Transactions on Information and Communications Technologies vol 8, © 1995 WIT Press, www.witpress.com, ISSN 1743-3517

The knowledge engineering approach to reliability analysis

J.A.B. Geymayr, N.F.F. Ebecken
COPPE/Federal University of Rio de Janeiro, Laboratory for Artificial Intelligence Research, Caixa Postal 68506, 21945-970 Rio de Janeiro, RJ, Brazil

ABSTRACT

This paper presents the FTAES system, a knowledge based environment designed for the assessment and measurement of reliability, availability, maintainability and safety of industrial systems using fault tree representation. Object oriented structures are used to represent the problem's domain, production rules, algorithms and database structures are the basic elements of the system. FTAES was structured into an open blackboard architecture in order to allow further inclusion of real time diagnostic modules and automatic fault tree generation. Uncertainty, vagueness and fuzzyness are represented and solved with fuzzy logic approaches.

1 INTRODUCTION

Procedural programming has frequently been used to implement algorithms for fault-tree evaluation. However the procedural approach suffers from the lack of support for many phases of the software lifecycle, for instance program maintenance. Amongst other features, the procedural approach may lead to re-writing almost the entire program in case of a module addition or deletion. Object oriented programming (OOP) frameworks for FTA have been described by Patterson-Hine and Koen[1]. The object oriented approach is especially suited for program maintenance and code reutilization due to its encapsulation properties. It has been shown that the success of a reliability analysis depends both on the experience of the reliability engineer and the process-specific knowledge by [13,14]. The performance of non-experts at using conventional tools is undesirable since neither the procedural nor the object oriented approach provide mechanisms to represent and process the expert's knowledge which is required for the analysis. In recent years, numerous attempts have been made to apply knowledge-based

fault tree expert systems to the tasks of process fault detection and diagnosis [9-12]. Reliability analysis expert systems have been also reported at literature [2-5]. The use of rule-based knowledge representation has been extensively used. However this approach suffers from a lack of generality (they contain a great deal of process-specific knowledge), poor handling of novel situations (they are likely to fail under unanticipated circumstances), and a lack of transparency since they are difficult to maintain and validate [5]. Many researchers in the area have come to the conclusion that some combination of rule based and object oriented programming must be used as a compromise between processing efficiency and qualitative performance [7].

This paper describes the architecture of FTAES (Fault Tree Analysis Expert System), an object-oriented, knowledge-based system for industrial FTA application. The system is available for several platforms. The knowledge base assists engineers at the different stages of the fault tree evaluation: fault-tree construction and simplification, minimal cut set evaluation, importance and common cause analysis, and failure data manipulation.

2 FTAES SYSTEM ARCHITECTURE

The FTAES system was designed with the following purposes:

a) Explore the characteristics of object oriented structures to represent the fault tree domain
b) Use meta-knowledge to analyse the relations between the events of the tree.
c) Integrate multiple sources of knowledge, procedures and databases.
d) Process uncertainty and vagueness to adjust and optimize results.
e) Provide an open architecture for real time diagnostic applications or automatic fault tree generation.
f) Integrate multiple sources of data and provide a portable tool for several platforms.

FTAES is structured into a *blackboard architecture*. The *blackboard architecture* provides a framework for integrating knowledge from several sources and representing multiple levels of problem decomposition. The blackboard is composed of a number of *knowledge sources* (KS) that are controlled by an *inference mechanism*. The KSs are independent chunks of knowledge and do not communicate with each other directly. Instead, they participate in the problem solving process by creating entries in a global database, the blackboard. Each KS knows which type of objects on the blackboard it is interested in, knows how to determine if it wants to update the blackboard, and knows how to update the blackboard. Figure 1 shows the FTAES architecture. The blackboard of the system contains the object definition and the control strategies required for FTA. The KSs were divided in two levels: *specialist* and *interface* levels. The *specialist* KSs contain the set of rules acquired from the experts to perform the analysis at different levels of abstraction. The specialist KSs of FTAES are

fault_tree_construction, tree_simplification, importance_analyis and **common_cause_analysis**. The *interface* KSs are responsible for the interaction between the blackboard, the databases and the algorithms. The interface KSs of the system are **plant_editing**,and **data_base_handler**.

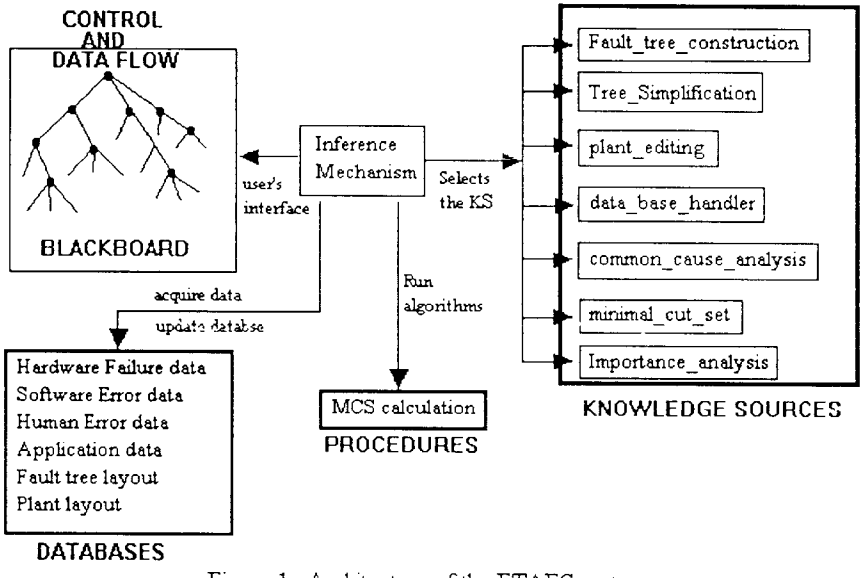

Figure 1 : Architecture of the FTAES system

Procedures, such as minimal cut set evaluation, are defined as *methods* or instances of a class named Minimum_Cut_Set_Procedures.

The *data-base* KS stores any useful information about previously analyzed systems and failure data. The *inference mechanism* processes the high level code, passes instructions to the computer and controls the data flow between the knowledge sources, procedures and databases. The *user interface* includes interactive menus, graphics editors of plant diagrams and fault tree layouts, explanation facilities and report generation. Public domain information is stored at the *blackboard* for common use. Individual KSs are loaded, executed and unloaded from the blackboard.

3 REPRESENTING THE FAULT TREE DOMAIN WITH OBJECTS

A fault tree is a combination of terminal and intermediate events. An *intermediate event* can be further decomposed into events. A *terminal event* is an event that is not resolved further into its causes. The suitability between a fault tree structure and the object oriented modeling facilities are obvious. Figure 2 shows some of FTAES' class definitions. Each class is defined with its particular properties, icons and procedures. Any element of the domain (class,object) can be decomposed, if

necessary, into additional levels (sub-classes,sub-objects). This strategy might be necessary to specify the particular behaviour of a goup of objects.

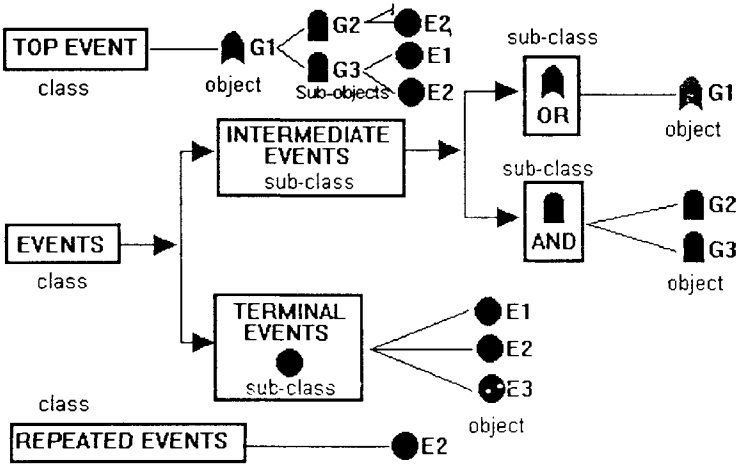

Figure 2: Class definition at FTAES blackboard

The class TOP EVENT is used to code the particular behavior of this type of event for the different stages. The class EVENTS is used to define the generic properties and strategies to be used for rules and methods construction. Particular procedures for calculation of probabilities and Boolean algebra are defined for the classes REPEATED_EVENTS, AND, OR, TERMINAL EVENTS and INTERMEDIATE EVENTS.

Objects representing the fault tree events are dynamically defined (runtime) as instances of the class definition of Figure 2. A graphic editor permits insertion, deletion or addition of events to the current structure. The tree configurations are stored at the database, and can be loaded, or combined, at the blackboard for further applications.

4 KNOWLEDGE REPRESENTATION

Classes, objects, properties and methods are used to define the fault tree to be analyzed by the system. *Rules* capture the knowledge necessary to solve particular domain problems and represent among other things, relations, heuristics, procedural knowledge, and the temporal structure of knowledge. Rules are used at the knowledge sources to perform the qualitative reasoning and control the data flow at the blackboard. Large sets of rules can be grouped according to intended purposes and they are represented by a Boolean property or *hypothesis*. Hypotheses at various levels of the blackboard are related through structural relationships. The hypothesis *absorption_laws* in Table 1 is associated with a rule to process the absorption laws of the Boolean Algebra for any intermediate event of the fault tree. This hypothesis is related with the KS named

"*Tree_simplification*". The conditional pointers A, N1 and N2 are used by the rule to select the appropriate objects from the blackboard database. The classes named EVENTS, AND and OR are defined according to figure 2. When the premise of the rule is satisfied, the related hypothesis is validated, and the correspond action executed by the inference mechanism of FTAES. The KS "*Tree_Simplification*" contain rules based on the Boolean Algebra and expert's heuristics. This KS is used by the blackboard to simplify and reduce the number of events of large fault tree definition. In many cases, the sets of rules for fault tree simplification are sufficient to reduce the tree to the minimal cut set configuration. In order to evaluate the rules of an hypothesis associated to a particular KS, the inference mechanism of the customized blackboard adopts the following procedure: (1) Load the related KS to the blackboard; (2) Evaluate the set of rules of the current hypothesis; (3) Unload the KS from the blackboard. The value of the hypothesis is stored at the blackboard and remains available for further evaluation. The KS "*minimal_cut_set*" contains the control rules that select and evaluate the appropriate minimal cut set procedure for the current application. Number of events, repeated events, and the dimension of probability and error rates are analyzed to select the best methodology for MCS evaluation.

Symbolic representation	Rule hypothesis : Absorption_laws
N2= A∩N1 N1= (A∪B) N2=A	Conditional pointer definition: For any A such that (A is a member of EVENTS); For any N1 such that (N1 is a member of OR) and (A is a member of N1); For any N2 such that (N2 is a member of AND) and (A is a member N2); Premise IF N1 is a member of N2 Action THEN Absorption_laws is TRUE and delete the connection from N2 to N1 and N2 is equal to A ELSE Absorption_laws is FALSE

Table 1: Rule representation of the absorption law of Boolean algebra at the G2 environment

The procedures for MCS evaluation were developed with a combination of rules and methods based on the following well-known minimal cut set algorithms [13]: Boolean algebra method, combination testing method, prime number method and binary bit string method. In order to increase the speed rate of calculation, the original fault tree is reduced before MCS. The KS *common_cause_analysis* interacts with the user in order to identify potential mechanisms that can cause more than one failure or degrades the performance of system components. This KS identifies the common causes and their domains, the terminal events susceptible to the common causes, the common cause candidates, the prime common cause candidates, significant common causes, and partially affected

minimal cut sets. Qualitative and quantitative analyses are performed at this stage. The KS *Importance_analysis* executes the Vesely-Fussell measure of importance for minimal cut sets and terminal events. Since the KS's are independent chunks of knowledge any other importance measure methodology can be defined by the programmer according to the user's needs. The KS of FTAES where developed and represented in order to assist non-expert user's at the fault tree analysis evaluation.

5 HANDLING AND PROCESSING UNCERTAINTY

Failure rates and error rates are important variables in equipment reliability and human reliability calculations, respectively. However, it is said that human judgement holds a central position in all safety analyses of complex systems because:

a) It is necessary to collect lots of data to estimate failure and error rates. In practice, since sample data collection is often not possible, failure and error rates are estimated by experts based on their engineering judgement.
b) Reliability rates may be affected by many factors: the environment in which equipment is operated, the environmental task condition, psychological stress of a human operator, etc. In conventional reliability analysis the basic error and failure rates are adjusted by experts based on experience and judgement in order to include the effect of many external and operational factors on reliability.

Although rules can be used within an expert system to code the required heuristics to adjust and process failure and error data, it is not easy to handle and process uncertainty with the traditional approach. Risk is a "fuzzy" concept, in the sense that a single risk score, such as the probability of failure of the top event on FTA, cannot summarize all the hazard implications. The degree of uncertainty, whether caused by equipment failure or human error can lead to a system accident. The relation between reliability and factors affecting reliability cannot be expressed clearly using traditional formulations. However, it is comparatively easy to express this kind of uncertainty qualitatively. The fuzzy set approach offers a qualitative methodology to represent and reason with uncertain, vague or fuzzy information. Although the theory of fuzzy sets is relatively new, the calculus of fuzzy sets is well developed, with various applications in engineering, such as the application of fuzzy sets to engineering design, structural optimization, structural damage assessment, safety failure analysis, risk analysis, fault tree analysis. Controversial publications have also been reported comparing probabilistic with the possibilistic (fuzzy) approaches. The authors of this work believe that the selection of an appropriate methodology (fuzzy or traditional) for a FTA application depends on data availability and the process specific knowledge. Whenever the uncertainty involved is "low", the traditional approach seems to be more applicable. Otherwise, the fuzzy approach may be more desirable. FTAES performs both the traditional and the fuzzy approaches.

The *fuzzy mode* evaluates the fault tree according to the qualitative evaluation of the basic events. Instead of probabilistic numbers, the user is able to represent the failure rate with linguistic variables, such as "low", "high", "probable", "unprobable". The fuzzy inference of FTAES processes the qualitative failure rates, represented with numerical membership functions[12]. The result of the analysis is a linguistic variable representing the "fuzzy" possibility of failure of the top event. Fuzzy algebra is also used to validate probabilistic failures based on the deep knowledge of the plant.

Example: To illustrate the advantages of the knowledge source integration of FTAES, consider the oil production plant of an off-shore platform shown in figure 3. The plant diagram was built with FTAES graphic editor. Each element of the plant is represented by an object at the blackboard.

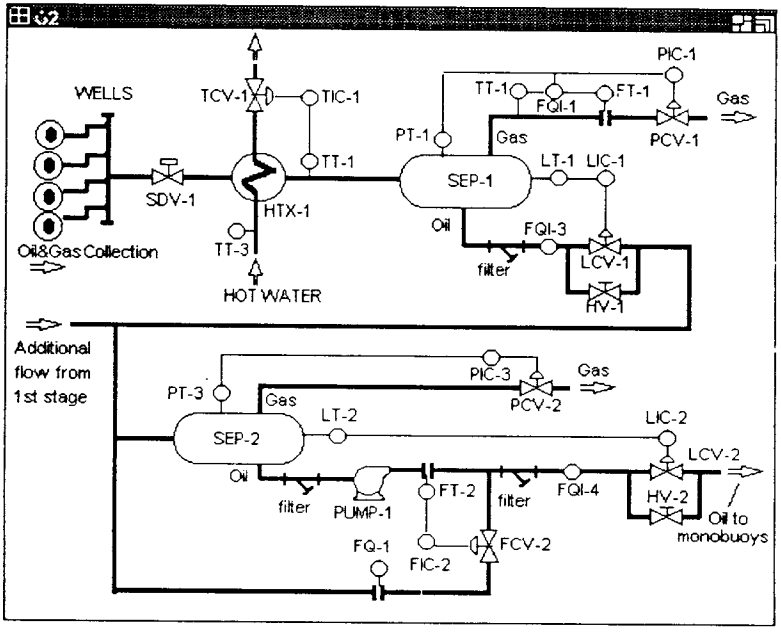

Figure 3: Gas & Oil Separation Plant

The production of the wells is gathered in the production collector that routes it to the heat exchanger HTX-1, in which the mixture is heated, The oil-gas separation occurs in the separator vessel as a result of the different densities of the fluids. In the two-phase separation plant considered here, only gas and oil are separated. The gas is then compressed, dehydrated and sent to gas pipelines, while oil goes to the second stage of separation. The part of the gas that deals with the processing

of gas is not considered in this application. The oil that leaves the first stage still carries some gas, thus a second stage of separation at a lower pressure is required. The atmospheric vessel SEP-2 separates any residual gas before oil exportation. The control loop FIC-2 acts on valve FCV-2 located at the reflux pipe to prevent PUMP-1 from operating below the minimum flow rate recommended by manufacturer. The entire plant was divided into subsystems. Each subsystem is represented by a fault tree at FTAES data base. Figure 4 shows the network of the current application. The Supervisory Control and data Acquisition System (SCADA) is connected to MONDIG, a real time fault detection and diagnoses expert system[7], which displays the process data to the operators via a user-friendly interface.. An ethernet network connects the single-loops and the PLC of the plant to the supervisory system. FTAES acquire PLC and sensor data from SCADA and failure data from MONDIG, performs the probabilistic evaluation of the basic events of the fault tree and updates the data base of the system.

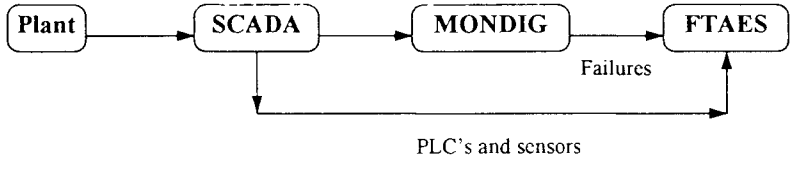

Figure 4: "Expert" Network of the example of figure 3

The risk of failure of basic events are evaluated and classified into "generic", "local" and "fuzzy" rates. The "generic" rate is retrieved from the available generic data bases for similar equipment. The "local" rate is calculated by FTAES based on the frequency distribution of failures acquired from the real time fault and diagnostic system. Local rates are only available when FTAES is connected to a real time diagnosis system. A "fuzzy" rate is defined with linguistic variables to qualify the "generic" rates. In the absence of "numeric" probabilistic rates, the user selects the appropriate fuzzy variables for the basic events. The "local" rates are used to modify the state of "generic" or "fuzzy" information based on the "deep knowledge" of the plant. Table 3 shows the influence of local data on the final probability rates of the components of Event G15 "Failure of the outlet pipe of SEP-1".

FAILURE EVENT	GENERIC RATE	LOCAL DATA FREQUENCY	FUZZY RATE	PROBABILITY RATE SUGGESTED BY FTAES
E15-1 HV-1 opened	$0.245x10^{-04}$	0.78	"Reasonably probable"	0.00368
E15-2 Hydraulic system of LCV-1	unknown	0.0	"Extremely remote"	$0.344x10^{-08}$
E15-3 Mechanic failure of LCV-1	$0.988x10^{-05}$	0.0	"remote"	$0.988x10^{-05}$
E15-4 Maintenance of FILTER-1	0.00105	0.22	"frequent"	0.00105

Table 2 : Probability rates of basic events of G15

In the specific case of event E15-2, where no "generic" data was found, the user establishes the possibility of failure with a fuzzy evaluator: "Extremely remote". A fuzzy logic analysis is performed by FTAES to infer the probability of failure. Data inconsistencies were also found by the system between events E15-1 ("reasonably probable") and E15-4 ("frequent"). The local rate of E15-1(0.78) is higher than the local rate of E15-4 (0.22). The generic data disagrees with the correspondent fuzzy rates. A warning message is shown to the user, in order to correct the inconsistencies or accept the system suggestions. In the above case, the system is responsible for the probability distribution arrangements.

6 CONCLUSION

The Fault tree analysis is a knowledge acquisition structure that has been extensively explored by knowledge engineers. Reliability engineers can take advantage of the several techniques and methodologies developed by this area of computer science to: 1)improve the data acquisition process; 2)explore the benefits of object oriented expert systems for reliability applications; 3)integrate the several sources of knowledge into a unique system; 4)explore the approximate reasoning to handle uncertainty; and 5)develop hybrid solution strategies combining expert's heuristics, conventional procedures and available failure data. FTA expert systems gather into a single program experts' experience, available algorithms, and the databases required for FTA, in order to improve the user's productivity and the quality of results. The primary benefit of structuring FTAES into a blackboard architecture is the potential use of multiple experts for different stages of the FTA. This architecture can accept any knowledge type and seems to be a reliable mechanism to integrate databases and procedures with the knowledge base. A fuzzy methodology for fault tree evaluation seems to be an alternative solution to overcome the drawbacks of the conventional approach (insufficient information concerning the relative frequencies of hazard events). To improve the quality of results, the membership functions must be approximated based on heuristic considerations. Process fault diagnosis systems can be included as knowledge sources of the FTAES blackboard, in order to automatically update the failure database of the system. Conventional algorithms for MCS where represented with an object-oriented programming. No further developments where made to improve the efficiency of such procedures. The purpose of this work is to describe the knowledge engineering approach, directed to integrate the different sources of knowledge involved in a FTA. Future developments foresee automatic fault tree generation. The Fault tree can be automatically created from the sub-trees stored at the FTAES database.

7 REFERENCES

1. Patterson-Hine F.A., Koen B.V. Direct evaluation of fault trees using object-oriented programming techniques, *IEEE Trans. Reliability*, vol 38, Nº.2, June, pp 186-192, 1989.
2. Garriba S., Guagnini, E. and Mussio, P. An expert system for tree consruction, *Proceedings Annual Reliability and Maintainability Symposium*, pp 82-88, 1985.
3. Kurzawinski, K.M. and Smurthwaite, R. Automated fault tree analysis via (AI/ES), *Proceedings Annual Reliability and Maintainability Symposium*, pp 331-335, 1988.
4. Poucet A. STARS - Knowledge based tools for safety and reliability analysis, *Reliability Engineering and Safety*, vol. 30, N1, pp 379-397, 1990.
5. Elliott, M. Knowledge-based systems for reliability analysis, *Proceedings Annual Reliability and Maintainability Symposium*, pp 481-489, 1990.
6. Gensym Corporation, "G2 Reference Manual for G2 V2.0", Cambridge, MA, 1990.
7. Teixeira E., Kaszkurewicz E., Bhaya A., Ebecken N., Filho M.,.Bogarin J and Xerez M. A Knowledge-based system for auit detection and diagnosis in oil production plants in offshore platforms, *III World Congress International Federation of Automatic Control*, vol. 5, pp 279-282, Sydney, Australia, 1993.
8. Himmelblau D.M. Fault detection and diagnosis in chemical and petrochemical processes, *Chemical Eng. Mon.*, 8, Elsevier , Amsterdan, 1978.
9. Kim I.S., Modarres M. Application of goal tree - success tree model as the knowledge-base of operator advisory systems, *Nuclear Eng. and Design*, vol. 104, 1987, pp 67-81.
10. Chen L.W., Modarres M. Autonomous decision making expert system for fault administration, *Published G2 Success Stories 1990*, Gensym Corporation, Cambridge, MA.
11. Patton R.P., Clark R. Fault diagnosis in dynamic systems: theory and applications, *Prentice Hall 1989*, Cambridge, GBr.
12. Singer D. A fuzzy set approach to fault tree and reliability Analysis, *Fuzzy sets and Systems*, vol. 34, pp 145-155, North Holland, 1990.
13. Sundararajan C. Guide to reliability engineering, *Van Nostrand Reinhold*, New York, NY, 1991.
14. Blockley D. Engineering safety, *McGraw-Hill Book Company*, London, 1992.