Algebraic Expression of the Structure Function of a subclass of Dynamic Fault Trees

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

HAL Id: hal-00394459
https://hal.science/hal-00394459

Submitted on 11 Jun 2009

Algebraic Expression of the Structure Function of a subclass of Dynamic Fault Trees

Guillaume Merle * **Jean-Marc Roussel** * **Jean-Jacques Lesage** *
Andrea Bobbio **

** LURPA, ENS Cachan, 94235 Cachan Cedex, France (e-mail:
{merle,roussel,lesage}@lurpa.ens-cachan.fr).
** Dipartimento di Informatica, Universita del Piemonte Orientale,
15100 Alessandria, Italy (e-mail: bobbio@mfn.unipmn.it).*

Abstract: This paper focuses on a subclass of Dynamic Fault Trees (DFTs), called Priority
Dynamic Fault Trees (PDFTs), containing only static gates and Priority Dynamic Gates (PAND
and FDEP) for which a priority relation among the input nodes completely determines the
output behavior. We define events as temporal variables and we show that, by adding to the
usual Boolean operators new temporal operators denoted BEFORE and SIMULTANEOUS,
it is possible to derive the structure function of the Top Event with any cascade of Priority
Dynamic Gates and repetition of basic events. A set of theorems are provided to express the
structure function in a sum-of-product canonical form. We finally show through an example
that the canonical form can be exploited in order to determine directly and algebraically the
failure probability of the Top Event of the PDFT without resorting to the corresponding Markov
model. The advantage of this approach is that it provides a complete qualitative description of
the system and that any failure distribution can be accommodated.

Keywords: Dynamic Fault Tree, Algebraic approach, Qualitative analysis, Quantitative
analysis.

1. INTRODUCTION

Fault Tree Analysis (FTA) is one of the oldest and
most diffused techniques in industrial applications, for
the dependability analysis of large safety-critical systems
(Henley and Kumamoto (1981); Stamatelatos and Vesely
(2002)). *FTA* is usually carried out at two levels: a qualita-
tive level in which the list of all the possible combinations
of events that lead to the Top Event (*TE*) is determined
(the *minimal cut sets*). A quantitative level, in which the
probability of occurrence of the *TE*, and of the other nodes
of the tree, is calculated; the quantitative level requires
the additional knowledge of the time-to-failure probability
distributions of all the basic events. One of the main
restrictive assumptions in *FTA* is that basic events must
be assumed as statistically independent (*s*-independent)
and their interaction is described by means of boolean
OR/AND gates, so that only the combination of events
is relevant and not their sequence. We refer to this model
as *Static Fault Tree (SFT)*. Several attempts have been re-
ported in the literature to remove these constraints and in-
clude various kinds of temporal and *s*-dependencies in the
model. A Priority-AND (PAND) gate has been introduced
in (Fussel et al. (1976)) to model situations in which the
failure of the gate occurs if the inputs fail in a preassigned
order. However, the model that has received the greatest
attention is the *Dynamic Fault Tree (DFT)*, proposed by
Dugan et al. (Dugan et al. (1992, 2000)). The DFT is based
on the definition of new gates that induce temporal as well

as *s*-dependencies: Priority-AND (PAND), Functional De-
pendency (FDEP), Warm Spare (WSP) and Sequence en-
forcing (SEQ). Some compositional techniques have been
later envisaged to build DFTs, either in terms of Stochastic
Petri Nets (Bobbio and Raiteri (2004)), or in terms of
Input/Output Interactive Markov Chains (Boudali et al.
(2007)), in order to include chains of dynamic gates. The
quantitative analysis of the DFT consists in exploding
minimal modules (Dutuit and Rauzy (1996)) of dynamic
gates into their state-space representation and computing
numerically the related occurrence probability by means of
a Continuous Time Markov Chain (Dugan et al. (1992)),
thus assuming exponential time-to-failure distributions. A
new approach, able to include any probability distribu-
tion, has been presented in (Amari et al. (2003)), where
closed form expressions are determined as a function of the
generic probability distributions of the basic events, and a
numerical integration is proposed to solve them.

In the present paper, we restrict the consideration of clas-
sical dynamic gates to priority gates PAND and FDEP,
only, for which a temporal relation completely defines the
output, and we refer to this restriction as Priority DFT
(PDFT). In order to build up an algebraic framework for
PDFTs, we define events as temporal binary variables and
we introduce, beside Boolean operators OR and AND,
temporal operators BEFORE (BF) and SIMULTANEOUS
(SM) (Merle and Roussel (2007)). We include the possibil-
ity that basic events are repeated without restriction and
we allow any cascade of Priority Dynamic Gates. We show

that it is possible to provide a complete qualitative description of the PDFT through an algebraic expression of the structure function that can be reduced to a sum-of-product *canonical form*. Each product term of the canonical form contains basic events connected by Boolean and temporal operators. Finally, we show how to compute the probability of occurrence of the *TE* from the canonical form, by assigning to basic events any failure time distribution.

The PDFT model with repeated events is formalized in Section 2, and the new temporal variables and operators are introduced in Section 3. Section 4 shows how to derive the canonical form of the structure function whereas the probabilistic analysis, with a completely developed example, is reported in Section 5.
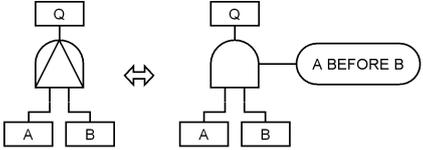
2. PRIORITY DYNAMIC FAULT TREES WITH REPEATED EVENTS

According to (Dugan et al. (2000)), DFTs comprise basic events, static gates (OR, AND and K-out-of-N) and dynamic gates (PAND, FDEP, WSP and SEQ). Dynamic gates can be divided into two categories according to their temporal and statistical behavior:

- gates PAND and FDEP have sequential or preemption-based behaviors and can be modeled by means of discrete mathematics, as presented in Section 3.3.
- Warm Spare (WSP) and Sequence enforcing (SEQ) gates are *s*-dependent on event duration, and their probability of occurrence is not completely defined by an order relation.

We have retained the term of *Priority Dynamic Gates* for gates PAND and FDEP since both gates express a semantics of "priority": a priority between input events for gate PAND; a preemption priority for gate FDEP. *FTs* containing Priority Dynamic Gates are denoted as Priority DFTs (PDFTs) and constitute a subclass of DFTs. The formal definitions of gates PAND and FDEP (Coppit et al. (2000); Stamatelatos and Vesely (2002)) is reminded in Table 1.

Table 1. Definitions of Priority Dynamic Gates

Symbol	Definition
PAND	from (Stamatelatos and Vesely (2002))
FDEP	*Asserts a functional dependency – that the failure of the trigger event causes the immediate and simulta-neous failure of the dependent basic events.* from (Coppit et al. (2000))

In a *FT*, simultaneity among events may arise in two ways. Basic events can occur simultaneously if they have a discrete probability distribution with a non-null probability mass exactly at the same time. Since usually, the

failure probabilities distributions are considered as continuous functions with infinite support, the simultaneous occurrence has null probability and can be neglected.

A second case of simultaneity may arise at any level of a *FT* when there are repeated basic events and has not yet been explored in its full generality.

Let us consider the PDFT in Figure 1, in which event A is a repeated basic event. If basic events A, B, C and
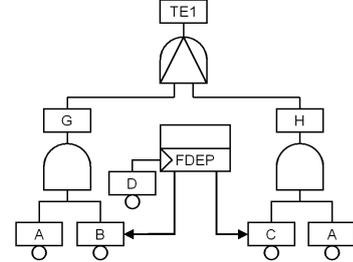

Fig. 1. An example of PDFT with one repeated basic event

D occur according to sequences $[B, C, A]$, $[C, B, A]$ or $[D, A]$, intermediate events G and H occur simultaneously at the same time as A occurs. This example shows that intermediate nodes of a *FT* can occur simultaneously because of the presence of repeated basic events. The simultaneity problem has been briefly addressed in (Boudali et al. (2007)) and has been solved resorting to the concept of "non-determinism", concept that is hardly acceptable in the engineering practice. We assert that a choice must be made regarding the semantics of simultaneous events and priority dynamic gates. For instance, in the case of simultaneous events in input to a PAND gate, two choices are possible (Figure 1):

- if the order relation is considered strictly, when intermediate events G and H occur simultaneously, *TE1* does not occur. Gate PAND would then be considered as being "non-inclusive".
- if the order relation is not considered strictly, when intermediate events G and H occur simultaneously, *TE1* occurs at the same time as G or H. Gate PAND would then be considered as being "inclusive".

Both interpretations of the order relation can be taken into account and algebraically modeled.

3. ALGEBRAIC FORMALIZATION OF PDFTS

3.1 Temporal events

In SFTs, basic events are considered as Booleans. However, the Boolean model cannot render the order of occurrence of events as previously defined for Priority Dynamic Gates. In order to take into account this temporal aspect, we consider the *TE*, the intermediate events and the basic events as *temporal functions*, which are piecewise right-continuous on $\mathbb{R}^+ \cup \{+\infty\}$ and whose range is $\mathbb{B} = \{0,1\}$. Since we consider non-repairable events, only, a generic timing diagram of an event a is given in Figure 2, where $d(a)$ is the unique date of occurrence of a. We denote by $\mathcal{E}_{nr}$ the set of non-repairable events.

The definition of Boolean operators OR and AND can be extended to $\mathcal{E}_{nr}$. The identity elements of these operators

in $\mathcal{E}_{nr}$, equivalent to 0 and 1, are denoted by $\perp$ and $\top$ to which the following dates can be assigned:

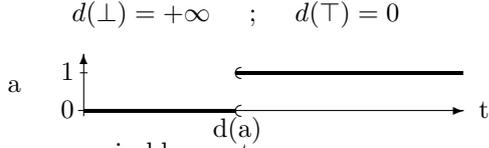$$d(\perp) = +\infty \quad ; \quad d(\top) = 0$$

Fig. 2. A non-repairable event

$(\mathcal{E}_{nr}, +, \cdot, \perp, \top)$ is an Abelian dioid, like $(\{0, 1\}, +, \cdot, 0, 1)$, so that the properties of Boolean algebra that are commonly used for the simplification of SFTs can still be applied with our model, and their structure functions can be determined as usual. A complete description of the algebraic framework developed for temporal events can be found in (Merle et al. (2008)). Because of the notation difference between the identity elements of $\mathcal{E}_{nr}$ and the identity elements of $\{0, 1\}$ for operators $+$ and $\cdot$, the rewriting of four common theorems of Boolean algebra is necessary:

$$a + \perp = a \qquad a \cdot \top = a$$
$$a + \top = \top \qquad a \cdot \perp = \perp$$

3.2 Temporal operators

In order to model priority relations among temporal events, we introduce a temporal operator non-inclusive BEFORE (BF, with symbol $\lhd$) and a temporal operator SIMULTANEOUS (SM, with symbol $\triangle$), whose formal definitions, based on the dates of occurrence of a and b, are as follows:

$$a \lhd b = \begin{cases} a & \text{if } d(a) < d(b) \\ \perp & \text{if } d(a) > d(b) \\ \perp & \text{if } d(a) = d(b) \end{cases}$$

$$a \triangle b = \begin{cases} \perp & \text{if } d(a) < d(b) \\ \perp & \text{if } d(a) > d(b) \\ a & \text{if } d(a) = d(b) \end{cases}$$

Based on the previous two operators, we can introduce a non-strict or INCLUSIVE BEFORE (IBF, with symbol $\trianglelefteq$) operator:

$$a \trianglelefteq b = a \lhd b + a \triangle b \qquad (1)$$

whose definition based on the dates of occurrence of a and b is:

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

Operator $\triangle$ is commutative, while $\lhd$ and $\trianglelefteq$ are not. These three operators satisfy the following theorems, which will be used later in the paper (A more complete set of theorems and their proofs can be found in (Merle et al. (2008))).

$$(a \trianglelefteq b) + b = a + b \qquad (2)$$
$$a \cdot (a \trianglelefteq b) = a \trianglelefteq b \qquad (3)$$
$$a \trianglelefteq (b \cdot c) = (a \trianglelefteq b) + (a \trianglelefteq c) \qquad (4)$$
$$a \trianglelefteq (b \trianglelefteq c) = (a \lhd b) + (a \cdot b \cdot (c \lhd b)) + (a \triangle b) \cdot (b \trianglelefteq c) \qquad (5)$$

$$(a \cdot b) \trianglelefteq c = (a \trianglelefteq c) \cdot (b \trianglelefteq c) \qquad (6)$$
$$(a \trianglelefteq b) \trianglelefteq c = (a \trianglelefteq b) \cdot (a \trianglelefteq c) \qquad (7)$$
$$(a \trianglelefteq b) \cdot (b \trianglelefteq c) \cdot (a \trianglelefteq c) = (a \trianglelefteq b) \cdot (b \trianglelefteq c) \qquad (8)$$
$$a \lhd a = \perp \qquad (9)$$
$$a \cdot (a \lhd b) = a \lhd b \qquad (10)$$
$$(a \trianglelefteq b) \cdot (b \lhd a) = \perp \qquad (11)$$

3.3 Algebraic model of Priority Dynamic Gates

In Section 2, we have shown how both a strict and a non-strict order relation can be taken into account and algebraically modeled. However, a non-strict inclusive interpretation of priority dynamic gates seems more coherent with the designers' expectations. For this reason, in the remainder of this paper, we define an algebraic model of gates PAND and FDEP by means of operator IBF ($\trianglelefteq$), only.

$$Q = (A \cdot B) \cdot (A \trianglelefteq B) \qquad A_T = (A \trianglelefteq T) + T \overset{(2)}{=} A + T$$
$$\overset{(3)}{=} B \cdot (A \trianglelefteq B) \qquad B_T = (B \trianglelefteq T) + T \overset{(2)}{=} B + T$$

(a) \hspace{3cm} (b)

Fig. 3. Algebraic models of gates PAND and FDEP

The algebraic expression of gate PAND is in Figure 3.a, whereas the expression for gate FDEP is in Figure 3.b. Regarding gate FDEP, basic events A and B can fail by themselves or are forced to fail by the trigger event T. We choose to denote the global behavior of basic events A and B by the substituted variables A_T and B_T to explicitly indicate the effect of trigger T. As already noticed in (Stamatelatos and Vesely (2002)), the algebraic formalization proves that gate FDEP can be represented by Boolean OR gates, only.

Furthermore, we assume that basic events are s-independent and have a continuous failure time distribution so that they cannot occur simultaneously. Hence, for any two basic events A and B with the above characteristics, the following relation holds:

$$A \triangle B = \perp \qquad (12)$$

In order to arrive to the determination of the structure function of any PDFT, special attention should be payed to the cascades of PAND gates.

3.4 Cascading PAND gates

Two elementary combinations of cascading PAND gates are possible, as represented in Figures 4.a and 4.b, respectively.

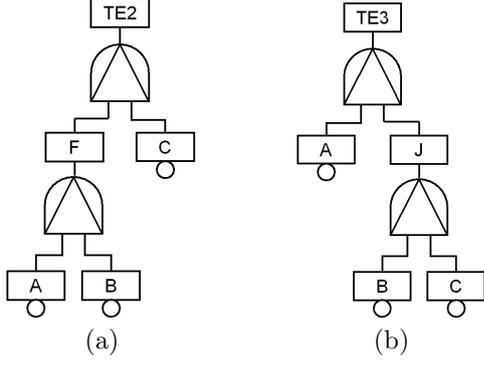The structure function of the PDFT in Figure 4.a can be written as:

Fig. 4. Basic PDFTs made of a cascade of PAND gates

$$
\begin{aligned}
TE2 &= C \cdot (F \trianglelefteq C) \\
&= C \cdot ((B \cdot (A \trianglelefteq B)) \trianglelefteq C) \\
&\overset{(6),(7)}{=} C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq B) \cdot (A \trianglelefteq C) \\
&\overset{(8)}{=} C \cdot (A \trianglelefteq B) \cdot (B \trianglelefteq C) \quad (13)
\end{aligned}
$$

The second possible combination of cascading PAND gates is given in Figure 4.b and its structure function can be determined and developed thanks to the theorems of Section 3.2. Note, in particular, that theorem (5) is somewhat counterintuitive, but simply states that $a \trianglelefteq (b \trianglelefteq c)$ is true iff $(a \triangleleft b)$ or if $(b \trianglelefteq c) = \bot$ is true.

$$
\begin{aligned}
TE3 &= J \cdot (A \trianglelefteq J) \\
&= C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq (C \cdot (B \trianglelefteq C))) \\
&\overset{(4)}{=} C \cdot (B \trianglelefteq C) \cdot ((A \trianglelefteq C) + (A \trianglelefteq (B \trianglelefteq C))) \\
&= C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq C) \\
&\quad + C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq (B \trianglelefteq C)) \\
&\overset{(5)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) + C \cdot (B \trianglelefteq C) \cdot (A \triangleleft B) \\
&\quad + C \cdot (B \trianglelefteq C) \cdot (A \cdot B \cdot (C \triangleleft B)) \\
&\quad + C \cdot (B \trianglelefteq C) \cdot (A \vartriangle B) \cdot (B \trianglelefteq C) \\
&\overset{(12)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) + C \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \\
&\quad + A \cdot B \cdot C \cdot (B \trianglelefteq C) \cdot (C \triangleleft B) \\
&\overset{(11)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) \\
&\quad + C \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \quad (14)
\end{aligned}
$$

4. CANONICAL FORM OF THE STRUCTURE FUNCTION

The algebraic models of Priority Dynamic Gates (Figures 3.a and 3.b) allow us to determine the structure function of any PDFT as a function of basic events that can be repeated without restrictions.

Given a PDFT with n basic events $\{b_i, i \in (1, ..., n)\}$, the structure function for the TE becomes an expression containing at most the n basic events and operators $+$, $\cdot$, $\triangleleft$, $\vartriangle$ and $\trianglelefteq$. The structure function can then be developed and simplified thanks to the theorems presented in Section 3.2, to arrive to a standardized sum-of-product *canonical form* where each product term contains operator $\cdot$ and

ordered pairs of variables linked by operator $\triangleleft$, only. The steps to be followed to arrive to the *canonical form* are:

(1) Starting from the TE, in a top down fashion, replace each FDEP gate by its algebraic expression in Figure 3.b and each PAND gate by its algebraic expression in Figure 3.a.
(2) In the case of cascading PAND gates, apply theorems (5) and (7).
(3) Eliminate the parenthesis by applying distributivity theorems, such as theorems (4) to (7).
(4) The structure function is then expressed in a sum of product terms as in (15):

$$
TE = \sum \left(\prod b_i \cdot \prod \left(b_j \trianglelefteq b_k \right) \cdot \prod \left(b_l \triangleleft b_m \right) \cdot \prod \left(b_o \vartriangle b_p \right) \right) \tag{15}
$$

(5) Since b_o and b_p are basic events, in virtue of theorem (12), function (15) can always be simplified to the following form:

$$
TE = \sum \left(\prod b_i \cdot \prod \left(b_j \trianglelefteq b_k \right) \cdot \prod \left(b_l \triangleleft b_m \right) \right) \tag{16}
$$

(6) Taking into account theorems (1) and (12), we can write $b_j \trianglelefteq b_k = b_j \triangleleft b_k$. Hence the expression in (16) becomes:

$$
TE = \sum \left(\prod b_i \cdot \prod \left(b_j \triangleleft b_k \right) \right)
$$

(7) According to theorem (9), $j = k \Rightarrow b_j \triangleleft b_k = \bot$, then the structure function can be simplified to:

$$
TE = \sum \left(\prod b_i \cdot \prod \left(b_j \triangleleft b_k \right) \right), j \neq k
$$

(8) Finally, according to theorem (10), $i = j \Rightarrow b_i \cdot (b_j \triangleleft b_k) = b_j \triangleleft b_k$, so we get the structure function in *canonical form*:

$$
TE = \sum \left(\prod b_i \cdot \prod \left(b_j \triangleleft b_k \right) \right), j \notin \{i, k\} \tag{17}
$$

5. PROBABILISTIC ANALYSIS OF PDFTS

In the case of DFTs, the determination of the failure probability of the TE from the failure probabilities of the basic events is computed numerically by developing dynamic modules into the corresponding Markov chain. Close form expressions for the dynamic gates with any distribution function are given in (Amari et al. (2003)). In this section, we show that the TE probability of any PDFT can be evaluated in a purely algebraic way from the canonical form of the structure function, for any possible time-to-failure distribution of basic events.

The quantitative analysis of PDFTs is illustrated by means of an example taken from (Fussel et al. (1976)). First, the traditional approach consisting in the generation and solution of the Markov chain is applied. Then the algebraic solution with exponential distributions is proposed starting from the canonical form, showing that the same procedure can be extended to any probability distribution (the Erlang distribution is considered as an example).

Figure 5 shows the PDFT of a non-repairable electrical supply system that has a principal power supply (P), a parallel spare (S), and a switch (C) that commutes on S when P fails (Fussel et al. (1976)). We assume that the principal power supply and the parallel spare fail with failure rates λ_p and λ_s, respectively, and that the switch fails with failure rate λ_c.
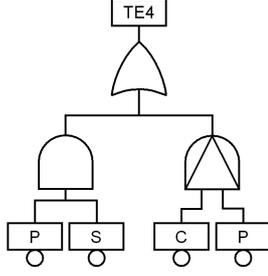
Fig. 5. Example of sample logic model from (Fussel et al. (1976))

5.1 Calculation of the failure probability with Markov chains

The state transition diagram of the corresponding Markov chain is shown in Figure 6, where state 8 is the only failure state and represents the *TE*. The state probabilities of the
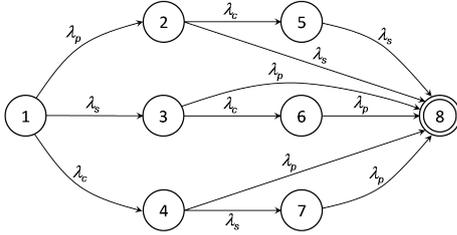

Fig. 6. State transition diagram of the Markov chain for the PDFT shown in Figure 5

Markov chain are obtained by solving the following system of differential equations:

$$\frac{d\boldsymbol{P}(t)}{dt} = \boldsymbol{P}(t) \cdot \boldsymbol{Q} \tag{18}$$

where $\boldsymbol{P}(t)$ is the state probability vector and $\boldsymbol{Q}$ the transition rate matrix given by:

$$
\begin{vmatrix}
-\lambda_p - \lambda_s - \lambda_c & \lambda_p & \lambda_s & \lambda_c & 0 & 0 & 0 & 0 \\
0 & -\lambda_c - \lambda_s & 0 & 0 & \lambda_c & 0 & 0 & \lambda_s \\
0 & 0 & -\lambda_c - \lambda_p & 0 & 0 & \lambda_c & 0 & \lambda_p \\
0 & 0 & 0 & -\lambda_p - \lambda_s & 0 & 0 & \lambda_s & \lambda_p \\
0 & 0 & 0 & 0 & -\lambda_s & 0 & 0 & \lambda_s \\
0 & 0 & 0 & 0 & 0 & -\lambda_p & 0 & \lambda_p \\
0 & 0 & 0 & 0 & 0 & 0 & -\lambda_p & \lambda_p \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{vmatrix} \tag{19}
$$

Solving Equation (18) with transition rate matrix (19) provides the following close form expression for the probability of state 8:

$$Pr\left\{TE4\right\}(t) = Pr\left\{8\right\}(t) = \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p + \lambda_s)t}$$

$$-e^{-\lambda_p t} - \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-\lambda_s t} + 1 \tag{20}$$

5.2 Calculation of the failure probability with the algebraic approach

When the structure function of the *TE* is expressed in canonical form (17), the probability can be calculated starting from the expressions of the product terms. Given

an event x with distribution function $F_x(t)$ and density function $f_x(t)$, the following expressions hold under the hypothesis of *s*-independence by extension of (Amari et al. (2003); Fussel et al. (1976)):

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

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

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

$$Pr\left\{b \cdot (a \lhd b)\right\}(t) = \int_0^t f_b(u)\, F_a(u)\, du \tag{21}$$

The canonical form of the structure function of the PDFT shown in Figure 5 is:

$$
\begin{aligned}
TE4 &= (P \cdot S) + (P \cdot (C \trianglelefteq P)) \\
&\overset{(1),(12)}{=} (P \cdot S) + (P \cdot (C \lhd P))
\end{aligned} \tag{22}
$$

We then calculate $Pr\left\{TE4\right\}$ as:

$$
\begin{aligned}
Pr\left\{TE4\right\} &= Pr\left\{P \cdot S\right\} + Pr\left\{P \cdot (C \lhd P)\right\} \\
&\quad - Pr\left\{(P \cdot S) \cdot (P \cdot (C \lhd P))\right\} \\
&= Pr\left\{P \cdot S\right\} + Pr\left\{P \cdot (C \lhd P)\right\} \\
&\quad - Pr\left\{S \cdot (P \cdot (C \lhd P))\right\} \\
&= Pr\left\{P\right\} \times Pr\left\{S\right\} \\
&\quad + (1 - Pr\left\{S\right\}) \times Pr\left\{P \cdot (C \lhd P)\right\}
\end{aligned} \tag{23}
$$

In the case of exponential distributions, we obtain from (21):

$$Pr\left\{P\right\}(t) = 1 - e^{-\lambda_p t} \qquad Pr\left\{S\right\}(t) = 1 - e^{-\lambda_s t}$$

$$Pr\left\{P \cdot (C \lhd P)\right\}(t) = \int_0^t \lambda_p e^{-\lambda_p u}(1 - e^{-\lambda_c u})\, du$$

$$= \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p)t} - e^{-\lambda_p t} + \frac{\lambda_c}{\lambda_c + \lambda_p}$$

Hence:

$$Pr\left\{TE4\right\}(t) = \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p + \lambda_s)t}$$

$$-e^{-\lambda_p t} - \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-\lambda_s t} + 1 \tag{24}$$

The result in (24) coincides with the one in (20). However, structure function (22) is suited to evaluate the *TE* probability with any distribution.

5.3 Case of non-exponential distributions

If the components of the studied systems do not exhibit an exponential behavior, application of the Markov chain procedure is unfeasible, whereas algebraic manipulation remains a viable solution.

In the case of mechanical systems, for instance, exponential distribution is not the most suitable one and other distributions, such as the Erlang distribution, are more

commonly used. We show that the failure probability of such systems can be determined algebraically by resorting to the expressions (21). The Erlang distribution has the expression shown in Equation (25).

$$F(t) = 1 - \sum_{n=0}^{k-1} \frac{(\lambda t)^n}{n!} e^{-\lambda t} \qquad f(t) = \frac{\lambda^k t^{k-1} e^{-\lambda t}}{(k-1)!} \quad (25)$$

Starting from the *TE* probability expression in (23) we obtain:

$$Pr\{P\}(t) = 1 - \sum_{n=0}^{k_p-1} \frac{(\lambda_p t)^n}{n!} e^{-\lambda_p t}$$

$$Pr\{S\}(t) = 1 - \sum_{n=0}^{k_s-1} \frac{(\lambda_s t)^n}{n!} e^{-\lambda_s t}$$

$$Pr\{P \cdot (C \lhd P)\}(t)$$
$$= \int_0^t \frac{\lambda_p^{k_p} u^{k_p-1} e^{-\lambda_p u}}{(k_p-1)!} \left(1 - \sum_{n=0}^{k_c-1} \frac{(\lambda_c u)^n}{n!} e^{-\lambda_c u}\right) du$$
$$= 1 - \sum_{n=0}^{k_p-1} \frac{(\lambda_p t)^n}{n!} e^{-\lambda_p t}$$
$$- \sum_{n=0}^{k_c-1} \binom{n+k_p-1}{k_p-1} \frac{\lambda_c^n \lambda_p^{k_p}}{(\lambda_c+\lambda_p)^{n+k_p}}$$
$$- \sum_{n=0}^{k_c-1} \sum_{q=0}^{n+k_p-1} \binom{n+k_p-1}{k_p-1} \frac{\lambda_c^n \lambda_p^{k_p} t^q e^{-(\lambda_c+\lambda_p)t}}{q!(\lambda_c+\lambda_p)^{n+k_p-q}}$$

Consequently:

$$Pr\{TE\}(t) = 1 - \sum_{n=0}^{k_p-1} \frac{(\lambda_p t)^n}{n!} e^{-\lambda_p t}$$
$$- \sum_{n=0}^{k_s-1} \sum_{q=0}^{k_c-1} \binom{q+k_p-1}{k_p-1} \frac{\lambda_c^q \lambda_p^{k_p} \lambda_s^n}{n!(\lambda_c+\lambda_p)^{q+k_p}} t^n e^{-\lambda_s t}$$
$$+ \sum_{n=0}^{k_s-1} \sum_{q=0}^{k_c-1} \sum_{r=0}^{q+k_p-1} \binom{q+k_p-1}{k_p-1} \frac{\lambda_c^q \lambda_p^{k_p} \lambda_s^n t^{n+r} e^{-(\lambda_c+\lambda_p+\lambda_s)t}}{n!r!(\lambda_c+\lambda_p)^{q+k_p-r}}$$

The calculation of the failure probability of the *TE* can be performed with any other non-exponential distribution. If the considered failure distribution is not analytically integrable (as for instance the Weibull distribution), the probabilistic relation deducted from the canonical form of the structure function can still be used by resorting to numerical integration.

6. CONCLUSION

In this paper, we have defined a subclass of DFTs, called *Priority Dynamic Fault Trees* (PDFTs), comprising *Priority Dynamic Gates*, PAND and FDEP, only. We have modeled both gates by means of new temporal operators called BF, SM and IBF defined on a set of temporal variables and allowing the simultaneity of intermediate events which can be caused by the use of repeated basic events. The definition of an algebraic model allows the determination of the structure function of any PDFT. Thanks to the theorems that we presented, this structure function can always be simplified to a sum-of-product canonical form, which can then be reduced by removing redundant terms. On the one hand, this canonical form can be used for the qualitative analysis of PDFTs. On the other hand, we presented a quantitative approach allowing the direct algebraic determination of the failure probability of the *TE* from the canonical form, whatever the failure distributions.

On-going work is now addressed to the determination of an algebraic model for WSP and SEQ gates in order to extend the work presented in this paper to the whole DFT formalism.

REFERENCES

Amari, S., Dill, G., and Howals, E. (2003). A new approach to solve dynamic fault-trees. In *Proceedings IEEE Annual Reliability and Maintainability Symposium (RAMS)*, 374–379. Tampa, FL USA.

Bobbio, A. and Raiteri, D.C. (2004). Parametric fault-trees with dynamic gates and repair boxes. In *Proceedings IEEE Annual Reliability and Maintainability Symposium (RAMS)*, 459–465. Los Angeles, CA USA.

Boudali, H., Crouzen, P., and Stoelinga, M. (2007). Dynamic Fault Tree analysis through input/output interactive Markov chains. In *Proceedings International Conference on Dependable Systems and Networks (DSN 2007)*, 25–38. IEEE Computer Society, Edinburgh, UK.

Coppit, D., Sullivan, K.J., and Dugan, J.B. (2000). Formal semantics of models for computational engineering: a case study on dynamic fault trees. In *International Symposium on Software Reliability Engineering (ISSRE'2000)*, 270–282. San Jose, CA USA.

Dugan, J.B., Bavuso, S., and Boyd, M. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability*, 41(3), 363–377.

Dugan, J.B., Sullivan, K., and Coppit, D. (2000). Developing a low-cost high-quality software tool for dynamic fault-tree analysis. *IEEE Transactions on Reliability*, 49(1), 49–59.

Dutuit, Y. and Rauzy, A. (1996). A linear-time algorithm to find modules of fault tree. *IEEE Transactions on Reliability*, 45(3), 422–425.

Fussel, J., Aber, E., and Rahl, R. (1976). On the quantitative analysis of priority-and failure logic. *IEEE Transactions on Reliability*, 25(5), 324–326.

Henley, E. and Kumamoto, H. (1981). *Reliability Engineering and Risk Assessment*. Prentice Hall. 568 p.

Merle, G. and Roussel, J.M. (2007). Algebraic modelling of fault trees with Priority AND gates. In *Proceedings 1st IFAC Workshop on Dependable Control of Discrete Systems (DCDS'07)*, 175–180. Cachan, France.

Merle, G., Roussel, J.M., and Lesage, J.J. (2008). Algebraic Framework for the Modelling of Priority Dynamic Fault Trees. Internal report: http://www.lurpa.ens-cachan.fr/isa/aadft/documents/LURPA-2008-Framework.pdf.

Stamatelatos, M. and Vesely, W. (2002). Fault tree handbook with aerospace applications. volume 1.1, 1–205. NASA Office of Safety and Mission Assurance.