10/10/2024

FRAMSYNT

Understanding the Challenger Disaster - A Systemic Approach

a FRAM- STPA approach | David Slater and James Pomeroy

UNDERSTANDING THE CHALLENGER DISASTER
A SYSTEMIC APPROACH

David Slater, Cardiff University, dslater@cambrensis.org

James Pomeroy, Cranfield Safety and Accident Investigation Centre, steadypom@gmail.com

ABSTRACT

The Challenger disaster remains a critical study in the consequences of organizational "culture" on safety, with previous analyses often focusing on singular causes like "normalization of deviance." This paper seeks to provide a more nuanced understanding through a dual application of two systemic analysis methods: System-Theoretic Process Analysis (STPA) and Functional Resonance Analysis Method (FRAM). The analysis re-examines the Challenger disaster by mapping the hierarchical structure of NASA and its contractors, highlighting decision-making processes at macro, meso, and micro levels. STPA reveals specific Unsafe Control Actions (UCAs) and control loop deficiencies, exposing gaps in NASA's risk management and communication. Simultaneously, FRAM models trace critical functional variability within NASA's organizational levels, The combined approach uncovers how political and budgetary constraints, normalized risk-taking, and diluted engineering feedback cumulatively degraded decision-making integrity, ultimately contributing to the Challenger's tragic launch decision. Lessons drawn emphasize the need for resilient structures, adaptable feedback mechanisms, and a culture that values caution alongside achievement. This analysis underscores the potential of integrating STPA and FRAM in complex systems to facilitate successful operations, to enhance safety and anticipate organizational issues.

Key Words- Accidents, Organisations, Systemic analysis, STPA, FRAM

INTRODUCTION

Pomeroy (1) notes that studying safety and risk often means examining disasters through the lens of theories, which can narrow our understanding of their complexity. In this view, well-known catastrophes are often paired with catchy, simplified explanations. For example, Chernobyl's disaster is frequently attributed to a lack of "safety culture,"(1), Aberfan is described as a "man-made disaster" caused by a "failure of foresight,"(2), and the Challenger explosion is linked to an organization that became "normalized to deviance." (3)

He adds that although such theories provide useful frameworks, they risk oversimplifying disasters into neat abstractions that fail to capture the full context, conditions, and personalities involved. This narrowed focus can limit our perspective, framing our understanding of events through others' interpretations and potentially stifling deeper insights.

This paper takes up that challenge and aims to apply a more detailed analysis of the system to try to understand where these risky behaviours originate in the system. To do this we intend to utilise, two methods which stand out for their distinct approaches to understanding socio-technical systems: Leveson's System-Theoretic Process Analysis (STPA)(4) and Hollnagel's

Functional Resonance Analysis Method (FRAM)(5). Following the above led this paper to attempt to re- examine the much-studied Challenger Disaster.

THE INCIDENT

The Challenger disaster(6) remains a powerful moment in history. On January 28, 1986, just seventy-three seconds after launch, the space shuttle Challenger tragically exploded, killing all seven crew members.

Higginbotham in his book (7) looking back to NASA's early years, focusses on its first major tragedy in 1967, when a fire in the Apollo capsule during a test which sadly killed three astronauts. This event was not the result of an in-space failure but rather a fire on the ground, exacerbated by poor construction and safety standards. Despite exposing significant failings, the tragedy did not halt the Apollo program, as political pressures to reach the Moon remained intense. Indeed, probabilistic risk assessments done by NASA often predicted slim chances of mission success; but being "of the right stuff", they launched anyway. The book concludes :

"Signals lost in the noise of a complacent can-do culture bred by repeatedly achieving the apparently impossible. Seduced by their own mythos, and blind to the subtleties of engineering complexity that none of them fully understood, the nation's smartest minds had unwittingly sent seven men and women to their deaths."

Higginbotham's narrative illustrates how these earlier incidents and systemic pressures set the stage for the events that would lead to the Challenger explosion. The Challenger disaster exemplifies the dangers of systemic failure in complex organizations, particularly within the US Government-funded programs where structural, procedural, and communicative breakdowns intersected across NASA's operational hierarchy.

This approach underscores the importance of taking a broader view when examining disasters, as understanding the larger context can often reveal patterns and underlying factors that contribute to seemingly isolated events.

Structural Overview of Decision-Making Functions at NASA

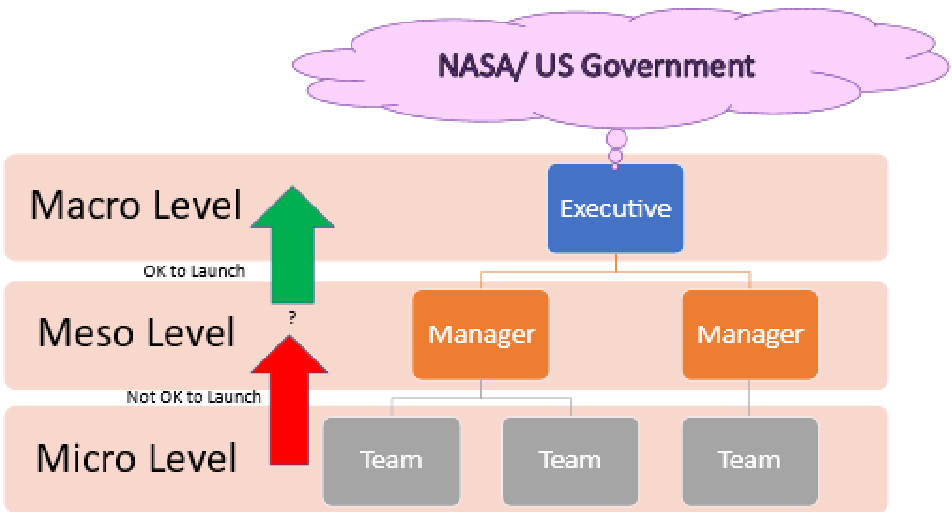

Fig. 1 - A simple illustration of the conventional view of NASA's organisational structure

At NASA, the organizational structure operated across three primary levels, each of which played a role in the Challenger decision-making processes: the macro level, represented by government oversight and NASA's upper management; the meso level, encompassing NASA's program management; and the micro level, consisting of the engineering teams. Each level carried distinct responsibilities, and their interactions were governed by control systems that were critical to managing operational safety.

Macro Level (Government Oversight and NASA Headquarters)

At the macro level, NASA's upper management faced intense pressure from Congress and federal stakeholders to maintain a regular shuttle launch schedule. The space shuttle program was not only a scientific initiative but a symbol of national pride. For this reason, NASA's leaders were tasked with justifying the program's substantial financial investments, often by demonstrating its feasibility through frequent, flawless missions. The macro-level expectation for productivity and minimal delays significantly influenced final decisions, where the need to demonstrate operational success often overshadowed safety concerns raised by technical teams. The influence of funding concerns and political agendas at this level became a decisive factor that impacted the meso and micro levels.

Meso Level (NASA Program Management)

Program management, responsible for coordinating with contractors like Morton Thiokol (who manufactured the solid rocket boosters), functioned at the meso level. This layer interpreted NASA's overarching goals and translated them into specific objectives for technical teams, often prioritizing organizational goals over safety. The meso level, while significant in determining launch readiness, often encountered conflicts between technical concerns and the pressing goals driven by upper management.

Micro Level (Engineering Teams and Technical Staff)

The engineers and technical staff, who directly understood the technical risks operated at the micro level. The lack of authority at the micro level limited the engineers' ability to influence the final decision. As pressures cascaded down from macro and meso levels, operational priorities outweighed technical caution, effectively sidelining the engineers' expertise.

Decision-Making Flow and Communication Challenges

This conventional hierarchical structure at NASA created multiple layers of management and decision-making bodies. Although the structure theoretically allowed for information flow from technical staff to top managers, it was often filtered or modified at each level to align with programmatic goals. This structure contributed to communication issues, engineering feedback, originating from the technical teams and Morton Thiokol, was diluted as it moved up the management chain. Program managers at various levels, under pressure to maintain schedules, often downplayed these technical concerns, contributing to a culture that underestimated the severity of risks.

Influence of Political and Budgetary Pressures

NASA's management structure and decision-making were heavily influenced by political and budgetary pressures from Congress and the White House. The agency was expected to deliver results that justified its substantial federal funding, and the shuttle program was marketed as a reliable and routine means of space travel. This overarching goal created an environment in which management prioritized operational timelines over technical caution. Political oversight thus directly shaped management priorities and placed significant pressure on NASA's middle managers to keep the shuttle launch schedule on track, regardless of emerging technical concerns.

METHODOLOGY

In the landscape of complex system modeling, two methods stand out for their distinct approaches to understanding socio-technical systems: Leveson's System-Theoretic Process Analysis (STPA) and Hollnagel's Functional Resonance Analysis Method (FRAM). Both have proven invaluable in tackling the challenges of modern systems, where interactions between technology, humans, and organizations create a complex web of interdependencies and emergent behaviors. Each method brings its own strengths—STPA with its focus on control loops and inadequate control actions, and FRAM with its attention to the variability and resonance of everyday functions. This work proposes a novel way to combine these methods, using STPA as a foundation to map out control loops and functions, and then leveraging FRAM to explore the deeper interactions and variability within those control structures.

STPA: MAPPING CONTROL LOOPS AND UNSAFE ACTIONS

STPA offers a structured way to analyze complex systems by focusing on control loops and the interactions between controllers (human or automated) and controlled processes. In contrast to traditional hazard analysis methods, which tend to isolate failures within individual components, STPA views safety as a dynamic control problem. Accidents are often the result of inadequate control actions or flawed feedback mechanisms within a system's control loops not simply isolated failures. By mapping out these loops, STPA allows analysts to identify points where control actions may fail or lead to unsafe outcomes.

The strength of STPA lies in its ability to systematically model these control loops and assess the risks associated with inadequate control actions. It provides a structured framework to capture the dynamic interactions between various system elements, highlighting where and how control may break down. This analysis is particularly useful in complex environments, such as aerospace, healthcare, and autonomous systems, where safety depends on both technical systems and human decision-making.

FRAM: UNDERSTANDING FUNCTION VARIABILITY AND EMERGENT RISKS

FRAM, on the other hand, takes a different approach by emphasizing the role of variability in everyday system functions. Rather than focusing on failures or isolated incidents, FRAM models a system as a set of interconnected functions, each of which has inherent variability. This variability can propagate through the system, potentially amplifying into unexpected and undesirable outcomes through what Hollnagel describes as resonance. FRAM's core premise is that complex systems are rarely static, and it is the interactions between normal functional variations that often lead to emergent behaviors and risks.

In recent years, FRAM has gained traction as a quantitative complex system modeling methodology, with studies by Slater and Hill (10), demonstrating that FRAM can be fully quantitative when integrated with metadata. This shift allows analysts to more precisely evaluate how variability within functions leads to resonant effects across the system. FRAM's focus on emergent risks makes it particularly valuable for analyzing socio-technical systems where human variability and environmental factors play critical roles.

COMBINING STPA AND FRAM: A COMPREHENSIVE APPROACH

By combining STPA and FRAM, we can achieve a more comprehensive and dynamic approach to modelling complex systems. STPA provides the structural backbone by identifying the control loops and potential failures in control actions. Once these loops are mapped, FRAM can be applied to examine how variability within these loops, and the interactions between them, might lead to emergent risks. The integration works by first using STPA to map out the controllers, controlled processes, feedback mechanisms, and information flows. This provides a clear picture of the system's structure and relationships between its various elements. STPA's identification of unsafe control actions serves as acritical input for the next stage, where FRAM can then be used to model how these control actions interact with other system functions.

FRAM's focus on variability is particularly valuable here, as it allows analysts to explore how changes or deviations within one control loop might propagate through the system. The six aspects of FRAM functions—input, output, preconditions, resources, time, and control—align well with the control aspects identified in STPA, providing a seamless way to transition from structural analysis to functional variability assessment. This combination offers a more holistic view of system behavior, capturing both the structural risks identified by STPA and the dynamic, emergent risks highlighted by FRAM.

MODELING THE DISASTER WITH FRAM: DEFINING FUNCTIONS AND VARIABILITY

Through the lenses of the Functional Resonance Analysis Method (FRAM) and System Theoretic Process Analysis (STPA), we can construct a detailed view of how NASA's decision-making structure, under immense pressure, contributed to this tragedy. The Challenger case study serves as a foundation to explore how variability within organizational functions and critical control actions influenced each level of decision-making, creating gaps that ultimately led to disaster.

The Functional Resonance Analysis Method (FRAM) can map out NASA's hierarchical structure and its interdependent functions. By identifying core functions within each level—macro, meso, and micro—we can illustrate how variability in processes led to a cascading breakdown.

DEFINING CORE FUNCTIONS

To create a set of Functional Resonance Analysis Method (FRAM) functions for the Challenger disaster, it's essential to break down each key decision, communication exchange, and the pressures influencing decisions from the individuals and organizational bodies involved. By tracing the sequence of interactions leading up to the launch, we can build a comprehensive model that reflects the functions and variability that ultimately led to the disaster.

Here's a detailed breakdown of the FRAM functions as they might be structured across the decision-making sequence, showing the involved individuals, their roles, and the pressures affecting their actions.

1. **Government Oversight and Funding Pressures (Macro Level)**

This function was subject to pressures from Congress, public expectations, and NASA's need to demonstrate program viability. Variability within this function arose from the high demands placed on NASA's performance, influencing operational demands and contributing to adherence to rigid schedules even in the face of safety warnings.

Function Set: **Set the Funding and Performance Expectations for NASA Shuttle Program**
Primary Agents: U.S. Congress, Office of the President, NASA Headquarters
Input: Public and congressional expectations, budget constraints
Preconditions: High national interest in space exploration as a symbol of technological prowess and national pride
Control: Pressure to maintain schedule reliability and cost-efficiency
Output: Aggressive shuttle launch schedule
Timing: Multi-year programmatic timelines, aligned with political cycles and public interest
Variability: This function exhibits variability under political pressure, as both Congress and NASA Headquarters needed to demonstrate NASA's value through reliable, frequent missions. These high-level expectations intensified the downstream pressure on NASA's program managers to avoid delays, implicitly encouraging decision-making that favoured schedules over technical caution.

2. **NASA Headquarters Directive to Meet Shuttle Launch Schedule (Macro Level)**

At this level, NASA management processed technical reports from contractors, balancing them against program schedules and risk management criteria. Variability emerged from conflicting goals—safety and timely launches—which affected decision-making as program managers minimized technical concerns to align with schedule expectations.

Function set: **Communicate Programmatic Priorities and Schedule Pressure to Centres**
Primary Agents: NASA Administrator (James Beggs), Deputy Administrator, Director of the Office of Space Flight
Input: National funding pressures and performance expectations
Preconditions: Desire to ensure NASA's perceived reliability and meet public expectations
Control: Authority from NASA Headquarters to dictate program priorities
Output: Directive to prioritize timely launches
Timing: Routine budget and schedule reporting intervals
Variability: Given the overarching goal of maintaining NASA's image as a dependable and advanced agency, Headquarters communicated programmatic priorities to NASA centres, with Marshall and Kennedy being most directly involved. The emphasis on timely launches created variability, as it pressured centres to minimize delays, impacting the evaluation of risks in launch decisions.

3. **Marshall Space Flight Centre's Role in Shuttle Component Oversight (Meso Level)**

Function Set: **Oversee Shuttle SRB and Technical Compliance**
Primary Agents: Lawrence Mulloy (SRB Project Manager), senior managers at MSFC
Input: Shuttle program goals, technical specifications from contractors (Morton Thiokol)
Preconditions: Need to balance schedule adherence with technical reliability
Control: Shuttle component management and oversight authority
Output: Finalized recommendation on SRB readiness and launch approval
Timing: Ongoing component review, with intensified scrutiny in pre-launch checks
Variability: Marshall's role placed it between NASA Headquarters and contractors like Morton Thiokol. MSFC managers, particularly Mulloy, were tasked with ensuring the SRBs met technical requirements but were also acutely aware of Headquarters' schedule priorities. This dynamic

influenced how they perceived and reacted to engineering concerns, as they faced implicit pressure to downplay delays.

4. **Morton Thiokol Engineering Risk Assessment (Micro Level)**

The engineers' task was to assess environmental data and technical performance indicators, like the O-rings' behavior in cold weather, to produce safety recommendations. The last-minute nature of this assessment, coupled with engineers' limited influence over the final decision, contributed to variability that weakened the impact of their concerns.

Function set: **Evaluate O-ring Integrity and Provide Risk Assessment**
Primary Agents: Roger Boisjoly (Thiokol engineer), Robert Ebeling, and other engineering staff
Input: Weather data indicating low temperatures, historical performance data on O-rings
Preconditions: Understanding of O-ring vulnerability in low temperatures
Control: Engineering standards for SRB safety, industry best practices
Output: Safety recommendation (initial recommendation to delay launch)
Timing: Late-night teleconference on January 27, hours before the scheduled launch
Variability: Thiokol's engineers were clear on the technical risks but lacked authority over the final launch decision. The engineers presented their concerns in a late-night teleconference, citing that the low temperatures could compromise the O-rings' performance. However, the engineers faced constraints in how effectively they could communicate this due to organizational pressures and communication filters.

5. **Morton Thiokol Management Decision under NASA Pressure (Micro Level)**

Function set: **Formulate Final Contractor Recommendation on SRB Readiness**
Primary Agents: Jerry Mason (Vice President of Thiokol), Bob Lund (Vice President of Engineering)
Input: Engineers' initial recommendation to delay, pushback from NASA's Marshall Space Flight Centre
Preconditions: Need to maintain good client relations and meet contractual obligations with NASA
Control: Influence from NASA's Marshall managers, particularly Mulloy's insistence on maintaining the schedule
Output: Final reversal of engineers' "no launch" recommendation to "launch approved"
Timing: Concluded late-night teleconference on January 27
Variability: Following intense questioning and pressure from NASA's Marshall Centre, Thiokol management overruled the engineers' concerns. Under Jerry Mason's instruction, management shifted their stance to support the launch, prioritizing contractual and client relationship concerns over safety, ultimately issuing an approval despite known risks.

6. **Marshall Space Flight Centre's Launch Readiness Review (Meso Level)**

Function set: **Conclude Launch Readiness with Contractor Approval**
Primary Agents: Lawrence Mulloy, other Marshall managers, Kennedy Space Centre representatives
Input: Final launch approval from Thiokol management, without direct access to unfiltered engineering data
Preconditions: Need to align technical readiness with NASA's operational goals
Control: Marshall's authority over SRB evaluation
Output: Conclusive approval of shuttle readiness for launch
Timing: Completed readiness review on the morning of January 28
Variability: Marshall's managers, reassured by Thiokol's revised stance, confirmed the shuttle's readiness. The communication flow from Thiokol to Marshall had removed direct engineering

concerns, enabling Marshall to validate launch readiness based on an incomplete understanding of the O-ring risk.

7. Kennedy Space Centre Final Launch Operations (Meso Level)

Function set: **Execute Final Launch Operations with Assumed Readiness**
Primary Agents: Kennedy Space Centre launch operations team
Input: Launch approval from Marshall and confirmation of component readiness
Preconditions: Assumption that all technical components meet launch criteria
Control: Launch operations management protocols
Output: Shuttle launch initiation
Timing: Morning of January 28, 1986
Variability: KSC launch operations were conducted under the assumption that Marshall and Thiokol's recommendations indicated full readiness. With no direct involvement in SRB design oversight, KSC operated based on trust in Marshall's and Thiokol's assessments, leading to the final decision to proceed with the launch.
These functions were built into a visualisation built using the FRAM method (ref), shown below in Figure 2

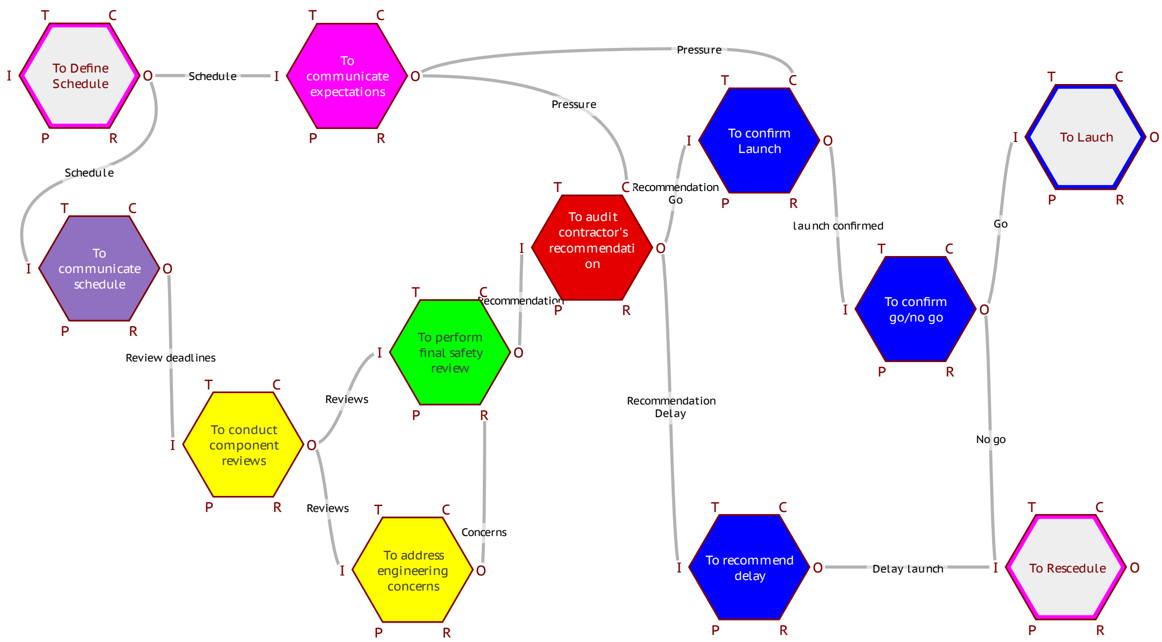

Fig. 2 – A FRAM built model of the decision-making system for the Challenger Launch.

This sequence of functions in the FRAM model shows how interdependent roles and functions contributed to the Challenger launch decision:

- **Oversight and Funding Pressures** created variability across NASA, emphasizing schedule adherence over safety, which resonated down to each level.
- **NASA Headquarters' Directives** reinforced this schedule pressure to centres, focusing program managers on operational targets.
- **Marshall's SRB Oversight and Role as an Intermediary** created a conflict between engineering integrity and schedule demands, leading them to exert pressure on Thiokol.

- **Morton Thiokol Engineering's Risk Assessment** highlighted the O-ring vulnerability, but their limited authority constrained them, as management ultimately prioritized contractual obligations.
- **Thiokol Management's Reversal** under Marshall's pressure shifted their position to support the launch.
- **Marshall's Confirmation of Launch Readiness** excluded critical engineering concerns, leading KSC to proceed with final launch operations without a full understanding of the risks.

Summary of Key Influences and Variability

To create a set of Functional Resonance Analysis Method (FRAM) functions for the Challenger disaster, it's essential to break down each key decision, communication exchange, and the pressures influencing decisions from the individuals and organizational bodies involved. By tracing the sequence of interactions leading up to the launch, we can build a comprehensive model that reflects the functions and variability that ultimately led to the disaster.

By modeling these interactions, FRAM illustrates how variability across functions led to a disconnect in critical information flows. For instance, high-level scheduling demands increased operational rigidity in decision-making, and communication barriers delayed or diluted the transmission of safety-critical data.

Using FRAM, we can visualize these interactions by connecting each function's aspects (e.g., input, control, timing). Input links represent the transmission of data from one function to another, while control links indicate hierarchical oversight that influences function execution. For example, program management relied on input from engineers, yet macro-level pressures meant safety recommendations were often downplayed. Similarly, communication was controlled by norms that aligned with NASA's operational goals, filtering out dissenting technical feedback.

This sequence of decisions leading up to the Challenger launch, helps in identifying critical steps and the variability that affected each function:

- **1. Macro-Level Influence**: NASA Headquarters establishes an overarching expectation for timely launches to maintain political and public support, initiating the sequence of decisions.
- **2. Meso-Level Oversight**: Marshall Space Flight Centre, responsible for SRB compliance, emphasizes schedule adherence. Marshall's communication with Thiokol applies direct pressure to reconsider the initial recommendation, creating tension between engineering assessments and managerial objectives.
- **3. Contractor Reassessment**: Morton Thiokol's engineers identify specific technical risks, but under pressure from Marshall and Thiokol management, the initial "no-go" recommendation is reversed to align with NASA's schedule expectations.
- **4. Final Readiness Check at KSC**: Kennedy Space Centre relies on Marshall's and Thiokol's confirmed recommendations, assuming that prior concerns have been addressed, leading to the final decision to launch.

- **5. Final Launch Execution**: Based on the sequential decisions and approvals across levels, the Kennedy Space Centre initiates the launch, unaware of the risks that had been filtered out.

This decision sequence framework illustrates how each level of NASA's organization contributed to the final decision through interconnected tasks, with cumulative pressures and filtered information undermining safety.

This FRAM model highlights how functions at every level were affected by external pressures and internal dynamics. Variability stemming from political and organizational demands distorted technical judgment, creating a resonance effect where multiple functions converged toward a decision that ultimately compromised safety.

COMBINING FRAM AND STPA: A UNIFIED MODEL OF THE DISASTER

Using STPA to Examine these "Control" Deficiencies

While FRAM maps functional variability, STPA allows us to identify specific Unsafe Control Actions (UCAs) that contributed to the disaster. STPA helps in understanding how control loops failed across NASA's structure, revealing where safety was compromised by absent or ineffective controls.

Oversight and Funding Pressure → Program Management Decision-Making
This control loop was marked by a lack of flexibility in response to technical concerns. The macro-level UCA was the enforcement of a strict schedule without incorporating safety margins, pressuring program management to prioritize timelines over safety.

Program Management Decision-Making → Engineering Risk Assessment
Control deficiencies here included downplaying engineering concerns to meet schedules, with program management exerting control over engineering recommendations. This created a filtering effect that minimized the impact of O-ring risks on the launch decision.

Engineering Risk Assessment → Communication and Reporting
Safety-critical data from engineers was hindered by bottlenecks within the reporting process. The UCA involved a failure to escalate concerns effectively, with engineers' recommendations diluted or delayed by hierarchical reporting norms.

Program Management Decision-Making → Oversight and Funding Pressure
This loop's deficiency lay in inadequate feedback mechanisms. Program managers lacked avenues to communicate operational constraints back to oversight bodies, allowing scheduling pressures to continue unchecked.

ANALYSIS

In defining the control loops described as being in place at that time, it becomes clear that there must have been extra functions to manage these controls, and this highlights the increase in the complexity of the system with a spider's web of implied reporting and communication lines. Of particular interest are the control loops which were set up to apply pressures and meet deadlines.

A recent development in the FRAM modelling, has established that these functions must behave more like neurons in neural nets rather than nodes and edges in classical predetermined networks. This means that functions, like neurons have "limits of tolerability" (ref), between which they will operate; to much or to little and the functions fail.

It can be seen from the model that there is pressure from the Centre on the Thiokol Management to sign off on the launch. If (as happened), the Thiokol management function fails under this pressure it has disastrous consequences. What is unclear is that debates about organisation design may be relevant in the broad sense, but this was a straight interaction between contractor and client which routinely happens in all kinds of situations – human factors?

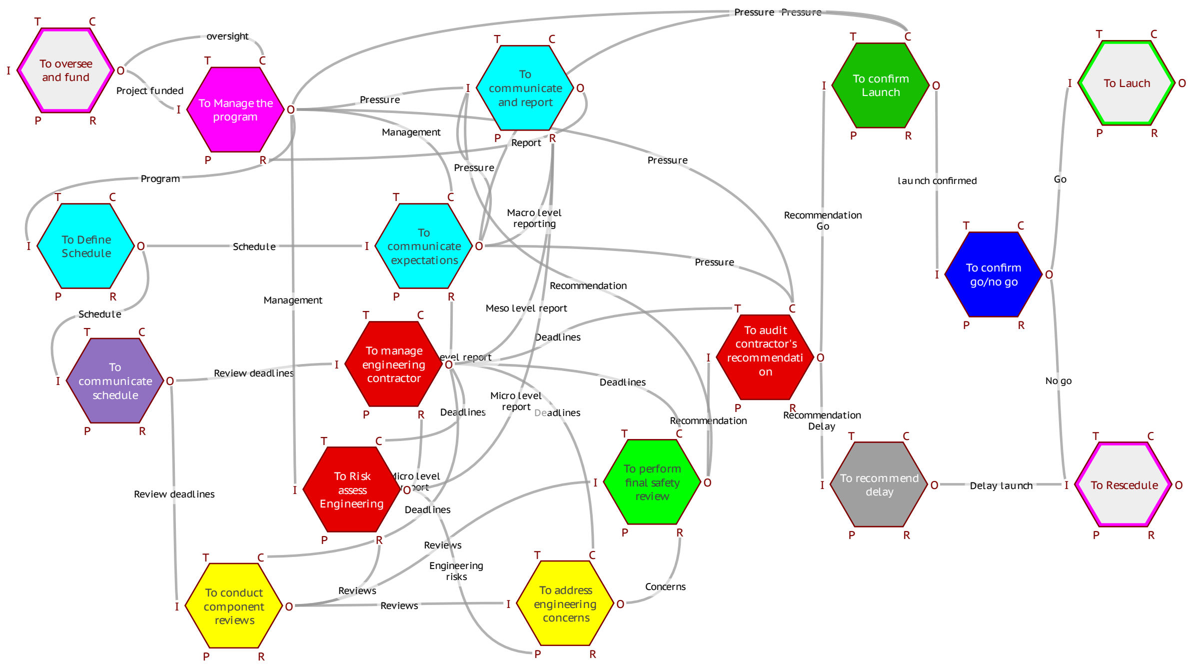

Fig. 3 – The FRAM model using STPA to enhance and define the control structures

LESSONS LEARNED?

It is very interesting to see that nowadays this relationship seems to have been reversed. NASA has been seemingly more cautious in dealing with another private contractor, Boeing, regarding the Starliner spacecraft, designed to transport astronauts to the International Space Station (ISS). The Starliner's crewed missions have faced multiple delays due to technical issues, including propulsion and system concerns that raised safety questions. Although Boeing has been keen to proceed, NASA opted to delay the latest launches to ensure all safety protocols are met, prioritizing astronaut safety over schedule. This approach reflects NASA's new culture, by insisting on verifying Starliner's readiness through comprehensive testing and risk assessment.

KEY ISSUES IDENTIFIED IN THE ANALYSIS

The Challenger disaster was a result of various systemic issues that originated from structural pressures and procedural weaknesses within NASA's organization.

The decision to launch the Challenger shuttle on January 28, 1986, was made through multiple layers of NASA's hierarchical structure, each influenced by external pressures, internal norms, and filtered information. Here's how the decision moved through NASA's structure, identifying key functions and levels responsible for that ultimate decision.

1. Micro Level: Engineering Teams and Morton Thiokol

Role in the Decision: Engineering teams at Morton Thiokol, the contractor responsible for the solid rocket boosters (SRBs), initially flagged concerns about the O-rings' performance at low temperatures expected on launch day. Engineers Roger Boisjoly and others warned that the O-rings, which sealed the SRBs, could become brittle and fail to seal correctly in the forecasted cold temperatures, potentially allowing hot gases to escape and compromise the shuttle.

Communication of Concerns: Morton Thiokol held a teleconference with NASA's Marshall Space Flight Centre the evening before the launch. During this meeting, Thiokol engineers recommended delaying the launch due to their concerns. Thiokol's senior management , however, reversed this recommendation following pressure from NASA officials at Marshall. This pressure included a question from NASA's Lawrence Mulloy, who famously responded to the delay recommendation by asking, "When do you want me to launch? Next April?" This pressure contributed to Thiokol managers overturning their engineers' recommendation and approving the launch.

2. Meso Level: Marshall Space Flight Centre (NASA Program Management)

Role in the Decision: Marshall Space Flight Centre (MSFC) in Huntsville, Alabama, was responsible for overseeing the shuttle's SRBs, including their design and manufacture by Morton Thiokol. MSFC served as an intermediary between NASA Headquarters and Morton Thiokol, managing technical and operational aspects of the shuttle's components.

Influence on the Decision: Marshall's program management was instrumental in shaping the final recommendation to launch. Managers at MSFC were under considerable pressure to maintain the shuttle's schedule, driven by expectations from NASA Headquarters and the public. The influence from Headquarters, combined with Marshall's role in balancing contractor input, placed MSFC in a position where they dismissed technical concerns in favour of operational goals. Their pressure on Morton Thiokol to reconsider their "no launch" recommendation directly contributed to Thiokol reversing its decision and supporting the launch.

3. Meso Level: Kennedy Space Centre (Launch Operations)

Role in the Decision: Kennedy Space Centre (KSC) in Florida was responsible for the final launch operations. While KSC primarily handled logistical preparations and vehicle inspections, it did not have direct oversight on technical design issues like the O-rings. However, the launch readiness reviews at KSC incorporated information passed down from MSFC and Thiokol.

Influence on the Decision: KSC relied on approval from MSFC and Morton Thiokol to ensure that all technical components, including the SRBs, met launch criteria. Because the concerns were dismissed by Marshall management and Thiokol, KSC accepted the assessment that the shuttle was ready to launch, despite the technical risks. The launch team at KSC did not receive unfiltered information about the engineers' concerns, as those had already been minimized by Marshall and Thiokol.

4. Macro Level: NASA Headquarters and Office of Space Flight

Role in the Decision: NASA Headquarters, particularly the Office of Space Flight, was responsible for setting overarching program goals and schedules. Senior officials at Headquarters were aware of the tight schedule and budget pressures, which had been communicated down to Marshall and other centres.
Influence on the Decision: The drive from Headquarters for NASA to demonstrate its ability to launch on time was immense. Congress and the public were closely watching the shuttle program as a symbol of national pride and technical progress, and NASA was under pressure to maintain the image of reliable and routine space flight. Although senior officials did not directly decide to launch Challenger that day, their emphasis on maintaining the schedule placed substantial pressure on Marshall and Thiokol to avoid delays, indirectly shaping the decision to launch.

The Final Decision and Contributing Factors

The final recommendation to launch Challenger was the result of cumulative decisions influenced by multiple levels within NASA:

- **Thiokol's engineers** initially opposed the launch, citing technical risks with the O-rings. However, following pressure from **Marshall Space Flight Centre**, Thiokol management reversed its position, supporting the launch with no delay.
- **Marshall Space Flight Centre**, in turn, pushed for the launch to stay on schedule, driven by implicit pressure from **NASA Headquarters** and the need to avoid delays that might jeopardize NASA's credibility and funding.
- **Kennedy Space Centre** proceeded with launch operations, assuming that Marshall's and Thiokol's technical approvals meant the vehicle was ready.

Several factors stand out as central to this failure:

Hierarchical Pressures and the Decision to Launch

The decision to launch Challenger was a layered and complex process where pressure to adhere to schedule goals was prioritized over technical caution. Each level—from engineering teams to NASA Headquarters—played a role, but the systemic issues lay in how information was filtered, and decisions were influenced by organizational priorities rather than safety considerations. NASA's hierarchical structure, combined with external political pressures, ultimately prevented effective communication of critical safety information, contributing to one of the agency's most tragic moments.

Yes, it was indeed the management at Morton Thiokol that overruled the recommendation of their engineers regarding the safety of the Challenger launch. On the night before the launch, during a critical teleconference with NASA officials from the Marshall Space Flight Centre, engineers at Morton Thiokol—most notably Roger Boisjoly—expressed serious concerns about the O-rings' performance in the low temperatures forecasted for launch day. The engineers warned that the O-rings, which were critical in sealing the solid rocket boosters, could become too brittle in the cold and fail to seal properly, posing a significant risk to the shuttle. One of those engineers, Roger Boisjoly had previously worked at Rockwell, and there learned from colleagues about a decision that McDonnell Douglas management had made to overrule concerns that their subcontractor's engineers had had regarding the safety of the design of the cargo bay doors locking mechanism on the DC10. The resulting explosive release of the doors in flight resulted in the loss of 336 passengers and crew. This left a lasting impression, and it is possible that by being aware of his heightened sensitivity was a factor in the subsequent management decisions.

So, when NASA's Marshall Space Flight Centre questioned Thiokol's recommendation to delay, pressure mounted. In particular, Lawrence Mulloy, the Marshall Space Flight Centre manager, expressed frustration and impatience with Thiokol's recommendation by asking, "When do you want me to launch, next April?" This statement, among others, created an atmosphere of intense pressure, subtly communicating that NASA wanted the launch to proceed as scheduled.

This reversal of the engineers' initial judgment illustrates how management decisions, driven by external pressures and internal dynamics, contributed significantly to the tragic outcome. The Rogers Commission, which investigated the Challenger disaster, identified this decision as a crucial factor, demonstrating how organizational pressures and communication barriers could lead to compromised safety.

Communication Breakdown

A significant communication breakdown existed across NASA's hierarchy. While engineers at the micro level were fully aware of the O-rings' risks, they lacked the empowerment needed to influence decision-making effectively. The organization's hierarchical structure limited the flow of critical information upward, leading to the dilution or outright disregard of safety concerns.

Pressure and Risk Normalization

Over time, NASA had normalized risk, largely due to prior successful missions that encountered but survived issues with the O-rings. This normalization fostered a culture where the perception of risk was reduced, leading to a downplaying of technical concerns in favour of maintaining operational schedules.

Lack of Systems Thinking

NASA's decision-making lacked a comprehensive systems approach, failing to account for complex interactions within its technical and organizational systems. The variability within key components, like the O-rings, was not adequately considered, leading to siloed decision-making that overlooked interdependencies and underestimated system-wide vulnerabilities.

Organizational Culture and Accountability

NASA's organizational culture prioritized success over caution, valuing the "can-do" spirit that emphasized reaching program milestones over halting for safety considerations. This culture also discouraged questioning decisions, with dissenting technical voices often disregarded. The lack of an accountability structure that empowered technical teams to assert safety concerns reinforced these systemic risks.

DISCUSSION

The Challenger disaster remains a profound case study for exploring systemic failure in complex, high-stakes environments, particularly within hierarchically structured organizations where pressure to meet operational goals can conflict with safety protocols. Using both FRAM and STPA to analyze the disaster highlights not only how specific failures occurred but also offers insight into broader organizational and cultural issues that can compromise safety. By combining these methodologies, we move beyond simple causal explanations to explore the intricate web of decisions, controls, and communications that shaped this tragic event.

The source of the "technical" pressure

NASA was charged with doing things that hadn't been done before, let alone "safely". As an organisation they produced groundbreaking technological solutions to achieve goals never attempted before; yes enthusiastically, but under tremendous political (sputnik) and reputational pressures to succeed. The designers produced the ideas and specified the performance to be delivered "as imagined" from the systems required. But, as always, the engineers on the ground, charged with this challenge worked around problem after problem, that kept emerging from the new engineering applications they were implementing.

For example, the propulsion system called for new rocket designs, both main engines and boosters, which would overload the central propulsion design teams.

- The work around was to contract outsourced solid-state boosters, proven in missile applications.

The manufacturer unfortunately was located in Idaho, which meant a 12-day rail journey on coupled flat cars to get these 150-foot rockets to the launch pads. During this journey, it was likely that the steel cylinders would become deformed.

- The workaround was to make them in segments and assemble at the launch site.

The segments were prefilled with propellant which made welding to reform the structural integrity of a tube was out of the question.

- The workaround was to use pinned tang and crevice joints to join the segments, sealed with normal "Viton" rubber "O" rings.

Exposure of rubber to 6,500 degrees Fahrenheit is not advisable,

- so, they were protected with an asbestos putty.

Under the stresses and strains of extreme temperature and pressure gradients and vibration, significant dynamic distortions could be expected.

- This had worked before in simpler missile applications and would be carefully checked after each launch.

So, this was the Design "as Done", but would the original designers, with their overall concept of system integrity, have countenanced an implementation that included potential exposure of ordinary rubber seals to combustion temperatures?

So as with Flixborough, Bhopal, Three Mile Island, Chernobyl, etc., the unintended compromise on system components was implemented without a mechanism to check against overall system design. Too late, too expensive, too embarrassing to start again from scratch, have to get on with what we've got?

Tragically the whole process was repeated later when the consequences of the decision to build the spaceplane out of aluminium instead of titanium, resulted in the mission integrity dependent on work arounds which included fragile foamed glass insulation tiles exposed to the same stresses and shocks, and which had not been fully tested before.

So, this is the downside of the invaluable ability of the human operator to adapt , respond and work around the real-world problems that emerge in implementing ideal designs in non-ideal real-life situations. It is a valuable and necessary attribute to be supported by expertise, (Longford), encouraged but carefully checked against the original system design intent. The normalisation of deviance is thus a natural instinct to embrace solutions to make the damn things work!

The Importance of Understanding Systemic Variability

In large, complex organizations, system variability is inevitable due to the diverse and interdependent functions that must work together toward a common goal. The FRAM model illustrates how variability across functions can lead to resonance effects—where fluctuations in one function influence others, amplifying risk in unanticipated ways. In the case of Challenger, variability in government oversight and program management functions, shaped by political and budgetary pressures, created a rigid operational structure that downplayed technical risks. This rigidity constrained the organization’s ability to adapt and make informed decisions in response to the engineering team’s warnings about the O-rings.

The discussion of variability is essential, as it underscores the need for adaptive mechanisms within organizations. A resilient structure would allow technical concerns to influence decisions more directly, even under pressure to meet schedules. This reinforces the value of systems thinking, where decision-makers must consider how interconnected elements, including political agendas and resource constraints, impact system safety.

The Role of Organizational Culture in Risk Management

There is a quote in Higinbotham’s book that summed up how NASA’s culture at the time was characterized by a “can-do” spirit that emphasized accomplishment over caution. While this attitude enabled the organization to achieve remarkable feats in space exploration, it also cultivated an environment where challenging decisions was discouraged. This cultural orientation created a sense of normalcy around risk-taking, leading to the gradual acceptance of deviations from safety standards—what sociologist Diane Vaughan described as the “normalization of deviance.” Over time, the organization became accustomed to accepting risks, even when those risks were potentially catastrophic.

STPA highlights how this culture influenced control deficiencies, with unsafe control actions (UCAs) stemming from decisions that prioritized schedule adherence over engineering assessments. This normalization of deviance illustrates how a strong culture of accomplishment, if left unchecked, can become a liability in high-stakes environments. Risk management frameworks need to prioritize open communication and empower employees to challenge decisions, regardless of the organizational hierarchy.

Communication as a Control Mechanism

One of the most striking insights from the Challenger disaster is the role of communication in effective risk management. Both FRAM and STPA reveal how the hierarchical structure at NASA hindered the transmission of critical information, particularly when engineering concerns were filtered or dismissed by management. This failure of communication acted as a critical breakdown in the control structure. Engineers who understood the technical risks were unable to convey the urgency of their concerns to those with decision-making authority, partly due to the organizational norms that prioritized operational goals over safety warnings.

The lack of an effective feedback loop, as illustrated by STPA, limited the engineers' ability to influence final decisions. In complex, high-stakes environments, communication must flow freely across all levels of an organization, ensuring that critical safety data reaches decision-makers unaltered. Establishing clear, reliable communication channels is a fundamental requirement in mitigating systemic risks, especially when dealing with complex, interdependent systems.

Lessons for Future Risk Management

There is a track record of formal safety analyses in NASA. Richard Feynman in a personal appendix to the formal investigation report (6) wrote that: -

"It appears that there are enormous differences of opinion as to the probability of failure with loss of vehicle and of human life. The estimates range from roughly 1 in 100 to 1 in 100,000. The higher figures come from the working engineers and the very low figures from management."

This was quoted in Spiegelhalter's book (12), where he adds ominously,

"But even Feynman may have underestimated the risks that the crews were facing."

He notes that in 2011, NASA carried out a retrospective risk analysis of 135 Shuttle missions. With their current knowledge, their new figures predicted a roughly 10% probability of catastrophic failure, a factor of ten worse than Feynman. He translates this to implying only a 6% chance of reaching the 25th launch (Challenger) without loss. This more realistic assessment reflects the can-do heritage of an organisation to whom the engineer's numbers would have seemed a concern to be worked around. But it does raise the issue as to what kind of risk assessments the management undertook to rebut the engineering numbers. It seems that today, NASA like many organisations has reverted to subjective, "semi" quantitative risk matrices (heat maps), to avoid confronting inconvenient uninformed numbers.

Ultimately, the Challenger disaster illustrates the essential need and respect for robust risk management. This perhaps should involve frameworks that go beyond addressing technical issues to encompass cultural and organizational dynamics. . Organizations like NASA must prioritize independent safety oversight, empower technical experts to influence decisions meaningfully, and build adaptive feedback loops to ensure critical information reaches those who need it most.

By incorporating FRAM and STPA, we gain a multidimensional understanding of risk, recognizing that complex failures rarely result from isolated errors but instead emerge from a combination of organizational pressures, control weaknesses, and cultural influences. The integration of FRAM and STPA provides a holistic view of how systemic failures can develop in complex organizations. Challenger's tragedy serves as a reminder of the dangers inherent in complex socio-technical systems, where organizational goals, structural pressures, and cultural norms converge to shape outcomes. This broader perspective is crucial for modern organizations, as it promotes the development of resilient systems capable of anticipating and managing the unexpected in increasingly complex operational environments.

Conclusions

The Challenger disaster provides a sobering reminder of the complexity and fragility of large, high-stakes organizations, especially those operating under public scrutiny. Through the combined use of Functional Resonance Analysis Method (FRAM) and System Theoretic Process Analysis (STPA), we gain a detailed, multi-faceted view of how system-level pressures, control weaknesses, and organizational dynamics culminated in a tragedy that could have been averted. This analysis shows that, far from being a simple mechanical failure, the Challenger disaster was the result of intersecting issues at multiple levels: intense political pressures, flawed decision-making structures, inadequate feedback loops, and a culture that had normalized deviance over time. This meant that:-
- The full rocket assembly was never fully tested.
- The budget they were working within was a fraction of what was required and unrealistic
- Like all 'Moon Shot' projects, this was absolutely on the edge of technical capability and so much of the innovation was groundbreaking and innovative.
- The engineers had a realistic assessment of the risks, but the NASA upper leadership were distant and increasingly came from a non-engineering background. This inhibited the full understanding of the risk, and undeliverable expectations!

But it was the management at Morton Thiokol that overruled the recommendation of their engineers regarding the safety of the Challenger launch. On the night before the launch, during a critical teleconference with NASA officials from the Marshall Space Flight Centre, engineers at Morton Thiokol—most notably Roger Boisjoly—expressed serious concerns about the O-rings' performance in the low temperatures forecasted for launch day. The engineers warned that the O-rings, which were critical in sealing the solid rocket boosters, could become too brittle in the cold and fail to seal properly, posing a significant risk to the shuttle.
However, when NASA's Marshall Space Flight Centre questioned Thiokol's recommendation to delay, pressure mounted. In particular, Lawrence Mulloy, the Marshall Space Flight Centre manager, expressed frustration and impatience with Thiokol's recommendation.
In response to this pressure, Morton Thiokol's senior management made a judgement as to possible overcaution in the engineering team and overruled their engineers' recommendation and decided to approve the launch. During the teleconference, Thiokol's vice president Jerry Mason reportedly told Bob Lund, Thiokol's vice president of engineering, to "take off your engineering hat and put on your management hat." After internal deliberation, the managers reversed the engineers' recommendation, issuing a statement of approval for the launch, despite the engineers' objections. This decision to prioritize organizational and client expectations over engineering caution became a defining moment in the Challenger disaster investigation, highlighting the influence of management pressure on safety-critical decisions.
Looking beyond NASA, this case study is instructive for all high-stakes environments, underscoring the need for organizations to build and maintain flexible decision-making structures that balance operational demands with technical risks. To prevent such systemic failures, organizations must prioritize open communication, enable independent oversight, and cultivate a culture that values caution as much as achievement. The Challenger disaster stands

as both a cautionary tale and an impetus for advancing organizational resilience, reminding us that success in complex, high-risk fields hinges as much on robust processes and cultural integrity as on technological prowess.
The application of FRAM in identifying functional variability emphasizes the importance of resilient structures in managing complex interdependencies and variability. Without adaptive mechanisms to address such variability, organizations become prone to resonant failures, as seen with NASA's prioritization of schedules over critical technical concerns. Meanwhile, STPA's focus on control actions reveals how specific unsafe control actions (UCAs) and inadequate communication channels contributed to the disintegration of essential safety barriers. By modeling the Challenger's decision-making structure, both methodologies underscore the need for control systems that respect and integrate technical expertise, empowering engineers and technical staff to influence decisions effectively.

References

1. Higginbotham, Adam (2019). Midnight in Chernobyl: the untold story of the world's greatest nuclear disaster (First Simon & Schuster hardcover ed.). Simon & Schuster. ISBN 978-1-5011-3464-7.
2. Turner, B. A. Pidgeon, N. F. (1987), Man Made Disasters, "The Failure of Foresight". Butterworths.
3. Vaughan, D. (1997), The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA, University of Chicago Press.
4. Pomeroy, J. (2024) "The Challenger Story" https://www.linkedin.com/pulse/challenger-story-james-pomeroy-gz1ee/?trackingId=DziV6t2WRnqFxX51%2Bd%2BliA%3D%3D [accessed Oct 28, 2024].
5. Leveson, N. and Thomas, J. (2018) STPA Handbook – MIT press, US. [accessed Oct 28, 2024].
6. US Government, (1986), Report to the President By the PRESIDENTIALCOMMISSION On the Space Shuttle Challenger Accident, https://sma.nasa.gov/SignificantIncidents/assets/rogers_commission_report.pdf (accessed 9/ 11 / 2024)
7. Hollnagel, E. (2012) FRAM: The Functional Resonance Analysis Method – modelling complex sociotechnical systems. Ashgate Press, UK.
8. Higginbotham, A. (2024) 'Challenger: A True Story of Heroism and Disaster on the Edge of Space' , Penguin, Random House, UK
9. Slater, D. (2024) STPA –"A Stairway to FRAM: Enhancing Complex System Modeling". Available from:https://www.researchgate.net/publication/384925927_STPA_-A_Stairway_to_FRAM_Enhancing_Complex_System_Modeling_ [accessed Oct 28 2024].
10. Slater, D. and Hill, R. (2023) How to use the Metadata Facility in FRAM https://www.researchgate.net/publication/384763526_HOW_TO_USE_THE_METADATA_FACILITY_IN_FRAM [accessed Oct 28, 2024].
11. Slater, D. (2024) Do FRAM Functions mimic Neurons? https://www.researchgate.net/publication/385205209_Do_FRAM_functions_mimic_Neurons [accessed Oct 28, 2024].
12. Spiegelhalter, D, (2024), The Art of Uncertainty: How to navigate Chance, Ignorance, Risk and Luck, A Pelican Book

