



Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events

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

► To cite this version:

Guillaume Merle, Jean-Marc Roussel, Jean-Jacques Lesage, Andrea Bobbio. Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events. *IEEE Transactions on Reliability*, 2010, 59 (1), pp. 250-261. 10.1109/TR.2009.2035793 . hal-00480014

HAL Id: hal-00480014

<https://hal.science/hal-00480014>

Submitted on 3 May 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events

Guillaume Merle, *Student Member, IEEE*, Jean-Marc Roussel, Jean-Jacques Lesage, *Member, IEEE*,
and Andrea Bobbio, *Senior Member, IEEE*

Abstract—This paper focuses on a sub-class of Dynamic Fault Trees (DFTs), called Priority Dynamic Fault Trees (PDFTs), containing only static gates, and Priority Dynamic Gates (Priority-AND, and Functional Dependency) 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, where each product represents a set of cut sequences for the system. We finally show through some examples that the canonical form can be exploited to determine directly and algebraically the failure probability of the Top Event of the PDDFT without resorting to the corresponding Markov model. The advantage of the approach is that it provides a complete qualitative description of the system, and that any failure distribution can be accommodated.

Index Terms—Algebraic approach, cut sequence sets, dynamic fault tree, qualitative analysis.

ACRONYM

BF	non-inclusive BEFORE operator
DFT	dynamic fault tree
FDEP	functional dependency gate
FTA	fault tree analysis
IBF	inclusive BEFORE operator
PAND	Priority-AND gate
PDFT	priority dynamic fault tree
SEQ	sequence enforcing gate
SFT	static fault tree
SM	SIMULTANEOUS operator
WSP	warm spare gate

NOTATION

\mathcal{E}_{nr}	set of temporal non-repairable events
--------------------	---------------------------------------

\triangleleft	non-inclusive BEFORE (BF) operator
\triangle	SIMULTANEOUS (SM) operator
\trianglelefteq	inclusive BEFORE (IBF) operator
\perp	identity element of operator OR in \mathcal{E}_{nr}
\top	identity element of operator AND in \mathcal{E}_{nr}
CSS	cut sequence set
\mathbb{S}	union of cut sequence sets
\setminus	set difference

I. INTRODUCTION

FAULT TREE ANALYSIS (FTA) is one of the oldest, most diffused techniques in industrial applications, for the dependability analysis of large safety-critical systems [13], [14], [19]. FTA is usually carried out at two levels: a qualitative 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*); and a quantitative level in which the probability of the 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 to be *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 reported in the literature to remove these constraints, and include various kinds of temporal and *s*-dependencies in the model. A Priority-AND (PAND) gate has been introduced in [11] 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.* [8], [9]. The DFT is based on the definition of new gates that induce temporal, as well as *s*-dependencies: Priority-AND (PAND), Functional Dependency (FDEP), Warm Spare (WSP), and Sequence enforcing (SEQ). Some compositional techniques have been later envisaged to build DFTs, either in terms of Stochastic Petri Nets [2], [6], or in terms of Input/Output Interactive Markov Chains [3], [4], to include chains of dynamic gates. The quantitative analysis of the DFT consists in exploding minimal modules [10] of dynamic gates into their state-space representation, and computing numerically the related occurrence probability by means of a Continuous Time Markov Chain [8], [12], thus assuming exponential time-to-failure distributions. In a recent paper [22], authors propose the exact computation of the TE of a FT with PAND gates and repeated events. However, the

Manuscript received November 17, 2008; revised June 28, 2009; accepted July 09, 2009. First published December 28, 2009; current version published March 03, 2010. Associate Editor: K. Suyama.

G. Merle, J.-M. Roussel, and J.-J. Lesage are with the LURPA, École Normale Supérieure de Cachan, Cachan, 94230, France (email: merle@lurpa.ens-cachan.fr; roussel@lurpa.ens-cachan.fr; lesage@lurpa.ens-cachan.fr).

A. Bobbio is with the Dipartimento di Informatica, Università del Piemonte Orientale, Alessandria, 15100, Italy (email: bobbio@mfn.unipmn.it).

Digital Object Identifier 10.1109/TR.2009.2035793

approach requires that the list of the minimal cut sequences is known, and is limited to exponential distributions only.

A new approach, able to include any probability distribution, has been presented in [1], 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 any case, the solution of a DFT forces a quantitative analysis. A common obstacle in any quantitative technique is the lack of accurate, reliable data on the failure distribution of the components. To overcome this well-known deficiency, the qualitative analysis is often the only valuable information on the system dependability. Nevertheless, the qualitative analysis of DFTs has never been fully considered in the literature, and the concept of minimal cut set needs to be revisited to account for the possible order of the failure events. Paper [20] proposes to decompose the qualitative analysis into a logical (Boolean) part, and into a timing part, but the procedure is not completely developed.

In the present paper, we restrict the consideration of classical 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). Priority relations among events impose that events are not repairable. To build 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) [16]. We include the possibility 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, and defines a *cut sequence set* (CSS), i.e. a set of sequences of (possibly ordered) basic events whose occurrence entails the *TE*. We give an algorithm to minimize the canonical form.


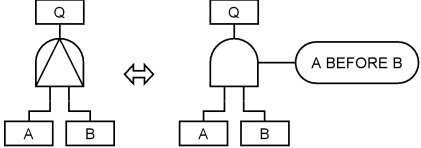

Finally, we show how to compute the probability of occurrence of the *TE* from the canonical form, by assigning to basic events any failure time distribution.

Hence, in synthesis, the main hypotheses, and the new achievements of the paper, can be condensed into the following points.

- i* - We introduce a new algebraic framework with temporal operators defined on a set of temporal variables.
- ii* - The PDFT may contain any cascade of Priority Dynamic Gates PAND, and FDEP; and basic events can be repeated without restriction.
- iii* - Combining Boolean operators (OR, AND) with temporal operators BF and SM, the algebraic expression of the *TE* can always be minimized to a sum-of-product canonical form.
- iv* - The canonical form provides a systematic way to generate a list of non-redundant CSSs whose occurrence leads to the *TE*.
- v* - The probability of occurrence of the *TE* can be expressed in closed form with any failure distribution.

The PDFT model with repeated events is formalized in

TABLE I: Definitions of Priority Dynamic Gates

Symbol	Definition
	 <p style="text-align: center;">from [19]</p>
	<p><i>Asserts a functional dependency – that the failure of the trigger event causes the immediate and simultaneous failure of the dependent basic events.</i></p> <p style="text-align: center;">from [7]</p>

Section II, and the new temporal variables and operators are introduced in Section III. Section IV shows how to derive the canonical form of the structure function; whereas the probabilistic analysis, with completely developed examples, is reported in Section V.

II. PRIORITY DYNAMIC FAULT TREES WITH REPEATED EVENTS

According to [9], 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 III-C; and
- 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 because both gates express a semantics of "priority":

- a priority between input events for gate PAND; and
- a preemption priority for gate FDEP.

FTs containing Priority Dynamic Gates are denoted as Priority DFTs (PDFTs), and constitute a sub-class of DFTs. The formal definition of gates PAND, and FDEP [7], [19] is reminded in Table I.

A. Simultaneity

In a *FT*, simultaneity among events may arise in two ways. Independent basic events can occur simultaneously if they have a discrete probability distribution with a non-null probability mass exactly at the same time. Because the failure probability distributions are usually 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. *FTs* with repeated events represent the

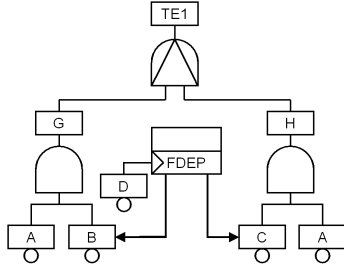


Fig. 1: An example of PDFT with one repeated basic event.

most powerful combinatorial model in dependability [15], and require ad hoc analysis techniques.

Nevertheless, the presence of repeated events across modules of dynamic gates has not yet been explored in its full generality. In [22], repeated events are allowed, but the paper does not provide any algorithm to derive the list of the cut sequences.

Let us consider the PDFT in Fig. 1, in which event A is a repeated basic event. If basic events A , B , C , and 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 [3], and has been solved by resorting to the concept of "non-determinism", a concept that is not easy to accept in engineering practice because many engineers believe that the behavior of technical systems, and in particular control systems, must necessarily be deterministic. 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 (Fig. 1):

- if the order relation is considered strictly, when intermediate events G and H occur simultaneously, $TE1$ does not occur, and gate PAND would then be considered as being "non-inclusive"; and
- 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 , and gate PAND would then be considered as being "inclusive".

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

III. ALGEBRAIC FORMALIZATION OF PRIORITY DFTS

A. Temporal Events

In SFTs, basic events are considered as Boolean. However, the Boolean model cannot render the order of occurrence of events as previously defined for Priority Dynamic Gates. 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 $\mathbb{B} = \{0,1\}$. Because we consider non-repairable events only, a generic timing diagram of an event a

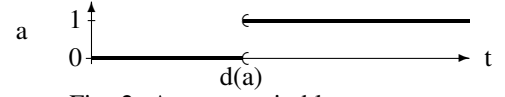


Fig. 2: A non-repairable event.

is given in Fig. 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 these dates can be assigned:

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

$(\mathcal{E}_{nr}, +, \cdot, \perp, \top)$ is an Abelian dooid, 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 [17]. 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:

$$\begin{aligned} a + \perp &= a & a \cdot \top &= a \\ a + \top &= \top & a \cdot \perp &= \perp \end{aligned}$$

B. Temporal Operators

To model priority relations among temporal events, we introduce a temporal operator non-inclusive BEFORE (BF, with symbol \triangleleft), and a temporal operator SIMULTANEOUS (SM, with symbol \triangle), whose formal definitions, based on the dates of occurrence of a and b , are

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

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

$$a \trianglelefteq b = a \triangleleft b + a \triangle b \quad (1)$$

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

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

The expected behavior of the composition of two events a and b by operator IBF is illustrated by the timing diagrams in Fig. 3 in three cases: Case 1: $d(a) < d(b)$, Case 2: $d(a) = d(b)$, Case 3: $d(a) > d(b)$. According to these timing diagrams, and to (1), $a \trianglelefteq b$ occurs in two cases: when a occurs strictly before b , Case 1 (which corresponds to $a \triangleleft b$); and when

a occurs at the same time as b , Case 2 (which corresponds to $a \triangle b$).

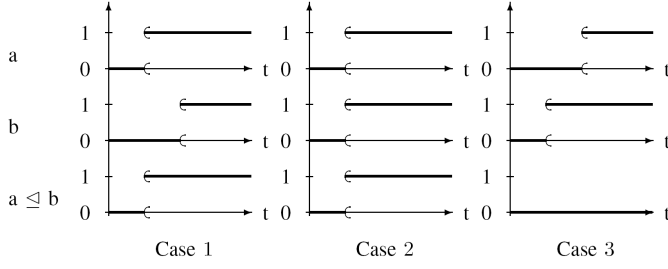


Fig. 3: Expected behavior for operator INCLUSIVE BEFORE (IBF).

Operator \triangle is commutative, while \triangleleft 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 [17]), for any non-repairable events a , b , and c .

$$a \trianglelefteq a = a \quad (2)$$

$$a + (a \trianglelefteq b) = a \quad (3)$$

$$(a \trianglelefteq b) + b = a + b \quad (4)$$

$$a \cdot (a \trianglelefteq b) = a \trianglelefteq b \quad (5)$$

$$a \trianglelefteq (b + c) = (a \trianglelefteq b) \cdot (a \trianglelefteq c) \quad (6)$$

$$a \trianglelefteq (b \cdot c) = (a \trianglelefteq b) + (a \trianglelefteq c) \quad (7)$$

$$a \trianglelefteq (b \trianglelefteq c) = (a \triangleleft b) + (a \cdot b \cdot (c \triangleleft b)) + (a \triangle b) \cdot (b \trianglelefteq c) \quad (8)$$

$$(a + b) \trianglelefteq c = (a \trianglelefteq c) + (b \trianglelefteq c) \quad (9)$$

$$(a \cdot b) \trianglelefteq c = (a \trianglelefteq c) \cdot (b \trianglelefteq c) \quad (10)$$

$$(a \trianglelefteq b) \trianglelefteq c = (a \trianglelefteq b) \cdot (a \trianglelefteq c) \quad (11)$$

$$(a \trianglelefteq b) \cdot (b \trianglelefteq c) \cdot (a \trianglelefteq c) = (a \trianglelefteq b) \cdot (b \trianglelefteq c) \quad (12)$$

$$a \triangleleft a = \perp \quad (13)$$

$$a \cdot (a \triangleleft b) = a \triangleleft b \quad (14)$$

$$a \triangleleft (b + c) = (a \triangleleft b) \cdot (a \triangleleft c) \quad (15)$$

$$(a \cdot b) \triangleleft c = (a \triangleleft c) \cdot (b \triangleleft c) \quad (16)$$

$$(a \triangleleft b) \cdot (b \triangleleft a) = \perp \quad (17)$$

$$(a \trianglelefteq b) \cdot (b \triangleleft a) = \perp \quad (18)$$

$$(a \triangleleft b) \cdot (b \triangleleft c) \cdot (a \triangleleft c) = (a \triangleleft b) \cdot (b \triangleleft c) \quad (19)$$

C. Algebraic Model of Priority Dynamic Gates

In Section II, 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.

The algebraic expression of gate PAND is in Fig. 4, whereas the expression for gate FDEP is in Fig. 5. Regarding gate FDEP, basic events A and B can fail by themselves, or are

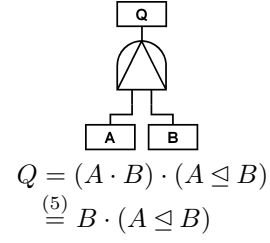
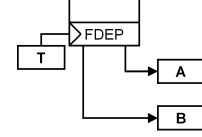


Fig. 4: Algebraic model of gate PAND.



$$A_T = (A \trianglelefteq T) + T \stackrel{(4)}{=} A + T$$

$$B_T = (B \trianglelefteq T) + T \stackrel{(4)}{=} B + T$$

Fig. 5: Algebraic model of gate FDEP.

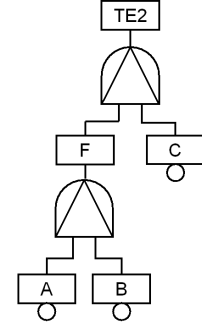


Fig. 6: A basic PDFT made of a cascade of PAND gates.

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 [19], 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.

$$a \triangle b = \perp \quad (20)$$

To arrive to the determination of the structure function of any PDFT, special attention should be paid to the cascades of PAND gates.

D. Cascading PAND Gates

Two elementary combinations of cascading PAND gates are possible, as represented in Figs. 6, and 7.

The structure function of the PDFT in Fig. 6 can be written

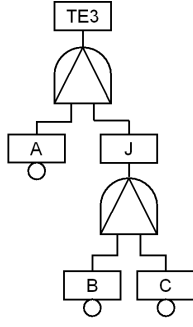


Fig. 7: Another basic PDFT made of a cascade of PAND gates.

as

$$\begin{aligned}
 TE2 &= C \cdot (F \trianglelefteq C) \\
 &= C \cdot ((B \cdot (A \trianglelefteq B)) \trianglelefteq C) \\
 &\stackrel{(10)}{=} C \cdot (B \trianglelefteq C) \cdot ((A \trianglelefteq B) \trianglelefteq C) \\
 &\stackrel{(11)}{=} C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq B) \cdot (A \trianglelefteq C) \\
 &= C \cdot (A \trianglelefteq B) \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq C) \\
 &\stackrel{(12)}{=} C \cdot (A \trianglelefteq B) \cdot (B \trianglelefteq C). \tag{21}
 \end{aligned}$$

Note that the last expression (21) contains the cut sequences of the PDFT in Fig. 6, i.e. indicates the order in which the failures of the basic components should appear to lead to the TE .

The second possible combination of cascading PAND gates is given in Fig. 7, and its structure function can be developed thanks to the theorems of Section III-B. Note, in particular, that theorem (8) is somewhat counterintuitive, but simply states that $a \trianglelefteq (b \trianglelefteq c)$ is true iff $(a \triangleleft b)$, or if $(b \trianglelefteq c) = \perp$ is true.

$$\begin{aligned}
 TE3 &= J \cdot (A \trianglelefteq J) \\
 &= C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq (C \cdot (B \trianglelefteq C))) \\
 &\stackrel{(7)}{=} C \cdot (B \trianglelefteq C) \cdot ((A \trianglelefteq C) + (A \trianglelefteq (B \trianglelefteq C))) \\
 &= C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq C) \\
 &\quad + C \cdot (B \trianglelefteq C) \cdot (A \trianglelefteq (B \trianglelefteq C)) \\
 &\stackrel{(8)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) + C \cdot (B \trianglelefteq C) \cdot (A \triangleleft B) \\
 &\quad + C \cdot (B \trianglelefteq C) \cdot (A \cdot B \cdot (C \triangleleft B)) \\
 &\quad + C \cdot (B \trianglelefteq C) \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \\
 &\stackrel{(20)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) + C \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \\
 &\quad + A \cdot B \cdot C \cdot (B \trianglelefteq C) \cdot (C \triangleleft B) \\
 &\stackrel{(18)}{=} C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) + C \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \tag{22}
 \end{aligned}$$

The two product terms in the last expression (22) contain the cut sequences (ordered sequences of failures) that verify the TE of the PDFT in Fig. 7.

IV. STRUCTURE FUNCTION, AND MINIMAL CANONICAL FORM

A. Canonical Form of the Structure Function

The algebraic models of Priority Dynamic Gates (Figs. 4 and 5), and of the cascades of PAND gates (Section III-D), 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 $\{b_i, i \in (1, \dots, n)\}$, the structure function for the TE becomes an expression containing at most the n basic events, and operators $+$, \cdot , \triangleleft , \trianglelefteq , and \trianglelefteq . The structure function can then be developed and simplified, thanks to the theorems presented in Section III-B, 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 Fig. 5, and each PAND gate by its algebraic expression in Fig. 4.
- 2) In the case of cascading PAND gates, apply theorems (8), and (11).
- 3) Eliminate the parenthesis by applying distributivity theorems, such as theorems (6) to (11), and (15) to (16).
- 4) The structure function is then expressed in a sum of product terms as in (23):

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \trianglelefteq b_k) \cdot \prod (b_l \triangleleft b_m) \cdot \prod (b_o \trianglelefteq b_p) \right). \tag{23}$$

- 5) Because b_o and b_p are basic events, in virtue of theorem (20), (23) can always be simplified to the form

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \trianglelefteq b_k) \cdot \prod (b_l \triangleleft b_m) \right). \tag{24}$$

- 6) Taking into account theorems (1) and (20), we can write $b_j \trianglelefteq b_k = b_j \triangleleft b_k$. Hence, the expression in (24) becomes

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

- 7) According to theorem (13), $j = k \Rightarrow b_j \triangleleft b_k = \perp$, then the structure function can be simplified to

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

- 8) Finally, according to theorem (14), $i = j \Rightarrow b_i \cdot (b_j \triangleleft b_k) = b_j \triangleleft b_k$, so we get the structure function in *canonical form*

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \triangleleft b_k) \right), j \notin \{i, k\}. \tag{25}$$

B. Minimization of the Canonical Form of the Structure Function

In the case of SFTs, a minimal form of the structure function can be determined easily thanks to the theorems of Boolean algebra, or by resorting to BDDs [18], [19]. Such minimal form provides the minimal cut sets of the SFT. In the case of DFTs, the concept of minimal cut must be refined to *minimal cut sequence* [20], representing the minimal (ordered) failure sequence of events that causes the occurrence of the TE . The exhaustive search of the minimal cut sequences of a DFT is an open problem, in the general case. The algebraic approach for PDFTs provides a sound theoretical basis for the determination of the $CSSs$.

In the canonical form of the structure function given in (25), each product term $\prod b_i \cdot \prod (b_j \triangleleft b_k)$ is not a single cut sequence, but an algebraic expression providing a sufficient condition on the order of basic event failures that leads to the TE which may contain more than one cut sequence, and actually is a *cut sequence set* (CSS). In the remainder of this paper, CSS_i will represent both a set of cut sequences (like in (27)), and the algebraic expression that characterizes this set of cut sequences (like in (26)).

Given that there are n product terms in (25), the canonical form can be rewritten in the compact form

$$TE = \sum_{i=1}^n CSS_i. \quad (26)$$

The set \mathbb{S} of all the cut sequences of the PDFT is the union of all the $CSSs$ previously defined:

$$\mathbb{S} = \bigcup_{i=1}^n CSS_i. \quad (27)$$

Nevertheless, a CSS may be included in one or more $CSSs$. CSS_i is included in one of the CSS_j if it satisfies the criterion [18]

$$CSS_i \cdot \sum_{j \neq i} CSS_j = CSS_i. \quad (28)$$

If CSS_i is included in one of the CSS_j , it is redundant, and can be removed from the structure function (26). Iterative application of the criterion (28), according to Algorithm 1, removes all the redundant $CSSs$, and returns the minimal set \mathbb{S}_{min} of non-redundant $CSSs$.

Algorithm 1 Algorithm for the minimization of the canonical form of the structure function of a PDFT

Require: \mathbb{S}

$\mathbb{S}_{min} \leftarrow \mathbb{S}$

for $i = 1$ to n **do**

$CSS \leftarrow \sum_{j \neq i} CSS_j$

if $CSS_i \cdot CSS = CSS_i$ **then**

$\mathbb{S}_{min} \leftarrow \mathbb{S}_{min} \setminus \{CSS_i\}$

end if

end for

return \mathbb{S}_{min}

Given that \mathbb{S}_{min} contains ($m \leq n$) cut sequence sets, the minimal canonical form of the structure function can be expressed as

$$TE = \sum_{i=1}^m CSS_i. \quad (29)$$

C. Examples

1) *Determination of the Canonical Form of the Structure Function of the PDFT in Fig. 1:* Let us consider the PDFT shown in Fig. 1. The derivation of the canonical form of its structure function proceeds along the following steps, where B_D and C_D include the effect of trigger D (Fig. 5).

$$\begin{aligned} TE1 &= H \cdot (G \leq H) \\ &= (A \cdot C_D) \cdot ((A \cdot B_D) \leq (A \cdot C_D)) \\ &= (A \cdot (C + D)) \\ &\quad \cdot ((A \cdot (B + D)) \leq (A \cdot (C + D))) \\ &\stackrel{(10)}{=} A \cdot (C + D) \cdot (A \leq (A \cdot (C + D))) \\ &\quad \cdot ((B + D) \leq (A \cdot (C + D))) \\ &\stackrel{(7)}{=} A \cdot (C + D) \cdot ((A \leq A) + (A \leq (C + D))) \\ &\quad \cdot ((B + D) \leq (A \cdot (C + D))) \\ &\stackrel{(2),(3)}{=} A \cdot (C + D) \cdot A \cdot ((B + D) \leq (A \cdot (C + D))) \\ &\stackrel{(7)}{=} A \cdot (C + D) \cdot (((B + D) \leq A) \\ &\quad + ((B + D) \leq (C + D))) \\ &\stackrel{(9)}{=} A \cdot (C + D) \cdot ((B \leq A) + (D \leq A) \\ &\quad + (B \leq (C + D)) + (D \leq (C + D))) \\ &\stackrel{(6)}{=} A \cdot (C + D) \cdot ((B \leq A) + (D \leq A) \\ &\quad + (B \leq C) \cdot (B \leq D) + (D \leq C) \cdot (D \leq D)) \\ &\stackrel{(2),(5)}{=} A \cdot (C + D) \cdot ((B \leq A) + (D \leq A) \\ &\quad + (B \leq C) \cdot (B \leq D) + (D \leq C)) \\ &= A \cdot C \cdot (B \leq A) + A \cdot C \cdot (D \leq A) \\ &\quad + A \cdot C \cdot (B \leq C) \cdot (B \leq D) + A \cdot C \cdot (D \leq C) \\ &\quad + A \cdot D \cdot (B \leq A) + A \cdot D \cdot (D \leq A) \\ &\quad + A \cdot D \cdot (B \leq C) \cdot (B \leq D) + A \cdot D \cdot (D \leq C) \\ &\stackrel{(5)}{=} A \cdot C \cdot (B \leq A) + A \cdot C \cdot (D \leq A) \\ &\quad + A \cdot C \cdot (B \leq C) \cdot (B \leq D) + A \cdot C \cdot (D \leq C) \\ &\quad + A \cdot D \cdot (B \leq A) + A \cdot D \cdot (D \leq A) \\ &\quad + A \cdot D \cdot (B \leq C) \cdot (B \leq D) + A \cdot D \cdot (D \leq C) \\ &\stackrel{(1),(20)}{=} A \cdot (D \triangleleft A) + A \cdot (D \triangleleft C) + A \cdot C \cdot (B \triangleleft A) \\ &\quad + A \cdot D \cdot (B \triangleleft A) + A \cdot C \cdot (B \triangleleft C) \cdot (B \triangleleft D) \\ &\quad + A \cdot D \cdot (B \triangleleft C) \cdot (B \triangleleft D) \end{aligned} \quad (30)$$

The last expression (30) is the canonical form of the structure function of the PDFT in Fig. 1.

2) *Determination of the Cut Sequences of the PDFT in Fig. 7:* Let us consider the PDFT shown in Fig. 7. The canonical form of its structure function can be determined

easily starting from (22):

$$\begin{aligned}
 TE3 &= C \cdot (A \trianglelefteq C) \cdot (B \trianglelefteq C) \\
 &\quad + C \cdot (A \triangleleft B) \cdot (B \trianglelefteq C) \\
 &\stackrel{(1),(20)}{=} C \cdot (A \triangleleft C) \cdot (B \triangleleft C) \\
 &\quad + C \cdot (A \triangleleft B) \cdot (B \triangleleft C). \quad (31)
 \end{aligned}$$

This structure function is composed by two cut sequence sets $CSS_1 = C \cdot (A \triangleleft C) \cdot (B \triangleleft C)$, and $CSS_2 = C \cdot (A \triangleleft B) \cdot (B \triangleleft C)$. Algorithm 1 allows us to check whether one of these CSS s is included in the other one, according to criterion (28), and to remove it from the structure function.

We start Algorithm 1 with $\mathbb{S} = CSS_1 \cup CSS_2$:

For $i = 1$, $CSS = CSS_2$. Consequently,

$$\begin{aligned}
 CSS_1 \cdot CSS &= CSS_1 \cdot CSS_2 \\
 &= C \cdot (A \triangleleft C) \cdot (B \triangleleft C) \\
 &\quad \cdot C \cdot (A \triangleleft B) \cdot (B \triangleleft C) \\
 &= C \cdot (A \triangleleft B) \cdot (B \triangleleft C) \cdot (A \triangleleft C) \\
 &\stackrel{(19)}{=} C \cdot (A \triangleleft B) \cdot (B \triangleleft C).
 \end{aligned}$$

Because $CSS_1 \cdot CSS \neq CSS_1$, CSS_1 is not included in CSS .

For $i = 2$, $CSS = CSS_1$. Consequently,

$$\begin{aligned}
 CSS_2 \cdot CSS &= CSS_2 \cdot CSS_1 \\
 &= C \cdot (A \triangleleft B) \cdot (B \triangleleft C) \\
 &\quad \cdot C \cdot (A \triangleleft C) \cdot (B \triangleleft C) \\
 &= C \cdot (A \triangleleft B) \cdot (B \triangleleft C) \cdot (A \triangleleft C) \\
 &\stackrel{(19)}{=} C \cdot (A \triangleleft B) \cdot (B \triangleleft C).
 \end{aligned}$$

Because $CSS_2 \cdot CSS = CSS_2$, CSS_2 is included in CSS , and can be removed. As a result of the minimization algorithm, \mathbb{S}_{min} contains a single element

$$\mathbb{S}_{min} = \{CSS_1\} = \{C \cdot (A \triangleleft C) \cdot (B \triangleleft C)\}.$$

The minimal canonical form of the structure function of the PDFT finally is

$$TE3 = C \cdot (A \triangleleft C) \cdot (B \triangleleft C). \quad (32)$$

The PDFT shown in Fig. 7 contains 3 basic events: A , B , and C . Neither single occurrences of these basic events, nor sequences of 2 of them, can engender the TE , but the occurrence of the 3 basic events is needed. They can occur in 6 different sequences: $[A, B, C]$, $[A, C, B]$, $[B, A, C]$, $[B, C, A]$, $[C, A, B]$, and $[C, B, A]$. The cut sequences of the PDFT are the sequences of basic events A , B , and C which verify (32), and hence engender the TE . There are only 2 such sequences among the 6 possible:

$$[A, B, C], \text{ and } [B, A, C]. \quad (33)$$

It is easy to check that the only sequence that satisfies CSS_2 is $[A, B, C]$, which is included in (33), making CSS_2 a redundant term.

3) *Cascading PAND Gates With Repeated Events*: Fig. 8 shows a PDFT example taken from [5] with cascading PAND gates. The procedure to arrive to the canonical form of the structure function is developed step by step. To make the analysis more straightforward, we arrest the development at intermediate events Q , S , and T , because they do not have basic events in common, and are thus s -independent.

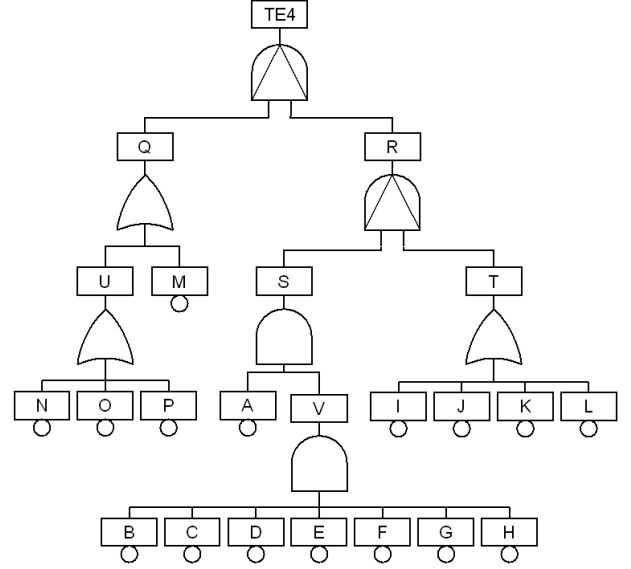


Fig. 8: An example of PDFT from [5].

$$\begin{aligned}
 TE4 &= R \cdot (Q \trianglelefteq R) \\
 &= T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq (T \cdot (S \trianglelefteq T))) \\
 &\stackrel{(7)}{=} T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq T) \\
 &\quad + T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq (S \trianglelefteq T))
 \end{aligned}$$

Because we can write

$$Q \trianglelefteq (S \trianglelefteq T) \stackrel{(8)}{=} Q \triangleleft S + Q \cdot S \cdot (T \triangleleft S) + (Q \triangleleft S) \cdot (S \trianglelefteq T),$$

the derivation of the canonical form may proceed in the following way.

$$\begin{aligned}
 TE4 &= T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq T) + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S) \\
 &\quad + T \cdot (S \trianglelefteq T) \cdot Q \cdot S \cdot (T \triangleleft S) \\
 &\quad + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S) \cdot (S \trianglelefteq T) \\
 &\stackrel{(18)}{=} T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq T) + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S) \\
 &\quad + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S)
 \end{aligned}$$

Simultaneity between Q , S , and T is excluded because they do not have basic events in common. Hence, $Q \triangleleft S = \perp$, $S \trianglelefteq T = S \triangleleft T$, and $Q \trianglelefteq T = Q \triangleleft T$.

$$TE4 = T \cdot (S \triangleleft T) \cdot (Q \triangleleft T) + T \cdot (S \triangleleft T) \cdot (Q \triangleleft S) \quad (34)$$

The result in (34) is the same as in (31) with $(Q, S, T) \equiv (A, B, C)$, so the structure function can be simplified to the form (32) that provides the minimal canonical form of the structure function of the system (35):

$$TE4 = T \cdot (S \triangleleft T) \cdot (Q \triangleleft T). \quad (35)$$

Let us now consider a case, not considered in [5], in which event A in Fig. 8 is a repeated basic event. In particular, we assume that $M \equiv A$, so that Q , and S are no longer s -independent because they share a common basic event. In this case, the structure function can be derived through the steps in this next equation set.

$$\begin{aligned} TE4_{M \equiv A} &= T \cdot (S \trianglelefteq T) \cdot (Q \trianglelefteq T) \\ &\quad + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S) \\ &\quad + T \cdot (S \trianglelefteq T) \cdot (Q \triangleleft S) \\ &= T \cdot ((A \cdot V) \trianglelefteq T) \cdot ((A + U) \trianglelefteq T) \\ &\quad + T \cdot ((A \cdot V) \trianglelefteq T) \cdot ((A + U) \triangleleft (A \cdot V)) \\ &\quad + T \cdot ((A \cdot V) \trianglelefteq T) \cdot ((A + U) \triangleleft (A \cdot V)) \\ &\stackrel{(10)}{=} T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \cdot ((A + U) \trianglelefteq T) \\ &\quad + T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \\ &\quad \cdot ((A + U) \triangleleft (A \cdot V)) + T \cdot (A \trianglelefteq T) \\ &\quad \cdot (V \trianglelefteq T) \cdot ((A + U) \triangleleft (A \cdot V)) \\ &\stackrel{(9)}{=} T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \cdot (A \trianglelefteq T) \\ &\quad + T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \cdot (U \trianglelefteq T) \\ &\quad + T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \\ &\quad \cdot ((A + U) \triangleleft (A \cdot V)) + T \cdot (A \trianglelefteq T) \\ &\quad \cdot (V \trianglelefteq T) \cdot ((A + U) \triangleleft (A \cdot V)) \\ &= T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \\ &\quad + T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \cdot (U \trianglelefteq T) \\ &\quad + T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \\ &\quad \cdot ((A + U) \triangleleft (A \cdot V)) + T \cdot (A \trianglelefteq T) \\ &\quad \cdot (V \trianglelefteq T) \cdot ((A + U) \triangleleft (A \cdot V)) \\ &= T \cdot (A \trianglelefteq T) \cdot (V \trianglelefteq T) \\ &\stackrel{(1),(20)}{=} T \cdot (A \triangleleft T) \cdot (V \triangleleft T) \end{aligned} \quad (36)$$

Note that, in the final expression (36), intermediate event U does no longer appear because it is absorbed due to the repetition of event A . This result, which is not evident from the inspection of Fig. 8, can be obtained thanks to the algebraic treatment.

V. 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 determined numerically by developing dynamic modules into the corresponding Markov chain [12]. Close form expressions for the dynamic gates with any distribution function are given in [1]. In this section, we show that the TE probability of any PDFT can be evaluated in a purely algebraic way from the minimal canonical form, for any possible time-to-failure distribution of basic events.

Given that the minimal canonical form (29) has m CSSs, we can compute the probability of the TE by resorting to the standard inclusion-exclusion formula [21]:

$$\begin{aligned} Pr\{TE\} &= Pr\{CSS_1 + CSS_2 + \dots + CSS_m\} \\ &= \sum_{1 \leq i \leq m} Pr\{CSS_i\} \\ &\quad - \sum_{1 \leq i < j \leq m} Pr\{CSS_i \cdot CSS_j\} \\ &\quad + \sum_{1 \leq i < j < k \leq m} Pr\{CSS_i \cdot CSS_j \cdot CSS_k\} + \dots \\ &\quad + (-1)^{m-1} Pr\{CSS_1 \cdot CSS_2 \cdot \dots \cdot CSS_m\} \end{aligned} \quad (37)$$

with $\forall i \in \{1, \dots, m\}, CSS_i \in \mathbb{S}_{min}$.

Each term of these sums contains the product of the algebraic expressions verified by the CSSs that can share the same basic events, and thus are not s -independent. However, in these product terms, some simplifications might be possible in two cases:

- if a basic component b_i or a term $(b_i \triangleleft b_j)$ appear in two or more CSSs, we can apply the idempotence theorem $b_i \cdot b_i = b_i$ or $(b_i \triangleleft b_j) \cdot (b_i \triangleleft b_j) = (b_i \triangleleft b_j)$; and
- if CSS_ℓ contains the term b_i , and CSS'_ℓ the term $(b_i \triangleleft b_j)$, by virtue of (14), $b_i \cdot (b_i \triangleleft b_j) = (b_i \triangleleft b_j)$.

As soon as the simplification of the different terms has been performed, their failure probabilities can be calculated. Given an event x with Cdf $F_x(t)$, and pdf $f_x(t)$, the following expressions hold under the hypothesis of s -independence [1], [11].

$$\begin{aligned} Pr\{a \cdot b\}(t) &= F_a(t) \times F_b(t) \\ Pr\{a + b\}(t) &= F_a(t) + F_b(t) - F_a(t) \times F_b(t) \\ Pr\{a \triangleleft b\}(t) &= \int_0^t f_a(u)(1 - F_b(u)) du \\ Pr\{b \cdot (a \triangleleft b)\}(t) &= \int_0^t f_b(u) F_a(u) du \end{aligned} \quad (38)$$

Of course, expression (37) may contain much more complex terms. To give a flavor of the way to arrive to a close form expression with any distribution, consider a term like $S' = (A \triangleleft B) \cdot (B \triangleleft C)$ that contains 3 basic events A , B , and C that are s -dependent through a chain of BF operators. The cut sequences that verify this expression can be determined. Single occurrences of A , B , and C cannot engender S' . Recall the 6 sequences of 2 basic events $[A, B]$, $[A, C]$, $[B, A]$, $[B, C]$, $[C, A]$, and $[C, B]$. Among them, $[A, B]$ is the only sequence that leads to the occurrence of S' . Finally, recall the 6 sequences of 3 basic events $[A, B, C]$, $[A, C, B]$, $[B, A, C]$, $[B, C, A]$, $[C, A, B]$, and $[C, B, A]$. Among them, $[A, B, C]$ is the only sequence that leads to the occurrence of S' . S' has only 2 cut sequences:

$$[A, B], \text{ and } [A, B, C].$$

$$Q = \begin{bmatrix} -\lambda_p - \lambda_s - \lambda_c & \lambda_p & \lambda_s & \lambda_c & 0 & 0 & 0 & 0 \\ 0 & -\lambda_c - \lambda_s & 0 & 0 & \lambda_c & 0 & 0 & \lambda_s \\ 0 & 0 & -\lambda_c - \lambda_p & 0 & 0 & \lambda_c & 0 & \lambda_p \\ 0 & 0 & 0 & -\lambda_p - \lambda_s & 0 & 0 & \lambda_s & \lambda_p \\ 0 & 0 & 0 & 0 & -\lambda_s & 0 & 0 & \lambda_s \\ 0 & 0 & 0 & 0 & 0 & -\lambda_p & 0 & \lambda_p \\ 0 & 0 & 0 & 0 & 0 & 0 & -\lambda_p & \lambda_p \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (39)$$

Given both sequences are mutually exclusive ¹,

$$Pr\{S'\} = Pr\{[A, B]\} + Pr\{[A, B, C]\}.$$

The algebraic expression of the probability of each mutually exclusive sequence can be computed for any sequence of states. In the present case,

$$Pr\{[A, B]\}(t) = (1 - F_C(t)) \int_0^t f_B(u) F_A(u) du$$

$$\begin{aligned} Pr\{[A, B, C]\}(t) &= \int_0^t f_C(u) Cdf\{B \cdot (A \triangleleft B)\} du \\ &= \int_0^t f_C(u) \left(\int_0^u f_B(v) F_A(v) dv \right) du. \end{aligned} \quad (40)$$

The probability expression (40) is obtained by a nested application of (38). The sketched method can provide the algebraic expression of any term of (37).

A. Example 1 From [11]

The quantitative analysis of PDFTs is illustrated by means of an example taken from Fussel *et al.* in [11]. 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).

Fig. 9 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 [11]. 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 .

1) *Calculation of the Failure Probability with Markov Chains:* The state transition diagram of the corresponding Markov chain is shown in Fig. 10, where state 8 is the only failure state, and represents the TE. The state probabilities of the Markov chain are obtained by solving the system of differential equations

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t) \cdot \mathbf{Q} \quad (41)$$

¹Note that the sequence $[A, B]$ is a shortened notation for a more correct expression $[A, B, \bar{C}]$.

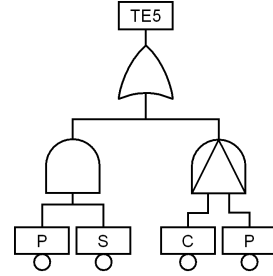


Fig. 9: Example of sample logic model from [11].

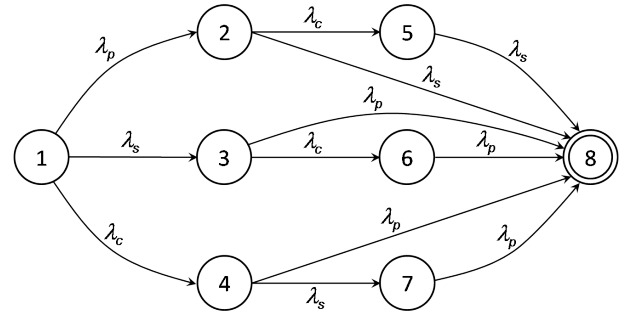


Fig. 10: State transition diagram of the Markov chain for the PDFT shown in Fig. 9.

where $\mathbf{P}(t)$ is the state probability vector, and \mathbf{Q} the transition rate matrix given by (39) shown at the top of the page. Solving (41) with transition rate matrix (39) provides the close form expression for the probability of state 8:

$$\begin{aligned} Pr\{TE5\}(t) &= Pr\{8\}(t) \\ &= \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p + \lambda_s)t} - e^{-\lambda_p t} \\ &\quad - \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-\lambda_s t} + 1. \end{aligned} \quad (42)$$

2) *Calculation of the Failure Probability With the Algebraic Approach:* To apply the algebraic approach, we first determine the minimal canonical form of the structure function of the PDFT in Fig. 9.

$$\begin{aligned} TE5 &= (P \cdot S) + (P \cdot (C \leq P)) \\ &\stackrel{(1),(20)}{=} (P \cdot S) + (P \cdot (C \triangleleft P)) \end{aligned} \quad (43)$$

We then calculate $Pr\{TE5\}$ as

$$\begin{aligned}
Pr\{TE5\} &= Pr\{(P \cdot S) + (P \cdot (C \triangleleft P))\} \\
Pr\{TE5\} &= Pr\{P \cdot S\} + Pr\{P \cdot (C \triangleleft P)\} \\
&\quad - Pr\{(P \cdot S) \cdot (P \cdot (C \triangleleft P))\} \\
Pr\{TE5\} &= Pr\{P \cdot S\} + Pr\{P \cdot (C \triangleleft P)\} \\
&\quad - Pr\{S \cdot (P \cdot (C \triangleleft P))\} \\
Pr\{TE5\} &= Pr\{P\} \times Pr\{S\} + Pr\{P \cdot (C \triangleleft P)\} \\
&\quad - Pr\{S\} \times Pr\{P \cdot (C \triangleleft P)\} \\
Pr\{TE5\} &= Pr\{P\} \times Pr\{S\} + (1 - Pr\{S\}) \\
&\quad \times Pr\{P \cdot (C \triangleleft P)\}. \tag{44}
\end{aligned}$$

In the case of exponential distributions, we obtain from (38) that

$$\begin{aligned}
Pr\{P\}(t) &= 1 - e^{-\lambda_p t} \quad Pr\{S\}(t) = 1 - e^{-\lambda_s t} \\
Pr\{P \cdot (C \triangleleft P)\}(t) &= \int_0^t \lambda_p e^{-\lambda_p u} (1 - e^{-\lambda_c u}) du \\
&= \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p)t} \\
&\quad - e^{-\lambda_p t} + \frac{\lambda_c}{\lambda_c + \lambda_p}.
\end{aligned}$$

Hence,

$$\begin{aligned}
Pr\{TE5\}(t) &= \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-(\lambda_c + \lambda_p + \lambda_s)t} \\
&\quad - e^{-\lambda_p t} - \frac{\lambda_p}{\lambda_c + \lambda_p} e^{-\lambda_s t} + 1. \tag{45}
\end{aligned}$$

The result in (45) coincides with the one in (42). However, minimal canonical form (43) is suited to evaluate the TE probability with any distribution.

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, the 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 (38). The Erlang distribution has the expression

$$\begin{aligned}
F(t) &= 1 - \sum_{n=0}^{k-1} \frac{(\lambda t)^n}{n!} e^{-\lambda t} \\
f(t) &= \frac{\lambda^k t^{k-1} e^{-\lambda t}}{(k-1)!}. \tag{46}
\end{aligned}$$

Starting from the TE probability expression in (44), we obtain

$$\begin{aligned}
Pr\{P\}(t) &= 1 - \sum_{n=0}^{k_p-1} \frac{(\lambda_p t)^n}{n!} e^{-\lambda_p t} \\
Pr\{S\}(t) &= 1 - \sum_{n=0}^{k_s-1} \frac{(\lambda_s t)^n}{n!} e^{-\lambda_s t}
\end{aligned}$$

$$\begin{aligned}
Pr\{P \cdot (C \triangleleft P)\}(t) &= \int_0^t \frac{\lambda_p^k u^{k_p-1} e^{-\lambda_p u}}{(k_p-1)!} \left(1 - \sum_{n=0}^{k_c-1} \frac{(\lambda_c u)^n}{n!} e^{-\lambda_c u}\right) du \\
&= 1 - \sum_{n=0}^{k_p-1} \frac{(\lambda_p t)^n}{n!} e^{-\lambda_p t} \\
&\quad - \sum_{n=0}^{k_c-1} \binom{n+k_p-1}{k_p-1} \frac{\lambda_c^n \lambda_p^{k_p}}{(\lambda_c + \lambda_p)^{n+k_p}} \\
&\quad - \sum_{n=0}^{k_c-1} \sum_{q=0}^{n+k_p-1} \binom{n+k_p-1}{k_p-1} \frac{\lambda_c^n \lambda_p^{k_p} t^q e^{-(\lambda_c + \lambda_p)t}}{q! (\lambda_c + \lambda_p)^{n+k_p-q}}.
\end{aligned}$$

Consequently,

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

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 deduced from the minimal canonical form of the structure function can still be used by resorting to numerical integration.

B. Example 2 From Section IV-C3 [5]

The TE probability of the example in Fig. 8 can be computed via the algebraic approach in both cases of different, repeated components.

When there is no repetition, the canonical form for the TE is given in (35), and thus its probability can be computed as

$$\begin{aligned}
Pr\{TE4\}(t) &= Pr\{T \cdot (S \triangleleft T) \cdot (Q \triangleleft T)\} \\
&\stackrel{(16)}{=} Pr\{T \cdot ((S \cdot Q) \triangleleft T)\} \\
&= \int_0^t f_T(u) \times F_{S \cdot Q}(u) du \\
&= \int_0^t f_T(u) \times F_S(u) \times F_Q(u) du.
\end{aligned}$$

To compare our results with those in [5], we assign to the basic events an exponential distribution with the same failure rates given in Table II. Hence,

$$\begin{aligned}
F_T(t) &= 1 - e^{-(\lambda_I + \lambda_J + \lambda_K + \lambda_L)t} \\
F_S(t) &= \prod_{i \in \{A, \dots, H\}} (1 - e^{-\lambda_i t}) \\
F_Q(t) &= 1 - e^{-(\lambda_M + \lambda_N + \lambda_O + \lambda_P)t}.
\end{aligned}$$

TABLE II: Failure rates of the basic events of the PDFT shown in Fig. 8, from [5]

Basic component	Failure rate
A	0.11
B	0.12
C	0.13
D	0.14
E	0.15
F	0.16
G	0.17
H	0.18
I	0.011
J	0.012
K	0.013
L	0.014
M	0.11
N	0.12
O	0.13
P	0.14

With a mission time equal to $T = 1$, we find a system unreliability of 2.01×10^{-10} , which coincides with the one in [5].

If event A is repeated, the canonical form has been obtained in (36), and its probability is

$$\begin{aligned}
 Pr\{TE4_{M \equiv A}\}(t) &= Pr\{T \cdot (A \triangleleft T) \cdot (V \triangleleft T)\} \\
 &\stackrel{(16)}{=} Pr\{T \cdot ((A \cdot V) \triangleleft T)\} \\
 &= \int_0^t f_T(u) \times F_{A \cdot V}(u) du \\
 &= \int_0^t f_T(u) \times F_A(u) \times F_V(u) du.
 \end{aligned}$$

With the exponential distributions, we have

$$\begin{aligned}
 F_A(t) &= 1 - e^{-\lambda_A t} \\
 F_T(t) &= 1 - e^{-(\lambda_I + \lambda_J + \lambda_K + \lambda_L)t} \\
 F_V(t) &= \prod_{i \in \{B, \dots, H\}} (1 - e^{-\lambda_i t}).
 \end{aligned}$$

With the failure rates of Table II, and a mission time equal to $T = 1$, the system unreliability becomes 5.6×10^{-10} .

The probabilistic analysis of PDFTs can be performed by using our algebraic approach, even in the case of repeated events.

VI. CONCLUSION

In this paper, we have defined a sub-class 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 in the case of non-repairable systems. 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 minimized by removing redundant terms.

On the one hand, this minimal canonical form can be used for the qualitative analysis of PDFTs because it contains all

the non-redundant CSSs whose occurrence leads to the TE . On the other hand, we presented a quantitative approach allowing the direct algebraic determination of the failure probability of the TE from the minimal canonical form, whatever the failure distributions.

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

REFERENCES

- [1] S. Amari, G. Dill, and E. Howals, "A new approach to solve dynamic fault-trees," in *Proceedings of the IEEE Annual Reliability and Maintainability Symposium*, Tampa, FL, USA, 2003, pp. 374-379.
- [2] A. Bobbio and D. Codetta Raiteri, "Parametric Fault-trees with dynamic gates and repair boxes," in *Proceedings of the IEEE Annual Reliability and Maintainability Symposium*, Los Angeles, CA, USA, 2004, pp. 459-465.
- [3] H. Boudali, P. Crouzen and M. Stoelinga, "Dynamic Fault Tree analysis through input/output interactive Markov chains," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2007)*, Edinburgh, UK, 2007, pp. 25-38.
- [4] H. Boudali, P. Crouzen and M. Stoelinga, "A compositional semantics for Dynamic Fault Tree in terms of interactive Markov chains," in *International Symposium on Automated Technology for Verification and Analysis (ATVA'07)*, 2007, vol. 4762, pp. 441-456.
- [5] H. Boudali and J. B. Dugan, "A discrete-time Bayesian network reliability modeling and analysis framework," *Reliability Engineering and System Safety*, vol. 87, no. 3, pp. 337-349, 2005.
- [6] D. Codetta Raiteri, "The Conversion of Dynamic Fault Trees to Stochastic Petri Nets, as a case of Graph Transformation," *Electronic Notes on Theoretical Computer Science*, vol. 127, no. 2, pp. 45-60, 2005.
- [7] D. Coppit, K. J. Sullivan, and J. B. Dugan, "Formal Semantics of Models for Computational Engineering: a Case Study on Dynamic Fault Trees," in *International Symposium on Software Reliability Engineering (ISSRE'2000)*, San Jose, CA, USA, 2000, pp. 270-282.
- [8] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Trans. Reliability*, vol. 41, no. 3, pp. 363-377, 1992.
- [9] J. B. Dugan, K. J. Sullivan, and D. Coppit, "Developing a low-cost high-quality software tool for Dynamic fault-tree analysis," *IEEE Trans. Reliability*, vol. 49, no. 1, pp. 49-59, 2000.
- [10] Y. Dutuit and A. Rauzy, "A linear-time algorithm to find modules of fault tree," *IEEE Trans. Reliability*, vol. 45, no. 3, pp. 422-425, 1996.
- [11] J. B. Fussell, E. F. Aber, and R. G. Rahl, "On the Quantitative Analysis of Priority-AND Failure Logic," *IEEE Trans. Reliability*, vol. 25, no. 5, pp. 324-326, 1976.
- [12] R. Gulati and J. B. Dugan, "A modular approach for analyzing static and dynamic fault-trees," in *Proceedings of the IEEE Annual Reliability and Maintainability Symposium*, Philadelphia, PA, USA, 1997, pp. 57-63.
- [13] E. J. Henley and H. Kumamoto, "Reliability Engineering and Risk Assessment," Englewood Cliffs: Prentice Hall, 1981.
- [14] N. G. Leveson, "Safeware: System Safety and Computers," Addison-Wesley, 1995.
- [15] M. Malhotra and K. Trivedi, "Power-hierarchy among dependability model types," *IEEE Trans. Reliability*, vol. 43, no. 3, pp. 493-502, 1994.
- [16] G. Merle and J. M. Roussel, "Algebraic modelling of fault trees with Priority AND gates," in *Proceedings of the 1st IFAC Workshop on Dependable Control of Discrete Systems (DCDS'07)*, Cachan, France, 2007, pp. 175-180.
- [17] G. Merle, J. M. Roussel, and J. J. Lesage, Algebraic Framework for the Modelling of Priority Dynamic Fault Trees 2008 [Online]. Available: <http://www.lurpa.ens-cachan.fr/isa/aadft/documents/LURPA-2008-Framework.pdf>, Internal report.
- [18] A. Rauzy, "Mathematical Foundations of Minimal Cutsets," *IEEE Trans. Reliability*, vol. 50, no. 4, pp. 389-396, 2001.
- [19] *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, 2002, pp. 1-205.
- [20] Z. Tang and J. B. Dugan, "Minimal cutset/sequence generation for dynamic fault trees," in *Proceedings of the IEEE Annual Reliability and Maintainability Symposium*, Los Angeles, CA, USA, 2004, pp. 207-213.
- [21] K. Trivedi, "Probability & Statistics with Reliability, Queueing & Computer Science applications," Wiley, 2nd ed., 2001.

- [22] T. Yuge and S. Yanagi, "Quantitative analysis of a fault tree with priority AND gates," *Reliability Engineering and System Safety*, vol. 93, no. 11, pp. 1577-1583, 2008.

Guillaume Merle (S'08) received the M.S. degree in Systems Engineering from the École Normale Supérieure de Cachan (France) in 2007. He is a PhD candidate at the LURPA (Automated Production Research Laboratory) of the École Normale Supérieure de Cachan. His main research interests span the area of algebraic methods, with application to performance evaluation, and reliability.

Jean-Marc Roussel received the PhD degree in 1994. He is currently Associate Professor of Automatic Control at the École Normale Supérieure de Cachan (France) and carries out research at the LURPA on the control of Discrete Event Systems with algebraic approaches.

Jean-Jacques Lesage (M'07) received the PhD degree in 1989, and the "Habilitation à Diriger des Recherches" in 1994. He is currently Professor of Automatic Control at the École Normale Supérieure de Cachan (France). His research topics are formal methods and models of Discrete Event Systems (DES), both for modeling synthesis and analysis. The common objective of his works is to increase the dependability of the DES control.

Andrea Bobbio (M'95–SM'03) is professor of Computer Science at the "Dipartimento di Informatica" of Università del Piemonte Orientale (Italy). His main research interests span the area of modeling and analysis of stochastic systems, with application to performance evaluation, and reliability. Bobbio has been visiting researcher in various universities in USA, Hungary, India, and France. He is author of several papers in international journals and conferences, and principal investigator of research projects with public and private institutions.