Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates

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

Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates

Guillaume Merle, Jean-Marc Roussel, and Jean-Jacques Lesage
LURPA, ENS de Cachan, Cachan, France
Nicolas Vayatis
CMLA, ENS de Cachan, Cachan, France

This paper focuses on one of the dynamic gates which are used in Dynamic Fault Trees (DFT): the Spare gate. We provide an algebraic model which allows to determine the structure function of DFTs with Spare gates from which qualitative analysis can be performed directly. We also provide a probabilistic model allowing to determine the failure probability of Spare gates without any restriction on the failure distribution for basic events.

1 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 (Henley and Kumamoto 1981; Leveson 1995; Stamatelatos and Vesely 2002). When the interactions between events can be described by means of boolean OR/AND gates only, so that only the combination of events is relevant, and not their sequence, Fault Trees are called *Static Fault Tree (SFT)*. Dugan et al. (Dugan, Bavuso, and Boyd 1990; Dugan, Sullivan, and Coppit 2000) proposed a new model allowing to include various kinds of temporal and statistical dependencies in the SFT model, which is the *Dynamic Fault Tree (DFT)*. The DFT is based on the definition of new gates: Priority-AND (PAND), Functional Dependency (FDEP), Warm Spare (WSP), and Sequence Enforcing (SEQ).

The first dynamic gate, gate Priority-AND, was introduced in 1976 (Fussel, Aber, and Rahl 1976) to model sequences of failures. Then, gate FDEP was introduced in 1990 (Dugan, Bavuso, and Boyd 1990) to model common cause failures, and the Spare gate was finally introduced in 2002 (Coppit and Sullivan 2002) to model redundancies.

Even though such dynamic gates allow to model failure scenarios that SFTs cannot handle, the analytical techniques commonly used to analyze SFTs cannot be used to analyze DFTs, and other types of techniques, mainly based on state models, must be used.

As stated in (Merle, Roussel, Lesage, and Bobbio 2010), gates PAND and FDEP have sequential or preemption-based behaviors and can easily be modeled by means of discrete mathematics. However, the Spare gate is more complex since statistically dependent on the failure order of events and its probability of occurrence is not completely defined by an order relation.

Many compositional techniques have been envisaged to analyze DFTs with Spare gates, either in terms of Stochastic Petri Nets (Bobbio and Raiteri 2004; Raiteri 2005), or in terms of Input/Output Interactive Markov Chains (Boudali, Crouzen, and Stoelinga 2007). In (Dutuit and Rauzy 1996), the quantitative analysis of the DFT consists in exploding minimal subtrees containing dynamic gates into their state-space representation, and computing numerically the related occurrence probability by means of a Continuous Time Markov Chain (Dugan, Bavuso, and Boyd 1992; Gulati and Dugan 1997), thus assuming exponential time-to-failure distributions. Another approach, based on Temporal Bayesian Networks, is introduced in (Boudali and Dugan 2005) and allows to include any probability distribution. In (Amari, Dill, and Howals 2003), 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 defi-

ciency, 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. The authors of (Tang and Dugan 2004) propose to decompose the qualitative analysis into a logical (Boolean) part, and into a timing part. Dynamic gates are replaced with the static gates which correspond to their logical constraints, the minimal cut sets of the resulting SFT are then generated, and each minimal cut set is expanded to minimal cut sequences by considering timing constraints. However, the procedure is not completely developed.

In previous papers, we presented an algebraic framework allowing to determine the structure function of DFTs with PAND gates (Merle and Roussel 2007) and FDEP gates (Merle, Roussel, Lesage, and Bobbio 2009; Merle, Roussel, Lesage, and Bobbio 2010). We also detailed how to perform the quantitative analysis of such DFTs from their structure function. In this paper, we recall the basics of this algebraic framework and we extend the previous results to the case of Spare gates.

The algebraic framework that we introduce to model Spare gates is presented in Section 2. The algebraic model of Spare gates is introduced in Section 3, and the probabilistic model which can be deduced from it is given in Section 4. Finally, a DFT example allows to highlight the usefulness of both models for the qualitative and quantitative analysis in Section 5.

2 BASICS AND NOTATIONS OF THE ALGEBRAIC FRAMEWORK

This algebraic framework was described in (Merle, Roussel, Lesage, and Bobbio 2010) and has been proposed to render the order of occurrence of events which is necessary for the modeling of dynamic gates. It will not be detailed here, and only the basics and notations needed to understand the remainder of this paper will be explained. To take into account the temporal aspect of events, we consider the top event, the intermediate events, and the basic events as *temporal functions* which are defined on the set of positive times and take Boolean values. As we consider non-repairable events only, a generic timing diagram of an event a is given in Fig. 1, where $d(a)$ is the unique date of occurrence of a. The never-occurring event is denoted by $\perp$.

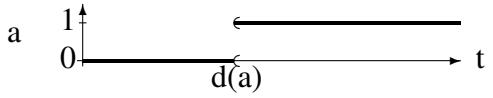

Figure 1: A non-repairable event.

This algebraic framework does not need to explicitly take time into account, since we only need to know the order in which events occur to model dynamic gates. We then defined three temporal operators to model dynamic gates, which are operators non-inclusive BEFORE (noted $\lhd$), SIMULTANEOUS (noted $\triangle$), and Inclusive BEFORE (noted $\trianglelefteq$). Thus, for instance, the algebraic model of the PAND gate in Fig. 2 becomes

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

which expresses that the output Q of the gate fails if A and B fail and if A fails before or at the same time as B.

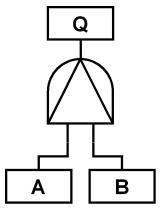

Figure 2: A PAND gate

As the non-inclusive BEFORE operator is sufficient to model Spare gates, it is the only temporal operator that will be retained in the remainder of this paper. Furthermore, we have demonstrated that this algebraic framework allows to determine the structure function of SFTs as it is commonly done by using the classical Boolean algebra of Boolean variables. Besides, the definition of the three temporal operators allows to determine the structure function of any DFT with gates PAND, and FDEP, and some theorems which were provided allows to reduce this structure function to the canonical form in (1), where TE is the Top Event of the DFT and the events b_i are the basic events of the DFT.

$$TE = \sum \left(\prod b_i \cdot \prod (b_j \lhd b_k) \right), j \notin \{i, k\}. \quad (1)$$

3 ALGEBRAIC MODEL OF THE SPARE GATE

Two factors impact the difficulty to model the Spare gate: the number of input events of the Spare gate, and the possibility for many Spare gate to share one or many spare events. This section presents the algebraic model of the Spare gate in an increasing order of complexity. The algebraic model of a single Spare gate with 2 to n input events is presented in Sections 3.1 to 3.3. The particular case of 2 Spare gates with 2 input events sharing a spare event is presented in Section 3.4, and we show how to generalize it to n Spare gates with 2 input events sharing a spare event in Section 3.5.

Besides, we consider that there is only one type of Spare gate, which is the Warm Spare gate, and that

Cold and Hot Spare gates (Stamatelatos and Vesely 2002) are particular cases of Warm Spare gates. Both of them are studied in Section 3.6.

3.1 Algebraic model of a single Spare gate with 2 input events

Let us consider a Spare gate with 2 input events – the primary event A and one spare event B – as shown in Fig. 3. As stated in (Stamatelatos and Vesely 2002),

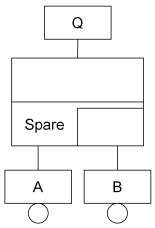

Figure 3: A single Spare gate with one primary event A and one spare event B

the output Q of the gate occurs when the primary and all spares have failed, so when A and B have failed, in this case. A and B are basic events and cannot fail simultaneously (noted $A \triangle B = \perp$) so Q will occur if A and B fail according to sequences $[A, B]$ or $[B, A]$. It is important to note that in sequence $[A, B]$, B fails while in its active mode (denoted as B_a), whereas in sequence $[B, A]$, B fails while in its dormant mode (denoted as B_d). It is essential to distinguish both failure modes by using two different variables, for quantitative analysis purposes. Indeed, B does not have the same failure distribution when it fails during its dormant mode ($B \equiv B_d$) or during its active mode ($B \equiv B_a$). As we aim at making possible the quantitative analysis of DFTs from their structure function, this structure function must hence provide sufficient information to know whether spare events are in their dormant or active mode. The algebraic behavior of gate Spare can hence be expressed as

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

which expresses that the output Q of the gate fails if A fails before B – $B_a \cdot (A \lhd B_a)$, B hence being in its active mode B_a – or if B fails before A – $A \cdot (B_d \lhd A)$, B hence being in its dormant mode B_d.

Furthermore, as B cannot be both in an active state and in a dormant state, we have

$$B_d \cdot B_a = \perp.$$

3.2 Algebraic model of a single Spare gate with 3 input events

Let us consider a Spare gate with 3 input events – the primary event A and two spare events B and C – as shown in Fig. 4.

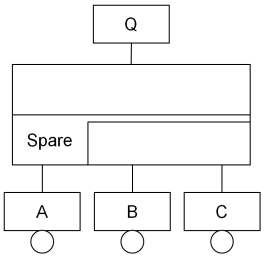

Figure 4: A single Spare gate with one primary event A and two spare events B and C

As stated in (Stamatelatos and Vesely 2002), the output Q of the gate occurs when the primary and all spares have failed, so when A, B, and C have failed. A, B, and C are basic events and cannot fail simultaneously so Q will occur if A, B, and C fail according to sequences $[A, B, C]$, $[A, C, B]$, $[B, A, C]$, $[B, C, A]$, $[C, A, B]$, or $[C, B, A]$. It is important to note that, when the quantitative analysis will be performed from the structure function, B and C will not have the same distribution function in the 6 sequences. For instance, in sequence $[A, B, C]$, both B and C fail during their active mode (denoted by B_a and C_a), whereas in sequence $[B, C, A]$, both B and C fail during their dormant mode (denoted by B_d and C_d). The algebraic behavior of gate Spare can hence be expressed as

$$\begin{aligned} Q \;=\; & C_a \cdot (A \lhd B_a) \cdot (B_a \lhd C_a) \\ & + B_a \cdot (A \lhd C_d) \cdot (C_d \lhd B_a) \\ & + C_a \cdot (B_d \lhd A) \cdot (A \lhd C_a) \\ & + A \cdot (B_d \lhd C_d) \cdot (C_d \lhd A) \\ & + B_a \cdot (C_d \lhd A) \cdot (A \lhd B_a) \\ & + A \cdot (C_d \lhd B_d) \cdot (B_d \lhd A) \end{aligned}$$

As B and C cannot be both in an active state and in a dormant state, we have

$$\begin{cases} B_d \cdot B_a = \perp \\ C_d \cdot C_a = \perp \end{cases}$$

3.3 Algebraic model of a single Spare gate with n input events

The algebraic model of a single Spare gate with n input events can be determined in the same way. It is just necessary to determine the $n!$ possible failure sequences of the input events of the Spare gate and denote the dormant and active mode of the $(n-1)$ spare events in these failure sequences. The algebraic model of the Spare gate will then be the algebraic sum of the expressions for which each failure sequences holds, with the additional condition that each spare

event cannot be both in an active and in a dormant mode.

3.4 Algebraic model of 2 Spare gates with 2 input events sharing a spare event

Let us consider 2 Spare gates with 2 input events – with primary events A and B – sharing a spare event C, as shown in Fig. 5.

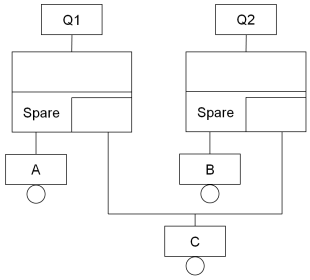

Figure 5: Two Spare gates sharing a spare event C

If we focus on the Spare gate on the left side, $Q1$ occurs as soon as A and C have failed – as stated in Section 3.1 – or if A fails and C is made unavailable because B has failed before A. As a consequence, the algebraic model of the first Spare gate is

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

The algebraic expression for $Q2$ can be determined in the same way by symmetry. Consequently, the final algebraic model of any of two Spare gates sharing a spare event is

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

3.5 Algebraic model of n Spare gates with 2 input events sharing a spare event

Let us consider n Spare gates with 1 output event Q_i and 2 input events: a primary event $P_i - i \in \{1, \cdots, n\}$ – and a spare event S.

If we focus on the first Spare gate, Q_1 will occur as soon as P_1 and S have failed – as stated in Section 3.1 – or if P_1 fails and S is made unavailable because the primary event of any of the other Spare gates has failed before P_1. As a consequence, the algebraic model of the first Spare gate is

$$\begin{cases} Q_1 = S_a \cdot (P_1 \lhd S_a) + P_1 \cdot (S_d \lhd P_1) \\ \qquad + \sum_{i \neq 1} P_1 \cdot (P_i \lhd P_1) \\ S_d \cdot S_a = \bot \end{cases}$$

The algebraic expression for $Q_i, i \in \{1, \ldots, n\}$, can be determined in the same way by symmetry. Consequently, the final algebraic model of any of n Spare gates sharing a spare event is

$$\begin{cases} Q_i = S_a \cdot (P_i \lhd S_a) + P_i \cdot (S_d \lhd P_i) \\ \qquad + \sum_{j \neq i} P_i \cdot (P_j \lhd P_i) \\ S_d \cdot S_a = \bot \end{cases}$$

3.6 Specific case of Cold and Hot Spare gates

The algebraic models presented in Sections 3.1 to 3.5 are the algebraic models of Spare gates in the general case of Warm Spare events. These algebraic models can be simplified in the specific cases of Cold and Hot Spare events:

- if a spare event S is a Cold Spare event, it cannot fail while in a dormant state, so S_d will never occur and any expression containing S_d in the algebraic models can be removed;
- if a spare event S is a Hot Spare event, it will have the same distribution function when in an active and in a dormant state, so $S_a \equiv S_d \equiv S$ and the algebraic models can be simplified.

It can be noted that the algebraic models defined involve the temporal operator which is used to model gates PAND and FDEP, so the expression (1) still holds in the case of a DFT with Spare gates, and the structure function of any DFT can be determined and reduced to the canonical form in (1) as well.

4 PROBABILISTIC MODEL OF THE SPARE GATE

The probabilistic model of the Spare gates can be deduced from their algebraic model presented in Section 3 by determining the failure probability of each failure sequence thanks to the standard inclusion-exclusion formula (Trivedi 2001) and the following expressions (Amari, Dill, and Howals 2003; Fussel, Aber, and Rahl 1976), which hold under the hypothesis of statistical independence:

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

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

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

$$Pr\{b \cdot (a \lhd b)\}(t) = \int_0^t f_b(u)\, F_a(u)\, du \qquad (2)$$

The probabilistic model of a single Spare gate with 2 input events is presented in Section 4.1 whereas the probabilistic model of 2 Spare gates with 2 input events sharing a spare event is presented in Section 4.2.

4.1 Probabilistic model of a single Spare gate with 2 input events

According to Section 3.1, the algebraic model of a single Spare gate with 2 input events is

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

On the one hand, the cumulative distribution function (Cdf) and probability density function (pdf) of B_d do not depend on A, so $Pr\{A \cdot (B_d \lhd A)\}(t)$ can be determined by means of the expressions (2) as

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

On the other hand, the Cdf and pdf of B_a depend on the failure date of A, so $Pr\{B_a \cdot (A \lhd B_a)\}(t)$ cannot be determined by means of the expressions (2). If we respectively denote by T_A and T_{B_a} the failure dates of A and B_a, $Pr\{B_a \cdot (A \lhd B_a)\}(t)$ can be defined as

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

where $\mathbb{1}$ is the *indicator function* and E is the *expectation value* such that

$$E[\mathbb{1}_A] = Pr\{A\}$$

According to the *law of total expectation* (Billingsley 1995), if X is an integrable random variable and if Y is any random variable, not necessarily integrable, on the same probability space, then

$$E[X] = E[E[X|Y]]$$

As a consequence,

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

The probabilistic model of a single Spare gate with 2 input events hence is

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

The probabilistic model of a single Spare gate with 3 or even n input events can be determined in the same way from the algebraic model of Spare gates presents in Sections 3.2 and 3.3.

4.2 Probabilistic model of 2 Spare gate with 2 input events sharing a spare event

According to Section 3.4, the algebraic model of the Spare gate on the left side in Fig. 5 is

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

It can be noted that the first two terms of this expression – $C_a \cdot (A \lhd C_a)$ and $A \cdot (C_d \lhd A)$ – do not depend on B while the third term – $A \cdot (B \lhd A)$ – does. As a consequence, these three terms are not disjunctive. This expression can be converted to an equivalent form which contains only disjunctive terms by introducing B in the first two terms:

$$\begin{aligned} Q1 &= C_a \cdot (A \lhd B) \cdot (B \lhd C_a) \\ &\quad + B \cdot (A \lhd C_a) \cdot (C_a \lhd B) \\ &\quad + C_a \cdot (A \lhd C_a) \cdot \bar{B} \\ &\quad + B \cdot (C_d \lhd A) \cdot (A \lhd B) \\ &\quad + A \cdot (C_d \lhd A) \cdot \bar{B} + A \cdot (B \lhd A), \end{aligned} \tag{3}$$

Its failure probability thus is

$$\begin{aligned} Pr\{Q1\}(t) &= Pr\{C_a \cdot (A \lhd B) \cdot (B \lhd C_a)\}(t) \\ &\quad + Pr\{B \cdot (A \lhd C_a) \cdot (C_a \lhd B)\}(t) \\ &\quad + Pr\left\{C_a \cdot (A \lhd C_a) \cdot \bar{B}\right\}(t) \\ &\quad + Pr\{B \cdot (C_d \lhd A) \cdot (A \lhd B)\}(t) \\ &\quad + Pr\left\{A \cdot (C_d \lhd A) \cdot \bar{B}\right\}(t) \\ &\quad + Pr\{A \cdot (B \lhd A)\}(t) \end{aligned} \tag{4}$$

and can hence be expressed according to the failure

distributions of A, B, and C as follows:

$$Pr\{Q1\}(t) =$$

$$\int_0^t \left(\int_w^t \left(\int_w^u f_B(v)dv \right) f_{C_a}(u,w)du \right) f_A(w)dw$$

$$+ \int_0^t \left(\int_0^u \left(\int_v^u f_{C_a}(w,v)dw \right) f_A(v)dv \right) f_B(u)du$$

$$+(1 - F_B(t)) \int_0^t \left(\int_v^t f_{C_a}(u,v)du \right) f_A(v)dv$$

$$+ \int_0^t \left(\int_0^u f_A(v) F_{C_d}(v)dv \right) f_B(u)du$$

$$+(1 - F_B(t)) \int_0^t f_A(u) F_{C_d}(u)du$$

$$+ \int_0^t f_A(u) F_B(u)du$$

The failure probability of $Q2$ can be determined in the same way, by symmetry. The probabilistic model of n Spare gate with 2 input events sharing a common event can be determined in the same way from the algebraic model in Section 3.5.

5 APPLICATION TO A DFT EXAMPLE

We propose to determine the failure probability of the Spare gates of a DFT example from (Boudali and Dugan 2005) which is depicted in Fig. 6.

This DFT models the failure of a cardiac assist system (HCAS) which is divided into 4 modules: Trigger, CPU unit, motor section, and pumps. The Trigger consists of a crossbar switch (CS) and a system supervision (SS). The failure of either CS or SS triggers the failure of both CPUs. The CPU unit is a warm spare, which has a primary P and a spare unit B having a dormancy of 0.5. For the motor section to function, either MOTOR or MOTORC need to be working. The pumps unit is comprised of two cold spares, each having a primary pump (PUMP_1 and PUMP_2), and sharing a common spare pump (Backup_PUMP). In order for the pumps unit to fail, all three pumps need to fail and CSP_1 needs to fail before (or at the same time as) CSP_2, i.e. PAND gate.

This DFT can be divided into 3 subtrees:

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

The failure probability of the two Spare gates of subtree 3 can be determined thanks to the probabilistic model of Section 4.2:

$$Pr\{CSP1\}(t) =$$

$$\int_0^t \left(\int_w^t \left(\int_w^u f_{P2}(v)dv \right) f_{BP_a}(u,w)du \right) f_{P1}(w)dw$$

$$+ \int_0^t \left(\int_0^u \left(\int_v^u f_{BP_a}(w,v)dw \right) f_{P1}(v)dv \right) f_{P2}(u)du$$

$$+(1 - F_{P2}(t)) \int_0^t \left(\int_v^t f_{BP_a}(u,v)du \right) f_{P1}(v)dv$$

$$+ \int_0^t f_{P1}(u) F_{P2}(u)du$$

where $CSP1$ denotes the output of the Spare gate $CSPGate\_1$, and $P1$, $P2$, and BP denote the basic events $PUMP\_1$, $PUMP\_2$, and $Backup\_PUMP$, respectively. It can be noted that, contrary to the probabilistic model of Section 4.2, this expression contains only 4 terms since BP is a cold spare event which can consequently not fail while in its dormant mode.

In the same way,

$$Pr\{CSP2\}(t) =$$

$$\int_0^t \left(\int_w^t \left(\int_w^u f_{P1}(v)dv \right) f_{BP_a}(u,w)du \right) f_{P2}(w)dw$$

$$+ \int_0^t \left(\int_0^u \left(\int_v^u f_{BP_a}(w,v)dw \right) f_{P2}(v)dv \right) f_{P1}(u)du$$

$$+(1 - F_{P1}(t)) \int_0^t \left(\int_v^t f_{BP_a}(u,v)du \right) f_{P2}(v)dv$$

$$+ \int_0^t f_{P2}(u) F_{P1}(u)du$$

where $CSP2$ denotes the output of the Spare gate $CSPGate\_2$.

In the particular case of exponential distributions,

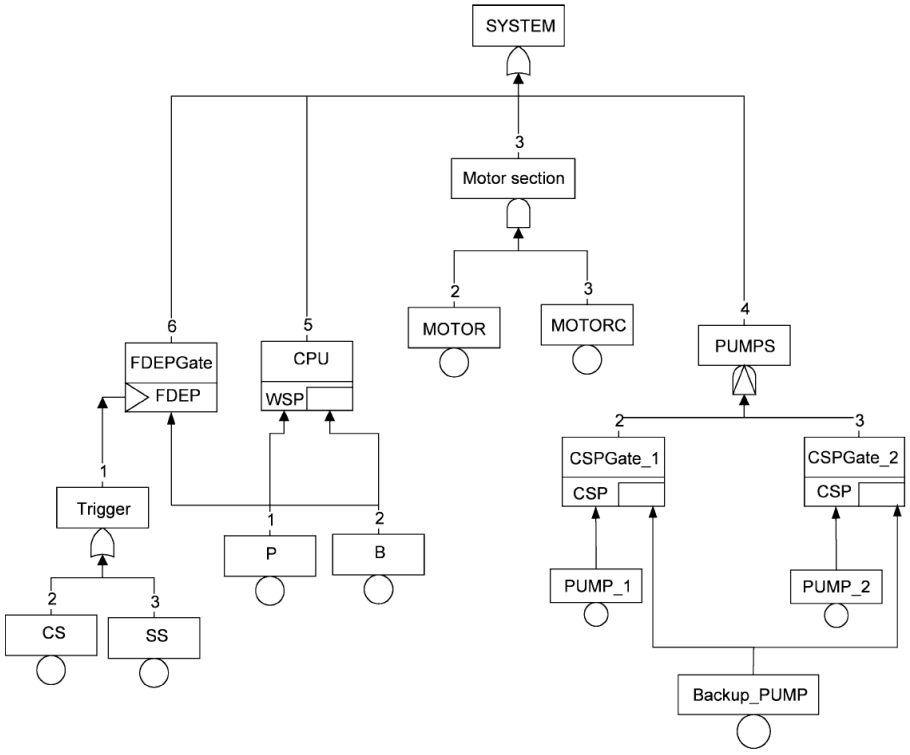

Figure 6: The HCAS Dynamic Fault Tree from (Boudali and Dugan 2005)

$$\begin{cases} F_{P1}(t) = 1 - e^{-\lambda_{P1} t} \\ F_{P2}(t) = 1 - e^{-\lambda_{P2} t} \\ F_{BP_d}(t) = 0 \\ F_{BP_a}(t, \min(t_{P1}, t_{P2})) = 1 - e^{-\lambda_{BP}(t - \min(t_{P1}, t_{P2}))} \end{cases}$$

If we consider failure rates $\lambda_{P1} = \lambda_{P2} = \lambda_{BP} = 2.5 \times 10^{-3}$ for $P1$, $P2$, and BP, we get a failure probability of 0.84 at mission time $T = 1,000$ hours for both Spare gates. This result is the same as the result obtained thanks to the tool Galileo (Dugan, Sullivan, and Coppit 2000). It can be noted that the failure probability of the Top Event of the DFT in Fig. 6 could be determined as well, thanks to the theorems and the probabilistic models of gates PAND and FDEP presented in (Merle, Roussel, Lesage, and Bobbio 2010).

However, a Weibull distribution would be more suitable to model the failure behavior – and the aging – of pumps, but such a distribution could not be handled by Continuous-Time Markov Chains or Stochastic Petri Nets based methods. The probabilistic model that we provide for Spare gates does not depend on the failure distribution considered for basic events, and thus allows to consider such a case. The Weibull distribution has the expression

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

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

so that

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

Let us consider that the failure of basic events is modeled by a Weibull distribution with a failure rate $\lambda(t) = 5 \times 10^{-3} - 10^{-6}t$, which means that the pumps have an "infant mortality" and will fail at a constant failure rate $\lambda = 2.5 \times 10^{-3}$ after $2,500$ hours. We thus obtain a failure probability of 0.98 at mission time $T = 1,000$ hours for both Spare gates.

6 CONCLUSION

In this paper, we have presented an algebraic model of Spare gates. This model can be determined for any number of Spare gates with any number of input events, whether they are sharing spare events or not, and for any type of Spare gate. This algebraic model allowed us to deduce a probabilistic model of Spare gates which does not depend on the failure distribution considered for basic events.

Ongoing work is currently addressed to the elaboration of efficient algorithms allowing to automatically perform the calculation of the structure function of DFTs and their analysis.

REFERENCES

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

Billingsley, P. (1995). *Probability and measure*. New York, USA: John Wiley & Sons.

Bobbio, A. and D. C. Raiteri (2004). Parametric Fault Trees with Dynamic Gates and Repair Boxes. In *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS)*, Los Angeles, CA, USA, pp. 459–465.

Boudali, H., P. Crouzen, and M. Stoelinga (2007). A compositional semantics for dynamic fault trees in terms of interactive markov chains. In *Proceedings of the 5th International Symposium on Automated Technology for Verification and Analysis (ATVA 2007)*, Tokyo, Japan, pp. 441–456.

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

Coppit, D. and K. J. Sullivan (2002). Designing Modeling Languages: A Case Study in Dynamic Fault Trees. *IEEE Transactions on Dependable and Secure Computing*.

Dugan, J., S. Bavuso, and M. Boyd (1990). Fault Trees and Sequence Dependencies. In *Proceedings of the Annual Reliability and Maintainability Symposium (RAMS 1990)*, pp. 286–293.

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

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

Dutuit, Y. and A. Rauzy (1996). A Linear-Time Algorithm to Find Modules of Fault Trees. *IEEE Transactions on Reliability 45*(3), 422–425.

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

Gulati, R. and J. Dugan (1997). A modular approach for analyzing static and dynamic fault trees. In *Proceedings of the Annual Reliability and Maintainability Symposium*, Philadelphia, PA, USA, pp. 57–63.

Henley, E. and H. Kumamoto (1981). *Reliability Engineering and Risk Assessment*. Englewood Cliffs: Prentice Hall.

Leveson, N. (1995). *Safeware: System Safety and Computers*. Addison-Wesley.

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

Merle, G., J.-M. Roussel, J.-J. Lesage, and A. Bobbio (2009). Algebraic Expression of the Structure Function of a subclass of Dynamic Fault Trees. In *Proceedings of the 2nd IFAC Workshop on Dependable Control of Discrete Systems (DCDS'09)*, Bari, Italy, pp. 129–134.

Merle, G., J.-M. Roussel, J.-J. Lesage, and A. Bobbio (2010). Probabilistic Algebraic Analysis of Fault Trees with Priority Dynamic Gates and Repeated Events. *IEEE Transactions on Reliability 59*(1), 250–261.

Raiteri, D. C. (2005). The Conversion of Dynamic Fault Trees to Stochastic Petri Nets, as a case of Graph Transformation. *Electronic Notes in Theoretical Computer Science 127*(2), 45–60.

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

Tang, Z. and J. Dugan (2004). Minimal cut set/sequence generation for dynamic fault trees. In *Proceedings of the Annual Reliability and Maintainability Symposium*, Los Angeles, CA, USA, pp. 207–213.

Trivedi, K. (2001). *Probability & Statistics with Reliability, Queueing & Computer Science Applications* (2 ed.). Wiley.