Dynamic Modeling of Reactor Protection System in Nuclear Power Plant for Reliability Evaluation Based on State Transition Diagram

Marwa A. Shouman
Computer Science and Engineering
Faculty of Electronic Engineering
Menoufia University Cairo, Egypt
marwa.shouman@el-eng.menofia.edu.eg

Amany S. Saber
Reactor Dept.
Nuclear Research CenterEgyptian Atomic Energy AuthorityCairo, Egypt
amanyss@el-eng.menofia.edu.eg

Mohamed K. Shaat
Reactor Dept.
Nuclear Research Center
Egyptian Atomic Energy AuthorityCairo, Egypt
m_shaat3073@yahoo.com

Ayman El-Sayed
Computer Science and Engineering
Faculty of Electronic Engineering
Menoufia University Cairo, Egypt
ayman.elsayed@el-eng.menofia.edu.eg

HanaaTorkey
Computer Science and Engineering
Faculty of Electronic Engineering
Menoufia University Cairo, Egypt
htorkey@el-eng.menofia.edu.eg

***Abstract*—Reliability assessment of a digital dynamic system using traditional Fault Tree Analysis (FTA) is difficult. This paper addresses the dynamic modeling of safety-critical complex systems such as the digital Reactor Protection System (RPS) in Nuclear Power Plants (NPPs). The digital RPS is a safety system utilized in the NPPs for safe operation and shut-down of the reactor in emergency events. A quantitative evaluation reliability analysis for the digital RPS with 2-out-of-4 architecture using the state transition diagram is presented in this paper. The study assesses the effects of independent hardware failures, Common Cause Failures (CCFs), and software failures on the failure of the RPS through calculating Probability of Failure on Demand (PFD). The results prove the validity of the proposed method in analyzing and evaluating reliability of the digital RPS and also show that the CCFs and longer detection time are the main contributions to the PFD of digital RPS.**

Keywords—Nuclear Power Plant, Reactor Protection System, State Transition Diagram

I. INTRODUCTION

The Reactor Protection System(RPS) is a safety critical complicated system, including various electronic components that designed to automatically shut-down the reactor when a calamitous event occurs in the Nuclear Power Plant(NPP) [1]. The safety function performed by the RPS stops the nuclear chain reaction and returns the NPP into a reliable controlled state. Defense-in-depth protection is one of the essential criterions for the digital RPS design. Reactor trip is the first level of automatic protection which inserts all control rods and stops the fission process. However, the core keeps on generating heat, so Engineered Safety Feature Actuation System (ESFAS) is the following level of protection which expels decay heat which could cause severe core damage. Containment cooling is the last level which protects the containment structure from over pressurization [2]. Failure of RPS to perform its function causes damage of the hardware and serious environmental impacts, so the digital RPS requires a very high reliability. Evaluating reliability of digital RPS safety function is an integral part of the digital RPS design which guaranteed the system will accomplish the required job under given conditions over time interval. Integrated fault coverage for reflecting characteristics of Fault-Tolerant Techniques (FTTs) in the reliability model of digital RPS in NPPs is presented at [3]; it considers the process of FTTs from detection to fail-safe generation process to increase failure detection. The Failure Mode and Effect Analysis (FMEA) method is presented at [4]for reliability analysis of digital RPS to identify failure modes, causes, effects, and expanded to include avoidance and mitigation. Basic phases of the Instrumentation and Control System (ICS) safety Markov models are presented at [5]; the models are obtained on the basis of the failure tree development and analysis. The study performs a classification of ICS in a normal operation mode, considering the different modes and diagnostics levels.

A reliability analysis method based on extenics is suggested at [6] for the digital RPS of CPR 1000 NPP by which the relation between the reliability and response time is established. A dynamic reliability model for the RPS in High Temperature Gas-Cooled Reactor Pebble bed Module (HTR-PM) based on the Markov chain theory is introduced at [7]. Dynamic and semi-dynamic methodologies for the probabilistic risk assessment of digital RPS and control systems are presented at [8]; the results show that the two superior methodologies are the Dynamic Flow graph Methodology (DFM) and the Markov methodology merged with the cell-to-cell mapping technique.

In [9], the entire system reliability is analyzed using DFM by studying the effect of software failure, hardware failure and external environment. The results show that DFM guarantee the reliability and safety of the entire system than conventional fault tree technique. In [10], a RPS reliability analysis based on the Monte Carlo method is introduced; involving static reliability analysis of the behavior of each component in the RPS, dynamic characters of the RPS based on the simulation period tests, and take out the reliability calculations over several simulations. At [11], a reliability analysis of Automatic Power Control System (APC) in NPP using DFM is proposed. Inductive and deductive reliability analysis is performed for estimation of suggested DFM.

The methodologies DFM and Markov/Cell-to-Cell Mapping Technique (CCMT) for reliability analysis of digital I&C systems in NPPs are suggested at [12]. Each methodology is tested and evaluated; the results show that the approaches presented can be used for Probabilistic Safety Assessments (PSA) risk informed assessment. A dynamic reliability model for the RPS based on Petri netsis proposed at [13]. The dynamic transition processes of all states are described by Petri nets, in which the Probability of Spurious Trip (PST) and maintenance are considered. Different from other models assuming the PST process following an exponential distribution, deterministic time duration of the PST is adopted in this model. The correctness and applicability of the model are analyzed by comparing the analytical solution and numerical solution. A comparison among the other two models and the proposed model is simulated.

In [14], Bayesian Network (BN) is utilized to predict the software fault in the software reliability analysis at the RPS of RSG-GAS based on Software Development Life Cycle (SDLC). The model structure consists of eight nodes. The results show that a software defect follows the binomial statistic distribution. Progression of a software defect concentration range of the posterior distribution compared with the prior's is also specified. At [15], the failure of control and safety systems can lead to radiation exposure to the public. Therefore, it is essential to ensure the stability of such systems. This paper proposes an effective methodology for stability and steady state analysis of control and safety systems of NPPs. The methodology includes Petri net modeling and analysis of its dynamic behavior.

Fault Tree Analysis(FTA) is one of the reliability analysis methods that applied in the nuclear industry. Despite FTA is helpful for static modeling, it is tricky to model reliability of the digital RPS units using traditional FTA strategy since it cannot precisely simulate the transitions around various states of digital segments. The state transition model is immensely applied for modeling of dynamic and dependent systems. In this study, a reliability evaluation method for the digital RPS using the state transition diagram is suggested. A model for the digital RPS in NPP is proposed; the relationship among the RPS failure modes is identified and the failures of RPS are detected by diagnostic or manual tests.

RPS functional safety state transition models are created for each RPS failures, including independent hardware failures, Common Cause Failures(CCFs), and software failures in order to evaluate reliability of digital RPS. Some salient measures such as the detection time of the failure, the repair time of failed components and Mean Time to Repair (MTTR) that relate to reliability are considered. The Probability of Failure on Demand(PFD) for the 2-out-of-4"2oo4"configuration of the digital RPS caused by independent hardware, Common Cause (CC), and software failures is calculated. The results prove the effectiveness of the proposed method in evaluating reliability of digital RPS, and also show that the CCFs and longer detection time result in higher PFD of digital RPS. The structure of this paper is as follows. In section 2, the digital RPS is described, failures of RPS are explained. In section 3, the RPS functional safety state transition models for a reliability modeling of digital component is proposed, a description of independent hardware, CC, and software failures are discussed. In section 4, the RPS failure event is calculated. In the last section, the concluding remarks will be offered.

II. THE DIGITAL REACTOR PROTECTION SYSTEM (RPS)

The RPS is designed with the "2oo4" architecture in this study as shown in Fig.1. It is composed of four redundant channels running in parallel, and every channel is implemented with the same architecture. A single channel of the RPS consists of Parallel Input/output (PI/O), Multiplexing Unit (MUX), Digital Trip Module (DTM), and Trip Logic Unit (TLU). The logic- trip signals produced by DTM by comparing the observed inputs with the predefined trip set-points values are transferred to the TLU which monitors the logic- trip status signals and activate a trip signal depending on "2oo4" voting. The trip signal is received by Output Logic Unit (OLU) and then sent to the Load Drivers (LDs). The difference in ESFAS that voting between signals is carried out by the Safety Logic Units (SLUs) to create the trip signal [16].

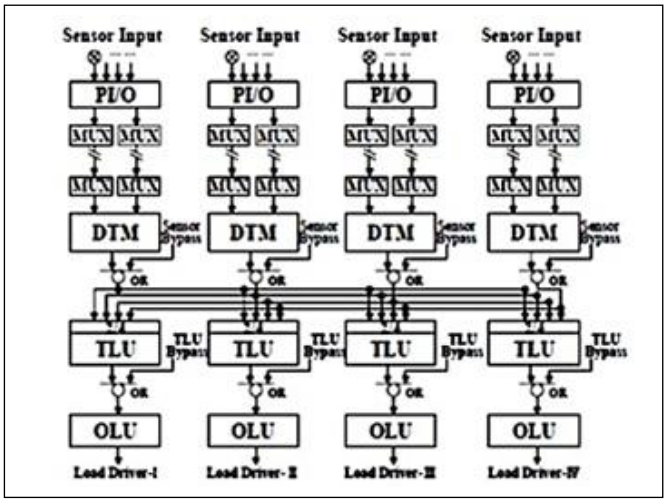

Fig. 1.The digital reactor protection system "2-out-of-4" configuration.

Upon failure to accomplish the required function of the reactor hardware design, the digital RPS automatically generates the trip signal by executing the following "2oo4" voting rules. When there is no failure, the four trains apply "2oo4"voting logic to generate a trip signal. When one train is failed, the remaining trains perform "2oo3"voting logic. If two or more trains are failed and the failures are detected, the reactor is tripped by the digital RPS. If safety measured parameters reached, or exceeds the trip set-limits and there is no output to the breaker, this failure mode is called failure on demand of the digital RPS. Hardware and software failures are considered, hardware failure is defined as the lack of jobof the RPS channel, including modules PI/O, MUX, DTM, TLU and OLU. The digital RPS channel hardware failure mode is categorized to independent failure, and CCFs.

Moreover, the failures are classified into the detected (D) failures which detected by the diagnostic test which runs continuously or by the operator and the undetected (U) failures which discovered by the manual test which is executed at a predefined interval T. Finally, the RPS software failure mode should be considered which is assumed to be detected by a manual test. A plant operator starts to repair the failed channel of the RPS after detectionof a single hardware fault by diagnostic test or

manual test. A Plant operator makes the reactor shut-down immediately after a detection of hardware fault of both channels by diagnostic function or manual test, or after a detection of software fault by a manual test. The reactor returns to the initial state after the shut-down state and restarts [17]. Table I shows the notations used in this paper.A repair of undetected hardware fault can be modeled by the exponential distribution with the constant repair rate which can be approximated as *1/MTTR*. A shut-down operation can be modeled by the exponential distribution with the constant transition rate which can be approximated as $1/T_{shut}$. The average failure duration is a regular function; it can be approximated by *T/2*. A mean failure-duration time of "double hardware faults" can be approximated as *T/3*; "triple hardware faults" can be approximated as *T/4*; "quadruple hardware faults" can be approximated as *T/5*; a mean failure-duration time of software fault can be approximated as *T/2* [18].

TABLE I. NOTATIONS USED IN THIS PAPER

H/W	Hardware
S/W	Software
S_i	State i
P_i	Probability of state i
λ	H/W Failure Rate
λ_D	Detected H/W Failure Rate [= $DC*\lambda$]
λ_U	Undetected H/W Failure Rate [= $(1 - DC) *\lambda$]
λ_{dem}	Number of demands of the RPS per unit time *t(*where: the RPS is not motivated at time *t)*
λ_{sw}	S/W Failure Rate
R_2	The ratio of the CC failures for $\lambda_D$and λ_U
R_3	The ratio of triple CC failures for$\lambda_D$and λ_U
R_4	The ratio of four CC failures for $\lambda_D$and λ_U
R_{es}	Restart Rate of the Reactor
W	Renewal Rate of the Reactor
$MTTR$	Mean Time To Repair
T	Manual Test Interval
T_{shut}	Reactor Shut-down Duration
μ_{R_1}	Repair Rate of Single Undetected Independent H/W Failure [= $1/(T/2+MTTR)$] [15]
μ_{R_2}	Repair Rate of Single Detected Independent H/W Failure [= $1/MTTR$]
μ_{R_3}	Repair Rate of Double Undetected Independent H/W Failure [= $1/(T/3+MTTR)$] [15]
μ_{R_4}	Repair Rate of Double Undetected CC H/W Failures[= $1/(T/3+MTTR)$] [15]
μ_{R_5}	Repair Rate of Double Detected CC H/W Failures [= $1/MTTR$]
μ_{shut_1}	Shut Down Transition Rate of triple Undetected H/W Failures [= $1/(T/4+T_{shut})$] [15]
μ_{shut_2}	Shut Down Transition Rate of Fourth Undetected H/W Failures [= $1/(T/5+T_{shut})$] [15]
μ_{shut_3}	Shut Down Transition Rate of detected H/W Failures [= $1/T_{shut}$]
$\mu_{shut_{sw}}$	Shut Down Transition Rate of S/W Failure [= $1/(T/2+T_{shut})$] [15]
PFD_{ct_1}	The PFD of RPS Caused by Independent H/W Failure and Demand per Calendar Time
PFD_{ct_2}	The PFD of RPS Caused by CC H/W Failures and Demand per Calendar Time
PFD_{ct_3}	The PFD of RPS Caused by S/W Failure and Demand per Calendar Time
PFD_{ct}	The PFD of RPS Event per Unit Calendar time
PFD_{Rot_1}	The PFD of RPS Caused by Independent H/W Failure and Demand per Reactor Operational time
PFD_{Rot_2}	The PFD of RPS Caused by CC H/W Failures and Demand per Reactor Operational time
PFD_{Rot_3}	The PFD of RPS Caused by S/W Failure and Demand per Reactor Operational time
PFD_{Rot}	The PFD of RPS Event per Reactor Operational time

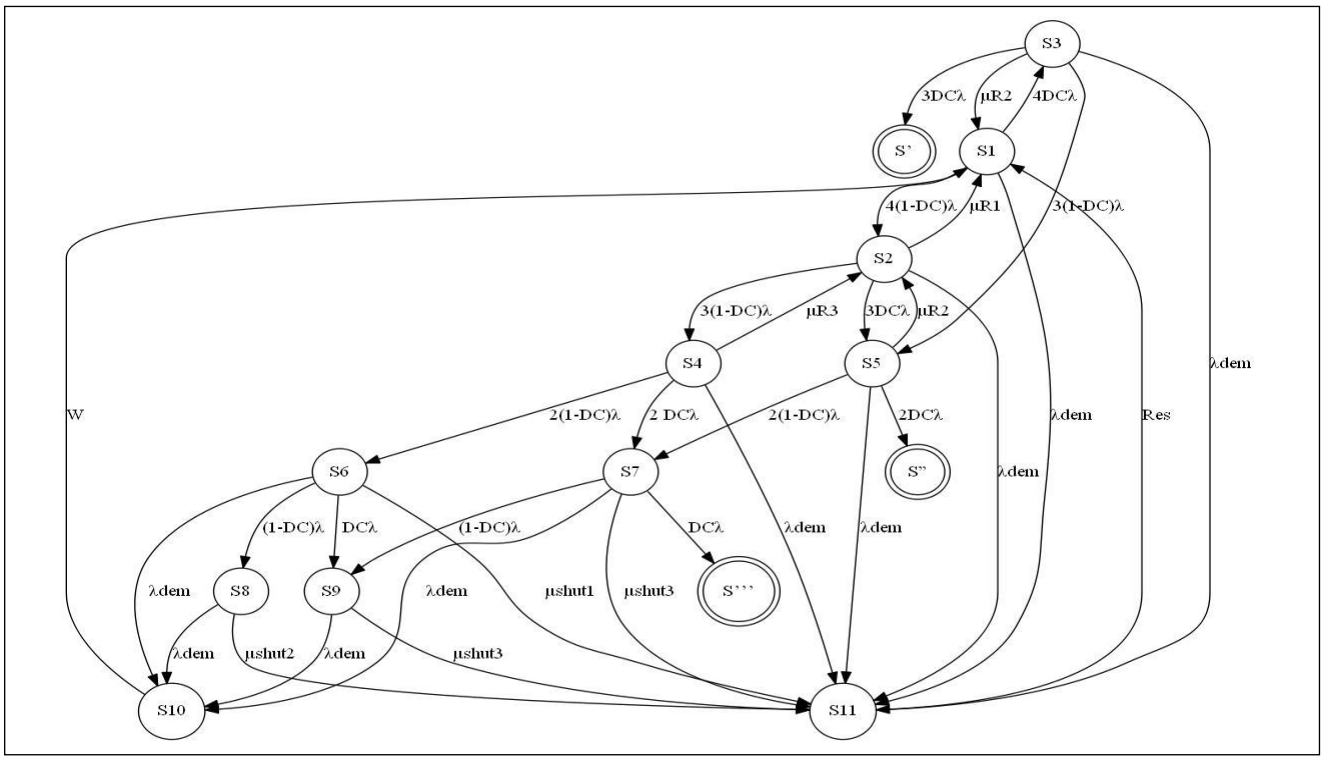

Fig. 2. Independent hardware failures of RPS state diagram.

III. RPS FUNCTIONAL SAFETY STATE TRANSITION PROPOSED MODELS

A. Independent Hardware Failure

The DTM, TLU, OLU, LD, PI/O, MUX, and SLU macro-components are composed of sub components. The failure rate of each macro-component can be evaluated as the sum of the failure rates of these subcomponents. Hardware failures are consisting of the detectable failures and non-detectable failures. The contribution of these two kinds of failures is taken into account when assessing the average probability of the hardware failure. This can be clarified by a state transition diagram shown in Fig. 2**.** The states are defined as follows:

i. ***State S_1***: Initial sate, no demand, no faults; ***State S_{10}***: Failure of RPS (RPS fails to trip); ***State S_{11}***: Shut-down state, no operation, plant is safe.

ii. ***State S_2***: One channel is in an undetected failure, no demand; ***State S_4***: Two channels are in undetected failures, no demand; ***State S_6***: Three channels are in undetected failures, no demand; ***State S_8***: Four channels are in undetected failures, no demand.

iii. ***State S_3***: One channel is in a detected failure, no demand; ***State S'***: Two channels are in detected failures, no demand.

iv. ***State S_5***: One channel is in an undetected failure and another one channel is in a detected failure, no demand; ***State S_7***: Two channels are in undetected failures and another one channel is in a detected failure, no demand; ***State S_9***: Three channels are in undetected failures and another one channel is in a detected failure, no demand; ***State S'"***: Two channels are in detected failures and another one channel is in an undetected failure, no demand; ***State S'"***: Two channels are in detected failures and two channels are in undetected failures, no demand.

The equations that describe the states and transitions in Fig. 2 are illustrated as follows:

$$\sum_{i=1}^{11} P_i = 1 \quad (1)$$

$$(\lambda_{dem} + 4\,(1-DC)\lambda + 4\,DC.\lambda)\,.P_1 = \mu_{R_1}\,.P_2 + \mu_{R_2}.P_3 + W.\,P_{10} + R_{es}.P_{11} \quad (2)$$

$$\left(\mu_{R_1} + 3\,(1-DC)\lambda + 3\,DC.\lambda + \lambda_{dem}\right).P_2 = 4\,(1-DC)\lambda\,.P_1 + \mu_{R_3}\,.\,P_4 + \mu_{R_2}.\,P_5 \quad (3)$$

$$\left(\mu_{R_2} + \lambda_{dem}\right).P_3 = 4\,DC.\lambda\,.P_1 \quad (4)$$

$$\left(\mu_{R_3} + 2\,(1-DC)\lambda + 2\,DC.\lambda + \lambda_{dem}\right).P_4 = 3\,(1-DC)\lambda\,.P_2 \quad (5)$$

$$\left(\mu_{R_2} + \lambda_{dem}\right).P_5 = 3\,DC.\lambda\,.P_2 \quad (6)$$

$$\left((1-DC)\lambda + DC.\lambda + \lambda_{dem} + \mu_{shut_1}\right).P_6 = 2\,(1-DC)\lambda\,.P_4 \quad (7)$$

$$\left(\lambda_{dem} + \mu_{shut_3}\right).P_7 = 2\,DC.\lambda.\,P_4 \quad (8)$$

$$\left(\lambda_{dem} + \mu_{shut_2}\right).P_8 = (1-DC)\lambda\,.P_6 \quad (9)$$

$$\left(\lambda_{dem} + \mu_{shut_3}\right).P_9 = DC.\lambda.\,P_6 \quad (10)$$

$$W.\,P_{10} = \lambda_{dem}\,.(P_6 + P_7 + P_8 + P_9) \quad (11)$$

$$R_{es}\,.P_{11} = \lambda_{dem}\,.(P_1 + P_2 + P_3 + P_4 + P_5) + \mu_{shut_1}.P_6 + \mu_{shut_2}.P_8 + \mu_{shut_3}.(P_7 + P_9) \quad (12)$$

The PFD of RPS caused by independent H/W failure and demand per unit calendar time is given by:

$$PFD_{ct_1} = \lambda_{dem}\,.(P_6 + P_7 + P_8 + P_9) = W.\,P_{10} \quad (13)$$

From (1) to (12) in (13):

$$PFD_{ct_1} = \lambda_{dem}\,.(P_6 + P_7 + P_8 + P_9) = W.\,P_{10} = \frac{\lambda_{dem}\,(X_{6\to4} + X_{7\to4} + X_{8\to4} + X_{9\to4})}{(1 + X_{1\to4} + X_{2\to4} + X_{3\to4} + X_{5\to4} + X_{6\to4} + X_{7\to4} + X_{8\to4} + X_{9\to4} + X_{10\to4} + X_{11\to4})} \quad (14)$$

Where:

$$X_{1\to4} = \frac{(\mu_{R_1}+3\,(1-DC)\lambda+3\,DC\lambda+\lambda_{dem})\,.\,X_{2\to4}-\mu_{R_3}-\mu_{R_2}\,.\,X_{5\to4}}{4\,(1-DC)\lambda}$$

$$X_{2\to4} = \left(\mu_{R_3}+2\,(1-DC)\lambda+2\,DC.\lambda+\lambda_{dem}\right)/3(1-DC)\lambda$$

$$X_{3\to4} = 4\,DC.\lambda\,.X_{1\to4}/(\mu_{R_2}+\lambda_{dem})$$

$$X_{5\to4} = 3DC.\lambda.X_{2\to4}/(\mu_{R_2}+\lambda_{dem})$$

$$X_{6\to4} = 2\,(1-DC)\lambda/\left((1-DC)\lambda+DC.\lambda+\lambda_{dem}+\mu_{shut_1}\right)$$

$$X_{7\to4} = 2\,DC.\lambda/\left(\lambda_{dem}+\mu_{shut_3}\right)$$

$$X_{8\to4} = (1-DC)\lambda.X_{6\to4}/\left(\lambda_{dem}+\mu_{shut_2}\right)$$

$$X_{9\to4} = DC.\lambda.X_{6\to4}/\left(\lambda_{dem}+\mu_{shut_3}\right)$$

$$X_{10\to4} = \lambda_{dem}\,.(X_{6\to4}+X_{7\to4}+X_{8\to4}+X_{9\to4})/W$$

$$X_{11\to4} = \begin{bmatrix}(\lambda_{dem}+4\,(1-\mathrm{DC})\lambda+4\,\mathrm{DC}.\lambda).X_{1\to4}-\mu_{R_1}.\,X_{2\to4}\\ -\mu_{R_2}.\,X_{3\to4}-W.\,X_{10\to4}\end{bmatrix}/R_{es}$$

The PFD of RPS caused by independent H/W failure and demand per reactor operational time is given by:

$$PFD_{Rot_1} = PFD_{ct_1}/1-P_{10}-P_{11} = \frac{\lambda_{dem}\,(X_{6\to4}+X_{7\to4}+X_{8\to4}+X_{9\to4})}{(1+X_{1\to4}+X_{2\to4}+X_{3\to4}+X_{5\to4}+X_{6\to4}+X_{7\to4}+X_{8\to4}+X_{9\to4})} \quad (15)$$

B. Common Cause Hardware Failures (CCFs)

The redundant digital components hardware failures are defined as CCFs. In the RPS when the plant variables approach the specified safety limits, the existence of CCF prevents the appropriate safety action of the RPS. Therefore, a CCF has a critical impact on the safety of the NPP. The component groups of the CCF are the TLU, DTM, PI/O and MUX for the RTS, and the SLU, DTM, PI/O and MUX for the ESFAS. This can be modeled by a state diagram as shown in Fig. 3. The states are defined as follows**:**

i. ***State S_1*:** Initial sate, no demand, no faults; ***State S_{10}*:** Failure of RPS (RPS fails to trip); ***State S_{11}***: Shut-down state, no operation, plant is safe.

ii. ***State S_A*:** Two channels are in undetected CCF, no demand; ***State S_C*:** Three channels are in undetected CCF, no demand; ***State S_E***: Four channels are in undetected CCF, no demand.

iii. ***State S_B*:** Two channels are in detected CCF, no demand; ***State S_D*:** Three channels are in detected CCF, no demand; ***State S_F*:** Four channels are in detected CCF, no demand.

The equations that describe the states and transitions in Fig. 3 are illustrated as follows:

$$P_1+P_A+P_B+P_C+P_D+P_E+P_F+P_{10}+P_{11}=1 \quad (16)$$

$$(6R_2.(1-\mathrm{DC})\lambda+6\,R_2.\mathrm{DC}\,\lambda+4R_3.(1-\mathrm{DC})\lambda+4R_3.\mathrm{DC}\,\lambda+R_4.(1-\mathrm{DC})\lambda+R_4.\mathrm{DC}\,\lambda+\lambda_{dem})\,.P_1 = \mu_{R_4}.P_A+\mu_{R_5}.P_B+\mathrm{W}.P_{10}+R_{es}.P_{11} \quad (17)$$

$$(\mu_{R_4}+\lambda_{dem})\,.P_A = 6\,R_2.(1-DC)\lambda.P_1 \quad (18)$$

$$(\mu_{R_5}+\lambda_{dem})\,.P_B = 6\,R_2.DC\,\lambda\,.P_1 \quad (19)$$

$$(\lambda_{dem}+\mu_{shut_1}).P_C = 4\,R_3\,.(1-DC)\lambda\,.P_1 \quad (20)$$

$$(\lambda_{dem}+\mu_{shut_3}).P_D = 4\,R_3\,.DC\,\lambda\,.P_1 \quad (21)$$

$$(\lambda_{dem}+\mu_{shut_2}).P_E = R_4\,.(1-DC)\lambda\,.P_1 \quad (22)$$

$$(\lambda_{dem}+\mu_{shut_3}).P_F = R_4\,.DC\,\lambda\,.P_1 \quad (23)$$

$$W.\,P_{10} = \lambda_{dem}\,.(P_C+P_D+P_E+P_F) \quad (24)$$

$$\mathrm{R_{es}}\,.\mathrm{P_{11}} = \lambda_{\mathrm{dem}}\,.(\mathrm{P_1}+\mathrm{P_A}+\mathrm{P_B})+\mu_{\mathrm{shut\,1}}\,.\mathrm{P_C}+\mu_{\mathrm{shut\,2}}.\mathrm{P_E}+\mu_{\mathrm{shut\,3}}.(\mathrm{P_D}+\mathrm{P_F}) \quad (25)$$

The PFD of RPS caused by CC hardware failure and demand per unit calendar time is given by:

$$PFD_{ct_2} = \lambda_{dem}\,.(P_C+P_D+P_E+P_F) = W.\,P_{10} \quad (26)$$

From (16) to (25) in (26):

$$PFD_{ct_2} = \lambda_{dem}\,.(P_C+P_D+P_E+P_F) = W.\,P_{10} = \lambda_{dem}\,.(\mathrm{X_3}+\mathrm{X_4}+\mathrm{X_5}+\mathrm{X_6})\Big/\begin{matrix}[1+C_1.(\mathrm{X_1}+\mathrm{X_2})+\\ C_2.\mathrm{X_3}+C_3.(\mathrm{X_4}+\mathrm{X_6})+\\ C_4.X_5+\lambda_{dem}/R_{es}]\end{matrix} \quad (27)$$

Where:

$$C_1 = \left(1+\frac{\lambda_{dem}}{R_{es}}\right)$$

$$C_2 = \left(1+\frac{\lambda_{dem}}{W}+\frac{\mu_{shut\,1}}{R_{es}}\right)$$

$$C_3 = \left(1+\frac{\lambda_{dem}}{W}+\frac{\mu_{shut\,3}}{R_{es}}\right)$$

$$C4 = \left(1+\frac{\lambda_{dem}}{W}+\frac{\mu_{shut\,2}}{R_{es}}\right)$$

$$X_1 = 6\;R_2(1-DC)\lambda/(\mu_{R_4}+\lambda_{dem})$$

$$X_2 = 6\;R_2.DC.\lambda/(\mu_{R_5}+\lambda_{dem})$$

$$X_3 = 4\;R_3(1-DC)\lambda/\left(\lambda_{dem}+\mu_{shut_1}\right)$$

$$X_4 = 4\;R_3.DC\,.\lambda/(\lambda_{dem}+\mu_{shut_3})$$

$$X_5 = R_4(1-DC)\lambda/\left(\lambda_{dem}+\mu_{shut_2}\right)$$

$$X_6 = R_4.DC\,.\lambda/(\lambda_{dem}+\mu_{shut_3})$$

The PFD of RPS caused by CC hardware failure and demand per reactor operational time is given by:

$$PFD_{Rot_2} = PFD_{ct_2}/1-P_{10}-P_{11} = \lambda_{dem}\,.\,(\mathrm{X_3}+\mathrm{X_4}+\mathrm{X_5}+\mathrm{X_6})/1+\mathrm{X_1}+\mathrm{X_2}+\mathrm{X_3}+\mathrm{X_4}+\mathrm{X_5}+\mathrm{X_6} \quad (28)$$

C. Software Failures of Digital Component

The RPS failure due to the software failure was assumed to occur in the DTM, TLU or SLU. The software failure probability of the PI/O or MUX is inferred to be considerably lower than that of the DTM, TLU or SLU; because software error should be detected thorough the verification and validation in case of the PI/O and MUX. This can be modeled by a state diagram as shown in Fig. 4**.** Thestates are defined as follows:

i. ***State S_1*:** Initial sate, no demand, no faults; ***State S_{10}***: Failure of RPS (RPS fails to trip); ***State S_{11}***: Shut-down state, no operation, plant is safe.

ii. ***State S_{sw}*:** Four channels are in software failures, no demand.

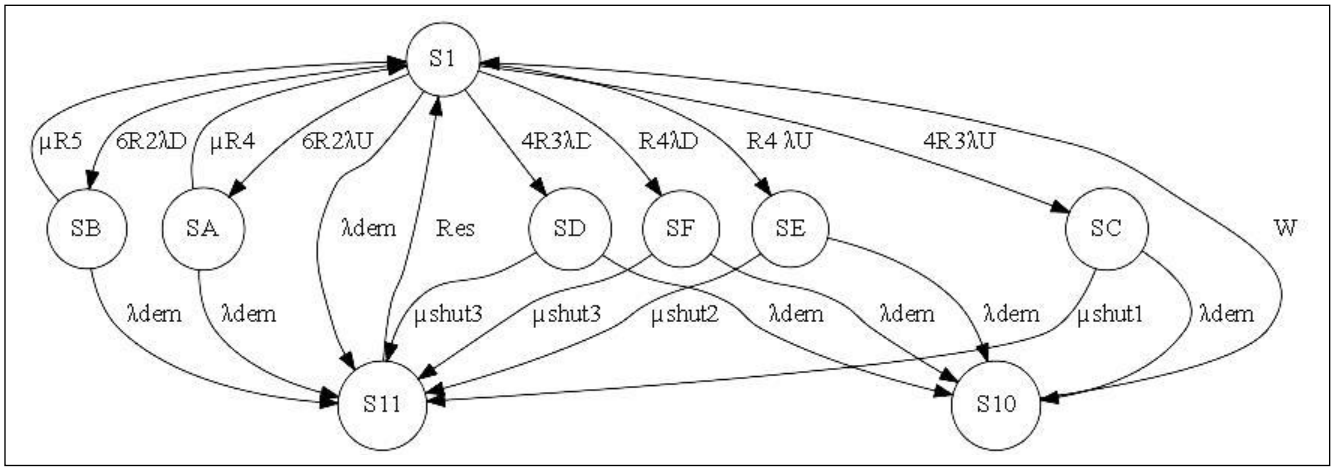

Fig. 3. Common cause H/W failures of RPS state diagram

The equations that describe the states and transitions in Fig. 4 are illustrated as follows:

$$P_1 + P_{sw} + P_{10} + P_{11} = 1 \quad (29)$$

$$(\lambda_{dem} + \lambda_{sw}) . P_1 = W. P_{10} + R_{es} . P_{11} \quad (30)$$

$$(\lambda_{dem} + \mu_{shut_{sw}}). P_{sw} = \lambda_{sw} . P_1 \quad (31)$$

$$W. P_{10} = \lambda_{dem} . P_{sw} \quad (32)$$

$$R_{es} . P_{11} = \lambda_{dem} . P_1 + \mu_{shut_{sw}} . P_{sw} \quad (33)$$

The PFD of RPS caused by software failure and demand per unit calendar time is given by:

$$PFD_{ct_3} = \lambda_{dem} . P_{sw} = \mathrm{W}. P_{10} \quad (34)$$

From (29) to (33) in (34):

$$PFD_{ct_3} = \lambda_{dem} * X_7/1 + X_7 + \frac{\lambda_{dem}}{W} * X_7 + \frac{\lambda_{dem}}{R_{es}} + \frac{\mu_{shut\,sw}}{R_{es}} * X_7 \quad (35)$$

Where: $X_7 = \lambda_{sw}/(\lambda_{dem} + \mu_{shut_{sw}})$

The PFD of RPS caused by software failure and demand per reactor operational time is given by:

$$PFD_{Rot_3} = PFD_{ct_3}/1 - P_{10} - P_{11} = \lambda_{dem} * X_7/(1 + X_7) \quad (36)$$

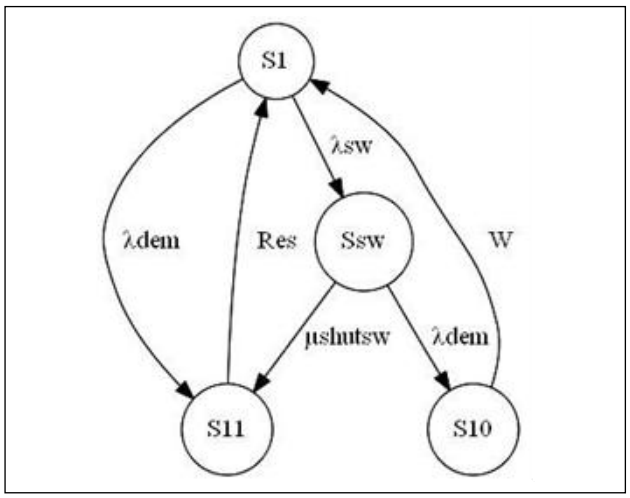

Fig. 4. Software failures of RPS state diagram.

IV. RESULTS AND DISSCUSION

RPS failure event calculation includes the PFD of RPS event per unit calendar timeand per reactor operational time which is the time considering the reactor is in operation excluding the time that the reactor is out of operation. The PFD of RPS event per unit calendar time and per reactor operational time is given by (37) and (38) respectively:

$$PFD_{ct} = PFD_{ct_1} + PFD_{ct_2} + PFD_{ct_3} \quad (37)$$

$$PFD_{Rot} = PFD_{Rot_1} + PFD_{Rot_2} + PFD_{Rot_3} \quad (38)$$

The functional model input parameters are shown in Table II [19,20]; the PFD of RPS caused by independent H/W failure, H/W CCFs, software failure and the digital RPS failure event are represented in Fig. 5. The results show that the digital RPS failure event almost raises proportional to the demand rate λ_{dem} with the given range. Also, the PFD of digital RPS caused by CCF is larger than independent H/W failure and software failure (i.e. CCF is the main contributor to the digital RPS failure event). The calculated results of PFD of the digital RPS failure event in this paper are compared by FTA method [21]. The results prove the superiority of the present study.

Fig. 6 shows the calculated results of the PFD for digital RPS caused by H/W CCFs at detection time intervals T=720 (hrs.) and T=8 (hrs.) The failure detection time has an inverse impact on the PFD of digital RPS; with longer detection time, the digital RPS will be more exposed to failure on demand and the system failure probability increased; with shorter detection time, the digital RPS will be less exposed to failure on demand and the system failure probability decreased.Thus, the results using proposed method show that with shorter detection time T=8 (hrs.), the asymptotic convergence of the functional safety PFD caused by H/W CCFs becomes lower and more failures are covered, therefore the digital RPS failure probability decreased. A short detection time would compromise reliability; since the detector would report as down a process that is up and more failures are covered. Longer detection time and H/W CCFs are the main reasons to the higher PFD. If higher reliability is required for instrumentation and control safety system, it is substantial toperform the diagnostic functions on the digital RPS that can reserve thehighest Diagnostic Coverage (DC).The DC is a measure of the effectiveness of diagnostics implemented in the system.

TABLEII. FUNCTIONAL MODEL INPUT PARAMETERS VALUES

Parameters		Values	Unit
λ_{dem}		1E-8 to 1E-2	(1/hr)
DC		0.99	
λ	*PI/O*	3.5E-7	(1/hr)
	MUX	1.1E-6	(1/hr)
	DTM	1.2E-6	(1/hr)
	TLU	1.5E-5	(1/hr)
	OLU	1.0E-6	(1/hr)
	LD	1.0E-6	(1/hr)
	SLU	1.2E-6	(1/hr)
λ_{sw}		1E-12	(1/hr)
R_{es}		1E-10	(1/hr)
W		1E-10	(1/hr)
R_2		1E-3	
R_3		1E-4	
R_4		1E-5	
MTTR		10	(hr)
T		720	(hr)
T_{shut}		0.1	(hr)

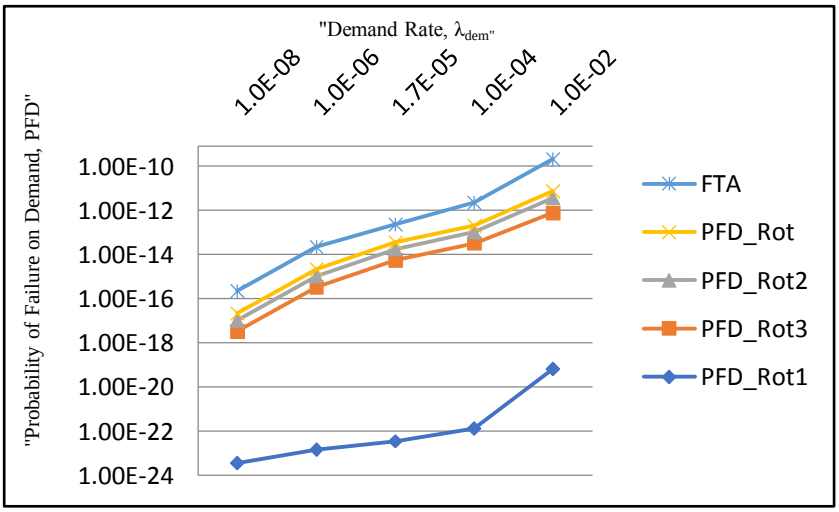

Fig. 5.Results of the PFD of digital RPS event analysis versus the input parameter λ_{dem}.

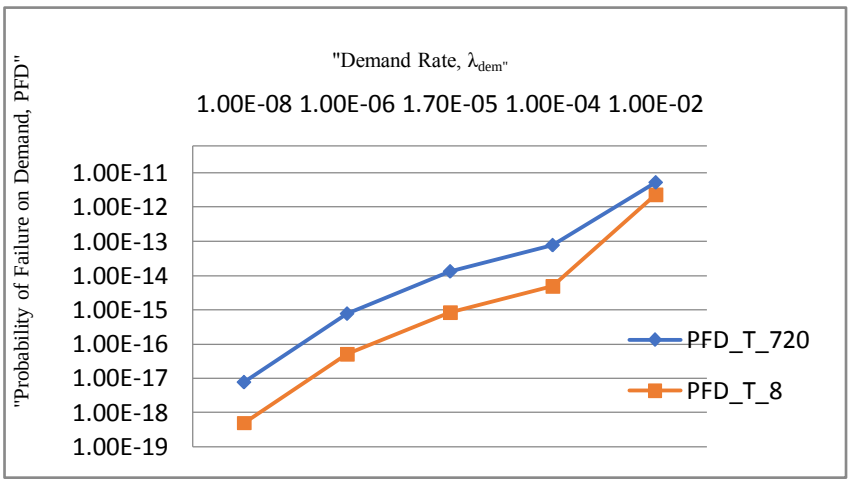

Fig. 6. Results of the PFD for digital RPS caused by H/W CCFs with T=720 (hrs.) and T=8 (hrs.)

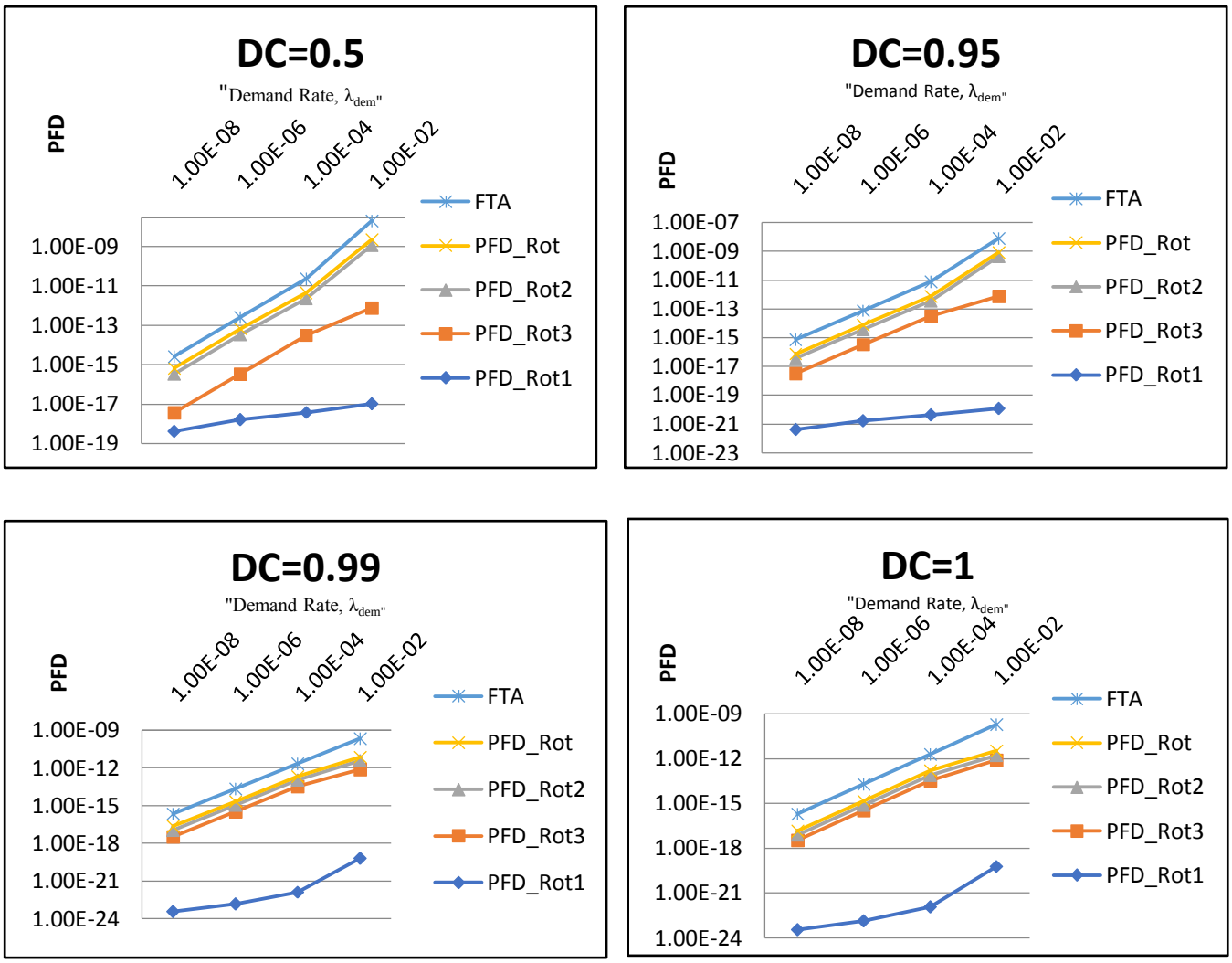

Fig. 7.Results of the PFD for RPS event analysis at different values of the DC.

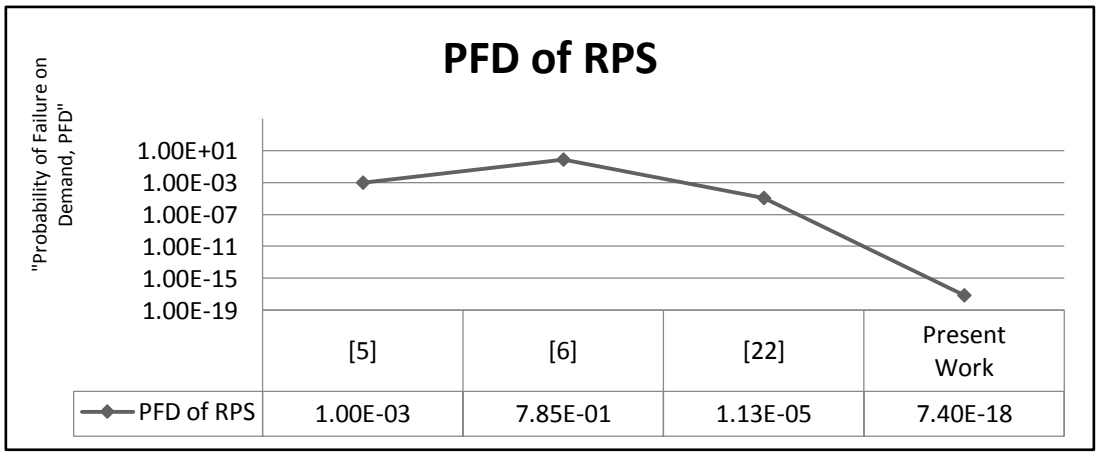

Fig. 8. The PFD of the digital RPS comparison of various methods.

It is the ratio of the failures detected and/or controlled by a safety mechanism to the total failures in the element.The efficiency of the DC function may affect the PFD event frequency. To study the DC impact on the PFD of digital RPS, Fig. 7 demonstrates the results of the analyses of the effect of changing values of DC in case of 0.5, 0.95, 0.99 and 1 on the PFD. From the figures, for DC equals 0.5, 0.95, 0.99, 1, the best values for PFD are 3.4E-16, 3.7E-17, 1.1E-17, 7.4E-18 respectively. Consequently, when DC becomes higher, the effectiveness of diagnostics implemented in the system will increase and most failures will be detected by a safety mechanism, so the PFD becomes lower, and vice versa.Comparing the results with FTA at various values of DC parameter shows that the proposed study gives better

results than FTA for the behavior of PFD function, especially when DC becomes higher; the difference between this technique and FTA technique becomes greater which demonstrate the notability of the proposed method. Finally, the PFD of the proposed method gives a minimum value equal to 7.40E-18 is compared to values of 1.00E-03, 7.85E-01, and 1.13E-05 calculated using other methods as shown in Fig. 8. The comparison of the supposed study result to the other different methods' results is based on the requirement of minimum unavailability of the RPS as stated in the NUREG/ CR-5500 [23]. Therefore, it is proper to analyze the reliability of the digital RPS using a dynamic approach considering different combinations of states of the system and state transitions to avoid unnecessary briefness.

V. CONCLUSION

This paper discussed the application case study of the digital systems provided in NPP in the aspect of reliability evaluation of a safety critical digital RPS. Reliability modeling of digital devices using the traditional FTA method is difficult. A well-established functional safety state transition models are proposed for the "2oo4" RPS architecture. The PFD calculation formula for the digital RPS failures, including the independent hardware failure, hardware CCFs, and software failure are developed. The results using the suggested method are compared with the results of the FTA methodand other methods to verify the effectiveness of the suggested method. The CCFs and longer detection time lead to a higher probability that a failure may be occurred and they are the main contributor to the system failure. In the future, reducing the effects of the CCFs during the plant design phase and the optimization of test intervals will be taken into consideration.

REFERENCES

[1] U.S. Nuclear Regulatory Commission, "Reactor concepts manual," 2001, https://www.nrc.gov/docs/ML0230/ML023020519.pdf. Accessed 21 June 2020.

[2] International Atomic Energy Agency (IAEA), "Defense in depth in nuclear safety," International Nuclear Safety Advisory Group (NSAG), No. 10, Vienna, 1996,https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1013e_web.pdf. Accessed 2 July 2020.

[3] B. G. Kim, H. G. Kang, H. E. Kim, and S. J. Lee, "Reliability modeling of digital component in plant protection system with various fault-tolerant techniques," Nuclear Engineering and Design, vol. 265, pp. 1005– 1015, 2013.

[4] X. X. Guo, Y. B. Liao, D. Y. Xia, and S. Q. Lin, "FMEA analysis for reactor protection system of nuclear power plant", Editorial Board of Nuclear Electronics & Detection Technology, 2015.

[5] Y. Bulba, Y. Ponochovny, V. Sklyar, and A. Ivasiuk, "Classification and research of the reactor protection instrumentation and control system functional safety Markov models in a normal operation mode," 2nd International Workshop on Theory of Reliability and Markov Modeling for Information Technologies, Kyiv, Ukraine, June 2016.

[6] J. Zhao, Y. N. He, P.F.Gu, W. H. Chen, and F.Gao, "Reliability of digital reactor protection system based on extenics," SpringerPlus, vol. 5, No. 1, 2016.

[7] S. Zhou, C. Guo, and D. Li,"Reliability analysis for the reactor protection system of HTR-PM," 11th International Conference on Reliability, Maintainability and Safety (ICRMS), China, 2016.

[8] S. A. Arndt, T. Aldemiret, D. W. Miller, and M.Stovsky, "Methodologies for the probabilistic risk assessment of digital reactor protection and control systems," Nuclear technology, vol. 159, No.2, pp. 167-191, 2017.

[9] C. Zhuo, Z. Bo, Y. Jian, and S. Jin-long, "Research on the reliability of digital instrumentation and control system of nuclear power plant based ondynamic flow graph methodology," 25th International Conference on Nuclear Engineering, China, 2017.

[10] D. Li, Z. hao, S. Zhou, and C. Guo, "Application of Monte Carlo methods in reactor protection system reliability research," 26th International Conference on Nuclear Engineering (ICONE), London, England, 2018.

[11] W. Hao, T. Cong, Z. Shiliang, L. Y. Yuan, and S. Ahmad, "Reliability analysis of the automatic control system of reactor power in nuclear power plant based on DFM," 24th International Conference on Nuclear Engineering (ICONE), Charlotte, North Carolina, USA, 2016.

[12] J. M. O. Pinto, I. B. Gomes, P. L. C. Saldanha, E. B. Furieri, and P. F. F. Melo, In Handbook of Automation and Control Trends, edited by Pedro Ponce.IntechOpen, 2016, Chapter 2.

[13] X. Cao, H. Xiong, C. Guo, D. Li, H. Zhang, and X. Huang, "Petri nets based reliability modeling of reactor protection system considering periodic surveillance test," 27th International Conference on Nuclear Engineering (ICONE), Japan, 2019.

[14] S. Santoso, S. Bakhri, and J. Situmorang, "A Bayesian network approach to estimating software reliability of RSG-GAS reactor protection system," Atom Indonesia,vol. 45, No. 1, pp. 43 – 49, 2019.

[15] B. Gupta, P. Singh, and L. Singh, "Stability and steady state analysis of control and safety systems of nuclear power plants," Annals of Nuclear Energy, vol. 147, 2020.

[16] M. Yamashita, S. Miura, M. Fukuda, and M. Hirano, "Reliability analysis of digital reactor protection system," 12th International Conference on Nuclear Engineering (ICONE), Arlington, Virginia USA, pp. 403-409, April 2004.

[17] H. Muta, and K.Muramatsu, "Quantitative modeling of digital reactor protection system using Markov state-transition model," Journal of Nuclear Science and Technology, vol. 51, No. 9, pp. 1073–1086, 2014.

[18] T. Shimodaira, Y. Sato, and K. Suyama, "Estimation of hazardous event rate for repairable 1-out-of-2 safety-related systems based on state transition models," Transactions of the Institute of Electronics, Information and Communication Engineers, vol. J88-A, No. 8, pp. 962–973, Japanese, 2005.

[19] International Atomic Energy Agency (IAEA), "Component reliability data for use in probabilistic safety assessment," IAEA-TECDOC-478, Vienna, 1988.

[20] International Electro-technical Commission (IEC) 61508, "Functional safety of electrical/electronic/programmable electronic safety related systems," Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, 2010.

[21] Japan Nuclear Energy Safety Organization (JNES), "The report of improvement of reliability model of digital reactor protection system," Japan Nuclear Energy Safety Organization, No. SAE10-013, Tokyo, Japan, 2010.

[22] Z. Ma, H. Yoshikawa, and M. Yang, "Reliability model of the digital reactor protection system considering the repair time and common cause failure," Journal of Nuclear Science and Technology, 2017.

[23] S. A. Eide,M. B. Calley,C. D. Gentillon,T. Wierman, D. Rasmuson, and D. Marksberry, "Reliability study: Westinghouse reactor protection system 1984-1995," U.S. Nuclear Regulatory Commission RegulationNUREG/CR-5500, vol.2,1998,https://nrcoe.inl.gov/resultsdb/publicdocs/SystemStudies/nureg-cr-5500-vol-2.pdf.Accessed 10 July 2020.