RELIABILITY ANALYSIS OF A SAFETY SYSTEM USING PETRI NET AND COMPARISON WITH SMART COMPONENT METHODOLOGY

Darpan K. Shukla[1], A. John Arul[2], Mark James Wootton[3,*], John Andrews[4,*]

[1]*Indira Gandhi Centre for Atomic Research, Homi Bhabha National Institute, Kalpakkam, TN, India, 603102, and darpanks@igcar.gov.in*
[2]*Indira Gandhi Centre for Atomic Research, Kalpakkam, TN, India, 603102, and arul@igcar.gov.in*
[*]*Faculty of Engineering, University of Nottingham, United Kingdom and* [3]*mark.wootton@nottingham.ac.uk,* [4]*john.andrews@nottingham.ac.uk*

For the reliability analysis of advanced nuclear reactor safety systems, though event tree-fault approach has been used over the years, they are inadequate from a modeling perspective. First, it involves making various levels of approximations depending on the complexity of the system being modeled and second, the responsibility of deriving the correct reliability model rests with the analyst. To overcome the problems mentioned above, various methods for the inclusion of dynamic aspects are being developed. Though many of the methods can more closely reflect the dynamic reliability aspects of the reliability model, they lack the features required for a user-friendly approach. Recently, a Smart Component Methodology based on the object-oriented representation of system structure and behavior, to perform dynamic reliability analysis has been proposed.

The dynamic reliability methods could be divided into two categories based on how close the initial formal representation is to the actual system description. For example, in the case of Petri nets, which is often used to perform dynamic reliability analysis, a dynamic system's structure and behavior have to be manually translated (as of now) to a Petri net to perform reliability analysis. Petri net and similar methods like dynamic event tree would fall into this category. In SCM since it uses object-oriented representation, which is closer to the system's design description/representation; this method would require the least reliability expertise to perform dynamic reliability analysis (would be the other category). Future methods which would automatically translate a system description/representation into a reliability model or automatically generate reliability metrics would fall into the latter category.

In this paper, we perform a comparative study of the dynamic reliability modeling of shutdown system of fast breeder reactor with Petri net model as well as the newly proposed SCM to bring out the differences and advantages of these two methods. The running time and ease of modeling aspects are brought out.

I. INTRODUCTION

Dynamic reliability analysis methods can incorporate dynamics associated with the process, hardware, software, and human actions and their interactions into reliability modeling. Various dynamic reliability methods have been developed in last two decades, and they have shown better modeling in comparison to the widely used traditional reliability methods such as Fault Tree/Event Tree (FT/ET). Often the reliability model of the system is not unique and is dependent on the analyst's skill. Even though various dynamic reliability methods have been developed, they have not attempted to solve the challenge of the correctness of modeling. (The burden of proof) We believe that it is the restriction for the wide-spread use of dynamic reliability methods. The key to success for such a development is to keep modeling of a dynamic system simple and intuitive. This is done by structuring the model as close to the actual one. The powerful modeling technique developed by C. A. Petri –Petri Nets (PN) is considered as a generic method for dynamic reliability analysis. For system analysis through PN, a dynamic system needs to be translated manually into a PN model. However, without sufficient proficiency and experience, PN modeling is difficult. Recently, a Smart Component Methodology (SCM) is developed at Indira Gandhi Centre for Atomic Research (IGCAR) for dynamic reliability analysis. The method is based on the object-oriented representation of the system structure and behavior. The methodology has been demonstrated for dynamic reliability estimation of example systems as well as industrial scale dynamic systems.[1,2] In this paper, the aim is to compare reliability modeling using PN and SCM methods. For the comparative evaluation, a shutdown system (SDS)[3] of a fast breeder reactor is selected. The system consists of redundant trains of subsystems (2 by 3

voting logic) and dependencies. PN and SC model of the SDS is developed incorporating these features. The computational time, modeling complexity is compared, and correctness verification aspects are discussed for the two methods.

Section II describes the two methods briefly. Section III describes the SDS. Section IV presents results and discussion. Section V concludes the comparison.

II. METHODOLOGY

In this section, Petri nets (PN) modeling is described in brief, and then the Smart Component Methodology (SCM) is presented.

II.A. Petri Net

PN is a graphical simulation method. It consists of places (circles), transitions (rectangles), arcs (arrows), and tokens. Places represent the state (discrete or continuous). Places are connected to one or many transition box using the arc. Transitions are fired when all its incoming places are having tokens greater than or equal to the weight of the arc. The weight of the transition arcs is given near to the arc in the square bracket. The numbers in the square bracket in places represent the number of tokens the place is holding. After firing of transition, the tokens are transferred from the incoming places to the outgoing places. Fig. 2 and 3 shows a PN model of SDS. Quantification of availability or reliability is estimated from the amount of time tokens are staying in the failed state and failure frequency is estimated from the number of times the transitions take place. For the execution of the nets, the MCS technique is used.

TABLE I. Elements of Petri Nets

	Place
	Transition -Timed/Instant/Cyclic
	Transition arc
[#]	Token
	Inhibitor arc

II.A.1. Common cause failure model in PN

The group based beta factor model of CCF for multiple common causes is implemented in PN. Components having a common cause for failure are grouped, and a representative component is selected for applying beta factor. The application of the beta factor is carried out using a failure transition from the representative component in the PN, which upon firing fails all the components of the CCF group. The firing of a CCF transition adds tokens in the CCF-flag-places, i.e., outgoing places. The CCF flag places activate the failure transition of the other working components of the same CCF group. Since the other than the representative component can be in working or failed, the flag places are required to conserve token in the component level PN. This PN CCF model is used in Fig. 2 and 3 for the PN models of SDS.

II.A.2. Hierarchical modeling in PN

Hierarchical modeling is used to build PN for a large system. Here, in hierarchical modeling, first, the component level model is built. The intermediate levels are determined based on the connections of the components. For example, for a series-parallel system, the first level is component level; the second level could be serially connected components. Next level would be aggregating the parallel groups. The exact nature would depend on the series-parallel configuration. The hierarchical technique is used to avoid largeness problems in PN.[4] The hierarchical modeling is illustrated in Fig. 2 and 3 for the PN models of the SDS.

II.B. Smart Component Methodology

SCM uses an object-oriented design for system structuring and MCS for reliability quantification. The simplified framework of the methodology is given in Fig. 1. The procedure for reliability evaluation of a dynamic system using SCM is of two steps, i.e., first, system structuring – building SC model, and second, reliability evaluation using SC simulator. As shown in Fig. 1, the SCM has an object model of the system, a set of global rules, a connector and simulator. The object model of the system consists of the description of all the components. The description of the components includes its attributes and functional behaviors. Attributes specify the reliability parameters, physical process variables, and, the state of the component. The function of the component is described in the component object itself. Connector table represents the interconnections of the components of the system. The global rule object is for encoding, system failure criteria, output monitoring for detection of the failure, simulation sequence for the system simulation. The object model, connector and global rule of a system together make an SC model of the system. The SC simulator operates on the SC model and estimates the reliability metrics. Since MCS can handle in principle any level of complexity, the simulator is based on MCS algorithms.

Two types of component reliability models are considered, i.e., (i) continuous and (ii) tested, e.g., see Table II second column. In the continuous model, the component is continuously monitored, and upon failure, repair is started immediately. The continuous model described using two states, i.e., 1=working, and 0=repair.

In the tested model, repair of the component is not started immediately, since the failure of the component is undetected, the component is tested periodically. Periodic tests are conducted at an interval of τ (hrs). So if the component is found in the failed state, then it is transferred to repair state with repair rate (μ). Hence, the tested reliability model consists of three states, i.e., 1=working, 0=fail, and 2=repair. It is assumed that the failure rate (λ), repair rate (μ) and test interval (τ) of the components are constant in the study. The tested model is used to represent the probability of failure on demand, which is explained in the next section.

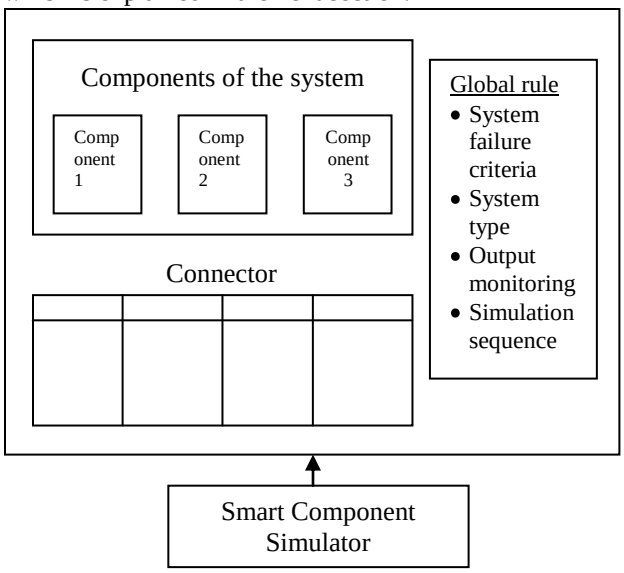

Fig. 1. Smart Component Framework

III. SHUTDOWN SYSTEM[3]

The shutdown system (SDS) of an FBR is a safety system used to shut down the reactor in detectable abnormal conditions. This system needs to have high reliability. Hence, SDS is designed with diverse physical detection and processing redundancy. The SDS of FBR consists of two subsystems, i.e., SDS1 and SDS2. For an illustration of the methods, in this paper, SDS2 is selected for reliability modeling. Fig. 3 presents SDS2 in block diagram format. From hereafter SDS2 is termed as SDS.

SDS consists of three TC (Thermo couple, to measure temperature in the core), three analog signal processing (ASP) circuits (to condition and process the signal from the sensors), and three comparators (to compare the signal with the threshold. The thresholds are set manually.), a pulse coded safety logic (for automatic decision making from the three channels. It is used for 2 by 3 voting mode.). These equipments are considered together as the Reactor Protection System (RPS). The signal for tripping the reactor is given by the RPS to the Actuation System (AS). The AS is consists of three pairs of parallel scram switches (switches are used to scram the reactor by magnetically dropping the safety rods), and three diverse safety rods (The safety rods are hung at the top of the reactor. Based on the signal from RPS they are dropped into the core.) The design of the rods is such that the dropping of two or more safety rods is considered success in case of temperature crossing the safety limits. Reliability models of each of the components and typical reliability parameters are given in Table II. It is to be noted that the reliability modeling of human error, considered in the manual setting of the reference in the comparators, is to be modeled using the probability of failure-on-demand. The human error probability for setting reference for the comparator is assumed to be 1E-5 on demand. The tested reliability model, discussed in the previous section, is used for incorporating the probability of failure on demand (p_f) in the availability estimation. That is, $p_f = \lambda[(\tau/2) + (1/\mu)]$, where τ and μ are chosen arbitrarily to derive λ. For example, see Table II, row eight, here, for the human error probability of 1E-5, with τ

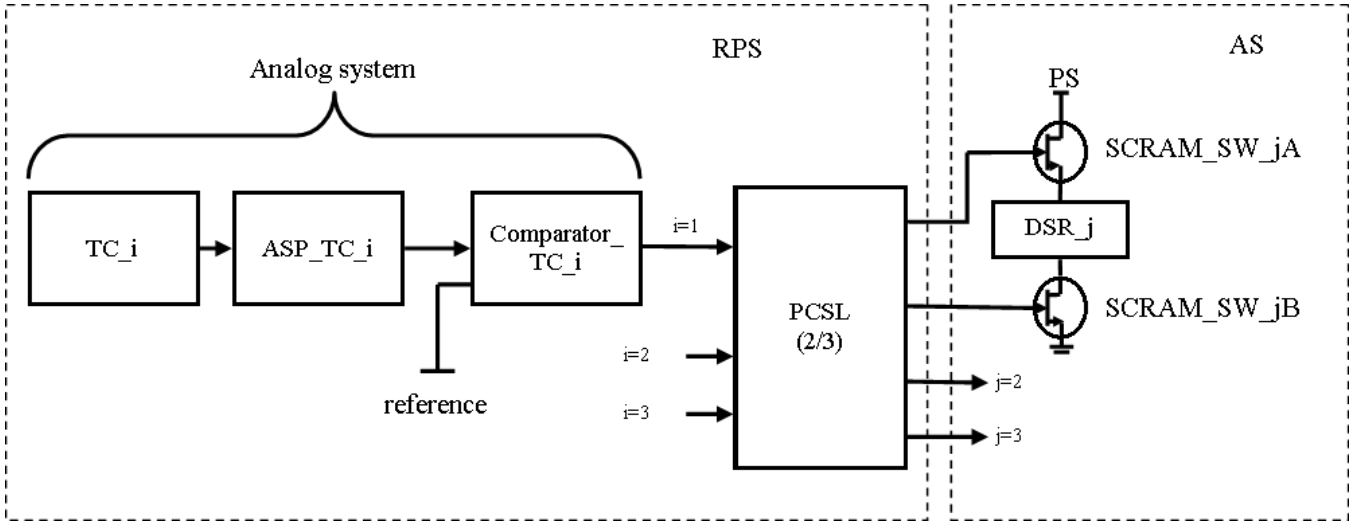

Fig. 2. Shutdown system

and μ be 24 hrs and .25 hr^{-1}respectively, λ is 6.25E-7 hr^{-1}. Since only one human is modeled CCF is not applied in row eight.

TABLE II. Reliability Parameters of the Components of SDS

Component	Reliability model	Reliability parameters ($\lambda(hr^{-1})$, $\mu(hr^{-1})$, $\tau(hr)$)	CCF Group (Beta)
TC	Continuous	1.6E-6, 1E-2	1 (5)
ASP	Continuous	3E-6, 2.5E-1	2 (5)
Comparator	Tested	2E-7, 2.5E-1, 24	3 (10)
PCSL	Continuous	1E-7, 2.5E-1	-
Scram SW	Tested	1E-6, 2.5E-1, 0.05	4 (1)
DSR	Tested	1.38E-8, 2.5E-1, 4320	5 (10)
Human error	Tested	6.25E-7, 2.5E-1, 24	-

IV. RESULTS AND DISCUSSIONS

IV.A. Petri Net

As mentioned earlier, the PN model of the SDS is built using the hierarchical technique. See Fig. 3 and 4 for the PN model of RPS and AS respectively. First, each component of SDS (red outlines) is built based on their reliability model described in Sec. III. The continuous reliability model is presented using two places (P1, P0) and two transitions. Similarly, the tested model is presented using three places (P1, P0, P2) and three transitions. The transition rates between the places are represented as failure rate (between P1 to P0), repair rates (between P2 to P1 or P0 to P1) and test interval (P0 to P2). The transition rates are represented using timed transitions, and the periodic test intervals are represented using cyclic transitions of the PN. The subsequent hierarchy levels, i.e., after the first level, are represented using only the instant transitions of the PN (green, blue etc). Since the hierarchy level after the first is essential for system structuring, they are used to find the system success or failure. They are given in Table III. In the table series connection between components are given by '-', parallel connections are represented by '||' and, the dependency by ':'.

A transition (failure or repair) of a component will affect the state of the next level hierarchy it belongs to. So a transition in a hierarchy affects next to it. For example, let assume that an ASP1 is failed in a transition, which is resulting in loosing of the token in ASP1P1 place (working) and adding a token in ASP1P0 place (failed). Token in ASP1P0 activates the instant transitions of next level hierarchy it is in, i.e., it activates the failure transition of [TC-ASP], since the series connection of TC and ASP is failed if either of the two is failed. Further, failure of [TC-ASP] results in the failure of next level transition, i.e., [{TC-ASP}-{COMP:HER}]. The next level transitions are not activated since the 2 by 3 success is met. Hence the system is not failed. Similarly, the failure effects are propagated through the instant transitions of subsequent hierarchy levels up to the system level. Hence, system success and failure are determined. The procedure is simulated randomly for a large number of transitions and the amount of time tokens present in all places are determined to calculate unavailability and, the number of times the transition triggered gives the measure for failure frequency.

TABLE III. Hierarchical Model of the SDS

Hierarchy level	Group of components
1	[TC], [ASP], [COMP], [PCSL], [SCRAM SW], [DSR], [HER]
2	[TC - ASP], [COMP:HER], [SCRAM SW 1 || SCRAM SW 2]
3	[{TC-ASP}-{COMP:HER}], [{SCRAM SW 1 || SCRAM SW 2} – {DSR}]
4	[{(TC-ASP)-(COMP:HER)} – {PCSL} – {(SCRAM SW 1 || SCRAM SW 2) – (DSR)}]

The modeling of CCF is carried out using the beta factor model applied to the representative component of the CCF groups. The CCF groups are indicated in Table II. The TC1, ASP1, COMP1, SCRAM SW1, and DSR1 are the representative components of the corresponding CCF group. A token in the representative component activates two failure modes, i.e., direct failure, and the CCF. The transition of the CCF mode fails all the component of the group at once.

IV.B. Smart Component Methodology

For reliability evaluation of SDS using SCM, in the first step, the object model of the system is built. Then, in the second step, SC simulator based on regenerative process simulation is used to estimate the steady state unavailability and failure frequency of the system and its components. The components of SDS are TC_i, ASP_i, $COMP_i$, PCSL, SCRAM $SW_{ij,}$ DSR_i, HER, where i = 1, 2, 3 and j = A, B. They are tabulated in Table IV-IX with their attributes and local rule respectively. The connector attributes between the components are tabulated in Table X. It manifests the interconnections between the components, i.e., for example, here, thermocouple sends an electrical signal to the signal processor if it is in working condition. This is given as the first entry in Table X. Due to space restriction, all the entry of connector are avoided, and only the representative entries are given.

The system is simulated by executing the local rules at each time steps following the predefined simulation sequence. For the SDS, it is intuitively given as simulation sequence = TC; ASP; COMP; PCSL; SCRAM SW; DSR. The success criterion is defined as the successful dropping of two or more DSRs. Since the system is operating continuously during the normal operating condition of the fast breeder reactor, the regenerative process model is used to estimate the reliability metrics.

TABLE IV. Thermo Couple Object

Parameters	Data
Hardware state	1
Reliability model	Continuous
Failure rate	1.6E-6
Repair rate	0.01
CCF	1
CCF ID	1
Beta	5%
Temperature	410
Electrical signal	350
Local rule	If state == 1 Then Electrical signal = Temperature End if

TABLE V. Analog Signal Processing Circuits

Parameters	Data
Hardware state	1
Reliability model	Continuous
Failure rate	3E-6
Repair rate	0.01
CCF	1
CCF ID	2
Beta	5%
Signal	150
Electrical signal	150
Local rule	If state == 1 Then Electrical signal = Signal End if

TABLE VI. Comparator Object

Parameters	Data
Hardware state	1
Reliability model	Tested
Failure rate	2E-7
Repair rate	0.25
Test interval	24
CCF	1
CCF ID	3
Beta	10%
Signal	1
Reference	1.1
Control signal	0
Local rule	If state == 1 Then If Signal > Reference Then Control signal = 1 End if End if

TABLE VII. Pulse Coded Safety Logic Object

Parameters	Data
Hardware state	1
Reliability model	Continuous
Failure rate	1E-7
Repair rate	0.25
CCF	0
Input 1	0
Input 2	0
Input 3	0
Output	0
Local rule	If state == 1 Then If Input1 + Input 2 + Input 3 >= 2 Then Output = 1 End if End if

TABLE VIII. Scram Switch Object

Parameters	Data
Hardware state	1
Reliability model	Tested
Failure rate	1E-6
Repair rate	0.25
Test interval	0.05
CCF	1
CCF ID	4
Beta	1%
Signal	0
Output	0
Local rule	If state == 1 Then Output = Signal End if

TABLE IX. Diverse Safety Rod Object

Parameters	Data
Hardware state	1

Reliability model	Tested
Failure rate	1.38E-6
Repair rate	0.041
Test interval	4320
CCF	1
CCF ID	5
Beta	10%
SW A	0
SW B	0
Position	UP
Local rule	If state == 1 Then If SW 1 == 1 or SW 2 ==1 Then Position = Down End if End if

TABLE X. Connector of SDS (i = 1, 2, 3, j = A, B)

OutComponent	OutAttribute	InComponent	InAttribute
TCi	Electrical Signal	ASPi	Signal
ASPi	Electrical Signal	COMPi	Measured Signal
COMPi	Control signal	PCSL	Inputi
PCSL	Output	SCRAM SWij,	Signal
SCRAM SWij	Output	DSRi	SWj

IV.C. Results and Discussions

The steady-state unavailability (Tables XI) and, failure frequency (Table XII) are estimated for the RPS, AS and SDS systems using both the PN and SCM. The average simulated time (T_s in hrs) per running time (T_w i.e. wall clock time in seconds) is measured (Table XIII). The simulation time is the time simulated by sampling and the running time is the time taken by a computer to perform simulations. All the simulations are performed in a Core 2 Duo processor with 2.53 GHz clock speed.

Simulation parameters for the SCM are:

- System simulation model = regenerative process
- Number of histories = 1E5 for RPS, 1E6 for both the AS and SDS
- Number of batches = 2

Simulation parameters for the simulation of PN models are:

- Number of steps for one simulation = 1E6
- Number of simulations = 2

As shown in the tables, the steady state unavailability ($\bar{A}$) and failure frequency results are matching well. Fractional error (f = standard deviation/mean) is calculated and compared. Hence, the SCM is validated with the equivalent PN model of the SDS. And, accuracy of both the methods is comparable. Moreover, the average simulation time per running time second ($\bar{t} = T_s/T_w$) is consistent for both the PN and SCM methods. Since the number of components increasing from RPS and AS to SDS, the average simulation time per second is decreasing in Table XIII, which demonstrates the consistent behavior of the methods. It may be noted that, SCM simulates more time per second than the PN for this application. This is because the determination of the system state in the object-oriented model is done through the propagation of the local rules (functions), which is a part of the system simulation. And the system state is checked using the global rule, i.e., here it is the dropping of the two or more DSRs. The PN probably takes more time due to the implementation of hierarchical modeling technique to manage complexity. In SCM, there is no hierarchical modeling. (Complexity is managed by OO paradigm itself.)

The modeling of multiple CCF of SDS increases the number of places and transitions in the PN model. While modeling the large system, the average simulation time per second is further reduces due to the consideration of additional transitions and places for triggering CCF in the group-based method. In addition to that, the PN model size is becoming complicated. In the contrary, as it can be seen from the Tables IV-IX, the SCM handles multiple CCF easily while structuring the object model. The object model of the CCF group is defined with the CCF group identification number and the beta factor. Hence, the burden of accurately considering the multiple CCF in the reliability evaluation is transferred to the SC Simulator engine rather than the analyst, like that in PN modeling.

Moreover, the definition of the SC model of SDS is more intuitive and simple, as can be seen from the Tables IV-X. That is, the component models and connector object constitute the system for evaluation using the simulator. It is experienced during the modeling in PN and SCM that the modification in the system is easy to implement in SCM than the PN since it is difficult to modify the large PN model. For example, a change in voting logic in a local rule of the PCSL component is easy to implement in SCM than that in the PN model.

PN model for flow of signal 1 (block-1)

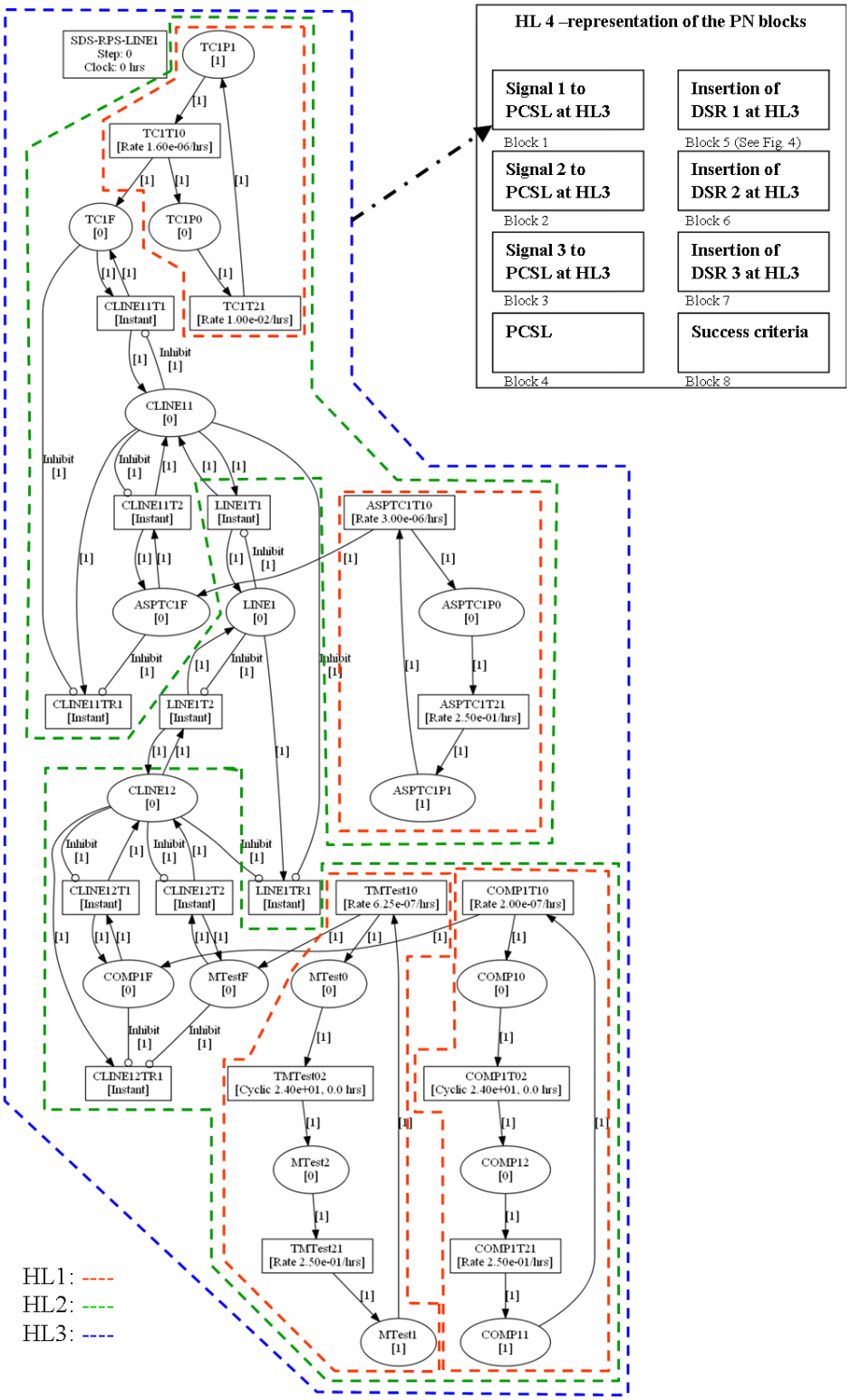

Fig. 3. PN modeling of signal-1 (temperature sensor) in HL3 level (block 1) is elaborated. HL1: component level described by red outline. HL2: series connections of (i) NS and ASP and (ii) comparator and human error in reference setting by green, and, HL3 by blue. The figure of the PN model is built using Macchiato PN [5] (MPN).

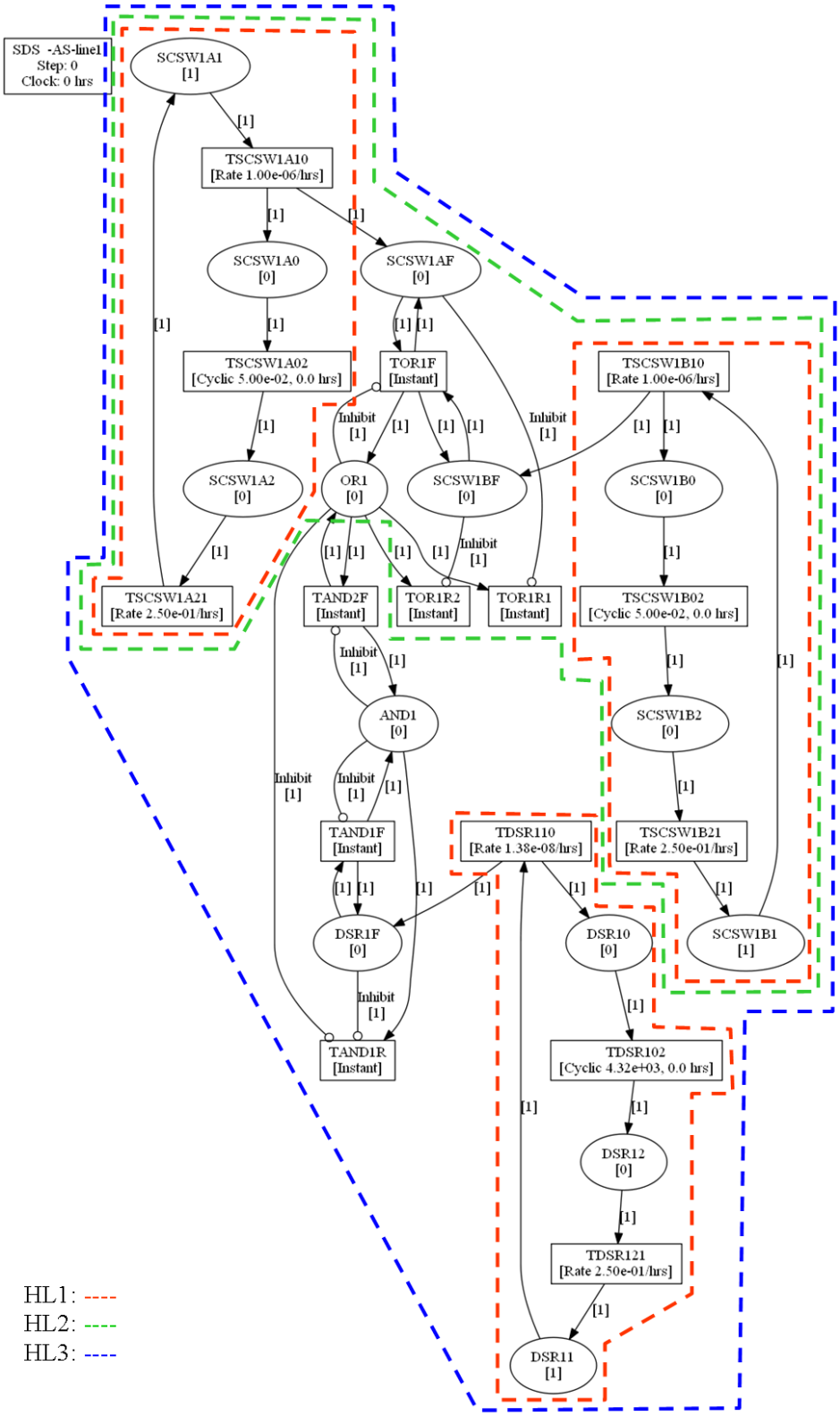

Fig. 4. PN model of insertion of DSR 1 (block 5) of SDS. HL1: component level described by red outline. HL2: parallel connections of two scram switches by green, and, HL3: successful insertion of DSR1 is subject to working of both two scram switches and dropping of DSR1 is covered by blue outline.

TABLE XI. Comparison of Steady State Unavailability Estimated From PN and SCM

System	PN		SCM	
	$\bar{A}$	f	$\bar{A}$	f
RPS	1.80E-05	9.09E-03	1.77E-05	1.61E-02
AS	2.58E-06	1.90E-01	3.08E-06	5.51E-02
SDS	2.15E-05	5.19E-02	2.08E-05	7.95E-03

TABLE XII. Comparison of Failure Frequency Estimated from PN and SCM

System	PN		SCM	
	Failure Freq. (/hr)	f	Failure Freq. (/hr)	f
RPS	9.75E-07	1.32E-03	9.68E-07	5.35E-03
AS	1.15E-08	6.03E-02	1.13E-08	2.61E-02
SDS	9.99E-07	1.28E-02	9.76E-07	1.01E-02

TABLE XIII. Comparison of Average Simulated Time (in hr) Per Running Time Second for PN and SCM

System	PN		SCM	
	T_s in hrs	$\bar{t}$ (hr/sec)	T_s in hrs	$\bar{t}$ (hr/sec)
RPS	9.55E+09	6.39E+06	6.61E+10	1.48E+07
AS	5.39E+10	1.52E+07	1.66E+11	2.79E+07
SDS	8.09E+09	2.01E+06	4.73E+10	4.61E+06

V. CONCLUSIONS

The reliability analysis of SDS is carried out using PN and SCM. PN model is built incorporating multiple CCF, component dependency, testing features of SDS, and, it is utilizing a hierarchical technique to avoid largeness problem in PN. The comparisons of the results show that both methods give similar results and similar fractional errors. This study also serves to validate the newly developed SCM. The modeling complexity of PN and SCM is compared, and it is found that the modeling of a system in SCM is simple and intuitive than that in PN. The running time comparison shows that SCM simulates faster than the PN.

ACKNOWLEDGMENTS

The authors thank Director, Reactor Design Group, IGCAR for their encouragement and support for completing the work. The first author thanks the Board of Research in Nuclear Studies, Mumbai, India, and Department of Atomic Energy, India for supporting through DGFS-PhD fellowship.

REFERENCES

1. Shukla, D. K. & Arul, A. J. A Smart Component Methodology for Reliability Analysis of Dynamic Systems. *Submitted for Publication.* (2018).
2. Shukla, D. K. & Arul, A. J. Development of Smart Component Based Framework for Dynamic Reliability Analysis of Nuclear Safety Systems. in *Int. Conf. Fast React. Relat. Fuel Cycles Next Gener. Nucl. Syst. Sustain. Dev.* 603 (2017).
3. Kumar, C. S., Arul, A. J., Singh, O. P. & Rao, K. S. Reliability analysis of shutdown system. *Ann. Nucl. Energy* 32, 63–87 (2005).
4. Sukhwani H., Bobbio A., Trivedi K. S., Largeness Avoidance in Availability Modeling using Hierarchical and Fixed-Point Iterative Techniques, *International Journal of Performability Engineering*, 11 (4) , 305-319 (2015).
5. Macchiato Petri Net software: developed by Mark Wootton and John D. Andrews, University of Nottingham, UK and email ID: mark.wootton@nottingham.ac.uk.