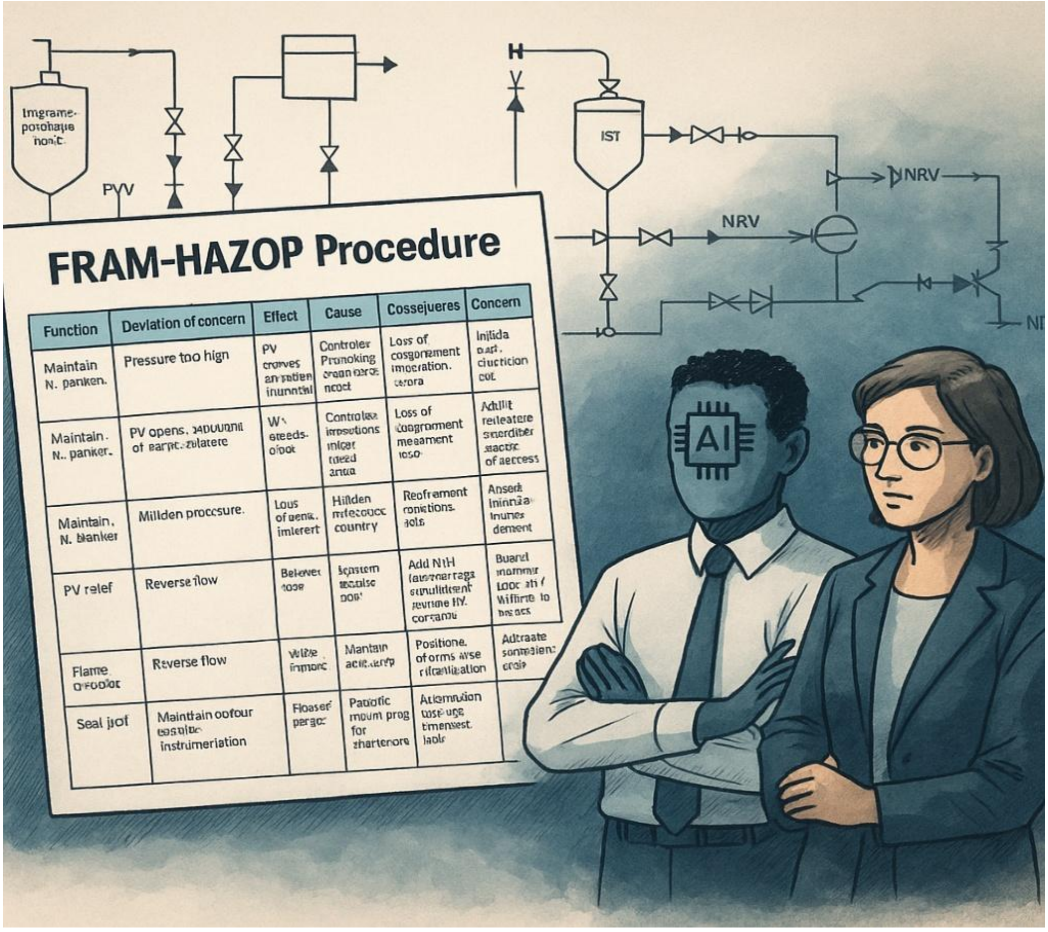

A Functional Systems Approach to Hazard and Operability Analysis

Abstract

Traditional Hazard and Operability (HAZOP) studies have proved invaluable for identifying deviations within process plants, yet their effectiveness declines as systems become more interconnected, automated, and software intensive. The classical node-based method, developed in the 1960s for linear piping systems, assumes that deviations propagate in a predictable and sequential way. Modern sociotechnical systems rarely behave so simply: feedback loops, shared controls, digital logic, and human interventions create dynamic couplings that can amplify or dampen disturbances in ways a static HAZOP cannot reveal. The ***FRAM-HAZOP Procedure*** *addresses this limitation by integrating the Functional Resonance Analysis Method (FRAM)—a systems approach based on functions and their variable couplings—directly into the HAZOP framework. In the FRAM-HAZOP, each FRAM function becomes a HAZOP node, and the traditional guide words (Too Much, Too Little, Too Soon, Too Late, Imprecise, None) are applied to the* ***outputs*** *of these functions. The consequences of each deviation are then propagated through the coupled functions within one to three hops, tracing their effect on system performance and barrier integrity. The paper presents the method in full, illustrates its application to a refinery Intermediate Storage Tank and petrol blending system, and demonstrates how this functional perspective captures emergent hazards, degraded protections, and resonance conditions that conventional HAZOPs overlook. By fusing*

FRAM's systemic modelling with HAZOP's procedural rigour, the FRAM-HAZOP provides a unified framework capable of analysing both linear process deviations and complex adaptive behaviour within the same methodological discipline.

Key words - FRAM-HAZOP; Functional Resonance Analysis Method; Process Safety; Systemic Hazard Analysis; Emergent Risk; Resilience Engineering.

1 Introduction

1.1 From Linear Systems to Complex Operations

Process industries have long relied on the HAZOP technique as the cornerstone of systematic hazard identification. By dissecting a process into discrete nodes—typically equipment items or pipe sections—and applying guide words such as *High*, *Low*, *More*, or *Less*, analysts could expose deviations from design intent and specify safeguards. The method's enduring success owes much to its procedural clarity and the quality of dialogue it promotes among engineers, operators, and safety specialists. However, the assumptions underpinning classical HAZOP—steady-state flow, clear physical boundaries, and single-variable causation—are increasingly strained in modern operations. Distributed control systems, instrumented safety layers, and human–automation interaction have transformed static process plants into highly coupled sociotechnical systems. In such environments, failure does not result from a single deviation but from the dynamic interaction of multiple variable functions that drift, mis-align, or reinforce each other over time.

1.2 The Functional Resonance Perspective

The *Functional Resonance Analysis Method (FRAM)*, introduced by Hollnagel (2012), offers an alternative paradigm. It models a system not as a collection of components but as an ensemble of **functions**—each representing an activity that must succeed for the system to perform as intended. Functions are defined through six aspects: *Input*, *Output*, *Precondition*, *Resource*, *Control*, and *Time*. Variability in any aspect can alter a function's performance, which in turn affects others through shared couplings. When multiple small variations combine or "resonate," emergent behaviour arises that cannot be predicted from the performance of individual components. FRAM thereby enables analysts to visualise complex interdependencies and understand how normal performance variability can drift into failure without any discrete component fault.

1.3 Rationale for Integration

While FRAM excels at capturing the dynamic and emergent nature of system behaviour, it lacks the prescriptive rigour of a traditional safety study: it does not specify guide words, tabular outputs, or structured recommendations for design action. Conversely, HAZOP provides strong procedural discipline but struggles to represent the non-linear relationships and time dependencies inherent in complex systems. The **FRAM-HAZOP Procedure** merges these complementary strengths. It retains HAZOP's systematic exploration of deviations and mitigations but relocates the unit of analysis from *equipment node* to *system function*. Each function's **output** becomes the point of application for HAZOP guide words, and its downstream couplings define the pathways through which consequences propagate. This approach preserves the traceability of classical HAZOP while enriching it with FRAM's capacity to reveal feedback loops, multi-function dependencies, and degraded barrier performance.

1.4 Objectives of This Paper

This paper sets out the **FRAM-HAZOP Procedure** as a repeatable, tool-supported method for analysing hazards and operability within complex systems. The objectives are fourfold:

1. To define a coherent workflow integrating FRAM model construction and HAZOP analysis;
2. To demonstrate the method on a representative process system—the Intermediate Storage Tank (IST) and transfer line to a petrol blending header;
3. To show how functional-node analysis identifies emergent risk pathways and barrier degradations that conventional node-based HAZOPs overlook; and
4. To discuss how the FRAM-HAZOP framework can support quantitative extensions such as metadata-driven Monte Carlo simulations or digital-twin integration.

The sections that follow outline the theoretical foundation of the procedure, describe its step-by-step implementation, and present the IST case study as empirical validation. The discussion concludes by positioning the FRAM-HAZOP within the broader safety-analysis landscape—alongside HAZOP, STPA, and resilience-engineering methods—and by suggesting how it may contribute to a new generation of systemic, model-driven safety assessments.

2 Methodology

2.1 Overview of the FRAM-HAZOP Procedure

The FRAM-HAZOP Procedure is a dual-layer analytical workflow designed to integrate the descriptive power of the Functional Resonance Analysis Method (FRAM) with the procedural discipline of classical HAZOP.
It proceeds in two complementary phases. The first builds a **functional model** of the system, capturing how work is intended to occur; the second overlays a **structured deviation analysis** that tests how variability in one function's output propagates through the model to affect overall system integrity.
The essential innovation lies in treating **each FRAM function as a HAZOP node**, and each of its **outputs as the locus of guide-word analysis**. By following the explicit producer-consumer links already defined in the FRAM model, the analyst can trace emergent behaviour systematically rather than intuitively.

2.2 Phase I – Functional Modelling (FRAM Layer)

(a) System definition and boundary conditions

The analyst begins by interpreting the reference documentation—typically a Process and Instrumentation Diagram (P&ID), control narrative, or operating procedure—to define what the system is designed to achieve and the constraints within which it operates. Each operational activity is then expressed as a *function* using FRAM's canonical six aspects:

Aspect	Description	Typical Example
Input (I)	What the function acts on	Flow signal, material feed
Output (O)	What the function produces	Controlled flow, alarm, report
Precondition (P)	What must exist before execution	Seal pot filled, permit valid
Resource (R)	What the function needs to act	Power, personnel, nitrogen supply
Control (C)	What governs or constrains it	Set-point, procedure, interlock
Time (T)	Temporal or sequencing constraints	Cycle interval, response delay

Each function is given an identifier and placed in a structured layout following process logic or control hierarchy. For traceability and tool compatibility, the model is stored in the FRAM Model Visualiser (.xfmv) format (Version 0.0.9.0), which ensures that every aspect has a unique producer and consumer, eliminating orphan links.

(b) Coupling and validation

Outputs from upstream functions are connected to inputs, controls, or preconditions of downstream functions through shared labels.
Validation criteria are:

- **Completeness:** every input has a producer; every output a consumer or sink.
- **Consistency:** no self-coupling within a single function.
- **Transparency:** metadata (set-points, limits, failure probabilities) are recorded explicitly.

The resulting model represents the system *as imagined* (Work-As-Imagined – WAI) and serves as the substrate for the subsequent hazard analysis.

2.3 Phase II – HAZOP Overlay (Functional Layer)

(a) From equipment nodes to functional nodes

Classical HAZOP decomposes a P&ID into equipment or pipe sections and applies guide words such as *High*, *Low*, or *Reverse* to process variables.
In FRAM-HAZOP, the decomposition is functional: each **function** becomes a **HAZOP node**. The **outputs** of that function represent the variables or results whose deviation can influence the system. This shift moves analysis from static hardware to dynamic behaviour, enabling examination of control loops, human actions, and digital logic within the same framework.

(b) Application of guide words to function outputs

For each output, the analyst applies the five standardised guide-word categories adapted for functional variability:

Guide-word category	Interpretation in functional terms
Too Much	Output magnitude or rate exceeds expectation

Guide-word category	Interpretation in functional terms
Too Little / None	Output insufficient, absent, or interrupted
Too Soon / Too Late	Output occurs out of sequence or with delay
Imprecise	Output uncertain, noisy, or inconsistent

Each deviation is assessed for:

1. **Plausible causes** (instrument failure, control drift, human intervention, environmental conditions).
2. **Immediate effects** on directly coupled downstream functions (first hop).
3. **Secondary propagation** to indirect couplings (second or third hop).
4. **Consequences** for system performance and safety barriers.
5. **Existing safeguards** (functional or physical).
6. **Recommendations** for improvement or further study.

2.4 Propagation Logic

Propagation is determined directly from the FRAM couplings: if Function A produces an output consumed as an input or control by Function B, any deviation in A's output modifies B's performance variability.
This one-to-three-hop tracing allows the analyst to observe **resonance chains**, where multiple small variations combine to create disproportionate effects.
By following these explicit paths, the FRAM-HAZOP maintains analytical discipline equivalent to fault-tree logic while retaining the flexibility to model emergent behaviour.

2.5 Recording and Reporting

Results are captured in a standardised tabular format that mirrors classical HAZOP practice but is keyed to functional identifiers:

| Function | Deviation of concern | Effect | Cause | Consequence | Concern | Recommendations |

This format preserves auditability and supports direct import into quantitative or simulation tools. The table can be exported as CSV, Excel, or Word formats, or embedded as metadata within the .xfmv file for live tracking in the FRAM Model Interpreter (FMI).

2.6 Quantitative and Digital-Twin Extensions

Each function and aspect can carry metadata such as:

- Nominal set-points and tolerance bands
- Probability of failure on demand (PFD) or spurious trip (PST)
- Confidence limits for measurement accuracy
- Response-time distributions

- Environmental modifiers (temperature, pressure, human workload)

These data enable **Monte Carlo simulation** or **Bayesian inference** to estimate how often particular resonance conditions may occur. The results can then be visualised as risk frequency-consequence (F–N) curves aligned with ALARP or R2P2 criteria (Fenton & Neil 2013; Public Health England 2018).
When connected to live plant or digital-twin data, the same metadata allow real-time assessment of barrier health and deviation trends.

2.7 Integration with Safety-Lifecycle Standards

The FRAM-HAZOP Procedure aligns with the principles of IEC 61882 (HAZOP Studies) and IEC 61511 (Functional Safety for the Process Industry).
Phase I corresponds to the conceptual design and hazard-identification stages; Phase II aligns with detailed design verification and operations HAZOP.
Because the functions and couplings are explicit, the resulting model provides a direct trace to Safety Instrumented Functions (SIFs), human-reliability tasks, and alarm-management logic, thereby strengthening the connection between qualitative analysis and quantitative verification.

2.8 Summary of Workflow

1. **Interpret source material** (P&ID, narrative, procedure).
2. **Identify functions** and assign FRAM aspects.
3. **Construct and validate** the .xfmv functional model.
4. **Apply guide-word deviations** to each function's outputs.
5. **Trace propagation** through coupled functions (1–3 hops).
6. **Evaluate consequences** and barrier performance.
7. **Record results** in the standard FRAM-HAZOP table.
8. **Optional:** attach metadata for quantitative simulation or digital-twin integration.

This workflow yields an analysis that is both procedurally auditable and systemically meaningful—combining the narrative richness of FRAM with the operational discipline of HAZOP.

3 Case Application: Intermediate Storage Tank System

3.1 System Description

The demonstration case concerns an **Intermediate Storage Tank (IST)** that receives C_6-fraction hydrocarbons from an upstream reflux drum and delivers them to a petrol blending header.

The tank acts as a **buffer** to decouple fluctuations in upstream distillation and downstream demand.

Operating pressure is maintained at approximately 500 Pa (gauge) through a **nitrogen-blanket control loop**, and level control is achieved via an **instrumented discharge train** comprising a level transmitter (LT), level controller (LIC), and level-control valve (LCV) feeding a **centrifugal transfer pump (J1)**.

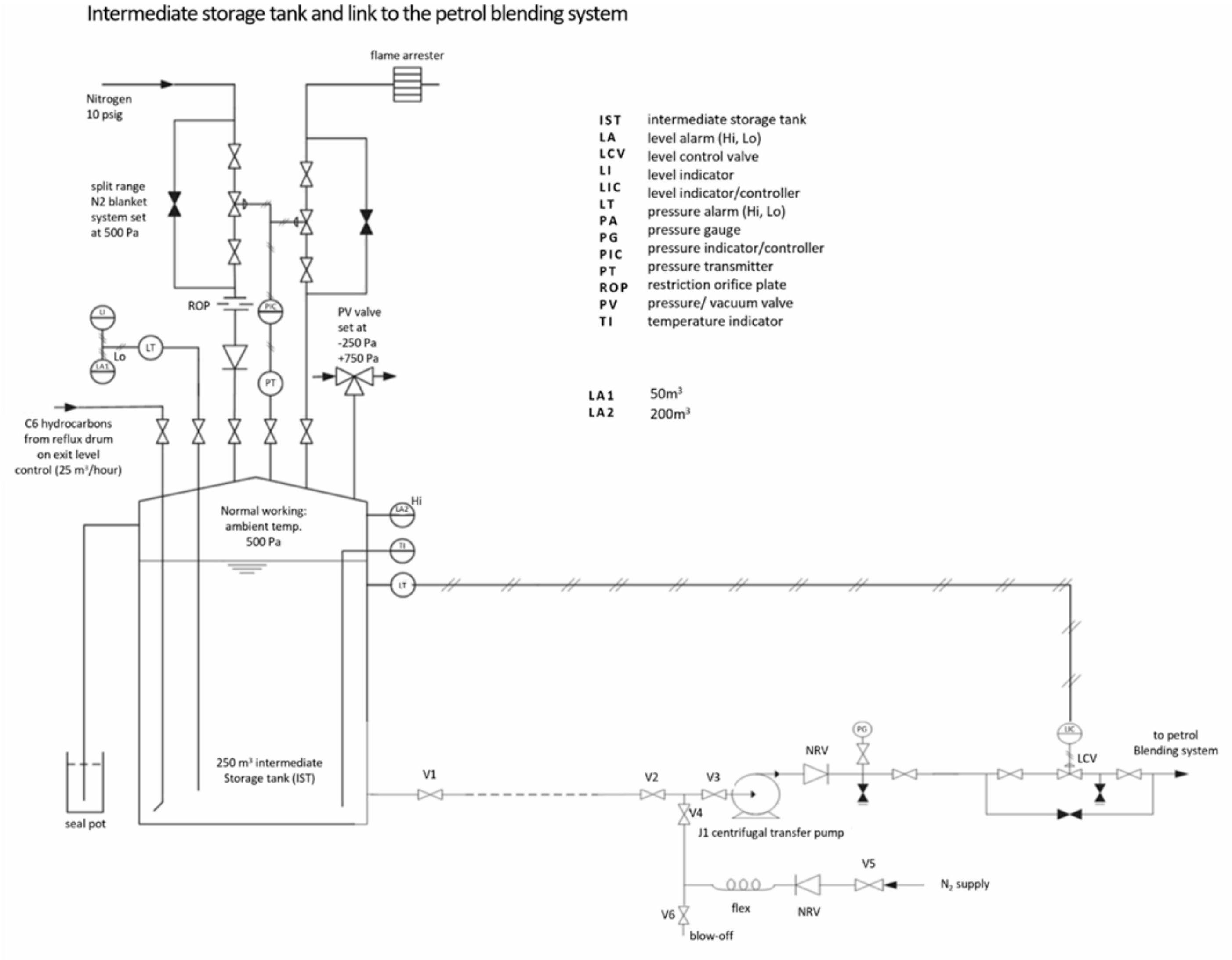

Fig. 3. The Reference P&ID (Crawley and Tyler 2015).

Protection systems include:

- a **pressure–vacuum (PV) relief valve** rated –250 Pa / +750 Pa;
- a **flame arrester** and **seal-pot** on the vent path;
- **non-return valves (NRVs)** on suction and discharge to prevent reverse flow;
- **manual isolation and blow-off valves** for maintenance purging.

The process is represented on a P&ID and forms the input to the FRAM-HAZOP analysis.

3.2 Functional Modelling (Phase I)

(a) Function identification

Fourteen functions were extracted from the P&ID to represent the process logic (Table 1). Each was defined using the standard FRAM aspects and modelled in the FRAM Model Visualiser (FMV) as a Work-As-Imagined (WAI) configuration.

ID	Function	Purpose
F1	Entry_C6_feed	Supply of hydrocarbon feed from reflux drum (25 $m^3\ h^{-1}$)
F2	Receive_inflow_to_IST	Buffer and distribute inflow within tank
F3	Sense_tank_pressure	Measure vapour-space pressure via PT/PG
F4	Maintain_N_2_blanket	Control blanket pressure through split-range N_2 valve
F5	PV_relief	Provide mechanical over-/under-pressure protection
F6	Measure_level	Transmit tank level to controller
F7	Level_controller	Compute discharge demand
F8	Level_control_valve	Regulate flow to pump suction
F9	Pump_transfer_J1	Transfer product to blending header
F10	Prevent_backflow	Ensure one-way integrity via NRVs
F11	Flame_arrester	Block flashback in vent path
F12	Seal_pot	Maintain vapour seal to instrumentation
F13	Blow-off_purge	Provide nitrogen purge for maintenance
F14	Exit_to_blending	Deliver controlled flow to blending system

(b) Coupling structure

Outputs and inputs were linked to reflect process dependencies:
Maintain_N_2_blanket → Sense_tank_pressure → PV_relief,
Measure_level → Level_controller → Level_control_valve → Pump_transfer → Prevent_backflow → Exit_to_blending.
Protective elements (flame arrester, seal-pot, PV valve) were modelled as controls or preconditions rather than direct flow nodes.

The validated .xfmv file contained no orphan aspects and represented the nominal behaviour of the tank system.

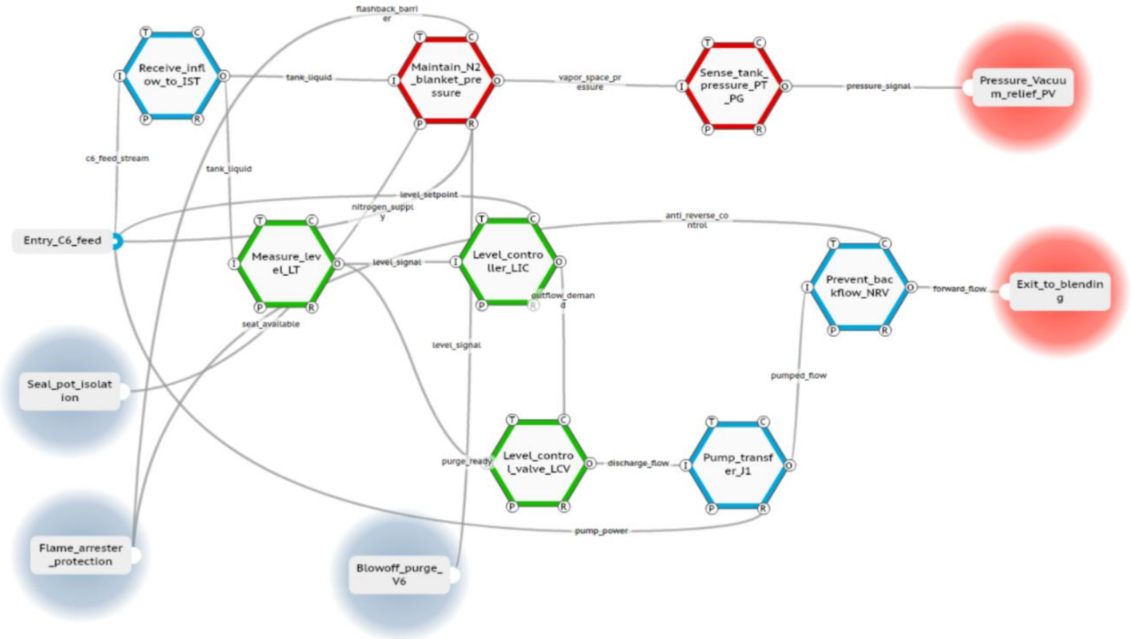

Figure – The AI generated FRAM model for systematic analysis using variability guide words

The validated .xfmv file contained no orphan aspects and represented the nominal behaviour of the tank system.

3.3 HAZOP Overlay (Phase II)

Each FRAM function became a HAZOP node; deviations were applied to the **outputs** and traced through coupled functions up to three hops.
The resulting table (excerpted in Table 2) shows representative findings.

Table 2 Excerpt from FRAM-HAZOP Analysis

Function	Deviation	Effect	Cause	Consequence	Concern	Recommendations
F4 Maintain N_2 blanket	Pressure too high (Too Much)	PV opens; emissions; blanket instability	Controller overshoot; valve stuck open	Loss of containment; equipment stress	Hidden vent restriction risk	Add HI-HI pressure trip; proof-test PV; monitor ΔP across arrester
F4 Maintain N_2 blanket	Pressure too low (Too Little)	Air ingress; vacuum on pump-out	N_2 supply failure	Flammability; shell collapse	LIC may continue discharge	Add LO-LO pressure trip to close LCV / stop J1
F7 Level controller	Outflow demand too high (Too Much)	LCV opens; pump cavitation	Aggressive tuning; LT bias low	Seal failure; vibration	Feedback amplifies via NRV chatter	Clamp LIC output; add suction low-P permissive
F8 Level control valve	Valve stuck open (Too Much)	Uncontrolled discharge	Stiction; bypass open	Low level; reverse flow risk	Operator may not see valve position	Position feedback; stiction alarm; LL trip to close
F9 Pump transfer J1	No/low delivery (Too Little)	Inventory rises	Trip; suction blockage	Overflow / production loss	Suction not monitored	Install suction low-P switch; discharge flow trip
F10 Prevent backflow	Reverse flow (None forward)	IST pressurised from header	NRV leak or fail open	PV lift; contamination	Single barrier only	Dual NRVs or NRV + auto isolation; leak-back tests

3.4 Propagation and Resonance Chains

Several three-hop resonance paths were identified:

1. **Pressure–Flow Coupling:** An overshoot in *Maintain N_2 blanket* (F4) → elevated *Sense tank pressure* (F3) → PV lift (F5) → partial blanket loss → air ingress on next cycle. This self-reinforcing loop can produce alternating over- and under-pressure events not predicted by steady-state design.
2. **Level–Flow Coupling:** A biased *Measure level* (F6) → excess *Level controller outflow demand* (F7) → open *LCV* (F8) → cavitating *Pump transfer* (F9) → damaged seal and vapor release.
3. **Header Feedback:** A downstream shutdown (*Exit to blending*, F14) → reverse pressure on *NRV* (F10) → pressurised IST → PV lift → emission cycle.

These paths demonstrate how variability propagates through functional couplings and why classical, equipment-node HAZOPs may miss coupled effects.

3.5 Barrier Assessment

Each protective function was graded (1–5, weak → strong) for reliability:

Barrier	Nominal Effectiveness	Degraded Mode	Restorative Measure
PV valve	4	Fouled spring/icing → 2	Proof-test and heat trace
Flame arrester	4	Condensate or fouling → 2	ΔP monitoring and cleaning
NRVs	3 (single)	Seat wear → 2	Dual installation or automated block
LIC–LCV loop	4	Stiction or sensor drift → 3	Functional testing; density compensation
Operator alarm response	2	Distraction / fatigue	Automated trip logic

The exercise confirmed that reliability depends less on any single safeguard and more on the *alignment* of control, protection, and human response.

3.6 Key Observations

1. **Functional transparency:** The FRAM model provided a clear map linking control variability, mechanical behaviour, and barrier interaction—impossible to see in a static P&ID.
2. **Coupled risk:** Small deviations (sensor bias, valve stiction) can create self-reinforcing loops that bypass traditional safeguard logic.
3. **Actionable output:** Each deviation yields both a qualitative explanation and concrete recommendations consistent with IEC 61882 and 61511.
4. **Reusability:** The .xfmv model serves as a digital asset for subsequent quantitative runs or digital-twin monitoring.

4 Discussion

4.1 Reframing Hazard Analysis Around Functional Variability

The FRAM-HAZOP Procedure represents a conceptual inversion of the traditional HAZOP logic. Instead of beginning with hardware and asking *"what if this component fails?"*, the analysis begins with **functional dependencies** and asks *"how might this function vary?"*. By shifting the analytical focus from equipment to function, the method captures phenomena that exist **between** components—delays, control-loop interactions, operator timing, and digital logic conflicts. This reframing reflects a broader evolution in safety science from deterministic failure analysis toward the study of **performance variability** and emergent outcomes. It allows deviations to be interpreted not merely as faults but as contextual fluctuations that can either stabilise or destabilise the system depending on alignment with other functions.

4.2 Comparison with Conventional HAZOP

Classical HAZOP offers an irreplaceable foundation for process-safety assurance: its structured dialogue, guide-word taxonomy, and clear traceability remain central to hazard management. However, its representational assumptions—that processes are linear and separable—become inadequate for highly automated or cyber-physical systems. The FRAM-HAZOP retains the HAZOP discipline but replaces static nodes with **living functions**, each already embedded in the network of controls, resources, and preconditions defined in FRAM. Three comparative benefits were observed in the IST study:

1. **Systemic Visibility.** Where the conventional HAZOP identified over-pressure and overflow as independent issues, the FRAM-HAZOP revealed them as outcomes of coupled variability between the N_2-blanket loop and the level-control loop.
2. **Resonance Recognition.** The ability to trace one-to-three-hop propagation paths exposed how minor deviations could resonate—illustrating why incidents often emerge from normal variability rather than gross design failure.
3. **Integrated Barrier Logic.** Barriers were evaluated as *functions* within the same model, enabling their conditional effectiveness to be quantified later through metadata rather than treated as binary "present/absent" safeguards.

Thus, the FRAM-HAZOP complements rather than replaces classical HAZOP. It provides a **supra-layer of functional interpretation**, particularly valuable in systems where human, software, and mechanical elements interact continuously.

4.3 Relationship to STPA and Other Systems Methods

The Systems-Theoretic Process Analysis (STPA) framework (Leveson, 2011) similarly examines control-loop structure and unsafe interactions. STPA operates at a higher level of abstraction, focusing on constraints and control responsibilities rather than performance variability. FRAM-HAZOP occupies the intermediate tier between STPA and equipment-level HAZOP.
Where STPA defines **why** a constraint may fail, FRAM-HAZOP explores **how** micro-variations propagate within and between functions to erode those constraints. It can therefore act as the **operational layer** within a multi-method safety architecture: STPA → FRAM-HAZOP → quantitative verification.

4.4 Quantitative Extension and the Role of Metadata

A distinctive strength of the FRAM-HAZOP is its ability to embed quantitative metadata directly in the model. Each function's aspects can include parameters such as measurement uncertainty, valve response delay, or probability of spurious trip. When simulated through Monte-Carlo or Bayesian networks, these metadata generate probability distributions for emergent states—overflow, emission, or loss of containment—rather than binary outcomes. This approach bridges qualitative reasoning and probabilistic risk assessment, permitting **F–N curve generation** and **confidence-band visualisation** (Fenton & Neil 2013; Public Health England 2018) while preserving the contextual fidelity of FRAM.

4.5 Integration with Digital-Twin and Real-Time Assurance

Because the FRAM model is machine-readable (.xfmv format) and explicitly defines every coupling, it can be connected to live process data streams. A digital-twin implementation could continuously monitor the effectiveness of barriers, detect drift in control alignment, and predict resonance conditions before thresholds are exceeded. The IST case demonstrated how metadata fields such as "PV blocked_prob" or "LIC bias" could be updated from operational telemetry to provide dynamic safety health indicators. In this way, the FRAM-HAZOP becomes not only a study method but also a **foundation for continuous assurance**.

4.6 Limitations and Practical Considerations

Despite its advantages, the method introduces new challenges.

- **Analytical load:** constructing a validated FRAM model requires more initial effort than delineating piping nodes.
- **Skill mix:** analysts must understand both process engineering and systems thinking; effective facilitation remains essential.
- **Tool maturity:** although the FRAM Model Visualiser and Interpreter support functional analysis, quantitative modules are still evolving.
- **Boundary definition:** over-abstraction can obscure physical failure mechanisms if not anchored to the underlying P&ID.

These limitations do not diminish the method's value but underline the need for training, tooling, and iterative integration with existing HAZOP workflows.

4.7 Implications for Safety Engineering Practice

The FRAM-HAZOP Procedure demonstrates that **functional modelling and classical hazard analysis can coexist within a unified methodological framework**. For practitioners, this means HAZOP teams can progressively migrate from equipment-centric to function-centric reasoning without abandoning established regulatory standards. For researchers, it offers a structured bridge between qualitative systems modelling and quantitative reliability analysis. More broadly, it signals a cultural shift: hazards are no longer viewed solely as deviations from design parameters but as emergent properties of complex adaptive performance.

5 Conclusion

The FRAM-HAZOP Procedure provides a structured means to analyse complex process systems in terms of **functional variability** rather than mechanical failure alone. By fusing the interpretive richness of the Functional Resonance Analysis Method (FRAM) with the procedural discipline of HAZOP, it enables hazards to be traced along pathways of coupling and feedback that conventional node-based studies cannot represent. The method retains the familiar grammar of HAZOP—guide words, tabular records, and action tracking—while relocating analysis from *equipment nodes* to *system functions* and their **outputs**.

The Intermediate Storage Tank (IST) case study demonstrated that apparently separate risks, such as over-pressure, overflow, and back-flow, are in fact coupled behaviours arising from mis-aligned control loops. The FRAM-HAZOP framework exposed these resonance chains, clarified the conditional performance of barriers, and translated its insights into actionable engineering recommendations. It thus links qualitative reasoning with quantitative potential: every function and aspect can host metadata for probability, timing, and confidence limits, allowing future Monte-Carlo or Bayesian simulation of functional resonance events.

Beyond the specific domain of hydrocarbon storage, the FRAM-HAZOP Procedure establishes a **general systems-based paradigm** for hazard and operability analysis. It can be applied to any socio-technical system—refineries, healthcare processes, rail operations, or autonomous technologies—where safety depends on the coordination of multiple interacting functions. By shifting attention from the behaviour of parts to the *resilience of the whole*, the FRAM-HAZOP supports a new generation of design, assurance, and learning processes capable of keeping pace with the complexity of modern operations.

References

Crawley, F. K., & Tyler, B. J. (2015). *HAZOP: Guide to Best Practice* (3rd ed.). Elsevier.

Fenton, N., & Neil, M. (2013). *Confidence in Risk Assessments: Quantifying Uncertainty to Support Decision-Making*. University of Bristol. Retrieved from https://research-information.bris.ac.uk/en/publications/confidence-in-risk-assessments

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. Ashgate.

International Electrotechnical Commission (IEC). (2001). *IEC 61882: Hazard and Operability Studies (HAZOP Studies) – Application Guide.* Geneva: IEC.

International Electrotechnical Commission (IEC). (2016). *IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector.* Geneva: IEC.

Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT Press.

Public Health England. (2018). *Technical Guide: Confidence Intervals*. Retrieved from https://fingertips.phe.org.uk/documents/PHDS%20Guidance%20-%20Confidence%20Intervals.pdf