ISSN 1453 – 7303 "HIDRAULICA" (No. 1/2018)
Magazine *of Hydraulics, Pneumatics, Tribology, Ecology, Sensorics, Mechatronics*

Fault Tree Analysis Used in Offshore Industry

Prof. Dr.Eng. **Mariana PANAITESCU[1],** Prof. Dr.Eng. **Fănel-Viorel PANAITESCU[1],**
Assist. Dr. Eng. **Ionuț VOICU[1]**, PhD. Student **Laurențiu-George DUMITRESCU**[2]

[1] Constanta Maritime University; panaitescumariana1@gmail.com, viopanaitescu@yahoo.ro, ctionut2009@yahoo.com

[2] Constanta OILTERMINAL, dumitrescu.laurentiugeorge@yahoo.com

Abstract: *Fault Tree Analysis is one of the engineering tools that provide a systematic and descriptive approach to the identification of systems under risk. Probabilistic Risk Assessment (PRA) is a method to determine the reliability of a system based on the probability of component(s) and/or system(s) failure. Fault Tree Analysis (FTA), which is a part of PRA, provides a method for determining how failures can occur both quantitatively and qualitatively. In this paper we present the FTA for offshore facility: safety flow chart of offshore production facility, fault tree diagrams for different levels (upper level, intermediate state, overpressure, underpressure, excess temperature, ignition, excess fuel). Also, FTA for subsea control systems is presented in this paper. In conclusions, reliability analysis of the surface facilities shows that mechanical components, pumps and compressors, have higher failure rates compared to other mechanical components.*

Keywords: *Fault tree, reliability, analysis, offshore, industry, diagram, facility, probability, risk, assessment, event, symbol*

1. Introduction

Fault tree analysis is one of the engineering tools that provide a systematic and descriptive approach to the identification of systems under risk. It also provides a visual aid in understanding the system's behaviour. Probabilistic Risk Assessment (PRA) is a method to determine the reliability of a system based on the probability of each component and/or system failure. Fault Tree Analysis (FTA), which is a part of PRA, provides a method for determining how failures can occur both quantitatively and qualitatively [1].

2. Fault Tree Diagrams

Fault Tree diagrams provide a means of visualizing all of the possible modes of potential failures, an understanding of the system failure due to component failures and redesign alternatives [2]. These diagrams are formed such that an undesired event appears on top of the diagram, called the top event. The causes that lead to the system failure are broken into hierarchical levels until effects of the basic system components that lead to the top failure can be identified. Branches using event statements and logic gates link the basic events, or fault events, that lead to the top event. The failure rate data must be available for those basic events at the lowest hierarchical level. Once the fault tree is formed, the probability of occurrence of the top event can be found.

- *Fault Tree symbols*

These are used to connect basic events to the top event, during fault tree construction. There are two kinds of fault tree symbols: event symbols (Fig. 1), and gate symbols (Fig. 2) [1], [2].

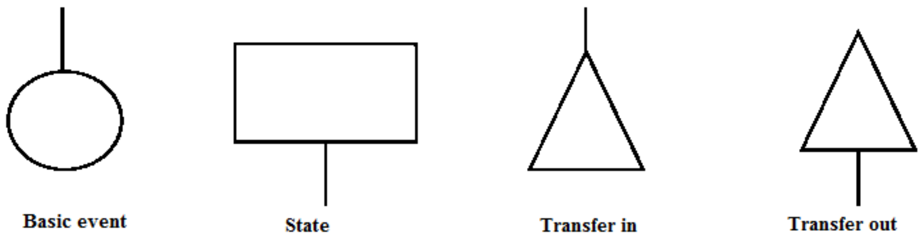

Fig. 1. The events symbols

Fig. 2. Gates symbols

- *Fault Tree Construction*

A fault tree (FT) is constructed such that the undesired event or top event exists at the highest level in the fault tree. Basic events and outputs of gates are connected so that they lead to that top event. Basic events and states are at lower levels.

- *Probability Calculations in Fault Trees*

The calculation of the probability of an undesired event can be done using the Boolean's algebra for the analysed system (with a program in the C^{++}). Using the FTA diagrams, and the results obtained from the calculations, which components and systems are safe was assessed.

2.1 FTA for offshore industry

For this area, first must present offshore production facility for safety flow chart (Fig. 3). In this chart, we can see that safety devices should be used to prevent the propagation of undesirable events. The release of hydrocarbons is the main factor to lead all top events.
The overall objectives of the safety system are: prevent undesirable events that could lead to hydrocarbon leak; shut the process partially or overall to prevent leak of hydrocarbons and fire; accumulate and recover the released hydrocarbons and gases that escape from the process.

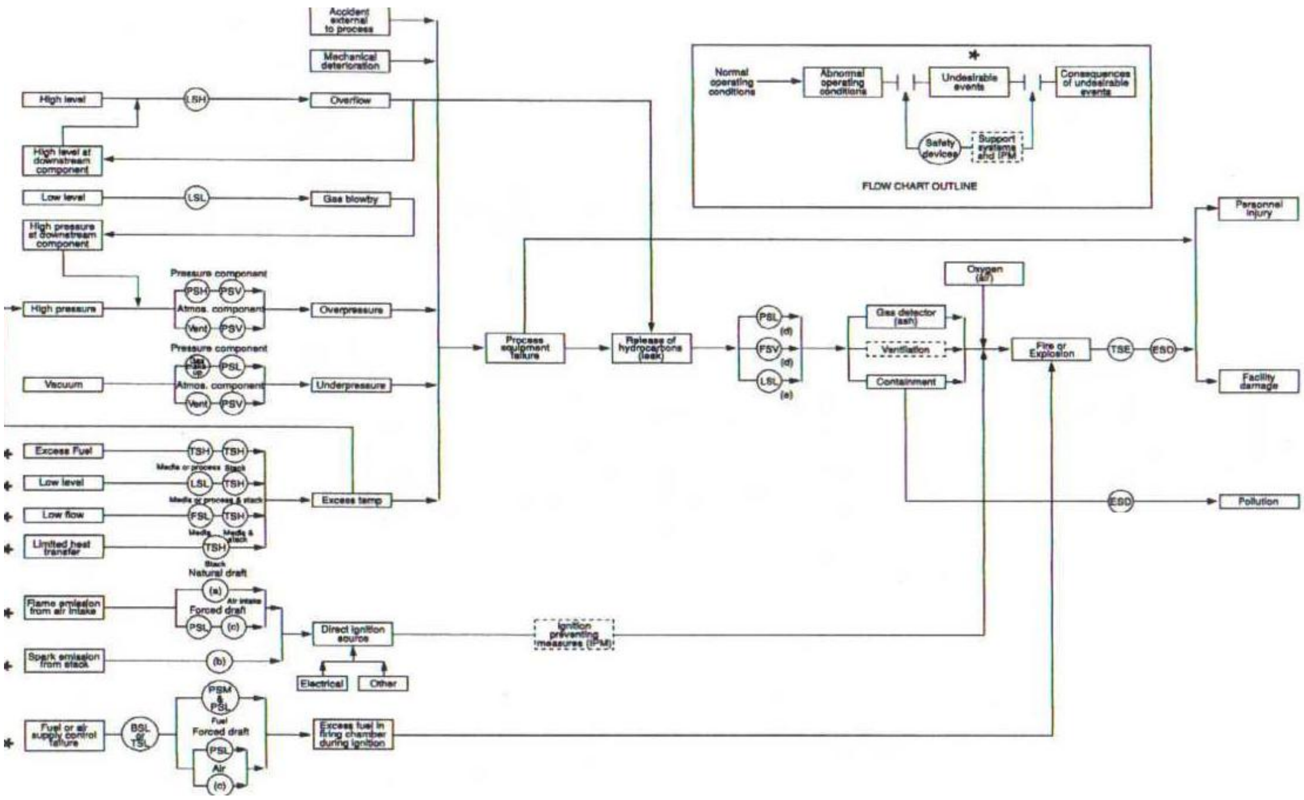

Fig. 3. Safety flow chart

Starting from safety flow chart, we construct: a) *upper level Fault Tree diagram* (Fig. 4), where the top event was personnel injury and/or facility damage; the intermediate state is the state of the safety chart after the release of hydrocarbons and three safety devices (PSL- Pressure Safety Valve, FSV- Flow Safety Valve, LSL- Level Safety Low);

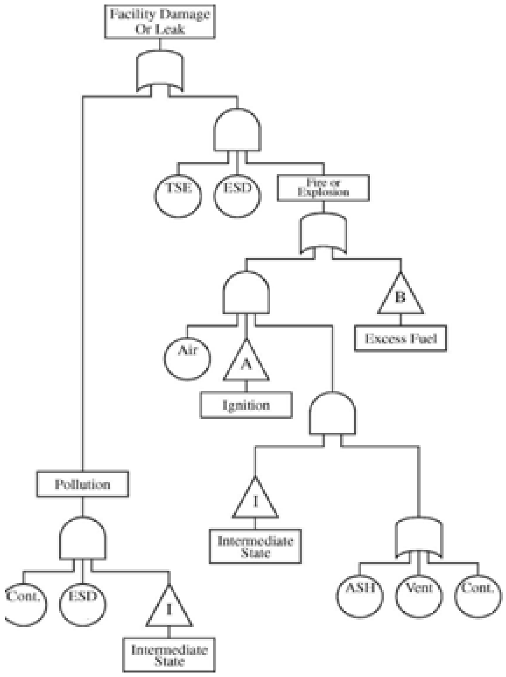

Fig. 4. Upper level Fault Tree diagram

Safety elements (Fig.4) are: temperature safety elements (TSE) (temperature sensors), an emergency shutdown system (ESD) (modeled by valve), containment (a system to collect and direct escaped liquid hydrocarbons to a safe location)[2], gas detector (ASH).
The triangle states are: I- Intermediate State (Fig.5), A-Ignition (Fig.6), B-Excess Fuel (Fig. 7).

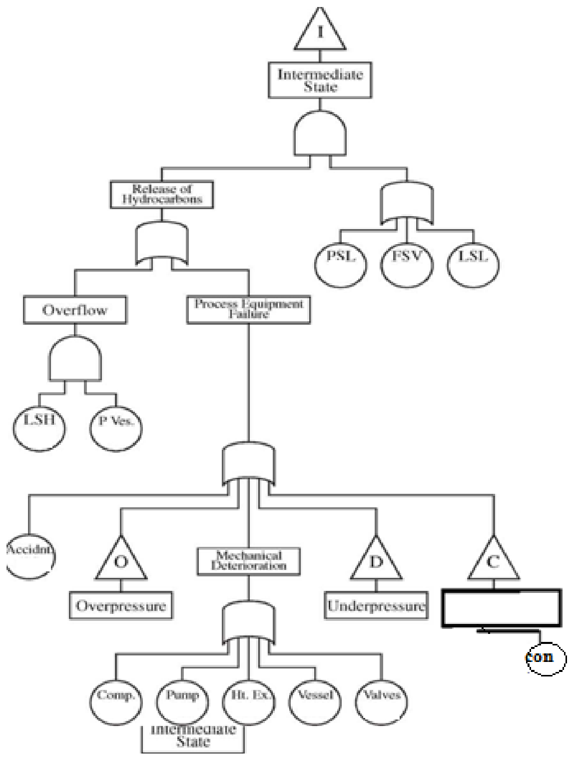

Fig. 5. Fault Tree Diagram of Intermediate State I

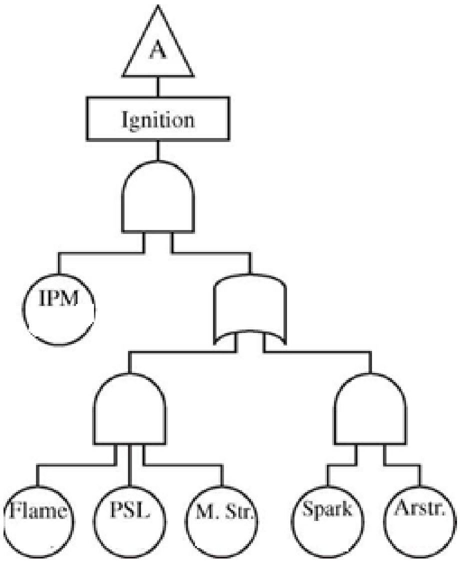

Fig. 6. Fault Tree Diagram of A-Ignition

An ignition source could be: the flame emission from the air intake arises with the failure of the low pressure sensor (PSL), the motor starter interlock failure, or spark emission from the stack arises with stack spark arrestor failure. Flame emission from air intake causes improper fuel usage (a failure of a pump).

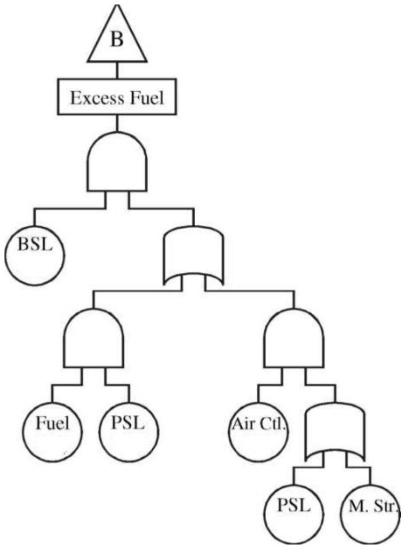

Fig. 7. Fault Tree Diagram of B-Excess Fuel

B represents the excess fuel intermediate state. Excess fuel may occur if the fuel is extraneous in the firing chamber and if the safety device, burner safety low (BSL), fails [2]. Excess fuel in the firing chamber could occur due the failure of the fuel supply control (failure of the pump control unit) and failure of the low pressure sensor, or due air supply control failure with the failure of the motor starter interlock and the low pressure sensor (PSL).

Process equipment failure is due to five factors: accident, O-overpressure (Fig.8), mechanical deterioration of hardware components, D-under pressure (Fig.9), C-excess temperature at component (Fig.10) [3].

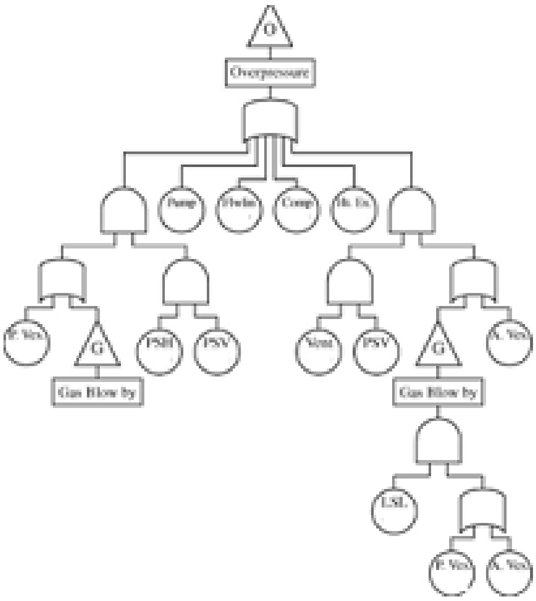

Fig. 8. Fault Tree Diagram of Overpressure

Note: The letters O, D, C-show the triangle states

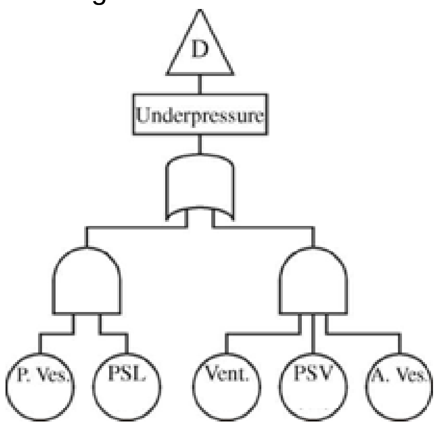

Fig. 9. Fault Tree Diagram of Underpressure

Fig. 10. Fault Tree Diagram of Excess Temperature

The Fault Tree diagrams (Fig.4....Fig. 10) present the causes for personnel injury and/or facility damage due to sensors, control unit failures of various hardware components [4].

2.1 FTA for subsea control systems

FTA for subsea control systems was analyzed using subsea architecture (Fig. 11). Failure modes for the subsea subsystems are: electrical power failure - pod (EFP); hydraulic power failure - connector (HFC); hydraulic power failure - line (HFL); hydraulic power failure - pod (HFP); signal transmission failure - connector (SFC); signal transmission failure - line (SFL); signal transmission failure - pod (SFP); signal transmission failure- surface (SFS). The block diagram of the subsea control subsystems shown in Fig.12.

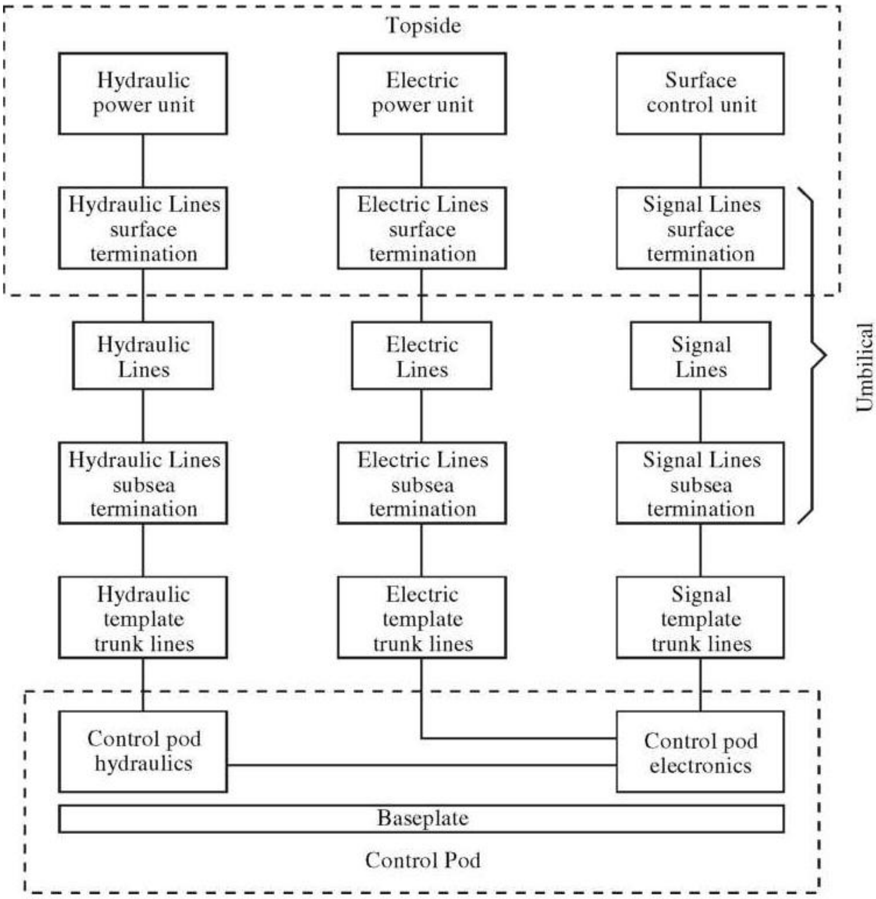

Fig. 11. Subsea architecture [4]

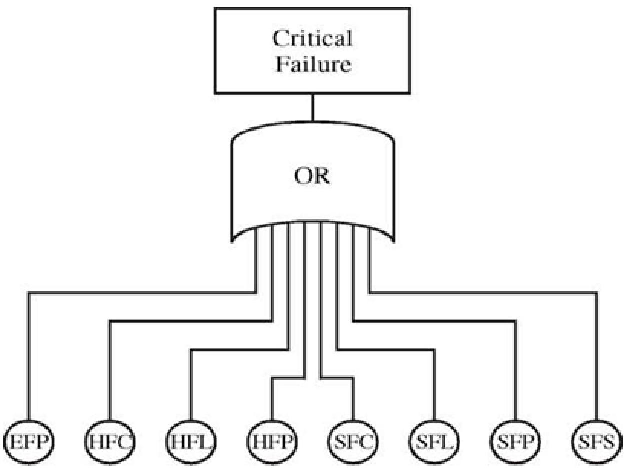

Fig. 12. The block diagram of the subsea control subsystems [5]

Note:

1) SFC- signal transmission failure in the components;
2) three basic events are actually combinations of two or more fundamental events (e.g.: EFP could be either a short circuit at the pod connector or a generic electric failure in the subsea control unit) [3].

The fault tree will consist of only basic events, "OR" gates and derived states, including the top event [5].

3. Conclusions

With this method (FTA) and its tools we can provide all possible modes of potential failures of the components of systems and redesign alternatives. Also, we can identification the risks of systems during operational time.

The use of FTA is a real support for design, construction, inspection and maintenance in offshore industry. The FTA tools are also useful in demonstrating the importance and effects of improving human and organizational aspects.

Acknowledgments

Acknowledgments of Mr. Egemen Kemal Cetinkaia from University of Missouri-Rolla, *Master of Science in Electrical Engineering*, who has provided specialized information from this field in his thesis.

References

[1] Kashubski, Michael. "Offshore Oil and Gas installations Security" *An International Perspective*, Accessed January 20, 2018. http://ref.cern.ch/CERN/CNL/2000/003/scada/.
[2] Çetinkaya, Egemen Kemal. *Reliability analysis of SCADA systems used in the offshore oil and gas industry,* Missouri-Rolla, 2001.
[3] API. *Recommended Practice 14C,* "Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms", sixth edition, March 1998.
[4] Dunn-Norman, S., K.T. Erickson, E.K. Çetinkaya, E.K. Stanek and A. Miller. "SCADA system trends in deepwater developments". Paper presented at Rio Oil & Gas Expo and Conference, October 2000.
[5] Musa, J.D, A. Iannino and K. Okumoto. *Software Reliability: Measurement, predictions, applications,* McGraw-Hill, 1987.