Static Fault Tree versus Dynamic Fault Tree gates - A case study in sewage treatment systems

C.L.S. Figueirôa Filho[1], E. M. Assis[2], A. L. B. Costa[2], L. S. Jordi[2],

[1] *Universidade Federal da Bahia,*
Postgraduate Program in Industrial Engineering, Salvador, Brazil
[2]*Universidade Católica do Salvador, Department of Mechanical Engineering, Salvador, Brazil*

e-mail: celso@g-rams.br

Abstract: The impact for environmental preservation of sewage treatment systems reliability is significant. Fault Tree Analysis (FTA) is a well-used method for reliability engineers but cannot express some dynamic behaviours of the system. Dynamic Fault Tree Analysis (DFTA) can describe some real scenarios that is not possible by static analysis. The aim of this paper is to compare between the application of static Fault Tree (FT) and Dynamic Fault Tree (DFT) analyses for a sewage treatment system. First, a static Fault Tree (FT) was elaborated in order to describe the tank overflow failure mode. Second, interviews with the company experts were carried out to detail the system's behaviour. Next, the 1st and 2nd orders cuts were identified. Each basic event was defined and the probability of failure for each branch of the fault tree was formulated. Some operating conditions in which static gates do not represent the reality have been found. Then, the necessity for DFT gates were identified. Finally, failure probability was calculated by DFT and was compared to the FT. The paper concluded that DFT modelling represents real scenarios better than the FTA in this case and probably in many others industrial systems,.
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 reliability of these systems is necessary 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 that a component failure produces a system failure [1]. Fault trees can be analyzed in several ways and can also be converted to other methodologies, such as Binary Decision Diagrams (BDD) (see [2]). 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 [3].

DFTs are extensions of the FTs. DFTs are used due to the ability to model dependence between failure events. 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 [4]. 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 an specific event, and arrangement with main and spare components.

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. Monte Carlo simulation was applied by [5] in sequential fault analysis comparing the results to the exact calculation performed by multiple integrations. Events were defined in [6] 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, [7] studied the semantics of dynamic failure trees and related formalisms.

2. PURPOSE

The aim of this paper is to compare between the application of static Fault Tree (FT) and Dynamic Fault Tree (DFT) analyses for a sewage treatment system. First, a static Fault Tree (FT) was elaborated in order to describe the tank overflow failure mode. Second, interviews with the company experts were carried out to detail the system's behaviour. Next, the 1st and 2nd orders cuts were identified.

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.

3. FAULT TREES AND DYNAMIC FAULT TREES

Fault Tree analysis are elaborated as a general description of how a system reacts when something fails. The top event chosen was 'Overflow of the sewage tank not treated for the environment'.

We have done interviews with the experts of the system. These interviews allowed to improve our understanding about the behaviour of a fail or a combination of them. At this step the borders of the analysed 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 1st and 2nd orders cuts of the system were listed. These order cuts drove directly to the top event. The vulnerabilities of the system and the possibilities to create barriers for these weaknesses were discussed at this moment.

The unreliability value 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 equipment found in other industries and (iii) expert estimation by interviews. So the probability of the top event was estimated and compared with the real historical data.

Then events combinations that needed the dynamic ports of the DFT were conducted. A new Dynamic Fault Tree was drawn. The DFT with dynamic gates is partially presented in Figure 1. An estimation of the failures probabilities Cumulative distribution functions ($F(t)$) were created for all scenarios identified by the DFT. Only the modified branches were presented in this paper in order to show the application of the dynamic ports.

3.1 Probabilistic formulation

AND

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

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

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 Figure 1

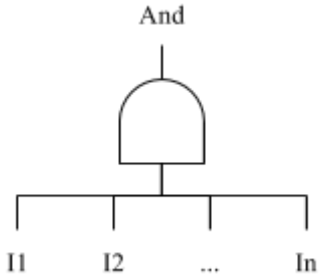

Figure 1 - Symbolic representation of an AND gate.

OR

The OR port 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 the OR gate is expressed by:

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

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

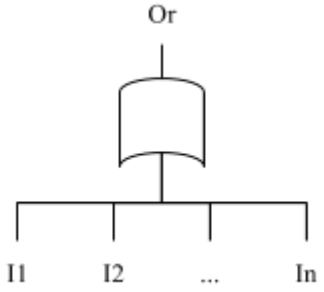

Figure 2 - Representation of an OR gate.

PDep (Probabilistic dependency)

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

$$PDep_i(t) = F_i(t) + \left[1 - F_i(t)\right] F_T(t) p_d . \quad (3)$$

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

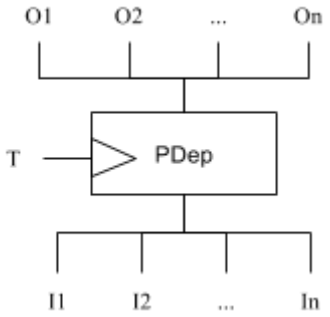

Figure 3 - PDep port.

PAnd (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 ports 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:

$$PAnd_{1,2}(t) = \int_{x=0}^{x=t} f_2(x) F_1(x) dx , \quad (4)$$

where $F_1(x)$ is the failure probability of item 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 Figure 4.

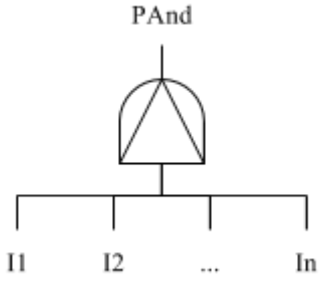

Figure 4 - Graphical representation of a Pand port.

4. RESULTS AND DISCUSSION

4.1 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 km² 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.

4.2 FT And DFT Cases

An analysis of the basic events was developed and a fault tree was built. It was observed that insufficient pump has originated in 3 events: low performance of the motor-pump assemblies, high demand of the system and failure of the motor-pump assembly.

Figure 5 shows the graphical representation of the fault tree in terms of static ports. The basic events of each input were modeled according to the Weibull distribution. Distribution fittings were made by least squares 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.

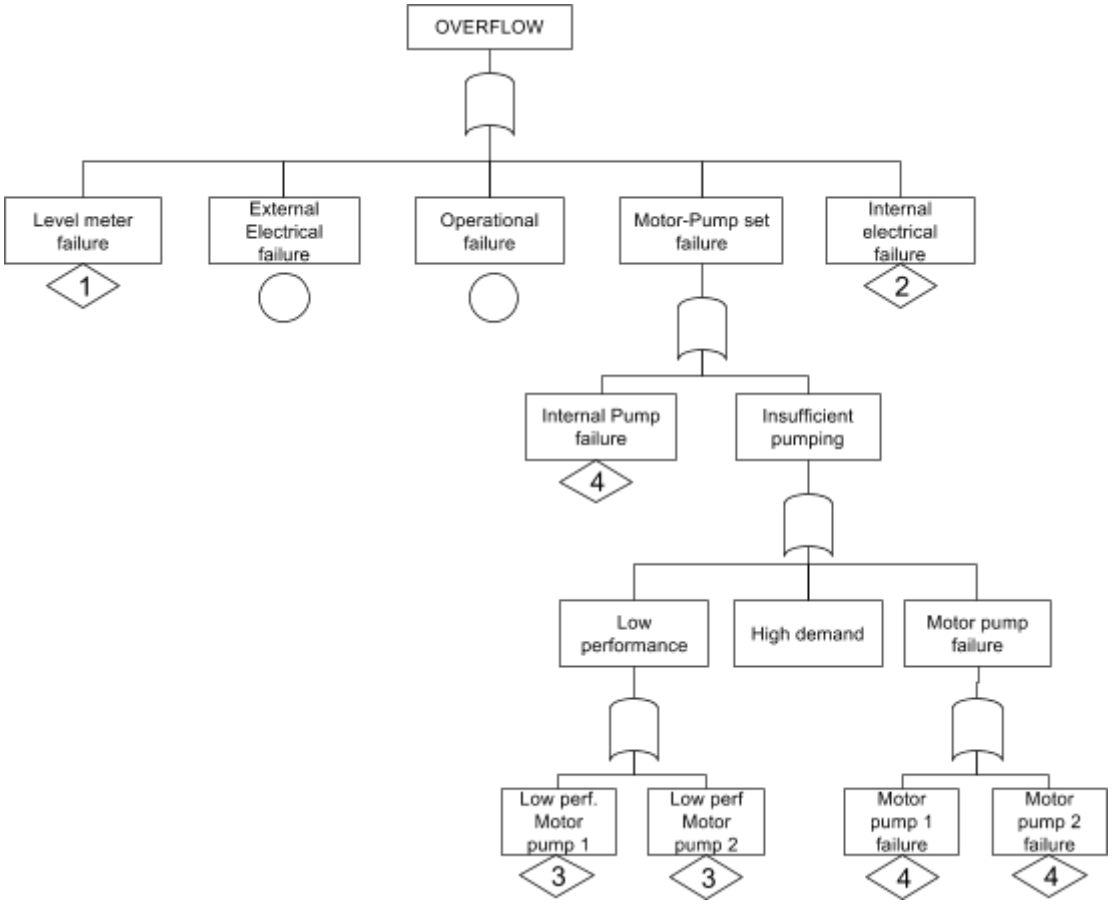

Figure 5 - Static FT version for events shown in Fig. 1

Table 1. Weibull parameters for each failure mode at Figure 1 FTA

	β	η (days)	t_0 (days)	Failure mode
I1	0.890624	174.972	114.144	Low performance motor pump 1
I2	0.890624	174.972	114.144	Low performance motor pump 2
I3	2.891311	24.741	-29	Motor pump 1 failure
I4	2.891311	24.741	-29	Motor pump 2 failure
I5	1	85	20	High demand
I6	2.08623	159.143	-48.595	Internal pump failure
I7	1.0	583.00	0	Level meter failure
I8	1.1	1150.00	0	External electrical failure
I9	1.6	47.880	0	Operational failure
I10	0.6	75.1389	1.736	Internal electrical failure

High Demand scenarios 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.

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.

The DFT representation is shown in Figure 6 where the PDep port models the low performance and motor pump failures according to the high demand trigger event.

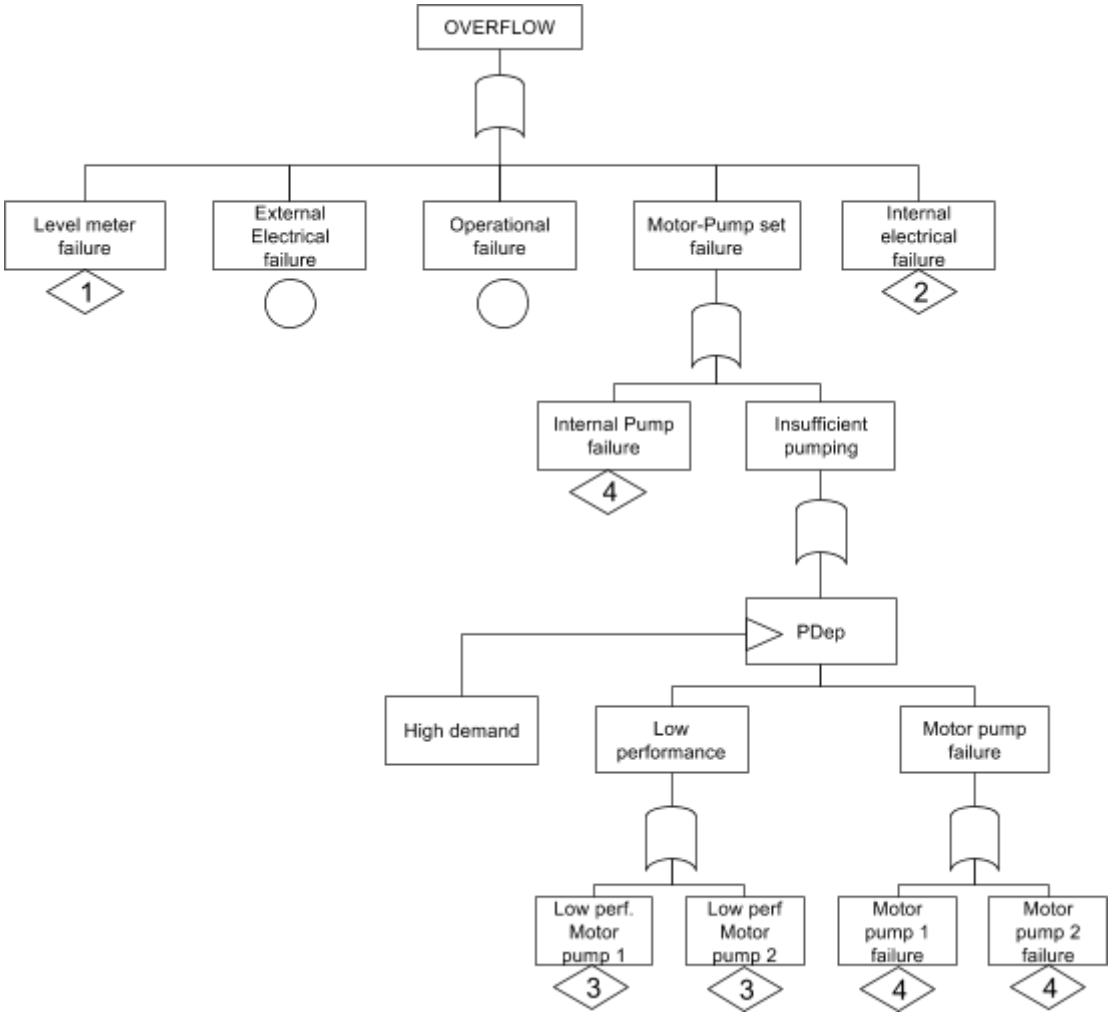

Figure 6 - DFT with the dynamic port PDep.

The failure probabilities for the FT and DFT versions were practically the same. Failure rates are very close, especially for times shorter than 20 days. The rate of failure of the DFT becomes greater than the FT from 20 days. Figure 7 shows these results.

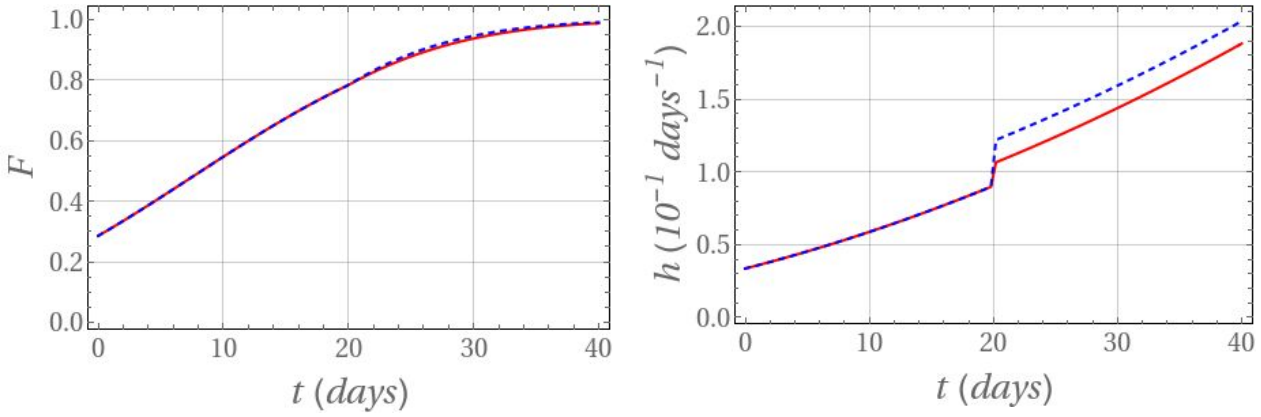

Figure 7 - Failure probability (left panel) and failure rate (right panel) for insufficient pumping: static fault tree gates configuration output shown in red-continuous line; dynamic configuration output presented in blue-dashed line

The FT and DFT were built to model the low-performance event on a motor-pump. The motor failure event due to seal leakage 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 port outputs fail only when the seal leaks before the motor protection fails. Figures 8 and 9 show the FT and the DFT created.

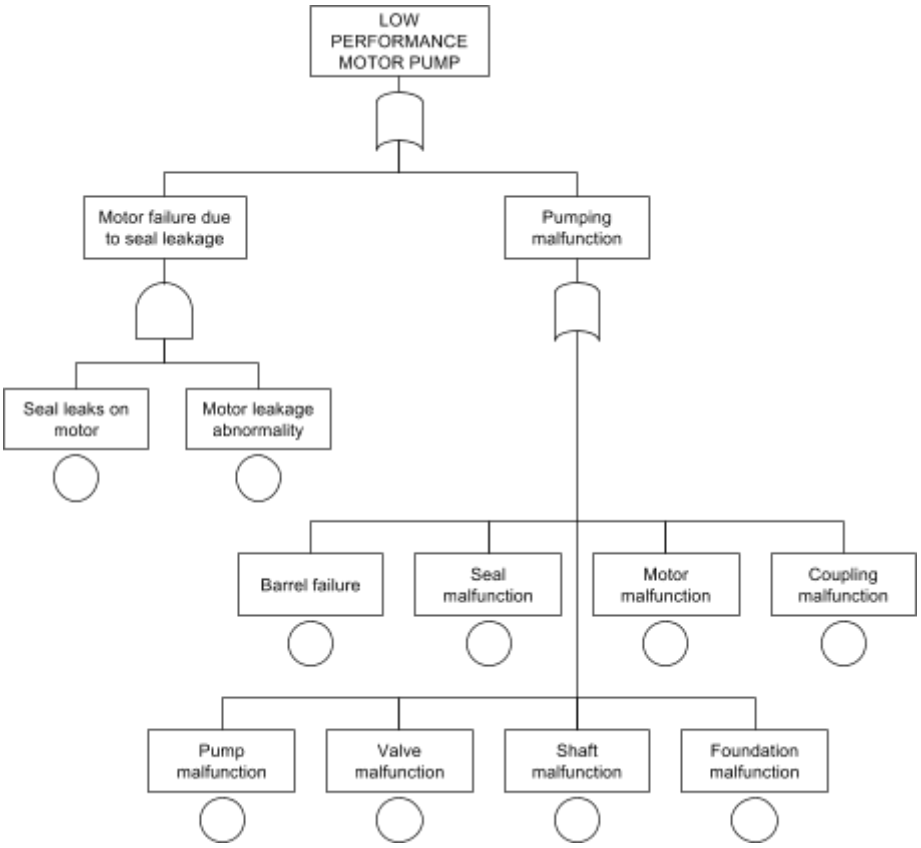

Figure 8 - Static FT for low performance motor pump

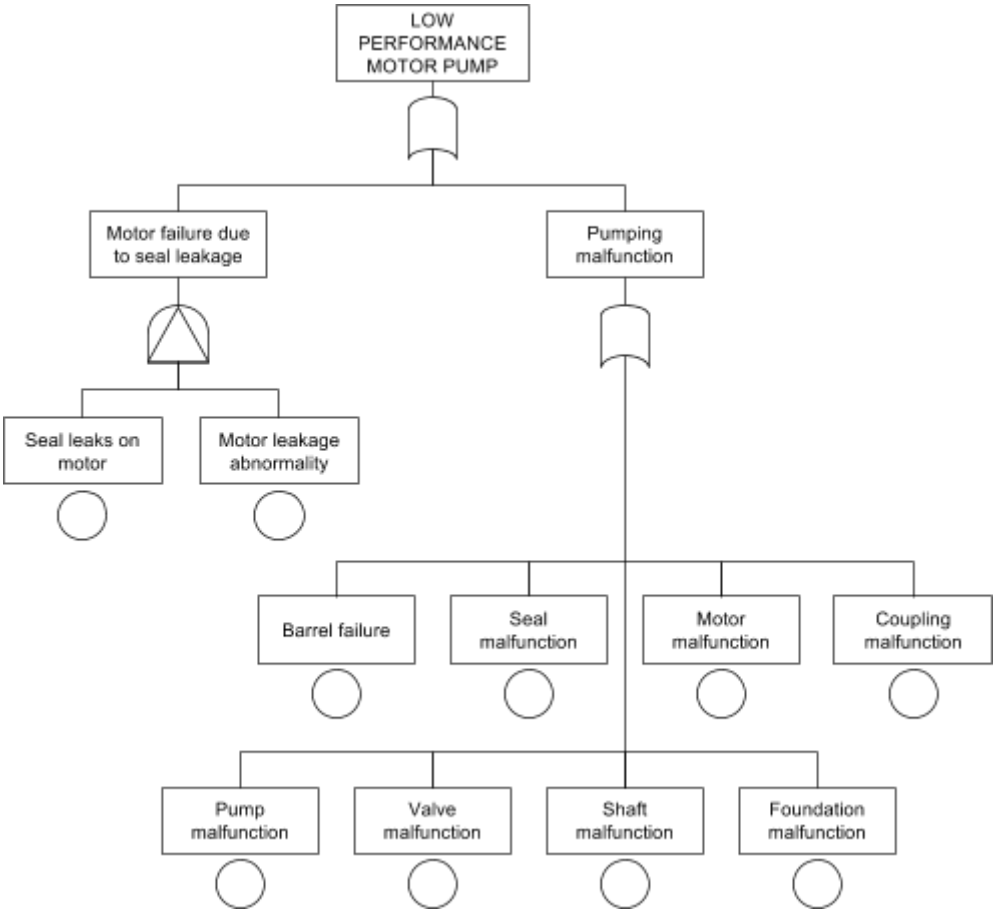

Figure 9 - DFT for low performance motor top pump event.

Table 2 shows the parameters of Weibull distribution for both two considered entries.

Table 2 - Weibull parameters for AND and PAnd entries

	β	η (days)	t_0 (days)	Failure mode
I1	1.4	416.66	0	Seal leaks on motor
I2	1.2	1940.0	0	Motor leakage abnormally

The failure probability and failure rate curves for the static and dynamic fault trees show very different behaviour. The probability of failure for the PAnd port is lower than the probability for AND gate. The difference between values reaches 27% at 4,000 h.

The failure rate shapes are completely different. The AND port produces a unimodal-increasing format while the PAnd port results unimodal shape. At 4,000h, the failure rate of the AND formulation is equal to 2.4 times that of PAnd.

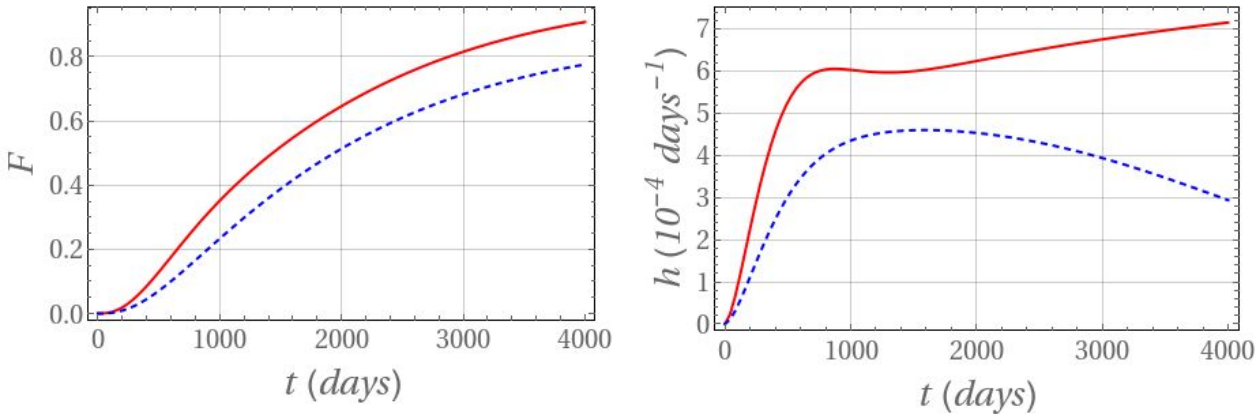

Figure 10 - Failure probability (left panel) and failure hate (right panel) for motor failure due to seal leakage: And output showed in red-continuous line; PAnd output in blue-dashed line

5. CONCLUSIONS

The results of the fault trees was discussed comparing (i) values, (ii) real situations (scenarios) that each one can model, and (iii) graphical reliability curves.

The PDep port applied in the 'Insufficient pump' event slightly changed the graphical results when compared to the OR gate. The real situation 'High demand' is difficult to model because of rare historical records and was admitted with constant failure rate. Thus, the difference between the PDep port and the OR was very small in the results. The failure rate was more sensitive to changes. Over 20 days, the difference appears in the failure rate. This behavior occurs because "High Demand" event was modeled with location parameter t0 = 20 days.

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 27%. The changes in failure rates are even greater.

For the first situation, the dynamic port showed a higher rate of failures than the static FT. However, the result of second branch analysed showed lower values when a dynamic port was applied.

The sewage treatment system in urban areas in Brazil has a continuous growing. So the reliability system is affected by these changes. This dynamic behaviour is best modeled by DFT. Also 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 situation tested in this paper shows that dynamic port conditions could represent behaviors and values different than static ports. The difference found between DFTs and FTs are consequences of dynamic situations treated by DFTs.

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

References

[1] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, “Fault Tree Handbook,” *NUREG-0492*. US NRC, Washington, 1981.

[2] Z. Jinglun and S. Quan, “Reliability analysis based on binary decision diagrams,” *J. Qual. Maint. Eng. Cybern.*, vol. 4, no. 2, pp. 150–161, 1998.

[3] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, “Improving the analysis of dependable systems by mapping fault trees into Bayesian networks,” *Reliab. Eng. Syst. Saf.*, vol. 71, pp. 249–260, 2001.

[4] S. A. Doyle and J. B. Dugan, “Dependability Assessment using Binary Decision Diagrams (BDDs),” in *Twenty-Fifth International Symposium on Fault-Tolerant Computing*, 1995, 1995.

[5] W. Long, Y. Sato, and H. Zhang, “Monte Carlo simulation for analysis of sequential failure logic,” *Ieice Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E83A, no. 5, pp. 812–817, 2000.

[6] G. Merle, J. M. Roussel, J. J. Lesage, and A. Bobbio, “Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events,” *Reliab. IEEE Trans.*, vol. 59, no. 1, pp. 250–261, 2010.

[7] Rauzy, Antoine; Blériot-Fabre, Chaire. Towards a sound semantics for dynamic fault trees. *Reliability Engineering and System Safety* v. 142, p. 184–191 , 2015.