



**Chiacchio, Ferdinando and Aizpurua, Jose Ignacio and D'Urso, Diego and Compagno, Lucio (2017) Coherence region of the Priority-AND gate : analytical and numerical examples. Quality and Reliability Engineering International. ISSN 0748-8017 (In Press) ,**

This version is available at <https://strathprints.strath.ac.uk/61969/>

**Strathprints** is designed to allow users to access the research output of the University of Strathclyde. Unless otherwise explicitly stated on the manuscript, Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Please check the manuscript for details of any other licences that may have been applied. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (<https://strathprints.strath.ac.uk/>) and the content of this paper for research or private study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to the Strathprints administrator: [strathprints@strath.ac.uk](mailto:strathprints@strath.ac.uk)

## Coherence region of the Priority-AND gate: analytical and numerical examples

Ferdinando Chiacchio<sup>1a</sup>, Jose Ignacio Aizpurua<sup>b</sup>, Diego D'Urso<sup>a</sup>, Lucio Compagno<sup>a</sup>

<sup>a</sup> Department of Electric, Electronic and Computer Engineering, University of Catania, Italy

<sup>b</sup> Department of Electronic and Electrical Engineering, University of Strathclyde, Scotland

### Abstract

In recent years, the need for a more accurate dependability modelling (encompassing reliability, availability, maintenance, and safety) has favoured the emergence of novel dynamic dependability techniques able to account for temporal and stochastic dependencies of a system. One of the most successful and widely used method is Dynamic Fault Tree that, with the introduction of the dynamic gates, enables the analysis of dynamic failure logic systems such as fault-tolerant or reconfigurable systems. Among the dynamic gates, Priority-AND (PAND) is one of the most frequently used gate for the specification and analysis of event sequences. Despite the numerous modelling contributions addressing the resolution of the PAND gate, its failure logic and the consequences for the coherence behaviour of the system need to be examined to understand its effects for engineering decision-making scenarios including design optimization and sensitivity analysis. Accordingly, the aim of this short communication is to analyse the coherence region of the PAND gate so as to determine the coherence bounds and improve the efficacy of the dynamic dependability modelling process.

**Keywords:** Markov Chains; Monte Carlo Simulation; Repairable Components; Failure Gates; Dynamic Gates Semantics

### 1. INTRODUCTION

Fault Tree Analysis is a widely applied technique for the dependability assessment of different applications. Dependability is a term that encompasses a range of attributes which include safety, reliability, availability, maintainability, confidentiality, and integrity<sup>1</sup>. We will not consider confidentiality and integrity attributes because security aspects are outside of the scope of this paper.

For complex systems with dynamic failure logic, the use of Fault Trees is limited because they are unable to accurately capture temporal and stochastic dependencies<sup>2</sup>. To overcome these limitations, Fault Trees have been extended with dynamic gates in the Dynamic Fault Tree (DFT) formalism. Dynamic Fault Trees allow modelling systems with standby logic, sequence of events and conditional triggering dependencies. Table 1 shows the graphical representation of the dynamic gates and their failure behaviour specification.

The design of a Dynamic Fault Tree follows a top-down procedure as with classical (Static) Fault Trees. The top-event represents the system failure condition and this condition is decomposed into a combination of intermediate events defined by Boolean logic and dynamic gates. Basic events are the lowest level events, and generally they represent system component faults. However, the probabilistic analysis of Dynamic Fault Tree models is more intricate than Static Fault Trees. In

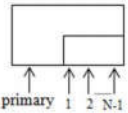
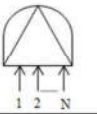
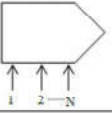
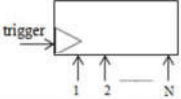
<sup>1</sup> Corresponding Author

Email Address: [chiacchio@dmi.unict.it](mailto:chiacchio@dmi.unict.it) (Ferdinando Chiacchio)

the last few years, different resolution techniques have been proposed to address the quantification problem. These techniques can be grouped into analytical and simulation approaches. Among the former, Markov chains<sup>3</sup> and state space reduction<sup>4</sup> are suitable when the time to failure/repair follows an exponential distribution, whereas analytical solutions based on structure function<sup>5</sup> or binary decision diagrams<sup>6</sup> are normally limited to non-repairable Dynamic Fault Trees. On the other hand, simulation approaches<sup>7</sup> overcome the limitations of the analytical methods, but they can require long computation times to achieve accurate results.

So as to evaluate the dependability of repairable systems through DFT models, the original formulation of Dynamic Fault Trees<sup>2</sup> were extended through a formal semantics that defines the behaviour of the DFT gates in case of repairable components (see Manno *et al.*<sup>8</sup> or Rauzy and Dutuit<sup>9</sup>).

Table 1. Dynamic gates of Dynamic Fault Tree

Name	Graphical Representation	Description (N input)
SPARE		It triggers only after the primary and all the N-1 spare occur. Spares can be shared with other spare gate. It is possible to identify three different types of spare on the basis of the dormancy factor $\alpha$ which is a multiplicative factor to the active failure rate (when the spare is not in use): <b>Cold:</b> $\alpha = 0$ , spare cannot fail as long as it is not active. <b>Hot:</b> $\alpha = 1$ , spare can fail at the same rate as when active. <b>Warm:</b> $0 < \alpha < 1$ , spare can always fail, but at a reduced failure rate when it is not in use.
PAND		It behaves like an AND gate but it triggers only if the input events occur in the order from the leftmost to the rightmost.
SEQ		It forces the input events to occur from the left to the right order. It can model the gradual degradation of a system. It behaves as a Cold Spare Gate.
FDEP		This gate models the failure of the dependent input events if the trigger occurs. The output is a dummy or an input for other gates. Note that input events can fail by themselves too.

The logic of dynamic gates enables the modelling of temporal dependencies of complex systems such as fault-tolerant and reconfigurable systems<sup>10</sup>. The semantics of some of these dependencies have been analysed in the literature<sup>4</sup> including the simultaneity of the events in a PAND gate, the order of components activation in a SPARE gate, the effects of the restoration of the trigger of a FDEP gate, or the treatment of constant probabilities.

Surprisingly, the coherence of the PAND gate<sup>11</sup> was never discussed in detail. The coherence is an important property of engineering systems and the most interesting point regarding coherence is that the increase of the reliability of the input components would imply the increase of the reliability of the gate. This is what the designers may be interested in, since they could improve the reliability of the whole system simply by improving the reliability of some basic components. For the PAND gate a detailed analysis of its coherence behaviour may identify useful patterns from the engineering usage perspective. In fact, the increase of the failure probability of the input components of the gate does not always result in an increase of the failure probability of a PAND gate. This is not a

1  
2  
3 common pattern for other positive static (e.g., AND, OR, XOR, VOTING) gates, as an increase in a  
4 component failure probability leads directly to an increase in the failure probability of the gate. This  
5 is not typical even for other negative logic gates<sup>12, 13</sup> (e.g., NOT, NAND, NOR) whose failure  
6 probability decreases with the increasing failure probabilities of the components. In fact, as it will  
7 be shown, the failure probability of a PAND gate presents a maximum value that depends on the  
8 configuration of its input components.  
9

10 In many industrial applications the identification and quantification of this property is not trivial.  
11 However, it may have many implications for engineering design applications. For instance, when  
12 engineers need to optimize the system design and this optimization process involves minimising the  
13 system failure probability (e.g., strengthen a system section through improved reliability of specific  
14 components<sup>17</sup> or maintenance plans which minimize cost and failure probability<sup>14</sup>), and the failure  
15 model includes time-sequences specified with PAND gates. Therefore, the coherence analysis of the  
16 system may be relevant to identify optimal design decisions.  
17

18 For a system to be coherent it must meet two requirements<sup>15</sup>:

- 19  
20 1) **Monotonicity**: the reliability improvement of any component will improve the system  
21 reliability, and  
22 2) **Relevance**: every component in the system contributes to the system reliability.

23 For the PAND gate, it will be shown that the monotonicity of the gate depends on its input  
24 parameters. Accordingly, the aim of this short communication is to discuss the failure behaviour of  
25 the PAND gate and provide a practical way to identify the conditions under which the PAND gate  
26 behaves as a coherent gate, within the so-called *coherence region* of the PAND gate. The  
27 identification of the coherence region can allow the users to setup a correct intervention for the  
28 improvement of a system (e.g., importance measure<sup>14,16</sup>, sensitivity analysis<sup>17</sup>) and better  
29 understand the results of dynamic dependability analyses, particularly for the class of novel  
30 techniques belonging to the Dynamic Probabilistic Risk Assessment (DPRA). DPRA techniques  
31 make use of non-fixed probability density functions for the failure/repair behaviour of  
32 components<sup>18, 19, 20</sup> that, according to the change of operational conditions, need to be interpreted  
33 also on the basis of the knowledge of the coherence region of the PAND gate.  
34  
35

36 The paper is organized as follows. Section 2 describes the failure logic of the PAND gate and  
37 frames the design-engineering questions related to its use. In Section 3 authors provide an answer to  
38 the questions raised in Section 2 and present a mathematical analysis of a 2-input PAND gate for  
39 both repairable and non-repairable components. Finally, Section 4 presents conclusions and  
40 discussions.  
41  
42

## 43 2. PAND GATE BACKGROUND: FAILURE LOGIC AND ENGINEERING CONSEQUENCES

44  
45  
46 The original PAND gate failure logic was introduced by Fussell *et al.*<sup>21</sup> and the definition states  
47 that the gate can represent a system that fails if and only if all its inputs fail in left to right order. In  
48 any other case the failure does not occur. The graphical representation of the  $n$ -input PAND gate is  
49 shown in Figure 1.  
50

51 The PAND gate version with repairable inputs was discussed by Manno *et al.*<sup>8</sup>  
52  
53  
54  
55  
56  
57  
58  
59  
60

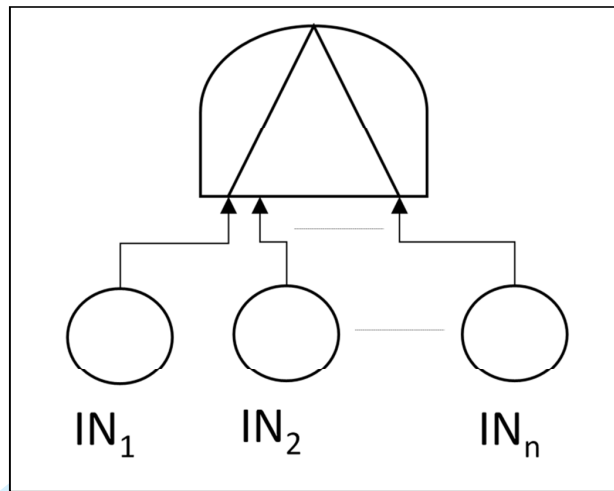


Figure 1: PAND gate with  $n$  inputs. The gate triggers iff inputs fail in the order from left to right.

Equivalently, the generic  $n$ -input PAND gate can be modelled with  $(n-1)$  interconnected 2-input PAND gates<sup>22</sup>. Generally, the left side input of the PAND gate corresponds with the monitoring system (sensors or alarms) whereas the right side input corresponds with the actuators<sup>2,4</sup>. For simplicity, the analysis presented in this paper focuses on the PAND gate with two inputs, but results are directly generalizable to  $n$ -input PAND gates.

Figure 2 shows the reachability graphs of a 2-input PAND gate for non-repairable<sup>2</sup> and repairable input events<sup>8</sup>, where the left and right inputs of the PAND gate are components A and B respectively.  $F_x$  and  $R_x$  denote respectively the failure and the repair transitions of component  $x$  associated to the generic failure and repair probability distributions.

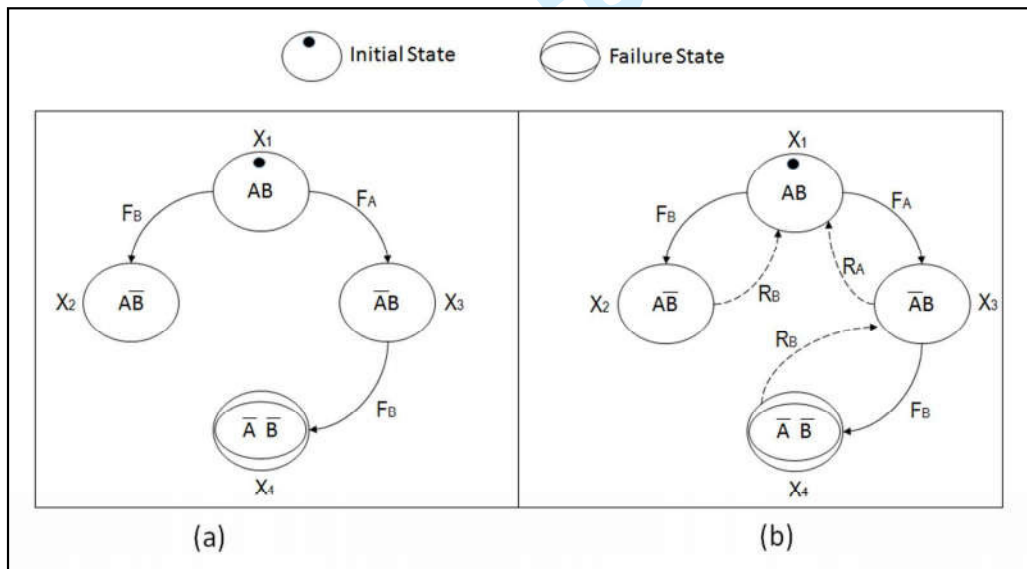


Figure 2: reachability graph for a 2-input PAND gate with (a) non-repairable and (b) repairable components

In the non-repairable model shown in Figure 2.a, if component B fails before A, it is possible to identify an absorbing safe state  $A\bar{B}$  in which the system remains permanently. As for the repairable version shown in Figure 2.b, the state  $A\bar{B}$  is not absorbing because it is assumed that component B can be repaired and this event brings the system back to the initial state.



Figure 3 shows the sensitivity analysis of the 2-input PAND gate varying the input failure rates in the range of values between  $[0, 10^{-3}]$  failures per hour ( $[h^{-1}]$ ) and Figure 4 shows the section of the 3D plot of Figure 3 by fixing the failure rate of input A,  $\lambda_A = 10^{-4} h^{-1}$ . Observing the two dimensional plot in Figure 4, it is possible to notice that the probability of failure of the PAND gate has an absolute maximum value in  $\lambda_B^*$  and starts decreasing for  $\lambda_B > \lambda_B^*$ .

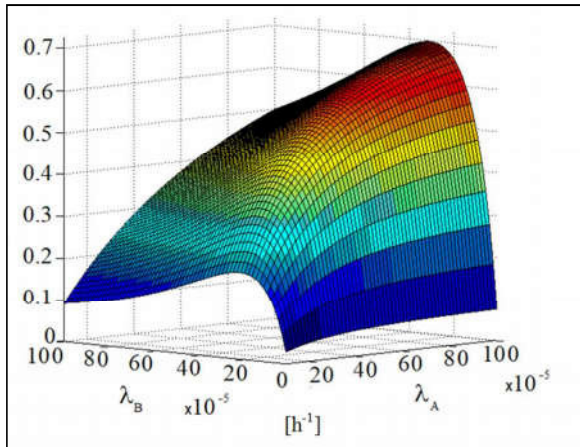


Figure 3: sensitivity analysis for a 2-input PAND gate (with  $t = 8760h$ )

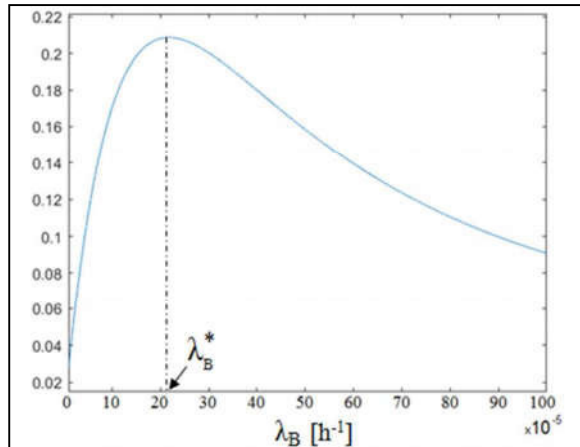


Figure 4: section in the plane  $\lambda_B$  ( $\lambda_A = 10^{-4} h^{-1}$ )

According to the results of this sensitivity analysis, the reliability of the PAND system can sometimes be improved by selecting a component B with a lower reliability. This is the typical characteristic of an incoherent system and, from a design-engineering point of view, raises questions that require some clarifications:

- 1) May the engineer design the system by selecting a component B (the actuator) less reliable than the component A (the monitoring component)?
- 2) How should the engineer select the system components if he/she is allowed to substitute them with other components having different reliability characteristics?

Due to the incoherent behaviour of the PAND gate, the answer to these questions is not straightforward. But, a qualitative analysis of the PAND gate with non-repairable components (Figure 2.a) can reveal some interesting properties that help to answer the first question. Namely, at steady-state the reliability of the system does not tend to zero, as expected in a system with non-repairable components, because it is distributed between the failure state  $\bar{A}\bar{B}$  and the safe state  $A\bar{B}$ . This observation allows us to answer to the first question and agree with the fact that engineers should design a system in which the actuator component (i.e., input component B) is less reliable than the monitoring component (i.e., input component A). In fact, when the system transits towards the safe state  $A\bar{B}$  (i.e., the actuator component fails), the failure of the system is avoided. This applies for both non-repairable (i.e., the system remains in the state  $A\bar{B}$ ) and repairable components.

In the repairable case, we can assume a hypothetical engineering scenario in which component B fails and gets repaired repeatedly such that the system transits from the initial state  $AB$  to the safe state  $A\bar{B}$  and back continuously. Clearly, from a practical point of view, this scenario is not desirable as it carries the major inconvenience linked with the service unavailability of the system and the economic loss of its maintenance and restoration. In order to be effective, it must remain as much as possible in the initial state  $AB$ .

An answer to the second question can offer the opportunity to tackle the paradox of the previous observation. In this case, the problem to solve is how to select the system components so as to

increase the system dependability, but avoiding the issue of the service unavailability. In the next section we will address this issue analysing in deep the incoherent nature of the PAND gate. We will provide some useful information about the PAND gate behaviour and a practical way to recognize the coherence region of the gate.

### 3. COHERENCE ANALYSIS OF THE PAND GATE

Let us define  $\mathbf{Y} = \{v_1, v_2, \dots, v_n\}$  as the vector of variables that characterize the probability density function (PDF) of the time to failure (or time to occur) of a component (or an event). For instance, the well-known Poisson PDF (modelling random failures) is characterized by a single parameter, called failure rate ( $v_1 = \lambda$ ), or the Weibull PDF (used to model the bathtub behaviour) has two variables, called shape ( $v_1 = \beta$ ) and scale ( $v_2 = \gamma$ ) parameters. Under this setting, it is possible to define the *coherence region*, CR, as:

$$CR: \{v_i \in \mathbb{R}: \frac{\partial F(\mathbf{Y})}{\partial v_i} \geq 0, i = 1, \dots, n\} \quad (\text{Eq. 1})$$

Eq. 1 defines a n-dimensional space in which the probability of failure of a PAND gate  $F(\mathbf{Y})$  is monotonically increasing in all its argument  $v_i$  belonging to the set of real number  $\mathbb{R}$ .

In order to simplify the problem, the behaviour of the gate can be studied using the corresponding Continuous Time Markov Chain model, assuming constant random failures/repairs rate ( $F_A = \lambda_A$ ,  $F_B = \lambda_B$ ,  $R_A = R_B = \mu$ ). Equations in (Eq. 2) show the Kolmogorov differential equations related to the transient analysis of the PAND gate with repairable components (Figure 2.b):

$$\begin{aligned} \dot{x}_1 &= (x_2 + x_3)\mu - x_1(\lambda_A + \lambda_B) \\ \dot{x}_2 &= x_1\lambda_B - x_2\mu \\ \dot{x}_3 &= x_1\lambda_A - x_3(\mu + \lambda_B) + x_4\mu \\ \dot{x}_4 &= x_3\lambda_B - x_4\mu \end{aligned} \quad (\text{Eq. 2})$$

To obtain the system of equations that defines the scenarios of Figure 2.a, it is possible to simply set  $\mu = 0$ . The system of differential equations in (Eq. 2) can be written in the matrix form, using the infinitesimal generator matrix (or Generator Matrix) Q:

$$\dot{\mathbf{X}} = \mathbf{Q}\mathbf{X} \quad (\text{Eq. 3})$$

$$\dot{\mathbf{X}} = \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} \quad \mathbf{Q} = \begin{bmatrix} -(\lambda_A + \lambda_B) & \mu & \mu & 0 \\ \lambda_B & -\mu & 0 & 0 \\ \lambda_A & 0 & -(\mu + \lambda_B) & \mu \\ 0 & 0 & \lambda_B & -\mu \end{bmatrix} \quad \mathbf{X} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

The probability  $P(X_i) = x_i(t)$  of the system to sojourn at time  $t$  in the  $i^{\text{th}}$  state can be found by integrating the system of differential equations (Eq. 3). According to the reachability graph in Figure 2, for the PAND gate, the failure of the system occurs in the state  $X_4$ .

The simplest case to solve analytically is the PAND gate with non-repairable input components (Figure 2.a). This scenario represents the most common example in literature of Dynamic Fault Trees. In the next sections we will examine the steady state and coherence region analysis by starting from the non-repairable case and we will gradually increase the complexity by including

repair rates (Section 3.2) and the restoration of component B in the failure gate<sup>8</sup> configuration (Section 3.3). The mission time and the failure rate of the components A and B are taken from a previous work<sup>23</sup> and represent the typical scenario of an industrial case of study. The failure and repair rates used in the numerical examples showed in the rest of the paper are measured respectively in number of failures and number of repairs per hours ([h<sup>-1</sup>]).

3.1 Non-repairable components

According to the reachability graph of Figure 2.a it is possible to identify two absorbing states (X<sub>2</sub> and X<sub>4</sub>) that are, by definition of PAND gate<sup>2</sup>, respectively a safe and a failure state. Equations (Eq. 4.a) to (Eq. 4.d) show the solution for the system (Eq. 2) with μ = 0:

$$x_1(t) = e^{-(\lambda_A + \lambda_B)t} \tag{Eq. 4.a}$$

$$x_2(t) = \frac{\lambda_B}{\lambda_B + \lambda_A} (1 - e^{-(\lambda_A + \lambda_B)t}) \tag{Eq. 4.b}$$

$$x_3(t) = e^{-\lambda_B t} - e^{-(\lambda_A + \lambda_B)t} \tag{Eq. 4.c}$$

$$x_4(t) = \frac{\lambda_A}{\lambda_A + \lambda_B} - e^{-\lambda_B t} + \frac{\lambda_B e^{-(\lambda_A + \lambda_B)t}}{\lambda_A + \lambda_B} \tag{Eq. 4.d}$$

Since the analytical determination of the coherence region is complex, it is possible to evaluate numerically the positivity of the partial derivatives of x<sub>4</sub>(t) = P(X<sub>4</sub>) by fixing the mission time and the failure rates of one of the two components alternatively. That is, so as to evaluate the partial derivative of the PAND gate with respect to the failure rate of component A, we fix the mission time and the failure rate of component B and vice-versa.

Figure 5 shows the partial derivative of x<sub>4</sub>(t) with respect to the failure rate of component A,  $\frac{\partial P(X_4)}{\partial \lambda_A}$ , in the range of values λ<sub>A</sub> ∈ [0, 10<sup>-2</sup>] h<sup>-1</sup> with mission time T<sub>m</sub> = 8760h, and λ<sub>B</sub> = 7.5x10<sup>-4</sup> h<sup>-1</sup>.

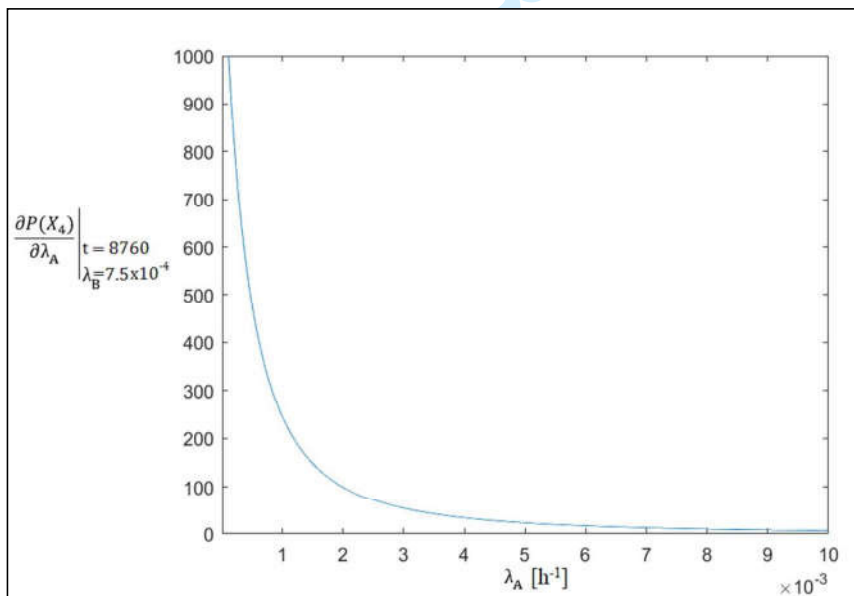


Figure 5: derivative of P(X<sub>4</sub>) with respect to the variable λ<sub>A</sub>, with t = 8760 and λ<sub>B</sub>=0.00075

According to results shown in Figure 5, when we compute the partial derivative of the PAND gate with respect to the failure rate of component A, the PAND gate will always behave as a



coherent system ( $\frac{\partial P(X_4)}{\partial \lambda_A} > 0, \forall \lambda_A \in [0, 10^{-2}] \text{ h}^{-1}$ ) and an increase of the failure rate of component A turns in the increase of the PAND gate unreliability.

Assuming the same parameters as in Figure 5, the partial derivative of  $x_4(t)$  with respect to the failure rate of component B is shown in Figure 6 (mission time  $T_m = 8760\text{h}$  and  $\lambda_A = 1.7 \times 10^{-4} \text{ h}^{-1}$ ).

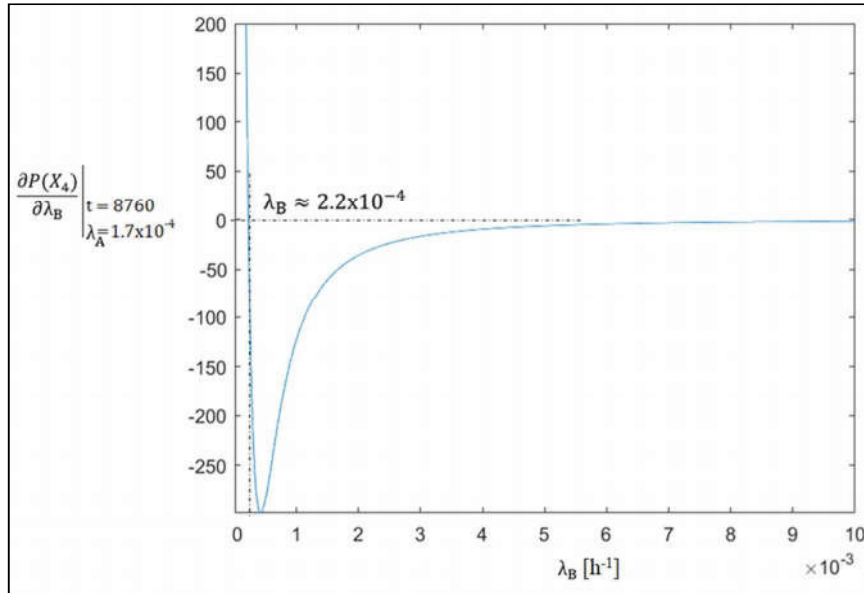


Figure 6: derivative of  $P(X_4)$  with respect to the variable  $\lambda_B$ , with  $t = 8760$  and  $\lambda_A = 0.00017$

We can see in Figure 6 that for failure rates higher than  $2.2 \times 10^{-4} \text{ h}^{-1}$  the system behaves incoherently ( $\frac{\partial P(X_4)}{\partial \lambda_B} < 0$ ) because the monotonicity condition is not satisfied. Notice also that when the failure rate of component B is much higher than the failure rate of component A ( $\lambda_B \gg \lambda_A$ ), in the long term  $P(X_2) = 1$ . That is, if  $t \rightarrow \infty$ ,  $P(X_1) = P(X_3) = 0$ ,  $P(X_2) = \lambda_B / (\lambda_A + \lambda_B)$  and  $P(X_4) = \lambda_A / (\lambda_A + \lambda_B)$ . Setting  $\lambda_B \gg \lambda_A$ ,  $P(X_2) = \lambda_B / (\lambda_A + \lambda_B) \approx 1$ , while  $P(X_4) = \lambda_A / (\lambda_A + \lambda_B) \approx 0$ . This is an inherent property of the PAND gate which is in contrast with the definition of the reliability of a system<sup>23</sup>. In fact, reliability is a monotonic decreasing probability function that tends to zero for  $t$  approaching infinity. In other words, all the absorbing states of the corresponding system reachability graph must be of failure for the system. This shortage has been tackled in Manno<sup>8</sup> with the introduction of the failure gate and, according to this design, authors suggest to include at least a repair rate from  $X_2$  to  $X_1$ , when interested in the evaluation of the system reliability (see Section 3.3).

### 3.2 Repairable components

In case of repairable components, it is more appropriate to grasp to the concept of system availability<sup>23</sup> and skip the transient analysis in favour of the steady-state regime. To do that, it is possible to solve the balance equations:

$$\dot{X} = QX = 0 \quad (\text{Eq. 5})$$

subject to the condition

$$\sum_i X_i = 1 \quad (\text{Eq. 6})$$

The solution of the algebraic system (Eq. 5-6) is:

$$P(X_1) = \frac{\mu^2}{(\lambda_A + \mu)(\lambda_B + \mu)} \quad (\text{Eq. 7.a})$$

$$P(X_2) = \frac{\lambda_B \mu}{(\lambda_A + \mu)(\lambda_B + \mu)} \quad (\text{Eq. 7.b})$$

$$P(X_3) = \frac{\lambda_A \mu}{(\lambda_A + \mu)(\lambda_B + \mu)} \quad (\text{Eq. 7.c})$$

$$P(X_4) = \frac{\lambda_A \lambda_B}{(\lambda_A + \mu)(\lambda_B + \mu)} \quad (\text{Eq. 7.d})$$

To determine the coherence region, it is sufficient to evaluate the positivity of the partial derivatives of  $P(X_4)$ . It can be shown that:

$$\frac{\partial P(X_4)}{\partial \lambda_A} = \frac{\lambda_B \mu}{(\lambda_A + \mu)^2 (\lambda_B + \mu)} \quad (\text{Eq. 8})$$

and

$$\frac{\partial P(X_4)}{\partial \lambda_B} = \frac{\lambda_A \mu}{(\lambda_B + \mu)^2 (\lambda_A + \mu)} \quad (\text{Eq. 9})$$

are always positive for each positive value of failure and repair rate. Since we are not interested in negative failure rates, we can conclude that the repairable PAND gate does not behave incoherently in  $\mathbb{R}^+$ .

### 3.3 Failure PAND Gate with repairable inputs

The adoption of the failure PAND gate<sup>8</sup> allows to solve the limit discussed in Section 3.1 concerning the absorbing nature of the safe state  $X_2$ . With this configuration we assume that component B can be repaired only when the component B fails before A. Figure 7 shows the reachability graph of this configuration and it is easy to observe that, at steady state,  $P(X_4) = 1$  for  $t \rightarrow \infty$ .

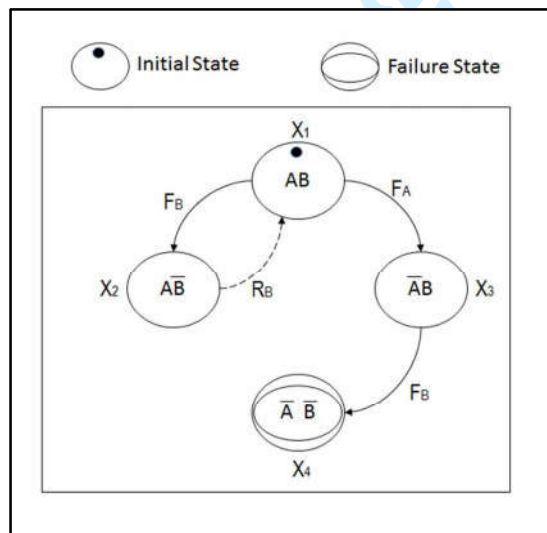


Figure 7: reachability graph for a 2-input failure PAND gate with repairable components

As in Section 3.1, the determination of the coherence region can be performed numerically. In this case, the model presents one more variable, namely the distribution function  $R_B$  linked to the repair transition. For the sake of simplicity, in the numerical example used we assume that this

transition is exponentially distributed with rate  $\mu = 1 \text{ h}^{-1}$ . This setting expresses the practical circumstance of a system in which repair transitions are much faster than faults ( $\mu \gg \lambda_A, \mu \gg \lambda_B$ ).

Again, setting the mission time to  $T_m = 8760\text{h}$ , Figure 8 and Figure 9 show the positivity of the partial derivative of  $x_4(t)$ , in the range of values  $\lambda \in [0, 10^{-1}] \text{ h}^{-1}$ , respectively for  $\frac{\partial P(X_4)}{\partial \lambda_A}$  and  $\frac{\partial P(X_4)}{\partial \lambda_B}$ , with  $\lambda_A = 1.7 \times 10^{-4} \text{ h}^{-1}$  and  $\lambda_B = 7.5 \times 10^{-4} \text{ h}^{-1}$ .

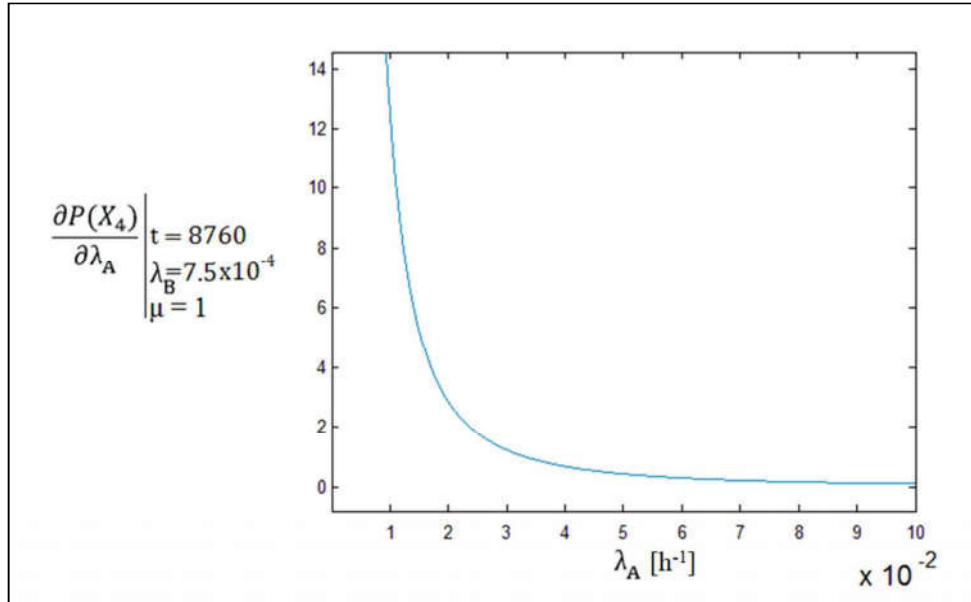


Figure 8: derivative of  $P(X_4)$  for the failure gate model, with respect to the variable  $\lambda_A$  ( $t = 8760 \text{ h}$  and  $\lambda_B = 0.00075 \text{ h}^{-1}$ )

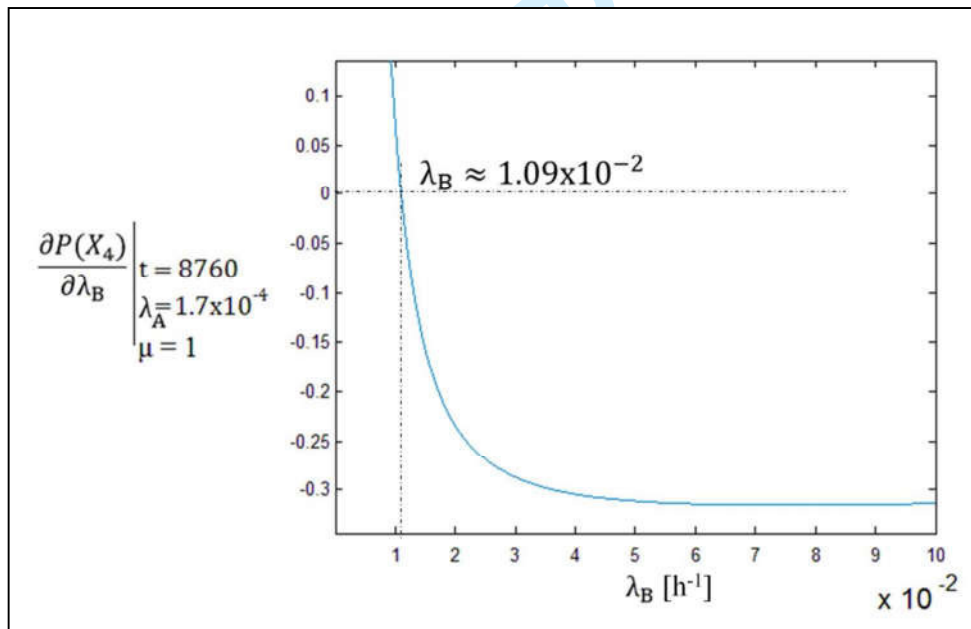


Figure 9: derivative of  $P(X_4)$  for the failure gate model, with respect to the variable  $\lambda_B$  ( $t = 8760 \text{ h}$  and  $\lambda_A = 0.00017 \text{ h}^{-1}$ )

Figure 8 demonstrates that, with reference to the failure rate  $\lambda_A$ , the PAND gate keeps behaving as a coherent system ( $\frac{\partial P(X_4)}{\partial \lambda_A} > 0, \forall \lambda_A \in [0, 10^{-1}] \text{ h}^{-1}$ ) and an increase of the failure rate of

component A turns in the increase of the PAND gate unreliability. Conversely, Figure 9 shows that values of failure rate higher than  $1.09 \times 10^{-2} \text{ h}^{-1}$  make the system behaving incoherently ( $\frac{\partial P(X_4)}{\partial \lambda_B} < 0$ ).

#### 4. CONCLUSIONS

This short communication discusses the incoherence nature of the PAND gate, one of the most important and utilised gates of Dynamic Fault Tree analysis. The incoherence of the PAND gate emerges due to the existence of the safe state in which the system sojourns in case the events do not trigger in the order specified by the failure logic (from left to right).

In this paper, a 2-input PAND gate for non-repairable and repairable components has been analysed. To simplify the experimental scenario, failure and repair times of occurrence have been set so as to follow the exponential distribution of probability. Results have shown that the failure probability of a PAND gate can present a maximum value; therefore the increase of the reliability of the input components does not always result in an increase of the gate reliability. This behaviour has been revealed for the PAND gate with non-repairable components and for a PAND gate in which the second input component can be repaired only if it fails before the first one. Conversely, the PAND gate with repairable components behaves always as a coherent system.

The coherence analysis may identify a useful region for optimization and sensitivity analysis purposes, and in order to better interpret the results of dynamic dependability models. To be aware of this behaviour, in particular when it is required to perform an improvement of the system reliability, it is suggested to identify the coherence region of operation, studying the positivity of the partial derivative of the failure probability function with respect to the input parameters. This method is not always feasible because the quantification of the closed analytical solution of the PAND gate can be tedious, in particular when systems present non-exponential distributions of probability and repairable components. In this latter case, a well-tuned simulation campaign can help into the identification of approximate boundaries.

#### References

1. Avizienis A, Laprie JP, Randell B, Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Volume 1 Issue 1, January 2004 Page 11-33.
2. Dugan JB, Bavuso SJ, Boyd MA. Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems, IEEE Transactions on Reliability, Vol. 41, No. 3, 1992 September.
3. Yevkin O. An Efficient Approximate Markov Chain Method in Dynamic Fault Tree Analysis, Quality and Reliability Engineering International, 32: 1509–1520.
4. Volk M, Junges S, Katoen JP. Advancing Dynamic Fault Tree Analysis - Get Succinct State Spaces Fast and Synthesise Failure Rates, (2016), Computer Safety, Reliability, and Security, Volume 9922 of the series Lecture Notes in Computer Science pp 253-265.
5. Merle G, Roussel JM, Lesage JJ. Quantitative Analysis of Dynamic Fault Trees based on the Structure Function. Quality and Reliability Engineering International, Wiley, 2014, 30 (1), pp. 143-156.
6. Ge D, Lin M, Yang Y, Zhang R, Chou Q. Quantitative Analysis of Dynamic Fault Trees Using Improved Sequential Binary Decision Diagrams, Reliability Engineering and System Safety, 2015.

- 1
  - 2
  - 3
  - 4
  - 5
  - 6
  - 7
  - 8
  - 9
  - 10
  - 11
  - 12
  - 13
  - 14
  - 15
  - 16
  - 17
  - 18
  - 19
  - 20
  - 21
  - 22
  - 23
  - 24
  - 25
  - 26
  - 27
  - 28
  - 29
  - 30
  - 31
  - 32
  - 33
  - 34
  - 35
  - 36
  - 37
  - 38
  - 39
  - 40
  - 41
  - 42
  - 43
  - 44
  - 45
  - 46
  - 47
  - 48
  - 49
  - 50
  - 51
  - 52
  - 53
  - 54
  - 55
  - 56
  - 57
  - 58
  - 59
  - 60
7. Rao KD, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, Srividya A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment, *Reliability Engineering & System Safety*, Volume 94, (2009) 872–883.
  8. Manno G, Chiacchio F, Compagno L, D'Urso D, Trapani N. Conception of Repairable Dynamic Fault Trees and resolution by the use of RAATSS, a Matlab® toolbox based on the ATS formalism. *Reliability Engineering & System Safety* Volume 121, January 2014, Pages 250–262.
  9. Rauzy A, Dutuit Y. Exact and truncated computations of prime implicants of coherent and non-coherent fault, *Reliability Engineering and System Safety* 58 (1997) 127-144.
  10. Aizpurua JI, Papadopoulos Y, Muxika E, Chiacchio F, Manno G. On Cost-effective Reuse of Components in the Design of Complex Reconfigurable Systems, *Quality and Reliability Engineering International*, 2017.
  11. Ruijters E, Stoelinga M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, *Computer Science Review*, Volumes 15–16, 2015, Pages 29–62.
  12. Andrews JD. The use of not logic in fault tree analysis, *Quality and Reliability Engineering International*, 2001; 17: 143–150.
  13. Contini S, Cojazzi GGM, Renda G. On the use of non-coherent fault trees in safety and security studies, *Reliability Engineering & System Safety*, Volume 93, Issue 12, December 2008, pp. 1886–1895.
  14. Lazakis I, Turan O, Aksu S. Increasing ship operational reliability through the implementation of a holistic maintenance management strategy, 2010, *Ships and Offshore Structures*, vol 5, no. 4, pp. 337–357.
  15. Hong Y, Meeker WQ. Confidence interval procedures for system reliability and applications to competing risks models, *Lifetime Data Analysis*, 2014, Volume 20, Issue 2, pp. 161–184.
  16. Liu D, Chen XJ, Li Y, Zhao ZW, Li XM. Dynamic Fault Trees Analysis for Importance Measures Based on Cut Sequence Set Model, *Applied Mechanics and Materials*, Vol. 232, pp. 578-582, 2012.
  17. Ou Y, Dugan JB, Sensitivity Analysis of Modular Dynamic Fault Trees, *Proc. Computer Performance and Dependability Symp. (IPDS '00)*, pp. 35-43, 2000.
  18. Aizpurua JI, Catterson VM, Papadopoulos Y, Chiacchio F, Manno G. Improved Dynamic Dependability Assessment through Integration with Prognostics, *IEEE Transactions on Reliability*, pp. 1-21, Issue: 99, 2017.
  19. Chiacchio F, D'Urso D, Manno G, Compagno L. Stochastic hybrid automaton model of a multi-state system with aging: Reliability assessment and design consequences, *Reliability Engineering & System Safety* 149, 1-13, 2016.
  20. Chiacchio F, D'Urso D, Compagno L, Pennisi M, Pappalardo F, Manno G. SHyFTA, a Stochastic Hybrid Fault Tree Automaton for the modelling and simulation of dynamic reliability problems, *Expert Systems with Applications* 47, pp. 42-57, 2016.
  21. Fussell JB, Aber EF, Rahl RG. On the Quantitative Analysis of Priority-AND Failure Logic, *IEEE Transactions on Reliability*, Volume: R-25, pp. 324-236, Issue: 5, 1976.
  22. Chiacchio F, Cacioppo M, D'Urso D, Manno G, Trapani N, Compagno L. A Weibull-based compositional approach for hierarchical dynamic fault trees. *Reliability Engineering & System Safety* 109, 45-52, 2013.
  23. Pham H. *System Reliability Concepts*, *System Software Reliability*, Springer Series in Reliability Engineering (2006), 9-75, Springer London.