

A Stochastic Approach for the Analysis of Fault Trees with Priority AND Gates

Peican Zhu, Jie Han, Leibo Liu and Ming J. Zuo

Abstract—Dynamic fault tree (DFT) analysis has been used to account for the dynamic behaviors such as the sequence-dependent, functional-dependent and priority relationships among the failures of basic events. Various methodologies have been developed to analyze a DFT; however, most methods require a complex analytical procedure or a significant simulation time for an accurate analysis. In this paper, a stochastic computational approach is proposed for an efficient analysis of the top event’s failure probability in a DFT with priority AND (PAND) gates. A stochastic model is initially proposed for a two-input PAND gate and a successive cascading model is then presented for a general multiple-input PAND gate. A stochastic approach using the proposed models provides an efficient analysis of a DFT compared to an accurate analysis or algebraic approach. The accuracy of a stochastic analysis increases with the length of random binary bit streams in stochastic computation. The use of non-Bernoulli sequences of random permutations of fixed numbers of 1’s and 0’s as initial input events’ probabilities makes the stochastic approach more efficient and more accurate than Monte Carlo simulation. Non-exponential failure distributions and repeated events are readily handled by the stochastic approach. The accuracy, efficiency and scalability of the stochastic approach are shown by several case studies of DFT analysis.

Index Terms—**Dynamic fault tree (DFT), reliability analysis, stochastic computation, non-Bernoulli sequence, priority AND (PAND) gate, stochastic logic.**

ACRONYM

FTA	fault tree analysis
DFT	dynamic fault tree
FDEP	functional dependency gate
PAND	priority AND gate
SEQ	sequence enforcing gate
WSP	warm spare gate
CSP	cold spare gate
pdf	probability density function
cdf	cumulative density function
BDDs	binary decision diagrams
SBDDs	sequential binary decision diagrams
MC	Monte Carlo
FPGA	Field Programmable Gate Array

NOTATION

→	symbol for an inclusive precedence in a failure order
---	---

t	mission time
A, B, C, D, \dots	basic events
λ	failure rate
$Ft(A)$	failure time of basic event A
$F(t_i)$	failure probability in the time interval $[t_i, t_i + \Delta t]$
$S(t_i)$	binary sequence at t_i
L	sequence length in the number of bits

I. INTRODUCTION

FAULT tree analysis (FTA) was first proposed in 1962 for evaluating a system's failure probability - the probability that a system fails during a specified mission time [1]. Failures can be disastrous for systems such as chemical plants, nuclear reactors, airplane and computer systems, or costly for systems such as online sales or commercial servers. FTA has developed rapidly and gained much attention in many applications, especially in the analysis of large safety-critical systems [2-7].

However, dynamic behaviors, such as sequence-dependent, functionally dependent and priority relationships, cannot be modeled properly by traditional FTA. To account for these dynamic behaviors, dynamic fault tree (DFT) analysis has been proposed by incorporating additional dynamic gates into FTA. Dynamic gates include the priority AND gate (PAND), the sequence enforcing gate (SEQ), the standby or spare gates that include the warm spare gate (WSP) and cold spare gate (CSP), and the functional dependency gate (FDEP) [8, 9]. The failure of a system is determined by the states of basic events and the interactions among them. The interactions can

be derived from a system's topology. A DFT relies on the interactions among static gates (including AND, OR, and K-out-of-N voting gate) and dynamic gates (PAND, FDEP, SPARE, and SEQ) [10]. Due to their operational characteristics, the dynamic gates are divided into two categories: (1) PAND and FDEP, which are referred to as priority dynamic gates; (2) WSP and SEQ, whose operations are dependent on the duration of failure events [11]. For systems with a perfect fault coverage, FDEP has been modeled as an OR gate [12 - 15]. In a redundant system with an imperfect fault coverage, however, uncovered or undetected faults can propagate and may have a global effect to system failure [16]. In this case, the OR-gate model is not applicable and a combinatorial method has been proposed for an efficient reliability analysis of systems with FDEP gates [16]. As a first study, this paper is focused on priority dynamic gates and, in particular, the PAND gate.

Various methodologies using Markov [2] and Bayesian [17] models have been proposed for evaluating the dependability of a fault tree. Due to the inevitable state-space explosion problem, however, these approaches incur a large complexity for the analysis of complex systems. Moreover, the evaluation of a large DFT using a state-space based method becomes difficult when a basic event's failure behavior is not exponentially distributed.

In [2], an Inclusion/Exclusion method is proposed for an exact analysis of a DFT that contains PAND gates and repeated events. However, this method is limited to the analysis of systems with exponentially distributed failure events; in addition, detailed information on the minimal cut set is usually required in advance. In [7] an integral-based analysis is proposed for handling any probability distribution; however an analytical expression is generally difficult to derive as a function of the basic events' failure distributions. Several approaches have been developed to simplify the process of deriving an exact analytical expression. These include those

using binary decision diagrams (BDDs) [18], sequential binary decision diagrams (SBDDs) [19, 20] and an algebraic analysis [11, 21]. In particular, the SBDD approach has been applied to the analysis of PAND gate [22]. Monte Carlo (MC) simulation [23] has been widely used to evaluate complex DFTs; however, a long run time and a large sample size are needed to meet an accuracy requirement, because of the slow convergence typically encountered in an MC simulation. Generally, it is challenging to efficiently and accurately evaluate the reliability of a DFT.

A stochastic approach has been proposed in [15] for an efficient evaluation of a system's reliability. In particular, the serial and parallel implementations of stochastic computation are considered and a speedup in analysis is obtained by a parallel implementation in FPGAs. In [15], the PAND gate is modeled as a three-input AND gate and a sequential event is considered as a basic event. In a general case, however, the input of a PAND gate is not limited to a basic event.

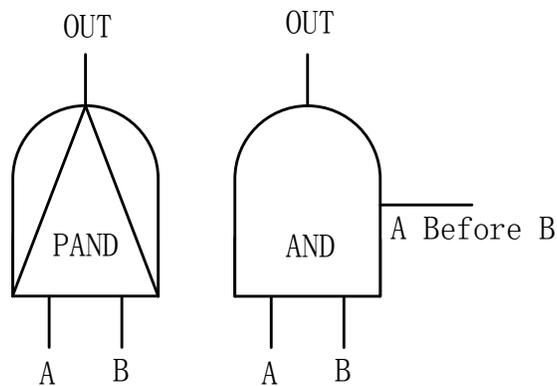
In this paper, a new stochastic approach is presented for an efficient analysis of fault trees with PAND gates. Initially, a stochastic computational model is proposed for the PAND gate; in this model, the output failure probability is obtained as a function of the basic inputs' failure probabilities. Thus, this model is applicable in the general case of a multiple-input PAND gate through a cascaded PAND model. Subsequently, non-Bernoulli sequences of random permutations of fixed numbers of 1's and 0's are used to represent initial event probabilities for an efficient implementation of stochastic computation. It has been shown that the use of the non-Bernoulli sequences as initial inputs provides a more efficient and accurate evaluation than using Bernoulli sequences [24, 25]. This paper shows that the non-Bernoulli sequences significantly improves the efficiency of a stochastic FTA. Hence, the advantage of the stochastic approach is not limited to those due to parallelization or a specific hardware implementation. Furthermore, repeated events, as frequently encountered in a general DFT, are inherently modeled by the

stochastic sequences that preserve signal correlation. Finally, the stochastic approach is general because it is applicable to any failure distribution by encoding failure probabilities into stochastic non-Bernoulli sequences.

The remainder of the paper is organized as follows. Section II reviews the definitions of PAND. Section III presents some hypotheses considered in this paper. The stochastic approach and the proposed model for the PAND gate are described in Section IV. In Section V, the accuracy and efficiency of the proposed approach are shown by the simulation results of several examples. Finally, Section VI concludes the paper.

II. REVIEW OF PAND GATE

A PAND gate is a special type of AND gate, for which an input indicates the firing of a basic event that occurs in a predetermined order and the output indicates whether a failure occurs [5, 26]. Without the loss of generality, the predefined order is assumed to be from left to right in this paper unless otherwise noted. The operational principles of a two-input PAND gate, as well as its symbols, are shown in Fig. 1 for an inclusive condition [11]. By an inclusive condition, if the two inputs of the PAND gate fail simultaneously, the output fails at the same time as the inputs.



(a)

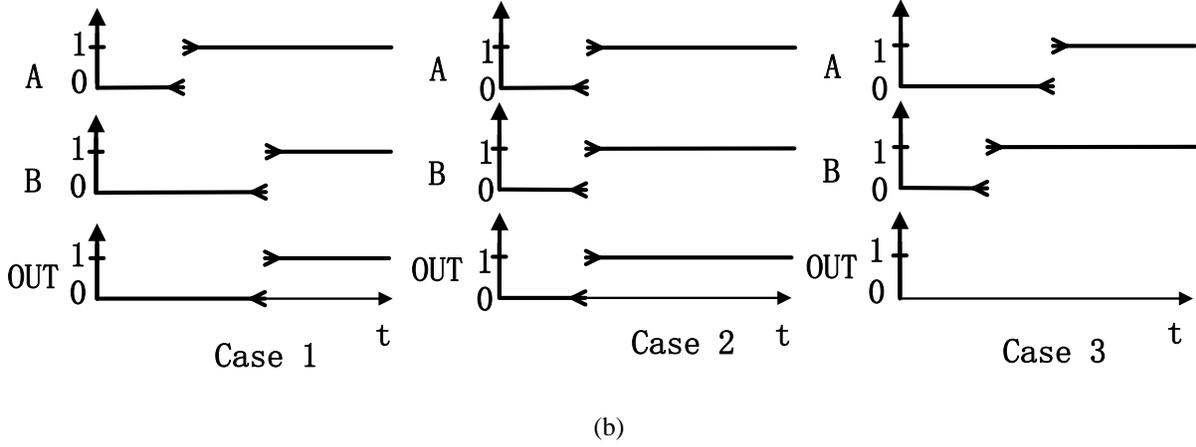


Fig. 1 (a) Symbols for a two-input PAND gate [5, 26]; (b) The expected behaviour of the two-input PAND gate for an inclusive condition (adapted from [11]); 1 and 0 indicate faulty and fault-free events respectively.

As shown in Fig. 1, the output of the PAND gate is 1 (i.e., it fails) when the basic event A fails before B or A and B fail at the same time; otherwise, the output of the PAND gate is 0, i.e., fault free. Let $Ft(A)$ and $Ft(B)$ be the failure time of basic events A and B respectively; the failure time of the PAND gate's output, $Ft(OUT)$, is given by:

$$Ft(OUT) = \begin{cases} Ft(B), & \text{if } Ft(A) < Ft(B) \\ Ft(A) \text{ or } Ft(B), & \text{if } Ft(A) = Ft(B) \\ \infty, & \text{if } Ft(A) > Ft(B) \end{cases} \quad (1)$$

III. HYPOTHESES

Some hypotheses of the paper are as follows:

- The quantization level of a basic event is denoted by a binary variable x , $x \in \{0,1\}$, with 0 indicating no fault;
- All basic events are fault-free at the beginning of the mission time;
- The basic events are non-repairable [5]. This means that if a basic event fails, the variable that indicates the status of the basic event, takes 1. Let $Ft(a)$ be the failure time of a basic

event a ; the status variable of a is 1 for time $t > Ft(a)$ and 0 otherwise. A generic timing diagram for a non-repairable basic event a is shown in Fig. 2.

- The probability density function (*pdf*) and cumulative density function (*cdf*) of an exponential distribution are given by:

$$f(t) = \lambda e^{-\lambda t}, \quad (2)$$

and

$$F(t) = \int_0^t f(t) dt = 1 - e^{-\lambda t}, \quad (3)$$

where t is the specified mission time and λ is the (constant) failure rate of a basic event for an exponential distribution.

- The failure probability of a basic event in a selected time interval $[t_i, t_i + \Delta t]$ is considered constant at the value in the beginning of the time interval, i.e., the failure probability is given by $p = F(t_i)$ for any time in this time interval. For simplicity, the time interval $[t_i, t_i + \Delta t]$ is referred to as time i in this paper.

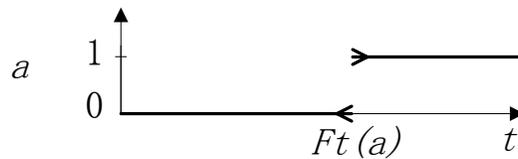


Fig. 2 A timing diagram for a non-repairable basic event a [5, 11]. A value of 0 indicates no fault while 1 means the event has failed; $Ft(a)$ is the failure time of the basic event a .

IV. STOCHASTIC PAND MODEL

A. Stochastic computational models

Stochastic computation was introduced in the 1960s for reliable circuit design [27]. In

stochastic computation, real numbers or probabilities are encoded into the statistics of random binary bit streams [27]. In the random streams, a proportional number of bits are set to a specific value (usually “1”) to indicate a probability. Fig. 3 illustrates the stochastic encoding using a sequence of 10 bits, although a longer sequence length is usually required in a practical application.

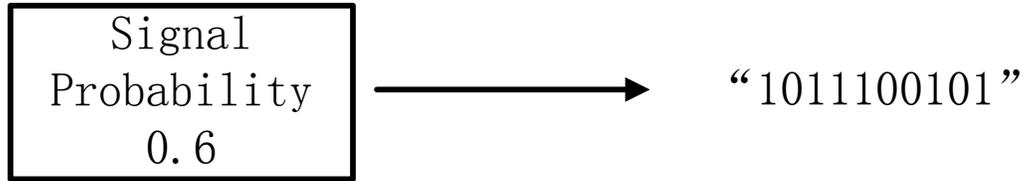


Fig. 3 A stochastic encoding using a sequence of 10 bits for a probability of 0.6.

Fig. 4 shows several stochastic logic operations. In Fig. 4, the input probabilities are coded in the form of binary sequences. Each bit in a sequence is processed by a logic gate and the result of a probabilistic analysis is encoded in the output sequence. By this way, the dependencies among signals are inherently maintained and propagated through a logic network – an example is shown in Fig. 4(c). Stochastic computation has several advantages such as computational simplicity, high speed and fault-tolerance [24, 25].

Due to inevitable stochastic fluctuations in stochastic computation, the number of 1’s in the output sequence is not deterministic but probabilistic. Hence, the output of a stochastic analysis follows approximately a Gaussian distribution when long random binary bit streams are used [25]. However, the use of non-Bernoulli sequences for initial input probabilities leads to a faster convergence of the result, as stated in the following lemma.

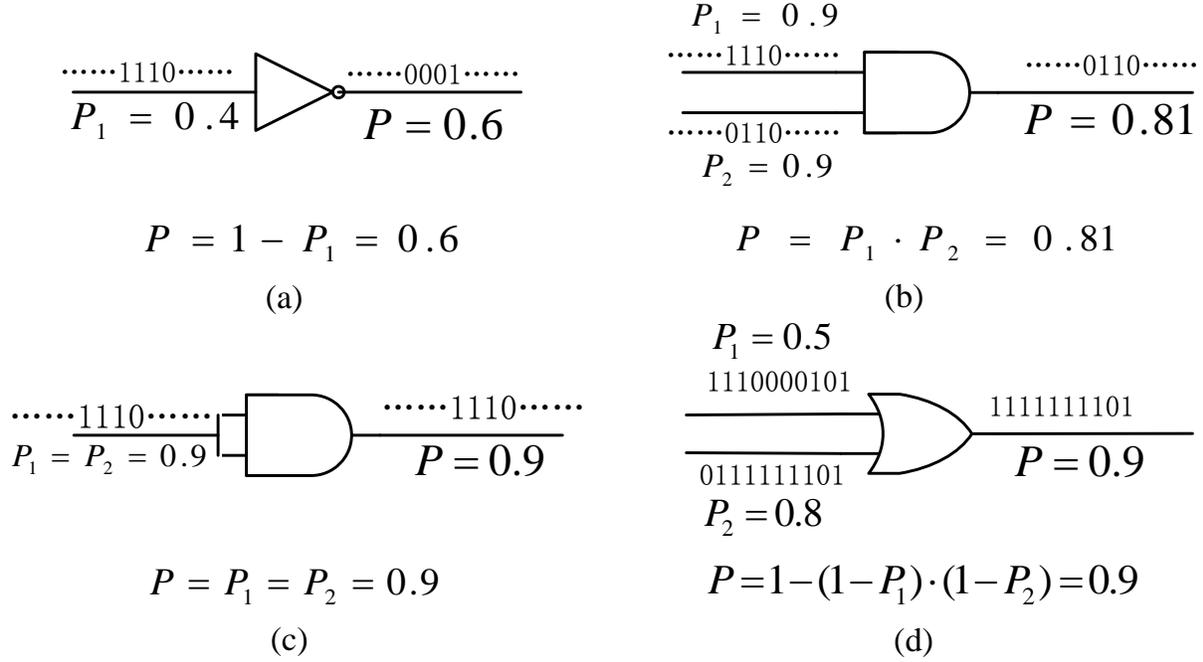


Fig. 4 Stochastic logic: (a) An inverter with a random binary bit sequence as the input; (b) An AND gate with independent inputs; (c) An AND gate with totally correlated inputs; (d) An OR gate with independent inputs.

Lemma 1. [Theorem 1 in [25]] Compared to the case when Bernoulli sequences are used to represent initial input probabilities, the use of large non-Bernoulli sequences as random permutations of fixed numbers of 1's and 0's results in an output sequence with the same mean number of 1's and a smaller variance for an AND gate with independent inputs.

Lemma 1 leads to the conclusion that, to meet a specific accuracy requirement, a smaller sequence length is required by using the non-Bernoulli sequences compared to the use of Bernoulli sequences for encoding initial input probabilities of an AND gate [25].

It is trivial to show that *Lemma 1* is also applicable to an inverter, thus any logic network (as combinations of inverters and AND gates) can be more efficiently and accurately evaluated by using the non-Bernoulli sequences as initial input probabilities. When the inputs of a gate are correlated, the output is also determined by the correlation between the input signals. However, signal correlation (usually caused by the reconvergence of signals) is handled efficiently in

stochastic computation. This is particularly a favorable property for handling the repeated input events in a complex DFT.

B. A two-input PAND gate model

Let A_{i-1} and B_{i-1} indicate the states of basic events A and B at time $i - 1$, and A_i and B_i for the states at time i . If both A and B fail at time i , i.e., $A_{i-1}B_{i-1} = 00$ and $A_iB_i = 11$, the failure time of the basic events A and B is given by:

$$Ft(A) = Ft(B) = i \cdot \Delta t. \quad (4)$$

Then, the failure time of the PAND gate's output is given by $Ft(OUT) = Ft(A) = Ft(B) = i \cdot \Delta t$, due to the model considered in Case 2 in Fig. 1(b).

If $A_{i-1}B_{i-1} = 10$ and $A_iB_i = 11$ at time $i - 1$ and i , the basic event B fails at time i while A fails before time i . The failure time of the basic event B is then:

$$Ft(B) = i \cdot \Delta t. \quad (5)$$

The relationship between the failure times of the basic events A and B is given by:

$$Ft(A) < Ft(B). \quad (6)$$

Thus, $Ft(OUT) = Ft(B)$, due to (1) and the model considered in Case 1 in Fig. 1(b).

For the other possible scenario, i.e., the basic event A fails after B , the top event of the PAND gate would not fail, i.e., with a failure time of infinity, due to the model considered in Case 3 in Fig. 1(b).

Since the basic events are non-repairable, the state of the two-input PAND gate's output event is affected by the gate's output at the previous time, hence the output of the PAND gate at time i , OUT_i , is determined by:

- (1) The current states of the input basic events A and B at time i , A_i and B_i ;
- (2) The inverted state of basic event B at time $i - 1$, $NOT(B_{i-1})$;

(3) The output of the PAND gate at time $i - 1$, OUT_{i-1} .

Hence, the output of the PAND gate at time i is given by

$$OUT_i = OUT_{i-1} + A_i \cdot B_i \cdot NOT(B_{i-1}) \quad (7)$$

A stochastic logic model can be constructed to determine the failure of the two-input PAND gate, as shown in Fig. 5.

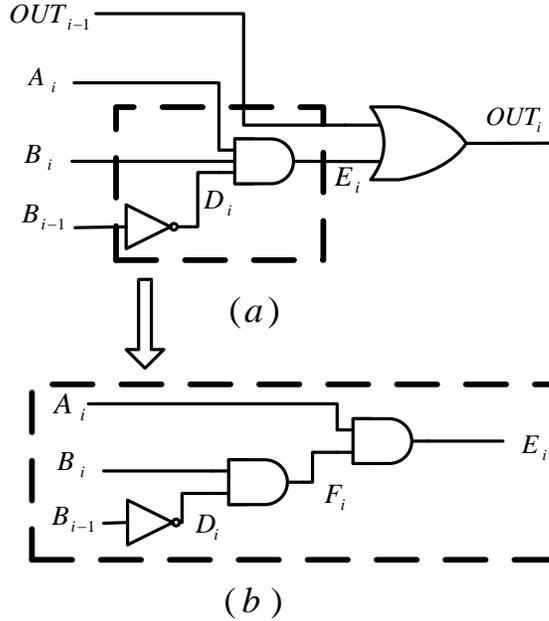


Fig. 5 (a) A stochastic logic model for a two-input PAND gate and (b) the decomposition of the three-input AND gate in (a) into two-input AND gates. A_{i-1} and B_{i-1} indicate the states of basic events A and B at time $i - 1$; A_i and B_i are the states at time i ; OUT_i and OUT_{i-1} are the states of the gate's output event at time i and $i - 1$ respectively.

As per the hypothesis in section III, all basic events are fault free at the beginning of the mission time; thus, the input signals of the model in Fig. 5 are zeros. In Fig. 5(a), if the basic event A fails before time i , $E_i = 1$ if $B_{i-1} = 0$ and $B_i = 1$. Then at time i , $OUT_i = 1$. However, if $OUT_{i-1} = 1$, which indicates that A fails before B or both events fail simultaneously at time $i - 1$, then $B_{i-1} = 1$ and $E_i = 0$. Since OUT_{i-1} and E_i cannot be 1 at the same time, either $OUT_{i-1} = 1$ or $E_i = 1$ results in $OUT_i = 1$. Otherwise, the state of the top event remains zero.

From this analysis, it can be seen that the stochastic PAND model in Fig. 5 computes (7), thus it accurately implements the function of the PAND gate.

C. Model validation

To validate the proposed stochastic PAND model, the discretization of a continuous probability distribution and the generation of stochastic non-Bernoulli sequences are introduced next, followed by a theoretical proof.

1) Discretization

Assume that the mission time t is divided into M equal time intervals, i.e., $\Delta t = t/M$. Due to the nature of discretization, a failure probability is estimated more precisely at time t with a larger M . However, a longer run time is required as more stochastic sequences need to be generated. Hence, M is determined by a tradeoff between accuracy and efficiency. With a reasonable M , the discretization provides a relatively accurate estimation of the continuous failure probability of a basic event.

2) Generation of non-Bernoulli sequences

Assume that the failure probabilities for the two adjacent time intervals, $[t_i - \Delta t, t_i]$ and $[t_i, t_i + \Delta t]$, are given by $F(t_i - \Delta t)$ and $F(t_i)$ respectively. If non-Bernoulli sequences of L bits, as random permutation of fixed number of 0's and 1's, are used, the number of 1's in these sequences for the two probabilities are given by:

$$\begin{cases} N(t_i - \Delta t) = L \cdot F(t_i - \Delta t), \\ N(t_i) = L \cdot F(t_i). \end{cases} \quad (8)$$

The difference of the number of 1's is then:

$$\Delta N = N(t_i) - N(t_i - \Delta t) = L \cdot [F(t_i) - F(t_i - \Delta t)]. \quad (9)$$

Further assume that the non-Bernoulli sequence for the probability in $[t_i - \Delta t, t_i]$ is

given by $S(t_i - \Delta t)$, then the sequence $S(t_i)$ for the probability in $[t_i, t_i + \Delta t]$ can be obtained by randomly assigning ΔN 1's to replace the 0's in $S(t_i - \Delta t)_j$. Since the 1's in $S(t_i - \Delta t)$ are a subset of those in $S(t_i)$, we obtain:

$$S(t_i - \Delta t) \text{ AND } S(t_i) = S(t_i - \Delta t). \quad (10)$$

3) Stochastic model validation

Theorem 1: Compared to an accurate analysis method, a stochastic simulation of the two-input PAND gate model in Fig. 5, using large non-Bernoulli sequences of random permutations of fixed numbers of 1's and 0's as initial input probabilities, produces the same increment in the failure probabilities of two adjacent time intervals when $\lambda \Delta t \rightarrow 0$.

Proof: Assume that the failure probabilities of the PAND gate at time i and $i-1$ are given by $F((A \rightarrow B)_i)$ and $F((A \rightarrow B)_{i-1})$, respectively; we show that the failure probability of E_i in the stochastic model in Fig. 5 is the same as the increment in the output failure probability of the PAND gate from time $i-1$ to i , i.e., $F(E_i) = F((A \rightarrow B)_i) - F((A \rightarrow B)_{i-1})$.

Given the basic events A and B with the probability density functions (*pdfs*) $f_A(t)$ and $f_B(t)$ respectively, the failure probability for the two-input PAND gate's output OUT (when both A and B fail or A fails before B , i.e., $A \rightarrow B$), is given by:

$$F(A \rightarrow B) = \int_0^t \int_{t_1}^t f_B(t_2) f_A(t_1) dt_2 dt_1, \quad (11)$$

For an exponential distribution, (11) becomes:

$$F(A \rightarrow B) = \int_0^t \int_{t_1}^t \lambda_B e^{-\lambda_B t_2} \lambda_A e^{-\lambda_A t_1} dt_2 dt_1, \quad (12)$$

which leads to the failure probability of the sequential event $A \rightarrow B$ as:

$$F(A \rightarrow B) = \frac{\lambda_A}{(\lambda_A + \lambda_B)} (1 - e^{-(\lambda_A + \lambda_B)t}) - e^{-\lambda_B t} (1 - e^{-\lambda_A t}). \quad (13)$$

(13) can be obtained by using an analytical approach [7] or a probabilistic algebraic analysis

[11].

By discretization, the failure probabilities of the sequential event $A \rightarrow B$ at time i and $i - 1$ are given by:

$$F((A \rightarrow B)_i) = \frac{\lambda_A}{(\lambda_A + \lambda_B)} (1 - e^{-(\lambda_A + \lambda_B) \cdot i \cdot \Delta t}) - e^{-\lambda_B \cdot i \cdot \Delta t} (1 - e^{-\lambda_A \cdot i \cdot \Delta t}), \quad (14)$$

and

$$F((A \rightarrow B)_{i-1}) = \frac{\lambda_A}{(\lambda_A + \lambda_B)} (1 - e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t}) - e^{-\lambda_B \cdot (i-1) \cdot \Delta t} + e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t}, \quad (15)$$

respectively. (14) can also be written as:

$$F((A \rightarrow B)_i) = \frac{\lambda_A}{(\lambda_A + \lambda_B)} (1 - e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t} \cdot e^{-(\lambda_A + \lambda_B) \cdot \Delta t}) - e^{-\lambda_B \cdot (i-1) \cdot \Delta t} \cdot e^{-\lambda_B \cdot \Delta t} + e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t} \cdot e^{-(\lambda_A + \lambda_B) \cdot \Delta t}. \quad (16)$$

Since $O((\lambda \cdot \Delta t)^i)$ for any $i \geq 2$ is negligible when $\lambda \Delta t \rightarrow 0$, applying a Taylor series expansion on (16) leads to:

$$F((A \rightarrow B)_i) = \left[\frac{\lambda_A}{(\lambda_A + \lambda_B)} (1 - e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t}) - e^{-\lambda_B \cdot (i-1) \cdot \Delta t} + e^{-\lambda_B \cdot (i-1) \cdot \Delta t} \cdot \lambda_B \cdot \Delta t + e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t} - e^{-(\lambda_A + \lambda_B) \cdot (i-1) \cdot \Delta t} \cdot \lambda_B \cdot \Delta t \right]. \quad (17)$$

From (15) and (17), the probability increment for two adjacent times is obtained as:

$$\begin{aligned} F(OUT_i) - F(OUT_{i-1}) &= F((A \rightarrow B)_i) - F((A \rightarrow B)_{i-1}) \\ &= \lambda_B \cdot \Delta t \cdot e^{-\lambda_B \cdot (i-1) \cdot \Delta t} \cdot (1 - e^{-(\lambda_A) \cdot (i-1) \cdot \Delta t}). \end{aligned} \quad (18)$$

Next, the stochastic analysis of the increased probability E_i between two adjacent times is pursued. Let $F_c(\cdot)$ and $F_d(\cdot)$ indicate the cumulative density functions (*cdf*s) for the continuous and discretized distributions respectively. By applying the discretization process to the exponential distributions of the basic events (i.e., A and B), we have:

$$\begin{cases} F_c(A) = \int_0^t f_A(t) dt = 1 - e^{-\lambda_A t}, \\ F_d(A) = 1 - e^{-\lambda_A \cdot M \cdot \Delta t}, \end{cases} \quad (19)$$

and

$$\begin{cases} F_c(B) = \int_0^t f_B(t) dt = 1 - e^{-\lambda_B \cdot t}, \\ F_d(B) = 1 - e^{-\lambda_B \cdot M \cdot \Delta t}, \end{cases} \quad (20)$$

where M is the number of equally discretized time intervals Δt .

Hence, the inputs' probabilities of A and B at time i and $i - 1$ are given by:

$$F(A_i) = (1 - e^{-\lambda_A \cdot i \cdot \Delta t}), \quad (21)$$

$$F(B_i) = (1 - e^{-\lambda_B \cdot i \cdot \Delta t}), \quad (22)$$

$$F(B_{i-1}) = (1 - e^{-\lambda_B \cdot (i-1) \cdot \Delta t}). \quad (23)$$

Let $S(A_i)$ be the stochastic sequence generated for the probability of the basic event A at time i ; $S(B_i)$ and $S(B_{i-1})$ be the stochastic sequences for the basic event B at time i and $i - 1$ respectively. In the model of Fig. 5, the inverter's output sequence, $S(D_i)$, is given by:

$$S(D_i) = NOT(S(B_{i-1})). \quad (24)$$

For the three-input AND gate in Fig. 5(a), its output sequence is obtained as:

$$S(E_i) = S(A_i) AND S(B_i) AND S(D_i) = S(A_i) AND (S(B_i) AND (NOT (S(B_{i-1}))))). \quad (25)$$

Similar as in (10), the probability encoded in the sequence $S(B_i) AND (NOT (S(B_{i-1})))$ is given by $F(B_i) - F(B_{i-1})$, i.e., the probability increment for the basic event B in two adjacent times.

By (22) and (23), this probability increment is thus:

$$F(B_i) - F(B_{i-1}) = e^{-\lambda_B \cdot (i-1) \cdot \Delta t} - e^{-\lambda_B \cdot i \cdot \Delta t} \quad (26)$$

Considering $F(E_i)$ as the probability encoded in the sequence $S(E_i)$, together with (21) and (26), the probability increment in E_i is given by:

$$F(E_i) = F(A_i)(F(B_i) - F(B_{i-1})) = (1 - e^{-\lambda_A \cdot i \cdot \Delta t}) \cdot (e^{-\lambda_B \cdot (i-1) \cdot \Delta t} - e^{-\lambda_B \cdot i \cdot \Delta t}). \quad (27)$$

The application of a Taylor series expansion on (27) leads to a first-order approximation given by (18). This shows that the proposed stochastic model accurately implements the function of a two-input PAND gate for exponentially distributed events, i.e.,

$$F(E_i) = F((A \rightarrow B)_i) - F((A \rightarrow B)_{i-1}). \quad (28)$$

Next, the proof of the theorem is pursued in the general case when the basic events are non-exponentially distributed. By an integral analysis, the failure probability of the two input PAND gate at time t is given by:

$$\begin{aligned} F((A \rightarrow B)_t) &= \int_0^t \int_{t_1}^t f_B(t_2) f_A(t_1) dt_2 dt_1 = \int_0^t (F_B(t) - F_B(t_1)) f_A(t_1) dt_1 \\ &= F_B(t) \int_0^t f_A(t_1) dt_1 - \int_0^t F_B(t_1) f_A(t_1) dt_1. \end{aligned} \quad (29)$$

Similarly, this failure probability at time $t - \Delta t$ is given by:

$$\begin{aligned} F((A \rightarrow B)_{t-\Delta t}) &= \int_0^{t-\Delta t} \int_{t_1}^{t-\Delta t} f_B(t_2) f_A(t_1) dt_2 dt_1 = \int_0^{t-\Delta t} (F_B(t - \Delta t) - F_B(t_1)) f_A(t_1) dt_1 \\ &= F_B(t - \Delta t) \int_0^{t-\Delta t} f_A(t_1) dt_1 - \int_0^{t-\Delta t} F_B(t_1) f_A(t_1) dt_1. \end{aligned} \quad (30)$$

The increment of the failure probabilities between t and $t - \Delta t$ is then:

$$\begin{aligned} F((A \rightarrow B)_t) - F((A \rightarrow B)_{t-\Delta t}) &= F_B(t) \int_0^t f_A(t_1) dt_1 - \int_0^t F_B(t_1) f_A(t_1) dt_1 - \\ &F_B(t - \Delta t) \int_0^{t-\Delta t} f_A(t_1) dt_1 + \int_0^{t-\Delta t} F_B(t_1) f_A(t_1) dt_1 = F_B(t) \int_0^{t-\Delta t} f_A(t_1) dt_1 + \\ &F_B(t) \int_{t-\Delta t}^t f_A(t_1) dt_1 - F_B(t - \Delta t) \int_0^{t-\Delta t} f_A(t_1) dt_1 - \int_{t-\Delta t}^t F_B(t_1) f_A(t_1) dt_1. \end{aligned} \quad (31)$$

When $\Delta t \rightarrow 0$, we have

$$\int_{t-\Delta t}^t F_B(t_1) f_A(t_1) dt_1 = \lim_{\Delta t \rightarrow 0} \{F_B(t - \Delta t) f_A(t - \Delta t) \Delta t\}. \quad (32)$$

and

$$\int_{t-\Delta t}^t f_A(t_1) dt_1 = \lim_{\Delta t \rightarrow 0} \{f_A(t - \Delta t)\Delta t\}. \quad (33)$$

In this case, (31) becomes:

$$\lim_{\Delta t \rightarrow 0} \{F((A \rightarrow B)_t) - F((A \rightarrow B)_{t-\Delta t})\} = \lim_{\Delta t \rightarrow 0} \{(F_B(t) - F_B(t - \Delta t)) \int_0^{t-\Delta t} f_A(t_1) dt_1 + F_B(t)f_A(t - \Delta t)\Delta t - F_B(t - \Delta t)f_A(t - \Delta t)\Delta t\}. \quad (34)$$

When $\Delta t \rightarrow 0$, hence,

$$F((A \rightarrow B)_t) - F((A \rightarrow B)_{t-\Delta t}) = (F_B(t) - F_B(t - \Delta t)) \left(\int_0^{t-\Delta t} f_A(t_1) dt_1 + \int_{t-\Delta t}^t f_A(t_1) dt_1 \right) = (F_B(t) - F_B(t - \Delta t)) \int_0^t f_A(t_1) dt_1. \quad (35)$$

Since $F_A(t) = \int_0^t f_A(t_1) dt_1$, we obtain:

$$F((A \rightarrow B)_t) - F((A \rightarrow B)_{t-\Delta t}) = (F_B(t) - F_B(t - \Delta t))F_A(t). \quad (36)$$

The right hand side of (36) is the failure probability increment computed by the stochastic model of PAND in Fig. (5). This proves *Theorem 1* in the general case. \square

4) Analysis of the increment in failure probability

If $S(B_i)$ and $S(B_{i-1})$ are the non-Bernoulli sequences for the failure probabilities of the basic event B , $F(B_i)$ and $F(B_{i-1})$, at time i and $i - 1$ respectively, the mean number of 1's in the non-Bernoulli sequence $S(B_{i-1})$ of L bits is then $L \cdot F(B_{i-1})$ and the variance is 0 (by the nature of the non-Bernoulli sequence). This indicates that the use of non-Bernoulli sequences results in a deterministic initial value. Since there is no variation in the input signal of the inverter, the variance in the inverter's output sequence $S(D_i)$ is 0 as $S(D_i) = NOT(S(B_{i-1}))$. Hence, the mean and variance of the number of 1's in the sequence $S(D_i)$ are given by:

$$\mu = L \cdot (1 - F(B_{i-1})), \quad (37)$$

and

$$v = 0, \quad (38)$$

respectively. In Fig. 5(b), the first AND gate's output sequence $S(F_i)$ is given by $S(F_i) = \text{AND}(S(B_i), \text{NOT}(S(B_{i-1})))$, where $S(B_i)$ is dependent on $S(B_{i-1})$, as discussed previously. The mean and variance of the number of 1's in the first AND gate's output sequence are then given by:

$$\mu' = L \cdot (F(B_i) - F(B_{i-1})), \quad (39)$$

and

$$v' = 0, \quad (40)$$

respectively. (39) and (40) indicate that $S(F_i)$ is also a non-Bernoulli sequence.

For the basic event A , a non-Bernoulli sequence at time i , $S(A_i)$, is generated for the failure probability $F(A_i)$. For the last AND gate in Fig. 5(b), the input sequences $S(F_i)$ and $S(A_i)$ are for two independent signals. Per *Lemma 1*, therefore, the use of non-Bernoulli sequences produces a more accurate result at the output of the last AND gate in Fig. 5(b) and thus at the output of the three-input AND gate in Fig. 5(a) than using Bernoulli sequences.

If the expected probability of E_i is given by $z = N(E_i)/L$, where $N(E_i)$ indicates the number of 1's in the sequence $S(E_i)$, through a combinatorial analysis and the application of Stirling's formula [28, 29], the number of 1's in the output stochastic sequence $S(E_i)$ of L bits, follows approximately a Gaussian distribution, i.e.,

$$F(z) \sim \frac{1}{\sqrt{2\pi L}} \sqrt{\beta} e^{-\theta L}, \quad (41)$$

where

$$\beta \sim \frac{1}{F(A_i)(1-F(A_i))(F(B_i)-F(B_{i-1}))(1-(F(B_i)-F(B_{i-1})))}, \quad (42)$$

$$\theta \sim \frac{(z-F(A_i)(F(B_i)-F(B_{i-1})))^2}{2F(A_i)(1-F(A_i))(F(B_i)-F(B_{i-1}))(1-(F(B_i)-F(B_{i-1})))}. \quad (43)$$

with a mean and variance given by $L \cdot F(A_i)(F(B_i) - F(B_{i-1}))$ and $L \cdot F(A_i)(1 -$

$F(A_i))(F(B_i) - F(B_{i-1}))(1 - (F(B_i) - F(B_{i-1})))$ respectively.

D. Generalization of the PAND model

A multiple-input PAND gate can be converted to a successively cascaded model of two-input PAND gates. Take a three-input PAND as an example, as shown in Fig. 6(a); its cascaded model is shown in Fig. 6(b). Assume that the failure order of the three inputs is from left to right, i.e., $A \rightarrow B \rightarrow C$; then, if the failures of the input events occur in this order, the output G is 1; otherwise, G is 0.

In the cascaded model in Fig. 6(b), a 1 at the gate output G indicates that the intermediate event D fails before the basic event C or both D and C fail at the same time. Since $D = 1$ is caused by the fact that the basic event A fails before B or both A and B fail at the same time, the gate output $G = 1$ means that the sequential event $A \rightarrow B \rightarrow C$ occurs; thus the cascaded model implements the function of a three-input PAND gate. This model can be generalized for an arbitrary multiple-input PAND gate.

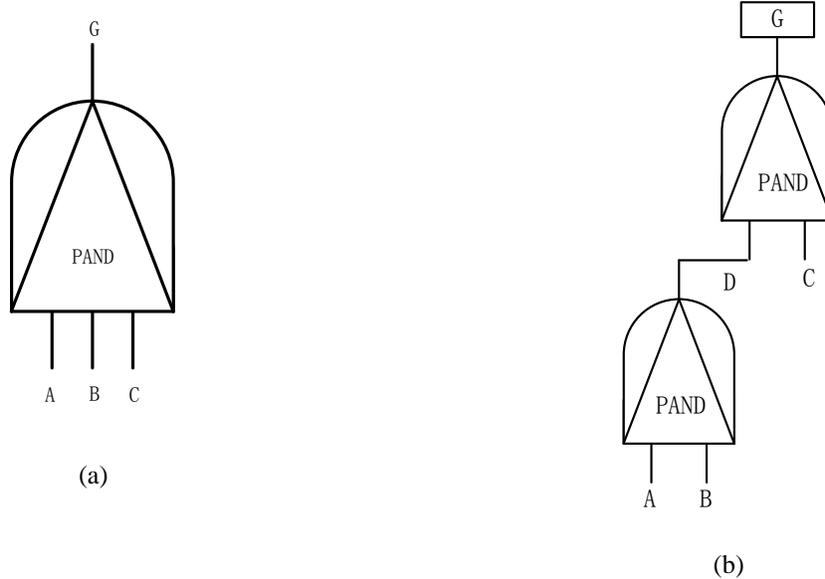


Fig. 6 (a) A three-input PAND gate; (b) A successive cascading model of the three-input PAND gate in (a).

In summary, for a DFT with priority relationships, the stochastic two-input PAND model and the successive cascading model can be utilized in an FTA using the non-Bernoulli sequences generated for discretized probabilities of the basic events. The failure probability of the top event is encoded in the statistics, i.e., the proportion of number of 1's, in the output sequence of the stochastic analysis.

V. CASE STUDIES AND VALIDATION RESULTS

In this section, several case studies are presented to show the accuracy, efficiency and the ability of dealing with repeated basic events of the stochastic PAND model. Simulations are performed for both exponential and non-exponential distributions of basic events. The results are compared with those obtained by using accurate analysis and simulation-based approaches. Simulations are run on a computer with a 3.10 GHz i3-2100 microprocessor and 6 GB memory.

A. Validation of the stochastic PAND models

Example 1: For a two-input PAND gate and a three-input PAND gate, as shown in Fig. 1(a) and Fig. 6(a), the failure probabilities of basic events are assumed to be exponentially distributed, with $\lambda_A = \lambda_B = \lambda_C = 0.01$. The mission time is 300 *hours* and the time interval for discretization is one hour, i.e., $\Delta t = 1$ *hour*.

A quantitative analysis of the two-input PAND gate is first performed using the stochastic PAND model. The results are compared with those obtained by using the Monte Carlo (MC) [23] and analytical [7] methods, as shown in Fig. 7. It can be seen that the stochastic approach produces very accurate results compared to the MC and accurate analysis methods.

Since a continuous failure distribution is discretized into M time intervals, the stochastic analysis results in a vector of the failure probability of the top event at every time interval, $\mathbf{F} = (F[1], F[2], \dots, F[M])$. Let \mathbf{F}_S , \mathbf{F}_A and \mathbf{F}_{MC} denote the failure probability vectors obtained by

the stochastic approach, an accurate analysis [7] and the MC method [23]. While an accurate result can be efficiently obtained by using an SBDD method [19, 20] or an algebraic analysis [11], a direct integral method is used in this work for an accurate analysis. Albeit very fast for a simple DFT analysis, such accurate analysis may become cumbersome in the evaluation of large DFTs. Further let $\Delta \mathbf{F}_{MC-A}$ be the difference in the failure probability vectors obtained from the MC method [23] and the accurate analysis [7], and $\Delta \mathbf{F}_{S-A}$ be the difference in the failure probability vectors obtained from the stochastic approach and the accurate analysis [7]. The three norms, $\|\cdot\|_1$, $\|\cdot\|_2$ and $\|\cdot\|_\infty$, are then used to measure the differences of the failure probability vectors. For a vector \mathbf{x} , the norms are defined as $\|\mathbf{x}\|_1 = \sum_{i=1}^n |x_i|$, $\|\mathbf{x}\|_2 = \sqrt{\sum_{i=1}^n |x_i|^2}$ and $\|\mathbf{x}\|_\infty = \max_{1 \leq i \leq n} |x_i|$.

The results are shown in Table 1 for the two-input PAND gate with various sequence lengths for the stochastic approach. The average run time is also shown for comparing the efficiency. Unless otherwise noted, ten experiments are run in each case study for obtaining the norm values and average run time. As shown in Table 1, the smaller norm values and shorter run time indicate that the stochastic analysis using the non-Bernoulli sequences is more accurate and more efficient than the MC method.

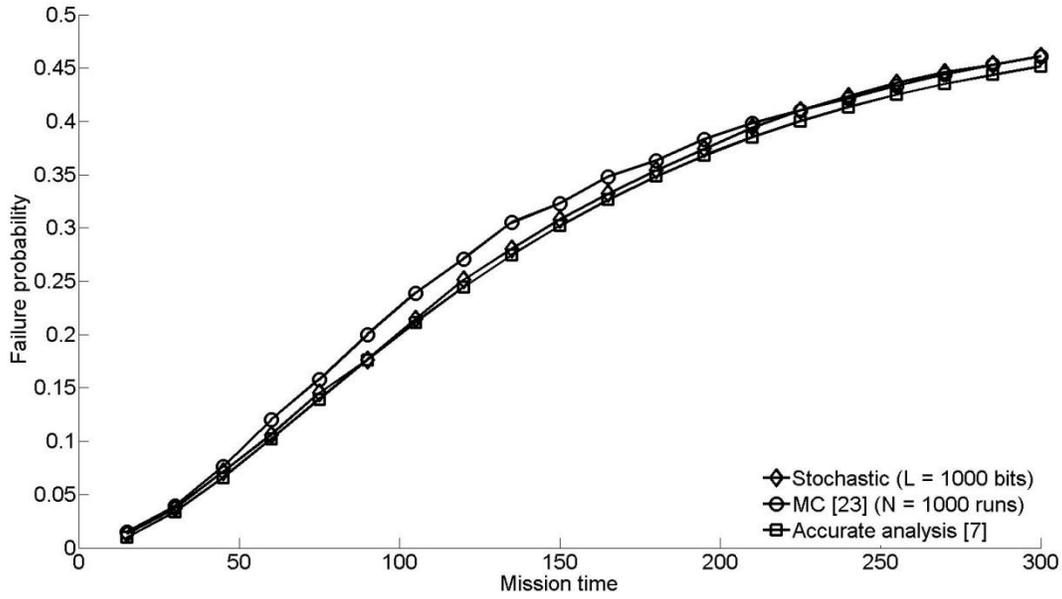


Fig. 7 The simulation results obtained by using the stochastic, Monte Carlo (MC) [23] and analytical [7] methods for the two-input PAND gate in Fig. 1(a). N : the number of simulation runs for the MC method; L : the sequence length for the stochastic approach. (In the captions of subsequent figures, the notations of N and L are the same and thus omitted for simplicity, wherever applicable.)

Table 1. Accuracy and run time of the stochastic approach and Monte Carlo (MC) simulation [23], compared to an accurate analysis [7], for the two-input PAND gate in Fig. 1(a). N : the number of simulation runs for the MC method; L : the sequence length for the stochastic approach. (In the titles of subsequent tables, the notations of N and L are the same and thus omitted for simplicity, wherever applicable.)

	N/L	1K	5K	10K	100K
MC simulation [23] vs. Accurate analysis [7]	$\ \Delta \mathbf{F}_{MC-A}\ _1$	2.8665	1.4030	1.0888	0.9853
	$\ \Delta \mathbf{F}_{MC-A}\ _2$	0.1984	0.0940	0.0729	0.0686
	Average run time for MC simulation (s)	2.1456	11.813	24.608	225.67
The stochastic approach vs. Accurate analysis [7]	$\ \Delta \mathbf{F}_{S-A}\ _1$	2.0604	0.9243	0.7085	0.6319
	$\ \Delta \mathbf{F}_{S-A}\ _2$	0.1338	0.0597	0.0455	0.0383
	Average run time for stochastic approach (s)	0.0339	0.1228	0.2461	4.7282

The accuracy of the stochastic approach can further be improved by using longer stochastic sequences. As shown in Fig. 8, the stochastic approach can produce very accurate results as compared to the accurate analysis [7] by using a large sequence length (e.g. 100K bits) for the two-input PAND gate.

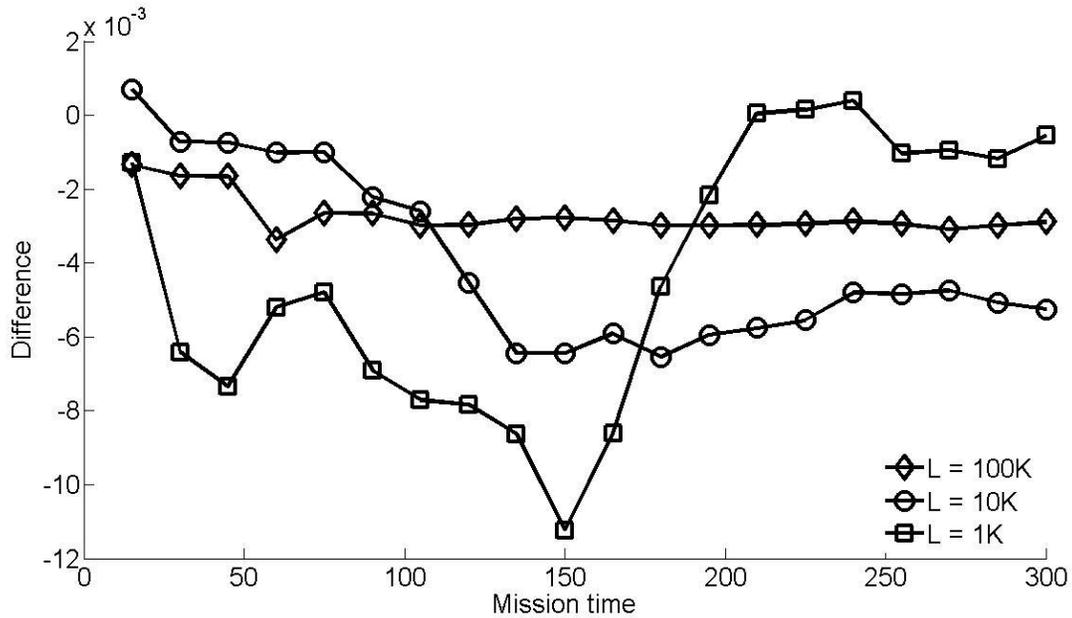


Fig. 8 The differences in the failure probability obtained by using the stochastic approach and an accurate analysis at different mission times for the two-input PAND gate.

Next, the failure probability of a three-input PAND gate is evaluated by using the successive cascading PAND model and the stochastic approach. Simulations are run for different sequence lengths and the obtained failure probability vectors are compared with those obtained by an accurate analysis. As revealed in Table 2, the norms of the differences of the computed failure probability vectors indicate that a stochastic analysis of the PAND model is more accurate and more efficient than an MC method. As shown in Fig. 9, moreover, the accuracy of the stochastic approach can further be improved by using longer stochastic sequences.

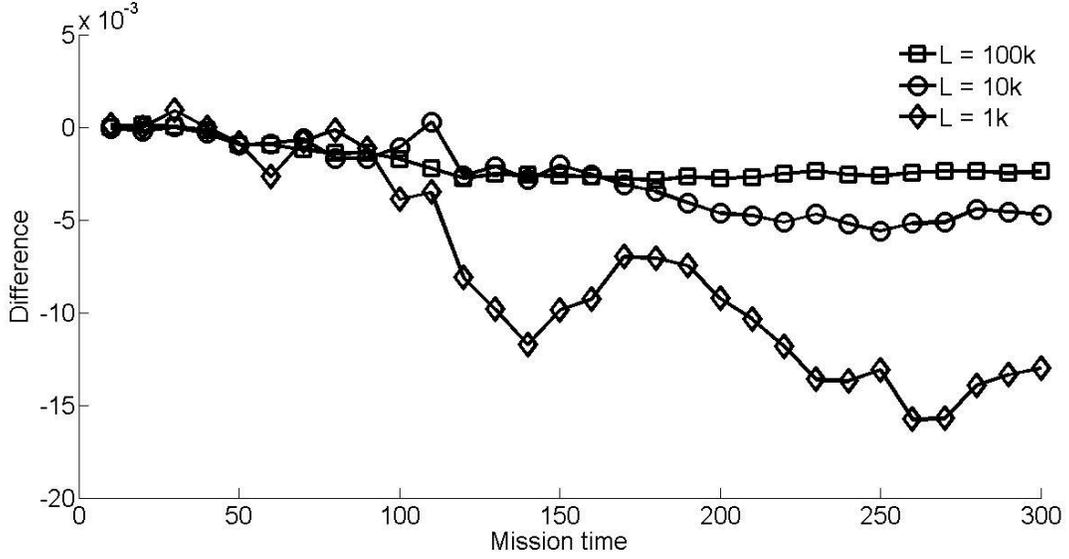


Fig. 9 The differences in the failure probability obtained by using the stochastic approach and an accurate analysis at different mission times for the three-input PAND gate.

Table 2. Accuracy and run time of the stochastic approach and Monte Carlo (MC) simulation [23], compared to an accurate analysis [7], for the three-input PAND gate in Example 1 (b).

The stochastic approach	L	$\ \Delta F_{S-A}\ _1$	$\ \Delta F_{S-A}\ _2$	$\ \Delta F_{S-A}\ _\infty$	Average time (s)
	1K	1.5643	0.1071	0.0121	0.6456
	10K	0.6408	0.0434	0.0045	6.8836
	100K	0.4827	0.0313	0.0027	66.335
MC simulation [23]	N	$\ \Delta F_{MC-A}\ _1$	$\ \Delta F_{MC-A}\ _2$	$\ \Delta F_{MC-A}\ _\infty$	Average time (s)
	1K	2.1041	0.1462	0.0156	5.0451
	10K	0.7312	0.0512	0.0055	54.602
	100K	0.5007	0.0324	0.0029	558.07

B. A DFT with repeated events

A DFT with PAND gates and repeated events is analyzed next using the stochastic

approach.

Example 2 (from [2]): A DFT consists of 5 logic gates (4 OR gates, 1 AND gate) and 2 dynamic gates (PANDs) with 9 basic events, as shown in Fig. 10. The failure rates of the basic events are exponentially distributed with $\lambda_i = 0.01$ for $i = 1, 2, \dots, 9$. The basic events e_2 and e_3 are repeated events. The maximum mission time is 300 hours.

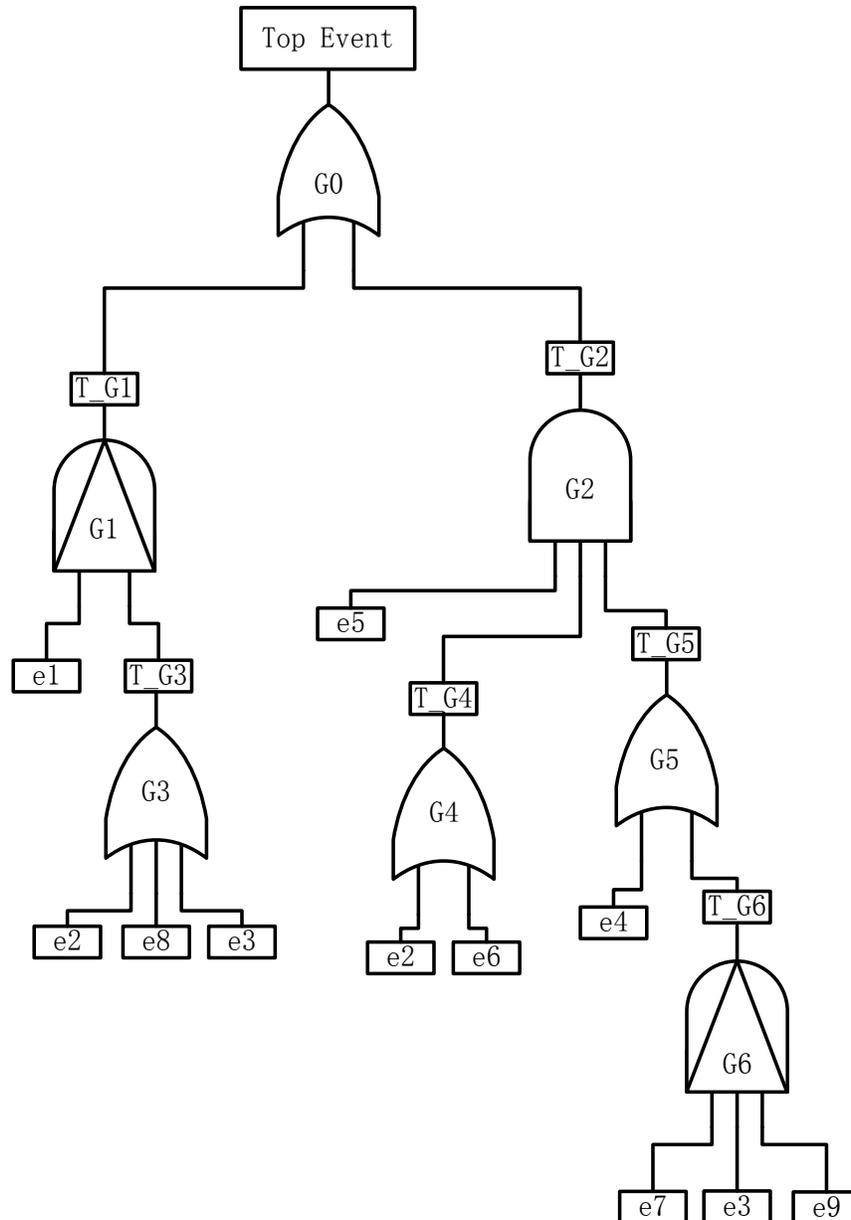


Fig. 10 Example 2: a DFT with repeated events e_2 and e_3 [2].

The simulation results by the stochastic approach with different sequence lengths and the MC method [23] with different numbers of simulations are shown in Table 3 for several mission times. As can be seen, the stochastic approach computes the failure probability of the top event with a better efficiency than the MC method. This indicates that the stochastic approach using the non-Bernoulli sequences as initial inputs can efficiently evaluate the reliability of a dynamic system with repeated events. The accuracy improves with the increase of the length of the stochastic sequences.

Table 3. The top event's failure probability of the DFT in Fig. 10. The total mission time is 300 hours and t indicates a sampled time.

t (hour)	Monte Carlo simulation [23]				The stochastic approach			
	$N = 1K$	$N = 5K$	$N = 10K$	$N = 100K$	$L = 1K$	$L = 5K$	$L = 10K$	$L = 100K$
50	0.1980	0.2104	0.2125	0.2165	0.2230	0.2134	0.2185	0.2172
100	0.4870	0.4988	0.4868	0.4952	0.5080	0.4954	0.4896	0.4953
150	0.6780	0.6996	0.6809	0.6886	0.7060	0.6786	0.6908	0.6909
200	0.8080	0.8156	0.8070	0.8121	0.8110	0.8118	0.8089	0.8092
250	0.8830	0.8890	0.8832	0.8860	0.8880	0.8878	0.8846	0.8868
300	0.9338	0.9336	0.9318	0.9314	0.9330	0.9328	0.9310	0.9315
Average time (s)	25.440	126.66	254.02	2543.3	2.7416	13.628	27.026	196.60

C. A DFT with events of non-exponential distributions

The presence of a large number of basic events makes it very difficult to derive the top event's failure probability using an accurate analysis approach, because a large number of states

need to be considered and the complexity of an analysis increases significantly with the number of basic events. It is also difficult to evaluate a PAND gate with intermediate events as inputs. The problem becomes even more challenging when the basic events' failures are not exponentially distributed. In this section, it is shown that these issues are effectively addressed by the stochastic approach, as illustrated by Examples 3.

Example 3 (from [23]): A DFT consists of a relatively large number of basic events, while the inputs of a PAND gate are two intermediate events, as shown in Fig. 11.

The failure probability of the top event can be obtained by the algebraic analysis in [11] as:

$$F\{(M \rightarrow N)\} = \int_0^t f_N(t_1) \cdot F_M(t_1) dt_1, \quad (44)$$

where

$$F_N(t_1) = 1 - \prod_{i \in \{H,I,J,K,L\}} (1 - F_i(t_1)), \quad (45)$$

$$F_M(t_1) = \prod_{j \in \{A,B,C,D,E\}} F_j(t_1). \quad (46)$$

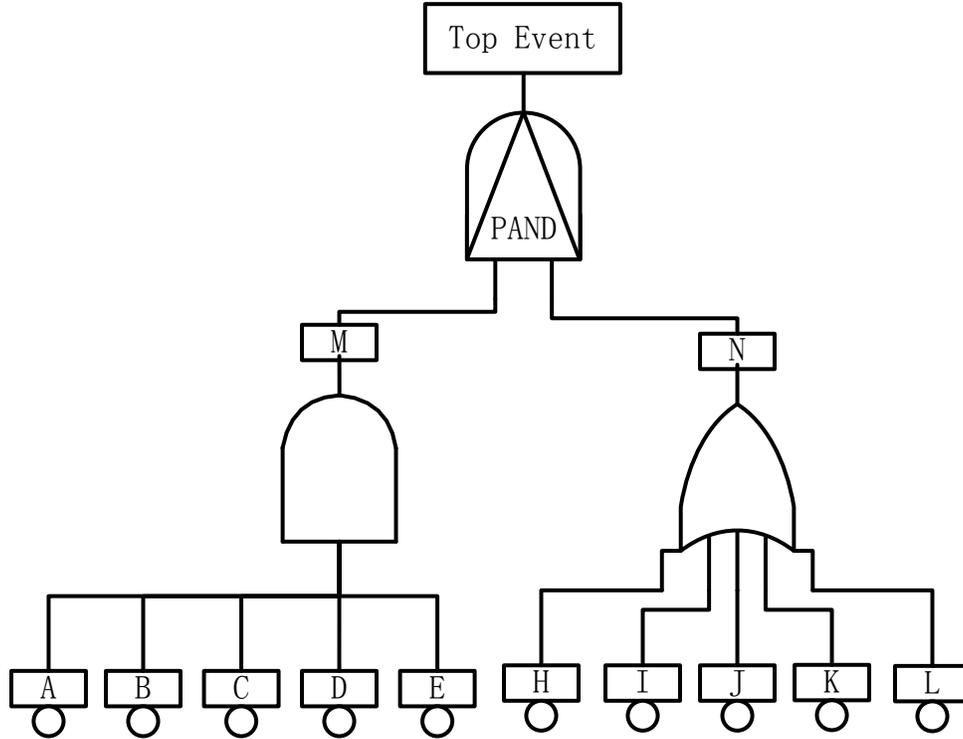


Fig. 11 Example 3: a DFT with intermediate events as the inputs of a PAND gate [23].

In a practical system, a non-exponential distribution may be required for a more accurate modeling of a basic event's failure. Although an approximate result can be obtained by using an algebraic analysis, it becomes cumbersome for an algebraic analysis to accurately evaluate such systems due to the complexity involved in deriving a closed form of analytical expressions.

In this section, the Weibull distribution is considered to show that a DFT with non-exponentially distributed basic events can be handled by the stochastic approach. The probability density function (*pdf*) and cumulative density function (*cdf*) of the Weibull distribution is given by:

$$f(t) = \frac{\alpha}{\lambda} \left(\frac{t}{\lambda}\right)^{\alpha-1} e^{-(t/\lambda)^\alpha}, \quad (47)$$

and

$$F(t) = 1 - e^{-(t/\lambda)^\alpha}, \quad (48)$$

respectively, where α and λ are the shape and scale parameters of the Weibull distribution.

Assume that in the DFT in Fig. 11, the basic events J, K, L follow a Weibull distribution with $\alpha = 0.1$ and $\lambda = 20$, while the other basic events are exponentially distributed with failure rates given in Table 4 [23].

Table 4. The failure rates of the basic events in Example 3 [23].

Basic event	Failure rate	Basic event	Failure rate
A	0.011	B	0.012
C	0.013	D	0.014
E	0.015	H	0.0011
I	0.0012		

For this system, the failure probability of the top event is plotted for a mission time of 300 hours, as shown in Fig. 12, for both the stochastic approach and the MC method [23]. Because the encoding of a failure probability into a stochastic sequence is not limited to those of exponential distributions, a DFT with non-exponentially distributed basic events can be accurately evaluated by the stochastic approach, as shown in Fig. 12. Hence, the proposed stochastic approach is applicable to both exponential and non-exponential distributions in a DFT analysis.

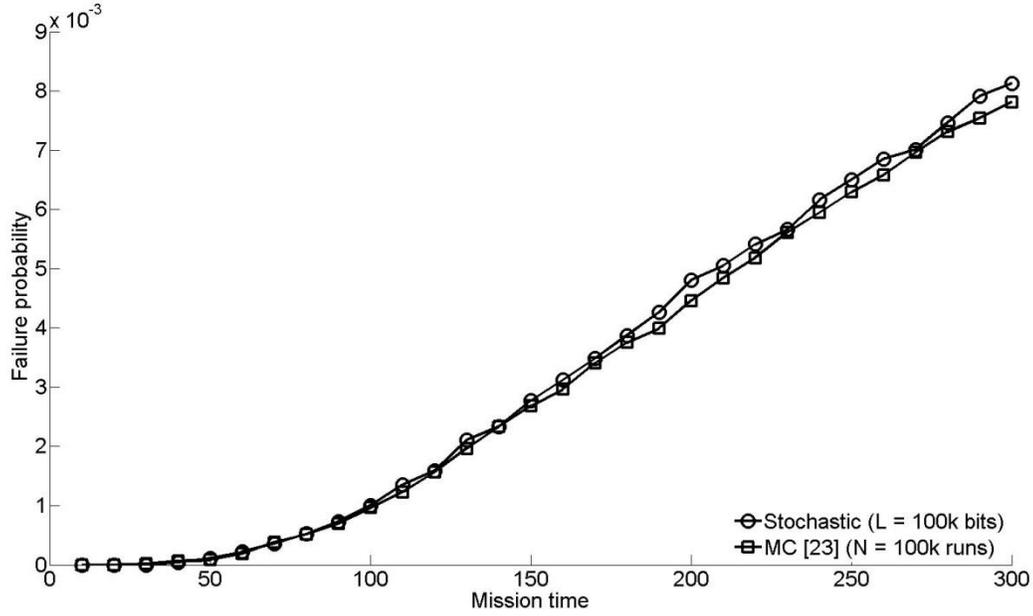


Fig. 12 The failure probability of the top event with non-exponentially distributed basic events. The norms of the differences of the failure probability vectors obtained by the stochastic and Monte Carlo (MC) methods are $\|\cdot\|_1 = 0.0357$, $\|\cdot\|_2 = 0.0028$ and $\|\cdot\|_\infty = 4.5 \times 10^{-4}$.

D. A fault tree with repeated events and non-exponential distributed ones

Finally, a fault tree without dynamic gates, but with repeated events and non-exponentially distributed ones, is considered. This fault tree is developed from the DFT in Fig. 11 by replacing the PAND gate with an AND gate and inserting a repeated event E , as Example 4 shown in Fig. 13. The failure rates of the exponentially-distributed basic events are assumed to be the same as those in Example 3, while the non-exponentially distributed events J , K , L follow a Weibull distribution with $\alpha = 0.5$ and $\lambda = 2$.

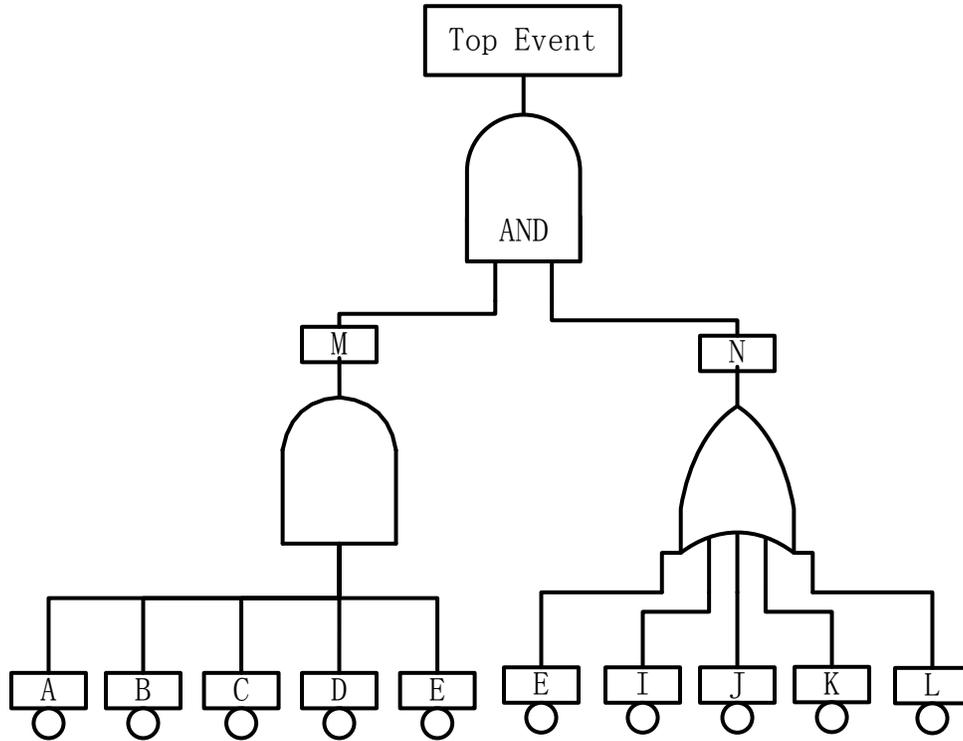


Fig. 13 Example 4: a fault tree with repeated events and non-exponentially distributed ones.

For this fault tree, the failure probability of the top event is plotted for a mission time of 300 hours, as shown in Fig. 14, for both the stochastic approach and the MC method [23]. A more detailed comparison is given in Table 5.

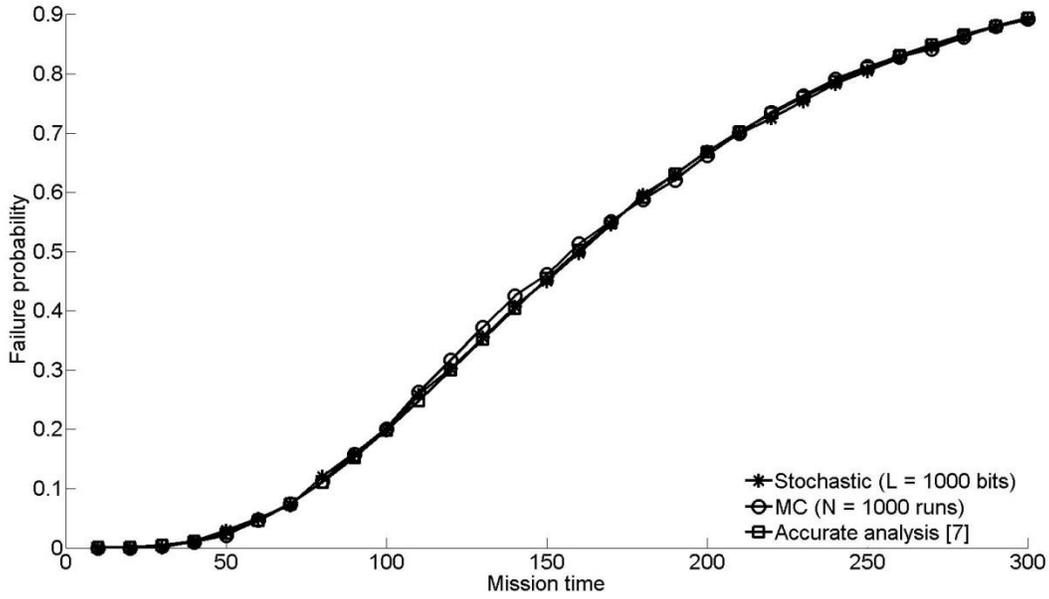


Fig. 14 The failure probability of the top event with non-exponentially distributed basic events.

Table 5. Accuracy comparison and run time of the stochastic approach and Monte Carlo (MC) simulation [23] for the DFT in Example 4.

Stochastic approach	L	$\ \Delta \mathbf{F}_{S-A}\ _1$	$\ \Delta \mathbf{F}_{S-A}\ _2$	$\ \Delta \mathbf{F}_{S-A}\ _\infty$	Average time (s)
	1k	0.9953	0.0747	0.0150	0.0947
	10k	0.4487	0.0348	0.0054	0.7499
	100k	0.0967	0.0081	0.0017	8.7146
MC simulation	N	$\ \Delta \mathbf{F}_{MC-A}\ _1$	$\ \Delta \mathbf{F}_{MC-A}\ _2$	$\ \Delta \mathbf{F}_{MC-A}\ _\infty$	Average time (s)
	1k	1.4800	0.1177	0.0203	8.3074
	10k	0.5461	0.0436	0.0081	85.366
	100k	0.1373	0.0123	0.0027	969.38

As revealed in Fig. 14 and Table 5, a stochastic analysis of the fault tree is more accurate

and more efficient than an MC method compared with the accurate analysis [7], as shown by the run time and norms of the differences in the failure probability vectors. Hence, a DFT with non-exponentially distributed basic events and repeated events can be efficiently evaluated by the stochastic approach.

VI. CONCLUSION

A stochastic model is proposed for the analysis of a two-input PAND gate in a dynamic fault tree (DFT). This model is then used in a successive cascading structure for the analysis of a general multiple-input PAND gate. For a DFT with PAND gates, a stochastic approach using the proposed models provides an efficient analysis of the DFT compared to an accurate or algebraic approach. The use of non-Bernoulli sequences of random permutations of fixed numbers of 1's and 0's as initial input event probabilities makes the stochastic approach more efficient and more accurate than Monte Carlo simulation. The stochastic approach has the following features:

- The failure probability of a basic event is not limited to an exponential distribution; any failure distribution can be analyzed by an appropriate sampling and coding into the stochastic non-Bernoulli sequences.
- Repeated events are correctly and readily handled in a DFT analysis, because signal correlation is maintained in the random binary bit streams and the propagation of the stochastic sequences in a fault tree analysis.
- The stochastic approach avoids the state-space explosion problem or the large computational complexity typically encountered in a Markov or analytical method, thus it is scalable for use in a general DFT analysis,

Ongoing work includes the stochastic modeling of other types of gates in a DFT and the incorporation of repair schemes and common cause failures into an FTA.

REFERENCES

- [1] Clifton A. Ericson II. "Fault tree analysis – a history". In Proceedings of the 17th International System Safety Conference, August 16–21, 1999.
- [2] Yuge T, Yanagi S. "Quantitative analysis of a fault tree with priority AND gates". *Reliab Eng Syst Safety* 2008; 93(11): 1577–83.
- [3] N.G. Leveson, "Safeware: System safety and computers". Addison-Wesley, 1995.
- [4] Boudali H, Crouzen P, Stoelinga M. "A rigorous, compositional, and extensible framework for dynamic fault tree analysis". *IEEE Transactions on Dependable and Secure Computing* 2010; 7(2): 128–43.
- [5] Stamatelatos, M. and W. Vesely (2002). "Fault Tree Handbook with Aerospace Applications". Volume 1.1, pp. 1–205. NASA Office of Safety and Mission Assurance.
- [6] E.J.Henley and H.Kumamoto, "Reliability Engineering and Risk Assessment". Englewood Cliffs: Prentice Hall, 1981.
- [7] Amari S, Dill G, Howald E. "A new approach to solve dynamic fault trees". In Annual IEEE reliability and maintainability symposium, 2003. p. 374–9.
- [8] M. A. Boyd. "Dynamic fault tree models: techniques for analyses of advanced fault tolerant computer systems". Phd dissertation, Dept. of Computer Science, Duke University, 1991.
- [9] J. B. Dugan, S. J. Bavuso, and M. A. Boyd. "Dynamic fault – tree models for fault-tolerant computer systems". *IEEE Transactions on Reliability*, 41(3): 363–377, September, 1992.
- [10] J.B. Dugan, K.J. Sullivan, and D. Coppit, "Developing a low–cost high–quality software tool for Dynamic fault-tree analysis," *IEEE Trans. Reliability*, vol.49, no, 1, pp.49-59, 2000.
- [11] G. Merle, J.-M. Roussel, J.-J. Lesage, A. Bobbio, "Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events," *IEEE Trans. Reliability*, vol. 59, no. 1, Mar. 2010, pp. 250-261.
- [12] Boudali, H., P. Crouzen, and M. Stoelinga (2007). "Dynamic Fault Tree analysis through input/output interactive Markov chains". In Proceedings of the International Conference on Dependable Systems and Networks (DSN 2007), pp. 25–38.
- [13] Ejlali, A. and S. Miremadi (2004). "FPGA-based Monte Carlo simulation for fault tree analysis". *Microelectronics Reliability* 44(6), 1017–1028
- [14] G. Merle, J.-M. Roussel and J.-J. Lesage. "Improving the Efficiency of Dynamic Fault Tree Analysis by Considering Gates FDEP as Static". In Proceedings of the European Safety & Reliability Conference 2010 (ESREL2010), Rhodes, Greece,

2010, pp 845–851.

- [15] Hananeh Aliee and Hamid Reza Zarandi. “A Fast and Accurate Fault Tree Analysis Based on Stochastic Logic Implemented on Field-Programmable Gate Arrays”. IEEE Trans on reliability volume: 62, issue: 1, page(s): 13 – 22, March 2013.
- [16] Xing L, Levitin G. “Combinatorial algorithm for reliability analysis of multistate systems with propagated failures and failure isolation effect”. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans 2011; 41(6): 1156–65.
- [17] L. Xing, “An efficient binary-decision-diagram-based approach for network reliability and sensitivity analysis,” IEEE Trans. Systems, Man, and Cybernetics, vol. 38, no. 1, pp. 105-115, Jan. 2007.
- [18] H. Boudali and J. B. Dugan, “A discrete-time Bayesian network reliability modeling and analysis framework,” Reliability Engineering and System Safety, vol. 87, no. 3, pp. 337–349, 2005.
- [19] O. Tannous, L. Xing, and J. B. Dugan, “Reliability Analysis of Warm Standby Systems using Sequential BDD,” in Proc. of The 57th Annual Reliability & Maintainability Symposium, FL, USA, 2011.
- [20] Liudong Xing, Ola Tannous, Joanne Bechta Dugan, “Reliability Analysis of Nonrepairable Cold-Standby Systems Using Sequential Binary Decision Diagrams”, IEEE Trans. on systems, man and cybernetics – part A: systems and humans, vol. 42, no. 3, May 2012.
- [21] A. Rauzy, "Sequence Algebra, Sequence Decision Diagrams and Dynamic Fault Trees," Reliability Engineering & System Safety 96(7):8, 2011
- [22] L. Xing, A. Shrestha & Y. Dai, "Exact Combinatorial Reliability Analysis of Dynamic Systems with Sequence-Dependent Failures," Reliability Engineering and System Safety 96(10): 1375-1385, 2011.
- [23] Durga RK, Gopika V, Sanyasi RV, et al. “Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment”. Reliab Eng Syst Safety 2009; 94 (4): 872–83.
- [24] H. Chen, J. Han, “Stochastic Computational Models for Accurate Reliability Evaluation of Logic Circuits,” Proc. Great Lakes Symp. VLSI (GLVLSI), Providence, RI, USA, pp. 61-66 (2010).
- [25] Jie Han, Hao Chen, Jinghang Liang, Peican Zhu, Zhixi Yang and Fabrizio Lombardi. “A Stochastic Computational Approach for Accurate and Efficient Reliability Evaluation”. IEEE Transactions on Computers, 2013, in press. Advance access in IEEE xplore.
- [26] Dugan JB, Bavuso SJ, Boyd MA. “Fault trees and sequence dependencies”. In: Proceedings of the Reliability and

Maintainable Symposium; 1990. p. 286–93.

[27] B. R. Gaines, “Stochastic Computing Systems,” *Advances in Information Systems Science*, Vol. 2, pp. 37-172, 1969.

[28] J. von Neumann, “Probabilistic logics and the synthesis of reliable organisms from unreliable components,” *Automata Studies*, Shannon C.E. & McCarthy J., eds., Princeton University Press, pp. 43-98, 1956.

[29] Jie Han, “Fault-Tolerant Architectures for Nanoelectronic and Quantum Devices”, Universal Press, Veenendaal, The Netherlands, 2004. A Ph.D. dissertation of the Delft University of Technology, 1-135. ISBN: 90-9018888-6.

Author biographies:

Peican Zhu received the B.S. degree in 2008 and the M.Sc. degree in 2011, both from the Northwestern Polytechnical University (NWPU), Xi'an, Shaanxi, China. He is currently working towards the Ph.D. degree in the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada.

His current research interests include stochastic computational models for system reliability analysis, gene network models and pathway analysis.

Jie Han received the B.Sc. degree in electronic engineering from Tsinghua University, Beijing, China, in 1999 and the Ph.D. degree from Delft University of Technology, The Netherlands, in 2004. He is currently an assistant professor in the Department of Electrical and Computer Engineering at the University of Alberta, Edmonton, AB, Canada.

His research interests include reliability and fault tolerance, nanoelectronic circuits and systems, novel computational models for nanoscale and biological applications. Dr. Han was nominated for the 2006 Christiaan Huygens Prize of Science by the Royal Dutch Academy of Science (Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) Christiaan Huygens Wetenschapsprijs). His work was recognized by the 125th anniversary issue of *Science*, for developing theory of fault-tolerant nanocircuits. Dr. Han served as a General Chair and Technical Program Chair in IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS) 2013 and 2012, respectively, and as a Technical Program Committee Member in several other international symposia and conferences.

Leibo Liu received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1999 and the Ph.D. degree in Institute of Microelectronics, Tsinghua University, in 2004. He currently serves as an Associate Professor in Institute of Microelectronics, Tsinghua University. His research interests include Reconfigurable Computing, Mobile Computing and VLSI DSP. Dr. Liu has published more than 70 refereed papers, and served as TPC member or reviewers for several international key conferences and leading journals.

Dr. Ming J Zuo received the Bachelor of Science degree in Agricultural Engineering in 1982 from Shandong Institute of Technology, China, and the Master of Science degree in 1986 and the Ph.D. degree in 1989 both in Industrial Engineering from Iowa State University, Ames, Iowa, U.S.A. He is currently Professor in the Department of Mechanical Engineering at the University of Alberta, Canada. His research interests include system reliability analysis, maintenance modeling and

optimization, signal processing, and fault diagnosis. He is Associate Editor of IEEE Transactions on Reliability, Department Editor of IIE Transactions (2005-2008, 2011-present), Regional Editor for North and South American region for International Journal of Strategic Engineering Asset Management, and Editorial Board Member of Reliability Engineering and System Safety, Journal of Traffic and Transportation Engineering, International Journal of Quality, Reliability and Safety Engineering, and International Journal of Performability Engineering. He is Fellow of the Institute of Industrial Engineers (IIE), Fellow of the Engineering Institute of Canada (EIC), Founding Fellow of the International Society of Engineering Asset Management (ISEAM), and Senior Member of IEEE.