Quantitative Analysis of Dynamic Fault Trees based on the Structure Function

Guillaume Merle, Jean-Marc Roussel, Jean-Jacques Lesage

Quantitative Analysis of Dynamic Fault Trees based on the Structure Function

G. Merle*, J.-M. Roussel, J.-J. Lesage

LURPA - ENS Cachan, 61 avenue du Président Wilson, Cachan, 94230, France

Abstract

This paper presents a probabilistic model of dynamic gates which allows to perform the quantitative analysis of any Dynamic Fault Tree (DFT) from its structure function. Both these probabilistic models and the quantitative analysis which can be performed thanks to them can accommodate any failure distribution of basic events. We illustrate our approach on a DFT example from the literature.

Keywords: Dynamic fault tree, structure function, probabilistic model, quantitative analysis.

1. Introduction

The structure function of a Static Fault Tree (SFT) – a Fault Tree (FT) which only contains gates OR, AND, and K-out-of-N – is a Boolean function which represents the failure of the Top Event (*TE*) according to the failure of the basic events (*BEs*) of the FT. This algebraic model is classically used to

*Corresponding author: Tel.: +33 6 23 79 54 51; fax: +33 1 47 40 22 20

Email addresses: guillaume.merle@lurpa.ens-cachan.fr (G. Merle), jean-marc.roussel@lurpa.ens-cachan.fr (J.-M. Roussel), jean-jacques.lesage@lurpa.ens-cachan.fr (J.-J. Lesage)

perform both the qualitative and quantitative analysis of SFTs directly. For complex systems, these analyses are most often performed thanks to BDD-based methods [1, 2, 3, 4] or other techniques such as Petri Nets [5], Bayesian Networks [6, 7], approximate reasoning methodologies [8], or combinatorial techniques [9, 10].

The introduction of dynamic gates – gates PAND, FDEP, and Spare – in FTs has changed the nature of the relation between the *TE* and the *BEs*. In a Dynamic Fault Tree (DFT), the failure of the *TE* depends not only on the failure of the *BEs* but also on the order of occurrence of these failures. As this last aspect is not taken into account in the Boolean model of failures (which only expresses whether a *BE* has occurred or not), a classic Boolean function cannot represent the dynamic relations between the *TE* and the *BEs* that exist in a DFT.

In a previous article, we presented an algebraic framework allowing to algebraically model dynamic gates and determine the structure function of any Dynamic Fault Tree (DFT) [11]. We also showed that the minimal cut sets and sequences of DFTs can be determined directly from this structure function, in the same way that the minimal cut sets of SFTs can be determined directly from their structure function.

In the current paper, we first present an algorithm which can calculate the structure function of any DFT under a minimal canonical form with the minimization criterion presented in [11]. Then, after recalling the probabilistic models of dynamic gates which have been presented in [12, 13, 14], we present a novel approach allowing to perform the quantitative analysis of any DFT from its structure function, thanks to the probabilistic model of

dynamic gates. Finally, we illustrate our approach on a DFT example from the litterature by considering Weibull failure distributions for basic events, which allows to emphasize the fact that our approach can accommodate any failure distribution of basic events. We chose Weibull distributions because they better model the aging of the pumps considered in our DFT example than the usual Markovian distributions

This paper is organised as follows. The most common approaches used to perform the quantitative analysis of DFTs are presented in Section 2. The algebraic framework that we have introduced to model DFTs is recalled in Section 3. Our approach and the probabilistic models of dynamic gates are detailed in Section 4, and our approach is illustrated on a DFT example in Section 5.

2. State of the art

Many approaches have been envisaged to perform the quantitative analysis of DFTs without using their structure function. In [15], each dynamic gate of the considered DFT is replaced by the static gate corresponding to its logic constraints; the minimal cut sets of the resulting SFT are then generated by using Zero-suppressed BDDs (ZBDDs), and these minimal cut sets are expanded to minimal cut sequences by considering the timing constraints. However, it can be noted that some constraints cannot be taken into account during this conversion of dynamic gates into static gates as this conversion leads to a too long list of sequences for the qualitative analysis: we showed in [16] that, during the conversion of many Spare gates sharing a spare event into static gates, the behaviour of the spare event cannot be correctly taken

into account. The authors of [17] propose to convert the DFT into a failure automaton which models the changing state of the system as failures occur. This failure automaton can then be converted into a Continuous Time Markov Chain (CTMC), and the solution of the corresponding set of differential equations allows to determine the failure probability of the *TE* of the DFT. These two approaches have been implemented in the Galileo tool [2].

Other model-based approaches also allow to perform the quantitative analysis of DFTs. For instance, in [18], the whole DFT is converted into a dynamic Bayesian Network and the failure probability of the *TE* of the DFT can be determined by using inference algorithms. In [9], the dynamic subtrees of DFTs are converted into a class of coloured Stochastic Petri Nets called Stochastic Well-formed Net (SWN). This SWN can be converted into a CTMC to determine the failure probability of the *TE* of the dynamic subtree, and this failure probability can then be cast back into the original DFT. These two approaches have been respectively implemented in the Windows [18] and Linux [19] version of the Drawnet tool. Finally, in [20], all the gates of DFTs are converted into Petri Nets, and counters are used to determine the number of times that each transition has been fired, and hence the average rate of occurrence of the system failure.

All these approaches, as well as the numerous ones which have not been cited in this section, are more or less performant. However, most of them can provide a litteral result only for exponential distributions, even though numerical simulation allows to get an approximate result of the failure probability of the *TE* for any distribution of *BEs*, with a higher computational effort.

One of the main goals of our approach is to extend the structure-function-based analysis approaches commonly used to analyze SFTs to DFTs, so as to accommodate any distribution of *BEs*. In the case of SFTs, static gates can be modelled by means of Boolean operators and the inclusion-exclusion formula [21] is sufficient to determine the failure probability of the *TE* of the FT thanks to the probabilistic model of static gates. In the case of DFTs, the inclusion-exclusion formula can still be used, but as we modelled dynamic gates by means of temporal operators, the expression obtained will contain probabilities of algebraic terms containing temporal operators, and a probabilistic model of dynamic gates is hence needed to perform quantitative analysis. We hence propose a probabilistic model of dynamic gates based on their behavioural model which was presented in [11]. The algebraic framework which has been introduced to determine this behavioural model of dynamic gates, and hence the structure function of DFTs, is recalled in Section 3.

3. Algebraic framework for the modelling of DFTs

3.1. Hypotheses

The hypotheses considered in this work are as follows:

- the DFTs that we consider are the DFTs defined in [22], which include static gates (OR, AND, and K-out-of-N) and dynamic gates (PAND, FDEP, and Spare);
- events are not repairable, in accordance with [23], so that each event has a single occurrence and can hence be assigned a single date of appearance;

- basic events have continuous failure time distributions, as considered in [24], so that independent basic events cannot occur simultaneously; and
- intermediate events of a DFT can still occur simultaneously if the DFT contains repeated events, as explained in [12].

3.2. Basics and notations of our algebraic framework

The Boolean model commonly used to model events and gates in SFTs does not allow to take into account the order of appearance of events which is needed to model dynamic gates. To be able to take into account this temporal aspect and hence model sequences of events, we consider events as Boolean functions defined on the set of positive times and which take Boolean values. As we consider non-repairable events, each non-repairable event a can be assigned a unique date of appearance $d(a)$. The timing diagram of a non-repairable event a is shown in Fig. 1.

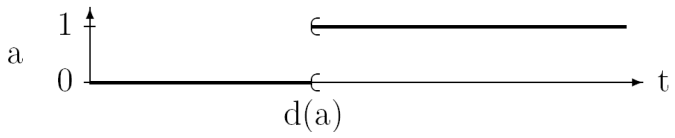


Figure 1: A non-repairable event

The identity elements of operators OR and AND in $\mathcal{E}_{nr}$ are denoted by $\bot$, and $\top$, respectively, to which these dates can be assigned:

$$d(\bot) = +\infty \quad , \quad d(\top) = 0.$$

$\bot$ is the never-occurring event whereas $\top$ is the always-occurring event.

In addition to classical operators OR ($+$) and AND ($\cdot$), we have defined three temporal operators on the set of non-repairable events (noted $\mathcal{E}_{nr}$) to model dynamic gates. These operators are: non-inclusive BEFORE ($\lhd$), SIMULTANEOUS ($\triangle$), and Inclusive BEFORE ($\trianglelefteq$). Their complete definitions can be found in [11] and are based on the date of appearance of their operands, as illustrated by the definition of the temporal operator Inclusive BEFORE:

$$d(a \trianglelefteq b) = \begin{cases} d(a) & \text{if } d(a) < d(b) \\ d(a) & \text{if } d(a) = d(b) \\ +\infty & \text{if } d(a) > d(b) \end{cases}$$

The three operators satisfy the following theorems, which will be used in the remainder of this paper, for all $a, b \in \mathcal{E}_{nr}$:

$$a \cdot (a \lhd b) = a \lhd b \tag{1}$$

$$a \triangle b = b \triangle a \tag{2}$$

$$a \cdot (a \triangle b) = a \triangle b \tag{3}$$

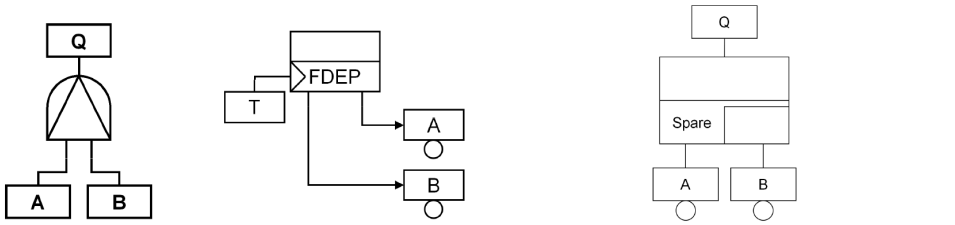
$$(a \lhd b) + (a \triangle b) + (a \cdot (b \lhd a)) = a \tag{4}$$

The exhaustive list of all the theorems verified by these three operators, as well as their proofs, can be found in [16].

3.3. Algebraic model of dynamic gates

The algebraic framework defined in [11] and recalled in Section 3.2 allows to determine the algebraic model of dynamic gates, which is briefly recalled in Fig. 2. In the case of gate FDEP, A_T and B_T denote the global failure

of basic events A and B, which can be caused by the failure of A and B by themselves, or by the failure of the trigger event T. We have showed in [13] that each –dynamic– FDEP gate is equivalent to a set of –static– OR gates, and that gate FDEP hence has a static behavior. In the case of gate Spare, B_d and B_a respectively denote the dormant and active mode of the spare event B.

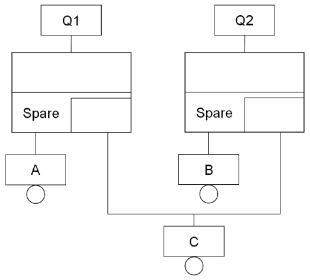


$Q = B \cdot (A \trianglelefteq B)$ $\quad A_T = T + A$ $\quad B_T = T + B$ $\quad Q = B_a \cdot (A \triangleleft B_a) + A \cdot (B_d \triangleleft A)$

Figure 2: Algebraic model of dynamic gates

Besides, the case of many Spare gates sharing a spare event has been considered in [11]. This case is a bit more complex as spare events have quite a specific behaviour: a spare event is used by the first gate whose previous events have failed, and it is made unavailable to all the other gates. For instance, the algebraic model of 2 Spare gates sharing a spare event is recalled in Fig. 3.

Finally, we have shown in [11] that Cold and Hot Spare gates can be considered as specific cases of Warm Spare gates. As the algebraic models of Spare gates presented in Tables 2 and 3 are the general algebraic models of Warm Spare gates, we will not detail the algebraic models of Cold and Hot



$$Q1 = C_a \cdot (A \lhd C_a) + A \cdot (C_d \lhd A) + A \cdot (B \lhd A)$$
$$Q2 = C_a \cdot (B \lhd C_a) + B \cdot (C_d \lhd B) + B \cdot (A \lhd B)$$

Figure 3: Algebraic model of 2 Spare gates sharing a spare event

Spare gates in this paper.

4. Quantitative analysis of DFTs based on the structure function

4.1. Minimal canonical form of the structure function

The algebraic model of dynamic gates presented in Section 3.3 allows to determine the structure function of any DFT. We have shown in [11] that this structure function can be reduced to a sum-of-product canonical form:

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \lhd b_k) \right), j \notin \{i, k\}, \tag{5}$$

where $\{b_i, i \in (1, ..., n)\}$ are the basic events of the DFT, and that the redundant terms of this canonical form – i.e. the algebraic terms which are included in one or many other algebraic terms – can be removed to obtain a minimal canonical form of the structure function. Such a minimal canonical form can be obtained for any DFT thanks to Algorithm 1, the expression for each intermediate and top event being determined under a canonical form

thanks to Algorithm 2. The removal of redundant terms at the end of Algorithm 1 guarantees that the expression obtained for the minimal canonical form of the structure function will not contain terms which can absorb each other. Indeed, any term A which may be absorbed by another term B will be included in B ($A \subset B$) and removed from the structure function by applying the minimization criterion presented in [12] (since $A \subset B \Rightarrow A \cdot B = A$).

Algorithme 1: Calculation of the structure function of a DFT

Input : DFT with gates OR, AND, PAND, WSP, and CSP

Output : Structure function under a minimal canonical form (SF)

begin

```
// Initialisation
Event = TopEvent
// Determination of the canonical form
SF = CanonicalForm(Event)
// Removal of redundant terms
SF = RedundancyFree(SF)
return SF
```

It is possible to get an idea of the complexity of such an algorithm by determining how many times each main function is called, thanks to the characteristics of the DFT:

- the function CanonicalForm() is called $(n_i + 1)$ times, n_i being the number of intermediate events in the DFT
- the function ORComposition() is called $(n_{e_{OR}} - n_{OR})$ times, $n_{e_{OR}}$ being

the number of input events to OR gates, and n_{OR} being the number of OR gates in the DFT

- the function ANDComposition() is called $(n_{e_{AND}} - n_{AND})$ times, $n_{e_{AND}}$ being the number of input events to AND gates, and n_{AND} being the number of AND gates in the DFT
- the function PANDComposition() is called n_{PAND} times, n_{PAND} being the number of PAND gates in the DFT
- the function WSPComposition() is called n_{WSP} times, n_{WSP} being the number of WSP gates in the DFT
- the function CSPComposition() is called n_{CSP} times, n_{CSP} being the number of CSP gates in the DFT

This minimal canonical form of the structure function can be determined for any DFT, whether it contains repeated events or not. Indeed, we showed in [12] that two intermediate events may occur simultaneously in a DFT which contains repeated events, and our approach is able to cope with this simultaneity problem thanks to the introduction of the operator SIMULTANEOUS.

Starting from (5), an expression of the failure probability of the *TE* of the DFT can now be determined thanks to the inclusion-exclusion formula [21]. On the one hand, this expression depends on the distribution functions of basic events, which is known. On the other hand, it also depends on the failure probability of algebraic terms containing the temporal operator $\lhd$, which is unknown *a priori*. As these algebraic terms result from the

algebraic model of dynamic gates, a probabilistic model of dynamic gates is then needed to determine the failure probability of such terms. A few useful probabilistic formulas which are necessary to determine this probabilistic model are recalled in Section 4.2, and the probabilistic model of dynamic gates is presented in Section 4.3.

4.2. Some useful probabilistic formulas

It is necessary to recall some useful probabilistic expressions to be able to determine the probabilistic model of dynamic gates. Let us consider an event x with *cumulative distribution function* (Cdf) $F(x)$ and *probability density function* (pdf) $f(x)$ ($f(x) = F'(x)$). The following expressions hold under the hypothesis of statistical independence [25, 24].

$$Pr\left\{a \cdot b\right\}(t) = F_a(t) \times F_b(t) \tag{6}$$

$$Pr\left\{a + b\right\}(t) = F_a(t) + F_b(t) - F_a(t) \times F_b(t) \tag{7}$$

$$Pr\left\{a \lhd b\right\}(t) = \int_0^t f_a(u)(1 - F_b(u))\, du \tag{8}$$

$$Pr\left\{b \cdot (a \lhd b)\right\}(t) = \int_0^t f_b(u)\, F_a(u)\, du \tag{9}$$

4.3. Probabilistic model of dynamic gates

4.3.1. Probabilistic model of gate FDEP

An FDEP gate with 2 dependent basic events is depicted in Fig. 4. As recalled in Section 3.3, the algebraic model of the FDEP gate is

$$\begin{cases} \mathrm{A_T} = \mathrm{T} + \mathrm{A} \\ \mathrm{B_T} = \mathrm{T} + \mathrm{B} \end{cases}$$

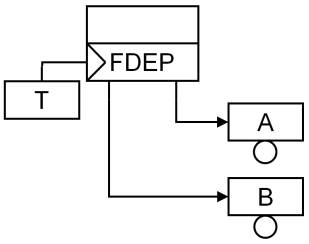


Figure 4: An FDEP gate with 2 dependent basic events

The FDEP gate hence is equivalent to a set of OR gates (one OR gate for each basic event), as demonstrated in [13]. Its probabilistic model hence is the same as the probabilistic model of the corresponding set of OR gates:

$$\begin{cases} Pr\{A_T\}(t) = Pr\{T + A\}(t) &= F_T(t) + F_A(t) - F_T(t) \times F_A(t) \\ Pr\{B_T\}(t) = Pr\{T + B\}(t) &= F_T(t) + F_B(t) - F_T(t) \times F_B(t) \end{cases}$$

4.3.2. Probabilistic model of gate PAND

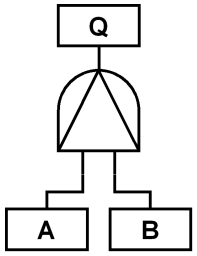


Figure 5: A PAND gate

A PAND gate is depicted in Fig. 5. As recalled in Section 3.3, the algebraic model of the PAND gate is

$$Q = B \cdot (A \trianglelefteq B)$$

The probability of occurrence of $B \cdot (A \lhd B)$ can be determined from the expression (9), but the probability of occurrence of $B \cdot (A \trianglelefteq B)$ is not known. We hence need to develop this expression to get expressions whose probability of occurrence is known. According to the definition of the temporal operator Inclusive BEFORE, $a \trianglelefteq b = a \lhd b + a \triangle b$, so[1]

$$\begin{aligned} Q &= B \cdot (A \lhd B + A \triangle B) \\ &= B \cdot (A \lhd B) + B \cdot (A \triangle B) \\ &\overset{(2),(3)}{=} B \cdot (A \lhd B) + A \triangle B \end{aligned}$$

If A and B are two statistically independent events, $A \triangle B = \perp$ and the probabilistic model of the PAND gate can be determined as

$$\begin{aligned} F_Q(t) = Pr\{Q\}(t) &= Pr\{B \cdot (A \lhd B)\}(t) \\ &\overset{(9)}{=} \int_0^t f_B(u)\, F_A(u)\, du \end{aligned}$$

If A and B are two dependent events, $A \triangle B \neq \perp$. A and B must hence be replaced by their corresponding expressions and the expression $A \triangle B$ must be developed to be able to determine the failure probability of the gate.

4.3.3. Probabilistic model of Spare gates with 2 input events

Failure distribution of spare events. Let us consider a Spare gate with 2 input events – the primary event A and one spare event B – as shown in Fig. 6.

[1] In the equation below, the notation $\overset{(2),(3)}{=}$ indicates that the expression $B \cdot (A \lhd B) + A \triangle B$ is obtained from the expression $B \cdot (A \lhd B) + B \cdot (A \triangle B)$ by applying theorems (2) and (3). This notation will be used in the remainder of this paper.

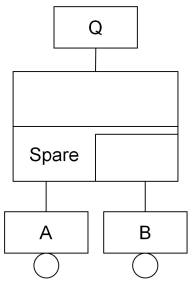


Figure 6: A single Spare gate with one primary event A and one spare event B

The failure distribution of the primary event A does not depend on B, so the Cdf and pdf of A are mere functions of time noted $F_A(t)$ and $f_A(t)$, respectively, as usual.

The failure distribution of the spare event B does not depend on A as long as B is dormant ($B \equiv B_d$), so the Cdf and pdf of B_d also are mere functions of time noted $F_{B_d}(t)$ and $f_{B_d}(t)$, respectively. However, the failure distribution of the spare event B depends on A when B is active ($B \equiv B_a$), since B becomes active at the failure date of A, which will be denoted by t_A. The Cdf and pdf of B_a hence depend both on time t and on the failure date of A (t_A). For the sake of clarity, we consider both functions as functions of the two variables t and t_A, which will be noted $F_{B_a}(t, t_A)$ and $f_{B_a}(t, t_A)$, respectively.

Let us illustrate this aspect on the particular case of exponential distributions, as this case is the most common one in reliability analyses. If A has a failure rate λ_A, for all $t \geq 0$, its Cdf and pdf are

$$\begin{cases} F_A(t) &= 1 - e^{-\lambda_A t} \\ f_A(t) &= \lambda_A e^{-\lambda_A t} \end{cases}$$

In the same way, if B has a failure rate λ_B and a dormancy α, for all $t \geq 0$, the Cdf and pdf of B_d are

$$\begin{cases} F_{B_d}(t) &= 1 - e^{-\alpha\lambda_B t} \\ f_{B_d}(t) &= \alpha\lambda_B e^{-\alpha\lambda_B t} \end{cases}$$

Regarding the Cdf of B_a, it is known that:

- it is exponential with failure rate λ_B;
- F_B is equal to F_{B_d} on $[0, t_A)$ and to F_{B_a} on $[t_A, +\infty)$, and is continuous at the failure date of A (t_A).

It can hence be assumed that $F_{B_a}(t, t_A) = 1 - e^{-\lambda_B(t - x(t_A))}$, where x is a function of t_A. By using the continuity of F_B at $t = t_A$, we have

$$\begin{aligned} & F_{B_a}(t_A, t_A) = F_{B_d}(t_A) \\ \Leftrightarrow \quad & 1 - e^{-\lambda_B(t_A - x(t_A))} = 1 - e^{-\alpha\lambda_B t_A} \\ \Leftrightarrow \quad & \lambda_B(t_A - x(t_A)) = \alpha\lambda_B t_A \\ \Leftrightarrow \quad & t_A - x(t_A) = \alpha t_A \\ \Leftrightarrow \quad & x(t_A) = (1 - \alpha)t_A \end{aligned}$$

As a consequence, for all $t \geq (1 - \alpha)t_A$,

$$\begin{cases} F_{B_a}(t, t_A) &= 1 - e^{-\lambda_B(t - (1-\alpha)t_A)} \\ f_{B_a}(t, t_A) &= \lambda_B e^{-\lambda_B(t - (1-\alpha)t_A)} \end{cases}$$

The notations used for the Cdf and pdf of the spare event B will be retained in the remainder of this dissertation, and they can be used for any spare event S by replacing t_A with the failure date of the event on which S depends, in the case of Spare gates with more than 2 input events.

Case of a single Spare gate. As recalled in Section 3.3, the algebraic model of a single Spare gate is

$$Q = B_a \cdot (A \lhd B_a) + A \cdot (B_d \lhd A).$$

As B cannot be both in its dormant and active mode, $B_a \cdot (A \lhd B_a) \cdot A \cdot (B_d \lhd A) \overset{(1)}{=} B_a \cdot (A \lhd B_a) \cdot A \cdot B_d \cdot (B_d \lhd A) = \bot$, so the two algebraic terms $B_a \cdot (A \lhd B_a)$ and $A \cdot (B_d \lhd A)$ are disjoint and

$$Pr\{Q\}(t) = Pr\{B_a \cdot (A \lhd B_a)\}(t) + Pr\{A \cdot (B_d \lhd A)\}(t)$$

On the one hand, the Cdf and pdf of B_d (B in its dormant mode) do not depend on A, so the probability of occurrence of the second term – $Pr\{A \cdot (B_d \lhd A)\}(t)$ – can be determined by means of the expression (9) as

$$Pr\{A \cdot (B_d \lhd A)\}(t) = \int_0^t f_A(u)\, F_{B_d}(u)\, du$$

On the other hand, the Cdf and pdf of B_a (B in its active mode) depend on the failure date of A, so $Pr\{B_a \cdot (A \lhd B_a)\}(t)$ cannot be determined by means of the expression (9). If we respectively denote by T_A and T_{B_a} the failure dates of A and B_a, $Pr\{B_a \cdot (A \lhd B_a)\}(t)$ can be defined as

$$\begin{aligned} Pr\{B_a \cdot (A \lhd B_a)\}(t) &= Pr\{T_A \leq T_{B_a} \leq t\} \\ &= E\left[\mathbb{1}_{\{T_A \leq T_{B_a}\}} \mathbb{1}_{\{T_{B_a} \leq t\}}\right], \end{aligned}$$

where $\mathbb{1}$ is the *indicator function* [26] defined as

$$\mathbb{1}_S(X) = \begin{cases} 1 & \text{if } X \in S \\ 0 & \text{if } X \notin S \end{cases}$$

and E is the *expectation value* [26] defined as

$$E\left[\mathbb{1}_S(X)\right] = Pr\left\{X \in S\right\}$$

S represents a set and X represents an element which may belong to S or not. For instance, in our case, $\mathbb{1}_{\{T_{B_a} \leq t\}}$ is a shorter notation for $\mathbb{1}_{[T_{B_a}, +\infty)}(t)$, and we should hence have $E\left[\mathbb{1}_{\{T_{B_a} \leq t\}}\right] = Pr\left\{T_{B_a} \leq t\right\}$.

According to the *law of total expectation* [27], if X is an integrable random variable and if Y is any random variable such that $E\left[E\left[X|Y\right]\right]$ has a meaning, the following relation holds:

$$E\left[X\right] = E\left[E\left[X|Y\right]\right]$$

As a consequence,

$$\begin{aligned} Pr\left\{B_a \cdot (A \lhd B_a)\right\}(t) &= E\left[\mathbb{1}_{\{T_A \leq T_{B_a}\}} \mathbb{1}_{\{T_{B_a} \leq t\}}\right] \\ &= E\left[E\left[\mathbb{1}_{\{T_A \leq T_{B_a}\}} \mathbb{1}_{\{T_{B_a} \leq t\}} | T_A\right]\right] \\ &= \int_0^t \left(\int_v^t f_{T_B|T_A}(u|T_A = v) du \right) f_{T_A}(v) dv \\ &= \int_0^t \left(\int_v^t f_{B_a}(u, v) du \right) f_A(v) dv \end{aligned}$$

Finally, the probabilistic model of a single Spare gate with 2 input events hence is

$$F_Q(t) = Pr\left\{Q\right\}(t) = \int_0^t \left(\int_v^t f_{B_a}(u, v) du \right) f_A(v) dv + \int_0^t f_A(u)\, F_{B_d}(u)\, du$$

This probabilistic model does not depend on the failure distribution considered for basic events. However, in the particular case of exponential distributions, we have shown in [16] that the expression obtained with this probabilistic model is the same as the expression obtained with Markov Chains.

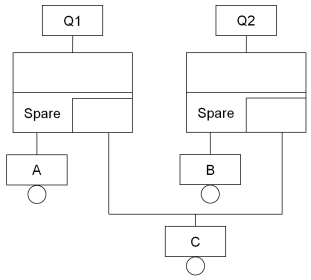


Figure 7: Two Spare gates sharing a spare event

Case of two Spare gates sharing a spare event. The case of two Spare gates sharing a spare event is depicted in Fig. 7. As recalled in Section 3.3, the algebraic model of any of two Spare gates sharing a spare event is

$$\begin{cases} Q1 = C_a \cdot (A \lhd C_a) + A \cdot (C_d \lhd A) + A \cdot (B \lhd A) \\ Q2 = C_a \cdot (B \lhd C_a) + B \cdot (C_d \lhd B) + B \cdot (A \lhd B) \end{cases}$$

Let us first consider the expression for $Q1$:

$$Q1 = C_a \cdot (A \lhd C_a) + A \cdot (C_d \lhd A) + A \cdot (B \lhd A)$$

It can be noted that the two first algebraic terms $C_a \cdot (A \lhd C_a)$ and $A \cdot (C_d \lhd A)$ do not contain B while the third algebraic term $A \cdot (B \lhd A)$ does. These three algebraic terms are hence not disjoint. This expression for $Q1$ can be transformed into another equivalent expression containing disjoint terms only by introducing B in the two first algebraic terms.

The first algebraic term $C_a \cdot (A \lhd C_a)$ corresponds to the failure sequence $[A, C_a]$, which does not depend on B. B can fail before A (sequence $[B, A, C_a]$), between A and C (sequence $[A, B, C_a]$), after C (sequence

$[A, C_a, B]$), or B may not fail at all (sequence $\left[A, C_a, \not{B}\right]$ [2]). The algebraic term $C_a \cdot (A \lhd C_a)$ is hence equivalent to

$$\begin{aligned} C_a \cdot (A \lhd C_a) &= C_a \cdot (B \lhd A) \cdot (A \lhd C_a) + C_a \cdot (A \lhd B) \cdot (B \lhd C_a) \\ &\quad + B \cdot (A \lhd C_a) \cdot (C_a \lhd B) + C_a \cdot (A \lhd C_a) \cdot \not{B}, \end{aligned}$$

where the four terms represent the four possible sequences obtained by including B in the sequence $[A, C_a]$.

The second algebraic term $A \cdot (C_d \lhd A)$ corresponds to the failure sequence $[C_d, A]$, which does not depend on B either. B can fail before C (sequence $[B, C_d, A]$), between C and A (sequence $[C_d, B, A]$), after A (sequence $[C_d, A, B]$), or B may not fail at all (sequence $\left[C_d, A, \not{B}\right]$). However, if B fails before C, C will become active, which is impossible since C is dormant in the term $A \cdot (C_d \lhd A)$. The algebraic term $A \cdot (C_d \lhd A)$ is hence equivalent to

$$A \cdot (C_d \lhd A) = A \cdot (C_d \lhd B) \cdot (B \lhd A) + B \cdot (C_d \lhd A) \cdot (A \lhd B) + A \cdot (C_d \lhd A) \cdot \not{B},$$

where the three terms represent the three possible sequences obtained by including B in the sequence $[C_d, A]$.

The algebraic model of the gate hence becomes

$$\begin{aligned} Q1 &= C_a \cdot (B \lhd A) \cdot (A \lhd C_a) + C_a \cdot (A \lhd B) \cdot (B \lhd C_a) \\ &\quad + B \cdot (A \lhd C_a) \cdot (C_a \lhd B) + C_a \cdot (A \lhd C_a) \cdot \not{B} \\ &\quad + A \cdot (C_d \lhd B) \cdot (B \lhd A) + B \cdot (C_d \lhd A) \cdot (A \lhd B) \\ &\quad + A \cdot (C_d \lhd A) \cdot \not{B} + A \cdot (B \lhd A) \end{aligned}$$

[2] $\not{B}$ is a symbolic representation of the fact that B does not appear at all.

and can be transformed to

$$\begin{aligned} Q1 \overset{(1)}{=} & A \cdot C_a \cdot (B \lhd A) \cdot (A \lhd C_a) + C_a \cdot (A \lhd B) \cdot (B \lhd C_a) \\ & + B \cdot (A \lhd C_a) \cdot (C_a \lhd B) + C_a \cdot (A \lhd C_a) \cdot \not{B} \\ & + A \cdot (C_d \lhd B) \cdot (B \lhd A) + B \cdot (C_d \lhd A) \cdot (A \lhd B) \\ & + A \cdot (C_d \lhd A) \cdot \not{B} + A \cdot (B \lhd A), \end{aligned}$$

in which the terms $A \cdot C_a \cdot (B \lhd A) \cdot (A \lhd C_a)$ and $A \cdot (C_d \lhd B) \cdot (B \lhd A)$ can be absorbed by the term $A \cdot (B \lhd A)$, thus leading to the following simplified expression

$$\begin{aligned} Q1 = & C_a \cdot (A \lhd B) \cdot (B \lhd C_a) + B \cdot (A \lhd C_a) \cdot (C_a \lhd B) \\ & + C_a \cdot (A \lhd C_a) \cdot \not{B} + B \cdot (C_d \lhd A) \cdot (A \lhd B) \\ & + A \cdot (C_d \lhd A) \cdot \not{B} + A \cdot (B \lhd A). \end{aligned}$$

It can be noted that all the terms of this expression are now disjoint. The failure probability of $Q1$ can hence be expressed as

$$\begin{aligned} Pr\{Q1\}(t) = & Pr\{C_a \cdot (A \lhd B) \cdot (B \lhd C_a)\}(t) \\ & + Pr\{B \cdot (A \lhd C_a) \cdot (C_a \lhd B)\}(t) \\ & + Pr\left\{C_a \cdot (A \lhd C_a) \cdot \not{B}\right\}(t) \\ & + Pr\{B \cdot (C_d \lhd A) \cdot (A \lhd B)\}(t) \\ & + Pr\left\{A \cdot (C_d \lhd A) \cdot \not{B}\right\}(t) + Pr\{A \cdot (B \lhd A)\}(t) \end{aligned}$$

By using the same approach as previously, the six probabilities of the six previous algebraic terms can be expressed under a form which does not

depend on the failure distribution considered for basic events:

$$Pr\left\{C_a \cdot (A \lhd B) \cdot (B \lhd C_a)\right\}(t) = \int_0^t \left(\int_w^t \left(\int_w^u f_B(v)dv \right) f_{C_a}(u,w)du \right) f_A(w)dw$$

$$Pr\left\{B \cdot (A \lhd C_a) \cdot (C_a \lhd B)\right\}(t) = \int_0^t \left(\int_0^u \left(\int_v^u f_{C_a}(w,v)dw \right) f_A(v)dv \right) f_B(u)du$$

$$Pr\left\{C_a \cdot (A \lhd C_a) \cdot \not{B}\right\}(t) = (1 - F_B(t)) \int_0^t \left(\int_v^t f_{C_a}(u,v)du \right) f_A(v)dv$$

$$Pr\left\{B \cdot (C_d \lhd A) \cdot (A \lhd B)\right\}(t) = \int_0^t \left(\int_0^u f_A(v)F_{C_d}(v)dv \right) f_B(u)du$$

$$Pr\left\{A \cdot (C_d \lhd A) \cdot \not{B}\right\}(t) = (1 - F_B(t)) \int_0^t f_A(u)F_{C_d}(u)du$$

$$Pr\left\{A \cdot (B \lhd A)\right\}(t) = \int_0^t f_A(u)F_B(u)du$$

The probabilistic model for $Q1$ can hence be deduced from these expressions, and the probabilistic model for $Q2$ can be determined by symmetry:

$$
\begin{aligned}
F_{Q1}(t) = Pr\{Q1\}(t) &= \int_0^t \left(\int_w^t \left(\int_w^u f_B(v)dv \right) f_{C_a}(u,w)du \right) f_A(w)dw \\
&+ \int_0^t \left(\int_0^u \left(\int_v^u f_{C_a}(w,v)dw \right) f_A(v)dv \right) f_B(u)du \\
&+ (1 - F_B(t)) \int_0^t \left(\int_v^t f_{C_a}(u,v)du \right) f_A(v)dv \\
&+ \int_0^t \left(\int_0^u f_A(v) F_{C_d}(v)dv \right) f_B(u)du \\
&+ (1 - F_B(t)) \int_0^t f_A(u) F_{C_d}(u)du \\
&+ \int_0^t f_A(u) F_B(u)du \\
F_{Q2}(t) = Pr\{Q2\}(t) &= \int_0^t \left(\int_w^t \left(\int_w^u f_A(v)dv \right) f_{C_a}(u,w)du \right) f_B(w)dw \\
&+ \int_0^t \left(\int_0^u \left(\int_v^u f_{C_a}(w,v)dw \right) f_B(v)dv \right) f_A(u)du \\
&+ (1 - F_A(t)) \int_0^t \left(\int_v^t f_{C_a}(u,v)du \right) f_B(v)dv \\
&+ \int_0^t \left(\int_0^u f_B(v) F_{C_d}(v)dv \right) f_A(u)du \\
&+ (1 - F_A(t)) \int_0^t f_B(u) F_{C_d}(u)du \\
&+ \int_0^t f_B(u) F_A(u)du
\end{aligned}
$$

This probabilistic model does not depend on the failure distribution considered for basic events. However, in the particular case of exponential distributions, we have shown in [16] that the expression obtained with this probabilistic model is the same as the expression obtained with Markov Chains.

4.4. Quantitative analysis of DFTs based on the structure function

The knowledge of the minimal canonical form of the structure function, of the probabilistic expressions provided in Section 4.2, and of the probabilistic model of dynamic gates provided in Section 4.3 is sufficient to perform the quantitative analysis of any DFT.

First, an expression for the failure probability of the Top Event of the DFT can be determined thanks to the inclusion-exclusion formula [21]. Indeed, as the structure function is expressed under its minimal canonical form:

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \lhd b_k) \right), j \notin \{i, k\}, \tag{10}$$

the inclusion-exclusion formula will allow to determine an expression for the failure probability of TE under the form:

$$Pr\{TE\}(t) = \sum_{k=1}^{n} (-1)^{k+1} Pr\left\{ \prod b_{i'} \cdot \prod (b_{j'} \lhd b_{k'}) \right\}(t), j' \notin \{i', k'\}, \tag{11}$$

each term $\prod b_{i'} \cdot \prod (b_{j'} \lhd b_{k'})$ being the algebraic product of k terms $\prod b_i \cdot \prod (b_j \lhd b_k)$, n being the number of terms in (10). For instance, if the minimal canonical form of a structure function is

$$TE = b \cdot (a \lhd b) + a \cdot (c \lhd a) + c \cdot (d \lhd c), \tag{12}$$

then the inclusion-exclusion formula will allow to determine $Pr\{TE\}(t)$ under the form:

$$\begin{aligned} Pr\{TE\}(t) \;=\; & Pr\{b \cdot (a \lhd b)\}(t) + Pr\{a \cdot (c \lhd a)\}(t) \\ & + Pr\{c \cdot (d \lhd c)\}(t) - Pr\{b \cdot (c \lhd a) \cdot (a \lhd b)\}(t) \\ & - Pr\{b \cdot c \cdot (a \lhd b) \cdot (d \lhd c)\}(t) - Pr\{a \cdot (d \lhd c) \cdot (c \lhd a)\}(t) \\ & + Pr\{b \cdot (d \lhd c) \cdot (c \lhd a) \cdot (a \lhd b)\}(t) \end{aligned} \tag{13}$$

Each term of the expression in (10) can then be calculated. Two cases can occur:

- if a term does not contain any spare event, the probabilistic expressions presented in Section 4.2 are sufficient to determine its failure probability;
- if a term contains spare events, the interdependence between these spare events and the main event of the corresponding gate must be taken into account: the probabilistic model of Spare gates presented in Section 4.3.3 is hence required to determine the failure probability of this term.

Finally, the failure probability of the *TE* of the DFT can be computed.

5. Quantitative analysis of a DFT example

We propose to perform the quantitative analysis of the DFT example which was considered in [11]. It is extracted from [28] and is depicted in Fig. 8.

This DFT models the failure of a cardiac assist system (HCAS) which is divided into 4 modules: Trigger, CPU unit, motor section, and pumps. The Trigger consists of a crossbar switch (CS) and a system supervisor (SS). The failure of either CS or SS triggers the failure of both CPUs. The CPU unit is a warm spare, which has a primary unit P and a spare unit B having a dormancy of 0.5. The motor section fails if both MOTOR (M) and MOTORC (MC) fail. The pumps unit is comprised of two cold spares, each having a primary pump (P1 and P2), and sharing a common spare pump (BP). In

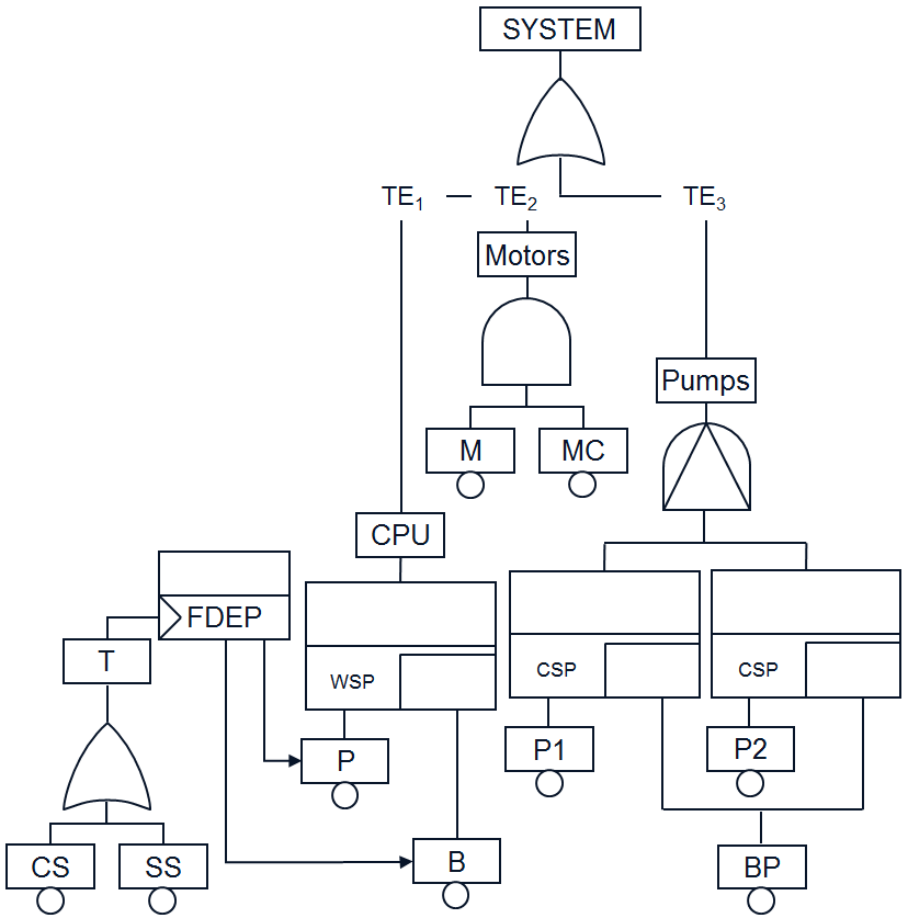


Figure 8: The Dynamic Fault Tree of the HCAS, from [28]

order for the pumps unit to fail, all three pumps need to fail and the left-hand side spare gate needs to fail before (or at the same time as) the right-hand side spare gate, i.e. PAND gate.

The minimal canonical form of the structure function of the DFT in Fig.

8 has been determined in [11] and is

$$\begin{aligned} TE &= CS + SS + MOTOR \cdot MOTORC + P \cdot (B_d \lhd P) + B_a \cdot (P \lhd B_a) \\ &\quad + BP_a \cdot (P2 \lhd P1) \cdot (P1 \lhd BP_a) + P2 \cdot (P1 \lhd BP_a) \cdot (BP_a \lhd P2) \end{aligned}$$

To make the calculation of the failure probability of the TE easier, this structure function can be divided into the 3 structure functions of the 3 subtrees of the DFT of the HCAS which were considered in [11]:

- subtree 1, which corresponds to the failure of the CPU unit: this subtree contains one OR gate, one FDEP gate, and one Warm Spare gate, and is hence dynamic;
- subtree 2, which corresponds to the failure of the motor section: this subtree contains a single AND gate and is hence static;
- subtree 3, which corresponds to the failure of the pumps unit: this subtree contains one PAND gate and two Cold Spare gates, and is hence dynamic.

The TEs of these 3 subtrees are respectively denoted by TE_1, TE_2, and TE_3, and can be determined as [11]:

$$\begin{aligned} TE_1 &= CS + SS + P \cdot (B_d \lhd P) + B_a \cdot (P \lhd B_a) \\ TE_2 &= MOTOR \cdot MOTORC \\ TE_3 &= BP_a \cdot (P2 \lhd P1) \cdot (P1 \lhd BP_a) + P2 \cdot (P1 \lhd BP_a) \cdot (BP_a \lhd P2) \end{aligned}$$

The failure probability of the TE of the DFT can hence be determined

as

$$\begin{aligned} Pr\{TE\}(t) &= Pr\{TE_1 + TE_2 + TE_3\}(t) \\ &= Pr\{TE_1\}(t) + Pr\{TE_2\}(t) + Pr\{TE_3\}(t) \\ &\quad -Pr\{TE_1\}(t) \times Pr\{TE_2\}(t) \\ &\quad -Pr\{TE_1\}(t) \times Pr\{TE_3\}(t) \\ &\quad -Pr\{TE_2\}(t) \times Pr\{TE_3\}(t) \\ &\quad +Pr\{TE_1\}(t) \times Pr\{TE_2\}(t) \times Pr\{TE_3\}(t) \quad (14) \end{aligned}$$

thanks to the inclusion–exclusion formula [21], since the 3 subtrees are statistically independent. The expressions for $Pr\{TE_1\}(t)$, $Pr\{TE_2\}(t)$, and $Pr\{TE_3\}(t)$ can then be determined as follows.

5.1. Calculation of $Pr\{TE_1\}(t)$

$$Pr\{TE_1\}(t) = Pr\{CS + SS + P \cdot (B_d \lhd P) + B_a \cdot (P \lhd B_a)\}(t)$$

According to the probabilistic model of a single Spare gate with 2 input events presented in Section 4.3.3,

$$\begin{aligned} Pr\{P \cdot (B_d \lhd P) + B_a \cdot (P \lhd B_a))\}(t) &= \int_0^t \left(\int_v^t f_{B_a}(u,v)du \right) f_P(v)dv \\ &\quad + \int_0^t f_P(u) F_{B_d}(u)du \end{aligned}$$

As a consequence, according to the inclusion–exclusion formula [21],

$$\begin{aligned} Pr\{TE_1\}(t) &= F_{CS}(t) + F_{SS}(t) - F_{CS}(t) \times F_{SS}(t) \\ &\quad +(1 - F_{CS}(t) - F_{SS}(t) + F_{CS}(t) \times F_{SS}(t)) \\ &\quad \times \left(\int_0^t \left(\int_v^t f_{B_a}(u,v)du \right) f_P(v)dv + \int_0^t f_P(u) F_{B_a}(u)du \right) \end{aligned}$$

5.2. Calculation of $Pr\{TE_2\}(t)$

The expression for $Pr\{TE_2\}(t)$ can be determined directly as

$$\begin{aligned} Pr\{TE_2\}(t) &= Pr\{MOTOR \cdot MOTORC\}(t) \\ &= F_{MOTOR}(t) \times F_{MOTORC}(t) \end{aligned}$$

5.3. Calculation of $Pr\{TE_3\}(t)$

The expression for $Pr\{TE_3\}(t)$ can be determined as

$$\begin{aligned} Pr\{TE_3\}(t) &= Pr\{BP_a \cdot (P2 \lhd P1) \cdot (P1 \lhd BP_a)\}(t) \\ &\quad + Pr\{P2 \cdot (P1 \lhd BP_a) \cdot (BP_a \lhd P2)\}(t) \\ &= \int_0^t \left(\int_w^t \left(\int_w^u f_{P1}(v)dv \right) f_{BP_a}(u,w)du \right) f_{P2}(w)dw \\ &\quad + \int_0^t \left(\int_0^w \left(\int_v^w f_{BP_a}(u,v)du \right) f_{P1}(v)dv \right) f_{P2}(w)dw \end{aligned}$$

thanks to the expression (9) and to the probabilistic model of Spare gates presented in Section 4.3.3.

5.4. Failure probability of the TE of the DFT of the HCAS

The expressions obtained for $Pr\{TE_1\}(t)$, $Pr\{TE_2\}(t)$, and $Pr\{TE_3\}(t)$ allow to determine the failure probability of the *TE* of the DFT of the HCAS thanks to the relation (14). As the expressions obtained in Sections 5.1 to 5.3 are valid whatever the distribution considered for basic events, the failure probability of the *TE* can always be calculated.

In order to compare our results to those obtained with DFT analysis tools, if we consider exponential distributions with the failure rates given in Table 1 and with a dormancy of 0.5 for the spare event B, relation (14)

allows to determine an unreliability of 36.35% for the HCAS at mission time $T = 1,000$ hours. The Galileo tool provides the same result.

However, if the experts consider that a Weibull distribution would be more suitable than an exponential distribution to model the failure behaviour – and the aging – of pumps, $Pr\{TE\}(t)$ can be calculated in the same way. The Weibull distribution has the expression

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{\eta}\right)^{\beta}}$$
$$\lambda(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}}$$

so that

$$F(t) = 1 - e^{-\int_0^t \lambda(u)du}$$

Let us consider that the failure of the three pumps is modeled by a Weibull distribution with a failure rate $\lambda(t) = 1.5 \times 10^{-3} - 4 \times 10^{-7}t$ for $t \in [0, 2500]$, which means that the pumps have an "infant mortality", and a constant failure rate $\lambda = 5 \times 10^{-4}$ after $2,500$ hours. We thus obtain an unreliability of 45.87% for the HCAS at mission time $T = 1,000$ hours. It can be noted that this unreliability is higher – and can be considered as a bit more representative – than the unreliability obtained when the pumps were modeled by exponential distributions.

6. Conclusion

In this paper, we showed that the structure function of DFTs, which already allowed to perform the qualitative analysis of DFTs directly, can also be used to perform the quantitative analysis of DFTs directly thanks to a probabilistic model of dynamic gates. This quantitative analysis can

accommodate any failure distribution for basic events as the probabilistic models that we provided for dynamic gates do not depend on the distribution considered for basic events.

This approach still needs to be implemented, as the underlying calculations allowing to determine the probability of appearance of the *TE* of the DFT are quite important. Besides, numerical integration may be required to take into account non-integrable failure distributions, and calculation algorithms may be useful in the process. Finally, the events that we consider in our approach are non-repairable, which severely limits its applicability since most systems have repairable elements. Extending our algebraic framework to the case of repairable events would hence represent a worthwhile advance, even though it will require the definition of a new model of events, of new behavioral and probabilistic models for dynamic gates, and the theorems that we presented in [11] will need to be updated as some of them may no longer apply to repairable events.

References

[1] Bartlett LM, Du S. New Progressive Variable Ordering for Binary Decision Diagram Analysis of Fault Trees. *Quality and Reliability Engineering International* 2005; **21**(4):413-425. DOI: 10.1002/qre.674

[2] Dugan JB, Sullivan KJ, Coppit D. Developing a low-cost high-quality software tool for Dynamic fault-tree analysis. *IEEE Transactions on Reliability* 2000, **49**(1):49-59. DOI: 10.1109/24.855536

[3] Mo Y, Zhong F, Liu H, Yang Q, Cui G. Efficient Ordering Heuristics in

Binary Decision Diagram-based Fault Tree Analysis. *Quality and Reliability Engineering International*, 2012. DOI: 10.1002/qre.1382

[4] Reay KA, Andrews JD. A fault tree analysis strategy using binary decision diagrams. *Reliability Engineering and System Safety* 2002, **78**(1):45-56. DOI: 10.1016/S0951-8320(02)00107-2

[5] Yang SK, Liu TS. Failure Analysis for an Airbag Inflator by Petri Nets. *Quality and Reliability Engineering International* 1997, **13**(3):139-151.

[6] Lampis M, Andrews JD. Bayesian Belief Networks for System Fault Diagnostics. *Quality and Reliability Engineering International* 2009, **25**(4):409-426. DOI: 10.1002/qre.978

[7] Zafiropoulos EP, Dialynas EN. Methodology for the Optimal Component Selection of Electronic Devices under Reliability and Cost Constraints. *Quality and Reliability Engineering International* 2007, **23**(8):885-897. DOI: 10.1002/qre.850

[8] Sharma RK, Kumar D, Kumar P. Modeling System Behavior for Risk and Reliability Analysis using KBARM. *Quality and Reliability Engineering International* 2007, **23**(8):973-998. DOI: 10.1002/qre.849

[9] Bobbio A, Codetta Raiteri D. Parametric Fault Trees with Dynamic Gates and Repair Boxes. *Proc. of the Annual Reliability and Maintainability Symp.*, Los Angeles, CA, USA, 2004; 459-465.

[10] Ortmeier F, Schellhorn G, Thums A, Reif W, Hering B, Trappschuh H. Safety analysis of the height control system for the Elbtunnel.

Reliability Engineering and System Safety 2003, **81**:(3):259-268. DOI: 10.1016/S0951-8320(03)00090-5

[11] Merle G, Roussel JM, Lesage JJ. Algebraic Determination of the Structure Function of Dynamic Fault Trees. *Reliability Engineering and System Safety* 2011, **96**(2):267-277. DOI: 10.1016/j.ress.2010.10.001

[12] Merle G, Roussel JM, Lesage JJ, Bobbio A. Probabilistic Algebraic Analysis of Fault Trees with Priority Dynamic Gates and Repeated Events. *IEEE Transactions on Reliability* 2010, **59**(1):250-261. DOI: 10.1109/TR.2009.2035793

[13] Merle G, Roussel JM, Lesage JJ. Improving the Efficiency of Dynamic Fault Tree Analysis by Considering Gates FDEP as Static. *Proc. of the ESREL'2010 Conf.*, Rhodes, Greece, 2010; 845-851.

[14] Merle G, Roussel JM, Lesage JJ, Vayatis N. Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates. *Proc. of the ESREL'2010 Conf.*, Rhodes, Greece, 2010; 794-801.

[15] Tang Z, Dugan JB. Minimal cut set/sequence generation for dynamic fault trees. *Proc. of the Annual Reliability and Maintainability Symp.*, Los Angeles, CA, USA, 2004; 207-213.

[16] Merle G. Algebraic modelling of Dynamic Fault Trees, contribution to qualitative and quantitative analysis. PhD thesis, École Normale Supérieure de Cachan, 2010.

[17] Coppit D, Sullivan KJ, Dugan JB. Formal semantics of Models for Computational Engineering: A Case Study on Dynamic Fault Trees. *Proc. of*

the 11th Int. Symp. on Software Reliability Engineering, San Jose, CA, USA, 2000; 270-282.

[18] Montani S, Portinale L, Bobbio A, Varesio M, Codetta-Raiteri D. DB-Net, a tool to convert Dynamic Fault Trees into Dynamic Bayesian Networks. Università del Piemonte Orientale, Technical Report TR-INF-2005-08-02-UNIPMN, 2005.

[19] Vittorini V, Franceschinis G, Gribaudo M, Iacono M, Mazzocca N. Drawnet: Model objects to support performance analysis and simulation of systems. *Proc. of the 12th Int. Conf. on Modelling Tools and Techniques for Computer and Communication System Performance Evaluation*, Springer Verlag - LNCS, **2324**, 2002; 233-238.

[20] Adamyan A, He D. System Failure Analysis Through Counters of Petri Net Models. *Quality and Reliability Engineering International* 2004; **20**(4):317-335. DOI: 10.1002/qre.545

[21] Trivedi K. *Probability & Statistics with Reliability, Queueing & Computer Science applications* (2nd edn). Wiley, 2001.

[22] Dugan JB, Bavuso S, Boyd M. Fault Trees and Sequence Dependencies. *Proc. of the Annual Reliability and Maintainability Symp.*, Los Angeles, CA, USA, 1990; 286-293.

[23] Stamatelatos M., Vesely W. *Fault Tree Handbook with Aerospace Applications*, vol. 1.1. NASA Office of Safety and Mission Assurance, 2002; 205.

[24] Fussell JB, Aber EF, Rahl RG. On the Quantitative Analysis of Priority-AND Failure Logic. *IEEE Transactions on Reliability* 1976, **R-25**(5):324-326. DOI: 10.1109/TR.1976.5220025

[25] Amari S, Dill G, Howals E. A new approach to solve dynamic fault-trees. *Proc. of the Annual Reliability and Maintainability Symp.*, Tampa, FL, USA, 2003; 374-379.

[26] Grimmett GR, Stirzaker DR. *Probability and Random Processes* (3rd edn). Oxford University Press: USA, 2001.

[27] Billingsley P. *Probability and measure*. John Wiley & Sons: New York, USA, 1995.

[28] Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. *Reliability Engineering and System Safety* 2005, **87**(3):337-349. DOI: 10.1016/j.ress.2004.06.004

Algorithme 2: Calculation of the canonical form of a non-basic event

Input : Intermediate or top event (Event), output event of a gate P

Output : Canonical form of the expression for this intermediate or top event (CanonicalForm(Event))

begin

```
// Calculation of the canonical form of the expression
   for each input event of P
for each input event e_i of P do
    CF(e_i) = CanonicalForm(e_i)
// Composition of canonical forms according to the type
   of the gate P
switch type of the gate P do
    case OR
        CF = CF(e_1)
        for each other input event e_i of P do
            CF = ORComposition(CF(e_i),CF)
    case AND
        CF = CF(e_1)
        for each other input event e_i of P do
            CF = ANDComposition(CF(e_i),CF)
    case PAND
        CF = PANDComposition(CF(e_1),CF(e_2))
    case WSP
        CF = WSPComposition(CF(e_1),CF(e_2))
    case CSP
        CF = CSPComposition(CF(e_1),CF(e_2))
return CF
```

Basic component	Failure rate (10^{-4})
CS	1
SS	2
P, B	4
P1, P2, BP	5
MOTOR	5
MOTORC	1

Table 1: Failure rates of the basic events of the DFT of the HCAS