CHEMICAL ENGINEERING TRANSACTIONS
VOL. 116, 2025
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani

ISBN 979-12-81206-18-2; **ISSN** 2283-9216
DOI: 10.3303/CET25116027

On the Use of Fault Tree Analysis to Capture Dynamic and Multistate Aspects in the Analysis of Hydrogen Systems

Dikshya Bhandari*, Jon Tømmerås Selvik

University of Stavanger, Department of Safety, Economics and Planning, Stavanger, Norway
dikshya.bhandari@uis.no; jon.t.selvik@uis.no

Hydrogen systems are being deployed to reduce fossil fuel dependence and support cleaner energy. Large-scale upscaling of hydrogen technology demands a strong understanding of reliability and risk. Fault tree analysis is a way to support this understanding, as a deductive technique utilized to assess failure paths and probabilities. However, traditional fault trees are often criticized for being static, having limited ability to model dynamic behaviors and multistate events, and relying on fixed probabilities for quantification. This paper explores alternatives to the traditional method and considers their relevance and attractiveness when assessing the reliability and risk of hydrogen systems. The focus is on how to capture dynamic behavior and multistate aspects in the technique. The applicability of the dynamic fault tree and multistate fault tree techniques was studied using three examples of a hydrogen storage explosion due to overpressure. The findings indicate that the two techniques add relevant aspects but also introduce complexities and uncertainties. To improve decision-making in this context, expanding the treatment of uncertainties is recommended to achieve more informed decision support. It is suggested that the strength of knowledge analysis be incorporated into the analyses.

1. Introduction

As hydrogen technology expands, understanding system reliability and risks is essential. Hydrogen is highly flammable, easily ignited, and weakens materials over time, raising failure risks. With increasing system complexity, practical and reliable tools grounded in solid math are needed to ensure safety (Buchacker, 2000) Fault Tree Analysis (FTA) is a deductive technique that is utilized to assess the likelihood of failures within such systems. FTA helps understand how individual component failures can lead to system failures. Traditional FTA (TFTA) uses simple gates, such as AND and OR gates, which are straightforward to understand. However, TFTA is often criticized for its static nature and limited ability to model dynamic and multistate behaviors. This limitation has led to challenges in prioritizing critical failures and in managing redundancy and dependency effectively (Huang & Chang, 2007).TFTA typically uses fixed probabilities to represent the likelihood of component failures, assuming these probabilities remain constant over time. However, maintenance activities such as repairing or replacing components can change these probabilities; consequently, TFTA cannot adapt to these changes dynamically (Andrews & Tolo, 2023). In response to these shortcomings, various extensions to TFTA have been proposed in the reliability literature. These modifications aim to address data uncertainties, improve visualization, and incorporate the complexities of engineering systems. The most researched and well-known extension is Dynamic Fault Trees Analysis (DFTA), which models the sequential and time-dependent failures, but other extensions such as Fuzzy Fault Tree Analysis (FFTA), State-Event Fault Tree Analysis (SEFTA), Repairable Fault Trees Analysis (RFTA), Stochastic Hybrid Fault Tree Automaton Analysis (SHFTA), and Multi-state Fault Tree Analysis (MSFTA) are gaining attention as well. The objective of this paper is to consider FTA techniques, specifically focusing on their relevance to hydrogen systems. Based on a literature review, possible improvements of FTA are identified, highlighting how various extensions address data uncertainties and improve visualization for complex engineering systems. The paper provides examples of DFTA and MSFTA, discusses their challenges and usefulness in risk assessment, and applies them to a case study of a hydrogen storage explosion due to overpressure.

Paper Received: 20 November 2024; Revised: 20 January 2025; Accepted: 19 April 2025
Please cite this article as: Bhandari D., Selvik J.T., 2025, On the Use of Fault Tree Analysis to Capture Dynamic and Multistate Aspects in the Analysis of Hydrogen Systems, Chemical Engineering Transactions, 116, 157-162 DOI:10.3303/CET25116027

2. Candidates for FTA improvement

FTA identifies root causes using Boolean logic through basic gates (e.g., AND and OR). These gates assume binary states for components (working or failed). For a more detailed description, reference is made to IEC 61025 (2006). However, as noted in the introduction, the traditional technique has limitations.
Recent FTA research has a focus on advanced methods that better capture dynamic change, multistate event, and their impact on risk levels. DFTAS are among the most studied extensions of TFTAs. They are recognized for their ability to capture sequence-dependent behavior, interactions among functionally dependent components, and event priorities (Ruijters & Stoelinga, 2015).

Table 1: Variation and focus of different alternatives of FTA

Improve FTA	Temporal	Visualization	Multi-state event	Data uncertainty
Dynamic FT	X	X		
Multistate FT		X	X	
State-event FT	X	X	X	
Repairable FT	X			
Fuzzy FT				X
Stochastic hybrid automation	X			X

Table 1 shows that the FFTA and SHFTA are specifically designed to handle data uncertainties, while DFT, SEFT, and MSFT focus on improving visualization. RFT can incorporate details about components that can be repaired and the strategies used to manage those repairs. DFTA is the only improved FTA that introduces additional gates for modeling time-dependent events, yet it still relies on a binary state representation. MSFTA overcomes this limitation by allowing for multiple operational states. This paper assesses the effectiveness of DFTA and MSFTA methods in the context of hydrogen systems.

3. Relevant FTA improvements for analysis of hydrogen systems

DFTA includes additional gates that help model spare components, manage backup systems, prioritize failures, and show how one failure can lead to another. MSFTA allows to model more than just ‘working’ or ‘failed’ conditions. It can represent different performance levels for the top event and other events in the system.

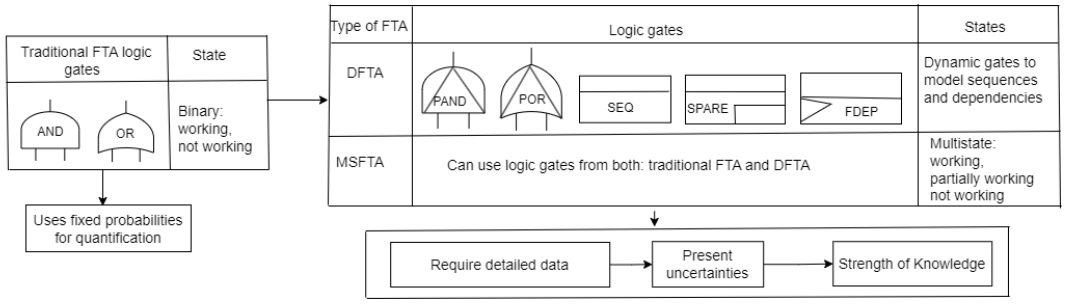

Figure 1: Representation of the difference between TFTA, DFTA, and MSFTA

Figure 1 compares the logic gates and system states used in TFTA, DFTA, and MSFTA. TFTA uses the basic gates with binary states (working or not working). DFTA adds dynamic gates like Priority AND (PAND), Priority OR (POR), Sequence Enforcing (SEQ), SPARE, and functional dependency (FDEP), which still assume binary states but introduce dynamic, sequence-based behaviors. MSFTA can use gates from both TFTA and DFTA while incorporating multistate conditions, allowing for partial failures and different performance levels. TFTA normally uses fixed probabilities for DFTA and MSFTA calculations, which require comprehensive data, which is often hard to obtain, uncertain, and based on assumptions. To improve the reliability of this information, integrating SoK helps assess the quality of the data and assumptions, managing epistemic uncertainties.

3.1 Dynamic FTA

DFTA, developed by Dugan et al. (1992), advances TFTA by incorporating sequence-dependent and time-sensitive failure behaviors. The DFTA has five dynamic gates: PAND, POR, SEQ, SPARE, and FDEP (Taylor & Kozine, 2023). PAND gate is a special type of AND gate in which outputs are true only if its inputs happen in

sequence, from left to right. In the POR gate, the first input is given priority, and the gate output is true only if the first input event happens first. The SEQ gate defines a specific failure sequence within a system where the failure of component B cannot occur before the failure of component A. It models scenarios where the correct sequence of events is critical. The SPARE gate models redundancy by using a main component and backup components. The main component is active first; if it fails, the backups take over in sequence. There are three types of spares: hot (always active), cold (inactive until needed), and warm (partially active). The FDEP gate captures cascading failures triggered by an initial event. These dynamic gates address the complexities of component interactions and varying performance levels, and various mathematical tools can be used for the calculations. For details, see Zhu and Zhang (2022).

3.2 Multistate FTA

MSFTA maintains the same underlying structure as TFTA (Lazarova-Molnar et al., 2020). Unlike TFTA, which only accommodates binary states, MSFTA allows for a more detailed representation of system states. In an MSFTA, both the system and its components may exist in M+1 possible states, ranging from 0 to M. Here, 0 denotes the completely failed state, M denotes the perfectly working state, and the other states represent various levels of degradation. It can be analyzed using various mathematical tools. see Luo et al. (2024).

3.3 Uncertainties

DFTA and MSFTA introduce uncertainties in risk analysis, as they rely on failure modes from historical accidents that may not reflect the complexities of the contemporary system. Additionally, system performance may be influenced by operational practices and environmental factors that are often not adequately captured in historical records. Both methods depend on assumptions about the system's behavior, which, if incorrect, can lead to misleading conclusions. Incomplete information and subjective expert opinions further complicate assessments. DFTA's focus on dynamic changes and MSFTA's multiple performance states add complexity, which is often overlooked in many studies that favour simplified factors over comprehensive uncertainty evaluation. One major issue with DFTA is the lack of well-defined guidelines for constructing and interpreting these models. This has led to inconsistencies in how different researchers apply DFTA, which creates uncertainty about its effectiveness in real-world scenarios. MSFTA involves multiple states for each component, which can increase the complexity. To manage uncertainties in probabilistic risk assessment in general, Aven (2017) suggests a way to assess the SoK that involves assessing reliable data, expert agreement, and reasonable assumptions to improve the quality of the analysis.

4. Examples and discussion

Hydrogen is often produced and stored in high-pressure tanks designed to withstand various stresses such as internal pressure, cyclic loads, and external forces. Overpressure is a critical concern for hydrogen storage tanks, as it can cause explosions if the pressure exceeds the tank limits (Sedmak et al., 2022). DFTA and MSFTA are used to model explosions in hydrogen storage tanks caused by overpressure. Factors such as utility failures, gas outlet blockages, thermal expansion, and pressure relief valve failure can lead to overpressure. The analysis illustrates how DFTA and MSFTA can be applied to an explosion scenario caused by overpressure by using various examples.

Example 1

Consider a simple scenario in which a hydrogen storage tank is at risk of exploding due to overpressure. This overpressure could be caused by the failure of the pressure relief valve (PRV) to open on demand (Event A), which would then lead to excessive pressure build-up in the tank (Event B).

In TFTA, such scenarios are often modeled using an AND gate, where both Event A and Event B must occur for the top event to take place. However, this approach does not specify the order in which these events occur. By extending the traditional AND gate to a PAND gate, the analysis specifies that Event A (failure of the PRV) must occur first, followed by Event B (buildup of excessive pressure), as shown in Figure 2. If the PRV fails to open, there is no mechanism to relieve the pressure, which inevitably leads to the buildup of excessive pressure. This extension defines the sequence of events, events which make the logic easier to understand.

The PAND gate itself does not provide specific time intervals between Event A and Event B. The PAND gate adds order to the analysis, but in some cases, this may not add much beyond what was already understood in the TFTA. To quantify the traditional AND gate, the probabilities of the events are simply multiplied, as they are considered to fail simultaneously. However, quantifying the PAND gate is more complex and typically requires simulation methods. Here, a Monte Carlo simulation is used to model the sequence and timing of failures. The components' time to failure is typically assumed to follow an exponential distribution(Baek & Heo, 2021) DFTA provided a lower risk estimate compared to the TFTA. This difference is logical because TFTA assumes PRV

failure and pressure buildup occur simultaneously, which isn't realistic. If the PRV works, it prevents buildup. The accident occurs only because the PRV fails to open, pressure isn't relieved, and buildup continues, possibly causing the hydrogen tank to explode.

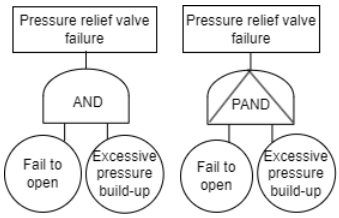

Figure 2: The TFTA AND gate on the left and the DFTA PAND gate on the right represent the failure of the pressure relief valve, which a hydrogen storage tank is at risk of exploding due to overpressure.

Example 2

Overpressure can occur if the pressure inside the tank exceeds safe limits. The cooling system is designed to regulate the temperature and prevent overpressure. If the cooling system fails, the PRV acts as a backup to release the pressure and prevent an explosion. If both the cooling system and the PRV fail, the tank could experience overpressure. This overpressure can result in catastrophic failure, such as an explosion.
DFTA used a SPARE gate to model this scenario as shown in Figure 3, represents the redundancy between the cooling system and the PRV. PRV is intended to prevent overpressure if the primary cooling system fails. But if both the cooling system and the PRV fail, the tank could explode.

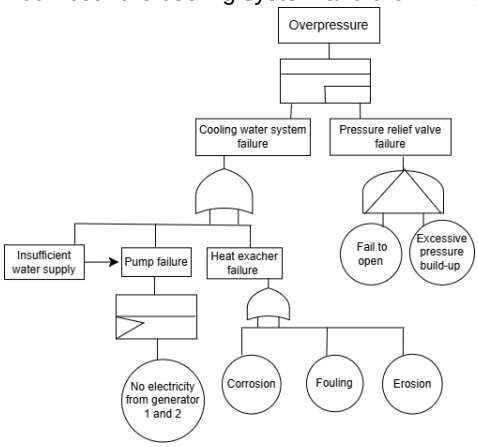

Figure 3: Dynamic FTA showing how overpressure can occur with a SPARE gate, illustrating how the pressure relief valve serves as a backup to prevent overpressure if the cooling system fails.

The SPARE gate can be quantified by using the Monte Carlo simulation as a formula for a PAND gate, but the logical expression is different from the PAND gate as these two gates model two different events. Quantifying the SPARE gate can be complex because the failure rates of the components vary depending on their states (e.g., hot, cold, warm). TFTA does not model this situation, as it assumes constant failure rates for components, regardless of their operational state. The SPARE gate in DFTA can visually represent varying states. Its quantification introduces complexity. It requires detailed data on each component and how different states affect failure rates. Modeling both standby and active components demands advanced analysis techniques.

Example 3

Overpressure in a hydrogen storage tank, which could cause an explosion, may result from the pressure relief valve failing to open (Event A) or from vent failure (Event B). To model this scenario using TFTA, an OR gate would typically be used to represent the failure of the pressure relief valve, assuming it fails either due to failure to open or vent failure, without considering the different states of each failure mode. MSFTA allows both the top event and the basic events to have multiple possible outcomes, as shown in Figure 4. It can take a range of scenarios, such as the pressure relief valve causing overpressure, not just because it failed to open or had a vent failure but also because of other possible failure states. The possible states for the pressure relief valve

(top event) are 1: The pressure relief valve is working fine, 2: It fails to open, 3: vent failure, and 4: Both fail to open and vent failure occurs.

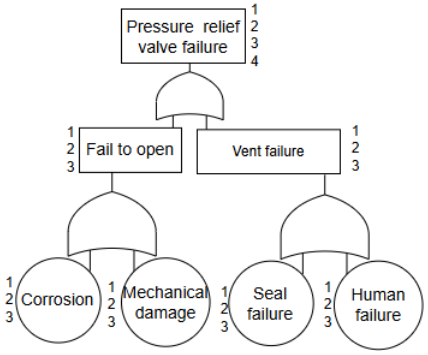

Figure 3: Multistate FTA of pressure relief valve failure, Numbers 1, 2, and 3 represent the different states.

Table 2 shows that MSFTA can capture different failure scenarios, such as a valve that fails to open but has no vent failure, a valve with vent failure but no fail-to-open condition, and both failure scenarios occurring at the same time. Considering different failure scenarios is more realistic in a complex system like hydrogen. Using this detailed approach provides a more comprehensive risk assessment.

Table 2: Different states for each event in the multistate FTA

Type	Failure mode/Basic event	State 1	State 2	State 3
Intermediate event	Fail to open	Function	Delayed opening	Complete failure
Basic event	Corrosion	correctly	Minor degradation	Major degradation
Basic event	Mechanical damage	No impact	Partial damage	Complete damage
Intermediate event	Vent failure	No impact	Reduced venting	Complete vent
Basic event	Seal failure	No venting issue	Minor seal degradation	Blockage
Basic even	Human error	No leakage	Minor error	Major seal
		No error		degradation
				Major error

Evaluation of SoK for FTA construction

Incorporating SoK into DFTA and MSFTA has the potential to improve their effectiveness and provide decision-makers with a clearer understanding of inherent uncertainties and limitations in modelling. The following attributes should then be considered to ensure that the background knowledge is well-understood while constructing and quantifying complex FTAs like DFTA and MSFTA.

- Understanding of phenomena: A clear understanding of failure modes is crucial for accurate risk assessment. This involves knowing how and why failures occur and using models that describe system behavior under failure conditions.
- Data availability: The quality of data for each failure event must be assessed. It is important to determine whether sufficient, high-quality data exists to support the failure events modeled in the tree.
- Assumptions: To avoid inaccuracies in the risk assessment, assumptions about system behavior must be examined. These assumptions should be reasonable and align with empirical data.
- Expert agreement: Consensus among experts on failure modes and fault tree structure is essential, especially when empirical data is limited, as it helps reduce bias and inconsistencies in FTA.

When applying advanced methods like DFTA and MSFTA, analysts must critically evaluate their analyses to ensure confidence in the results. If a low SoK is identified, they should be cautious and investigate further to improve the reliability of their findings. Evaluating the FTA with SoK improves transparency among decision-makers and analysts. It allows decision-makers to assess how confident the analysts are in their conclusions and understand any limitations associated with the analysis.

4.5 Overall considerations

DFTA can be useful for modeling dynamic behaviors and sequence-dependent failures, which is good for modeling scenarios where the timing of component failures influences the overall risk of the system. MSFTA

provides a realistic representation of hydrogen systems by allowing components to operate at various performance levels rather than just binary states. DFTA is the only extension that introduces an additional gate for modeling time-dependent events, but still relies on a binary state representation. MSFTA addresses this limitation by enabling multiple operational states. Integrating DFTA and MSFTA into a single approach, known as multistate dynamic FTA, could improve risk assessments by capturing both dynamic interactions and multistate performance. However, this integration poses challenges, as it requires a deep understanding of the system and high-quality data for accurate quantification. Different uncertainties can arise in developing DFTA and MSFTA, including gaps in knowledge and subjective perceptions about events. To mitigate these uncertainties, applying the SoK is essential. Despite existing challenges, the proposed techniques help bridge gaps when applied to hydrogen systems and allow for enhanced analysis of complex systems with multiple subsystems and interactions.

4 Conclusions

This paper evaluates the usefulness of DFTA and MSFTA by modeling the hydrogen storage tank explosion due to overpressure. DFTA introduces sequence-dependent and time-sensitive failure behaviors, which improve the modeling of complex failure scenarios. MSFTA allows for multiple failure states, which offer a more detailed risk evaluation. Both DFTA and MSFTA require a thorough understanding of the system, along with detailed failure rate data and advanced quantification techniques. These methods rely on broad assumptions about the system's behavior, timing, and states, which can introduce uncertainty. The uncertainties inherent in both methods may lead to a narrow understanding of risk. To improve this picture, it is suggested that SoK be incorporated while constructing and quantifying the DFTA and MSFTA. SoK evaluates the reliability of the data and assumptions, which is essential in managing the complexities associated with hydrogen systems.

Acknowledgments

The authors are thankful to the Norwegian Research Council and Consortium Partners in FME HyValue for the possibility to publish this paper. RCN Project number: 333151.

References

Andrews, J., & Tolo, S. 2023, Dynamic and dependent tree theory (D2T2): A framework for the analysis of fault trees with dependent basic events. Reliability Engineering & System Safety, 230, 108959.

Aven, T. 2017, Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. Reliability Engineering & System Safety, 167, 42–48.

Baek, S., & Heo, G. (2021). Application of dynamic fault tree analysis to prioritize electric power systems in nuclear power plants. Energies, 14(14), 4119.

Buchacker, K. 2000, Modeling with extended fault trees. Proceedings. Fifth IEEE international symposium on high assurance systems engineering (HASE 2000), (pp. 238–246). IEEE.

Dugan, J. B., Bavuso, S. J., & Boyd, M. A. 1992, Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability, 41(3), 363–377.

Huang, C.-Y., & Chang, Y.-R. 2007, An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees. Reliability Engineering & System Safety, 92(10),1403–1412.

IEC 61025. 2006, Fault tree analysis (FTA). In 61025: IEC - International Electrotechnical Commission.

Lazarova-Molnar, S., Niloofar, P., & Barta, G. K. 2020, Automating reliability analysis: Data-driven learning and analysis of multi-state fault trees. European Safety and Reliability Conference Conference (ESREL),

Luo, X., Li, Y., Bai, X., Tang, R., & Jin, H. 2024, A novel approach based on fault tree analysis and Bayesian network for multi-state reliability analysis of complex equipment systems. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 238(4), 812–838.

Ruijters, E., & Stoelinga, M. 2015, Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review, 15, 29–62.

Sedmak, A., Martic, I., Jeremić, L., Kirin, S., & Golubovic, T. 2022, Effects of Over-Loading on Pressure Vessel Integrity. Procedia Structural Integrity, 42, 356–361.

Taylor, J. R., & Kozine, I. 2023, Continuum fault trees. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 237(6), 1209–1222.

Zhu, C., & Zhang, T. 2022, A review on the realization methods of dynamic fault tree. Quality and Reliability Engineering International, 38(6), 3233–3251.