy 2 increases the allowable bypass times and decreases the frequency of testing for both the logic trains and the channels. As a result, the probability of spurious scrams and consequently the probability of core damage from spurious scrams become small. The core damage probability as a result of an ATWS increases for policy 2 because the probability of ATWS increases owing to the increase in the RPS unavailability.

Table 3 summarizes the results of calculation of the two attributes for policy 1 and policy 2.

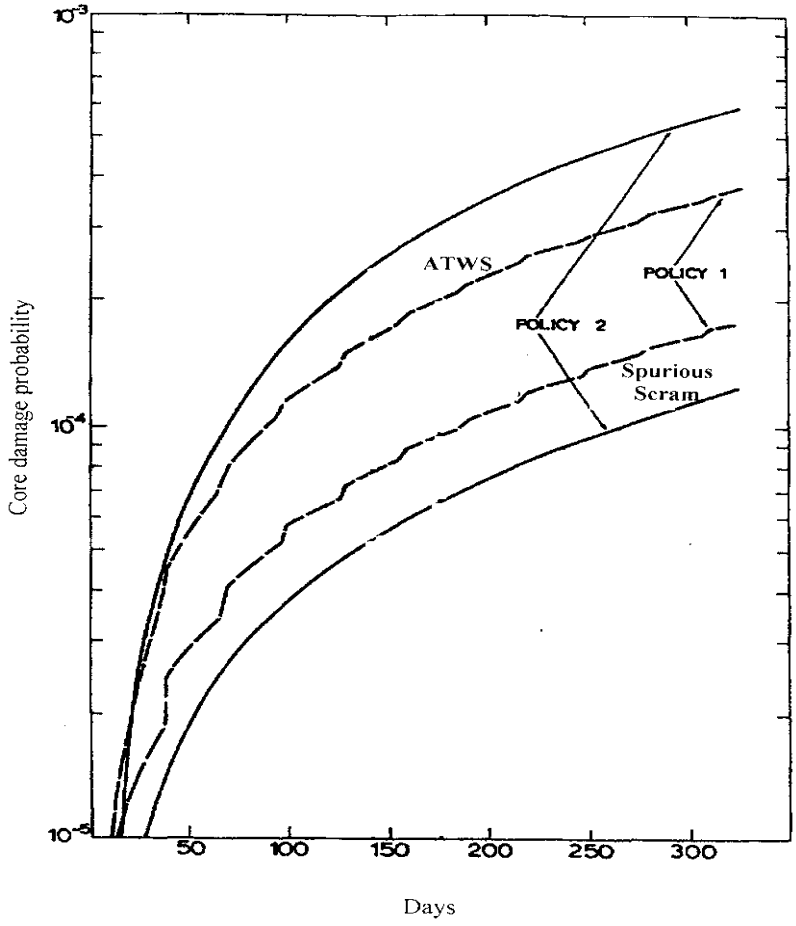

Fig. (5): Probability of core damage and its constituents as a function of time for two TS policies.

Table (3): Comparison of two polices

Policy	Core damage probability/RY	Reactor down time
Policy 1	1.31(-4)	3.5(-2)
Policy 2	1.67(-4)	3.11(-2)

6. CONCLUSIONS

A technique and its application for the probabilistic evaluation of alternative plant technical specifications was developed. The Markov model is more appropriate for such problem where multiple states and stochastic behavior of the components and the system are important.

A Markov model was developed for the RPS and evaluated for the two specific testing policies (two sets of technical specifications). The model calculated two attributes, i.e., core damage probability (CDP) per year of reactor operation and average reactor downtime (ARD) per year of reactor operation. The Markov model is more appropriate for such problem where multiple states and stochastic behavior of the components and the system are important.

The point value calculations allow that the change from policy 1 to policy 2 results in an increase of CDP by 27 percent and in a decrease of ARD by 11 percent. Thus, Policy 1 is preferred to policy 2 if the core damage probability is the sole attribute of performance, while police 2 is preferred to policy 1 if the reactor downtime is the sole attribute of performance. Deciding on one policy against the other requires a decision maker's value tradeoffs between the attributes of performance.

REFERENCES

1. M.C. Kim and P.H. Seong, "A computational method for the probabilistic safety assessment of I&C systems", Reliab. Eng. & Syst. Safe., Vol.91, 2006.

2. H.G. Kang and T. Sung, "An analysis of safety critical digital systems for risk-informed design", Reliability Engineering and Systems Safety 78, 2002.

3. H.G. Kang and T.Sung, " A quantitative study on important factors of the PSA of safety-critical digital systems", J. Korea Nucl Soc. 33 (6), 2001

4. Westinghouse Electric Corporation, Plant Protection System, Nuclear Services, 2007.

5. G.Y. Park, et al., "Safety analysis of safety-critical software for nuclear digital protection system", Computer Safety, Reliability and security, Vol. 4680/2007, 2007.

6. J. H. Bickel, "Risk implications of digital reactor protection system operating experience", Reliability Engineering & System Safety, Vol.93, issue 1, Jan. 2008.

7. C.A. Clarotti and A. Mallucci, "Safety assessment for computerized nuclear reactor protection systems: The Markov approach", Nuclear Engineering and Design Vol.58, issue 3, 2003.

8. S.K. Nam, et al., "The software development process to produce highly reliable safety software for digital reactor protection, ANS 2004 Embedded Topical Meeting on Operating Nuclear Facility (ONFS), 2004.

9. G. Vinod, et al., "Integrating safety critical software system in probabilistic safety assessment," Nuclear Engineering and Design, Vol.238, 2008.

10. Y. Meng, L. Cheng and A. Robert, "A Markov model approach to proliferation resistance assessment of nuclear energy systems," Nuclear Technology, Vol. 162, 2008.

11. T. Echeverria, S. Martorell and A. Thompson, " Modelling test strategies effects on the probability of failure on demand for safety instrumented systems", Proceed. Of the European safety and reliability conference ESREL'08, Spain, 2008.