information

MDPI

Editorial

Editorial for the Special Issue on "Fault Trees and Attack Trees: Extensions, Solution Methods, and Applications"

Daniele Codetta-Raiteri

DiSIT, Computer Science Institute, Università del Piemonte Orientale, 15121 Alessandria, Italy;
daniele.codetta@uniupo.it

Fault Trees are well-known models for the reliability analysis of systems, used to compute several kinds of qualitative and quantitative measures, such as minimal cut-sets, system failure probability, sensitivity (importance) indices, etc. Fault Trees represent the possible combinations of component failures leading to system failure by means of logic gates (or ports). During the years, Fault Trees have been extended to increase their modeling power and deal with component dependencies, multistate components, repair, etc. The modeling elements introduced to this end, such as new gates, required the definition of new solving procedures, typically based on the Fault Tree conversion into other models, such as *Binary Decision Diagrams* (BDD), *Markov chains*, *Petri nets*, *Bayesian networks*, etc. Besides their application in reliability analysis, Fault Trees have been exploited to model attack modes and evaluate the security level of systems. In this field, they are called *Attack Trees* and have been extended to represent both attacks and countermeasures. Software tools and libraries for Fault/Attack Trees have been developed and improved over the years. The goal of this Special Issue is to collect recent developments in Fault/Attack Tree extensions, solution methods, software tools, and applications in reliability/security evaluation.

The articles in this Special Issue cover a wide range of case studies examined by means of *Fault Tree Analysis* (FTA), where the models are constructed following approaches defined for the application fields. FTA, based on BDD, is applied to wind turbines in [1]; given the many interrelations among the components, the size of the BDD influences the computational cost of the analysis and depends on the order of the components (events) considered; so, different heuristic ranking methods are tested in the BDD construction. Besides system reliability, importance measures are computed for each component, providing the basis for maintenance strategies. Another case study, concerning the power system of a fishing vessel, is evaluated in [2]. Since this system operates with different operational configurations (according to the current activity of the vessel), system dependability metamodeling is applied: a detailed metamodel is built and then adapted to the operational status under exam, thanks to a vector of external events. For each configuration, the most critical components are identified by computing specific importance measures. In [3], the application of FTA clarifies the causes of troubles involving *Embedded Control Software* (ECSW) and suggests countermeasures. First, *Fault Tree Templates* (FTT) are prepared and reflect the instructions of the ECSW; then, the Fault Tree is developed by combining FTTs according to backtracing of the instructions' execution. This approach helps the analyst in the construction of the model; in the computation of appropriate results; and finally, in the improvement of the safety level of ECSW.

Besides these cases of reliability assessment through FTA, in [4], Attack Trees are security models of vehicles characterized by sensors interacting with the surrounding environment. In order to identify, assess, and mitigate the vehicle vulnerabilities and the corresponding threats, the authors present the *Software, Asset, Vulnerability, Threat, and Attacker* (SAVTA) method, which combines different existing modeling approaches to create a comprehensive and hybridized model. The model is, in turn, an aid to construct general Attack Trees, where every subtree is dedicated to a specific attack.

Citation: Codetta-Raiteri, D. Editorial for the Special Issue on "Fault Trees and Attack Trees: Extensions, Solution Methods, and Applications". *Information* **2021**, *12*, 175. https://doi.org/10.3390/info12040175

Received: 14 April 2021
Accepted: 15 April 2021
Published: 20 April 2021

FTA is easy to implement, but is based on the simplified hypothesis that components' malfunctions are independent from each other and from the system's working conditions. Recent contributions have shown the potential to improve the accuracy of FTA. In [5], *Stochastic Hybrid Fault Tree Automaton* (SHyFTA) combines a dynamic model with a physics-based deterministic model of the system process and is supported by a software library. To demonstrate its utilization, generating further dependability indicators, three different case studies are solved through SHyFTA models. *Finite Degradation Models* (FDM), presented in [6], consider the states of the models as the degradation levels of the system. In this way, FDMs generalize and unify models like *Fault Trees*, *Attack Trees*, *Reliability Block Diagrams*, etc. In order to extract from FDM the most relevant scenarios of failure (minimal cut-sets), the authors define algorithms based on decomposition theorem and BDD. Implementation and performance issues are discussed with the aid of a use-case from the oil and gas industry.

In summary, this Special Issue about Fault/Attack Tree modeling and analysis covers aspects like the model construction according to the application domain, extensions to the modeling power with the necessary solution techniques, and case studies from different fields. We hope that these articles help us advance in our understanding of Fault/Attack Tree capabilities in reliability/security assessment of infrastructures characterized by dependability requirements.

Funding: This work is original and has a financial support of the Università del Piemonte Orientale.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BDD	Binary Decision Diagram
ECSW	Embedded Control Software
FDM	Finite Degradation Models
FTA	Fault Tree Analysis
FTT	Fault Tree Templates
SAVTA	Software, Asset, Vulnerability, Threat, and Attacker
SHyFTA	Stochastic Hybrid Fault Tree Automaton

References

1. García Márquez, F.P.; Segovia Ramírez, I.; Mohammadi-Ivatloo, B.; Marugán, A.P. Reliability Dynamic Analysis by Fault Trees and Binary Decision Diagrams. *Information* **2020**, *11*, 324. [CrossRef]
2. Chybowski, L. Importance Analysis of Components of a Multi-Operational-State Power System Using Fault Tree Models. *Information* **2020**, *11*, 29. [CrossRef]
3. Takahashi, M.; Anang, Y.; Watanabe, Y. A Proposal of Fault Tree Analysis for Embedded Control Software. *Information* **2020**, *11*, 402. [CrossRef]
4. Hamad, M.; Prevelakis, V. SAVTA: A Hybrid Vehicular Threat Model: Overview and Case Study. *Information* **2020**, *11*, 273. [CrossRef]
5. Chiacchio, F.; Aizpurua, J.I.; Compagno, L.; Khodayee, S.M.; D'Urso, D. Modelling and Resolution of Dynamic Reliability Problems by the Coupling of Simulink and the Stochastic Hybrid Fault Tree Object Oriented (SHyFTOO) Library. *Information* **2019**, *10*, 283. [CrossRef]
6. Rauzy, A.; Yang, L. Decision Diagram Algorithms to Extract Minimal Cutsets of Finite Degradation Models. *Information* **2019**, *10*, 368. [CrossRef]