24th COBEM - 2017

24th ABCM International Congress of Mechanical Engineering
December 3-8, 2017, Curitiba, PR, Brazil

COBEM-2017-2054
RELIABILITY ANALYSIS BY DYNAMIC FAULT TREES - A CASE STUDY IN SEWAGE TREATMENT SYSTEMS

Celso Luiz Santiago Figueirôa Filho
Industrial Engineering Program, Federal University of Bahia, Polytechnic School, Salvador, Brazil
celso@g-rams.br
Edilson Machado de Assis
Lucas Jordi Nascimento da Silva
Ana Luiza Brasileiro Costa
Institute of Exact Sciences and Technologies, Catholic University of Salvador, Salvador, Brazil
edilsonassis@gmail.com
lucasjordi@hotmail.com
eng.analuizabrasileiro@gmail.com

Abstract. *Fault trees (FT) are an important reliability analysis tool. Dynamic fault trees (DFT) are extensions of this method capable of describing scenarios where dependability is crucial. The objective of this article is to compare the results in terms of unreliability and failure rate obtained by a FT and a DFT. A real practical example based on a sewage treatment system was used. The FT was developed to describe the tank overflow event, and details of system behavior were discussed through interviews with the company's experts. The 1^{st} and 2^{nd} order minimum cuts were defined and their basic events were specified by Weibull distributions. Some operating situations were improperly described and a DFT was prepared to cover these non-combinational conditions. Finally, the probability of failure and the failure rate were calculated as a function of time by closed mathematical expressions. A detailed graphical analysis of all events of both trees (FT and DFT) was performed. The results show that the results of the analyzes can lead to mistaken managerial actions and that the DFTs should be preferred although there is a little computational increment to its solution.*

Keywords: *reliability, fault tree, sewage treatment, environment impact*

1. INTRODUCTION

Urban areas have a complex network of sewage treatment systems. Such systems shall maintain continuously a safe operation of urban sanitary sewage. The suitable level of reliability of these systems is necessary in order to guarantee both low risks to the health of its users and acceptable levels of environmental contamination. These systems have, as central industrial installation, motor-pump assemblies that must operate with minimum failures. The demand for operationally reliable installations has driven companies to the use of reliability tools.

Failure Tree analysis method initially addresses qualitatively to the system reliability, directing installation weaknesses. Subsequently, accumulated failure functions are linked to each event and the branches of the tree generate probabilistic function from combination of failures.

Fault Trees (FT) are structures that use Boolean gates to represent the way a component failure produces a system failure (Vesely *et al.*, 1981). Fault trees can be analyzed in several ways and can also be converted to other methodologies, such as Binary Decision Diagrams (BDD) (see (Jinglun and Quan, 1998)). A Fault Tree can be converted directly into a Bayesian Network (BN) and the basic inference techniques of a BN can be used to obtain the classic parameters of a Fault Tree (Bobbio *et al.*, 2001).

DFTs are extensions of the FTs. DFTs are used due to the ability to model dependence between failure events. A DFT uses the traditional OR, AND, and KofN gates present in the FTs but include four other ports: PAND, PDEP, WSP, and SEQ. These gates add the ability to model dependencies such as sequence failures, failures that are triggered by a specific event, and arrangement with main and spare components. DFTs provide fault analyses that are applicable to both fault tolerant systems and non-tolerant systems. Fault-tolerant systems can actively respond to failures and errors. They are programmed to anticipate certain types of failures and errors and include detection, recovery or reconfiguration techniques (Doyle and Dugan, 1995).

Markov models are commonly used to solve dynamic gates. These models suffer from two main limitations: the restriction of the use of exponential distribution and the fact that they are explosive when the number of tree events increases greatly. Guo *et al.* (2011) propose the application of Weibull in a Markov model with the purpose of quantitatively evaluating a DFT.

Xing *et al.* (2011) present an analytical method based on a binary sequential decision diagram. In this way they intend to accurately calculate the reliability of non-repairable dynamic systems subject to sequence failure. The model also solves combinatorial relations of events with any distribution

One of the main differences between FT and DFT is that, in the latter tree, the sequence of failures can be considered. The mathematical modeling of sequentiality can be done in an exact way or by simulation, among other methods. Long *et al.* (2000) applied Monte Carlo simulation in sequential fault analysis comparing the results to the exact calculation performed by multiple integrations. Merle *et al.* (2010) defined events as temporal variables, and with the creation of two temporal operators, it modeled the ports with priority. A DFT is also capable of modeling safety and security systems in which an equipment may fail in operation or in standby mode. In this paper we created a formalism in order to represent the Dynamic Fault Tree by means of closed mathematical expressions. Although the DFTs are expressed by a relatively old formalism, Rauzy and Blériot-Fabre (2015) studied the semantics of DFTs and related formalisms.

The aims of this paper are to show a description of the pumping system, to present the main differences between FT and DFT, to recognize dynamic gates structures in the system, and to compare the results of both two fault tree analyses. DFT was calculated by closed mathematical expressions using the Weibull distribution. The real context explored in this paper generated others papers about system reliability and data collect process, including applications of dynamic fault trees. Those paper will be published soon and are complementary to this paper.

2. PUMPING SYSTEM CHARACTERISTICS

The system analyzed is a typical elevation pumping station for sewage systems in urban areas. Also some sewage treatment stations were included because the design solution and application are very similar. The whole system covers an area of 4,000 km^2 with 22 stations. The systems are composed of two pumps with electrical motors, an electrical command system, a tank and instrumentation for level and flux.

Maintenance reports were used to generate the input data for this work. All maintenance actions are first opened in the form of a Maintenance Order in this system and then performed. After the service runs, the supervisors close the Orders or send them to the maintenance planners to close them on the system with the runtime information. The fault definition may have its origin in the maintenance, operation or engineering teams.

3. FAULT TREES AND DYNAMIC FAULT TREES

Fault Tree analysis are elaborated as a general description of how a system reacts when something fails. AND, OR, PDep and PAnd gates were used in order to model the studied case.

AND gate output results failed state if all its entries are faulty. This gate represents a component association in parallel if the function of interest is unreliability. The resulting reliability in an AND gate due to the unreliabilities of its input components is expressed by:

$$AND_{list}(t) = \prod_{j=1}^{n} F_{list_j}(t)\,, \tag{1}$$

where $list$ is a set of indexes representing all input components of the AND gate, n is the total number of gate inputs and t is the time instant.

The representation of AND gate with n inputs is shown in Fig. 1.

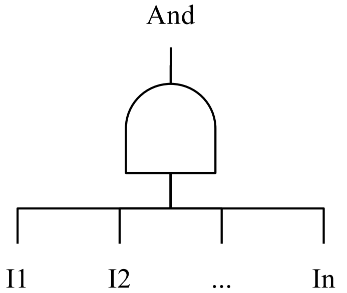

Figure 1. Symbolic representation of an AND gate.

OR gate results in a failed state if at least one of its inputs fails. This port represents a series association and produces failed state if one or more components fail. The cumulative distribution function for OR gate is expressed by:

$$OR_{list}(t) = 1 - \prod_{j=1}^{n} \left[1 - F_{list_j}(t)\right] \ , \tag{2}$$

where t is the time instant, n is the number of port entries and $list$ is a set with the identification indexes of all port input components. The Fig. 2 shows an OR gate.

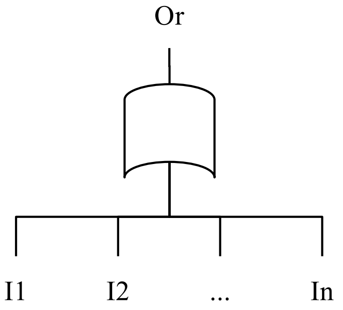

Figure 2. Representation of an OR gate.

Probabilistic dependency (PDep) gate represents an association that a trigger event (T) induces failure on dependent components, whatever their operational states (faulty or not faulty). Every time a trigger event occurs, its dependent components fail with probability $p_d \leq 1$. The component failure has no influence on the trigger event. The probability of occurrence of the trigger event is $F_T(t)$.

The failure probability of i-th component at time t is $F_i(t)$. The probability of a component fails exclusively due to the trigger is p_d, so the probability of failure for each PDep component is:

$$PDep_i(t) = F_i(t) + \left[1 - F_i(t)\right] F_T(t) p_d, \tag{3}$$

Figure 3 shows a PDep gate with its inputs, output and trigger event.

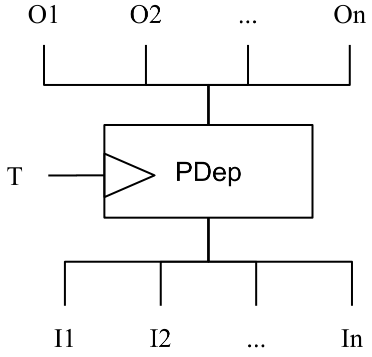

Figure 3. Graphical representations of PDep gate.

Priority And (PAnd) results in failed state if all of its entries fail in a predefined order. The main difference between the PAnd and And gates is that in And the failure of all their inputs generates output failure whereas in a PAnd it is necessary that the faults to occur in a specified order, although any order is possible to occur. The probability of item 1 failures before item 2 is defined as:

$$PAnd_{1,2}(t) = \int\limits_{x=0}^{x=t} f_2(x) F_1(x) dx \tag{4}$$

where $F_1(x)$ is the failure probability of item 1 at x and $f_2(x)$ is the value of probability density function at x for item 2. The graphical representation of PAnd is shown in Fig. 4.

4. FT AND DFT CASES

The top event chosen was *Overflow of the sewage tank not treated for the environment*. This sentence will henceforth be called *overflow*.

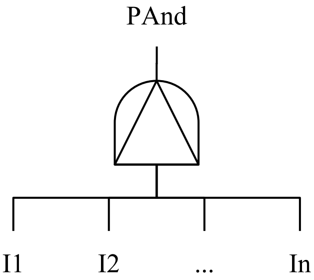

Figure 4. Graphical representation of a Pand gate.

An analysis of the basic events was developed and the fault tree was built. Figure 5 shows the graphical representation of the fault tree in terms of static gates and events partially detailed. The 1^{st} and 2^{nd} orders cuts of the system were listed. These order cuts drove directly to the top event. The FT shows many OR gates so the vulnerabilities of the system and the possibilities to create barriers for these weaknesses were discussed at this moment in order to support design changes of the system.

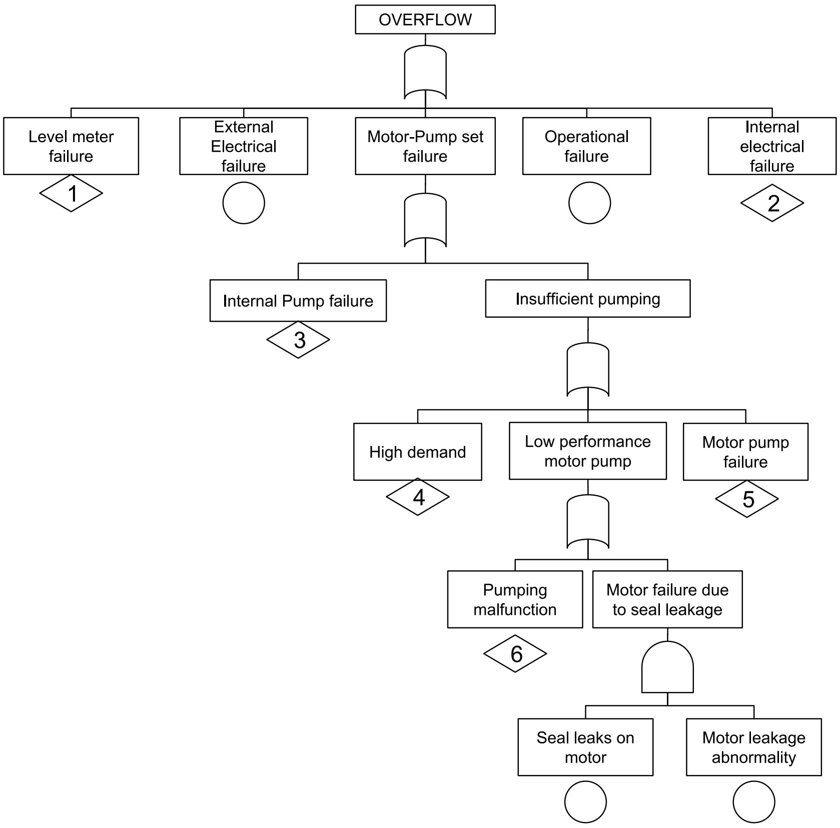

Figure 5. Static FT.

It was observed that *Insufficient pump* event has originated in 3 events: i) High demand of the system, ii) Low performance of the motor-pump, and iii) Motor-pump failure.

We have done interviews with the experts of the system. These interviews allowed to improve our understanding about the behavior of a fail or a combination of them. At this step the borders of the system was well defined and some events were eliminated since they were out of the team's control. An example of this is the loss of electrical energy supplied by external companies.

The unreliability function for each basic event is needed to find the probability of occurrence of the Top Event. This estimation process used three sources: (i) company history of failures; (ii) similar failure mode for the similar equipment found in other industries; and (iii) expert estimation by interviews.

The basic events of each input were modeled according to the Weibull distribution. This mathematical model is well used to explain electromechanical failures and is composed by three parameters, for shape, life characteristic and time localization. Distribution fittings were made by coefficient of determination maximization method for events with historical data. Data banks and specialist knowledge were used for the other situations. Table 1 shows the parameters of the distributions.

Table 1. Weibull parameters for each failure mode at Fig. 5

i	β	η(days)	t_0(days)	Failure mode
I1	1.4	416.66	0	Seal leaks on motor
I2	1.2	1940	0	Motor leakage abnormality
I3	1	1000	0	Pumping malfunction
I4	1	85	20	High demand
I5	2.89	24.74	-29	Motor pump failure
I6	3.2	163	0	Internal pump failure
I7	1	583	0	Level meter failure
I8	2.5	3500	0	External electrical failure
I9	1	4500	0	Operational failure
I10	4	1500	0	Internal electrical failure

High Demand scenario are difficult to estimate because it varies seasonally, daily, by weather changes, by the population social conditions, by the number of houses attended by the installation, due to the installation localization, and due to the contamination of the system caused by the wastewater and rain collector systems.

Then events combinations that needed the dynamic gates of the DFT were conducted. A Dynamic Fault Tree was drawn. The DFT with dynamic gates is presented in Fig. 6 An estimation of the failures probabilities functions $(F(t))$ were created for all scenarios identified by the DFT.

The concepts of High demand and Low performance are interconnected, as well as the failure of the motor-pump assembly. The performance of the motor-pump assemblies will be considered low if demand exceeds its level. The motor pump will be failure if it does not meet the required demand. Thus the high demand is the trigger that causes the failed state in the low performance and motor pump inputs.

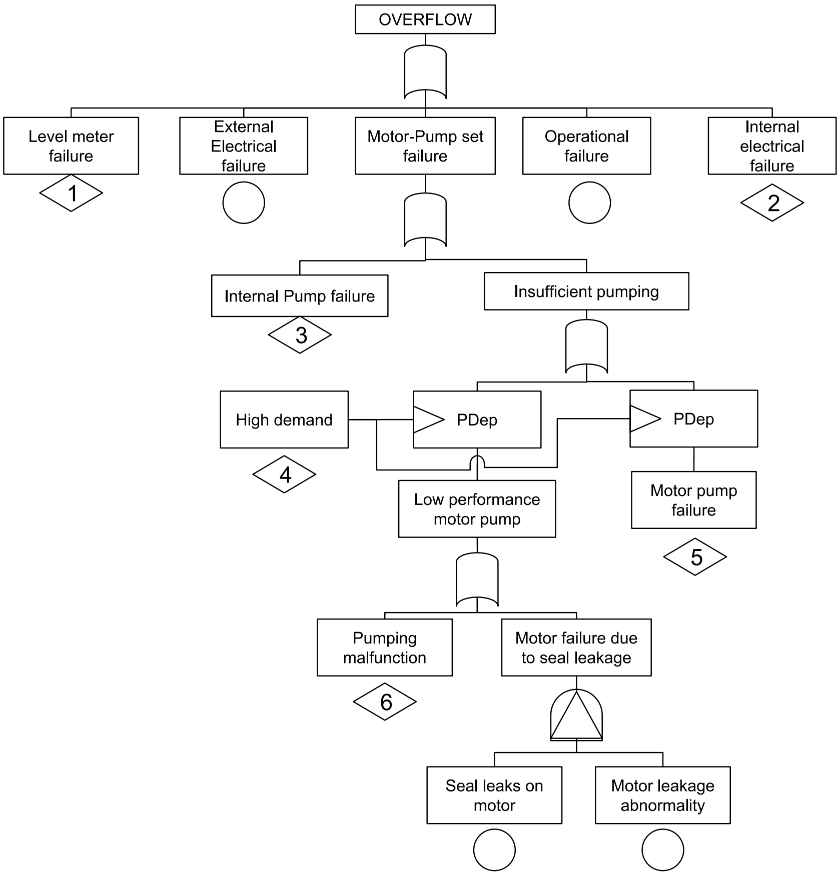

Figure 6. DFT representation for the system.

The Motor failure due to Seal leakage event was modeled in two different ways. In order to model the FT, it was used an AND gate for the basic events *Seal leaks on the motor* and *Motor failed due to seal leak.* In the DFT, the sequence of events matters and the Pand gate outputs fail only when the seal leaks before the motor protection fails.

Figure 7 shows that failure probability curves deviate as time increases. During all time intervals, the Pand gate gives lower unreliability values. The difference reaches 20% for values close to 6000 days.

The failure rate functions curves have very different formats. While Pand port responds with a unimodal format (inverted U), AND returns a unimodal-increasing behavior, which increases failure rate, as t grows above 2,000 h. The AND failure rate is always greater than the calculated Pand and for 6,000 days the difference is higher than 600% (see Fig. 7).

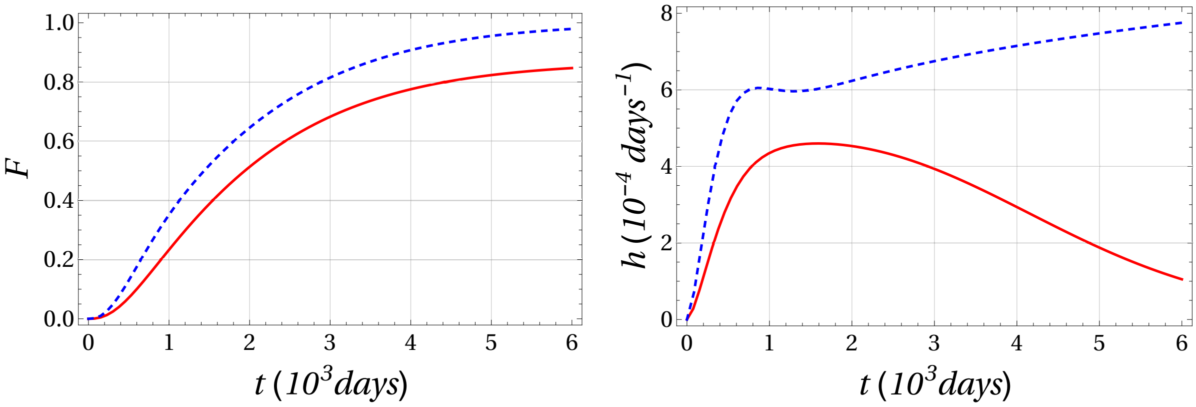

Figure 7. Motor failure due to Seal leakage event curves for DFT plotted in red-continuous line and for FT in blue-dashed line. Left panel: probability of failure $F(t)$. Right panel: failure rate $h(t)$.

For the Low performance motor pump event, unreliability curves are quite near as can be seen in Fig. 8. This is caused by *Pumping Malfunction* event below the *Low Performance Motor Pump* event in a OR gate that reduces the influencing of *Motor Failure* event. It should be noted that the failure rate shapes are very similar to the ones found at Fig. 7. This is due to the fact that *Pumping Malfunctioning* has been characterized as constant failure rate ($\beta = 1$) so its influence in the shape is practically null.

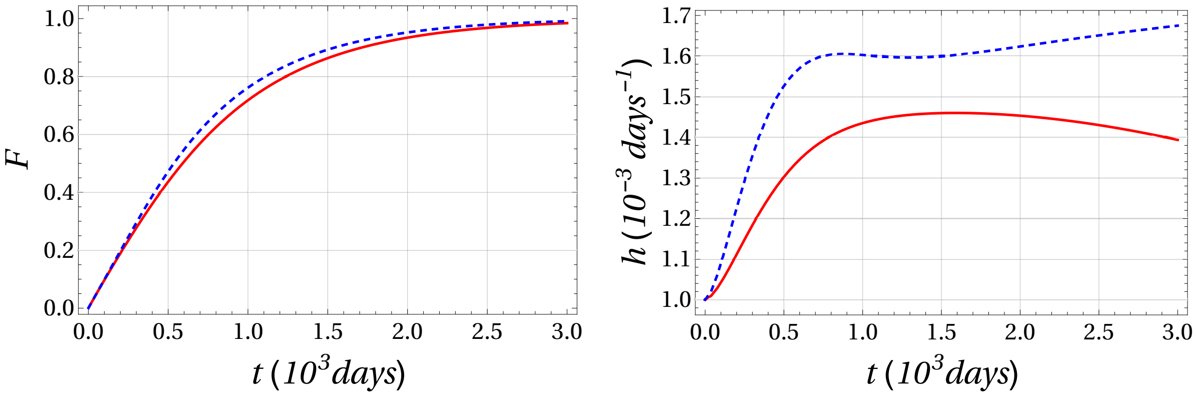

Figure 8. Low performance motor pump event curves for DFT drawn in red-continuous line and FT in blue-dashed line. Left panel: probability of failure $F(t)$. Right panel: failure rate $h(t)$.

The unreliability curve of *Insufficient Pumping* event increases faster than the result of *Low performance motor pump* event as show at (Fig. 9). Note that $F(t)$ is approximately 1 at 60 days whereas in Fig. 8 it occurs at 3,000 days. The Motor Pump Failure event is responsible for this effect. The step in the failure rate function is due to the *High Demand* event with its minimum life t_0 different from zero. This behavior occurs because *High Demand* event was modeled with location parameter $t_0 = 20$ days. Equation (2) and Eq.(3) explain the level difference between the steps. Pdep gate was used in DFT modeling and OR gate carried out the results in FT.

The parameter life characteristic η for *Internal pump failure* event ($\eta \approx$163 days) values more than six times the same parameter of Motor pump failure event ($\eta \approx$25 dias). This difference is high enough to justify that the influence of this additional event (*Internal pump failure*) on Or gate is practically imperceptible when Fig. 9 and Fig. 10 are compared.

Figure 11 shows the the results for the top event *Overflow*. The latest events added in the fault tree analysis (Level meter failure, External electrical failure, Operational failure e Internal electrical failure) have characteristics life higher than 500 days. The shape parameter of all these latest event are equal or higher than 1, so there is no effect of decrease failure rate being added and also no vertical asymptotic behaviour in $h(t)$ graph. In these cases the shapes of the curves are maintained very similar to the shapes of the events shown in Fig 9 and 10.

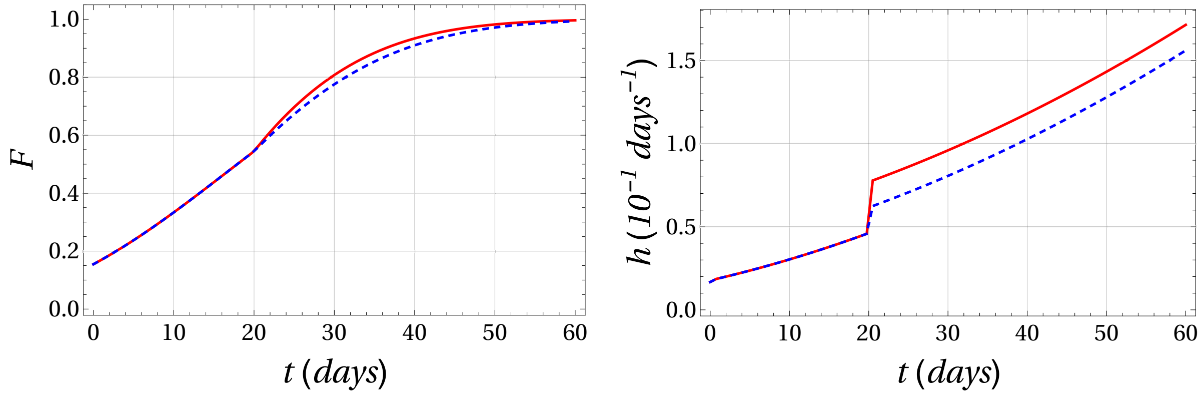

Figure 9. Insufficient pumping event curves for DFT drawn in red-continuous line and FT in blue-dashed line. Left panel: failure probability $F(t)$. Right panel: failure rate $h(t)$.

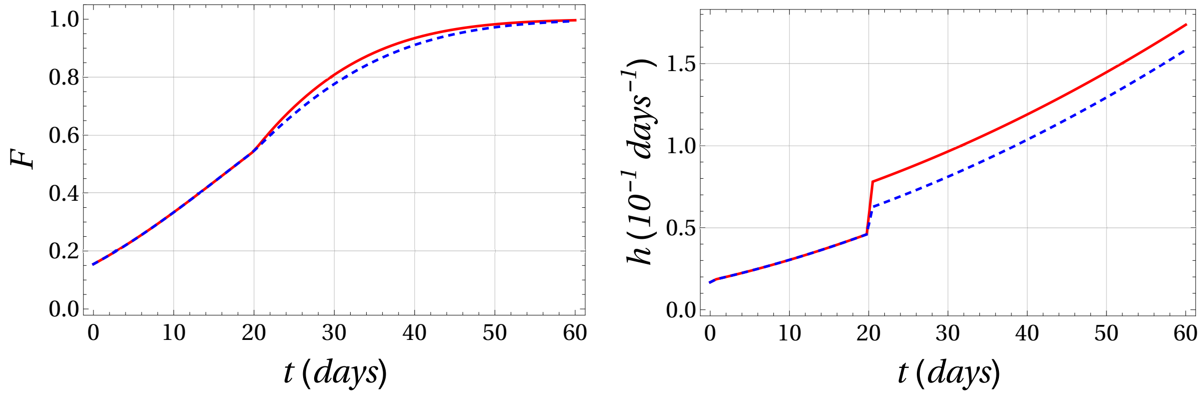

Figure 10. Motor-Pump set failure event curves for DFT drawn in red-continuous line and FT in blue-dashed line. Left panel shows probability of failure $F(t)$ curves and right panel presents failure rate $h(t)$ plots.

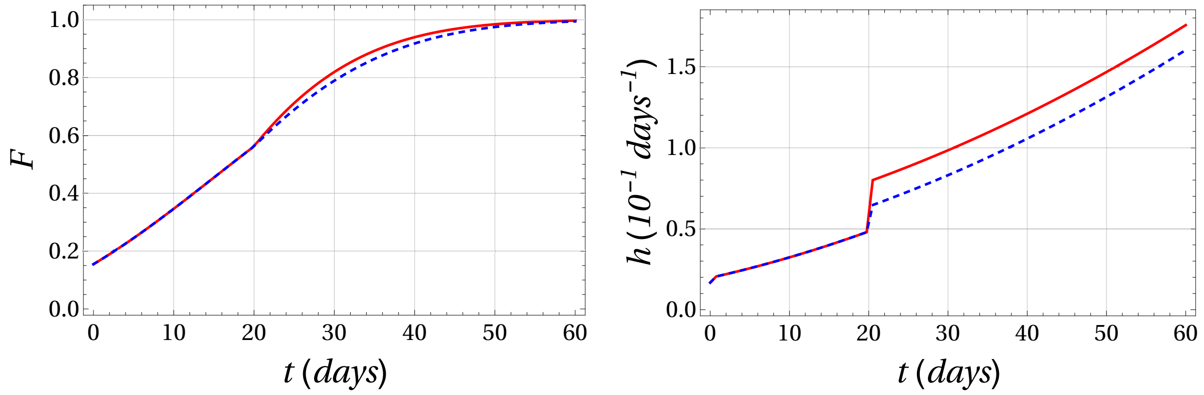

Figure 11. Top Event Overflow curves for DFT drawn in red-continuous line and FT in blue-dashed line. Left panel: probability of failure $F(t)$. Right panel: failure rate $h(t)$.

5. CONCLUSIONS

Building a dynamic or static fault tree involves a series of steps to gain an adequate knowledge of the system. Interviews with persons responsible for the system, the search for historical time-to-failure data and even the query to the databases of equipment failures are necessary for the definition of the events of a fault tree.

The calculation steps of an FT or DFT in which the failure probability and failure rate functions are determined allow us to progressively know the influence of each event on the composition of the top event. In this paper, the DFT was entirely calculated by closed mathematical expressions.

The case discussed in this paper shows that the use of static gates (AND and OR) leads to different results than those produced when dynamic gates (PAnd and PDep) are introduced. The existence of several first order cuts in the fault trees (FT and DFT) reduced the differences between the values obtained in the two methodologies, but this result can not be extended to any system.

The concepts that define the expressions of the PDep and OR gates are quite different. While the PDep causes the state to fail in its inputs when the trigger event occurs, the OR gate produces failed state if at least one input is failed. The parameters of the distributions that model the events can accentuate or reduce this conceptual difference. In this case, the PDep port applied in the *Insufficient pump* event slightly changed the graphical results when compared to the OR gate.

The PAnd port applied to the *Motor failure* event led to very different results from those found with the AND gate. The requirement of sequential failure of inputs to produce the failed state in output, changes the failure probability values by 20%. The changes in failure rates are even greater.

The sewage treatment system in urban areas in Brazil has a continuous growing. This dynamic changes system reliability and interferes in design of the solution. Many elements of a facility unit influence the failure modes of other one in the same system. DFTs demonstrate that can represent better these situations.

The case study observed in this paper can be applied in many others industrial systems that has similar situations, therefore a DFT modeling can be more useful than the traditional static FT.

6. REFERENCES

Bobbio, A., Portinale, L., Minichino, M. and Ciancamerla, E., 2001. "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks". *Reliability Engineering and System Safety*, Vol. 71, pp. 249–260.

Doyle, S.A. and Dugan, J.B., 1995. "Dependability Assessment using Binary Decision Diagrams (BDDs)". In FTCS-25, ed., *Twenty-Fifth International Symposium on Fault-Tolerant Computing, 1995*. doi:10.1109/FTCS.1995.466973.

Guo, W.G., Han, W. and Liu, S.Y., 2011. "Dynamic Fault Tree Based on Weibull Distribution". *Advanced Materials Research*, Vol. 308-310, pp. 1322–1327. ISSN 1662-8985. doi:10.4028/www.scientific.net/AMR.308-310.1322. URL `http://www.scientific.net/AMR.308-310.1322`.

Jinglun, Z. and Quan, S., 1998. "Reliability analysis based on binary decision diagrams". *Journal of Quality in Maintenance Engineering Cybernetics*, Vol. 4, No. 2, pp. 150–161.

Long, W., Sato, Y. and Zhang, H., 2000. "Monte Carlo simulation for analysis of sequential failure logic". *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences*, Vol. E83A, No. 5, pp. 812–817.

Merle, G., Roussel, J.M., Lesage, J.J. and Bobbio, A., 2010. "Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events". *Reliability, IEEE Transactions on*, Vol. 59, No. 1, pp. 250–261.

Rauzy, A. and Blériot-Fabre, C., 2015. "Towards a sound semantics for dynamic fault trees". *Reliability Engineering and System Safety*, Vol. 142, pp. 184–191. ISSN 09518320. doi:10.1016/j.ress.2015.04.017. URL `http://dx.doi.org/10.1016/j.ress.2015.04.017`.

Vesely, W.E., Goldberg, F.F., Roberts, N.H. and Haasl, D.F., 1981. "Fault Tree Handbook".

Xing, L., Shrestha, A. and Dai, Y., 2011. "Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures". *Reliability Engineering and System Safety*, Vol. 96, No. 10, pp. 1375–1385. ISSN 09518320. doi:10.1016/j.ress.2011.05.007. URL `http://dx.doi.org/10.1016/j.ress.2011.05.007`.

7. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.