Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment

K. Durga Rao a,*, V. Gopika a, V.V.S. Sanyasi Rao a, H.S. Kushwaha a, A.K. Verma b, A. Srividya b

a Bhabha Atomic Research Centre, Mumbai, India
b Indian Institute of Technology Bombay, Mumbai, India

ARTICLE INFO

Article history:
Received 21 July 2007
Received in revised form 22 September 2008
Accepted 24 September 2008
Available online 11 October 2008

Keywords:
Dynamic fault trees
Markov models
Monte Carlo simulation
Probabilistic safety assessment
Reactor regulation system

ABSTRACT

Traditional fault tree (FT) analysis is widely used for reliability and safety assessment of complex and critical engineering systems. The behavior of components of complex systems and their interactions such as sequence- and functional-dependent failures, spares and dynamic redundancy management, and priority of failure events cannot be adequately captured by traditional FTs. Dynamic fault tree (DFT) extend traditional FT by defining additional gates called dynamic gates to model these complex interactions. Markov models are used in solving dynamic gates. However, state space becomes too large for calculation with Markov models when the number of gate inputs increases. In addition, Markov model is applicable for only exponential failure and repair distributions. Modeling test and maintenance information on spare components is also very difficult. To address these difficulties, Monte Carlo simulation-based approach is used in this work to solve dynamic gates. The approach is first applied to a problem available in the literature which is having non-repairable components. The obtained results are in good agreement with those in literature. The approach is later applied to a simplified scheme of electrical power supply system of nuclear power plant (NPP), which is a complex repairable system having tested and maintained spares. The results obtained using this approach are in good agreement with those obtained using analytical approach. In addition to point estimates of reliability measures, failure time, and repair time distributions are also obtained from simulation. Finally a case study on reactor regulation system (RRS) of NPP is carried out to demonstrate the application of simulation-based DFT approach to large-scale problems.

© 2008 Elsevier Ltd. All rights reserved.

1. Introduction

Fault tree (FT) analysis has gained wide spread acceptance for the quantitative reliability and safety analysis. FT is graphical representation of various combinations of basic failures that lead to the occurrence of undesirable top event. Starting with the top event all possible ways for this event to occur are systematically deduced. The methodology is based on three assumptions: (i) events are binary events, (ii) events are statistically independent, and (iii) relationship between events are represented by means of logical Boolean gates (AND, OR, and Voting). The analysis is carried out in two steps: a qualitative step in which the logical expression of the top event is derived in terms of prime implicants (the minimal cut-sets); a quantitative step in which on the basis of the probabilities assigned to the failure events of the basic components, the probability of occurrence of the top event is calculated.

The traditional static fault trees with AND, OR, and Voting gates cannot capture the dynamic behavior of system failure mechanisms such as sequence-dependent events, spares and dynamic redundancy management, and priorities of failure events. In order to overcome this difficulty, the concept of dynamic FTs is introduced by adding sequential notion to the traditional FT approach. System failures can then depend on component failure order as well as combination [1]. This is done by introducing dynamic gates into FTs. With the help of dynamic gates, system sequence-dependent failure behavior can be specified using dynamic FTs that are compact and easily understood. The modeling power of dynamic FTs has gained the attention of many reliability engineers working on safety critical systems [2].

Several researchers [1–3] proposed methods to solve dynamic FTs. Dugan et al. [1,4,5], has shown through a process known as modularization, it is possible to identify the independent sub-trees with dynamic gates and to use different Markov model for each of them. It was applied to computer-based fault tolerant systems successfully. But, with the increase in the number of basic elements, there is problem state space explosion. To reduce state space and minimize the computational time, an improved
decomposition scheme where the dynamic sub-tree can be further modularized (if there exist some independent sub-trees in it) is proposed by Huang and Chang [6]. Amari et al. [2], proposed a numerical integration technique for solving dynamic gates. Though, this method is solving the state-space problem, it cannot be easily applied for repairable systems. Bobbio et al. [3,7], proposed Bayesian network-based method to further reduce the problem of solving dynamic FTs with state-space approach. Keeping the importance of sophisticated modeling for engineering systems in dynamic environment, several researches [8–11] contributed significantly to the development and application of dynamic FTs.

However, state-space approach for solving dynamic gates becomes too large for calculation with Markov models when the number of gate input increases. This is the case especially with probabilistic safety assessment (PSA) of nuclear power plant (NPP) where there is large number of cut sets. In addition, Markov model is applicable for exponential failure and repair distributions and also modeling test, maintenance information on spare components is difficult. Many of the methods to solve dynamic FTs are problem specific and it may be difficult to generalize for all the scenarios. In order to address some of these limitations of the above-mentioned methods, Monte Carlo simulation approach is attempted here to implement dynamic gates. Scenarios which may often be difficult to solve with analytical solutions are easily tackled with the Monte Carlo simulation approach. Monte Carlo simulation-based reliability approach, due to its inherent capability in simulating the actual process and random behavior of the system, can eliminate uncertainty in reliability modeling [12,13]. A software tool, Dynamic Reliability with SIMulation (DRSIM) is developed to do comprehensive dynamic FT analysis. Two reliability problems are solved with the tool and found that results are exactly matching with the analytical approaches. After validation of the approach, it is extended to a case study on RRS of NPP.

2. Dynamic fault tree analysis: dynamic gates

Dynamic fault trees (DFTs) introduces four basic (dynamic) gates: the priority AND (PAND), the sequence enforcing (SEQ), the standby or spare (SPARE), and the functional dependency (FDEP) [1]. They are discussed here briefly.

The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (from left to right in graphical notation). A SEQ gate forces its inputs to fail in a particular order: when a SEQ gate is found in a DFT, it never happens that the failure sequence takes place in different orders. While the SEQ gate allows the events to occur only in a pre-assigned order and states that a different failure sequence can never take place, the PAND gate does not force such a strong assumption: it simply detects the failure order and fails just in one case (in Fig. 1—PAND: failure occurs if A fails before B, but B may fail before A without producing a failure in G).

SPARE gates are dynamic gates modeling one or more principal components that can be substituted by one or more backups (spares), with the same functionality (Fig. 1). The SPARE gate fails when the number of operational powered spares and/or principal components is less than the minimum required. Spares can fail even while they are dormant, but the failure rate of an unpowered spare is lower than the failure rate of the corresponding powered one. More precisely, $\lambda$ being the failure rate of a powered spare, the failure rate of the unpowered spare is $\lambda z$, where $0 < z < 1$ is the dormancy factor. Spares are more properly called "hot" if $z = 1$ and "cold" if $z = 0$.

In the FDEP gate (Fig. 1), there will be one trigger-input (either a basic event or the output of another gate in the tree) and one or more dependent events. The dependent events are functionally dependent on the trigger event. When the trigger event occurs, the dependent basic events are forced to occur. In the Markov-chain generation, when a state is generated in which the trigger event is satisfied, all the associated dependent events are marked as having occurred. The separate occurrence of any of the dependent basic events has no effect on the trigger event.

3. Monte Carlo simulation-based approach for dynamic gates

Monte Carlo simulation is a very valuable method which is widely used in the solution of real engineering problems in many fields. Lately the utilization of this method is growing for the assessment of availability of complex systems and the monetary value of plant operations and maintenances [12–15]. The complexity of the modern engineering systems besides the need for realistic considerations when modeling their availability/reliability renders analytical methods very difficult to be used. Analyses that involve repairable systems with multiple additional events and/or other maintainability information are very difficult to solve analytically (dynamic FTs through state space, numerical integration, Bayesian network approaches). Dynamic FT through simulation approach can incorporate these complexities and can give wide range of output parameters.

Simulation technique estimates the reliability indices by simulating the actual process and random behavior of the system in a computer model in order to create a realistic lifetime scenario of the system. This method treats the problem as a series of real experiments conducted in a simulated time. It estimates the probability and other indices by counting the number of times an event occurs in simulated time. The required information for the analysis is: probability density functions (PDF) for time to failure and repair of all basic components with the parameter values; maintenance policies; interval and duration of tests and preventive maintenance.

Components are simulated for a specified mission time for depicting the duration of available (up) and unavailable (down) states. Up and down states will come alternatively, as these states are changing with time they are called state time diagrams. Down state can be due to unexpected failure and its recovery will

![Fig. 1. Dynamic gates.](image-url)
depend upon the time taken for repair action. Duration of the state is random for both up and down states. It will depend upon PDF of time to failure and time to repair, respectively.

3.1. Evaluation of time to failure or time to repair for state time diagrams

Consider a random variable $x$ is following exponential distribution with parameter $\lambda$, $f(x)$ and $F(x)$ are given by the following expressions:

$$f(x) = \lambda \exp(-\lambda x),$$
$$F(x) = \int_0^x f(x) \, dx = 1 - \exp(-\lambda x).$$

Now $x$ derived as a function of $F(x)$

$$x = G(F(x)) = \frac{1}{\lambda} \ln \left( \frac{1}{1-F(x)} \right).$$

A uniform random number is generated using any of the standard random number generators. Let us assume 0.8 is generated by random number generator then the value of $x$ is calculated by substituting 0.8 in place of $F(x)$ and say 1.8/yr ($5e^{-3}$/h) in place of $\lambda$ in the above equation

$$x = \frac{1}{5e^{-3}} \ln \left( \frac{1}{1-0.8} \right) = 321.8 \text{h.}$$

This indicates time to failure of the component is 321.8 h (see Fig. 2). This procedure is applicable similarly for repair time also and if the shape of PDF is different accordingly one has to solve for $G(F(x))$.

The four basic dynamic gates are solved here through simulation approach.

3.2. PAND gate

Consider PAND gate having two active components, A and B. Active component is the one which is in working condition during normal operation of the system. Active components can be either in success state or failure state. Based on the PDF of failure of component, time to failure is obtained from the procedure mentioned above. The failure is followed by repair whose time depends on the PDF of repair time. This sequence is continued until it reaches the predetermined system mission time. Similarly for the second component also state time diagrams are developed.

For generating PAND gate state time diagram, both the components state time profiles are compared. The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (usually from left to right). As shown in Fig. 3 (first and second scenarios), when the first component failed followed by the second component, it is identified as failure and simultaneous down time is taken into account. But, in third scenario of Fig. 3, both the components have failed simultaneously but second component has failed first hence it is not considered as failure.

3.3. Spare gate

Spare gate will have one active component (say A) and remaining spare components (say B). Component state-time diagrams are generated in a sequence starting with the active component followed by spare components in the left to right order. The steps are as follows:

(i) Active components: Time to failures and time to repairs based on their respective PDFs are generated alternatively till they reach mission time.
(ii) Spare components: When there is no demand, it will be in standby state or may be in failed state due to on-shelf failure. It can also be unavailable due to test or maintenance state as per the scheduled activity when there is a demand for it. This makes the component to have multi-states and such stochastic behavior needs to be modeled to represent the practical scenario. Down times due to the scheduled test and maintenance policies are first accommodated in the component state-time diagrams. In certain cases test override probability has to be taken to account for its availability during testing. As the failures occurred during standby period cannot be

![Fig. 2. Exponential distribution.](image)

![Fig. 3. PAND gate state-time possibilities.](image)
revealed till its testing, time from failure till identification has to be taken as down time. It is followed by imposing the standby down times obtained from the standby time to failure PDF and time to repair PDF. Apart from the availability on demand, it is also required to check whether the standby component is successfully meeting its mission. This is incorporated by obtaining the time to failure based on the operating failure PDF and is checked with the mission time, which is the down time of active component. If the first standby component fails before the recovery of the active component, then demand will be passed on to the next spare component.

Various scenarios with the spare gate are shown in Fig. 4. The first scenario shows, demand due to failure of the active component is met by the stand-by component, but it has failed before the recovery of the active component. In the second scenario, demand is met by the stand-by component. But the stand-by failed twice when it is in dormant mode, but it has no effect on success of the system. In the third scenario, stand-by component is already in failed mode when the demand came, but it has reduced the overall down time due to its recovery afterwards.

3.4. FDEP gate

The FDEP gate's output is a 'dummy' output as it is not taken into account during the calculation of the system's failure probability. When the trigger event (T) occurs, it will lead to the occurrence of the dependent event (say A and B) associated with the gate. Depending upon the PDF of the trigger event, failure time, and repair times are generated. During the down time of the trigger event, the dependent events will be virtually in failed state though they are functioning. This scenario is depicted in Fig. 5. In the second scenario, the individual occurrences of the dependent events are not affecting the trigger event.

Various scenarios with the spare gate are shown in Fig. 4. The first scenario shows, demand due to failure of the active component is met by the stand-by component, but it has failed before the recovery of the active component. In the second scenario, demand is met by the stand-by component. But the stand-by failed twice when it is in dormant mode, but it has no effect on success of the system. In the third scenario, stand-by component is already in failed mode when the demand came, but it has reduced the overall down time due to its recovery afterwards.

3.4. FDEP gate

The FDEP gate's output is a 'dummy' output as it is not taken into account during the calculation of the system's failure probability. When the trigger event (T) occurs, it will lead to the occurrence of the dependent event (say A and B) associated with the gate. Depending upon the PDF of the trigger event, failure time, and repair times are generated. During the down time of the trigger event, the dependent events will be virtually in failed state though they are functioning. This scenario is depicted in Fig. 5. In the second scenario, the individual occurrences of the dependent events are not affecting the trigger event.
3.5. **SEQ gate**

It is similar to PAND gate but occurrence of events are forced to take place in a particular fashion. Failure of first component forces the other components to follow. No component can fail prior to the first component. Consider a three input SEQ gate having repairable components. The following steps are involved with Monte Carlo simulation approach.

1. Component state time profile is generated for first component based upon its failure and repair rate. Down time of first component is mission time for the second component. Similarly the down time of second component is mission time for the third component.
2. When first component fails, operation of the second component starts. Failure instance of the first component is taken as \( t = 0 \) for second component. Time to failure (TTF2) and time to repair/component down time (CD2) is generated for second component.
3. When second component fails, operation of the third component starts. Failure instance of the second component is taken as \( t = 0 \) for third component. Time to failure (TTF3) and time to repair/component down time (CD3) is generated for third component.
4. The common period in which all the components are down is considered as the down time of the SEQ gate.
5. The process is repeated for all the down states of the first component (Fig. 6).

### 4. Validation with examples

#### 4.1. Example 1—DFT problem from Ref. [2]

Consider a PAND gate with AND and OR gates as inputs (see Table 1 and Fig. 7). Amari et al. [2] suggested an approach based on the numerical integration technique to solve this problem and compared it with Markov-model approach. For mission time 1000 h, the top event probability is 3.6e\(-1\), and overall computation time is less than 1.0e\(-2\) s. State-space approach generated 162 states and computation time is 25 s. However, both the methods need lot of time for the development of analytical expression and multiple states, respectively. Once the analytical

<table>
<thead>
<tr>
<th>Gate</th>
<th>Failure rate of basic events</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>1.1(\times)10(-2)</td>
</tr>
<tr>
<td>OR</td>
<td>1.1(\times)10(-3)</td>
</tr>
</tbody>
</table>

**Table 1** Failure data for the basic events

![Fig. 7. Fault tree having dynamic gate (PAND).](image_url)

![Fig. 8. Failure time distributions.](image_url)
expression is developed, calculation is straightforward. However, the former method is limited for non-repairable basic events only. The disadvantage with the later method is number of states in the Markov model which increases exponentially as the number of basic events increase. Solution to this problem has been obtained with the simulation approach as explained in the previous section. Simulation is carried out for 10,000 iterations with a mission time of 1000 h. The top event probability is obtained same as Amari et al. [2] method. Apart from the mean value of failure probability, randomness in the failure time is characterized by the probability distribution as shown in Fig. 8. Mean time to failure is obtained as 290.1 h with simulation approach.

4.2. Example 2—simplified electrical (AC) power supply system of typical NPP

Electrical power supply is essential in the operation of process and safety system of any NPP. Grid supply (off-site-power supply) known as Class IV supply is the one which feeds all these loads. To ensure high reliability of power supply, redundancy is provided with the diesel generators known as Class III supply (also known as on-site emergency supply) in the absence of Class IV supply to supply the loads. There will be sensing and control circuitry to detect the failure of Class IV supply which triggers the redundant Class III supply [16]. Loss of off-site power supply (Class IV) coupled with loss of on-site AC power (Class III) is called station blackout. In many PSA studies [17], accident sequences resulting from station blackout conditions have been recognized to be significant contributors to the risk of core damage. For this reason the reliability/availability modeling of AC Power supply system is of special interest in PSA of NPP.

The reliability block diagram is shown in Fig. 9. Now this system can be modeled with the dynamic gates to calculate the unavailability of overall AC power supply of a NPP. The dynamic FT (Fig. 10) has one PAND gate having two events, namely, sensor and Class IV. If sensor fails first then it will not be able to trigger the Class III, which will lead to non-availability of power supply. But if it fails after already triggering Class III due to occurrence of Class IV failure first, it will not affect the power supply. As Class III is a stand-by component to Class IV, it is represented with a spare gate. This indicates their simultaneous unavailability will lead to supply failure. There is a FDEP gate as the sensor is the trigger signal and Class III is the dependent event.

This system is analyzed using both analytical and Monte Carlo simulation approaches.

4.2.1. Solution with analytical approach

Station blackout is the top-event of the FT (Fig. 10). The failure of sensor and Class IV is modeled by PAND gate in the FT. This is solved by state-space approach by developing Markov model as shown in Fig. 11. The bolded state where both the components failed in the required order is the unavailable state and remaining states are all available states. ISOGRAPH software has been used to solve the state-space model.

Dynamic gates can be solved by developing state-space diagrams and their solutions give required measures of reliability. However, for sub-systems which are tested (surveillance), maintained, and repaired if any problem is identified during check-up,
cannot be modeled by state-space diagrams. Though, there is a school of thought that initial state probabilities can be given as per the maintenance and demand information, this is often debatable. A simplified time averaged unavailability expression is suggested in IAEA P-4 [18] for stand-by subsystems having exponential failure/repair characteristics. The same is applied here to solve stand-by (SPARE) gate. If $Q$ is the unavailability of stand-by component, it is expressed by the following equation:

$$Q = \frac{1}{C_0} \left[ \frac{1 - e^{-\lambda T}}{\lambda T} + \frac{T}{\tau} + [f_m T_m] + [\lambda T_r] \right],$$

where $\lambda$ is failure rate, $T$ is test interval, $\tau$ is test duration, $f_m$ is frequency of preventive maintenance, $T_m$ is duration of maintenance, and $T_r$ is repair time. It is sum of contribution from failures, test outage, maintenance outage and repair outage. In order to obtain the unavailability of stand-by gate, unavailability of Class IV is multiplied with the unavailability ($Q$) of stand-by component Class III.

Input parameter values used in the analysis are shown in Table 2 [19]. The sum of the both the values (PAND and SPARE) give the unavailability of station blackout scenario which is obtained as $4.8 \times 10^{-6}$.

### Table 2
Component failure and maintenance information

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure rate (h)</th>
<th>Repair rate (h)</th>
<th>Test period (h)</th>
<th>Test time (h)</th>
<th>Maint. period (h)</th>
<th>Maint. time (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class IV</td>
<td>$2.3 \times 10^{-4}$</td>
<td>2.6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sensor</td>
<td>$1.0 \times 10^{-4}$</td>
<td>2.5 $\times 10^{-1}$</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Class III</td>
<td>$5.3 \times 10^{-4}$</td>
<td>8.7 $\times 10^{-2}$</td>
<td>168</td>
<td>8.3 $\times 10^{-2}$</td>
<td>2160</td>
<td>8</td>
</tr>
</tbody>
</table>

4.2.2. Solution with Monte Carlo simulation

As one can see Markov model for a two-component dynamic gate is having 5 states with 10 transitions, thus state space becomes unmanageable as the number of components increases. In case of stand-by components, the time-averaged analytical expression for unavailability is only valid for exponential cases.
To address these limitations, Monte Carlo simulation is applied here to solve the problem.

In simulation approach, random failure/repair times from each components failure/repair distributions are generated. These failure/repair times are then combined in accordance with the way the components are reliability-wise arranged with in the system. As explained in the previous section, PAND gate and SPARE gate can easily be implemented through simulation approach. The difference from normal AND gate to PAND and SPARE gates is that the sequence of failure has to be taken into account and stand-by behavior including the testing, maintenance, dormant failures have to be accommodated. The unique advantage with simulation is incorporating non-exponential distributions and eliminating S-independent assumption.

Component state-time diagrams are developed as shown in Fig. 12 for all the components in the system. For active components which are independent, only two states will be there, one is functioning state (up—operational state), and second is repair state due to failure (down—repair state). In the present problem, Class IV and sensor are active components where as Class III is stand-by component. For Class III, generation of state-time diagrams of state of Class IV is checked. DRSIM tool developed by authors has been used for implementing this problem. Unavailability obtained is 4.8e–6 for a mission time of 10,000 h with 10^6 simulations. This is in good agreement with the analytical solution obtained in Section 4.2.1. Failure time, repair time, and unavailability distributions for the system are shown in Figs. 13–15, respectively.

4.3. Sensitivity of system reliability results to dynamic gate representation

Evaluating dynamic gates and their modeling is resource intensive by both analytical and simulation approaches. It is important to see the benefit achieved while doing such analysis. This is the case especially with PSA of NPP where there are number of systems with many cut-sets. PAND and SEQ gates are special cases of static AND gate. Evaluations are carried out with different cases of input parameters to see the sensitivity of the results to the dynamic and static representations of a gate. Consider a two input for both the gates AND and PAND with their

<table>
<thead>
<tr>
<th>Case</th>
<th>Scenario</th>
<th>Unavailability</th>
<th>% difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A&lt;A &gt; B</td>
<td>8.2e-5</td>
<td>2.0e-3</td>
</tr>
<tr>
<td>2</td>
<td>A&lt;A &gt; B</td>
<td>1.9e-3</td>
<td>2.0e-3</td>
</tr>
<tr>
<td>3</td>
<td>A&lt;A &lt; B</td>
<td>4.5e-5</td>
<td>1.1e-3</td>
</tr>
<tr>
<td>4</td>
<td>A&lt;A &lt; B</td>
<td>1.9e-3</td>
<td>2.0e-3</td>
</tr>
</tbody>
</table>
 respective failure and repair rates as shown in Table 3. Unavailability has been evaluated for both the gates with different cases. It is interesting to note that for all these combinations, the static AND gate is yielding the result in the same order. However, the PAND gate differs by 2500% with AND gate in Cases 1 and 3, where \( \mu_A \neq \mu_B \). From these results it can be observed that irrespective of values of failure rates, the unavailability is found to be much less in case of dynamic gate when \( \mu_A \neq \mu_B \). The difference is marginal in other cases. Nevertheless, the system uncertainty bounds and importance measures can vary with the dynamic modeling in such scenarios. Dynamic reliability modeling reduces any uncertainties that may arise due to the modeling assumptions.

5. Case study: dual processor hot standby reactor regulation system (DPHS-RRS) of NPP

5.1. System description [20,21]

The dual processor hot standby reactor regulation system (DPHS-RRS) regulates reactor power (Fig. 16). It is a computer-based feedback control system. The regulating system is intended to control the reactor power at a set demand from \( 10^{-7} \text{FP} \) to 100% FP by generating control signal for adjusting the position of adjuster rods and adding poison to the moderator in order to supplement the worth of adjuster rods. This is achieved by controlling the movement of adjuster rods based upon difference between measured reactor power and set demand power. It consists of various sensors for measurement of power as well as for monitoring the actuation of reactivity devices. It actuates the reactivity devices to control the reactor power and to execute the setback and other functions.

The RRS has DPHS configuration with two systems namely, system A and system B. Each system shall comprise of dual microprocessors. All inputs (analog and digital or contact) are fed to system A as well as system B. The dual processors in each system shall perform all the functions in identical manner. These processors shall compare the signals at various levels for system diagnostics and information. However, only one processor may provide all the required outputs. Each of the system is capable of providing control signals for all the rods. Normally half of the total number of adjuster rods will be controlled by system-A and the remaining half by system-B. The other outputs are spare. On failure of system-A or -B, control transfer unit (CTU) shall automatically change over the control from system-A to system-B vice versa, if the system to which control is transferred is healthy. Control transfer shall also be possible through manual command by an external switch. This command shall be ineffective if the system, to which control is desired to be transferred, is declared unhealthy. Transfer logic shall be implemented through CTU. All the adjuster rods shall be given a signal to drive them “IN” in the event of failure of both systems A and B. To summarize, the above described computer-based system has failures needs to happen in a specific sequence, to be declared as system failure. Dynamic FT should be constructed for realistic reliability assessment. The parameter of interest is the frequency of failure to control one set of regulating rods, considering only the computerized logic involved.

5.2. Dynamic fault tree modeling

The important issue that arises in modeling is the dynamic sequence of actions involved in assessing the system failure. The top event for RRS, “failure of reactor regulation”, will have following sequence of failures to occur:

1. computer system A or B fails
2. transfer of control to hot standby system by automatic mode through relay switching and CTU fails
3. transfer of control to hot standby system by manual mode through operator intervention and hand switches fails after the failure of auto mode.

PAND and SEQ gate are used, as shown in Fig. 17, to model these dynamic actions. PAND gate has two inputs, namely, auto transfer and system A/B failure. Auto transfer failure after the failure of system A/B does not affect as the switching action has already taken place. Sequence gate has two inputs, one from PAND gate and another from manual action. Chances of manual failure only arise after the failure of Auto and system A/B. Manual action
has four events, in which three are hand switch failures and one is operator error (OE). Auto has only two events, failure of control transfer unit and failure of relay. System A/B has 17 basic events and failure of any these basic events will lead to the failure, represented with OR gate.

5.3. Results and discussion

Failure in RRS can initiate loss of regulation accident (LORA) in NPP. This event calls for reactor trip to prevent core damage type of accident. Since the contribution to core damage is considerable, the reliability of computer-based systems in safety critical system needs to be ensured to a great degree. Hence, the failure of this event has significant effect on plant risk. This demand for a comprehensive approach for handling all issues in modeling computer-based systems for PSA.

The dynamic FT of RRS has been evaluated using the tool DRSIM, comprehensive code developed at BARC for dynamic FT analysis using Monte Carlo simulation approach. There are 500 number of minimal cut sets obtained. Unlike the earlier two problems presented in Section 4, the FT of RRS has some cut sets containing two dynamic gates, PAND and SEQ. The output of PAND is the input to SEQ gate. Simulation using the tool DRSIM has been carried out with mission time of 10,000 h and 10⁶ iterations. The component failure and repair information that is used in the quantification is shown in Table 4 [22]. LORA frequency has been found to be in the order of 3.7e⁻³/yr. The unavailability of RRS has been found to be 5e⁻⁶.

![Fig. 17. (a) Dynamic fault tree of DPHS-RRS, (b) sub-tree of DPHS-RRS, (c) sub-tree of DPHS-RRS and (d) sub-tree of DPHS-RRS.](image-url)
In order to simplify the complex reliability problems, conventional approaches make many assumptions to make it to a simple mathematical model. Use of dynamic FT approach eliminates many of the assumptions that are inevitable with conventional approaches to model the complex interactions. It is found that in certain scenarios, assuming static AND in place of PAND can give erroneous results by several orders. This is explained in the paper with an example (PAND/AND with two inputs). The difference in the results is significant where the repair rate of first component is larger than the second component (repair time of first component is smaller than the second), irrespective of their failure rates.

The solution for dynamic gates through analytical approaches such as Markov models, Bayesian Belief methods, and numerical methods have limitations in terms of number of basic events, non-exponential failure or repair distributions, incorporating test and maintenance policies and in a situation where the output of one dynamic gate being input to another dynamic gate. Monte Carlo simulation-based dynamic FT approach, due to its inherent capability in simulating the actual process and random behavior of the system, can eliminate these limitations in reliability modeling. Although computational time is the constraint, the incredible development in the computer technology for data processing at unprecedented speed levels is further emphasizing the use of simulation approach to solve dynamic reliability problems.

### Table 4
Failure and repair information of RRS system

<table>
<thead>
<tr>
<th>Sl. no.</th>
<th>Component name</th>
<th>Description</th>
<th>Failure rate (h) or Prob.</th>
<th>Repair rate (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CTU</td>
<td>CTU Logic card &amp; switch board failure</td>
<td>5.4e−6</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>RLYS-1</td>
<td>Relays fail to transfer (22 nos.)</td>
<td>5.2e−4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>HS-136F, HS-138F, HS-139F</td>
<td>Hand switch failure</td>
<td>1.0e−3</td>
<td>–</td>
</tr>
<tr>
<td>4</td>
<td>OE</td>
<td>Operator error</td>
<td>1.0e−1</td>
<td>–</td>
</tr>
<tr>
<td>5</td>
<td>ADA27</td>
<td>Analog data acquisition module</td>
<td>6.7e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>6</td>
<td>ANAMB-P16</td>
<td>Analog Motherboard P1 module</td>
<td>3.2e−7</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>7</td>
<td>ANAMB-P17</td>
<td>Analog motherboard P2 module</td>
<td>3.2e−7</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>8</td>
<td>CPU86-102, CPU86-105</td>
<td>Main processor module</td>
<td>9.5e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>9</td>
<td>DIFIT31, DIFIT32</td>
<td>Digital input with FIT module</td>
<td>1.0e−5</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>10</td>
<td>DOSCB-1-DCHS5, DOSCB-1-DCHS5</td>
<td>Dual O/P signal conditioning module</td>
<td>7.0e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>11</td>
<td>DPMBMB-P31, DPMBMB-P32</td>
<td>Dual processor bus motherboard P1 module</td>
<td>4.3e−7</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>12</td>
<td>ISOCTX31, ISOCTX32</td>
<td>Isolated current transmitter module</td>
<td>8.1e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>13</td>
<td>MEM527</td>
<td>Memory module</td>
<td>3.9e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>14</td>
<td>RORB31, RORB32</td>
<td>Relay O/P with read back mode</td>
<td>2.9e−6</td>
<td>4.1e−2</td>
</tr>
<tr>
<td>15</td>
<td>SMM-271</td>
<td>Supply monitoring module</td>
<td>4.4e−6</td>
<td>4.1e−2</td>
</tr>
</tbody>
</table>

### 6. Conclusions

In order to simplify the complex reliability problems, conventional approaches make many assumptions to make it to a simple mathematical model. Use of dynamic FT approach eliminates many of the assumptions that are inevitable with conventional approaches to model the complex interactions. It is found that in certain scenarios, assuming static AND in place of PAND can give erroneous results by several orders. This is explained in the paper with an example (PAND/AND with two inputs). The difference in the results is significant where the repair rate of first component is larger than the second component (repair time of first component is smaller than the second), irrespective of their failure rates.
In this work all the basic dynamic gates (PAND, SEQ, SPARE, and FDEP) have been implemented with Monte Carlo simulation approach. A tool for carrying dynamic FT analysis based on Monte Carlo simulation approach, DRSIM, has also been developed. The developed simulation approach has been validated with dynamic reliability problems. In the example 1, the simulation result is compared with numerical integration technique. The top event probability is found to be in good agreement. However, it is found that this analytical technique based on numerical integration approach would be difficult to be applied for repairable systems. The example 2 (typical electrical power supply scheme of NPP), which contained repairable and standby tested systems, has been solved with both analytical and simulation approaches. Though Markov model could solve PAND gate, incorporating surveillance testing and preventive maintenance information with the SPARE gate is found to be not feasible. Moreover, the analytical approaches are difficult to be applied with non-exponential failure/repair distributions.

Importance of realistic modeling is further emphasized by applying the dynamic modeling to critical systems. Case study on RRS of NPP has been carried out to calculate frequency of initiating event LORA. The problem of output of one dynamic gate as input to another dynamic gate is addressed in this case study. The capability of simulation approach to solve large-scale problems is demonstrated with this application.

Acknowledgements

Authors are grateful to Dr. A.K. Ghosh, Mr. Vipin Saklani, and Mr. M. Pavan Kumar for the invaluable support provided during the development of DRSIM tool.

References