Algebraic Dynamic Fault Tree Analysis for Avionic Systems

Neda Baghalizadeh Moghadam, Yvon Savaria, Yves Audet, and Claude Thibeault

***Abstract*—This paper presents a Dynamic Fault Tree (DFT) analysis dedicated for aircraft based on algebraic functions describing dynamic gates. The aircraft model consists of four subtrees composed of PAND and FDEP dynamic gates along with OR gates. The subtrees are designed to model failures in flight control computers, elevators, ailerons, and rudder in the avionic control systems of the aircraft. Using temporal operators and some related theorems, the behavioral and the probabilistic models of the dynamic gates are separately determined. Compared to traditional computerized methods such as Monte Carlo simulations and Markov analysis, the proposed algebraic method is simpler to implement, and less computer intensive to solve a DFT rapidly and accurately.**

***Index Terms*—Algebraic dynamic fault tree analysis, failure probability, dynamic gates, failure rates.**

I. INTRODUCTION

Fault Tree Analysis (FTA) has gained a great deal of attention in many applications where quantitative reliability and safety analysis are crucial. It exploits logical and probabilistic analysis for all possible ways an undesired state called top event (TE) can occur in a given system. As the system possesses several types of dynamic metrics, the FT becomes larger and results in a more complex analysis. Dynamic FTA (DFTA) is used to model the dynamic behavior of a system. In addition to the combination of failure events in DFTA, their order of occurrence is also considered.

Much research has been conducted on methods of solving DFTs [1]–[3]. Markov analysis is one the most common methods for solving dynamic gates in DFT analyses. A limitation of this method is that it tends to generate a large number of system states, even for moderate size FTs, which increases the system complexity and the computing time of the analysis [1]. To circumvent this issue, Monte Carlo simulations are widely used to solve DFTs without relying on Markov states. In this technique, the actual process and random behavior of a system is simulated on a computer-based model to estimate the probability of occurrence of an event as a function of time. However, simulation-based DFTA methods generally require more computational time to achieve a high level of accuracy [2]. Compared to other methods, algebraic methods have proven to be promising candidates for solving dynamic fault trees as they are more straightforward and less computer intensive while providing a similar level of accuracy [4].

N. B. Moghadam, Y. Savaria, and Y. Audet are with the Electrical Engineering Department, École Polytechnique, Montréal, QC, Canada.

Claude Thibeault is with the Electrical Engineering Department, École de Technologie Supérieur (ETS), Montréal, QC, Canada.
Corresponding author: Neda Baghalizadeh Moghadam,
(Email: neda.baghalizadeh-moghadam@polymtl.ca).

II. THEORY OF THE ALGEBRAIC MODEL

A. PAND and FDEP Dynamic Gates

A fault tree is used to model the probability of failure of a system based on subtrees of possible faulty events. Using FTA, the potential causes that can lead to system failures are identified and the probability of the TE is evaluated. Faults can originate from several sources, such as hardware components, human operations, software, etc. Such an analysis is represented by a graphical structure called a fault tree (FT) that describes the logical interrelationships between basic events causing the undesired TE. The FT allows to determine the operational relationship among different components under different modes to derive analytical expressions of the failure probability. A general static FTA is mainly based on the graphical representation of different combinations of basic events which result in the TE. In this static analysis, all possible ways that can lead to the TE occurrence are logically investigated such that all events are considered as binary events, statically independent, and their relationships are represented by logical Boolean gates.

Unlike traditional logical gates like AND, OR, etc., dynamic gates can express dynamic behavior of failure mechanisms in a system with dependent events and failures. A DFTA uses dynamic gates in its FT to represent sequential events that can lead to system failure [3]–[5]. By considering the order of failures in DFTAs, the dynamic relationships between the TE and the basic events can also be analyzed, contrary to the traditional static FTs which only express the occurrence of basic events. DFTA has always been a promising method for systems requiring a high level of safety [4]. A typical DFT has at least one dynamic gate along with a combination of static gates, i.e., AND ($\cdot$), OR ($+$), and voting gates. In this work, we exploit two common types of dynamic gates; the priority AND (PAND) and the functional dependency (FDEP) gates shown in Fig. 1.

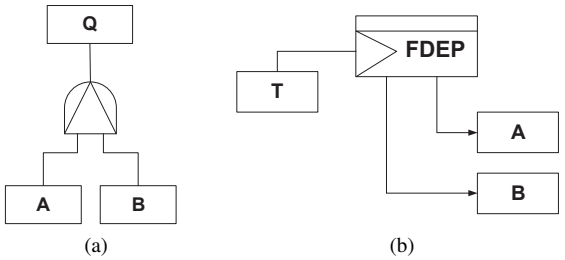


Fig. 1. Schematic illustration of dynamic gates used in DFTA; (a) the priority AND (PAND) gate, and (b) the functional dependency (FDEP) gate.

The PAND gate depicted in Fig. 1a is logically similar to the traditional AND but the occurrence order of its input events affects the occurrence of its output event Q. The output Q of a PAND gate with two inputs becomes true (failure state) if and only if both basic events A and B have reached failure such that A has failed before B.
In the FDEP gate shown in Fig. 1b, basic events A and B may fail either by themselves, or due to the trigger event T. The dependent basic events occur as a consequence of the trigger input, which means that the individual occurrence of any dependent basic event will not affect the trigger event. Once the trigger event takes place in the gate, the dependent events (A and B) of the gate occur. The effect of trigger T can be modeled by using substituted variables A_T and B_T. In this regard, the basic event A_T fails if it is forced to fail by T. It may also fail by itself before failure of T.

B. Behavioral Models of PAND and FDEP Gates

Using temporal operators, such as non-inclusive BEFORE ($\lhd$), SIMULTANOUS ($\triangle$) and Inclusive BEFORE ($\trianglelefteq$), for any non-repairable events, several theorems with their proofs are given in [6]. $a \lhd b$ occurs if event a occurs before event b, or if a occurs and b never occurs, i.e., $b \equiv \perp$, where $\perp$ denotes zero. The operator $\triangle$ is used for modelling simultaneous events. $a \trianglelefteq b$ occurs if a occurs before b ($a \lhd b$) or if a and b occur simultaneously ($a \triangle b$). Using these theorems and according to [6], the behavioural models of the PAND and FDEP gates can be determined and simplified as follows

$$\begin{aligned} PAND:\ Q &= (A \cdot B) \cdot (A \trianglelefteq B) \\ &= B \cdot (A \trianglelefteq B) = B \cdot (A \lhd B + A \triangle B), \end{aligned} \tag{1}$$

$$FDEP: \begin{cases} A_T = T + (A \trianglelefteq T) = T + A, \\ B_T = T + (B \trianglelefteq T) = T + B. \end{cases} \tag{2}$$

C. Probabilistic Model of PAND and FDEP Gates

The next step is to determine the probabilistic model of the dynamic gates used in this paper. For an exponential distribution, $f(x) = F'(x)$ where $f(t)$ represents the probability density function (*pdf*) and $F(t)$ denotes the cumulative distribution function (*cdf*) According to [4], and [7], some useful probabilistic expressions to determine the probabilistic models of the PAND and FDEP gates are:

$$Pr\{a \cdot b\}(t) = F_a(t) \times F_b(t), \tag{3}$$

$$Pr\{a + b\}(t) = F_a(t) + F_b(t) - F_a(t) \times F_b(t), \tag{4}$$

$$Pr\{a \lhd b\}(t) = \int_0^t f_a(u)\,(1 - F_b(u))\,du. \tag{5}$$

According to [6], and using equations (1) and (5), the probabilistic model of the PAND gate with independent input events, i.e., $A \triangle B = \perp$, can be given by

$$\begin{aligned} PAND: F_Q(t) = Pr\{Q\}(t) &= Pr\{B \cdot (A \lhd B)\}(t) \\ &= \int_0^t f_B(u)\,F_A(u)\,du. \end{aligned} \tag{6}$$

In the case of the FDEP gate, using (2), (3), and (4), its probabilistic model can be determined by

$$FDEP: \begin{cases} F_{A_T}(t) = Pr\{A_T\}(t) = Pr\{T + A\}(t) \\ \qquad = F_A(t) + F_T(t) - F_A(t) \times F_T(t), \\ F_{B_T}(t) = Pr\{B_T\}(t) = Pr\{T + B\}(t) \\ \qquad = F_B(t) + F_T(t) - F_B(t) \times F_T(t). \end{cases} \tag{7}$$

III. ALGEBRAIC ANALYSIS OF THE DFTA FOR AVIONIC SYSTEMS

In this section, the avionic system failure probability of an aircraft is obtained through algebraic analysis of a DFT that is designed using PAND and FDEP dynamic gates along with OR static gates. As shown in Fig. 2, the DFT consists of four independent subtrees starting from the left side of the figure:

- Subtree 1: Flight control computers failure with the top event $TE1$,
- Subtree 2: Elevators failure with the top event $TE2$,
- Subtree 3: Ailerons failure with the top event $TE3$,
- Subtree 4: Rudder failure with the top event $TE4$.

The failure probabilities of the four subtrees, can be determined by using the probabilistic models of the PAND gate and FDEP gate given by equations (6) and (7), respectively. As can be seen in Fig. 2, subtree 1 consists of a cascade of two PAND gates to represent the three flight control computers $FC1$, $FC2$, and $FC3$ of the aircraft. During a flight if $FC1$ fails $FC2$ will take over, and in the event that $FC2$ also fails, $FC3$ will be solicited. The failure of $FC3$ after $FC1$ and $FC2$, respectively, results in subtree 1 failure ($TE1$). The structure of subtrees 2, 3 and 4 consist of the same gates: a cascade of an OR gate and an FDEP gate, each having different basic events. Subtrees 2 and 3 model failure probabilities of elevators and ailerons in the aircraft with the top events $TE2$ and $TE3$, respectively. Both elevators and ailerons are activated by their corresponding control stick by means of electronic and hydraulic systems. The elevators are used for controlling the pitch of the aircraft. Applying forward pressure to the control stick, moves the elevators downward, whereas backward pressure on the control stick moves it upward. The ailerons which are moveable plates at the outer trailing edge of the wings are used to control the movement of the aircraft around its longitudinal axis, i.e., roll control. The controlling mechanism of the ailerons is the same as the elevators. Finally, Subtree 4 represents the failure probability of the rudder which has the same gate structure as subtrees 2 and 3. The rudder is a movable plate mounted on a fixed surface of the vertical tail unit to manipulate the movement of the aircraft around its vertical axis with the right and left pedals for swinging from side to side, i.e., yaw control.

Given the dynamic fault tree of the avionic system illustrated in Fig. 2, the event $TE1$ is the top event of two cascaded PAND gates. Using equations (1) and (6), and considering the fact that the cascaded PAND gates in the DFT have independent input events ($FC1$, $FC2$, and $FC3$) the behavioural model of the event $TE1$ can be expressed as

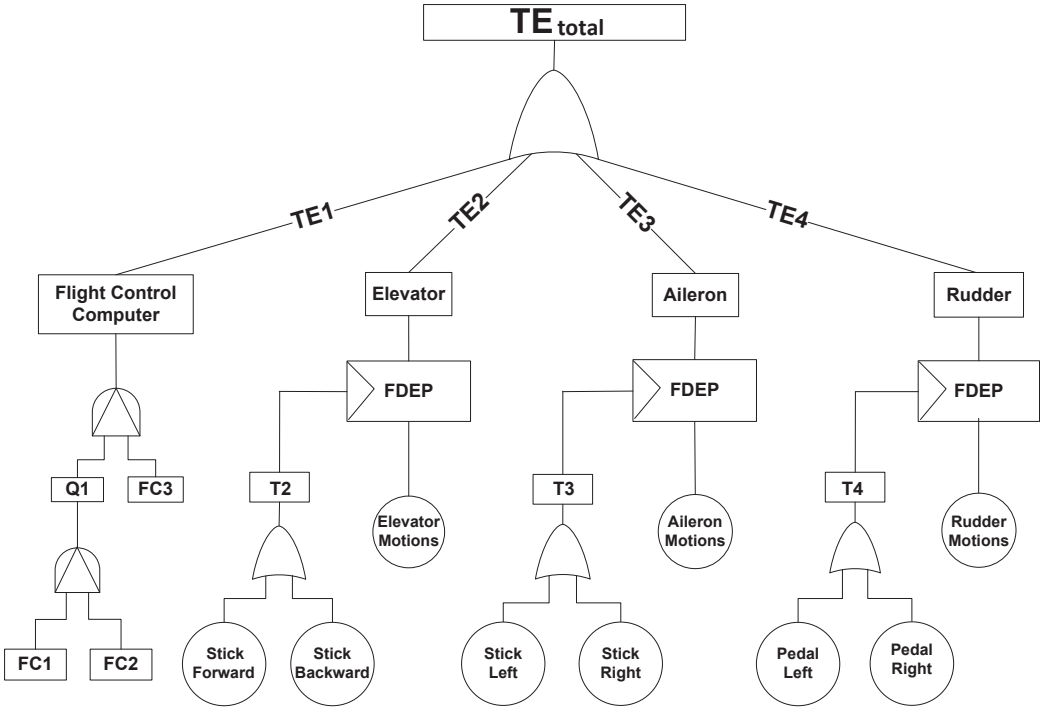


Fig. 2. Schematic illustration of the DFT for the avionic systems of an aircraft.

$$TE1 = FC3 \cdot \Big((FC2 \cdot (FC1 \trianglelefteq FC2)) \trianglelefteq FC3 \Big). \tag{8}$$

From the theorem presented in [6], and knowing that the cascaded PAND gates in the DFT have independent input events ($FC1$, $FC2$, and $FC3$), $TE1$ can be simplified to

$$TE1 = FC3 \cdot (FC1 \triangleleft FC2) \cdot (FC2 \triangleleft FC3). \tag{9}$$

According to equation (6), the failure probability of $TE1$ can be determined by

$$Pr\{TE1\}(t) = \int_0^t \left(\int_0^u \Big(\int_0^v f_{FC1}(w)\, dw \Big)\, f_{FC2}(v)\, dv \right) f_{FC3}(u)\, du. \tag{10}$$

In the case of the events $TE2$, $TE3$, and $TE4$ which are composed of an OR gate whose output serves as the trigger of an FDEP gate. The FDEP gates have one basic event being trigged by the trigger event $T2$, $T3$ and $T4$, respectively. Therefore, using equations (2), (4) and (7), the failure probability of $TE2$ can be given by

$$\begin{aligned} Pr\{TE2\}(t) &= Pr\{E + T2\}(t) \\ &= F_E(t) + F_{T2} - F_E(t) \times F_{T2}(t) \\ &= F_E(t) + F_{SB}(t) + F_{SF}(t) \\ &- F_E(t) \times F_{SB}(t) - F_E(t) \times F_{SF}(t) - F_{SB}(t) \times F_{SF}(t) \\ &+ F_E(t) \times F_{SB}(t) \times F_{SF}(t), \end{aligned} \tag{11}$$

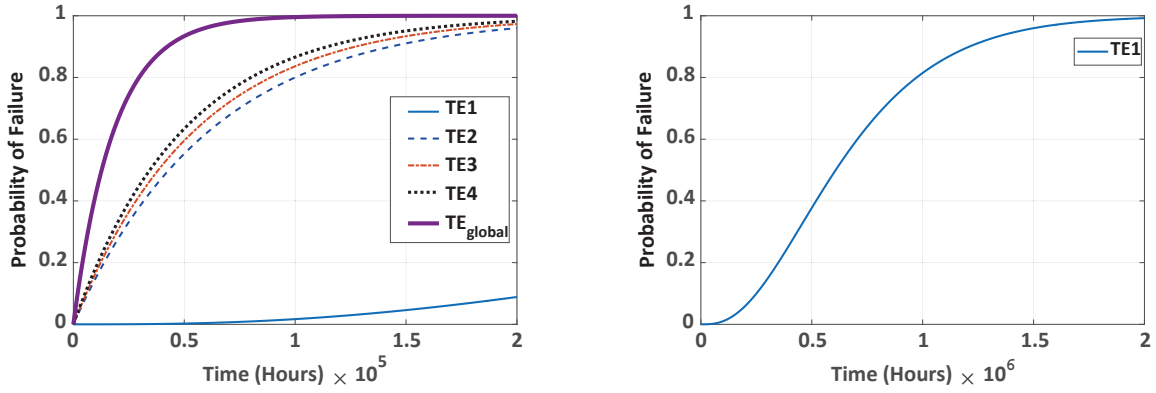
where E, SB, and SF represent elevator motions, stick backward and stick forward events in $TE2$, respectively. Similarly, the failure probability of $TE3$ and $TE4$ can be obtained by

$$\begin{aligned} Pr\{TE3\}(t) &= Pr\{Ai + T3\}(t) \\ &= F_{Ai}(t) + F_{SR}(t) + F_{SL}(t) \\ &- F_{Ai}(t) \times F_{SR}(t) - F_{Ai}(t) \times F_{SL}(t) - F_{SR}(t) \times F_{SL}(t) \\ &+ F_{Ai}(t) \times F_{SR}(t) \times F_{SL}(t), \end{aligned} \tag{12}$$

$$\begin{aligned} Pr\{TE4\}(t) &= Pr\{R + T4\}(t) \\ &= F_R(t) + F_{SR}(t) + F_{SL}(t) \\ &- F_R(t) \times F_{SR}(t) - F_R(t) \times F_{SL}(t) - F_{SR}(t) \times F_{SL}(t) \\ &+ F_R(t) \times F_{SR}(t) \times F_{SL}(t), \end{aligned} \tag{13}$$

where Ai, SR, SL denote aileron motions, stick right and stick left events in $TE3$, and R, PR, PL represent rudder motions, pedal right and pedal left events in $TE4$, respectively. Therefore, using the inclusion-exclusion equation described in [8], the entire failure probability of the DFT shown in Fig. 2 with the top event, TE_{global}, can be expressed as

$$\begin{aligned} &Pr\{TE_{global}\} = Pr\{TE1 + TE2 + TE3 + TE4\}(t) = \\ &Pr\{TE1\}(t) + Pr\{TE2\}(t) + Pr\{TE3\}(t) + Pr\{TE4\}(t) \\ &- Pr\{TE1\}(t) \times Pr\{TE2\}(t) - Pr\{TE1\}(t) \times Pr\{TE3\}(t) \\ &- Pr\{TE1\}(t) \times Pr\{TE4\}(t) - Pr\{TE2\}(t) \times Pr\{TE3\}(t) \\ &- Pr\{TE2\}(t) \times Pr\{TE4\}(t) - Pr\{TE3\}(t) \times Pr\{TE4\}(t) \\ &+ Pr\{TE1\}(t) \times Pr\{TE2\}(t) \times Pr\{TE3\}(t) \\ &+ Pr\{TE1\}(t) \times Pr\{TE2\}(t) \times Pr\{TE4\}(t) \\ &+ Pr\{TE1\}(t) \times Pr\{TE3\}(t) \times Pr\{TE4\}(t) \\ &+ Pr\{TE2\}(t) \times Pr\{TE3\}(t) \times Pr\{TE4\}(t) \\ &- Pr\{TE1\}(t) Pr\{TE2\}(t) \times Pr\{TE3\}(t) \times Pr\{TE4\}(t). \end{aligned} \tag{14}$$



(a) (b)

Fig. 3. Failure probabilities of (a) the four subtrees, separately, and the whole avionic system, (b) $TE1$ on a longer time scale.

TABLE I
FAILURE RATES (FAILURES×HOUR^{-1}) OF THE BASIC EVENTS IN THE DFT FROM [9].

Flight Control Computer			**Elevator**			**Aileron**			**Rudder**		
$FC1$	$FC2$	$FC3$	SF	SB	E	SL	SR	Ai	PL	PR	R
1E-9	1E-9	1E-9	8E-6	8E-6	1E-7	9E-6	9E-6	1E-7	1E-5	1E-5	1E-7

In this paper, to determine the failure probability of the DFT for the avionic system, the standard failure rates (failures per hour) of the constituent components given in [9] are used. Table I summarizes the standard failure rates for the different components in the DFT of the avionic system given in Fig. 2. Using the failure rates of [9], failure probabilities of the four subtrees in the DFT shown in Fig. 2, can be individually determined as a function of time in hours. These obtained values can then be used in equation (14) to obtain the failure probability of the whole system $Pr\{TE_{global}\}(t)$.

Fig. 3a shows the failure probabilities obtained for the four subtrees and for the whole avionic system as a function of time in hours. It can be inferred from the figure that subtree 2 to 4 follow the same trend as they have the same architecture. The only difference comes from the speed in which they converge towards one in accordance to the difference in stick and pedal failure rates employed in the model as displayed in Table I. In the case of $TE1$, given the triple redundancy dedicated to the flight control computers, the failure rate of the flight control system increases with time much slower compared to the other branches of the system. Fig. 3b shows the probability of failure for $TE1$ on a longer time scale, proving that it will eventually reach one as expected for every branch of the system.

IV. CONCLUSION

A DFT to model failures in avionic systems was designed and investigated. The failure probability of the DFT structure was determined by an algebraic analysis including four subtrees of the avionic system: flight control, aileron, rudder, and elevator. To this end, temporal operators such as non-inclusive BEFORE ($\lhd$), SIMULTANOUS ($\triangle$) and Inclusive BEFORE ($\trianglelefteq$) along with some other algebraic theorems were used to define the behavioural and probabilistic models of PAND and FDEP gates, as the building-blocks of the DFT. Results show the consistency of the model with respect to the failure rates and the level of redundancy defined for the subtrees.

ACKNOWLEDGMENT

This work has been funded by the research consortium CARIC under the project number AVIO-1603 and by MITACS. We are also grateful for the expertise and the financial contributions of our industrial partners: Bombardier Aeronautics, Solutions Isoneo, Star Navigation, CMC Electronics, and Bubble Technology.

REFERENCES

[1] C.-Y. Huang and Y.-R. Chang, "An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees," *Reliability Engineering & System Safety*, vol. 92, no. 10, pp. 1403–1412, 2007.

[2] J. B. Dugan, K. J. Sullivan, and D. Coppit, "Developing a low-cost high-quality software tool for dynamic fault-tree analysis," *IEEE Transactions on reliability*, vol. 49, no. 1, pp. 49–59, 2000.

[3] K. D. Rao, V. Gopika, V. S. Rao, H. Kushwaha, A. K. Verma, and A. Srividya, "Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment," *Reliability Engineering & System Safety*, vol. 94, no. 4, pp. 872–883, 2009.

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

[5] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Transactions on reliability*, vol. 41, no. 3, pp. 363–377, 1992.

[6] G. Merle, J.-M. Roussel, J.-J. Lesage, and A. Bobbio, "Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events," *IEEE Transactions on Reliability*, vol. 59, no. 1, pp. 250–261, 2010.

[7] J. Fussell, E. Aber, and R. Rahl, "On the quantitative analysis of priority-and failure logic," *IEEE Transactions on Reliability*, vol. 25, no. 5, pp. 324–326, 1976.

[8] K. S. Trivedi, *Probability & statistics with reliability, queuing and computer science applications*. John Wiley & Sons, 2008.

[9] V. Hilderman, "Do-178b to do-178c: Impact on avionics verification & certification," 2011.