Comparative Safety Analysis of FHA, STPA, and FRAM: Insights from the TAM Flight 3054 Accident

Vitor Henrique Oliveira Bourguignon[1], Guilherme Conceição Rocha[2]
[1]Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil
[2] Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

***Abstract* – This paper evaluates three hazard analysis methods in the context of aircraft system safety: Functional Hazard Assessment (FHA), Systems-Theoretic Process Analysis (STPA), and the Functional Resonance Analysis Method (FRAM). The study applies these methods to the TAM Flight 3054 accident case, highlighting the capabilities and limitations of each approach. The analysis shows that while FHA meets regulatory requirements by identifying functional failure conditions, STPA expands the analysis by addressing human interactions and control logic issues. FRAM complements both by revealing how normal performance variability and organizational factors can combine to produce accidents. The findings indicate that no single method alone is sufficient to ensure safety in complex systems. A combined approach integrating these methodologies is recommended to provide a more robust and comprehensive safety assessment in aeronautical system design.**

***Keywords* – Aviation safety, hazard analysis, FHA, STPA, FRAM.**

I. INTRODUCTION

Commercial aviation safety relies on rigorous system safety assessment to identify and mitigate potential hazards early in design and throughout operation. Industry standards such as SAE ARP4761A [2] and regulatory guidance (e.g. FAA 14 CFR Part 25.1309 [3]) require systematic hazard analysis of aircraft functions and systems to demonstrate that catastrophic failures are "extremely improbable" (on the order of 10^{-9} per flight hour for transport category) [1]. Traditional safety processes under ARP4761A [2] include methods like Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA), and Failure Mode and Effects Analysis (FMEA) to comply with these stringent safety targets. FHA, in particular, is performed at the aircraft and system level to identify failure conditions and assign hazard severities that drive design requirements [2].

However, the increasing complexity of modern aircraft – with highly integrated avionics, software-intensive controls, and tightly coupled human–automation interactions – has exposed limitations in traditional hazard analysis. Accidents can arise not just from component failures, but also from unsafe interactions or human performance issues in the absence of any single failure. This recognition has motivated newer methodologies such as Systems Theoretic Process Analysis (STPA) and the Functional Resonance Analysis Method (FRAM.

BOURGUIGNON, V.H.O, bourguignon@ita.br; ROCHA, G.C., grocha@ita.br.

In this paper, we compare three hazard analysis approaches in the context of aircraft system safety: Functional Hazard Assessment (FHA), Systems Theoretic Process Analysis (STPA), and Functional Resonance Analysis Method (FRAM). We begin with an overview of each methodology's origins, theoretical basis, and typical use in commercial aviation. We then hypothesize that none of the three methods alone is sufficient or infallible for assuring safety in a complex aircraft environment, given that each has strengths and latent gaps. To explore this hypothesis, we apply FHA, STPA, and FRAM retrospectively to a real-world accident – TAM Airlines Flight 3054 (Airbus A320-233) in 2007 – analyzing how each method would account for the causes and contributing factors. The case study allows us to see which insights each method reveals or misses. We then discuss whether the findings support the idea that a combination of methods is needed to address the full spectrum of hazards in modern aviation.

II. OVERVIEW OF HAZARD IDENTIFICATION METHODS

A. Functional Hazard Assessment (FHA)

Origins and Context: FHA serves as a key pillar in the traditional safety assessment process defined in SAE ARP4761 (first issued 1996, updated as ARP4761A in 2023 [2]). ARP4761's FHA is used to demonstrate compliance with airworthiness requirements like 14 CFR 25.1309 [3] for transport-category aircraft. In practice, FHA is typically conducted early in aircraft design to identify hazards associated with functional failures.

Theoretical Basis: FHA takes a top-down, functional view of the system. It begins by enumerating the aircraft's high-level functions (e.g. maintain controlled flight, provide pressurization, decelerate on landing, etc.) and then postulates credible failure conditions for each function. For each functional failure condition, the FHA evaluates the effects on the aircraft, crew, and occupants, assuming the failure occurs in isolation [1]. The key question is: "What would happen if this function were lost or degraded?" [1]. The FHA then qualitatively assigns a hazard severity classification based on the worst-case outcome of that failure condition (typically Catastrophic, Hazardous, Major, Minor, or No Safety Effect., as defined in AC 25.1309-1B [3]). For example, loss of a critical flight control function might be classified as Catastrophic if it could lead to loss of the aircraft, whereas a lower-severity failure might be Major or Minor if controllable [1]. These hazard classes are tied to safety objectives (Catastrophic conditions must be "extremely improbable", ~10^{-9} per flight hour) [3]. The FHA

thus establishes high-level safety requirements; for instance, if a hazard is Catastrophic, the design must include mitigating provisions or redundancies to reduce its probability below the required threshold.

Application in Aviation Safety: FHA is widely used by aircraft manufacturers and certification authorities as the first step in safety analysis. It provides a functional safety baseline that informs subsequent analyses like Preliminary System Safety Assessment (PSSA) and System Safety Assessment (SSA) [2]. FHA's strength lies in its systematic and comprehensive coverage of functional failures. The method's focus on "what if X function fails?" aligns well with the failure-driven accident models traditionally used in aviation safety. FHA is also supported by decades of industry experience and is documented in certification artifacts, making it a trusted technique for regulators and engineers alike.

Limitations: Because FHA defines hazards in terms of functional loss or malfunction, it inherently concentrates on component failures and their direct consequences. It may not naturally capture hazards arising from unexpected interactions between nominally functioning components or from human error and organizational factors. FHA assumes a relatively linear cause-effect chain (a function fails → leads to outcome) and can miss scenarios where no single function fails outright, but rather a combination of partial actions, latent conditions, or human mistakes produce a hazard. Indeed, regulators have recognized that conventional safety assessments (anchored by FHA/FTA/FMEA) have gaps related to human factors and complex interactions, noting that losses can occur "with zero failures" in the system [4].

B. Systems-Theoretic Process Analysis (STPA)

Origins and Context: STPA was developed in the 2000s by Nancy Leveson and colleagues at MIT as part of the STAMP (System-Theoretic Accident Model and Processes) framework for safety. Leveson's insight, published in Engineering a Safer World (2012), was that traditional hazard analysis (like FHA/FMEA) was rooted in a reliability-centric accident model (accidents caused by component failures), which struggles to handle software complexity and human/operator error. STAMP proposes an alternative accident model based on systems theory and control: accidents are seen as the result of inadequate enforcement of safety constraints in a complex control structure, rather than just chains of failures. STPA is the hazard analysis method emerging from this model.

Theoretical Basis: STPA is grounded in a control-theoretic view of safety. STPA models the system as a set of control loops involving controllers (which can be human or automated), actuators, sensors, and the controlled process. The methodology seeks to identify instances of unsafe control actions (UCAs) that could lead the system into a hazardous state [5]. An unsafe control action might be, for example, a controller not providing a necessary command, providing an incorrect command, providing a correct command at the wrong time, or stopping a command too soon/too late [6]. STPA consists of two main steps: (1) Identify Hazards and Safety Constraints – define the losses and hazards of concern and derive high-level safety constraints. (2) Identify Unsafe Control Actions and Causal Scenarios – examine each control loop in the system to find how a control action could be unsafe with respect to the hazard (the UCA), then brainstorm possible causes for each UCA.

Application in Aviation Safety: In a commercial aviation context, STPA can be applied during design to derive safety requirements for complex functions (especially those involving automation). For example, STPA has been used to analyze aircraft collision avoidance systems, autopilot modes, and even organizational safety management processes [4]. A benefit noted in the literature is STPA's ability to explicitly include software and human operator behavior in the hazard analysis. STPA generates causal scenarios that often resemble what-if narratives: e.g., "If the auto-brake system does not command braking when required due to a software logic flaw, then hazard X could occur". These scenarios help in identifying design weaknesses or missing requirements.

Limitations: Although robust, one challenge is that STPA can yield a large number of scenarios and constraints, which may be difficult to prioritize without some notion of probability or risk – STPA by design does not directly incorporate probability, focusing on qualitatively plausible scenarios. There is also a level of subjectivity and required expertise: modeling the control structure diagram and identifying UCAs relies on the analyst's understanding of the system. Additionally, STPA is relatively new to the conservative aviation certification culture. Finally, STPA tends to identify single-point hazards (one control action at a time); it may not explicitly reveal hazards that only arise from combinations of several small deviations.

C. Functional Resonance Analysis Method (FRAM)

Origins and Context: FRAM was introduced by Erik Hollnagel in 2004 (and elaborated in his 2012 book) as part of the Safety-II or resilience engineering paradigm. Unlike traditional "Safety-I" approaches that focus on what goes wrong (failures and errors), Safety-II emphasizes understanding normal performance variability and how it can lead to both successful and unsuccessful outcomes. FRAM was initially proposed as an accident investigation and systems modeling tool to capture how complex socio-technical systems actually function in real life, recognizing that linear cause-effect chains often do not explain accidents in these systems [7]. Over the past two decades, FRAM has been applied in domains as varied as aviation, air traffic management, healthcare, nuclear power, and railways.

Theoretical Basis: FRAM represents a fundamentally different view of causation. It posits that in complex systems, success and failure stem from the same normal variability in performance [7]. People and systems always adjust their performance to meet current conditions (due to time pressure, resource limitations, etc.), and usually these adjustments lead to success, but occasionally they combine in unexpected ways to produce a bad outcome – an accident. This nonlinear interaction is metaphorically called resonance (hence

"Functional Resonance") [7]. FRAM models a system as a network of functions (human or technical activities/ processes) rather than components. Each function is described by six aspects: Inputs, Outputs, Preconditions, Resources, Time (temporal constraints), and Control (monitoring/oversight) [7]. Functions are linked not by simple chains, but through these aspects – for example, the Output of one function might be a Resource or Precondition for another. Once the analyst identifies essential functions and their couplings, the FRAM approach is to examine how variability in each function's performance could affect the others. Variability can come from human variability (differences in how an operator performs a task), technical variability (fluctuations in system performance), or external conditions. If multiple functions' variabilities happen to align (or resonate), the system can move towards a hazardous outcome even if no function failed per se [7].

Application in Aviation Safety: FRAM has been applied mostly in retrospective investigations or in safety management. For instance, Woltjer and Hollnagel's FRAM analysis of the Alaska 261 accident revealed how maintenance practices, sensor degradation, and pilot actions resonated to cause the loss of control [8]. FRAM encourages a holistic examination of the socio-technical system: it considers technical systems, human operators (pilots, controllers), organizational policies, and environmental conditions all as interacting functions.

Limitations: As a method originally devised for analysis rather than design, FRAM faces some limitations when used for hazard identification. One challenge is practicality and scope – constructing a full FRAM model of a complex aviation operation can be time-consuming and requires extensive expertise and data about how work is actually done. FRAM does not inherently prioritize which combinations of variability are more probable or more hazardous; it produces a web of potential interactions that an analyst must subjectively evaluate. Another limitation is that FRAM, by focusing on emergent outcomes from normal performance, might underplay the role of specific component failures or technical malfunctions. FRAM offers a comprehensive perspective but may lack the precision necessary to establish specific design requirements or probabilistic assessments.

III. Hypothesis

No single hazard analysis method – whether FHA, STPA, or FRAM – is by itself complete or infallible for assuring comprehensive aviation system safety. We hypothesize that each method has inherent strengths and weaknesses, and each illuminates different aspects of risk; therefore, relying on any one alone could leave important hazard facets unaddressed. Support for this hypothesis comes from observations in industry and academia. Despite decades of using FHA/FTA, accidents still occur due to factors not effectively captured by those analyses (e.g. pilot actions under stress, confusing automation behavior, maintenance lapses). Conversely, while STPA and FRAM promise to capture those factors, they are relatively new and can be difficult to integrate into the rigorous certification process that demands quantitative evidence and proven techniques.

To evaluate this hypothesis, we now turn to a case study: the TAM Airlines Flight 3054 accident. By applying FHA, STPA, and FRAM lenses to this event, we can concretely see what each method highlights or misses. If indeed each method finds unique insights and has latent gaps that the others cover, it will support the argument that a combined approach is advisable for comprehensive safety assurance. It is important to recognize that the FHA/STPA/FRAM case study presented here was conducted after the accident. It is therefore subject to the unavoidable hindsight bias that comes from being aware of the causal factors that led to the accident. However, the case study still provides valuable insight into the kinds of hazards emphasized by the FHA/STPA/FRAM framework.

The present study does not aim to re-investigate the accident, which has already been thoroughly analyzed by the Brazilian Aeronautical Accident Investigation and Prevention Center (CENIPA). Instead, the goal is to assess whether any hazard analysis method could have, during the design phase of the A320 aircraft, provided a sufficiently robust safety analysis to prevent the accident from occurring in 2007.

IV. Case Study: TAM Flight 3054 Accident Analysis

A. Accident Background

Overview of TAM 3054: On July 17, 2007, TAM Airlines Flight 3054, an Airbus A320-233 (registration PR-MBK), crashed during landing at São Paulo's Congonhas Airport. The aircraft, inbound from Porto Alegre, failed to decelerate on the wet runway 35L, overran the runway at high speed, crossed a busy road, and collided with a fuel station and an airport building, exploding on impact [9]. All 187 passengers and crew on board were killed, along with 12 people on the ground [9]. The accident occurred in rainy conditions during evening darkness. Critically, the A320's #2 (right) engine thrust reverser was deactivated in accordance with the Minimum Equipment List (MEL), under an approved maintenance deferral for this flight [9], meaning that upon landing only the left engine had reverse thrust available.

Cause Summary: The Brazilian investigation (CENIPA) concluded that one of the causes of the accident was the pilots' configuration of the throttles – specifically, the captain left the right engine throttle in the CL (Climb) detent (providing go-around power) instead of retarding it to idle, while the left engine was retarded to idle and its reverser deployed [9]. In essence, one engine was commanding forward thrust at touchdown, whereas the other was trying to reverse – a scenario that led to asymmetric thrust and an inability to slow down [9]. The aircraft's systems, detecting that one throttle was not at idle, did not automatically deploy the ground spoilers or autobrakes, because the logic is designed to prevent spoiler deployment if a throttle is advanced. Thus, the A320 landed with no spoilers (which significantly reduced wheel braking effectiveness) and only manual braking on a contaminated runway, while one engine continued to push the aircraft forward. The crew applied maximum manual brakes, but with one engine effectively

accelerating the plane and the contaminated runway, deceleration was minimal. The aircraft experienced a leftward runway excursion at approximately 90–100 knots [9], leading to the fatal crash.

Multiple contributing factors were identified in addition to the thrust lever misconfiguration. Investigators observed that São Paulo/Congonhas Airport featured a relatively short runway with no Runway End Safety Area (RESA) and, at the time of the occurrence, lacked surface grooving. The runway was known to exhibit reduced surface friction under wet conditions [9].

Operational pressures were also cited as contributing elements. The operator's dispatch decision was subject to post-accident scrutiny: although authorizing a fully loaded Airbus A320 to operate into Congonhas with one thrust reverser deactivated in accordance with the MEL was technically compliant with regulatory standards, it provided minimal operational safety margin under degraded runway conditions.

Flight crew training and human performance considerations were also emphasized. The decision-making process of the experienced captain was central to the investigation.

In summary, the accident involving TAM Flight 3054 exemplified a sociotechnical system failure, resulting from the convergence of design characteristics (thrust lever and spoiler deployment logic), human factors (thrust lever mispositioning), environmental conditions (wet, ungrooved runway), and organizational influences (operational policies and infrastructure constraints).

We will now analyze this accident using each of the three hazard analysis methods:

- **FHA perspective:** What hazards should have been identified in design, and how were they addressed or not?
- **STPA perspective:** What unsafe control actions and system interactions led to the accident?
- **FRAM perspective:** How did normal performance variability resonate to create the conditions of this accident?

B. FHA Analysis of Flight 3054

In the context of a FHA, the relevant aircraft functions are systematically analyzed alongside their associated failure conditions. For the case study, a top-level aircraft function of operational interest is the capability to decelerate and stop safely within the available runway length following touchdown. A credible failure condition associated with this function would be defined as: "Aircraft fails to decelerate as intended upon landing, resulting in a runway excursion." An FHA conducted during the type certification phase of the A320 program would be expected to identify this failure condition and assign a severity classification based on its potential consequences. In the case of TAM 3054, the operational outcome included aircraft hull loss and multiple fatalities, consistent with a Catastrophic severity classification as defined in SAE ARP4761 and FAA AC 25.1309-1B.

For the hazard discussed, engineers would consider possible causes. Some causes are purely mechanical: e.g. total brake failure, jammed spoilers, or loss of hydraulic power. However, in this accident, the root cause was not a component failure but a configuration or operational issue (thrust lever position). Would a traditional FHA catch this scenario? Partially. The FHA would certainly include a scenario like "Ground spoilers fail to deploy upon landing" as a potential failure condition, since spoiler non-deployment can significantly increase landing distance. Spoiler or autobrake failure might be categorized as a Hazardous or Major condition (short of catastrophic, assuming crew could still stop the plane with manual braking on a dry runway). In the TAM 3054 case, spoiler non-deployment occurred because one throttle was not at idle. If the FHA was thorough, it should consider "spoilers fail to deploy when required" and note that on a wet or short runway, this could indeed become catastrophic (if braking alone cannot stop the aircraft). The design mitigation for spoiler failure on Airbus is that pilots are trained to monitor spoiler deployment (there's an ECAM indication) and to manually deploy spoilers if they don't auto-deploy, as well as apply maximum braking. The FHA would rely on such procedural mitigation, and possibly on performance calculations that assume reversers are not available.

What FHA does not deeply examine is the human procedural aspect. The FHA process alone would not have guaranteed deeper scrutiny into this scenario. Thus, FHA identified the hazard in general, but did not fully address the sociotechnical factors that allowed it to occur. All the physical systems (brakes, spoilers, engines) were functional, but the system state (one engine at climb power) was equivalent to multiple failures (no spoiler, asymmetric thrust).

C. STPA Analysis of Flight 3054

Using STPA, we examine the accident as a control problem with unsafe control actions. Therefore, we identify the relevant control structure for landing deceleration. A closer analysis of specific control loops is presented below to illustrate their role in system behavior and safety implications:

Pilot–Engine Thrust Control Loop: The Pilot is the controller, the engines (thrust level) are the controlled process. An UCA in this loop was: Pilot does not reduce Engine #2 thrust on landing. We then ask: why did this UCA occur? Possible causes include: (a) the pilot's mental model or procedure may have been flawed. (b) Pilot might have intended to go around and changed mind too late. STPA would flag the need for clear procedures and feedback: Was there a cockpit indication that throttle lever #2 remained above idle? In STPA terms, a feedback flaw could be: "Lack of immediate feedback to pilot that one throttle is not at idle (e.g., no warning or discrete alert for high thrust on ground)." Therefore, STPA might suggest a new requirement: provide a warning if thrust remains above idle after touchdown.

Automatic Ground Spoiler Control Loop: Here the controller is the Flight Spoiler Logic in the aircraft systems,

and the controlled process is spoiler surface deployment. The logic uses inputs like weight-on-wheels sensors and throttle positions. In the accident, the spoiler system did not deploy spoilers because one throttle was not at idle. From STPA perspective, an UCA occurred in this loop as well: Spoilers were not deployed when needed, leading to hazard. Why did it occur? By design – it was a logical consequence of the throttle position. STPA would treat the design decision (inhibit spoilers if throttle > idle) as a potential unsafe logic under certain contexts (i.e., if that throttle position was erroneous). Therefore, STPA highlights that design choice is part of the causal chain.

Airline Operational Control Loop (Organizational): STPA can also be applied to higher-level organizational structures. In this case, the relevant control action was the airline's decision to authorize the dispatch of the flight under MEL conditions with one thrust reverser deactivated. A potential Unsafe Control Action (UCA) is: Dispatch authorizes the flight despite contextual factors such as wet, short runway and high payload, which reduce system resilience if deviations occur during landing. Possible causal factors include organizational pressure to maintain schedules, reliance solely on regulatory MEL compliance without additional internal safety buffers, and overreliance on pilot expertise to manage adverse scenarios. STPA would then suggest organizational-level safety constraints, such as adopting more conservative dispatch policies for operations into critical airports, reinforcing crew training, and improving communication of operational risks

In sum, the STPA analysis of TAM 3054 reveals multiple UCAs and causal scenarios: the pilot's failure to idle the throttle, the spoiler system's inhibited action, and the company's decision to operate in those conditions were all "control failures" contributing to the hazard. Where STPA is perhaps limited is in capturing the simultaneity of issues: STPA looks at each unsafe action in isolation. It would not necessarily highlight that all these factors aligning was the real problem.

D. FRAM Analysis of Flight 3054

Using FRAM, we analyze TAM 3054 by modeling the functions involved in the landing phase and examining how performance variability across these functions interacted to contribute to the accident. While a large number of functions could be represented within the FRAM model, the scope of this paper requires focusing on the most significant ones. Accordingly, six core functions - encompassing both human and technical activities - were selected for detailed analysis. These include:

F1: Execute Landing Flare and Touchdown – performed by the pilots (flying and monitoring). Its output: aircraft on ground at correct touchdown point and speed. Preconditions: correct approach speed, configuration, etc. (In this accident, F1 was nominal – the touchdown was on the runway. We will not focus on the approach since the primary issues occurred after touchdown.)

F2: Retard Thrust Levers to Idle – performed by the pilot(s) at touchdown. Input: callouts/height (20ft "RETARD" auto-call), knowledge of reverser MEL procedure. Output: both thrust levers at idle (or idle + reverse on #1). This function failed partially – left engine was retarded (with reverse selected), right engine lever was not. We can consider that a variability in performance of F2: normally both would be idle; here only one was. The variability could be due to human factors (stress, miscommunication between pilots, or a memory slip by the captain).

F3: Deploy Ground Spoilers – performed by the aircraft automation once weight-on-wheels is detected and throttles at idle. In the accident, the input condition "throttles at idle" was not met, so spoilers did not deploy. This is a variability of function F3 – normally they would, but here they stayed retracted.

F4: Apply Wheel Brakes – could be partly automated and partly manual. In our scenario, because spoilers didn't deploy, the autobrake might not have activated. The pilots did apply manual brakes fully. Its variability: without spoilers, wheel braking is less effective (less weight on wheels initially, potential for hydroplaning). Therefore, F4's performance was degraded by external condition and lack of spoiler assist.

F5: Crew Monitor and Cross-Check – the first officer (monitoring pilot) typically would monitor that spoilers deploy, call out "Spoilers!" or "No spoilers", monitor engine indications, etc. This function's output is detection of deviations and prompting corrections. In the accident, there's no indication from the CVR that the crew noticed the spoilers hadn't deployed or that engine #2 was still at climb power until it was far too late. This monitoring function did not catch the throttle mis-set quickly. Variability: sometimes crews catch errors, sometimes (under stress) they miss them.

F6: Airline Operational Planning – deciding aircraft dispatch and approach strategy. Input: MEL items, weather info. Output: a "go/no-go" or operational plan. As discussed, this function at TAM allowed a risky situation: dispatch did not restrict the landing despite the combination of factors. Variability: on another day, maybe a diversion or delaying until weather improved could have been chosen; that day, they proceeded, possibly due to external pressure.

In FRAM's perspective, all these functions usually succeed: Pilots almost always retard throttles correctly; spoilers usually deploy; crews monitor effectively; airlines avoid compounding operational risks. The FRAM model shows how the accident was the emergent outcome of several "normally acceptable" deviations happening together. The FRAM analysis underscores the lack of resilience in the system.

On the other hand, FRAM offers limited guidance regarding the implementation of specific mitigation measures – it does not provide prescriptive guidance such as "add this design element" or "revise this section of code".

V. RESULTS AND DISCUSSION

Analyzing the TAM 3054 accident with all three methods, we can now directly compare what each method revealed and what each missed, relating back to our hypothesis:

Table I. FHA, STPA, AND FRAM APPLIED TO TAM FLIGHT 3054

Aspect	***FHA***	***STPA***	***FRAM***
Analytical Focus	Functional failure conditions and severity classification	Unsafe control actions in a control structure	Variability of normal performance
Methodological Strength	Structured and aligned with regulatory compliance	Captures human, software, and systemic control failures	Reveals emergent accidents due to everyday performance adjustments
Key Insight	Validated that design had accounted for loss of deceleration	Identified specific points where safety constraints were breached, including missing cockpit feedback	Showed how 'normal' actions, under degraded conditions, combined to create an unsafe situation
Strengths	Widely accepted in certification, clear safety targets, systematic and repeatable	Strong in identifying causality in complex interactions, human-in-the-loop, and latent design flaws	Holistic view incorporating organizational, environmental, and human variabilities
Weaknesses	Limited scope for human error and control interactions; assumes isolated failures	Generates many plausible scenarios without quantification; may overproduce false positives	No direct link to system requirements or mitigation strategies; high modeling effort required
Gaps in the Case Study	Did not foresee the combined effects of procedural deviation and logic constraints	Did not fully capture the cumulative risk from multiple simultaneous deviations	Did not emphasize specific technical failures or assign criticality to identified variabilities

Evaluating the Hypothesis: The case study supports our hypothesis that each method sees the accident through a different perspective. FHA gave the regulatory/design perspective. STPA gave a process perspective. FRAM gave a systemic perspective. Notably, no contradictions arose between the methods; rather, they interlock: each method's findings enrich the others. Together, they form a more comprehensive understanding.

Given the complementary findings, we argue that an integrated approach to hazard analysis is beneficial. It is plausible to consider a safety assessment process where FHA establishes the baseline and compliance with quantitative requirements, STPA is applied to identify additional unsafe scenarios (especially involving humans, software, and interactions), and FRAM is used to evaluate operational contexts and organizational factors that might bypass those safety measures. This combined approach addresses the "gaps" that were noted in the current practice [4]. Accidents like TAM 3054 serve as compelling evidence that more holistic hazard analysis is necessary.

VI. CONCLUSION

In conclusion of the discussion, the TAM case reinforces the idea that safety is an emergent property requiring multiple analytical perspectives. The hypothesis that none of these methods is infallible on its own holds true. Therefore, a multi-method safety assessment strategy is recommended. In practice, this means using FHA, STPA, and FRAM in a complementary manner. The results of this paper's case study strongly indicate that such a combined approach would have better anticipated and mitigated the TAM 3054 accident scenario. Future work in this area includes developing integrated frameworks and guidelines for combining these methods, so that the outcome is a coherent safety case rather than disparate analyses.

REFERENCES

National Transportation Safety Board (NTSB), "System Safety and Certification Specialist's Report: NTSB ID No.: DCA19RA017," Office of Aviation Safety, Washington, D.C., USA, Aug. 21, 2019.

SAE International Recommended Practice, Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment, SAE Standard ARP4761A, Revised December 2023, Issued December 1996, https://doi.org/10.4271/ARP4761A.

Federal Aviation Administration, "System Design and Analysis," Advisory Circular AC 25.1309-1B, Washington, D.C., USA, Aug. 30, 2024. [Online]. Available:https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1B.pdf.

J. P. Thomas and J. G. Van Houdt, "Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety," Federal Aviation Administration, Atlantic City, NJ, USA, Tech. Rep. DOT/FAA/TC-24/16, Jul. 2024.

D. Slater, "STPA – A Stairway to FRAM: Enhancing Complex System Modeling," LinkedIn, Oct. 15, 2024. [Online]. Available: https://www.linkedin.com/pulse/stpa-stairway-fram-enhancing-complex-system-modeling-david-slater-atyoe/.

SUN, Liangliang; LI, Yan-Fu; ZIO, Enrico. Comparison of the HAZOP, FMEA, FRAM, and STPA methods for the hazard analysis of automatic emergency brake systems. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, v. 8, n. 3, p. 031104, 2022.

M. Tishehzan, "FRAM in a Nutshell," *PAN-European Training, Research and Education Network on Electromagnetic Risk Management (PETER)*, Feb. 11, 2021. [Online]. Available: https://etn-peter.eu/2021/02/11/fram-in-a-nutshell/.

WOLTJER, Rogier; HOLLNAGEL, Erik. The Alaska Airlines flight 261 accident: a systemic analysis of functional resonance. In: 2007 International Symposium on Aviation Psychology. 2007. p. 763.

Centro de Investigação e Prevenção de Acidentes Aeronáuticos (CENIPA), *Relatório Final: Ocorrência com a aeronave PR-MBK, modelo Airbus A-320, em 17 de julho de 2007*, RF A-67/CENIPA/2009, Comando da Aeronáutica, Brasília, DF, Brasil, 2009.