

FAULT TREE ANALYSIS FEATURES IN INDUSTRIAL SYSTEMS SAFETY ASSESSMENT: A CASE STUDY

Assoc.Prof.Ph.D. Roland Iosif MORARU, Department of Mining Engineering and Industrial Safety, University of Petroșani, Romania, roland_moraru@yahoo.com

Abstract: *Fault tree analysis is useful both in designing new products/services or in dealing with identified problems in existing ones. In the quality planning process, the analysis can be used to optimize process features and goals and to design for critical factors and human error. As part of safety process improvement, as it is emphasized in the present paper, it can be used to help identify root causes of undesired events such as occupational injuries and illnesses. A case study of application in industrial safety systems illustrates the aim, principle and structure of the technique, allowing better prevention measures selection and implementation.*

Keywords: fault tree analysis, safety assessment, probability of occurrence, minimal cut set, system safety

1. FAULT TREE ANALYSIS: HISTORY, AIM AND PRINCIPLE












Failure tree analysis (FTA) was, in terms of time, the first method designed to achieve a systematic review of industrial risk. Developed in the early 1960s by Bell Telephone Company, the method has been tested for safety of missile launching systems [2,9]. Aimed at determining the causal chain and combinations of events that can cause an undesirable event, failure tree analysis is currently applied in many fields such as aeronautics, nuclear industry, petrochemical industry, etc. The technique provides a graphical aid for the analysis and it allows many failure modes including common cause failures. FTA is widely used in the design phase of nuclear power plants, subsea control and distribution systems, and for oversight studies in layers of protection studies for process safety and loss control in chemical plants and refineries so as to prevent accidents and control the costs of risks [2,14].

The method can also be used for retrospective analysis of accidents in this case the ultimate undesired event being already occurred, so its production scenario has been observed. In this case, the method is called the *root-cause analysis* [4, 6]. FTA is deductive method. [3, 15]. In principle, it aims at building, from an undesired event defined a priori, chains of events or combinations of events that can generate the top event. Basically, it goes from one cause to another, until there are reached those basic events likely to be at the origin of unwanted events [7, 8, 12]. Basic events generally correspond to:

- elementary events sufficiently known and described in other ways, so it is not useful to look for primary causes; some of them may be frequent enough so that one can estimate the probability of occurrence based on statistics;
- events which can not be considered as basic, but for whom is not relevant to identify the causes;
- events whose causes will be further analyzed, e.g. by a new application of the method;
- events that normally occur and are repeated during the process or plant operation.

The method uses a particular graphic symbolism, which allows presentation of the results as a tree structure. Symbols and significance of events and logic gates that can be used in the construction of fault trees are shown in Table 1. Auxiliary details of logical symbols used can be found in the standard IEC 61025:1990 "Fault Tree Analysis" [5].

Table 1. Symbols used to represent events and logic gates [5]

Symbol	Definition
	Circle symbolizes the event "primary failure"
	Rectangle : symbolizes the event "fault" resulting from the combination of primary events through logic gates.
	Pentagon : symbolizes the event "failure" which is expected to occur normally.
	Rhomb : symbolizes the event "failure" which is not developed until his root causes.
	Ellipse : symbolizes a conditional event. The symbol indicates any condition or restriction imposed on a gate.
	Double rhomb : symbolizes the event "failure" which is not developed until his root causes and requires developments.
	Triangle : symbolizes the transfer <i>to</i> and <i>within</i> the fault tree. și în arborele de defectare.
	Logic gate „AND” : for the output event to occur, it is necessary that all input events to exist
	Logic gate „OR” . for the output event to occur, it is necessary that at least an input events to exist
	Inhibition gate (hexangle) : symbolize the causal relationship between two failure type events. Input fault will generate directly the output fault if the inhibition condition is satisfied.
	Special gate (square) : used to highlight any other combination of input events that give rise to output event occurrence

2. STRUCTURE OF THE ANALYSIS PROCEDURE

In essence, the method requires going through the following three stages: (i) the definition of the top undesired event; (ii) the fault tree development; (iii) the tree valorization. They are preceded by a preliminary step, consisting in system's description [10, 18]. This stage is vital to conduct analysis and often require prior identification of risks.

Starting from the top event, placed on top of the tree, branching develops through logical connections of intermediate events and combinations of events that can lead to primary failure of system's parts. The tree is complete when all branches are developed until primary failures. Selecting and defining intermediate events is performed step by step, paying attention to identifying direct and immediate causes, which must be necessary and sufficient. Otherwise the result will be, partially or totally, wrong [1, 13, 16].

The development of the fault tree is in accordance with the flowchart shown in Figure 1. The basic requirement consists in the systematic search for direct, necessary and sufficient causes. Qualitative analysis of the tree aims to establish the extent to which a failure event corresponding to a basic causal chain can propagate to the final "top" event. Calculation rules are of the type presented for purposes of illustration in Table 2.

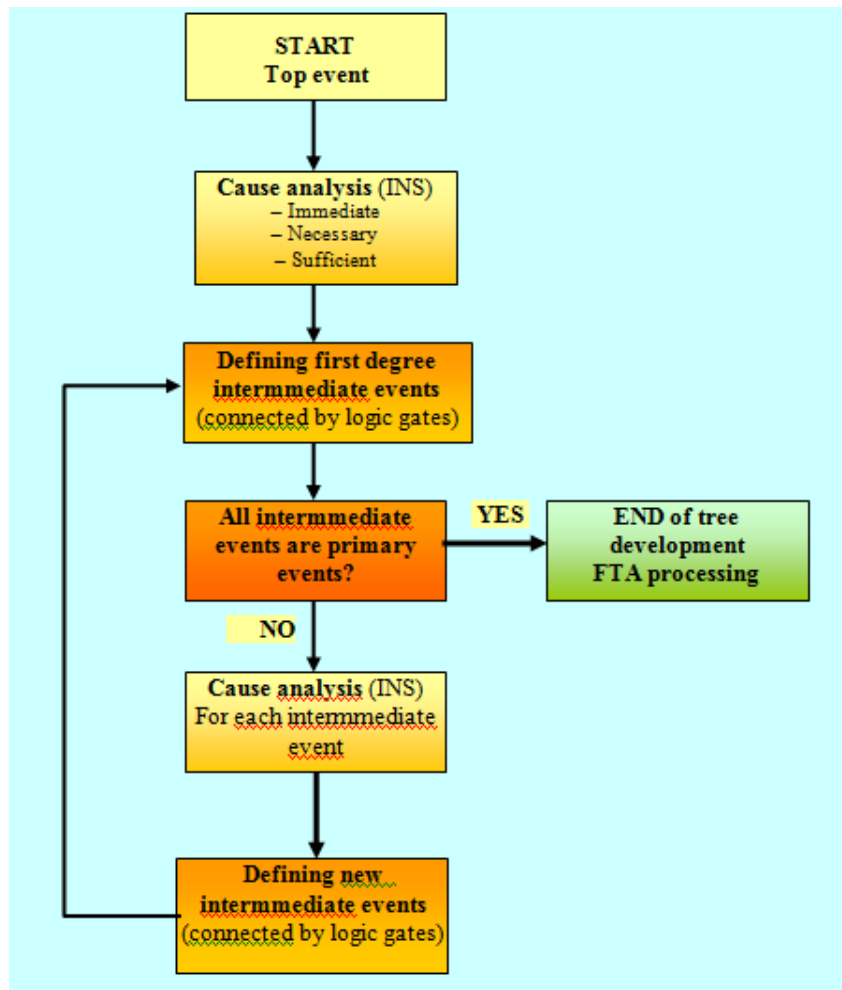


Fig. 1. FTA development flow-sheet

Table 2. Rules for Fault Tree's quantitative analysis valorization [5]

Poartă SAU	Poartă ȘI
<p style="text-align: center;">S P(S)</p> <p style="text-align: center;">E₁ E₂ P(E₁) P(E₂)</p>	<p style="text-align: center;">S P(S)</p> <p style="text-align: center;">E₁ E₂ P(E₁) P(E₂)</p>
$P(S) = P(E_1) + P(E_2) - P(E_1).P(E_2)$ (Poincaré's theorem)	$P(S) \approx P(E_1).P(E_2)$

It is accepted that, for low probability primary events, the occurrence probability of the final event is the sum of the probabilities associated with minimal cut sets. If quantitative analysis is done, the goal is to estimate based on probability of occurrence of basic events, the probability of occurrence of the final event, as well as intermediate events (see Fig. 2).

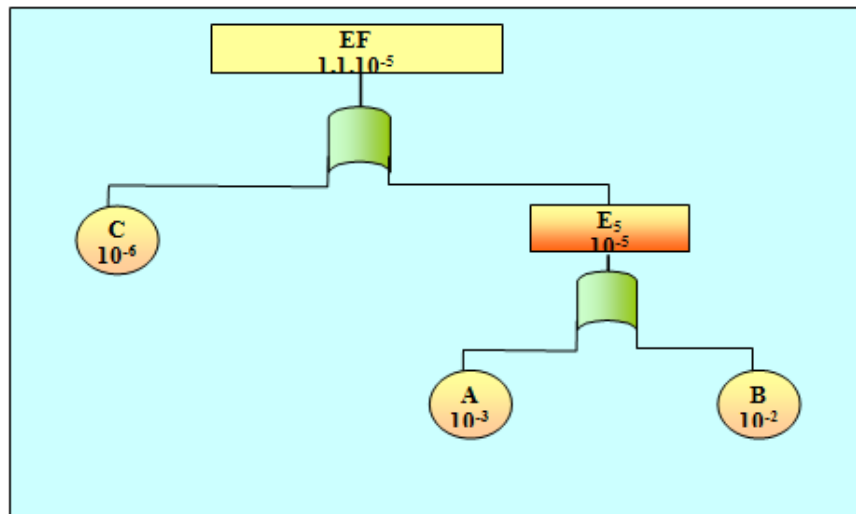


Fig. 2. Determining the final event probability

Assuming that data are available for events A, B and C, then they can be considered as primary events, and there is no need to further develop the fault tree.

3. QUANTITATIVE ANALYSIS OF THE FAULT TREE

Each tree failure is associated with a finite number of minimal cuts that are unique paths leading to the top event occurrence. Generally, the smaller the rank of a minimal cut, then its contribution to the system failure is more important. Therefore, special attention should be given to these components to eliminate or, if this is not possible, at least to minimize their effect [17].

The occurrence of the top event (T) can be expressed in terms of finite minimal cut sets (K_i) by the expression:

$$T = K_1 \cup K_2 \cup \dots \cup K_k = \bigcup_{i=1}^k K_i \quad (1)$$

Identification of minimal cuts of a fault tree can be done by various methods. *Top-down* and *bottom-up* assessments methods are used, based on Boolean algebra and differing only by the place wherefrom the analysis is initiated.

For *top-down* methods, the minimal cut sets are identified starting from the top event and descending to the primary events, while when *bottom-up* techniques are used the process is started at lowest level and mounts progressively to the top event.

Quantitative analysis of fault tree synthesis consists in synthesizing the top event reliability features based on primary events reliability features. Quantitative assessment is carried out in steps, calculations are performed starting from basic levels corresponding to primary events towards the top event.

If the fault events are independent, the following assessments can be performed, based on failure probabilities or failure rates.

3.1. Failure probability-based assessments

For an "AND" logic gate with n inputs, the output events can be expressed by the following equation:

$$P(E_1 \cap E_2 \cap \dots \cap E_n) = P(E_1) \cdot P(E_2) \cdot \dots \cdot P(E_n) \quad (2)$$

For an "OR" logic gate with n inputs, the output events can be expressed by the following equation:

$$P(E_1 \cup E_2 \cup \dots \cup E_n) \approx P(E_1) + P(E_2) + \dots + P(E_n) \quad (3)$$

3.2. Failure rates-based assessments

Admitting the hypothesis that, input events E_i do have constant λ_i failure rates, the equations below will express the failure rate λ_E for the output event:

- for an "OR" logic gate with n inputs:

$$\lambda_E = \sum_{i=1}^n \lambda_i \quad (4)$$

- for an "AND" logic gate with n inputs:

$$\lambda_E = \frac{\sum_{i=1}^n \lambda_i \cdot \frac{1}{1 - \exp(-\lambda_i t)}}{\prod_{i=1}^n \frac{1}{1 - \exp(-\lambda_i t)} - 1} \quad (5)$$

The previously calculated indicators are punctual reliability characteristics of the analyzed system. In the case of fault trees containing one or more repeated events the above method can not be applied because some events to output port are no longer independent. In this case top event's occurrence probability calculation is done using minimal set cuts identified during the qualitative analysis of the fault tree. Also, the method based on the set of minimal cuts can be applied to any type of tree, with or without repeated events.

Let K_i ; $i=1 \dots k$ be the minimal set cuts of a fault tree. The occurrence of a top event T , the analysed critical event as a function of K_i can be expressed as in the eq. (6), given below:

$$T = K_1 + K_2 + \dots + K_k = \bigcup_{i=1}^k K_i \quad (6)$$

while the top event probability is:

$$P(T) = P\left(\bigcup_{i=1}^k K_i\right) \quad (7)$$

Equation (6) can be written as:

$$P(T) = \sum_{i=1}^k P(K_i) - \sum_{i=2}^k \sum_{j=1}^{i-1} P(K_i \cap K_j) + \dots + (-1)^{k-1} P(K_1 \cap K_2 \cap \dots \cap K_k) \quad (8)$$

In this expression the first term has the highest significance, the second term has a lower significance since he is a multiplication of probabilities, and so on, each term is less significant than the previous.

Equation (7), containing numerous terms, and gives the precise value of the top event probability of occurrence, can be considerably simplified, retaining only the first or the two first terms. Approximations that are obtained in both cases are as much closer to the actual values, as the components failure probabilities are smaller. It is easily found that:

$$\underbrace{\sum_{i=1}^k P(K_i) - \sum_{i=2}^k \sum_{j=1}^{i-1} P(K_i \cap K_j)}_{\text{Lower margin}} \leq P(T) \leq \underbrace{\sum_{i=1}^k P(K_i)}_{\text{Upper margin}} \quad (9)$$

The approximate relationship allowing to calculate the upper margin is also known in probability theory as the *law of rare events*.

Another method for approximating the upper limit for the probability of top event occurrence, also based on the use of minimal cut sets is presented below.

Following notations are made:

$P(T)$ - probability of top event occurrence;

$P(K_i)$ - probability of minimal cut sets occurrence K_i ;

$P(\overline{K_i})$ - probability of minimal cut sets non-occurrence K_i ;

From equation (7) it comes that:

$$P(T) \leq \sum_{i=1}^k P(K_i) \quad (10)$$

$$\text{But while } \sum P(K_i) = 1 - \sum \overline{K_i} \quad (11)$$

equation (9) is rewritten as it follows:

$$P(T) \leq 1 - \sum_{i=1}^k P(\overline{K_i}) \quad (12)$$

The event „non-occurrence of none minimal cut set” is given by the intersection of $\overline{K_i}$ events, so it comes that:

$$\sum_{i=1}^k P(\overline{K_i}) \geq \prod_{i=1}^k P(\overline{K_i}) \quad (13)$$

From relationships (11) and (12) results:

$$P(T) \leq 1 - \prod_{i=1}^k [1 - P(K_i)] \quad (14)$$

Finally:

$$P(T) \leq 1 - \prod_{i=1}^k [1 - P(K_i)] \leq \sum_{i=1}^k P(K_i) \quad (15)$$

It follows that this mode of approximation to the likelihood of top event occurrence leads to an error lower than when using the approximation based on the law of rare events.

4. CASE-STUDY: FTA FOR THE WATER SUPPLY SYSTEM OF AN INDUSTRIAL FACILITY

We have analysed and built the fault tree for a water supply system of an industrial secondary facility (SA). The analysed system, presented in Figure 3, consists of two pipes which simultaneous operation is permanently required to supply water into the SA system. The two pipes start from the same reservoir (tank) R and have installed on them in series one manual valve V, an electric powered pump P and a clapper valve C. The pipes themselves are not considered, for simplicity.

- *Safety function:* The SA system must be supplied with a given Q water quantity.
- *System's environment:* is not considered (no external aggression risk).
- *Initial state of components:* valves are opened, pumps activated, sunt deschise, pompele sunt activate, valves allow water to flow towards the SA system and the tank is full.

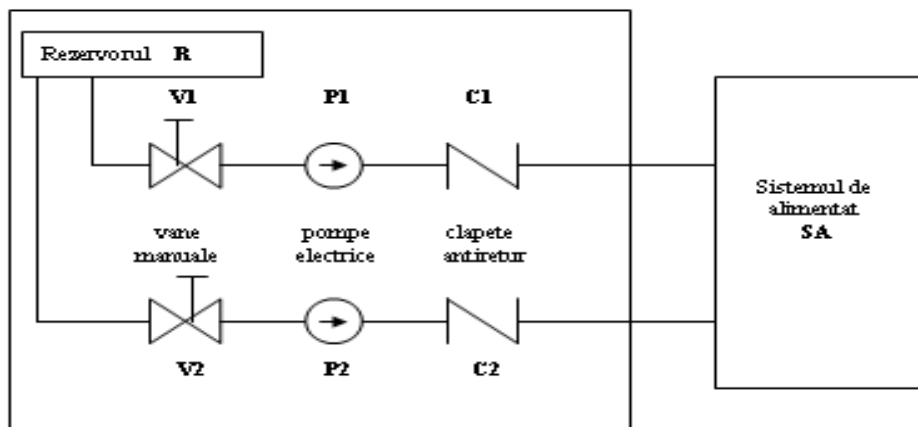


Fig. 3. Schematic representation of the analyzed system

Top unwanted event definition: It is denominated "SA system not feeded" briefly written as " $Q_{SA}=0$ ".

Logical diagram of the fault tree development: It starts from placing the unwanted top event in the top diagram: $Q_{SA} = 0$. This event is classified as "failures on the system", which does not give any information of "input" type wherefrom it comes. In our case, it can be noticed that if the system is not supplied for that flow downstream of valves C1 and C2 is zero, we can build the second level of the tree, see Fig. 4.

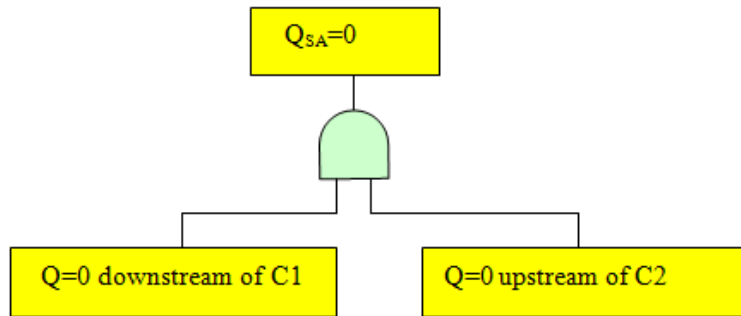


Fig. 4. Fault tree's second level

Developing the intermediate event $Q=0$, downstream of C1, it has as immediate causes the occurrence of event "C1 blocked" or " $Q=0$ upstream of C1". Achievement of one of the two events is enough to produce the intermediate event.

At this stage of decomposition occurs for the first time an event that relates directly to a component, namely event "C1 blocked", which will be followed by a three-input OR and entries stating:

- primary failure (due to damper flap stiffness, e.g. C1 in closed position);
- secondary failure (which is usually due to a failure conditions of use, such as a corrosion preventing throttle opening; this event will be further developed and is represented by a rhomb), and
- failure due to inadequate controls, but not related to valve; The tree now has the structure given in Fig. 5:

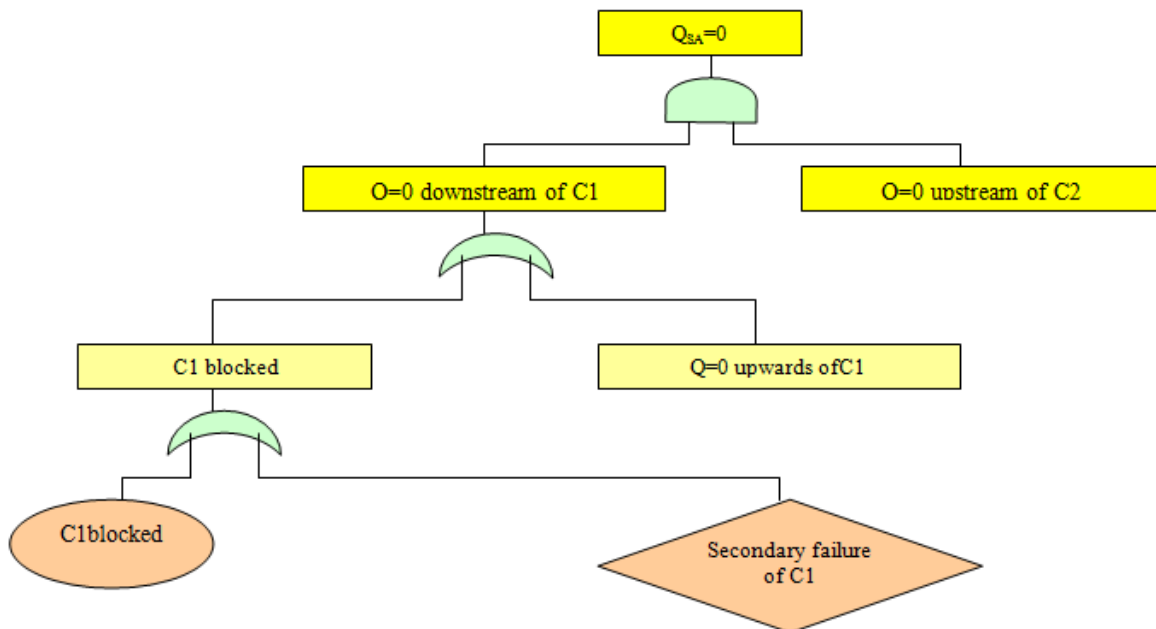


Fig.5. Fault tree's 3rd level development

Further developing the intermediate event " $Q = 0$ upstream of C1" which is the category of defects on the system and is equivalent to " $Q = 0$ downstream of P1" reaching at the previously treated case of C1 valve. By doing in the same manner, we reach to achieve the decomposition in the following scheme, which notes that " $P1$ does not work". Consequently, it follows a three-input OR-gate, one entry corresponds to a control malfunction, reduced to basic event " $Loss$ of electrical power supply" (see Fig. 6). For this branch, the deductive procedure ends with the decomposition of event " $Q = 0$ upstream of P1" which is identical to " $Q = 0$ downstream of V1". A closer look at the diagram representing the system allows emphasizing the immediate causes of this last event, which are " $V1$ closed" and " $Q = 0$ upstream of V1". We notice that appears, for the second time, a malfunction due to inappropriate orders, in this case non-execution of an operation which this time is attributable to a man who could have several reasons: simple forgetfulness or disregard, the operator is confident that he opened the valve but he did not.

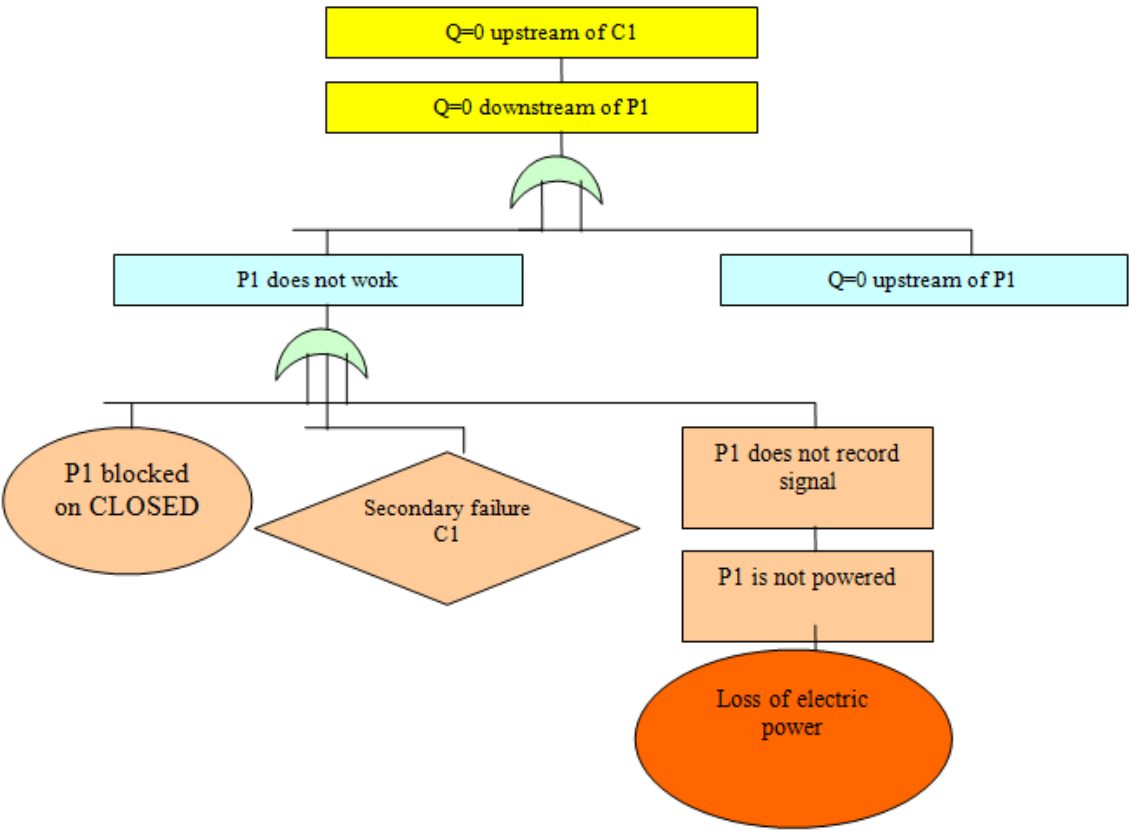


Fig. 6. Fault tree's 4th level development

The flowchart of the Fault Tree, relative to the second route, is developed in the same manner, being symmetrical to that achieved for the first route is shown in Fig. 7.

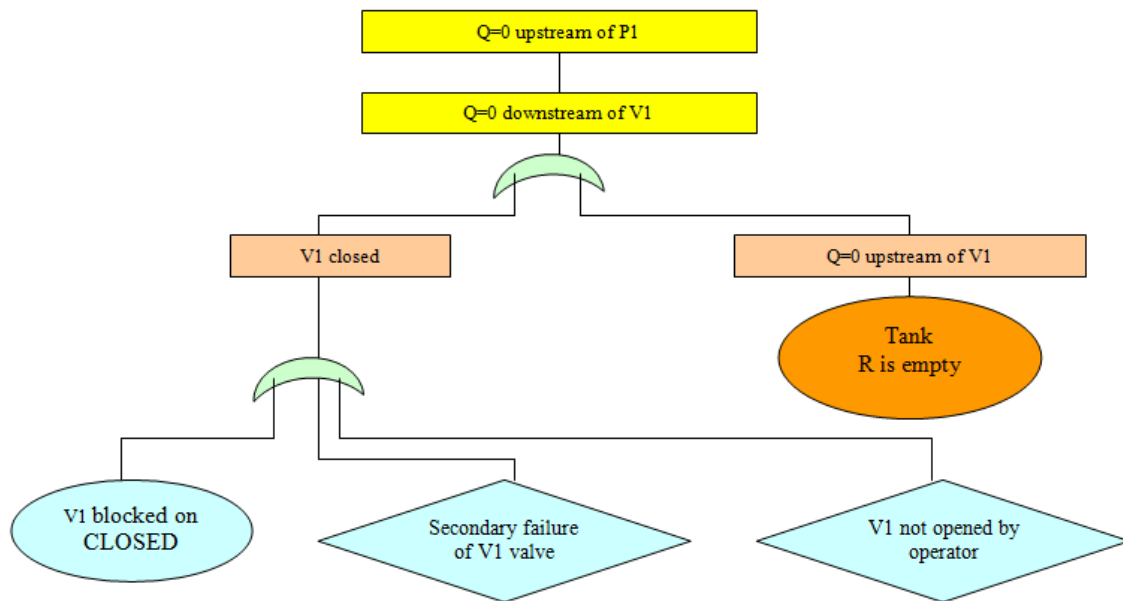


Fig. 7. Flowchart of the Fault Tree, relative to the second route

It is noted that the same events occur in the two paths of logical scheme such as events "empty tank" or "loss of electrical power." These events are called as "common cause faults" and must be reviewed carefully.

5. SUMMARY AND CONCLUSIONS

As illustrated through the case study performed on a water supply system of an industrial facility, the fault tree analysis is a systematic, deductive and probabilistic risk assessment tool which elucidates the causal relations leading to a given undesired event. It was also highlighted that quantitative FTA requires a fault tree and failure data of basic events. Development of a fault tree and subsequent analysis require a great deal of expertise, which may not be available all the time. An undesired state of a system is analyzed using [boolean logic](#) to combine a series of lower-level events. This analysis method is mainly used in the field of [safety engineering](#) and [reliability engineering](#) to determine the probability of a safety accident or a particular system level (functional) failure

FTA is very good at showing how resistant a system is to single or multiple initiating faults. It is not good at finding all possible initiating faults. After the fault tree has been assembled for the specific analyzed undesired event, it will be evaluated and analyzed for any possible improvement or in other words study the risk management and find ways for system improvement. This stage is as an introduction for the final step which will be to control the hazards identified.

The tool aids the design process, shows weak links that cause failures, and in the critical legs of the trees helps to define maintenance strategies for which pieces of equipment and processes should be defended with the greatest maintenance vigour to prevent "Murphy" from shutting down the process or causing serious safety issues.

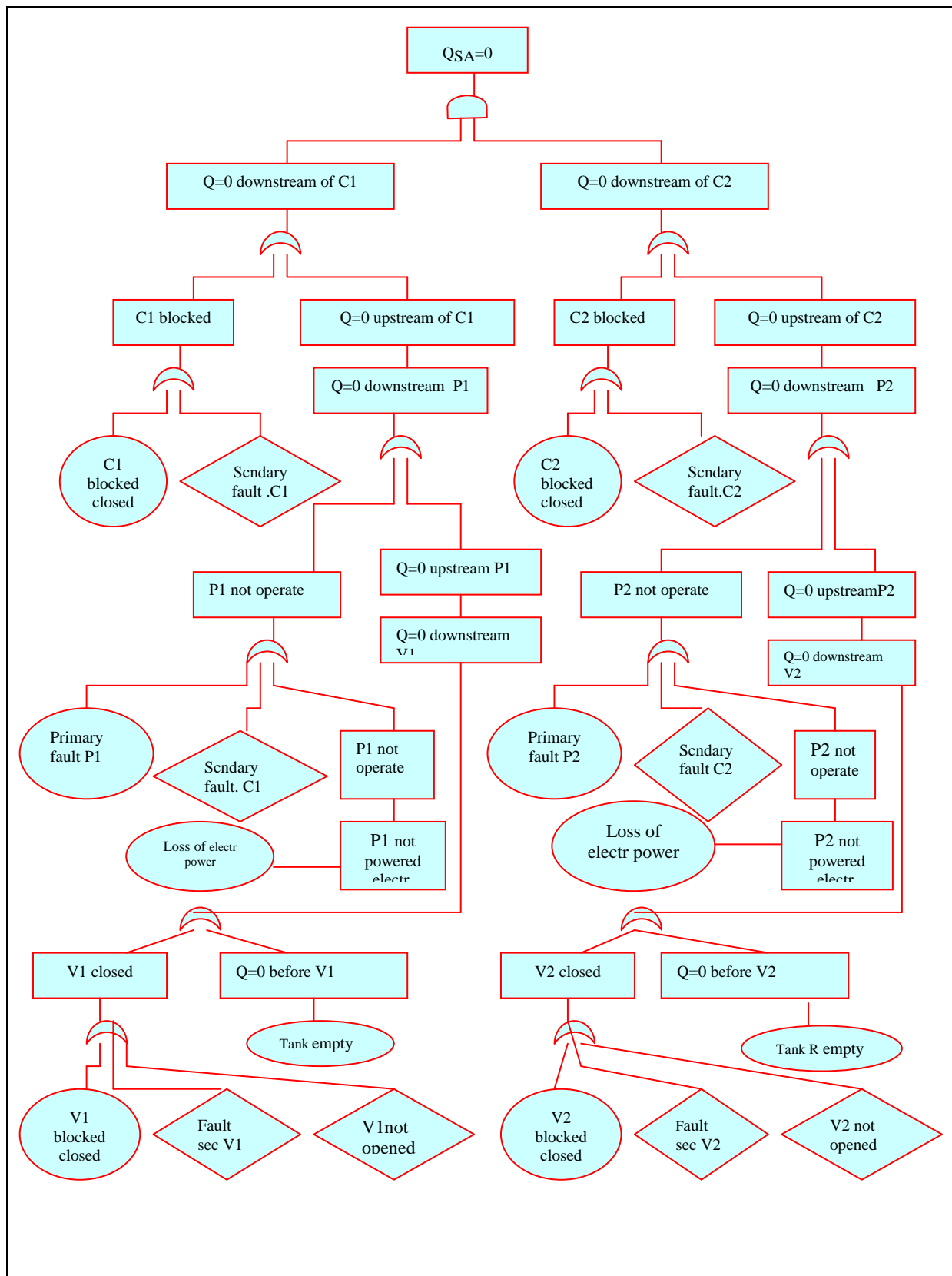


Fig. 8. The final logical diagram of the Fault Tree for the quantitative analysis

The technique is helpful for identifying critical fault paths, observing vague failure combinations before they occur in reality, comparing alternate designs for safety, and setting a methodology to provide management with a tool to evaluate the overall hazards in a system and avoid single sources of critical failures.

Finally when thinking top down about failures and where/how they can occur, the methodology gives a diagram for setting maintenance strategies for protecting key pieces of equipment/processes to prevent failures and provide occupational health and safety of workers.

REFERENCES

- [1] **Desroches, A.** - *Concepts et méthodes probabilistes de base de la sécurité*. Editions Lavoisier TEC&DOC, Paris, 1995.
- [2] **Favaro, M., Monteau, M.** - *Bilan des méthodes d'analyse a priori des risques*. Cahiers de Notes Documentaires, nr. 139/1990, pag. 363.
- [3] **Fadier, E.** - *L'intégration des facteurs humains dans la sûreté de fonctionnement*. Revue de la sûreté de fonctionnement - Phoebus, numéro spécial, pag. 59-78, 1998.
- [4] **Kirwan, B.** - *Validation of human reliability assessment techniques –Part 1 & 2*. Safety Science, vol. 27, nr. 1/1997, pag. 25-75, Elsevier.
- [5] **IEC 61025.** *Fault Tree Analysis International Standard IEC 61025*, 1990 IEC, Geneva
- [6] **Laprie, J.C.** - *Guide de la sûreté de fonctionnement*. Editions Cépaduès, 1995.
- [7] **Mäckel, O., Rothfelder, M.** Challenges and Solutions for Fault Tree Analysis Arising from Automatic Fault Tree Generation: Some Milestones on the Way. ISAS-SCI (1) 2001: 583-588
- [8] **Macwan, A., Mosleh, A.** - *A methodology for modelling operator errors of commission in probabilistic risk assessment*. Reliability Engineering and System Safety, Elsevier Science Limited, pag. 139-157, 1994.
- [9] **Moraru, R., Băbuț, G.** - *Analiză de risc*. Editura Universitat, Petroșani, 2000.
- [10] **Moraru, R., Băbuț, G., Matei, I.** - *Ghid pentru evaluarea riscurilor profesionale*. Editura FOCUS, Petroșani, 2002.
- [11] **Moraru, R., Băbuț, G.** - *Managementul riscurilor; Abordare globală-Concepte, principii și structură*. Editura Universitat, Petroșani, 2009.
- [12] **Moraru, R., Băbuț, G.** - *Evaluarea și managementul participativ al riscurilor profesionale*, Editura Focus, Petroșani, 2010, ISBN:978-973-677-206-1.
- [13] **Price, H.E.** - *The allocation of functions in systems*. Human factors, vol. 27, pag. 33-45, 1985.
- [14] **Rasmussen, J.** - *Risk management in a dynamic society: a modelling problem*. Safety Science, vol. 27, nr. 2-3/1997, pag. 183-213.
- [15] **Reason, J.** - *A system approach to organisational error*. Ergonomics, vol. 38, nr. 8/1995, pag. 1708-1721.
- [16] **Vanderhaegen, F., Polet, P.** - *Evaluation des performances dans l'analyse des risques*, Communication présentée au Groupement pour la Recherche en Productique, <http://www.univ-savoie.fr/grp2000>, Annecy, Franța, 23-24.03. 2000.
- [17] **Vesely, W. E., Goldberg, F. F., Roberts, N. H., Haasl, D.F.** *Fault Tree Handbook*. U. S. Nuclear Regulatory Commission, NUREG-0492, Washington, 1981