4

Dynamic Fault Tree Analysis: State-of-the-art in modelling, analysis and tools

4.1 Introduction

Safety-critical systems have become an integral part of our life. Over the years, new functionality and capabilities have been added to such systems, and information and communication technologies are increasingly used to make them more sophisticated. While additional features and sophistication bring significant benefits, this leads to additional complexity, making the system development and assuring safety and reliability properties more challenging. Safety is the avoidance of harm to people and the environment, and reliability is the ability to perform the intended function uninterrupted by a failure, which is often a precondition for safety. Both properties are crucial, and as systems become more complex, their prediction via analysis plays a vital role in the successful design and development of the system. Safety and reliability analysis are important tasks performed throughout the system lifecycle, which systematically explore the potential safety related issues in a system to verify whether a system is safe to use or not.

Over the years, several methodologies have been developed to facilitate safety and reliability analysis of systems. Among them, Fault Tree Analysis (FTA) is one of the oldest and most popular techniques widely used to perform safety and reliability analysis of systems. In traditional FTA, systems and their components are usually consider to have two states: *working* and *failed*. To model the logical interaction between different failure events Boolean AND and OR gates are used, and the causes of system failure are determined in the form of combinations of events. To facilitate reliability analysis, each of such component can have its probability of failure or failure rate or distribution of time of failure or steady-state or instantaneous (un)availability defined. At the same time, if the component can be repaired then a repair rate is defined. However, modern large scale complex systems have the capacity to work in different states and they can have a complex repair process. A component in such system can work as a primary component at a particular point in time, and in another time instance the same component can work as a secondary component. Moreover, if a component acts as a spare component in a system, it can be in a different mode of spare such as cold, warm, and hot spares.

Such multi-modal operation capability of systems and complex interactions between their components gives rise to different dynamic failure characteristics like priorities among events and functionally dependent events. However, using a classical fault tree approach it is not possible to explicitly consider system dynamics and sequencing/timing of events while performing analyses, which may produce inaccurate results (Kabir, 2017). The limitations of the classical analysis techniques have not gone unnoticed and it was recognised that methodologies with more powerful modelling capabilities are required to take into account the dynamic behaviour of systems for a comprehensive and accurate analysis of complex systems.

Several attempts have reported in the literature to improve the modelling power of SFTs through augmentation to include different types of temporal and statistical dependencies in the FT model. In 1976, the concept of Priority-AND (PAND) gate was introduced by Fussell et al. (1976). Later, several extensions to the SFTs such as the DFT (Dugan et al., 1992, 2000), temporal fault trees (Palshikar, 2002; Walker, 2009), and State/event fault trees (Kaiser et al., 2007) have been proposed. Among these extensions, DFT is the most popular dynamic extension of SFTs. The DFT retains the PAND gate and additionally, it introduces new dynamic gates like Functional Dependency (FDEP), SPARE and Sequence Enforcing (SEQ) gates.

Over the years, significant advancement has been made in the area of dynamic system analysis using DFTs. In this chapter, we reviewed different such development in DFT analysis, which include both qualitative and quantitative analysis approaches for DFT analysis. Development in qualitative analysis started with the extension of the concept of minimal cut sets of SFTs to the minimal cut sequences (MCSQs) of DFTs. This was followed by the introduction of approaches for the determination of MCSQs from the structure of DFTs. On the other hand, the development in the quantitative analysis area mainly focuses on the quantitative evaluation of the top event of the DFT based on the quantitative failure behaviour related information, e.g. failure rate or probability of the basic events. To accomplish this task, a number of existing approaches such as Markov models, Bayesian networks, Petri nets, mathematical formulations, and simulations have been utilised. In addition, uncertainty analysis through importance measure and sensitivity evaluation of DFTs is another important area that received noticeable attention from both academia and industries. Regarding the uncertainty handling in DFT analysis, application of fuzzy set theory has been reported in the literature, a brief review of those methods will also be provided. Moreover, developed software and applications with the ability of handling DFTs will be reviewed. The capabilities and limitations of those applications will be addressed briefly.

In addition to reviewing the above developments in DFT analysis, as a state-of-the-art in future trends and cutting-edge research, a combination of machine learning with reliability models especially DFTs will be discussed.

The combination of machine learning with reliability models can be classified into five main categories; I) Using the reliability model as a core in Machine Learning with the aim of fault detection and diagnosis, II) Selection of predefined and co-evaluated models through Machine Learning, III) Updating the value of failure rates through Machine learning-based algorithms, IV) Reconfiguration of DFTs through process mining, and V) Updating the membership functions of fuzzy models via Machine Learning. The paper will be finalized through a concise discussion on the current challenges and potential future trends in DFT-related research.

4.2 Overview of DFT

DFT has a similar logical structure to its static counterpart. The event at the top of the tree is known as the top event (TE), which almost always represents a system failure. This top event is decomposed into a combination of intermediate events (IE). Unlike the static fault tree, DFT uses both Boolean and dynamic gates to specify logical relationships among events to represent the IEs. IEs are further decomposed down to lowest-level events, which are known as basic events (BEs).

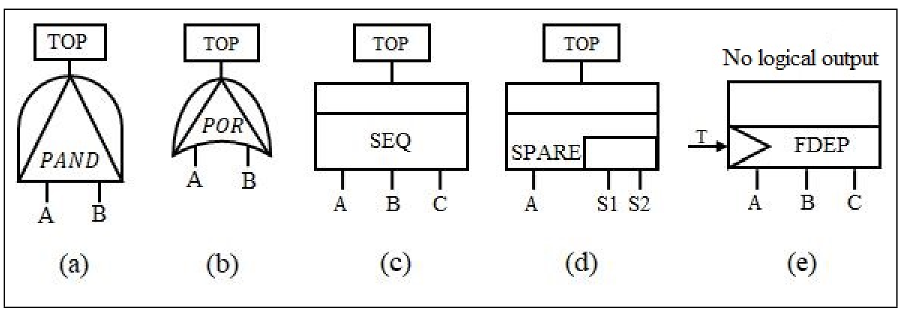


FIGURE 4.1
DFT Logic Gates

To allow the fault tree to model sequence/time dependent failure behaviour of systems, several dynamic gates have been introduced. Fig. 4.1 shows the commonly used DFT gates. Priority-AND (PAND) gate is a special version of the AND gate. It delineates the priority behaviour in a dynamic system. In this gate, the output will be true when both inputs occur and the first input (event A) occurs sooner than the second input (event B). In other words, the occurrence time of event A should be less than the occurrence time of event B and both of them should fail to have the failure as the output of this gate. Like the PAND gate, the Priority-OR (POR) gate also delineates a sequence, however, it defines an ordered disjunction rather than an ordered conjunction. In this gate, first input (event A) has priority over other inputs. This event must happen first for the POR gate output to be true, but does not require all other events to occur (Walker, 2009). If other non-priority events occur, they must occur after the priority input. The Sequence-Enforcing gate (SEQ) gate represents the sequential failure behaviour of events A, B and C respectively. It means events B and C cannot fail before the failure of event A. Also, event C cannot fail before the failure of event B.

The SPARE gate is used to model redundancy in system design. The inputs to the SPARE are all BEs. The leftmost of the input corresponds to a primary event and other inputs represent spare components. In SPARE gate of Fig. 4.1(d), the input A is the primary component and S1 and S2 are two spare components. The behaviour of this gate is defined as such that when the primary component (A) fails the first spare (S1) will be activated; and if S1 fails then S2 will be activated. Finally, the outcome of the gate will become true when all of its inputs become true. A SPARE gate can represent three different types of dynamic redundancy; I) CSP: Cold Standby Spare in which the spare parts will be activated to be replaced when the primary unit (A) fails. That means in the cold spare mode the spare components are deactivated until they are required. II) HSP: Hot Standby Spare in which the spare part starts to work in parallel with primary unit and when it fails the spare part will be replaced immediately. III) WSP: Warm Standby Spare in which the spare part partially works in parallel with the primary unit to be replaced when needed. In other words, the spare components are neither on nor off, instead they are kept in-between these two states, i.e., components are kept in a reduced readiness state until required.

The Functional dependency (FDEP) gate represents the functional dependency of some events to another trigger event. This gate helps to design a scenario when the operations of some components of a system are dependent on the operation of another component of the system. For example, when many components of a system receive power from a single source of supply, then failure of the power supply would cause all the dependent components to fail. In the FDEP gate there is only one trigger event (either a basic event or an intermediate event) but there could be multiple functionally dependent events. As illustrated, the event T is the trigger event and the events A, B, and C are the dependent events, and they will fail if T occurs. In other words, those events (A, B, and C) are functionally dependent to event T. However, they can have their own individual failure, which will not affect the occurrence of the trigger events. The FDEP gate is particularly useful for modelling networked systems, where communication between connected components takes place through a common network element, and failure of the common element isolates other connected components. This type of gate can also model interdependencies, which would otherwise introduce loops in the fault trees.

4.3 DFT Analysis Methodologies

As DFTs introduce dynamic gates in classical fault trees, the typical combinatorial analysis techniques available for classical fault tree analysis cannot be directly applied to analyse DFTs. Several methodologies have been developed for both qualitative and quantitative analyses of DFTs. Qualitative analysis mainly focuses on determining cut sequences from DFTs. On the other hand, quantitative analysis aims at determining the probability of the top event given the failure rate or failure probability or failure probability distribution of the basic events of the DFTs. Additionally, criticality analysis of events is also performed as part of quantitative evaluation of DFTs. The approaches used for developing methodologies for DFT analysis include, but not limited to, Markov models, Petri Nets, Bayesian Networks, Analytical solution, and Monte Carlo simulation. In the following subsections, we briefly discussed the qualitative and quantitative analysis approaches for DFTs.

4.3.1 Qualitative Analysis of DFTs

In a qualitative analysis of traditional static fault trees, minimal cut sets (MCSs) are determined from the fault tree structure. An MCS represents the minimal combination of events that can cause the top event of the fault tree. An MCS-based qualitative analysis of a DFT is possible if the dynamic gates of the DFT are replaced by static gates. For instance, by replacing the FDEP gates by OR gates and replacing PAND and SPARE gates by AND gates. However, in this case, the temporal dependencies between events would not be retained. In (Xiang et al., 2012), a method was proposed to allow combinatorial analysis of DFT with priority-AND gate only. In their work, the PAND gate was transformed to an AND gate by adding some conditioning events and the new gate was called CAND. The work was later extended in (Xiang et al., 2013).

To capture the temporal dependencies between events, the concept of minimal cut sequences (MCSQ) was proposed by Tang and Dugan (2004). An MCSQ is the minimal sequence of events that is sufficient and necessary to cause the top event of the DFT. To generate the cut sequences for a DFT, the zero-suppressed binary decision diagrams (ZSBDD) (Minato, 2001) were used. It was shown that the dynamic gates can be replaced by the static gates to determine the cut sets and then cut sequences can obtained by adding necessary sequencing information into the cut sets. Later, for cut sequence generation, Liu et al. (2007a) proposed an algorithm called Cut sequence set algorithm (CSSA) using the notion of sequential failure symbol (SFS). SFS is a mechanism to describe the sequential failure between two independent events. Later, the concept of the extended cut sequence was proposed based on the general cut sequence by Zhang et al. (2011). In the above approaches, the concept of cut sequence was under the assumption of non-repairability of system components. In (Chaux et al., 2013), a new definition of cut sequences was provided for binary systems, i.e., the system can either be in working or in failed states, with repairable components.

In (Walker, 2009), Walker proposed a qualitative analysis approach for the Pandora temporal fault tree. He also provided temporal laws for to facilitate the minimization of the temporal sequences of events. One year later, Merle (2010) introduced an algebraic method for determining and expressing cut sequences of dynamic fault trees. This approach was based on the extension of the structure function used for classical static fault tree analysis. In (Rauzy, 2011), Rauzy introduced a variant of ZSBDD approach proposed in (Minato, 2001) to include sequencing information. This variant can be used for the determination of cut sequences of DFT. In (Kabir et al., 2017), a model-based approach was proposed for qualitative analysis of dynamic failure behaviour of systems. Elderhalli et al. (2017) integrated theorem proving and model checking to propose a comprehensive approach for qualitative and quantitative analysis of DFTs. Most recently, Piriou et al. (2019) provided a new definition of MCSQ for dynamic, repairable and reconfigurable systems. Afterwards, an algorithm was proposed to derive the MCSQs from Generalized Boolean logic Driven Markov Processes (GBDMP) (Piriou et al., 2017) models.

4.3.2 Quantitative Analysis of DFTs

A brief taxonomy of DFTs' quantitative solution techniques reviewed in this chapter is shown in Figure 4.2. The meaning of each sign has been explained at the bottom of the figure. As an example in this figure, 'R' sign stands for the ability to model and solve the repairable DFTs, 't' refers to a time consuming procedure, and 'D' means the solution is applicable for on-demand safety analysis.

4.3.2.1 Algebraic Solutions for DFTs

In SFTs, mathematical formulas are often used to quantify the probability of the Boolean gates, thus evaluating the probability of the MCSs and the top event. However, in DFTs, the logic gates not only model the effects of a combination of events, but also the effects of the order of the failure. By taking the sequencing into account, at first, Fussell et al. (1976) provided an algebraic method to find an approximate solution to the Priority-AND gate. In 2000, Long et al. (2000) provided a solution for DFT with priority-AND gate. In their work, they use sequential failure logic (SFL) to model the behaviour of the PAND gate and then mathematical equations with multiple integration was proposed to quantify the SFL model.

There are algebraic approaches which utilised the inclusion-exclusion (IE) method to determine the MCSQs of the DFT first. Subsequently, the IE principle is used to quantify the MCSQs to determine the probability of the top

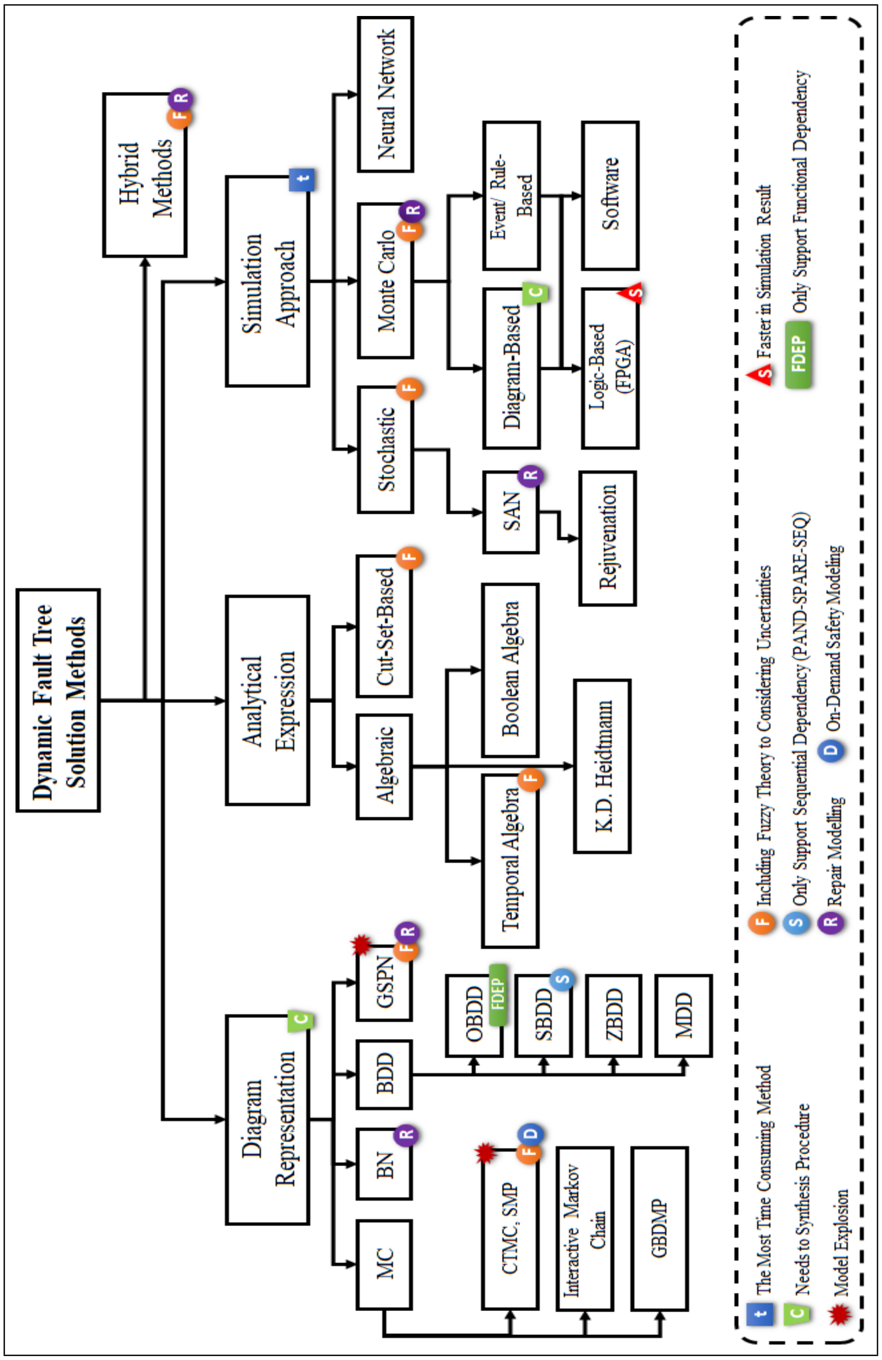


FIGURE 4.2
Taxonomy of solutions for DFTs

event. One such approach is (Liu et al., 2007b), which used the similar technique like (Long et al., 2000). In this work, MCSQs are expressed as sequential failure expressions (SFE) and SFE are solved using different multi-integration formulas. Finally, the top event probability is evaluated by summing the probabilities of different SFEs. At the same time, Yuge and Yanagi (2008) proposed an algebraic method for computing the exact top event probability of the DFT containing PAND gate and repeated events. This approach also assumed that the basic events are statistically independent, exponentially distributed, and the components associated with the events are non-repairable. Note that, the above mentioned methods can quantify DFTs with PAND gate only, not with other dynamic gates like SPARE gate. By considering all the dynamic gates of DFTs, Merle et al. (2010, 2011) determined the structure function of any DFTs and then proposed an algebraic framework for algebraically modelling DFTs' gates. This initial solution was only applicable to exponentially distributed data. Later, an extension was proposed in (Merle et al., 2014, 2016) to consider non-exponentially distributed data. Based on Merle's work, Edifor et al. (2012) proposed an algebraic approach to solve Priority-OR gate of temporal fault trees. Ni et al. (2013) proposed a new algebraic framework for quantitative analysis of DFTs by taking Boolean state, probability and timing of events into account. The framework modelled the behaviour of the gates in three steps. In the first step, the Boolean functions are converted into the sum-of-product forms. Then the repeated events are eliminated as much as possible. Final step reduces the structure of the complex inclusion-exclusion formula. For implementing the concept, they used the variable array definition. To improve the computational efficiency of the existing algebraic approaches and to make them applicable for analyzing highly coupled DFTs, Ge et al. (2015b) proposed an approach by using adapted K.D. Heidtmann algorithm (Heidtmann, 1989). In (Aliee and Zarandi, 2013), stochastic logic has been used to propose equivalent templates for static and dynamic gates of the DFTs, and provided a fast solution to DFTs using FPGA based implementation.

Note that all the above algebraic approaches for DFT analysis require precise failure rate or failure probability data of the basic events to be able to perform the analysis. However, in practical applications, it is difficult to obtain precise failure data for all the basic events for complex systems. Fuzzy set theory has been widely with classical SFTs to address the issue of data uncertainty(Garg, 2014; Garg et al., 2014a). Fuzzy set theory based concept has also been used by Garg et al. (2014b) and Garg and Sharma (2011) to provide a solution to bi-objective and multi-objective reliability-redundancy allocation problem under the condition of uncertainty, respectively. A comprehensive review of fuzzy set theory based relaibility analysis approaches is available in (Kabir and Papadopoulos, 2018). However, the application of fuzzy set theory to facilitate DFT analysis under the condition of uncertainty is still not prevalent. Only a handful of approaches such as (Verma et al., 2006; Ping, 2011; Jiang et al., 2018) utilised fuzzy set theory for uncertainty handling in DFT analysis. For instance, Jiang et al. (2018) proposed a method for fuzzy DFT analysis using the concept of weakest n-dimensional t-norm arithmetic operations on fuzzy sets. The authors used sequential binary decision diagram (SBDD) to model the dynamic behaviour of systems. Subsequently, SBDD is transformed into DFTs. In the quantitative analysis of DFTs, to handle uncertainty in failure data, fuzzy set theory has been utilised. The weakest n-dimensional t-norm arithmetic operations are used on fuzzy failure data of basic events, thus allowing reducing fuzzy accumulation. There are a couple of approaches (Kabir et al., 2014a, 2016) that utilised fuzzy set theory to handle data uncertainty in temporal fault tree analysis. In these approaches, fuzzy operators for the temporal gates have been developed first. Subsequently, fuzzy failure rates of basic events of DFT were used in the fuzzy operators of the logic gates to evaluate the top event probability of the DFTs. Most recently, intuitionistic fuzzy set theory has been combined with expert elicitation by Kabir et al. (2020) to quantify temporal fault trees with uncertain data.

4.3.2.2 Markov Models for quantifying DFTs

Solving the DFT by the use of Continuous-Time Markov Chain (CTMC) is regarded as one of the first and most important solution methods developed for quantitative evaluation of DFTs. This method has been employed in the structure of software tools such as Galileo, DIFtree and HiRel (Dugan et al., 1997; Bavuso et al., 1994).

As shown in Figure 4.3, Markov models can be categorized into five types; I) Homogenous Continuous Time Markov Chain (HCTMC) known as a traditional CMTC and it can model failures with exponential probability distribution with constant failure rates. II) The second type is the Non-Homogenous Continuous Time Markov Chain (NHCTMC) that can model global clock and exponential type failures with time variant failure rates. III) Semi-Markov Process (SMP) is the third category that enables to consider non-exponential probability distributions and renewal processes. IV) The fourth category is Markov Regenerative Process (MRGP) which is capable of considering operational mode changes in one transition. V) The Phased Type Markov Process (PH) is the last category and it can model multiple general distributions through diving the systems' states into some degraded states (more degraded states more accuracy) (Trivedi and Bobbio, 2017). It should be noted that there are some other extensions of Markov models such as Input/output Interactive Markov Chains and Generalized Boolean logic Driven Markov Processes (GBDMP) which are obtained from the combination of Markov theorem and Automata. In fact, each of those introduced Markov types can be merged with Automata or similar theories to generate the extended versions. In Figure 4.3, the modelling capability is increasing from top to bottom while the complexity of computation is also raising. Having categorized Markov models, the use of these models for reliability evaluation of DFTs is briefly studied as follows. In 1991, the first concept of dynamic fault tree and its dynamic gates

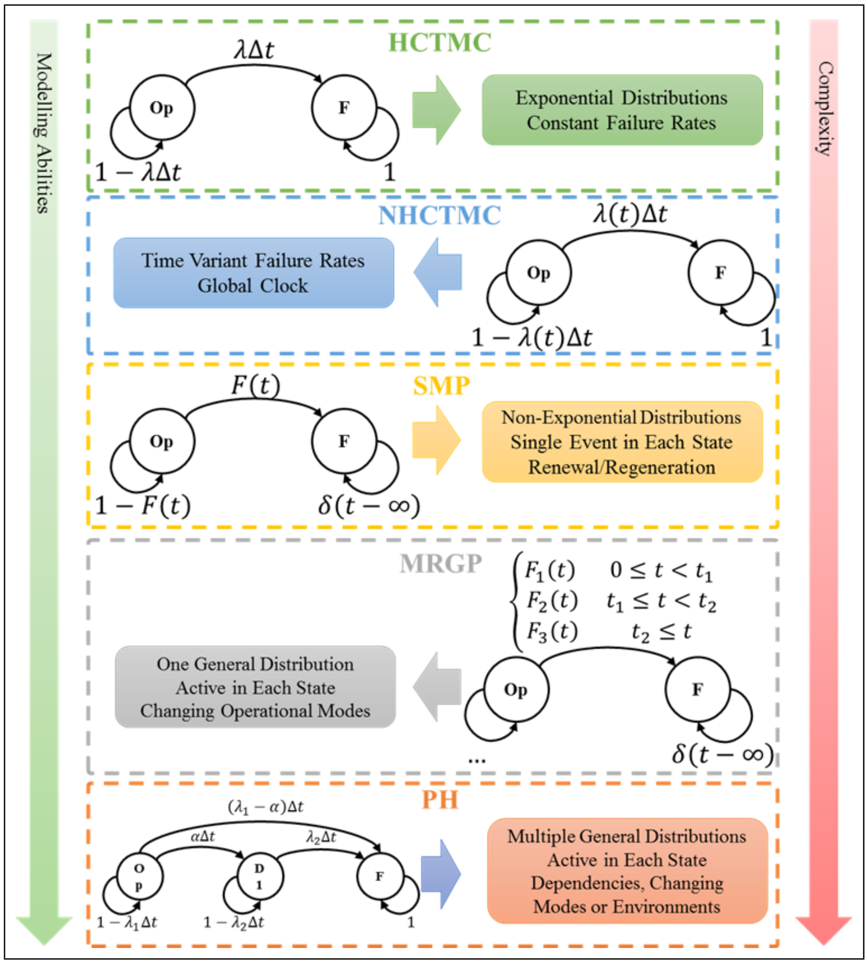


FIGURE 4.3
Classification of Markov Models

such as PAND, SPARE, SEQ and FDEP have been introduced through their CTMCs (Boyd, 1992). The reference also recommended an automatic way for conversion of DFT to its equivalent Markov Chain. Following this, in 1993, evaluation of the system behaviours considering imperfect coverage has been studied (Dugan et al., 1993). Two benchmarks named Fault Tolerant Parallel Processors (FTPP) and Mission Avoidance Systems (MAS) that are used later by many researchers, were also introduced in this article. The reliability analysis of DFT in the presence of transient and permanent faults, failure dependencies, recovery of a system and reconfiguration of FTPP benchmark was studied in (Dugan, 1993). From 1993 to 2009 several studies have been performed to address different issues such as the accuracy of conversion procedure from DFT to CTMC (Manian et al., 1999), uncertainty analysis (Yin et al., 2001), imperfect coverage consideration (Vesely et al., 2002), decomposing DFTs into independent modules (Huang and Chang, 2007), introducing new Markov models for components' failures (Dominguez-Garcia et al., 2008), considering repeated events and their effects in state-space modelling (Yuge and Yanagi, 2008) in DFT-based reliability analysis.

In 2009, Norberg et al. (2009) presented a model for merging static fault tree with availability CTMC, so that it could evaluate the risk parameter. By the use of this method, reliability, risk, availability, failure rate, failure interval, MTBF and MTTF were induced from fault tree. This paper employed this method on drinking water supply system. Verma et al. (2010) studied different methods for reliability modelling and then discussed the behaviour of dynamic gates along with CTMC. In addition, they described DFT solutions by the use of CTMC and Monte Carlo theories. Although, in general, the CTMC-based approaches are applicable only to exponentially distributed data, Guo et al. (2011) proposed an approach combining failure rates with Weibull distribution with CTMC. Zixian et al. (2011) reprorted a widespread use of reliability methods in evaluating the risk of surgery and with this purpose, they evaluated time independent risk and time dependent risk through merging CTMC and static fault tree. By calculating failure rate of medical facilities, they evaluated surgery frequency, rescue timeliness and risk of gastric-esophageal surgery using fault tree. Then by using sensitivity analysis, the effect of retrieval time factor and rescue timeliness was measured. A Power Factor Correction (PFC) using CTMC in DFT of power systems has been presented in (Ranjbar et al., 2011).

In 2012, the Fuzzy-CTMC models have been proposed by Li et al. (2012) to solve the Fuzzy DFTs and evaluate their reliability under the condition of uncertainty. They presented an example of automatic hydraulic system cutting machine (CNC). Their study only considered a dynamic fault tree example with FDEP gate and fuzzy evaluation of other gates are left vague. This fuzzy approach was also used in another paper for the reliability evaluation of driver in array of solar cells (Huang et al., 2013). A year later, the statistical reliability evaluation of a dynamic fault tree with PAND gate has been proposed by Xiang et al. (2013) in which the conversion of the PAND gate into AND gate along with considering some dependent conditional events was introduced. Moreover, the newly introduced AND gate called CAND was assumed to be dependent upon conditional events. In this study, CTMCs for PAND and CAND gates were provided with a discussion about their differences and used in the reliability evaluation of FTPP's benchmark. The combination of BDD and CTMC for reliability evaluation of DFTs has been introduced in (Hao et al., 2014).

The use of Shannon's decomposition theory has been proposed by Ge and Yang (2015) to solve DFTs. The proposed method increased the computational efficiency. However, the paper only considered PAND gate and the method was not generalized for other dynamic gates. Brameret et al. (2015)

proposed a framework called “AltaRica” to reduce the state explosion through combining the Dijkstra’s algorithm and notion of the distance factor for the DFT solution. An approximate solution for DFT through truncating Markov chain states has been presented in 2016 by Yevkin (2016).The method was appropriate for both repairable and non-repairable systems. In 2017, the research work of Ge and Yang (2015) has been extended and published in (Ge and Yang, 2017). The research has covered spare and sequence gates through De Morgan theorem, and for negating a generalized cut sequences, they have improved explicit formula. In 2018, a new state-space generation approach for solving the DFTs has been proposed by Volk et al. (2018). The presented method has the ability of model reduction through model checking theories. A hierarchical and approximate solution for availability analysis in DFTs based on equivalent two-state Markov models has been proposed by Ramezani et al. (2016). Their approach was only tailored for exponential failure distribution based events. An automated tool for the evaluation of repairable DFT has been presented by Manno et al. (2014). The paper proposed a mapping from DFT entity to adaptive transition system entity, and a conception of failure gates for the evaluation of both reliability and availability has been illustrated. This paper used the SMP for reliability evaluation of DFTs. A novel hierarchical SMP-based solution for reliability assessment of DFTs was also proposed by Aslansefat (2014) in which the computational complexity and the state explosion of the SMP have decreased significantly.

As mentioned before, Input/Output Interactive Markov Chain (I/O IMC) is an extension for CTMC which is used for DFT solutions (refer to (Hermanns, 2002; Crouzen, 2006; Boudali et al., 2007b,a, 2010; Arnold et al., 2013a,b)). The use of I/O IMCs can reduce state space explosion. In addition, these models enable us to consider the standby spare behaviours in the basic events. Generalized Boolean logic Driven Markov Processes (GBDMP) another extension of Markov Process has been also used for qualitative and quantitative analysis of the DFT by Piriou et al. (2017). Moreover, Sequential Binary Decision Diagram (SBDD) and its extensions have been used in (Xing et al., 2011; Xing et al., 2012; Tannous et al., 2011; Ge et al., 2015a, 2016) for quantitative evaluation of DFTs. Markov process has been used by Niwas and Garg (2018) to propose an approach to evaluate the reliability, availability of an industrial system under the cost free warranty policy, where where the working period of a system is followed by a rest period. To address the issue of uncertain failure data in Markov chain based reliability evaluation, Garg (2015) used a fuzzy Markov model of a repairable system to develop the the n^{th}-order fuzzy Kolmogorov’s differential equations. Later the fuzzy reliability of the system both in transient and steady state was evaluated using Runge–Kutta method. Aslansefat and Latif-Shabgahi (2019) article is one of the recent research works that proposed a novel hierarchical SMP-based approach as a solution for reliability evaluation of DFTs. The paper presented a number of hypothetical and industrial examples. It also has an example related to the repair consideration in DFTs and its SMP-based solution.

4.3.2.3 Petri Nets for quantifying DFTs

Petri nets are formal graphical and mathematical modelling scheme used widely for the specification and analysis of complex, distributed and concurrent systems. Graphically a PN model is represented by a directed bipartite graph composed of a set of places, a set of transitions, and a set of directed arcs. PNs have been widely used in systems safety and reliability analysis domain, and a review of PN-based safety, reliability, and risk assessment approaches is available in (Kabir and Papadopoulos, 2019).

Early application of PNs to evaluate static fault trees can be found in (Hura and Atwood, 1988; Malhotra and Trivedi, 1995; Liu and Chiou, 1997; Bobbio et al., 2003). The underlying reachability graph of a PN model is isomorphic to Continuous Time Markov Chain (CTMC) and there are established approaches for mapping between CTMCs and PNs. As a result of this, similar to Markov chains, PNs are also used to solve DFTs. In the literature, the readers can find many extensions of PNs that can model transitions governed by both exponentially and non-exponentially distributed rates. For instance, the use of Weibull distribution in PN was shown in (Fecarotti et al., 2016; Le and Andrews, 2016) and in addition to the Weibull distribution, the use of other types of distributions such as normal and lognormal distribution was shown in (Bernardi et al., 2011; Volovoi, 2004). A number of Petri net tools that can offer the above mentioned modelling capability are reported in (Longo et al., 2016). Therefore, while the Markov chain based approaches are applicable only to systems with exponentially distributed lifetime, the PN-based approaches can be used for the analysis of systems with both exponentially and non-exponentially distributed lifetime. Moreover, approaches had been developed in (Knezevic and Odoom, 2001; Garg, 2013) to address the issue of uncertainty in failure data in PN-based reliability analysis.

The first approach to evaluate DFTs via Petri nets was provided by Codetta-Raiteri (2005). In her approach, she provided graph transformation rules to translate dynamic gates of DFT to Petri nets. Similar approaches for evaluating DFTs and temporal fault trees were proposed in (Zhang et al., 2009; Herscheid and Tröger, 2014; Kabir et al., 2015; Junges et al., 2018) as well. In the DFT to PN transformation process, each basic events and logic gates of a DFT is translated into a sub-net and then all the sub-nets are combined together to form the PN model of the DFT. Fig. 4.4 shows the PN model of a BE of a DFT. A token (the black dot) in the place *x.up* represents that at the beginning of system operation the component associated with the BE x is fully functional, i.e., BE has not occurred. The firing rate of the timed transition *x.f* is determined according to the failure rate of the component represented by this BE. If the component has an exponentially distributed failure rate λ, then the probability of the transition *x.f* firing at time t is $1 - e^{-\lambda t}$. As mentioned earlier, in a PN model, this kind of timed transitions can be characterised by non-exponentially distributed failure rate as well. On firing of the transition $x.f$ the place $x.dn$ will get a token, which will mark the occurrence of the basic event, i.e., failure of the corresponding component.

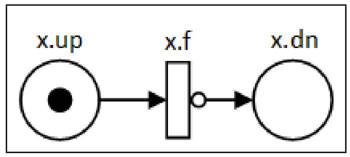
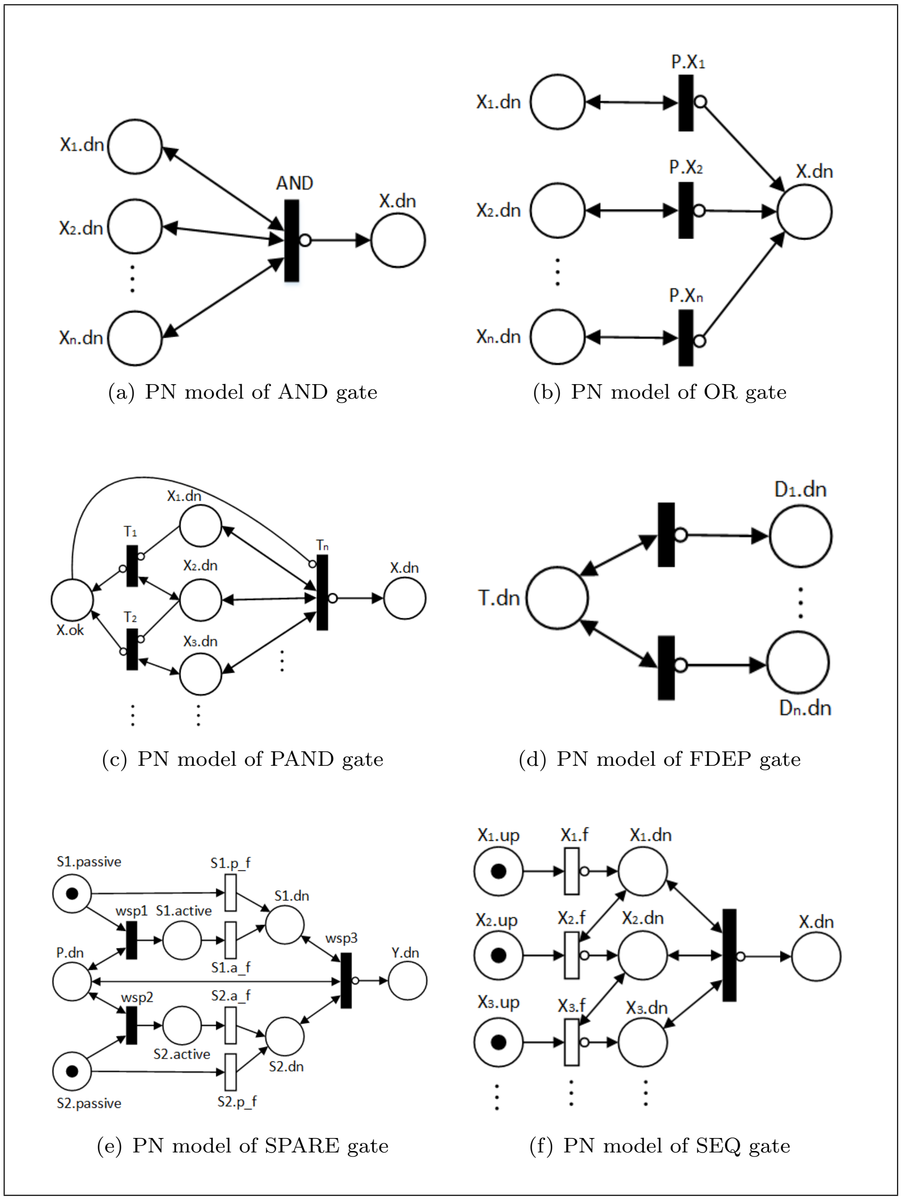


FIGURE 4.4
PN of a BE

Fig. 4.5 shows the PN models of the Boolean and dynamic gates used in DFTs. As seen in the PN model of the AND gate in Fig. 4.5(a), all input places: $X_1.dntoX_n.dn$ are connected to the single immediate transition called *AND*. That means when all the input places get a token each then the transition *AND* will fire to make the AND gate output true by depositing a token to the place $X.dn$. In the contrary, the PN model of the OR gate in Fig. 4.5(a) models a disjunctive behaviour. In this model, each of the input places $X_i.dn$ is connected to a distinct immediate transition. This will ensure that whenever any of the input places get a token the respective transition will fire to make the OR gate output true by depositing a token to the place $X.dn$. The PN model of the PAND gate is shown in Fig. 4.5(c). This PN model is designed in such a way that will ensure that the place ($X.dn$) representing the output of the PAND gate will get a token if and only if the input places get token in a sequential order, i.e., the occurrence of the BEs obey the required sequencing. If the order of occurrence of the BEs is violated, the place $X.ok$ will get a token, which will eventually prohibit the transition T_n from firing, thus forcing the PAND output to be false.
It is seen in section 4.2, the FDEP gate does not have a logical output, but the occurrence of the trigger event would force the dependent events to fail. In the PN model of the FDEP gate in Fig. 4.5(d), the place $T.dn$ would get a token if the trigger event occurs, and in the presence of a token in the place $T.dn$ will cause all the immediate transitions to fire to deposit tokens to the places $D_i.dn$, thus forcing the dependent events to fail. The PN model of Fig. 4.5(e) models a hot SPARE gate with a primary component P and two spare components *S1* and *S2*.
At the beginning of system operation, the primary component acts as the active component and the spare components are in passive mode, which is represented by the tokens in places *S1.passive* and *S2.passive*. The places *S1.dn* and *S2.dn* represent the failed state of the two spare components. It can be seen in the figure that as the spare components are in the hot spare mode their failed states can be reached in two different ways. Firstly, they can go to the $S_i.dn$ state from their passive mode through the firing of transitions $S_i.p\_f$, which are the failure rates of the components in the passive mode. Secondly, the spare components will reach to their active states (represented



(a) PN model of AND gate

(b) PN model of OR gate

(c) PN model of PAND gate

(d) PN model of FDEP gate

(e) PN model of SPARE gate

(f) PN model of SEQ gate

FIGURE 4.5
PN models of Boolean and dynamic gates

by places *Si.active*) due to the failure of the primary component, and then their failed state can be reached from the active state through the firing of the transitions $S_i.a\_f$.
The PN model of the SEQ gate is presented in Fig. 4.5(f). This model ensures that the input events of the SEQ gate will occur in a predefined sequence. For instance, in this model, the place $X_1.dn$ will get a token when the transition $X_1.f$ fires. However, the transition $X_2.f$ would not fire to deposit a token to $X_2.dn$ until $X_1.dn$ gets a token. This means the event X_2 cannot occur until the event X_1 occurs. This way the model ensures all the events in the SEQ gate will occur in a sequence and the occurrence of all the events will put a token in the place $X.dn$, denoting the occurrence of the output of the gate. Given the transformation rules for the basic event and the DFT's gates, Fig. 4.6 shows a pseudocode of a function that converts a DFT to GSPN in the course of a depth first traversal of the DFT.

```
dftTOgspn (dft node) {

dft rn

  if (node is basic event) {
       translate node to GSPN module
       add new GSPN module to list of GSPN modules
  }
  else {                                        //node is a gate
      if (child of node has GSPN translation) { //gate inputs have GSPN translations
              translate node to GSPN module     //create GSPN module for gate
              add new GSPN module to list of GSPN modules
       }
       else {                                   //gate inputs not translated
              for (rn = child of node and all siblings) {    //all gate inputs
                     dftTOgspn (rn)             //recursive call
              }
       }
  }
}
```

FIGURE 4.6
Pseudocode to convert DFT to GSPN (Kabir et al., 2018b)

After the PN model is formed, it can be evaluated in many different ways to perform different analysis. For instance, in the PN model, if all the timed transitions are exponentially distributed, then the PN model can be evaluated by evaluating an underlying Markov model. In this case, as the analysis is performed based on Markov model, it is clear that its application will also be limited only to exponentially distributed failure data. On the other hand, if the PN model contains non-exponentially distributed timed transitions, then simulation like Monte Carlo simulation can be used for evaluation. Due to the use of simulation, this type analysis could be computationally time consuming. Although PNs provide more flexibility in terms of using different types of distributions, it has many features in common with Markov model. For instance, like Markov model based approaches PN-based approaches have to generate the state space of the system for analysis, as a result they face state space explosion problem while analysing moderately complex systems.

4.3.2.4 Bayesian Networks for quantifying DFTs

Bayesian networks (BNs) as a probabilistic graphical model have flexible architecture, which can make decisions under uncertainty and can provide a global assessment about different dependability properties such as reliability, availability by combining local level information from different sources. Widespread use of BNs for system dependability assessment had been reported in (Weber et al., 2012; Kabir and Papadopoulos, 2019; Yazdi and Kabir, 2017, 2018). In the pioneering work, Bobbio et al. (2001) showed how a classical static fault tree can be evaluated by translating it to BN. Afterwards, inspired by this approach, modelling capability of Bayesian networks has been utilized in different methods for evaluating DFTs.

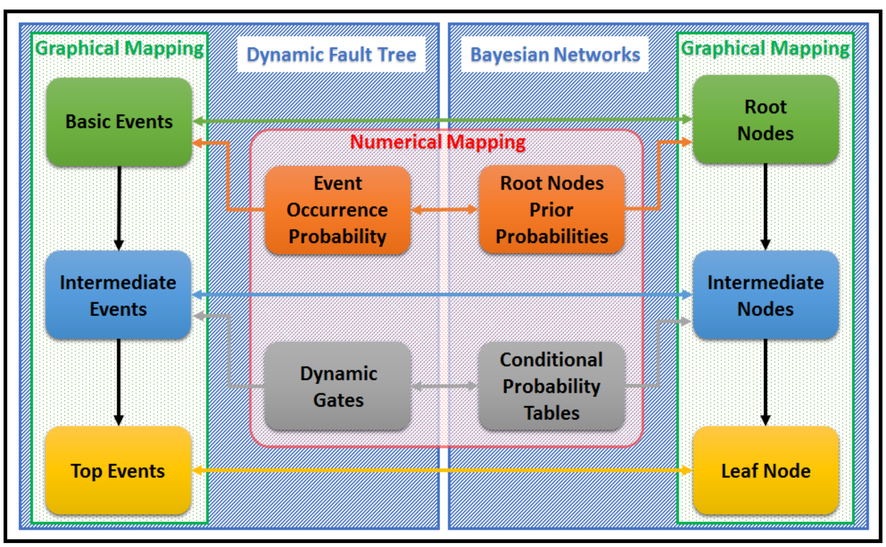


FIGURE 4.7
DFT to BN conversion process

At first, in (Boudali and Dugan, 2005), a method was introduced for quantitative analysis of DFTs by translating them into discrete time BNs. The general idea of the translation process is shown in Fig. 4.7. The translation is performed in two steps: qualitative and quantitative. Qualitative translation involves translating the basic events, the logic gates, and the top event of a DFT to root nodes, intermediate events, and leaf node of a BN, respectively. On the other hand, quantitative translation requires generating prior probabilities of the root nodes based on the failure probabilities of the basic events, conditional probability tables for the intermediate nodes and leaf node based on the logical specification of the DFT gates. As the approach in (Boudali and Dugan, 2005) uses a discrete time BN, it requires to decide the granularity of time-discretisation before the translation process. Similar to this approach, Montani et al. (2005) proposed a dynamic Bayesian network based DFT analysis method, which also considered discretised model. Later, they performed further research in (Montani et al., 2006b) to automate the DFT to BN generation process. In (Montani et al., 2006a), a tool named RADYBAN was presented for automatic conversion of DFTs to a 2-time-slice BNs (2TBNs)(Weber and Jouffe, 2003). Other discrete-time BN based approaches for DFT analysis could be found in (Kabir et al., 2014b, 2018a). All the above approaches consider system components to be non-repairable. However, to allow the modelling of repairable systems, the concept of a repair box gate was introduced in (Portinale et al., 2010).

In addition to the discrete-time model, continuous time BNs (CTBN) have also been used for the quantitative analysis of DFTs. For instance, Boudali and Dugan (2006) introduced a CTBN-based DFT analysis method. In this approach, due to the use of a continuous model of time, probability density functions and joint probability density functions were used instead of prior and conditional probability tables. One advantage of such approach over discrete-time BN-based approaches is that it can provide an exact closed form solution to DFTs. However, analysis using such approaches may face state space explosion problem.
In (Marquez et al., 2008, 2010), both discrete and continuous nodes were used in the same BN for DFT evaluation. As a result, it was possible to use both empirical and parametric distributions for the time-to-failure of system components. The recent contributions on CTBN-based DFT analysis include (Codetta-Raiteri, 2015; Codetta-Raiteri and Portinale, 2017; Li et al., 2015), where a Generalised Continuous Time Bayesian Network (GCTBN) was used for the quantification of DFT in (Codetta-Raiteri and Portinale, 2017). In order to solve GCTBN models, it was required to convert them to GSPN models, which leads to state-space explosion problem. In (Li et al., 2015), CTBN was used under fuzzy environment to quantify DFTs. Some application of BN-based DFT analysis for fault detection, identification, and analysis could be found in (Codetta-Raiteri and Portinale, 2015; Mi et al., 2016).

From the above discussion, it is clear that the discrete-time BN-based approaches for DFT evaluation can provide a fast non-exact solution to DFTs. However, the accuracy of the results can be improved significantly by increasing the number of discretized time intervals, but at the cost of higher computation time. On the other hand, CTBN-based approaches can readily provide exact solutions to DFTs, but may suffer from the state-space explosion problem. To alleviate this problem, approximate algorithms instead of exact algorithms can be used for analysis BN models. However, based on the nature of the application, the users can always make an informed decision by making a trade-off between the computing time and the precision of the results required.

4.3.2.5 Simulation Approaches for quantifying DFTs

Simulation approaches can be used when a system is too complex and an approximate result is acceptable. The idea behind the simulation approaches is that one I) simulates the behaviour of a system, II) determines the mission time, III) repeats the simulation for a huge number of iterations (e.g. 10e+8) and for each iteration check whether the system failed before the mission time or not, and finally, IV) evaluates the system reliability by dividing the number of failures to the number of iterations. It is also possible to I) decompose the system into its components, II) determine the mission time, III) check whether each component fails during this mission time, IV) provide a rule-set, or some similar logical models such as DFT, Petri Nets, Automata, etc. V) repeat the simulation procedure for a huge number of iterations (e.g. 10e+8) and for each iteration check whether the overall system failed before the mission time or not and VI) in the last step, evaluate the system reliability by dividing the number of failures of the overall system to the number of iterations. These two types of simulation approaches are common for reliability evaluation of complex system. The figure 4.8 illustrates these two procedures as (a) and (b) respectively.

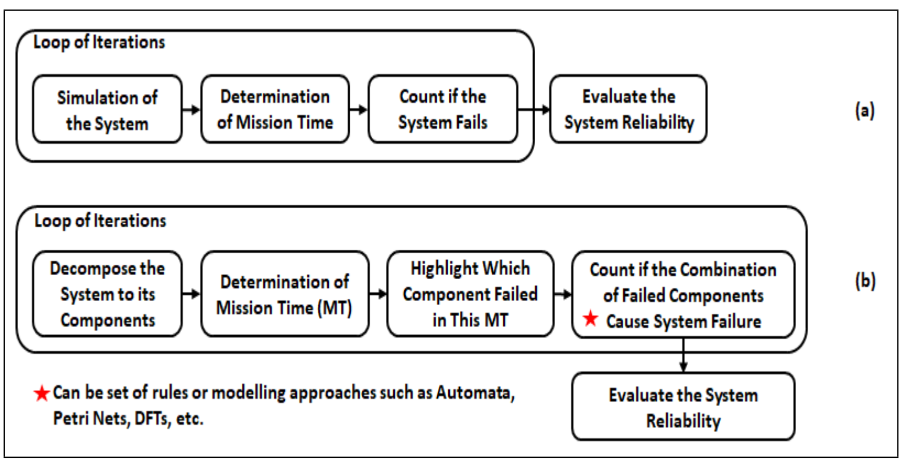


FIGURE 4.8
Two Common Simulation Approaches

In 1998, Marseguerra et al. (1998) remarked the concepts and principles in methods for evaluating dynamic reliability and then mentioned some Monte Carlo simulating algorithms. In order to decrease calculation time and also providing a practical simulation method for evaluating dynamic reliability, this paper introduces memory possessing methods and effective estimators.

Using "Time-to-failure (TTF)" tree, which is a tree that shows the time relation between system failure time and each component's failure time, Ejlali and Miremadi (2004) solved dynamic fault tree. In this tree, AND gate is converted into MAX, OR and FDEP gate is converted to MIN, PAND and SEQ gate is converted to ADDER and spare gates are converted into selector all of which are convertible to logic circuits (Ejlali and Miremadi, 2003). In this study, after designing time-to-failure tree, the logic circuits of the new tree are synthesized by VHDL language on FPGA programmable chip and Monte Carlo simulations are performed on this chip. Eventually, a comparison between efficiency and velocity of this method is performed using computer simulation which indicates that evaluation using FPGA chip is almost 471 times faster than computer simulation.

In 2006, Zonouz and Miremadi (2006) suggested fuzzy Monte Carlo method for evaluating dynamic fuzzy fault tree (only spare gate). In this study, the Weibull distribution is used for components' failure and fault tree is solved after being converted into time-to-failure tree. The comparison between simulation time in two studies shows that fuzzy Monte Carlo simulation takes as much time as the typical Monte Carlo simulation, thus this method makes problem solving much slower. In 2009, Kara-Zaitri and Ever (2009) dealt with evaluating fault tree with repairable components and the implemented simulation on FPGA chips have hastened its evaluation process. In fact, in this study, a semi-analytical method is employed, since failure rates and repair rates are achieved through analytical method and later by using Monte Carlo method the failure probability of the final event is calculated. This method is introduced as a less costly and a flexible method with the ability of modelling more complex scenarios. However, in this study only exponential distribution is considered for failure, thus not considering different failure distributions such as Weibull and normal is regarded as one disadvantage of this study.

Rao et al. (2009) proposed a solution process for each of the dynamic gates using Monte Carlo simulation. In this study, time curves are considered for each of the dynamic gates, so that time-dependent failure of each gate becomes tangible. First of all, this paper dealt with solving and validating the proposed method for evaluating non-repairable dynamic fault tree and also compares its solution with integral methods. Afterwards, an example of an electricity supply system with spare components in a nuclear power station is considered and solved considering repairability. The results achieved from the simulations are then compared with results obtained from solving Markov model. It was shown that in some cases the solution of the simulation is somehow similar to the analytical solution and in other cases significant differences exist. In addition to reliability evaluation, this article also evaluated system availability and performed its simulations using DRSIM tool.

Yevkin (2010) provided various methods for improving the efficiency of Monte Carlo simulations for both static and dynamic fault trees. In this paper variance reduction, parallel processing and enhancement based on structural information of the tree has been used and the results are validated on an industrial benchmark. A year later, Chiacchio et al. (2011) presented a Matlab-based open source software for reliability evaluation using DFTs. Through considering the four common benchmarks for validating the results, the results are compared with respect to accuracy and simulation time using Relex commercial software, Galileo commercial-research software, and DFTSIM research software. This software has appropriate relative accuracy and compare to other software, it possesses an acceptable computing speed. Following Chiacchio et al. (2011)'s study, Manno et al. (2012a) proposed a toolbox, named MatCarloRe, in the Simulink environment (Matlab) which allows the users to solve dynamic fault tree and evaluate reliability in a specific mission time using the Monte Carlo simulation method. In this study, for each of dynamic and static gates a block is considered and the output of each gate consists of failure time and failure signal is attached to inputs of the top gates in the tree and eventually a point-to-point solution of dynamic fault tree through simulation is achieved. Among the advantages this toolbox offers, we can refer to a block, named basic event, which allows the users to consider various failure distribution functions for system components. Also, for dynamic gate of the spare, a general block is considered which is able to model all (hot, cold and medium) spares. At the end of the paper, fault tree benchmark of the Hypothetical Cardiac assist system is used for validating the toolbox.

Lindhe et al. (2012) solved dynamic fault tree through two methods such as estimated Markov model and Monte Carlo simulation for evaluating the risk of drinking water supply. In this method, failure rate and the average time of system failure is evaluated at each level of the tree. This method is employed on three water supply scenarios and the results achieved from them are compared. In 2013, Aghassi and Aghassi (2012) presented a software based on Monte Carlo simulation for evaluating reliability of dynamic fault tree. This software manages to make a fault tree evaluation 310 times faster using parallel processing in the GPU. It should be noted that this software converts a fault tree into time-to-failure in the first place, and then performs the simulations. A new quantitative reliability evaluation of DFTs by means of event-driven-based Monte Carlo simulations has been proposed by Gascard and Simeu-Abazi (2018). The approach has been implemented in a Java-based framework called DFTEDS. Chiacchio et al. (2019) focused on MATLAB Simulink based modelling and proposed a new solution as a library called Stochastic Hybrid Fault Tree Object Oriented (SHyFTOO). Generally, the difference between analytical-based approaches like CTMC and simulation-based methods like Monte Carlo Simulation can be summarized as Table 4.1.

4.3.2.6 Modularisation Approaches for quantifying DFTs

Analysing large fault trees, including DFT is a big challenge for safety analysis experts. Modularisation has been proved as a powerful method to improve the computational performance of approaches while solving large fault trees (Patterson-Hine and Dugan, 1992). Modularisation techniques are also known

TABLE 4.1
Comparison between simulation and analytical methods

Attributes	**Simulation Based Methods**	**Analytical Methods**
Computation Time	Time consuming (depends on number of iterations)	Usually faster than simulation
Final Results	Approximate	Exact / Precise
Complexity Consideration	It would be easier to evaluate complex systems through simulation	Simplification is needed for large-scale systems
Further Results Extraction	Only statistical calculation	It is possible to drive other factors like MTTF/MTBF from results directly

as hierarchical or compositional approaches. In modularisation techniques, a divide-and-conquer strategy is followed. Under this strategy, a large DFT is divided into smaller independent static and dynamic modules. These independent modules are then solved using appropriate approaches depending on their type.

In 1997, Dugan et al. (1997) proposed the first modularisation technique called DIFtree for DFT analysis. They used Binary Decision Diagrams (BDDs) and Markov chains to solve the static and dynamic sub-trees of the DFT. Solution of the smaller sub-trees are combined together to obtain the solution for the larger tree. This work was later extended in (Gulati and Dugan, 1997). A similar solution to DFT was also proposed in (Anand and Somani, 1998). As the DIFtree approach is only applicable to exponentially distributed failure data, Manian et al. (1998) extended it by including Monte Carlo simulation to allow the use of non-exponential distributions.

The limitations of the above mentioned approaches are that they cannot perform sensitivity analysis due to modularisation and if a module is dynamic then no further modularisation is performed in that module. To address these issues, Huang and Chang (2007) proposed a hierarchical approach by modularising the fault tree, which allows decomposition of independent sub-trees of a dynamic module. In 2011, Yevkin (2011) also proposed an improved modular approach for dynamic fault tree by considering systems without repairable components. He evaluated five different scenarios with the possibility of separating dynamic fault tree modules and the approach was employed on three DFT benchmarks.

In 2012, Manno et al. (2012a) proposed a modular method where each independent sub-tree of a fault tree is detected and solved hierarchically, as other approaches do, a dynamic sub-tree is replaced by a single basic event where the probability of occurrence of the basic event is the probability of the occurrence of the sub-tree. In 2013, Chiacchio et al. (2013) proposed an algorithm of a hierarchical approach for the reliability evaluation of dynamic fault trees. The approach used a parametric function (a 4-paramters Weibull) to solve the problem of dynamic evolution of the cumulative distribution function with different gates including PAND gate. The proposed approach used MatcarloRE (Manno et al., 2012a) tool to reduce the least square error fitting. In (Amari et al., 2003), a new modular approach was proposed in which both static and dynamic sub-modules of a DFT were solved using algebraic formulas, i.e., using multi-level integrals. This approach is different from other modularisation techniques in the sense that it did evaluate the dynamic modules without converting them into CTMCs.

4.3.2.7 Application of Machine Learning with DFTs

The use of Machine Learning algorithms alongside safety models is one of the cutting-edge research topics in safety and reliability analysis area (Simen et al., 2018). Figure 4.9 categorizes the combination of Machine learning with safety models in five categories. I) Using the reliability model as a core in Machine Learning with the aim of fault detection and diagnosis, II) Selection of predefined and co-evaluated models through Machine Learning, III) Updating the value of failure rates through Machine learning-based algorithms, IV) Reconfiguration of the safety model through process mining, and V) Updating the membership functions of fuzzy models via Machine Learning. Regarding the third category, in 2018, Aizpurua et al. (2017b,a) proposed a method for combining failure rate and Remaining Useful Life (RUL) as the basic event in DFTs. As we know the RUL can be estimated through Machine Learning approaches (Sikorska et al., 2011). For the other categories, Lampis and Andrews (2009); Askarian et al. (2016); Chen and Ge (2018); Getir et al. (2018); Cheng et al. (2019) can be consulted. However, none of the current researches of those categories consider DFT as a safety model.

In addition to the above mentioned works, there exist some other works where Machine learning has been used with DFTs. For instance, Zhou et al. (2006) proposed an approach for designing dynamic systems using recursive neural networks. The reliability of the system is designed based on DFTs and neural network. The DFT is mapped into the recursive neural network with the feed-forwards technique. Raptodimos and Lazakis (2017) proposed a new approach for predictive maintenance of ship machinery. The proposed approach combined DFT with machine learning to facilitate forecasting of the health of selected system components to optimise maintenance task. The approach aims to predict and monitor the future values of different components' physical parameters by using an autoregressive dynamic time series neural network modelling approach. The neural network model was trained in real time where there is no bug or fault occurred in the system. Yassmeen Elderhalli and Tahar (2019) use machine learning to facilitate automating the proof

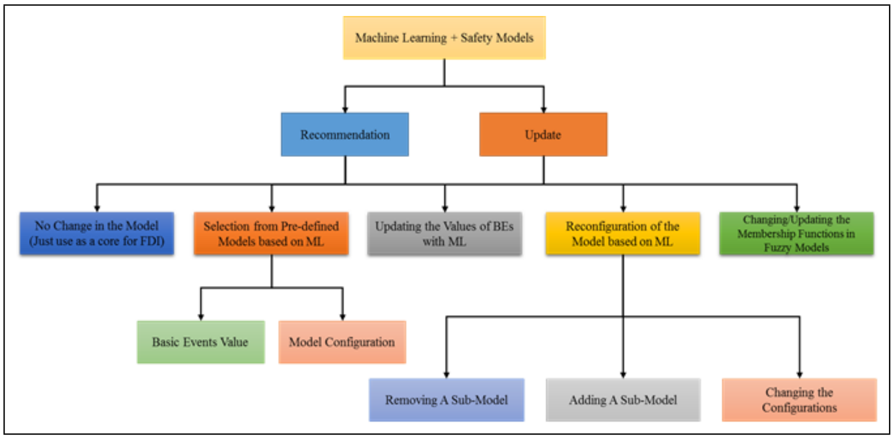


FIGURE 4.9
A classification of different approaches where Machine learning can be combined with DFTs

of the sub goals. The sub goals verification is performed in two steps. The first step is evaluating the existing sub goals and the second step involves real-time reasoning to verify the remaining sub goals. From the proposed techniques we can understand that the use of machine learning with DFT is to come up with a tool that can analyse dynamic system with minimum user intervention in the formal DFT analysis. Linard et al. (2019) has provided a new evolutionary-based approach to generate fault tree from observational data. A novel idea to merge machine learning algorithm and update fault tree has been provided by Gheraibia et al. (2019). In this research, a one-class support vector machine with a decision tree has been used to update the fault tree of safety critical systems.

4.4 Sensitivity Analysis in DFTs

Given that the reliability evaluation is an important aspect in designing safety-critical and fault tolerant systems, the evaluation of the importance factor and the sensitivity can be a useful tool for analyzing this parameter. With the help of the factor of importance and sensitivity, the following can be achieved:

- Finding out the part of the system that has the most contribution in system failure (failure bottleneck(s)).
- Finding a path (a set of sequential events in a tree) that mostly contributes to the system failure.

- Finding the uncertainty of the tree's results regarding the accuracy of the input parameters (for example, the estimated failure rate).
- Finding the most affordable way to increase system's reliability.
- Determining the components for which investments in maintenance and repairs have the most impact on system performance (Xing, 2004).
- Assessing the impact of the mission of a subsystem on the entire mission risk (Zixian et al., 2011).

Table 4.2 summarizes the sensitivity and the importance analysis approaches found in the literature.

4.5 Tool Support

As already seen that the development made with DFT-based safety and reliability is not just theoretical, they have practical applications as well. Moreover, several tools have been developed as outcomes of successful researches. A list of such DFT analysis tools including the methodologies used in these tools and what dependability parameters can be measured by them are summarized in Table 4.3.

In parallel with the existing academic DFT tool, there are some useful commercial tools such as ReliaSoft (ReliaSoft, 2016), OpenFTA (Auvation, 2016), Isograph Fault Tree+ (Isograph, 2016), ITEM Toolkit (ITEM Software, 2016), EPRI CAFTA (EPRI, 2013). However, these mentioned commercial tools have a limited functionality related to the DFT analysis. They have PAND and POR gates, but they cannot support sequence gate, repair action gate or spare gate. For more details regarding the existing commercial tools, readers are referred to check section 2.7 in Ruijters and Stoelinga (2015).

4.6 Discussion and Future Research Directions

Reliability analysis is an integral part of dependable system design and development. Over the years, several approaches have been developed for reliability evaluation. FTA is one of the most widely used approaches for reliability and risk assessment. To meet the increasing demand of the society, different new and complex functionality have been continuously added to the modern systems, thus making it difficult to analyse the failure behaviour of such systems using classical FTA. The issue of the inability of fault tree to model the complex time dependent dynamic failure behaviour and different types

TABLE 4.2
Sensitivity and importance analysis approaches

Fault Tree Analysis							Measured Factor
Dynamic				Static			
Stochastic Equation	Cut-Set	BDD	MC	Simulation	Non-coherent	Coherent	
Petkov and Pekov (2009)	-	Xing and Dugan (2002)	Ou and Dugan (2000); Chiacchio et al. (2018); Noroozian et al. (2019); Ou (2003); Ou and Dugan (2003); Lo et al. (2005)	Marseguerra et al. (2005)	Beeson (2002)	Iman (1987); Dugan and Lyu (1995); Contini et al. (2010); László (2011); Aslansefat and Latif-Shabgahi (2015)	Sensitivity
Liping and Fuzheng (2009)	Liu et al. (2012)	Dutuit and Rauzy (2001); Chang et al. (2004)	Ou (2003)	Marseguerra and Zio (2004); Zio et al. (2004)	Andrews and Beeson (2003); Beeson and Andrews (2003); Xing (2004); Lu and Jiang (2007); Vaurio (2010); Contini and Matuzas (2011)	Lu and Jiang (2007); Contini and Matuzas (2011); Contini et al. (2010)	Importance

TABLE 4.3
Different DFT analysis tools

Software	Method	Measurements Types	Release Year	Remarks
Radyban (Montani et al., 2008)	Bayesian networks	Reliability, Availability	2008	BE Dependencies Not Exact
Galileo (Sullivan et al., 1999)	BDD and Markov methods	Reliability, Availability, Sensitivity, On-demand Safety	1990	Exact Solution State-space explosion
SHARPE (Sahner and Trivedi, 1987)	Modularisation	Reliability, Availability, Sensitivity	1987	Non-Exponential Complex BE
MatCarloRe (Manno et al., 2012a)	Monte Carlo	Reliability, Availability, Sensitivity	2012	Non-Exponential Not Exact
PANDORA (Walker, 2009)	Algebraic	Reliability	2009	Non-Exponential Temporal Gates (POR, pSAND)
RAATSS (Manno et al., 2012b)	Adaptive Transitions System	Reliability, Availability, Sensitivity	2012	Non-Exponential Complex Systems
DFTCalc (Arnold et al., 2013a)	Stochastic model checking	Reliability, Availability, Sensitivity	2013	No State-Space Explosion
DFTSim (Boudali et al., 2009)	Monte Carlo	Reliability, Availability, Sensitivity	2009	Repair Modelling Accept Non-Markovian Properties
DIFtree (Dugan et al., 1997)	Modularisation	Reliability	1997	Complex BE
SHADE Tree^{TM} (Pullum and Dugan, 1996)	Modularisation	Reliability	1996	Simple Solution
The AltaRica (Boiteau et al., 2006)	Markov chain	Reliability	2006	Model Simplification Complex BE

of redundancy has not gone unnoticed. Researchers have extended the modelling power of the static fault tree by proposing dynamic fault tree through introducing new dynamic logic gates. While the inclusion of dynamic gates improves the expressiveness of the fault tree model, it complicates the evaluation of fault tree. Many approaches have been considered in the literature, including algebraic formulas, Markov models, Petri nets, Bayesian networks, and so on to develop different methodologies for qualitative and quantitative analysis of DFTs. In this chapter, we have provided a high-level overview of these methodologies.

From the review it is noticed that the DFT analysis approaches have their own strengths and weaknesses. Although the approaches have some shared capabilities, they do have their distinct capabilities and one approach may perform relatively better than others in some specific situations. For instance, if the components of a system have exponentially distributed lifetime then classical Markov chain-based approaches can be used to anlayse the DFT of such systems. However, system with non-exponentially distributed system cannot be analysed using Markov chain-based approaches. On the other hand, Semi-Markov processes, Petri Nets, Bayesian Networks, and Monte Carlo simulation based approaches can analyse DFTs having basic events with both exponentially and non-exponentially distributed lifetime. From a different point of view, the Markov chain and Petri nets based approaches suffer from state space explosion while evaluating DFTs of complex systems. Therefore, application of these approaches are limited to small scale systems. As the algebraic solutions to DFTs use mathematical formulas, they do not have the issue of state space explosion problem. However, for a DFT of large and complex system, defining mathematical expressions would be a difficult task. With regards to state space explosion, the BN-based approaches show better performance as they can avoid the state space explosion problem by avoiding the state space generation by exploiting the local dependencies between variables while modelling complex behaviour. Another strength of BN-based approaches over other DFT analysis approaches is that they can perform diagnostic analysis in addition to predictive analysis. In diagnostic analysis, BN-based approaches can propagate new evidence through the network to obtain new beliefs about the failure probability of the events and update prior beliefs. Unlike other DFT analysis approaches, BNs are therefore able to adapt and refine their diagnostic ability over time. However, if a continuous time model is used for BNs, then for an internal node with many parents with a probability density function, expressing the joint probability distribution would be tedious.

Although extensive research has been performed, there exist some challenges that need additional research. For instance, most of the DFT analysis approaches reviewed in this paper perform the analysis under the assumption that the DFT of a system is already available, and in most cases, a DFT of a system is derived from a pre-defined fixed architecture of the system. However, the advancement of technologies has brought loosely connected systems. Typical examples of such systems are Cyber-Physical Systems and the Internet of Things. These are systems where temporary system architectures/configurations are formed during operation by combining several smaller systems and these architectures may cease to exist after a certain period of time to form a new architecture. As a result, there may exist infinite possible configurations of such a system, and it is difficult to ensure certainty about a particular system architecture during safety and reliability assessment. This will also affect the structure of the DFT. Therefore, assessment of such open systems using DFT would require taking into account the uncertainty of the system architecture at a certain point in time. This opens new research avenues to investigate how a meaningful safety and reliability assessment can be performed for open and adaptive systems by taking into account the architectural uncertainty.

Similar to architectural uncertainty, data uncertainty is an important, but less researched topic in DFT analysis. In SFTs, this issue has been addressed in many different ways. One of the prominent way is to use the fuzzy set theory to address the data uncertainty. From the literature review, we have noticed that there is much less research in DFT analysis involving fuzzy set theory. Therefore, in the future, it would be worthwhile to perform more research in this area to address the data uncertainty issue.

Another important issue worth mentioning is that even there exists tool support for creating and analysing DFTs, it requires a lot of manual effort for this. This could also introduce error into the analysis. Model-based safety analysis (Sharvia et al., 2015), which attracted significant interest from industry and academia, can automate the static fault tree generation process from system models. This offers important advantages, not least the reduction in both effort and potential for error, and supports a more iterative design process via automatic synthesis of fault trees. Although the auto generation of static fault trees as part of MBSA and availability of tool supports for this task were reported in the literature, to the best of the authors' knowledge, limited effort has been made to replicate the same for the automatic generation of DFTs from system models by considering dynamic behaviour. Therefore, future research could be directed to address this issue.

In terms of application of DFTs, there are some potential to use DFT for alarm management in different industries. For instance, Simeu-Abazi et al. (2011) used the combination of Petri Nets and DFT for alarm filtering and showed its capabilities for alarm nuisance reduction. In addition, the automata models of dynamic gates with the aim alarm modelling have been introduced by Gascard et al. (2011). Recently, Aslansefat et al. (2019); Bahar-Gogani et al. (2017) used Priority AND gate for performance evaluation of alarm system with variable threshold. Therefore, there is still some potential to use other dynamic or temporal gates such as SEQ, SPARE, and pSAND for the performance evaluation of alarm systems. Moreover, Xu et al. (2011); Taheri Kalani et al. (2017) used Markov models to evaluate $n-$sample delay timers for only one component of alarm systems. Based on the idea provided in Kabir et al. (2019); Papadopoulos et al. (2019), in the future, such Markov models can be used as a complex BE in DFTs to combine and obtain the performance of large scale dynamic alarm systems.

As mentioned in section 4.3.2.7, in safety and reliability engineering domain, the utilisation of machine learning (ML) algorithms with safety models has become an emerging research topic. Therefore, there is a large scope to use DFTs as a safety model together with ML for the safety assurance and reliability management of complex, modern systems. One potential way of using DFT with ML algorithms would be to use it as a core model within a ML algorithm for fault detection and diagnosis of systems under the condition uncertainty. Another way ML could be used with DFTs to help updating the DFT models and failure probability of the basic events within the DFT models by learning from the emerging behaviour and changing operation environment of the systems. These future researches have the potential to revolutionize the way of performance assessment for many future generation autonomous self adaptive systems.

4.7 Conclusion

Reliability engineering and management of complex and dynamic systems is a complicated task. There are many dynamic interactions between system components and multiple temporal and stochastic dependencies between them that need to be taken into account, and not all the existing safety and reliability analysis formalisms are able to capture these dependencies. DFT is one of the popular mechanisms widely used to model dynamic failure behaviour systems to evaluate the dynamic reliability of systems. Many new developments and an upward trend is observed in DFTs' application in reliability engineering and management of complex systems. This chapter reviews many such developments in DFT-based reliability analysis. The review provided insights into the working mechanism, applicability, strengths, and challenges of different DFT analysis approaches. A discussion is provided on the reviewed methodologies and a direction to potential future research has been provided based on the identified challenges.

ACKNOWLEDGMENT

This work was partly supported by the DEIS H2020 Project under Grant 732242. We would like to thank EDF Energy Research and Development UK Centre, AURA Innovation Centre and the University of Hull for their support.

CONFLICT OF INTEREST

The author confirms that they have no conflict of interest to declare for this publication.

Bibliography

Aghassi, H., Aghassi, F., 2012. Fault tree analysis speed-up with GPU parallel computing. Computer Information Systems and Industrial Management Applications, Tehran 5, 106–114.

Aizpurua, J.I., Catterson, V.M., Papadopoulos, Y., Chiacchio, F., D'Urso, D., 2017a. Supporting group maintenance through prognostics-enhanced dynamic dependability prediction. Reliability Engineering & System Safety 168, 171–188.

Aizpurua, J.I., Catterson, V.M., Papadopoulos, Y., Chiacchio, F., Manno, G., 2017b. Improved dynamic dependability assessment through integration with prognostics. IEEE Transactions on Reliability 66, 893–913.

Aliee, H., Zarandi, H.R., 2013. A fast and accurate fault tree analysis based on stochastic logic implemented on field-programmable gate arrays. IEEE Transactions on Reliability 62, 13–22. doi:10.1109/TR.2012.2221012.

Amari, S., Dill, G., Howald, E., 2003. A new approach to solve dynamic fault trees, in: Annual Reliability and Maintainability Symposium, 2003., IEEE. pp. 374–379.

Anand, A., Somani, A.K., 1998. Hierarchical analysis of fault trees with dependencies, using decomposition, in: Proceedings of Annual Reliability and Maintainability Symposium,, pp. 69–75. doi:10.1109/RAMS.1998.653591.

Andrews, J.D., Beeson, S., 2003. Birnbaum's measure of component importance for noncoherent systems. IEEE Transactions on Reliability 52, 213–219.

Arnold, F., Belinfante, A., Van der Berg, F., Guck, D., Stoelinga, M., 2013a. DFTCalc: a tool for efficient fault tree analysis, in: International Conference on Computer Safety, Reliability, and Security, Springer. pp. 293–301.

Arnold, F., Belinfante, A., Van Der Berg, F., van der Berg, F.I., Guck, D., Stoelinga, M.I.A., 2013b. DFTCalc: a tool for efficient fault tree analysis (extended version). Technical Report. Centre for Telematics and Information Technology (CTIT).

Askarian, M., Zarghami, R., Jalali-Farahani, F., Mostoufi, N., 2016. Fusion of micro-macro data for fault diagnosis of a sweetening unit using bayesian network. Chemical Engineering Research and Design 115, 325–334.

Aslansefat, K., 2014. A novel approach for reliability and safety evaluation of control systems with dynamic fault tree. MSc. Thsis, Abbaspur Campus, Shahid Beheshti University .

Aslansefat, K., Gogani, M.B., Kabir, S., Shoorehdeli, M.A., Yari, M., 2019. Performance evaluation and design for variable threshold alarm systems through semi-markov process. ISA Transactions , 1–14doi:10.1016/j.isatra.2019.08.015.

Aslansefat, K., Latif-Shabgahi, G., 2015. A systematic approach to sensitivity analysis of fault tolerant systems in nmr architecture. Journal of Intelligent Procedures in Electrical Technology (JIPET) 5, 3–14.

Aslansefat, K., Latif-Shabgahi, G., 2019. A hierarchical approach for dynamic fault trees solution through semi-markov process. IEEE Transactions on Reliability , 1–18doi:10.1109/TR.2019.2923893.

Auvation, 2016. OpenFTA. URL: http://www.openfta.com/.

Bahar-Gogani, M., Aslansefat, K., Shoorehdeli, M.A., 2017. A novel extended adaptive thresholding for industrial alarm systems, in: 2017 Iranian Conference on Electrical Engineering (ICEE), pp. 759–765. doi:10.1109/IranianCEE.2017.7985140.

Bavuso, S.J., Rothmann, E., Dugan, J.B., Trivedi, K.S., Mittal, N., Boyd, M.A., Geist, R.M., Smotherman, M.D., 1994. HiRel: Hybrid Automated Reliability Predictor (HARP) Integrated Reliability Tool System (Version 7.0). NASA Technical Paper 3452, 1–4.

Beeson, S., Andrews, J.D., 2003. Importance measures for noncoherent-system analysis. IEEE Transactions on Reliability 52, 301–310.

Beeson, S.C., 2002. Non-coherent fault tree analysis. Ph.D. thesis. © Sally Christian Beeson.

Bernardi, S., Campos, J., Merseguer, J., 2011. Timing-failure risk assessment of UML design using Time Petri Net bound techniques. IEEE Transactions on Industrial Informatics 7, 90–104.

Bobbio, A., Ciancamerla, E., Franceschinis, G., Gaeta, R., Minichino, M., Portinale, L., 2003. Sequential application of heterogeneous models for the safetyanalysis of a control system: a case study. Reliability Engineering & System Safety 81, 269–280.

Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering & System Safety 71, 249–260. doi:10.1016/S0951-8320(00)00077-6.

Boiteau, M., Dutuit, Y., Rauzy, A., Signoret, J.P., 2006. The AltaRica dataflow language in use: modeling of production availability of a multi-state system. Reliability Engineering & System Safety 91, 747–755.

Boudali, H., Crouzen, P., Stoelinga, M., 2007a. A compositional semantics for Dynamic Fault Trees in terms of Interactive Markov Chains, in: International Symposium on Automated Technology for Verification and Analysis, Springer. pp. 441–456.

Boudali, H., Crouzen, P., Stoelinga, M., 2007b. Dynamic fault tree analysis using input/output interactive Markov chains, in: 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), IEEE. pp. 708–717.

Boudali, H., Crouzen, P., Stoelinga, M., 2010. A rigorous, compositional, and extensible framework for dynamic fault tree analysis. IEEE Transactions on Dependable and Secure Computing 7, 128–143.

Boudali, H., Dugan, J.B., 2005. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering & System Safety 87, 337–349.

Boudali, H., Dugan, J.B., 2006. A Continuous-Time Bayesian Network Reliability Modeling, and Analysis Framework. IEEE Transaction on Reliability 55, 86–97.

Boudali, H., Nijmeijer, A., Stoelinga, M.I., 2009. DFTSim: A simulation tool for extended dynamic fault trees, in: Proceedings of the 2009 Spring Simulation Multiconference, Society for Computer Simulation International. p. 31.

Boyd, M.A., 1992. Dynamic fault tree models: techniques for analysis of advanced fault tolerant computer systems. Ph.D. thesis. Duke University.

Brameret, P.A., Rauzy, A., Roussel, J.M., 2015. Automated generation of partial Markov chain from high level descriptions. Reliability Engineering & System Safety 139, 179–187.

Chang, Y.R., Amari, S.V., Kuo, S.Y., 2004. Computing system failure frequencies and reliability importance measures using OBDD. IEEE Transactions on Computers 53, 54–68.

Chaux, P.Y., Roussel, J.M., Lesage, J.J., Deleuze, G., Bouissou, M., 2013. Towards a unified definition of minimal cut sequences. IFAC Proceedings Volumes 46, 1 – 6. doi:`https://doi.org/10.3182/20130904-3-UK-4041.00013`. 4th IFAC Workshop on Dependable Control of Discrete Systems.

Chen, G., Ge, Z., 2018. Hierarchical bayesian network modeling framework for large-scale process monitoring and decision making. IEEE Transactions on Control Systems Technology .

Cheng, J., Zhu, C., Fu, W., Wang, C., Sun, J., 2019. An Imitation medical diagnosis method of hydro-turbine generating unit based on Bayesian network. Transactions of the Institute of Measurement and Control , 0142331219826665.

Chiacchio, F., Aizpurua, J.I., Compagno, L., Khodayee, S.M., D'Urso, D., 2019. Modelling and resolution of dynamic reliability problems by the coupling of simulink and the stochastic hybrid fault tree object oriented (shyftoo) library. Information 10, 283.

Chiacchio, F., Aizpurua, J.I., D'Urso, D., Compagno, L., 2018. Coherence region of the priority-and gate: Analytical and numerical examples. Quality and Reliability Engineering International 34, 107–115.

Chiacchio, F., Cacioppo, M., D'Urso, D., Manno, G., Trapani, N., Compagno, L., 2013. A weibull-based compositional approach for hierarchical dynamic fault trees. Reliability Engineering & System Safety 109, 45–52.

Chiacchio, F., Compagno, L., D'Urso, D., Manno, G., Trapani, N., 2011. An open-source application to model and solve dynamic fault tree of real industrial systems, in: 2011 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA) Proceedings, IEEE. pp. 1–8.

Codetta-Raiteri, D., 2005. The conversion of dynamic fault trees to stochastic Petri nets, as a case of graph transformation. Electronic Notes in Theoretical Computer Science 127, 45–60.

Codetta-Raiteri, D., 2015. Applying generalized continuous time Bayesian networks to a reliability case study. IFAC-PapersOnLine 48, 676–681.

Codetta-Raiteri, D., Portinale, L., 2015. Dynamic Bayesian networks for fault detection, identification, and recovery in autonomous spacecraft. IEEE Transactions on Systems, Man, and Cybernetics: Systems 45, 13–24.

Codetta-Raiteri, D., Portinale, L., 2017. Generalized Continuous Time Bayesian Networks as a modelling and analysis formalism for dependable systems. Reliability Engineering & System Safety 167, 639–651.

Contini, S., Fabbri, L., Matuzas, V., 2010. A novel method to apply importance and sensitivity analysis to multiple fault-trees. Journal of Loss Prevention in the Process Industries 23, 574–584.

Contini, S., Matuzas, V., 2011. New methods to determine the importance measures of initiating and enabling events in fault tree analysis. Reliability Engineering & System Safety 96, 775–784.

Crouzen, P., 2006. Compositional analysis of dynamic fault trees using input/output interactive markov chains. Master's thesis. University of Twente. Enschede, Netherlands.

Dominguez-Garcia, A.D., Kassakian, J.G., Schindall, J.E., Zinchuk, J.J., 2008. An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems. Reliability Engineering & System Safety 93, 1628–1649.

Dugan, J., 1993. Analysis of a hardware and software fault tolerant processor for critical applications, in: 9th Computing in Aerospace Conference, p. 4573.

Dugan, J., Sullivan, K., Coppit, D., 2000. Developing a low-cost high-quality software tool for dynamic fault-tree analysis. IEEE Transactions on Reliability 49, 49–59. doi:10.1109/24.855536.

Dugan, J.B., Bavuso, S., Boyd, M., 1992. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability 41, 363–377.

Dugan, J.B., Bavuso, S.J., Boyd, M.A., 1993. Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. Reliability Engineering & System Safety 39, 291–307.

Dugan, J.B., Lyu, M.R., 1995. System-level reliability and sensitivity analyses for three fault-tolerant system architectures, in: Dependable Computing for Critical Applications 4. Springer, pp. 459–477.

Dugan, J.B., Venkataraman, B., Gulati, R., 1997. DIFTree: a software package for the analysis of dynamic fault tree models, in: Annual Reliability and Maintainability Symposium, IEEE. pp. 64–70.

Dutuit, Y., Rauzy, A., 2001. Efficient algorithms to assess component and gate importance in fault tree analysis. Reliability Engineering & System Safety 72, 213–222.

Edifor, E., Walker, M., Gordon, N., 2012. Quantification of priority-or gates in temporal fault trees, in: International Conference on Computer Safety, Reliability, and Security, Springer. pp. 99–110.

Ejlali, A., Miremadi, S.G., 2003. Time-to-failure tree, in: Annual Reliability and Maintainability Symposium, 2003., IEEE. pp. 148–152.

Ejlali, A., Miremadi, S.G., 2004. FPGA-based Monte Carlo simulation for fault tree analysis. Microelectronics Reliability 44, 1017–1028.

Elderhalli, Y., Hasan, O., Ahmad, W., Tahar, S., 2017. Dynamic Fault Trees Analysis using an Integration of Theorem Proving and Model Checking. CoRR abs/1712.02872. arXiv:1712.02872.

EPRI, 2013. EPRI CAFTA. URL: http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001015514.

Fecarotti, C., Andrews, J., Chen, R., 2016. A Petri net approach for performance modelling of polymer electrolyte membrane fuel cell systems. international journal of hydrogen energy 41, 12242–12260.

Fussell, J., Aber, E., Rahl, R., 1976. On the Quantitative Analysis of Priority-AND Failure Logic. IEEE Transactions on Reliability R-25, 324–326.

Garg, H., 2013. Reliability analysis of repairable systems using petri nets and vague lambda-tau methodology. ISA transactions 52, 6–18.

Garg, H., 2014. Reliability, availability and maintainability analysis of industrial systems using pso and fuzzy methodology. Mapan 29, 115–129.

Garg, H., 2015. An approach for analyzing the reliability of industrial system using fuzzy kolmogorov's differential equations. Arabian Journal for Science and Engineering 40, 975–987.

Garg, H., Rani, M., Sharma, S., 2014a. An approach for analyzing the reliability of industrial systems using soft-computing based technique. Expert systems with Applications 41, 489–501.

Garg, H., Rani, M., Sharma, S., Vishwakarma, Y., 2014b. Bi-objective optimization of the reliability-redundancy allocation problem for series-parallel system. Journal of Manufacturing Systems 33, 335–347.

Garg, H., Sharma, S., 2011. Multi-objective optimization of crystallization unit in a fertilizer plant using particle swarm optimization. International Journal of Applied Science and Engineering 9, 261–276.

Gascard, E., Simeu-Abazi, Z., 2018. Quantitative analysis of dynamic fault trees by means of monte carlo simulations: Event-driven simulation approach. Reliability Engineering & System Safety 180, 487–504.

Gascard, E., Simeu-Abazi, Z., Younes, J., 2011. Exploitation of built in test for diagnosis by using dynamic fault trees: Implementation in matlab simulink, in: Advances in Safety, Reliability and Risk Management. CRC Press, pp. 457–465.

Ge, D., Li, D., Chou, Q., Zhang, R., Yang, Y., 2016. Quantification of highly coupled dynamic fault tree using IRVPM and SBDD. Quality and Reliability Engineering International 32, 139–151.

Ge, D., Lin, M., Yang, Y., Zhang, R., Chou, Q., 2015a. Quantitative analysis of dynamic fault trees using improved sequential binary decision diagrams. Reliability Engineering & System Safety 142, 289–299.

Ge, D., Lin, M., Yang, Y., Zhang, R., Chou, Q., 2015b. Reliability analysis of complex dynamic fault trees based on an adapted KD Heidtmann algorithm. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 229, 576–586.

Ge, D., Yang, Y., 2015. Reliability analysis of non-repairable systems modeled by dynamic fault trees with priority and gates. Applied Stochastic Models in Business and Industry 31, 809–822.

Ge, D., Yang, Y., 2017. Negating a generalized cut sequence: Bridging the gap between dynamic fault trees quantification and sum of disjoint products methods. Quality and Reliability Engineering International 33, 357–367.

Getir, S., Grunske, L., van Hoorn, A., Kehrer, T., Noller, Y., Tichy, M., 2018. Supporting semi-automatic co-evolution of architecture and fault tree models. Journal of Systems and Software 142, 115–135.

Gheraibia, Y., Kabir, S., Aslansefat, K., Sorokos, I., Papadopoulos, Y., 2019. Safety + AI: A Novel Approach to Update Safety Models using Artificial Intelligence. IEEE Access 7, 135855–135869. doi:10.1109/ACCESS.2019.2941566.

Gulati, R., Dugan, J.B., 1997. A modular approach for analyzing static and dynamic fault trees, in: Annual reliability and maintainability symposium, IEEE. pp. 57–63.

Guo, W.G., Han, W., Liu, S.Y., 2011. Dynamic fault tree based on weibull distribution, in: Advanced Materials Research, Trans Tech Publ. pp. 1322–1327.

Hao, J., Zhang, L., Wei, L., 2014. Reliability analysis based on improved dynamic fault tree, in: Engineering Asset Management 2011. Springer, pp. 283–299.

Heidtmann, K.D., 1989. Smaller sums of disjoint products by subproduct inversion. IEEE Transactions on Reliability 38, 305–311.

Hermanns, H., 2002. Interactive markov chains, volume 2428 of. Lecture Notes in Computer Science .

Herscheid, L., Tröger, P., 2014. Specification of Dynamic Fault Tree Concepts with Stochastic Petri Nets, in: Eighth International Conference on Software Security and Reliability, IEEE. pp. 177–186.

Huang, C.Y., Chang, Y.R., 2007. An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees. Reliability Engineering & System Safety 92, 1403–1412.

Huang, H., Li, Y., Sun, J., Yang, Y., Xiao, N., 2013. Fuzzy dynamic fault tree analysis for the solar array drive assembly. Journal of Mechanical Engineering 49, 70–76.

Hura, G.S., Atwood, J.W., 1988. The use of Petri nets to analyze coherent fault trees. IEEE Transactions on reliability 37, 469–474.

Iman, R.L., 1987. A matrix-based approach to uncertainty and sensitivity analysis for fault trees 1. Risk analysis 7, 21–33.

Isograph, 2016. Isograph FaultTree+. URL: http://www.isograph.com/software/reliability-workbench/fault-tree-analysis/.

ITEM Software, 2016. ITEM ToolKit. URL: http://www.itemsoft.com/item_toolkit.html.

Jiang, G., Hongjie, Y., Peichang, L., Peng, L., 2018. A new approach to fuzzy dynamic fault tree analysis using the weakest n-dimensional t-norm arithmetic. Chinese Journal of Aeronautics 31, 1506–1514.

Junges, S., Katoen, J.P., Stoelinga, M., Volk, M., 2018. One net fits all, in: Khomenko, V., Roux, O.H. (Eds.), Application and Theory of Petri Nets and Concurrency, Springer International Publishing, Cham. pp. 272–293.

Kabir, S., 2017. An overview of fault tree analysis and its application in model based dependability analysis. Expert Systems with Applications 77, 114–135.

Kabir, S., Aslansefat, K., Sorokos, I., Papadopoulos, Y., Gheraibia, Y., 2019. A Conceptual Framework to Incorporate Complex Basic Events in HiP-HOPS, in: International Symposium on Model-Based Safety and Assessment, Springer. pp. 109–124.

Kabir, S., Edifor, E., Walker, M., Gordon, N., 2014a. Quantification of Temporal Fault Trees Based on Fuzzy Set Theory, in: Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Springer International Publishing, Brunów. pp. 255–264. doi:10.1007/978-3-319-07013-1_24.

Kabir, S., Geok, T.K., Kumar, M., Yazdi, M., Hossain, F., 2020. A Method for Temporal Fault Tree Analysis Using Intuitionistic Fuzzy Set and Expert Elicitation. IEEE Access 8, 980–996. doi:10.1109/ACCESS.2019.2961953.

Kabir, S., Papadopoulos, Y., 2018. A review of applications of fuzzy sets to safety and reliability engineering. International Journal of Approximate Reasoning 100, 29–55. doi:10.1016/j.ijar.2018.05.005.

Kabir, S., Papadopoulos, Y., 2019. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: a review. Safety Science 115, 154–175.

Kabir, S., Papadopoulos, Y., Walker, M., Parker, D., Aizpurua, J.I., Lampe, J., Rüde, E., 2017. A model-based extension to HiP-HOPS for dynamic fault propagation studies, in: International Symposium on Model-Based Safety and Assessment, Springer. pp. 163–178. doi:10.1007/978-3-319-64119-5_11.

Kabir, S., Walker, M., Papadopoulos, Y., 2014b. Reliability Analysis of Dynamic Systems by Translating Temporal Fault Trees into Bayesian Networks, in: Ortmeier, F., Rauzy, A. (Eds.), Model-Based Safety and Assessment. Springer International Publishing, Cham. volume 8822 of *Lecture Notes in Computer Science*, pp. 96–109. doi:10.1007/978-3-319-12214-4.

Kabir, S., Walker, M., Papadopoulos, Y., 2015. Quantitative evaluation of Pandora Temporal Fault Trees via Petri Nets. IFAC-PapersOnLine 48, 458–463. doi:10.1016/j.ifacol.2015.09.569.

Kabir, S., Walker, M., Papadopoulos, Y., 2018a. Dynamic system safety analysis in HiP-HOPS with Petri nets and Bayesian networks. Safety Science 105, 55–70.

Kabir, S., Walker, M., Papadopoulos, Y., Rüde, E., Securius, P., 2016. Fuzzy temporal fault tree analysis of dynamic systems. International Journal of Approximate Reasoning 77, 20–37. doi:10.1016/j.ijar.2016.05.006.

Kabir, S., Yazdi, M., Aizpurua, J.I., Papadopoulos, Y., 2018b. Uncertainty-aware dynamic reliability analysis framework for complex systems. IEEE Access 6, 29499 – 29515. doi:10.1109/ACCESS.2018.2843166.

Kaiser, B., Gramlich, C., Förster, M., 2007. State/event fault trees- A safety analysis model for software-controlled systems. Reliability Engineering & System Safety 92, 1521–1537.

Kara-Zaitri, C., Ever, E., 2009. A hardware accelerated semi analytic approach for fault trees with repairable components, in: 2009 11th International Conference on Computer Modelling and Simulation, IEEE. pp. 146–151.

Knezevic, J., Odoom, E., 2001. Reliability modelling of repairable systems using petri nets and fuzzy lambda–tau methodology. Reliability Engineering & System Safety 73, 1–17.

Lampis, M., Andrews, J., 2009. Bayesian belief networks for system fault diagnostics. Quality and Reliability Engineering International 25, 409–426.

László, P., 2011. Sensitivity investigation of fault tree analysis with matrix-algebraic method. Theory and Applications of Mathematics & Computer Science 1, 34–44.

Le, B., Andrews, J., 2016. Petri net modelling of bridge asset management using maintenance-related state conditions. Structure and Infrastructure Engineering 12, 730–751.

Li, Y.F., Huang, H.Z., Liu, Y., Xiao, N., Li, H., 2012. A new fault tree analysis method : fuzzy dynamic fault tree analysis. Eksploatacja i Niezawodnosc-Maintenance and Reliability 14, 208–214.

Li, Y.F., Mi, J., Liu, Y., Yang, Y.J., Huang, H.Z., 2015. Dynamic fault tree analysis based on continuous-time Bayesian networks under fuzzy numbers. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability , 1–12doi:10.1177/1748006X15588446.

Linard, A., Bucur, D., Stoelinga, M., 2019. Fault trees from data: Efficient learning with an evolutionary algorithm. arXiv preprint arXiv:1909.06258 .

Lindhe, A., Norberg, T., Rosen, L., 2012. Approximate dynamic fault tree calculations for modelling water supply risks. Reliability Engineering & System Safety 106, 61–71.

Liping, H., Fuzheng, Q., 2009. Possibilistic entropy-based measure of importance in fault tree analysis. Journal of Systems Engineering and Electronics 20, 434–444.

Liu, D., Chen, X.J., Li, Y., Zhao, Z.W., Li, X.M., 2012. Dynamic fault trees analysis for importance measures based on cut sequence set model, in: Applied Mechanics and Materials, Trans Tech Publ. pp. 578–582.

Liu, D., Xing, W., Zhang, C., Li, R., Li, H., 2007a. Cut sequence set generation for fault tree analysis, in: Embedded Software and Systems, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 592–603.

Liu, D., Zhang, C., Xing, W., Li, R., Li, H., 2007b. Quantification of cut sequence set for fault tree analysis, in: High Performance Computing and Communications, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 755–765.

Liu, T., Chiou, S., 1997. The application of Petri nets to failure analysis. Reliability Engineering & System Safety 57, 129–142.

Lo, H.k., Huang, C.y., Chang, Y.r., Huang, W.c., Chang, J.r., 2005. Reliability and sensitivity analysis of embedded systems with modular dynamic fault trees, in: TENCON 2005-2005 IEEE Region 10 Conference, IEEE. pp. 1–6.

Long, W., Sato, Y., Horigome, M., 2000. Quantification of sequential failure logic for fault tree analysis. Reliability Engineering & System Safety 67, 269 – 274. doi:https://doi.org/10.1016/S0951-8320(99)00075-7.

Longo, F., Scarpa, M., Puliafito, A., 2016. WebSPN: A Flexible Tool for the Analysis of Non-Markovian Stochastic Petri Nets, in: Principles of Performance and Reliability Modeling and Evaluation. Springer, pp. 255–285.

Lu, L., Jiang, J., 2007. Joint failure importance for noncoherent fault trees. IEEE transactions on reliability 56, 435–443.

Malhotra, M., Trivedi, K.S., 1995. Dependability modeling using Petri-nets. IEEE Transactions on Reliability 44, 428–440.

Manian, R., Coppit, D.W., Sullivan, K.J., Dugan, J.B., 1999. Bridging the gap between systems and dynamic fault tree models, in: Annual Reliability and Maintainability. Symposium. 1999 Proceedings (Cat. No. 99CH36283), IEEE. pp. 105–111.

Manian, R., Dugan, J.B., Coppit, D., Sullivan, K.J., 1998. Combining Various Solution Techniques for Dynamic Fault Tree Analysis of Computer Systems, in: Proceedings of Third IEEE International High-Assurance Systems Engineering Symposium, IEEE, Washington DC. pp. 21–28. doi:10.1109/HASE.1998.731591.

Manno, G., Chiacchio, F., Compagno, L., D'Urso, D., Trapani, N., 2014. Conception of repairable dynamic fault trees and resolution by the use of raatss, a matlab® toolbox based on the ats formalism. Reliability Engineering & System Safety 121, 250–262.

Manno, G., Chiacchio, F., Compagno, L., D'Urso, D., Trapani, N., 2012a. Matcarlore: An integrated ft and monte carlo simulink tool for the reliability assessment of dynamic fault tree. Expert Systems with Applications 39, 10334–10342.

Manno, G., Chiacchio, F., D'Urso, D., Trapani, N., Compagno, L., 2012b. Raatss, an extensible matlab® toolbox for the evaluation of repairable dynamic fault trees, in: International Conference on Probabilistic Safety Assessment and Management, ESREL, pp. 1–10.

Marquez, D., Neil, M., Fenton, N., 2008. Solving Dynamic Fault Trees using a New Hybrid Bayesian Network Inference Algorithm, in: 16th Mediterranean Conference on Control and Automation, IEEE. pp. 609–614.

Marquez, D., Neil, M., Fenton, N., 2010. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering & System Safety 95, 412–425.

Marseguerra, M., Zio, E., 2004. Monte Carlo estimation of the differential importance measure: application to the protection system of a nuclear reactor. Reliability Engineering & System Safety 86, 11–24.

Marseguerra, M., Zio, E., Devooght, J., Labeau, P.E., 1998. A concept paper on dynamic reliability via Monte Carlo simulation. Mathematics and Computers in simulation 47, 371–382.

Marseguerra, M., Zio, E., Podofillini, L., 2005. First-order differential sensitivity analysis of a nuclear safety system by Monte Carlo simulation. Reliability Engineering & System Safety 90, 162–168.

Merle, G., 2010. Algebraic modelling of Dynamic Fault Trees, contribution to qualitative and quantitative analysis. Ph.D. thesis. ENS CACHAN.

Merle, G., Roussel, J.M., Lesage, J.J., 2011. Algebraic determination of the structure function of dynamic fault trees. Reliability Engineering & System Safety 96, 267–277.

Merle, G., Roussel, J.M., Lesage, J.J., 2014. Quantitative analysis of dynamic fault trees based on the structure function. Quality and Reliability Engineering International 30, 143–156.

Merle, G., Roussel, J.M., Lesage, J.J., Bobbio, A., 2010. Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events. IEEE Transactions on Reliability 59, 250–261.

Merle, G., Roussel, J.M., Lesage, J.J., Perchet, V., Vayatis, N., 2016. Quantitative analysis of dynamic fault trees based on the coupling of structure functions and Monte Carlo simulation. Quality and Reliability Engineering International 32, 7–18.

Mi, J., Li, Y.F., Yang, Y.J., Peng, W., Huang, H.Z., 2016. Reliability assessment of complex electromechanical systems under epistemic uncertainty. Reliability Engineering & System Safety 152, 1–15.

Minato, S.i., 2001. Zero-suppressed BDDs and their applications. International Journal on Software Tools for Technology Transfer 3, 156–170.

Montani, S., Portinale, L., Bobbio, A., 2005. Dynamic Bayesian networks for modeling advanced fault tree features in dependability analysis, in: Proceedings of the sixteenth European conference on safety and reliability, pp. 1415–22.

Montani, S., Portinale, L., Bobbio, A., Codetta-Raiteri, D., 2006a. Automatically translating dynamic fault trees into dynamic Bayesian networks by means of a software tool, in: The First International Conference on Availability, Reliability and Security, IEEE. pp. 1–6.

Montani, S., Portinale, L., Bobbio, A., Codetta-Raiteri, D., 2008. Radyban: A tool for reliability analysis of dynamic fault trees through conversion into dynamic bayesian networks. Reliability Engineering & System Safety 93, 922–932.

Montani, S., Portinale, L., Bobbio, A., Varesio, M., Codetta-Raiteri, D., 2006b. A tool for automatically translating dynamic fault trees into dynamic Bayesian networks, in: Annual Reliability and Maintainability Symposium, IEEE. pp. 434–441.

Ni, J., Tang, W., Xing, Y., 2013. A simple algebra for fault tree analysis of static and dynamic systems. IEEE Transactions on Reliability 62, 846–861.

Niwas, R., Garg, H., 2018. An approach for analyzing the reliability and profit of an industrial system based on the cost free warranty policy. Journal of the Brazilian Society of Mechanical Sciences and Engineering 40, 265.

Norberg, T., Rosén, L., Lindhe, A., et al., 2009. Added value in fault tree analyses, in: 20Safety, Reliability and Risk Analysis: Theory, Methods and Applications', joint ESREL (European Safety and Reliability) and SRA-Europe (Society for Risk Analysis Europe) conference, Valencia, Spain, 22nd–25th September, pp. 1041–1049.

Noroozian, A., Kazemzadeh, R.B., Zio, E., Niaki, S.T.A., 2019. Importance analysis considering time-varying parameters and different perturbation occurrence times. Quality and Reliability Engineering International .

Ou, Y., 2003. Dependability and sensitivity analysis of multi-phase systems using Markov chains. Phd thesis. University of Virginia.

Ou, Y., Dugan, J.B., 2000. Sensitivity analysis of modular dynamic fault trees, in: Proceedings IEEE International Computer Performance and Dependability Symposium. IPDS 2000, IEEE. pp. 35–43.

Ou, Y., Dugan, J.B., 2003. Approximate sensitivity analysis for acyclic markov reliability models. IEEE Transactions on Reliability 52, 220–230.

Palshikar, G.K., 2002. Temporal fault trees. Information and Software Technology 44, 137–150.

Papadopoulos, Y., Aslansefat, K., Katsaros, P., Bozzano, M., 2019. Model-Based Safety and Assessment. Springer.

Patterson-Hine, F., Dugan, J.B., 1992. Modular techniques for dynamic fault tree-analysis, in: Annual Reliability and Maintainability Symposium 1992 Proceedings, IEEE. pp. 363–369.

Petkov, G., Pekov, M., 2009. Ageing effects sensitivity analysis by dynamic system reliability methods (go-flow and atrd). Report from Technical University of Sofia, Bulgaria .

Ping, Y.L., 2011. Analysis on Dynamic Fault Tree Based on Fuzzy Set. Applied Mechanics and Materials 110-116, 2416–2420.

Piriou, P.Y., Faure, J.M., Lesage, J.J., 2017. Generalized boolean logic driven markov processes: A powerful modeling framework for model-based safety analysis of dynamic repairable and reconfigurable systems. Reliability Engineering & System Safety 163, 57–68.

Piriou, P.Y., Faure, J.M., Lesage, J.J., 2019. Finding the minimal cut sequences of dynamic, repairable, and reconfigurable systems from Generalized Boolean logic Driven Markov Process models. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability , 1–12doi:10.1177/1748006X19827128.

Portinale, L., Codetta-Raiteri, D., Montani, S., 2010. Supporting reliability engineers in exploiting the power of dynamic Bayesian networks. International journal of approximate reasoning 51, 179–195.

Pullum, L.L., Dugan, J.B., 1996. Fault tree models for the analysis of complex computer-based systems, in: Proceedings of 1996 Annual Reliability and Maintainability Symposium, IEEE. pp. 200–207.

Ramezani, Z., Latif-Shabgahi, G.R., Khajeie, P., Aslansefat, K., 2016. Hierarchical steady-state availability evaluation of dynamic fault trees through equal markov model, in: 2016 24th Iranian Conference on Electrical Engineering (ICEE), IEEE. pp. 1848–1854.

Ranjbar, A.H., Kiani, M., Fahimi, B., 2011. Dynamic markov model for reliability evaluation of power electronic systems, in: 2011 International conference on power engineering, energy and electrical drives, IEEE. pp. 1–6.

Rao, K.D., Gopika, V., Rao, V.S., Kushwaha, H., Verma, A.K., Srividya, A., 2009. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment. Reliability Engineering & System Safety 94, 872–883.

Raptodimos, Y., Lazakis, I., 2017. Fault tree analysis and artificial neural network modelling for establishing a predictive ship machinery maintenance methodology, in: International Conference on Smart Ship Technology, Royal Institution of Naval Architects. pp. 1–11.

Rauzy, A.B., 2011. Sequence algebra, sequence decision diagrams and dynamic fault trees. Reliability Engineering & System Safety 96, 785 – 792. doi:`https://doi.org/10.1016/j.ress.2011.02.005`.

ReliaSoft, 2016. BlockSim: System Reliability and Maintainability Analysis Software Tool. URL: `http://www.reliasoft.com/BlockSim/index.html`.

Ruijters, E., Stoelinga, M., 2015. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review 15, 29–62.

Sahner, R.A., Trivedi, K.S., 1987. Reliability modeling using sharpe. IEEE Transactions on Reliability 36, 186–193.

Sharvia, S., Kabir, S., Walker, M., Papadopoulos, Y., 2015. Model-based dependability analysis: State-of-the-art, challenges, and future outlook, in: Software Quality Assurance: In Large Scale and Complex Software-intensive Systems. Elsevier, pp. 251–278. doi:`10.1016/B978-0-12-802301-3.00012-0`.

Sikorska, J., Hodkiewicz, M., Ma, L., 2011. Prognostic modelling options for remaining useful life estimation by industry. Mechanical systems and signal processing 25, 1803–1836.

Simen, E., Agrell, C., Hafver, A., Børre Pedersen, F., 2018. AI + SAFETY: Safety implications for Artificial Intelligence. Technical Report. DNV GL, Group Technology & Research. URL: `https://ai-and-safety.dnvgl.com`.

Simeu-Abazi, Z., Lefebvre, A., Derain, J.P., 2011. A methodology of alarm filtering using dynamic fault tree. Reliability Engineering & System Safety 96, 257–266.

Sullivan, K.J., Dugan, J.B., Coppit, D., 1999. The galileo fault tree analysis tool, in: Digest of Papers. Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing (Cat. No. 99CB36352), IEEE. pp. 232–235.

Taheri Kalani, J., Aslansefat, K., Latif Shabaghi, G., 2017. A systematic approach to design and analysis of univariate alarm systems using penalty approaches. Journal of Control 10, 1–15.

Tang, Z., Dugan, J.B., 2004. Minimal cut set/sequence generation for dynamic fault trees, in: Annual Reliability and Maintainability Symposium, pp. 207–213. doi:`10.1109/RAMS.2004.1285449`.

Tannous, O., Xing, L., Dugan, J.B., 2011. Reliability analysis of warm standby systems using sequential BDD, in: Proceedings of Annual Reliability and Maintainability Symposium (RAMS), IEEE. pp. 1–7.

Trivedi, K.S., Bobbio, A., 2017. Reliability and availability engineering: modeling, analysis, and applications. Cambridge University Press.

Vaurio, J.K., 2010. Ideas and developments in importance measures and fault-tree techniques for reliability and risk analysis. Reliability Engineering & System Safety 95, 99–107.

Verma, A., Srividya, A., Prabhudeva, S., Vinod, G., 2006. Reliability analysis of Dynamic fault tree models using fuzzy sets. Communications in Dependability and Quality Management 9, 68–78.

Verma, A.K., Srividya, A., Karanki, D.R., 2010. System reliability modeling. Reliability and Safety Engineering , 71–168.

Vesely, W.E., Stamatelatos, M., Dugan, J., Fragola, J., Minarick, J., Railsback, J., 2002. Fault tree handbook with aerospace applications.

Volk, M., Junges, S., Katoen, J.P., 2018. Fast dynamic fault tree analysis by model checking techniques. IEEE Transactions on Industrial Informatics 14, 370–379.

Volovoi, V., 2004. Modeling of system reliability Petri nets with aging tokens. Reliability Engineering & System Safety 84, 149–161.

Walker, M., 2009. Pandora: A Logic for the Qualitative Analysis of Temporal Fault Trees. Phd thesis. University of Hull.

Weber, P., Jouffe, L., 2003. Reliability modelling with dynamic Bayesian networks. IFAC Proceedings Volumes 36, 57–62.

Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence 25, 671–682.

Xiang, J., Machida, F., Tadano, K., Yanoo, K., Sun, W., Maeno, Y., 2012. Combinatorial Analysis of Dynamic Fault Trees with Priority-AND Gates, in: 23rd International Symposium on Software Reliability Engineering Workshops, pp. 3–4. doi:10.1109/ISSREW.2012.27.

Xiang, J., Machida, F., Tadano, K., Yanoo, K., Sun, W., Maeno, Y., 2013. A Static Analysis of Dynamic Fault Trees with Priority-AND Gates, in: Sixth Latin-American Symposium on Dependable Computing, pp. 58–67. doi:10.1109/LADC.2013.14.

Xing, L., 2004. Maintenance-oriented fault tree analysis of component importance, in: Annual Symposium Reliability and Maintainability, 2004-RAMS, IEEE. pp. 534–539.

Xing, L., Dugan, J.B., 2002. Analysis of generalized phased-mission system reliability, performance, and sensitivity. IEEE Transactions on Reliability 51, 199–211.

Xing, L., Shrestha, A., Dai, Y., 2011. Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures. Reliability Engineering & System Safety 96, 1375–1385.

Xing, L., Tannous, O., Dugan, J.B., 2012. Reliability Analysis of Nonrepairable Cold-Standby Systems Using Sequential Binary Decision Diagrams. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 42, 715–726. doi:10.1109/TSMCA.2011.2170415.

Xu, J., Wang, J., Izadi, I., Chen, T., 2011. Performance assessment and design for univariate alarm systems based on far, mar, and aad. IEEE Transactions on Automation Science and Engineering 9, 296–307.

Yassmeen Elderhalli, O.H., Tahar, S., 2019. Using machine learning to minimize user intervention in theorem proving based dynamic fault tree analysis. 4th Conference on Artificial Intelligence and Theorem Proving 2019, 1–2.

Yazdi, M., Kabir, S., 2017. A fuzzy Bayesian network approach for risk analysis in process industries. Process Safety and Environmental Protection 111, 507–519.

Yazdi, M., Kabir, S., 2018. Fuzzy evidence theory and Bayesian networks for process systems risk analysis. Human and Ecological Risk Assessment: An International Journal , 1–30.

Yevkin, O., 2010. An improved Monte Carlo method in fault tree analysis, in: 2010 Proceedings-Annual Reliability and Maintainability Symposium (RAMS), IEEE. pp. 1–5.

Yevkin, O., 2011. An improved modular approach for dynamic fault tree analysis, in: 2011 Proceedings-Annual Reliability and Maintainability Symposium, IEEE. pp. 1–5.

Yevkin, O., 2016. An efficient approximate Markov chain method in dynamic fault tree analysis. Quality and Reliability Engineering International 32, 1509–1520.

Yin, L., Smith, M.A., Trivedi, K.S., 2001. Uncertainty analysis in reliability modeling, in: Annual Reliability and Maintainability Symposium. 2001 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 01CH37179), IEEE. pp. 229–234.

Yuge, T., Yanagi, S., 2008. Quantitative analysis of a fault tree with priority and gates. Reliability Engineering & System Safety 93, 1577–1583.

Zhang, H., Zhang, C., Liu, D., Li, R., 2011. A method of quantitative analysis for dynamic fault tree, in: Proceedings of Annual Reliability and Maintainability Symposium, pp. 1–6. doi:10.1109/RAMS.2011.5754471.

Zhang, X., Miao, Q., Fan, X., Wang, D., 2009. Dynamic fault tree analysis based on Petri nets, in: 8th International Conference on Reliability, Maintainability and Safety(ICRMS), IEEE, Chengdu. pp. 138–142.

Zhou, Z., Yan, Z., Zhou, J., Jin, G., Dong, D., Pan, Z., 2006. Design of dynamic systems based on dynamic fault trees and neural networks, in: 2006 IEEE International Conference on Automation Science and Engineering, IEEE. pp. 124–128.

Zio, E., Podofillini, L., Levitin, G., 2004. Estimation of the importance measures of multi-state elements by monte carlo simulation. Reliability Engineering & System Safety 86, 191–204.

Zixian, L., Xin, N., Yiliu, L., Qinglu, S., Yukun, W., 2011. Gastric esophageal surgery risk analysis with a fault tree and markov integrated model. Reliability Engineering & System Safety 96, 1591–1600.

Zonouz, S.A., Miremadi, S.G., 2006. A fuzzy-monte carlo simulation approach for fault tree analysis, in: RAMS'06. Annual Reliability and Maintainability Symposium, 2006., IEEE. pp. 428–433.