A tool supporting evaluation of non-Markovian Fault Trees

G.Bucci, L.Carnevali, E.Vicario
Dipartimento Sistemi e Informatica - Università di Firenze
bucci@dsi.unifi.it, carnevali@dsi.unifi.it, vicario@dsi.unifi.it

Abstract—Fault Trees are widely employed in the industrial practice to support safety and reliability analysis. Various works have improved the classic formulation by replacing fixed probabilities of leaf events with Markovian distributions over time. We present operation principles, user interface and implementation architecture of a tool supporting editing and evaluation of Fault Trees where the time of occurrence of leaf events follows a generalized probability density function.

I. INTRODUCTION
Fault Trees (FT) are widely employed in the industrial practice as a means to represent the hierarchical relationships among causal factors that can yield an undesired outcome called Top Event (TE). FT Analysis (FTA) supports reliability and safety analysis through the derivation of the TE probability as a combination of the probabilities of leaf events according to the system fault tolerance architecture.

In the classic formulation, probabilities are associated with leaf events with no reference to their time of occurrence. However, reliability of system components often evolves over time, due to such factors as components aging; operation modes changing over time; maintenance and rejuvenation processes. In these cases probability of the TE at different instants of time must be repeatedly recomputed in a kind of polling process.

In [8], leaf events of a Fault Trees with Repeated Events (FTRE) [9] can be associated with an exponential distribution and the TE probability over time is derived by composition of exponential rates through approximate analysis. In [10], the time of occurrence of each leaf event is associated with a probability distribution function and the FTRE is translated into a Generalized Stochastic Petri Net (GSPN) model [11]. Thus, under the assumption that all leaves have a negative exponential probability distribution function, the evaluation of the FT is reduced to the analysis of a Continuous Time Markov Chain (CTMC). This also opens the way to extend modeling power with state space concepts that may account for dependencies and complex repair mechanisms. In [12] a parametric fault tree is translated into a Stochastic Well-Formed Coloured Net in order to generate a lumped Markov chain. As a common trait, in all these works the time of occurrence of leaf events is associated with a negative exponential probability distribution function. This rules out representation of relevant patterns occurring in reliability engineering such as a periodic operation or maintenance process which results in a synchronous recurrent regeneration.

II. USER INTERFACE AND ANALYSIS PRINCIPLES
The tool provides two operation modes for the editing and analysis stages. Fig.2 shows the interface in the editing mode. The panel on the left supports graphical interactive creation of a FT composed by leaf and intermediate events, connected through AND, OR and KofN gates. The panel on the right supports definition of probability density functions (pdfs) associated with leaf events; the interface natively features exponential, uniform and Weibull distributions, while any user-defined density function can be expressed in textual form following the syntax of the Mathematica formalism [13].

Fig.3 shows the interface in the analysis mode. In this case, the tree on the left panel becomes non-modifiable and operates as a selector to focus the analysis on any leaf, or on any intermediate event or on the Top Event. The interface supports qualitative analysis consisting in the enumeration of Minimal Cut Sets (MCS), i.e minimal combinations of leaf events that lead to the occurrence of the TE. In general, quantitative evaluation of a Fault Tree can follow either an indirect approach which derives the probability of the TE...
Fig. 2. A screen shot showing the panel for the editing stage.

Fig. 3. A screen shot showing the panel for the analysis/simulation stage.

by combining the probabilities of all the MCS, or a direct approach which repeatedly combines nodes probabilities at each gate of the tree [8]. The present version of the tool uses the direct approach, which prevents representation of repeated events but reduces the computational effort and provides as a by-product the probability functions at intermediate nodes of the tree. Results of the evaluation are shown in the right panel, which provides a view on Mean Time To Failure and on reliability, unavailability and failure rate functions of each event selected in the tree. For any selected time, the left panel also highlights the most critical MCS, i.e. the MCS that exposes the highest contribution to the current probability of the TE. Finally, the user can assert the occurrence of events of failure or substitution (which indeed result in the replacement of a leaf event) to simulate operation conditions and to help the identification of maintenance policies that can maintain an acceptable level of reliability within a given mission period.

III. IMPLEMENTATION ARCHITECTURE

The architectural schema of the tool is reported in Fig. 4. The graphic user interface (GUI) permits interactive model editing and provides visualization of the results of the analysis. The Application Engine implements the logic to perform FT analysis/simulation. Since tree events are associated with a distribution over time (rather than with a fixed probability), the evaluation involves symbolic manipulation of pdfs, which is delegated to the kernel of Mathematica [13] through J/Link libraries. Mathematica also supports plots of functions derived in safety analysis. Both the GUI and the Application Engine take advantage of FaultCat libraries [14], which have been extended so as to allow symbolic definition of pdf for basic events.

The tool was developed as a part of a research Project aimed at the development of a decision support system for maritime transportation. In this context, the Application Engine has been cast into a client/server architecture receiving data concerning the actual operating conditions and providing predictions on the occurrence of undesirable events. The SW interface relies on a web-service interface which features three main web services supporting: upload from the client of the XML encoding of a FTRE, which includes serialization of leaf event pdfs encoded in the syntax of the Mathematica formalism; request from the client for the encoding of pdfs and/or their graphical plot in GIF format; request from the client for a change in pdfs of leaf events.

Acknowledgments This work has been supported by the GIESDAM Project, partially funded by Tuscany Regional Government, under Measure 1.8 of Dopup 2000-2006. The ITEA-DS Graphical User Interface was developed by Rigel Engineering, in the context of ITEA-DS Project (IST1999-20254) funded by the European Community.

REFERENCES