Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen

doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4382-cd

Comparative Analysis of STPA and FRAM: The Effect of Process Delays for Enhanced Safety and Resilience

Tobias Demmer

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany.
E-mail: tobias.demmer@dlr.de

Babette Tecklenburg

Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR), Germany.
E-mail: babette.tecklenburg@dlr.de

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany.
E-mail: daniel.lichte@dlr.de

Frank Sill Torres

Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR), Germany.
E-mail: frank.silltorres@dlr.de

Understanding process delays can be significant for implementing effective long-term resilience enhancing measures. And looking into those delays also helps understanding the impact of unintended side-effects arising from short-term safety measures. To do that, this work compares the methods System Theoretic Process Analysis (STPA) and Functional Resonance Analysis Method (FRAM) in regard to the implementation and representation of process delays. STPA is a famous example for the combination of control engineering and safety science. It models system failures and successes involving complex dynamic processes. FRAM tackles the same problem from the opposite direction: it was created from the resilience community to analyse system processes. We apply the two methods to the same infrastructure model from the literature and focus especially on how the methods handle delays within processes.

Keywords: STPA, FRAM, Resilience, Infrastructure, Decision Analysis

1. Introduction

The governance of shared resources and human-made infrastructure is a fundamental challenge for societies aiming to promote wellbeing and sustainability. Human societies increasingly depend on complex, interdependent systems that combine natural infrastructures (e.g. rivers, forests, or ecosystems) with human-made infrastructures (e.g. roads, railways, and energy grids), and social infrastructures (e.g., institutions, norms, and governance mechanisms). The management of these systems involves resource users, public infrastructure providers, and the ecological systems they interact with, all of which must coordinate their actions to avoid the overexploitation of resources or the collapse of essential infrastructure.

This complexity is compounded by the fact that the dynamics of infrastructure provision and maintenance often unfold over long timescales, while resource dynamics and user behaviors may change rapidly in response to shifting social, economic, and environmental conditions. The resulting feedback loops in between those can lead to behaviors that are difficult to predict.

System theory offers tools to better understand and model these dynamic interactions: In particular, approaches like Functional Resonance Analysis Method (FRAM) and System Theoretic Process Analysis (STPA) provide complementary perspectives for analyzing complex systems. Both approaches seem to be similar at the first sight and offer valuable insights into the resilience and safety of coupled socio-technical systems.

In this contribution, we apply and compare these two frameworks, FRAM and STPA, within the context of the coupled infrastructure-resource management system presented in Muneeperakul & Anderies (2017). We explore how these frameworks can identify critical leverage points for improving governance and infrastructure management, ensuring that public goods are adequately provided and maintained, and that resource systems remain resilient to both human and environmental pressures.

Through this analysis, we hope to contribute to the growing body of literature on socio-technical resilience by explaining how infrastructure dynamics can be better understood and what is the granular difference between the two methods.

2. Background

In general, the two methods were compared to each other only on very few examples: In Toda et al. (2018), the STPA is used in combination with the FRAM model to detect hazards at a railway crossing. By focusing on each function defined in the system step by step, they propose combining both methods to gain a more comprehensive understanding of the system. McCormack et al. (2018) applied both methods by different analysts to evaluate the risks of a hypothetical hazardous manual task. The results were then compared to a benchmark analysis to assess their alignment. Qiao et al. (2019) analysed incidents in coal mines and concluded that the STPA analysis is more comprehensive than the FRAM but has not such a good graphical representation resulting in the results are not that easy to catch. De Linhares et al. (2021) studied a submarine accident in which a mechanical failure led to flooding and loss of control, resulting in the deaths of all crew members. They concluded that while the STPA and FRAM can be seen as complementary, they differ significantly in detail and scope, and their use may depend on the specific focus of the intended analysis. Yousefi et al. (2019) conducted a method comparison based on a refinery accident. They identified the key difference in that the STPA defines the control structure at a hierarchical level, whereas the FRAM allows for a broader view of the system's subsequent effects.

2.1. The Infrastructure Model

The infrastructure model used in this work is presented in Muneeperakul & Anderies (2017) and describes a coupled socio-ecological system focused on managing resources. The system has four interacting components. Natural Infrastructure, which includes resources such as water, governed by regenerative capacities. Human-made Infrastructure (I_{HM}) which includes both hard (e.g., canals, roads) and soft (e.g., institutions, algorithms) infrastructure that facilitate the extraction and use of natural resources. Resource Users (RU) who use the infrastructure to extract and harvest natural resources. And Public Infrastructure Providers (PIP) who are entities or organizations responsible for maintaining or providing the infrastructure. The model explores how these actors coordinate to provide and maintain public infrastructure and how the condition of this infrastructure impacts the sustainability of natural resource systems.

2.2. FRAM

The Functional Resonance Analysis Method (FRAM) is a system analysis approach typically used to understand complex, dynamic systems by examining the interactions and dependencies between different system functions (Hollnagel 2012). FRAM is claimed to be particularly useful for socio-technical systems where multiple functions interact in uncertain ways (Ghasemi et al. 2024) such as in this case of Resource Users and Public Infrastructure Providers. The method emphasizes identifying how variability in individual system functions can resonate (or amplify) and contribute to overall system behavior, including failure or success (Patriarca et all. 2022). In the beginning of the analysis the analyst does not need full knowledge of the topic of the FRAM. The aspects (see below) help the analyst to gain the necessary knowledge. Of course, an exchange with process owners or experts increases the quality of the FRAM. (Smith et al. 2016)

The first step in FRAM is to identify the (key) functions in the system and describe their inputs, outputs, and interactions. FRAM requires to describe each function based on six components:

1) Input: What is required to perform the function?
2) Output: What is produced by the function?
3) Preconditions: What must be true for the function to occur?
4) Resources: What resources are needed for the function?
5) Control: What controls the function or its execution?
6) Time: When does the function occur?

After this is done, we can already represent these functions graphically and identify how they interact and influence each other. The second step is to look at the variability of the functions within the FRAM model in terms of time and precision. With the gained information the functional resonance is to be determined and recommendation how to deal with that variability should be developed. (Hollnagel 2012) This work only focuses on the identification and representation of the functions as well as the vulnerability of the functions are determined within the FRAM.

2.3. STPA

The System Theoretic Process Analysis (STPA) is a system safety analysis methodology that claims to help to identify potential hazards in complex systems, particularly when systems have multiple interacting components and feedback loops (Leveson 2004). STPA is grounded in systems theory and shifts the focus from merely identifying component failures or faults to understanding the system as a whole, with an emphasis on unsafe control actions and the control structure of the system (Leveson 2016). This method aims to uncover hazards that might not be apparent from a purely component-based analysis, and to assess how interactions between system components can lead to catastrophic outcomes. Four steps are needed to do so:

1) It is especially highlighted that a system description with the key components, their interactions, and system goals is fundamental. The system description forms the foundation for the subsequent analysis, ensuring that no critical elements are overlooked.
2) Once the system is described, the next step is to identify the control loops within the system. These loops consist of controllers, which are the decision-making entities, controlled processes, which are the resources being managed, and feedback channels, which provide information to adjust the control actions. This step highlights the relationships between the different system components and ensures that the influence of feedback mechanisms is fully considered. In many complex systems, control loops are not immediately obvious, and identifying them is crucial for understanding potential hazards that arise from their interactions.
3) After identifying the control loops, the next step is to determine which control actions could lead to unsafe situations. These unsafe control actions may arise from factors such as inadequate system design, improper communication, or failure to detect and respond to changing system conditions.
4) The final step is to describe the system hazards that could result from the unsafe control actions identified in the previous step. These hazards are typically related to the potential for system failures that could lead to catastrophic outcomes, such as accidents, environmental damage, or loss of life.

An extensive literature review for the STPA is given in Patriarca et al. (2022). The review indicates that STPA has been extensively applied across various industry sectors for over 20 years in many journals and conference proceedings. The main application areas are in aviation and automotive industries, while healthcare has gained attention in recent years. They also give the reminder that the involvement of industry professionals is essential for the validation of the analysis results.

3. Application

In the following, the two approaches are applied independently of each other to the infrastructure model from Muneeperakul & Anderies (2017) introduced in Chapter 2. This means that one author did FRAM, while the other followed the instructions of STPA. And only after the development of the models the authors exchanged and discussed the similarities and differences.

3.1. FRAM

Based on the descriptions of Muneeperakul & Anderies (2017) the functions as well as the aspects are derived. While they model the dependencies between the actors, for the FRAM model a sequence of the actions is necessary. As the main process the authors selected the topic "mining of resources" and analyzed that with FRAM. In total two start function exists "community with resource needs" and "discussion about the usage of resources". Inter mediate functions are for example "accessible through public infrastructure" or "development of further parts of the resource". The ending function is "usage of natural resources". That could be for example raw materials, rivers or wind. The entire model can be seen in Fig. 1.

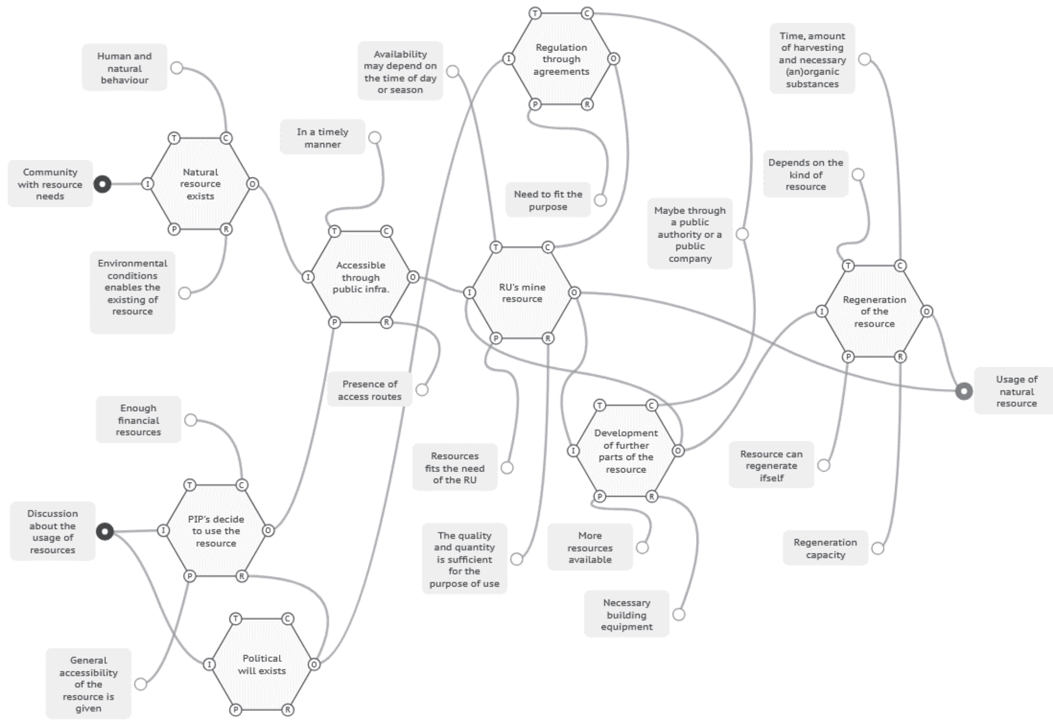

Fig. 1 FRAM model of the usage of resources

After the depiction in the graphical model, for each function the vulnerability is determined as follows: For each function the effect of change in the positive direction or negative direction were determined. And together with the graphical representation the impact of the change to the process evaluated.

The results of this process are shown in Table 1. For example, an increased political will might lead to a faster usage of the resource, because administrative difficulties can be overcome faster. But a decreased political will might lead to a slower process are complete abortion of the usage.

To execute this process the FRAM community developed the "FRAM model visualizer", which allows to examine an entire cycle of the FRAM, including the duration of each function. Within the tool the current active connection is highlighted and remains visible as long as a precondition or resource is not present. Once it is fulfilled the following function is triggered or the process is interrupted. In a depiction as in Fig. 1 the sequence of actions is revealed by the context of the studied system. Hence, the user needs to know before modeling with the FRAM what happens in case of a delay. The user also has to implement if for example another function is activated or if the FRAM stops at this process step. Therefore, while not implicitly showing delays within the FRAM model, the modelling process forces the user to think about process times and timings. This makes the application of the FRAM subjective, which can lead to variability in the analysis process and result in different FRAM models for the same system or process. This is due to the absence of a standardized approach for data collection.

Table 1: Vulnerability of the functions of the FRAM

Function	Form	Effect
Natural resource exists	increased	Higher proportion of resources can be mined, higher political will to mine resources
	decreased	less resources can be mined; resource source might not be considered as worthy enough to access
Accessible through public infrastructure	increased	Better access ways (faster, higher capacity...) lead to an increased mining rate
	decreased	no use of resource is possible
RUs mine resource	increased	capacity of resource decreases
	decreased	no or less resources are consumed
PIPs decide to use the resource	increased	faster accessibility of resource, because more emphasis on the accessibility
	decreased	longer time until accessibility of resource, or no accessibility of resource
Development of further parts of the resources	increased	more capacity of the resource can be mined
	decreased	if no regeneration is possible, the resource will be exhausted
Regeneration of the resource	increased	Higher capacity of resource → more parts of the resource can be mined
	decreased	less resource capacity → decreased usage of resource or exhausted resource
Political will exists	increased	superior power supports the matter → difficulties can be overcome faster
	decreased	less focus on the project → might lead to a faster stop of the project

3.2. STPA

STPA directs the operator more to describe the governing structures and work as imagined. Based on the provided description and differential equations, we identified three main control loops.

1) The RU pay fees (C) to the PIPs to maintain infrastructure (I_{HM}), and in return, they gain access to the resources. The RUs decisions (to work within the system or not) depend on their payoffs from these activities.
2) The infrastructure state (I_{HM}) impacts the productivity of RU, which in turn affects the total harvest and the revenue for PIP. The state of I_{HM} is influenced by maintenance decisions made by the PIP (Eq. 4 in Muneeperakul & Anderies (2017)).
3) The regeneration rate of the natural infrastructure (R) and its exploitation by RUs are governed by the feedback between RUs' use of infrastructure ($NURH(I_{HM})$) and the resource dynamics ($G(R)$). (Eq. 3 in Muneeperakul & Anderies (2017)

The detailed resulting control structure gained from step 1 of the STPA is depicted in Fig. 2

When looking at the system description, the following control actions may result in a system failure, such as a collapse of infrastructure or unsustainable resource use:

1) If the fees (C) or the payoffs for RU are too low, they may choose to leave the system and work outside, leading to the collapse of governance and resource extraction.

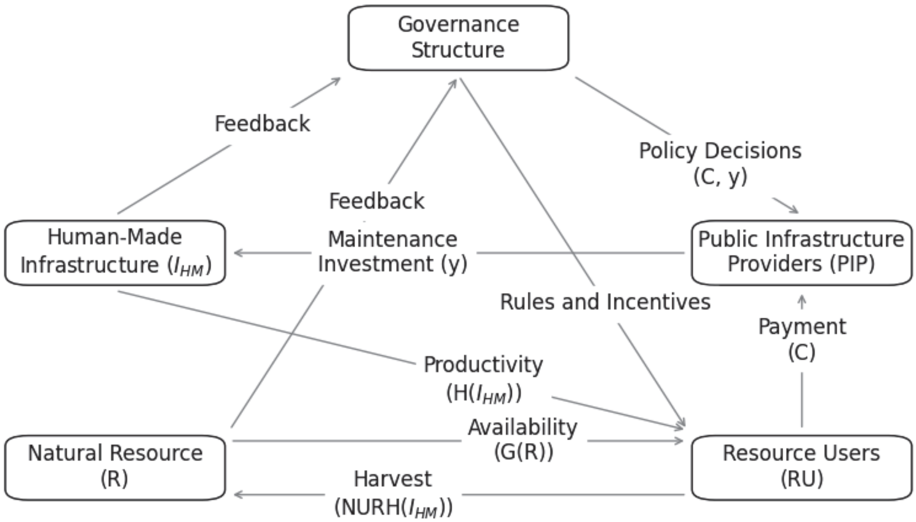

Fig. 2 Control Structure Diagram resulting from the STPA

2) If the PIP invest insufficiently in infrastructure (y too low), the quality of I_{HM} could degrade past a critical threshold, reducing the productivity of RU and potentially collapsing the system.
3) If RU overharvest the resource (R), or if the resource regeneration rate ($G(R)$) cannot keep up with demand, the natural infrastructure collapses, leading to long-term degradation.

From these unsafe control actions, we are able to derive the following resulting hazards: If maintenance investment (y) or the resource fees (C) are too low, the infrastructure could deteriorate to the point ($I_{HM} = 0$) where it is no longer functional and not capable of supporting the RU. Over-exploitation of the resource (e.g., through excessive water extraction) could lead to a collapse of the natural resource ($R = 0$), causing long-term unsustainability and possibly forcing both RU and PIP to abandon the system. If RU find it more profitable to work outside the system (W), or if PIP abandon the system for other opportunities, it could lead to a breakdown in the governance and resource management structure. A negative feedback spiral could occur if infrastructure quality degrades, leading to lower productivity, which in turn discourages investment or usage by RU and PIP, eventually causing system collapse. Process delays are to some extend integrated into STPA as factors that can influence control actions and feedback within the system. The possible delays within the connections are not obvious after the first step, because this models the main control structure and focuses on who controls whom. The step that identifies unsafe control actions afterwards also does not explicitly consider how a missing or delayed control action affects the system. However, this should be implicitly considered when an expert carries out the STPA. Following that the final step should also consider how missing or delayed feedback might lead to a hazard.

For the given example we stated that the amount of fees and payoffs could lead to a collapse, but it is important to mention that the delay in adjustments could result in the same result. The same applies for the invest in infrastructure maintenance. Whenever the infrastructure deteriorates for too long it may become unusable. This issue also extends to harvesting, an overharvesting can happen because of delayed feedback. Although the following hazards remain the same it is important to explicitly mentioned that control actions are always not only about the correct amount but also the timing. Within the STPA handbook delays are mentioned in many scenarios and an expert in STPA should be capable of identifying unsafe control actions and hazards resulting from any process delays.

4. Comparison

Both resulting system representations describe the interactions within the system ex-ante disruptions and try to expose possible disruptions to the operator.

The FRAM focuses on functional interactions or tasks in the system and the primary concern in using the FRAM is the variability in function performance and how it can accumulate through interactions and resonate across the system. The STPA in contrast, focuses more on the governance and the control structure of the system, specifically on unsafe control actions and the identification of hazards that can emerge from those. The primary concern in the STPA is to identify unsafe control actions (e.g., bad decisions, errors, or insufficient control) and how these actions may lead to hazardous outcomes, such as system failure or risks to system safety. In that sense STPA is more about how work is planned, while the FRAM wants to represent how work is actually executed. But both of the methods focus on the success and the failure of systems unlike for example fault trees which only focus on the failure.

Resilience, meant as dealing with disruptions, is the key concept in the FRAM. The method aims for the practitioner to understand how small changes in one function can propagate and amplify across the system leading either to system failure or adaptation. It is more focused on understanding how systems self-organize and how emergent behaviors (like system collapse or sustainability) arise from these interactions. In contrast, in the STPA safety and failure prevention are more prominent. The goal of the STPA is to identify gaps or failures in control actions and propose safety measures to prevent hazards.

The FRAM pursues a similar aim: To guide and make decision makers learn more about the system and think about it in a structured way. The STPA with a more technical background leaves less freedom and can be more compared with a technical control plan.

Table 2. Comparison of the main aspects of both methods

Aspect	FRAM	STPA
Focus	Functional interactions and variability	Control actions and hazard prevention
Approach	Systems approach emphasizing resonance, and emergent behaviours	Control system approach focusing on unsafe control actions and safety
Hazard Identification	Focus on how variability resonates across functions leading to failure	Focus on identifying unsafe control actions that lead to hazards
System Dynamics	Interdependencies and feedback loops between functions	Control loops and unsafe actions within those loops
Process Delays	Part of functional interactions, analysis of propagation	Impact on the performance in relation to safety constraints and control actions
Key Concept	Resilience and resonance	Failure prevention and safe decision-making
Level of Analysis	Function-level analysis of interactions	Control-level analysis of decision-makers and safety

Finally, the effectiveness of methodologies is heavily influenced by the quality and clarity of the provided guidelines. Well-defined and comprehensive guidelines facilitate better comparison and evaluation between different operators, leading to more consistent and reliable outcomes across various system contexts. Both methods offer extensive descriptions with the “FRAM Manual” and “STPA handbook” and are complemented by many scientific contributions.

However, both approaches are difficult to validate due to their conceptual nature and reliance on qualitative data. The challenge in validation arises because both methods are based on dynamic interactions and human factors that are hard to quantify or test in a controlled setting.

This makes it challenging to assess their accuracy or predict outcomes in real-world scenarios.

Another huge difference is in the aim of the methods, while the FRAM in its original form tends to be more an iterative tool with a high degree of freedom for socio-technical processes, the STPA fits them into a technical flow chart.

5. Conclusion

To have an unbiased comparison, one author applied the FRAM and the other applied the STPA to the infrastructure model given in Muneeperakul & Anderies (2017). Based on our research, it is neither sensible nor possible to say that one method is preferable to another. Both methods provide valuable insights into a system, leading to similar conclusions about the key issues within it. Afterwards it is to decide whether these issues need or can be prevented. If preventing the failure is not possible or economically viable, strategies for coping with the disturbance need to be found.

The primary difference between the two methods lies more in their overall aim. In cases where the operator wants to actively prevent disruptions STPA is the choice, because it focuses on identifying and mitigating potential hazards. In contrast, to gain a better understanding about how the system deals with disruptions FRAM seems to be more adequate. From this perspective a practical approach would be to first use the STPA to address any foreseeable hazards and apply the FRAM afterwards to see how to cope with the unavoidable.

After conducting this research, we view these two methods complementing each other although looking to be very similar at the beginning.

6. References:

De Linhares, T. Q., Maia, Y. L., & e Melo, P. F. F. (2021). The phased application of STAMP, FRAM and RAG as a strategy to improve complex sociotechnical system safety. Progress in Nuclear Energy, 131, 103571.

Ghasemi, F., Zarei, E., Salehi, V. (2024). Unraveling Complexity: FRAM Applications in Sociotechnical Systems Safety Analysis. In: Zarei, E. (eds) Safety Causation Analysis in Sociotechnical Systems: Advanced Models and Techniques. Studies in Systems, Decision and Control, vol 541. Springer doi: 10.1007/978-3-031-62470-4_10

Hollnagel, E. (2012). FRAM: the functional resonance analysis method: modelling complex socio-technical systems. Cognition, Technology & Work, 15(1), 117–118. doi:10.1007/s10111-012-0246-3

Leveson, N. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237–270. doi:10.1016/s0925-7535(03)00047-x

Leveson, N. G. (2016). Engineering a safer world. London, England: MIT Press.

McCormack, P., Read, G. J., Hulme, A., Lane, B. R., McLean, S., & Salmon, P. M. (2023). Using systems thinking-based risk assessment methods to assess hazardous manual tasks: a comparison of Net-HARMS, EAST-BL, FRAM and STPA. Ergonomics, 66(5), 609-626.

Muneepeerakul, R., and J. M. Anderies. 2017. Strategic behaviors and governance challenges in social-ecological systems. Earth’s Future 5 (8): 865–876. doi: 10.1002/2017EF000562.

Patriarca, R., Chatzimichailidou, M., Karanikas, N., & Di Gravio, G. (2022). The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. Safety science, 146, 105566. doi:10.1016/j.ssci.2021.105566

Qiao, W., Li, X., & Liu, Q. (2019). Systemic approaches to incident analysis in coal mines: Comparison of the STAMP, FRAM and “2–4” models. Resources Policy, 63, 101453.

Smith, D., Veitch, B., Khan, F. & Tylor, R (2016). Understanding industrial safety: Comparing Fault tree, Bayesian networks, and FRAM approaches. *Journal of Loss Prevention in the Process Industries 45*, 88–101.

Toda, Y., Matsubara, Y., & Takada, H. (2018). FRAM/STPA: Hazard analysis method for FRAM model. In Proceedings of the 2018 FRAM Workshop. Cardiff, Wales (pp. 1-17).

Yousefi, A., Rodriguez Hernandez, M., & Lopez Peña, V. (2019). Systemic accident analysis models: A comparison study between AcciMap, FRAM, and STAMP. Process Safety Progress, 38(2), e12002.