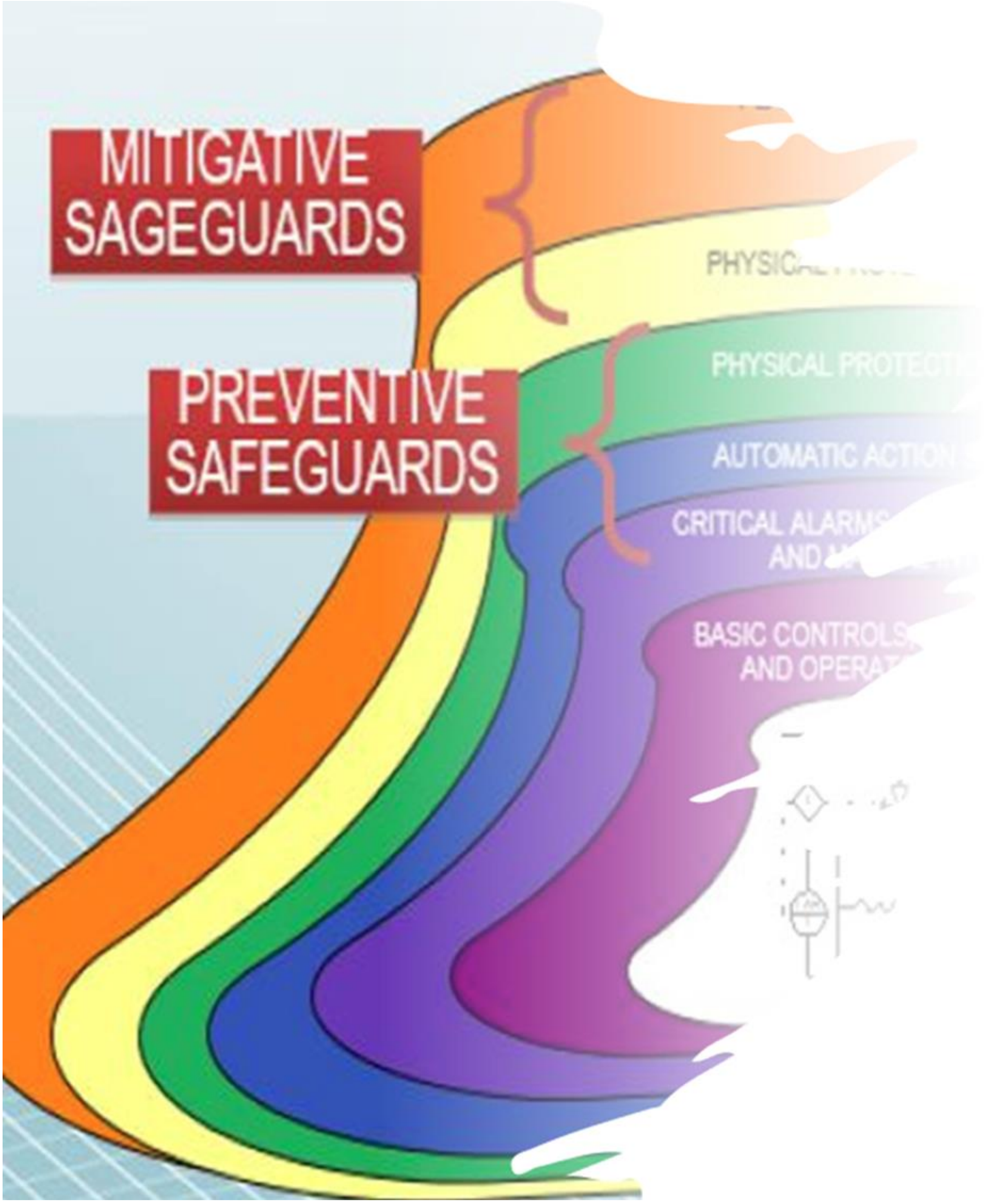
12/1/2024



Layers of Protection (©AIChE-CCPS) *after S L Chakravorty*

CAMBRENSIS

Functional System Integrity Assessment

The illusion of LOPA | David Slater

FUNCTIONAL SYSTEM INTEGRITY ASSESSMENT

David Slater, Cardiff University, dslater@cambrensis.org

ABSTRACT

Traditional approaches to risk assessment in complex systems often rely on the assumption that individual components, or barriers, operate independently. This reductionist mindset, while simplifying calculations, overlooks the interdependencies and interactions that are intrinsic to real-world systems. As Russell L. Ackoff emphasized, the essence of a system lies not in its parts but in the interactions between them. This paper explores the limitations of analyzing systems as collections of independent components and examines the implications of how failure probabilities are combined under assumptions of independence using straightforward multiplication, as seen in Layers of Protection Analysis (LOPA).

In contrast, when taking into account the fact that in systems, dependencies exist, methods employing conditional probabilities such as Bayes' Theorem offer a more accurate way to quantify risk by accounting for how the failure of one function increases the likelihood of subsequent failures. These distinctions are crucial for accurately assessing system resilience and identifying emergent risks that arise from complex interactions.

It highlights the importance of holistic methodologies such as the Functional Resonance Analysis Method (FRAM). By modeling how upstream functions influence the success or failure of downstream functions, FRAM provides a framework for understanding the propagation of variability and failure within a system.

Ultimately, the insights derived underscore the necessity of moving beyond reductionist analysis to embrace a systemic perspective. By recognizing and modeling interdependencies, risk assessments become more reflective of reality, enhancing our ability to anticipate vulnerabilities and design resilient systems. This shift toward holistic analysis, grounded in systems thinking, ensures a deeper understanding of system behaviour and more effective risk mitigation strategies.

Key Words – Bow Ties, LOPA, Bayes, FRAM

INTRODUCTION

In the analysis of complex systems, the temptation to reduce the system into discrete, independent components has been both pervasive and, ultimately, misleading. As Russell L. Ackoff, a pioneer in systems thinking, profoundly observed, **"A system is not the sum of its parts; it is the product of their interactions."** (1). This insight challenges the reductionist mindset that isolates components in an attempt to understand the whole. When systems are dissected and their elements are analyzed individually, the essential relationships and interactions — the very essence that defines system behaviour — are lost. The emergent properties, those characteristics that arise only through the dynamic interplay between parts, cannot be deduced by examining the parts alone.

Ackoff argued that systems must be understood holistically, where the context, purpose, and relationships between components are given due prominence. Components within a system do not exist in isolation; they derive their meaning and function from the larger system to which they belong. For example, a car's performance cannot be inferred solely by studying its engine, wheels, or brakes in isolation. It is the interaction of these components, governed by design and purpose, that gives the vehicle its functionality. Similarly, in biological systems, the health of an organ can only be understood in the context of the body's intricate web of interdependencies.

This perspective holds critical implications for the fields of **risk assessment** and **resilience engineering**, particularly when analyzing protective barriers in safety-critical systems. Traditional methodologies, such as **Layers of Protection Analysis (LOPA)**, (2), often assume that barriers operate independently, allowing failure probabilities to be combined multiplicatively. While such assumptions simplify calculations, they may lead to significant underestimations of risk. Real-world systems, whether socio-technical or purely technical, are rarely collections of independent components; they are complex networks where the failure or success of one function can influence the behavior of others.

A recent report (3) pointed out these inconsistencies in the Layers of Protection Analysis method for predicting probabilities of failure of barriers designed to protect systems from threats. It questions whether the comfort of compliance from the low probabilities typically calculated using this method, is in fact, illusory. This calls into question its adoption for certifying system Integrity levels used by many current codes and standards. But this in turn, raises the valid question, of, if not LOPA what? This paper examines alternative approaches and makes a case for retaining the basic LOPA approach and PFD's but tests using the FRAM methodology to take into account their mutual interdependencies in their interactions with the rest of the complex system.

ALTERNATIVE APPROACHES.

1. BAYES

The most obvious alternative methodology candidate to test is the Bayesian approach to calculating these probabilities in the light of evidence of performance (good or concerning) from the rest of the system. To calculate the combination of probabilities using **Bayes' Theorem**, (4), we need to frame the problem in terms of **conditional probabilities**. Bayes' Theorem helps us update the probability of an event based on new evidence, and it can be particularly useful when events are **dependent** or when we want to understand how one event influences the likelihood of another.

Imagine you have three barriers (A, B, and C) that are designed to prevent a hazardous event. We want to calculate the probability that all three barriers fail, but we'll explore two cases:

1. **Independent Barriers**: The failures of A, B, and C are independent.
2. **Dependent Barriers**: The failure of one barrier increases the likelihood that another barrier fails.

Let's use the following probabilities:

- **P(A)**: Probability that Barrier AAA fails = 0.1 (10%)
- **P(B)**: Probability that Barrier BBB fails = 0.05 (5%)
- **P(C)**: Probability that Barrier CCC fails = 0.02 (2%)

For the **dependent case**, let's assume:

- **P(B|A)**: Probability that B fails given that A has failed = 0.2 (20%)
- **P (C| (A∩ B)**: Probability that C fails given that A and B have both failed = 0.5 (50%)

CASE 1: INDEPENDENT BARRIERS

Since the barriers are independent, the probability that all three barriers fail is the product of their individual probabilities:

$$P(A \cap B \cap C) = P(A) \times P(B) \times P(C))$$

Substituting the values:

$$P(A \cap B \cap C) = 0.1 \times 0.05 \times 0.02 = 0.0001$$

This means there is a **0.01%** chance that all three independent barriers fail.

***Case 2: Dependent Barriers (Using Bayes' Theorem*)**

The likelihood that all three barriers fail:

1. **Step 1**: Calculate P(B∩A) (probability that A and B both fail):

$$P(B \cap A) = P(B|A) \times P(A)P(B) = P(B|A) \times P(A)$$

Substituting the values:

$$P(B \cap A) = 0.2 \times 0.1 = 0.02$$

2. **Step 2**: Calculate P(C∩B∩A) (probability that A, B, and C all fail):

$$P\,(C \cap B \cap A) = P(C|A \cap B) \times P(B \cap A)$$

Substituting the values:

$$P\,(C \cap B \cap) = 0.5 \times 0.02 = 0.01$$

This means there is a **1%** chance that all three dependent barriers fail.

Comparison of Results

Scenario	Probability of All Three Failures
Independent Barriers	0.0001 (0.01%)
Dependent Barriers	0.01 (1%)

Independent Barriers: When barriers are independent, the combined probability of failure is significantly lower because each barrier provides a unique and isolated layer of protection.

Dependent Barriers: When barriers are dependent, the failure of one barrier increases the likelihood that others will fail. This leads to a higher combined probability of failure, reflecting the reduced effectiveness of dependent protections.

(A fuller derivation is given in Appendix B.)

2. FRAM

The Bayesian approach can tell us how the overall probability of failure is dependent on how the different barriers themselves affect each other. But that still leaves the question of how these barriers are affected by what is going on in the total system (Ackoff's criterion). For that we need an approach that can model the critical interactions across the whole system. The Bow tie methodology does attempt to give a wider overview, but only on the linear sequences of Barriers. This makes it a natural system analysis method to use as a precursor to the LOPA process. But if we need a bona fide system model which includes all the functions, not just those that provide the barriers against threats, we need a more systems oriented approach.

The **Functional Resonance Analysis Method (FRAM)** (5) embraces this systemic perspective, providing a framework to model variability and interdependencies between functions. In FRAM, each function's success depends on aspects — inputs, controls, resources — that are often supplied by upstream functions. The failure of an upstream function propagates through the system, affecting the likelihood of success for downstream functions. This interconnectedness aligns with Ackoff's assertion that optimizing individual components does not necessarily optimize the system as a whole. Indeed, improving the reliability of a single barrier may prove ineffective if the dependencies that connect it to other functions are not understood or managed.

By recognizing and quantifying these interactions, FRAM offers a means to capture the **emergent risks** that arise from the dynamic interplay of system components. The approach reflects Ackoff's conviction that systems must be analyzed in context, where the relationships between elements are considered as crucial as the elements themselves. This holistic approach not only enhances the accuracy of risk assessments, but also strengthens the resilience of systems by identifying points of vulnerability that would otherwise remain hidden in a reductionist analysis.

In summary, the limitations of analyzing systems as collections of independent components are well-documented, and the insights of systems thinkers like Ackoff provide a compelling rationale for adopting holistic methodologies. In the realm of safety-critical systems, embracing systemic approaches allows us to move beyond simplistic models of failure and toward a more nuanced, accurate, and ultimately resilient understanding of risk and performance. The following section attempts to spell out how this could be achieved.

Implementing The FRAM LOPA Method

1. Process description

As in all these studies, we will first need a process description; an identification of what the system is supposed to deliver, and the critical steps needed to deliver the desired outcome(s). This will also identify issues such as history of incidents, upsets, difficulties, and outages. It should in addition, produce a list of "THREATS" to the successful delivery and the critical point of no return where process control is lost, and the measures needed to recover from it.

This then results in a list of "BARRIERS"; that are needed to address these issues. Defensive "PREVENTIVE" barriers to ensure control is maintained and "MITIGATION" barriers to ensure recovery or safe landing if the incident is not preventable. This list of barriers is then used in the next step.

2. The Bow Tie "picture"

The analyst builds a Bow tie of the role, responsibility, and sequence of operation of these barriers, as normal, probably using commercial software such as Kenexis, or BOWTIE XP. (6)

Each Barrier is thus defined as to type, state, sequence, and probably a Probability of Failure on Demand (PFD), for a subsequent Layers of Protection (LOPA) calculation of System Integrity Levels (SIL's).

This picture is a system overview of just the safety critical systems, barriers, tasks, or FUNCTIONS designed to protect the system's vulnerability to threats and to cope with potential consequences of these threats being realised.

3. THE SYSTEM MODEL

Using the FRAM Model Visualiser (FMV Bow Tie version), each of the list of barrier functions identified above, is entered as a FRAM function. It is simpler now to lay out these functions on the visualiser as pictured in the Bow Tie diagram previously produced. (7)

The software will ask the user to define the Barrier type and whether it is a Human task, an Organisational task, or a Technical system or component, (H, O, T), and probably its state (status).

It will then ask for a probability of failure on demand (PFD).

With the functions laid out in sequence, the FRAM analysis then enables the software to couple the relevant functions with the available Aspects, to each of the separate barriers to form a system model that can produce the outcome required. (8)

What are the inputs needed to activate these functions and where do they come from? – the analyst can now add the functions necessary.

What are the preconditions and resources required to enable the function to work, and where do they come from? The software will automatically link to existing functions if they are the sources required, or if not, the supplying functions need to be added. (Power supplies, resources, maintenance etc.). Are they common to more than one barrier?

Particularly important are the aspects that enable control of the system and in particular the effectiveness of the barriers. Here a System Theoretic Process Analysis (STPA) is a great help. Lastly obviously timing and sequence are crucial to the effectiveness of the barrier operation. (9).

We now have a Functional Barrier Bow Tie model that is capable of being analysed as to the interactions and interdependencies of the barriers and other system functions. (10)

4. ANALYSIS OF THE MODEL

What if?

This model now allows the analyst to systematically query what happens to these functions if some of the connecting functions as happens in real life, produce less than perfect expected timings, controls, resources. What effects do these potential variabilities have on the successful operation of the barriers and outcomes of the process?

If the organisation is accustomed to HAZOP's, the same systematic approach can be more formally applied. Particularly important is the identification of unexpected links between functions not formally considered in the sequence of barrier challenges – so called Resonance effects.

5. CALCULATION OF SYSTEM INTEGRITY

The FRAM built model is more than a picture.

The software has a built-in interpreter which checks the validity of the model and its viability as a dynamic model of how the process progresses. (11)

The software has an ability to assign a set of metadata to a function. This not only stores the information input from the standard Bow Tie model, (Type, PFD, Status, etc.) but also can allow the downstream functions to process that data with algorithms that can specify how these properties develop dynamically through the process. (12, 13))

For example, the properties can be varied deliberately or randomly to test the what if reactions of the whole system. If required, this could be done automatically using a Monte Carlo approach and recycling the model many times with a set of randomly generated metadata.

A probability of success or failure to deliver the expected outcomes can be derived at an individual functional, or system level. This (using exactly the same metadata) can yield a much more appropriate measure of system Integrity than the simplistic LOPA methodology.

6. IMPLEMENTATION

The analyst has complete control over the metadata and equations used to calculate the variabilities and probabilities employed in the software. Most experienced users of the FRAM approach will develop and insert their own requirements.

The standard version has a set of default keys, values, and equations for the convenience of inexperienced, occasional, or users to whom numbers are an anathema, The metadata set out in the table 1. below seemed to provide a very useful set for an analyst to use in an initial exploration of the propagation of individual function and total system performances as the instantiations progress. For our purposes in studying the Bhopal scenario (Appendix A.)we felt they gave the most acceptable insights into the system behaviours.

Table 1– Metadata used by the FMV to model performance probabilities.

Parameter	Key	Value	Equation
Probability that function fails to activate. (or successfully activates (PSD) if preferred?)	PFD		User Input in the FMV
Probability of Function/ system instantiation failure	Pfd	PFD	= PFD
Probability of Function/ System producing required output	Pso		= 1 - Pfd
Probability of Function failing, given the probabilities of linking aspects.	Pfd		= Amax_Pfd*Pfd
Probability of function activating, given the probabilities of linking aspects	Psd		= Amin_Psd*Psd

Other sets of equations were tested, including: -

A, **multiplying the predictions from using all the aspect upstream probabilities in turn and multiplying the results.**

If Pii = Pfd(input) x Pfd (function), and

$$\text{Pin} = \text{Pfd (aspect n)} \times \text{Pfd (Function), then}$$

$$\text{Pfd (output)} = \prod_{n} \text{Pin}$$

B. **a full Bayesian formulation with the Function Pfd as a Prior and the aspect probabilities as evidence to modify the prior** (Full equations here (15)

But they did not make the analysis easier and worth the considerable extra calculations involved. So, relying on Ockham's razor – the simplest approach is probably sufficiently accurate!

As the difference is marginal (0.4%), for our initial analysis we felt could use the LOPA independent PFD's but use the FRAM method to link those aspects that the function is dependent on and use their probability of failure to calculate the resulting probability of failure.

We can then therefore also propagate the probability of failure on demand to calculate the probability of failure of a downstream function in a FRAM model. This is particularly useful when modeling the dependencies between functions and understanding how failures in upstream functions affect downstream outcomes. The results of using such an approach is shown in Appendix A.

CONCLUSIONS

The analysis of complex systems demands a departure from traditional reductionist thinking and an embrace of systemic, holistic approaches. As Ackoff's insights remind us, systems cannot be fully understood by isolating their individual components; their true nature is found in the dynamic interactions and relationships between these components. This understanding is critical in the domain of risk assessment and resilience engineering, where the interplay between protective barriers or functions dictates overall system behaviour. Reductionist methodologies, which assume independence among barriers and functions, can lead to significant underestimations of risk, obscuring the potential for cascading failures and emergent vulnerabilities.

We explored how probabilities of failure propagate through systems, illustrating the difference between independent and dependent functions. When functions are assumed to operate independently, failure probabilities can be combined multiplicatively, providing a straightforward yet limited assessment of risk. However, real-world systems often exhibit dependencies where the failure of one function increases the likelihood of subsequent failures. In these cases, conditional probabilities and Bayes' Theorem offer a more nuanced and accurate way to model risk, reflecting the interconnectedness inherent in complex systems.

The Functional Resonance Analysis Method (FRAM) however seems to provide the whole system framework for capturing these interdependencies, emphasizing how the success or failure of a function depends on upstream aspects — inputs, controls, resources, and timing. This approach aligns with Ackoff's principle that system performance is a product of interactions, not just the sum of individual actions. By propagating failure probabilities through these interconnected aspects, FRAM helps reveal vulnerabilities that reductionist methods would overlook. This systemic approach enhances our ability to anticipate emergent risks and identify where additional safeguards or interventions are necessary.

Are the probability numbers now more accurate? The adage “all models are wrong, but some are useful” (15) applies here. The numbers are a guide to the extent of the potential interactions and interdependencies that can affect the performance of the system as a whole. They convey an element of importance, priority, and perhaps, concern, that is more useful to an engineer than just qualitative discourse. Are they accurate, probably not; but despite that, enable a more realistic analysis of the system, certainly more useful than treating the barriers as standalone components.

Ultimately, the insights gained here reinforce the importance of holistic analysis in understanding and managing complex systems. The resilience of a system is not merely a function of its individual barriers or components but of how these elements interact and adapt under varying conditions. By integrating systems thinking principles, such as those championed by Ackoff, into methodologies like FRAM and Layers of Protection Analysis, we move toward a deeper, more reliable understanding of system behaviour. This shift not only improves risk assessment accuracy, but also fosters the development of systems that are better equipped to withstand variability and unexpected challenges.

In conclusion, recognizing and addressing the interdependencies within systems is essential for capturing the full scope of risk and enhancing system resilience. The path forward lies in embracing complexity, understanding interactions, and rejecting the simplicity of isolated analysis in favour of a more interconnected, systemic perspective.

References

1. Ackoff, R. L. (1971). Towards a System of Systems Concepts. Management Science, 17(11), 661–671. https://doi.org/10.1287/mnsc.17.11.661
2. Centre for Chemical Process Safety (CCPS). (2001). Layers of Protection Analysis: Simplified Process Risk Assessment. American Institute of Chemical Engineers (AIChE).
3. Slater, D., (2024), The Paradox of PFD's | The Buncefield Disaster: A Case Study in Safety Failures and Systemic Oversight, Report number: FRMsynt 12/24Affiliation: Cardiff University, DOI: 10.13140/RG.2.2.33966.63046 https://www.researchgate.net/publication/386503508_The_Paradox_of_PFD's_The_Buncefield_Disaster_A_Case_Study_in_Safety_Failures_and_Systemic_Oversight
4. Bayes, T., & Price, R. (1763). An Essay Towards Solving a Problem in the Doctrine of Chances. Philosophical Transactions of the Royal Society of London, 53, 370–418. https://doi.org/10.1098/rstl.1763.0053
5. Hollnagel, E. (2012). FRAM: The Functional Resonance Analysis Method – Modelling Complex Socio-technical Systems. Ashgate Publishing.
6. CCPS/EI (Centre for Chemical Process Safety / Energy Institute). (2014). Standardisation of Bow Tie Methodology and Terminology via a CCPS/EI Book. IChemE. Retrieved from (https://www.icheme.org/media/15543/poster-09.pdf)
7. Hollnagel, E., Hill, R., and Slater, D., (2923) The FRAM model Visualiser (FMV)-The Web Version, DOI: 10.13140/RG.2.2.23719.32162 (https://www.researchgate.net/publication/372591806_The_FRAM_model_Visualiser_FMV-The_Web_Version)
8. Hollnagel, E. and Slater, D, (2022) A FRAM HANDBOOK (https://www.researchgate.net/publication/364959115_A_FRAM_HANDBOOK)

9. Slater, D., (2024) STPA -A Stairway to FRAM: Enhancing Complex System Modeling, (https://www.researchgate.net/publication/384925927_STPA_-A_Stairway_to_FRAM_Enhancing_Complex_System_Modeling)
10. Slater, D. and Hill, R. (2024), Building Nonlinear, Systemic Bow Ties, Using Functional Barriers, DOI: 10.20944/preprints202406.1433.v1 (https://www.researchgate.net/publication/381583186_Building_nonlinear_systemic_Bow_Ties_using_Functional_Barriers)
11. Slater, D. (2022) FRAM Model Validation (https://www.researchgate.net/publication/360627678_FRAM_Model_Validation)
12. Hill, R. and Slater, D., (2024) Using a Metadata Approach to Extend the Functional Resonance Analysis Method to Model Quantitatively, Emergent Behaviours in Complex Systems, Systems 12(3) DOI: 10.3390/systems12030090 (https://www.researchgate.net/publication/378877076_Using_a_Metadata_Approach_to_Extend_the_Functional_Resonance_Analysis_Method_to_Model_Quantitatively_Emergent_Behaviours_in_Complex_Systems)
13. Hill, R. and Slater, D., (2024) HOW TO USE THE METADATA FACILITY IN FRAM, Report number: FRMsynt 9/24, Report number: FRMsynt 9/24, DOI: 10.13140/RG.2.2.31512.81924 (https://www.researchgate.net/publication/384763526_HOW_TO_USE_THE_METADATA_FACILITY_IN_FRAM)
14. Slater, D., Hill, R., Ale, B.J.M., Hollnagel, E. (2024) THE PROBABILISTIC INTERPRETATION OF EMERGING BEHAVIOURS IN COMPLEX ADAPTIVE SYSTEMS USING FRAM, Conference: FRAMily2024, Lund DOI: 10.13140/RG.2.2.20540.24964 (www.researchgate.net/publication/381183852_THE_PROBABILISTIC_INTERPRETATION_OF_EMERGING_BEHAVIOURS_IN_COMPLEX_ADAPTIVE_SYSTEMS_USING_FRAM)
15. Box, G. E. P., & Draper, N. R. (1987). Empirical Model-Building and Response Surfaces. John Wiley & Sons, p. 424.

APPENDIX A. AN EXAMPLE APPLICATION –

THE BHOPAL DISASTER,

also known as the **Bhopal gas tragedy**, was one of the world's worst industrial accidents. It occurred on the night of **December 2–3, 1984**, in Bhopal, Madhya Pradesh, India, at a pesticide plant owned by Union Carbide India Limited (UCIL), a subsidiary of the American company Union Carbide Corporation (UCC).

Overview of the Incident

A highly toxic gas, **methyl isocyanate (MIC)**, leaked from the plant. The gas spread over densely populated areas around the factory, exposing over half a million people to the lethal chemical. The immediate effects were devastating. The **Bhopal disaster** occurred due to **barrier failures**.

The **Bow Tie approach** effectively highlights where these barriers were intended to function and where they ultimately failed, offering critical lessons for industries handling hazardous chemicals.

ANALYSIS

First, the Bow Tie method was used to visualize pathways leading to hazardous events and the barriers in place to prevent or mitigate those events. In the case of the Bhopal disaster, applying a Bow Tie analysis helps clarify the preventive and mitigative barriers designed to ensure the plant's safe operation, as well as the failures that led to the catastrophic gas release. This Bow tie was then used to build the FRAM equivalent below (Figure 1) for the Bhopal plant, using the Bow Tie / FRAM Methodology described above.

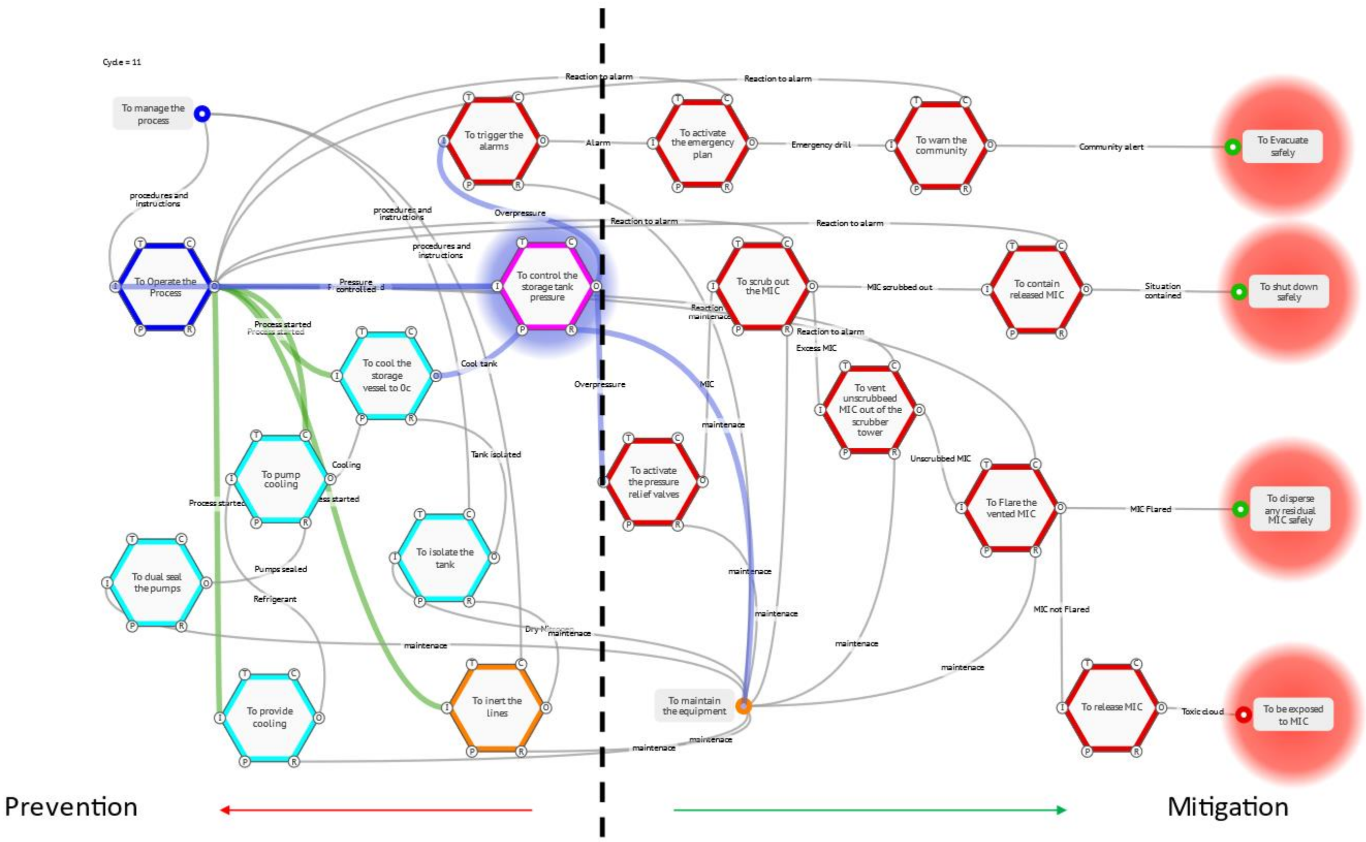


Fig. 1. – The FRAM built "Bow Tie" model of the safety barriers designed for the Bhopal Sevin plant.

THE PFD'S USED IN THE METADATA

Estimating the **Probability of Failure on Demand (PFD)** for safety barriers involves analyzing their reliability under both ideal and actual operating conditions. In the context of the **Bhopal disaster**, we can assess the PFD for each barrier based on available data and reported operational practices.

1. Tank Isolation Procedures

- **Ideal Conditions:** Properly implemented isolation procedures, including the use of slip-blind plates and closed valves during maintenance, are highly reliable. Assuming regular training and adherence to protocols, the PFD could be estimated at **0.01** (1% chance of failure).
- **Bhopal Conditions:** Reports indicate that slip-blind plates were not installed during maintenance, and isolation procedures were inadequate PFD **= 1?** This negligence likely increased the PFD to approximately **0.5** (50% chance of failure).

2. Transfer Pumps

- **Ideal conditions**
- **Bhopal Conditions**

3. Refrigeration System

- **Ideal Conditions:** A functioning refrigeration system maintaining MIC at recommended temperatures would have a low PFD, around **0.1** (10% chance of failure).
- **Bhopal Conditions:** The refrigeration system was shut down to save costs, leading to MIC being stored at higher temperatures. This operational decision effectively rendered the barrier non-existent, resulting in a PFD of **1.0** (100% chance of failure).

4. High-Temperature Alarms

- **Ideal Conditions:** Operational high-temperature alarms alert operators to unsafe conditions, with a PFD of about **0.1**.
- **Bhopal Conditions:** Alarms were disabled due to frequent triggering from elevated. This disabling increased the PFD to **1.0**.

5. Nitrogen Blanket System

- **Ideal Conditions:** A nitrogen blanket prevents corrosion and contamination, with a PFD around **0.05**.
- **Bhopal Conditions:** The nitrogen system was compromised due to cost-cutting measures, leading to corrosion and potential contamination. This likely raised the PFD to **0.5**.

6. Dual Pump Seals

- **Ideal Conditions:** Dual seals reduce leakage risk, with a PFD near **0.05**.
- **Bhopal Conditions:** Maintenance issues and the use of inappropriate materials led to frequent seal failures. This could have increased the PFD to **0.3**.

7. Pressure relief valves

- **Ideal-**
- **Bhopal**

8 Vent Gas Scrubber

- **Ideal Conditions:** An operational scrubber neutralizes toxic gases, with a PFD of **0.1**.
- **Bhopal Conditions:** The scrubber was non-functional during the incident, resulting in a PFD of **1.0**.

9. Flare Tower

- **Ideal Conditions:** A flare tower burns off hazardous gases, with a PFD of **0.1**.
- **Bhopal Conditions:** The flare tower was out of service, leading to a PFD of **1.0**.

8. ESD

- The Bhopal plant **did not have a single "panic button"** or an emergency switch that could shut down the entire plant safely in the event of a crisis. PFD of **1.0**

9. Water Spray Systems

- **Ideal Conditions:** Effective water sprays can mitigate gas releases, with a PFD of **0.2**.
- **Bhopal Conditions:** The system was inadequately maintained and ineffective, increasing the PFD to **0.9**.

10. Emergency Response Plan

- **Ideal Conditions:** A well-prepared plan minimizes impact, with a PFD of **0.2**.
- **Bhopal Conditions:** Lack of proper planning and community awareness likely raised the PFD to **0.8**.

11. Community Notification System

- **Ideal Conditions:** Effective systems alert the public promptly, with a PFD of **0.1**
- **Bhopal Conditions:** No such system was in place, resulting in a PFD of **1.0**

Note: These PFD values are estimations based on available information and standard industry practices. Actual values would require detailed quantitative risk assessments.

- **Ideal conditions –** Barriers in place with "normal" probabilities of performance.
- **Bhopal Conditions:** With vital barriers not in place, resulting in PFD's of **1.0**.

In ideal conditions, the combined PFD of these barriers would be low, indicating high reliability However, at Bhopal, due to systemic failures, cost-cutting, and poor maintenance, the PFDs were significantly higher, leading to the catastrophic failure of safety systems.

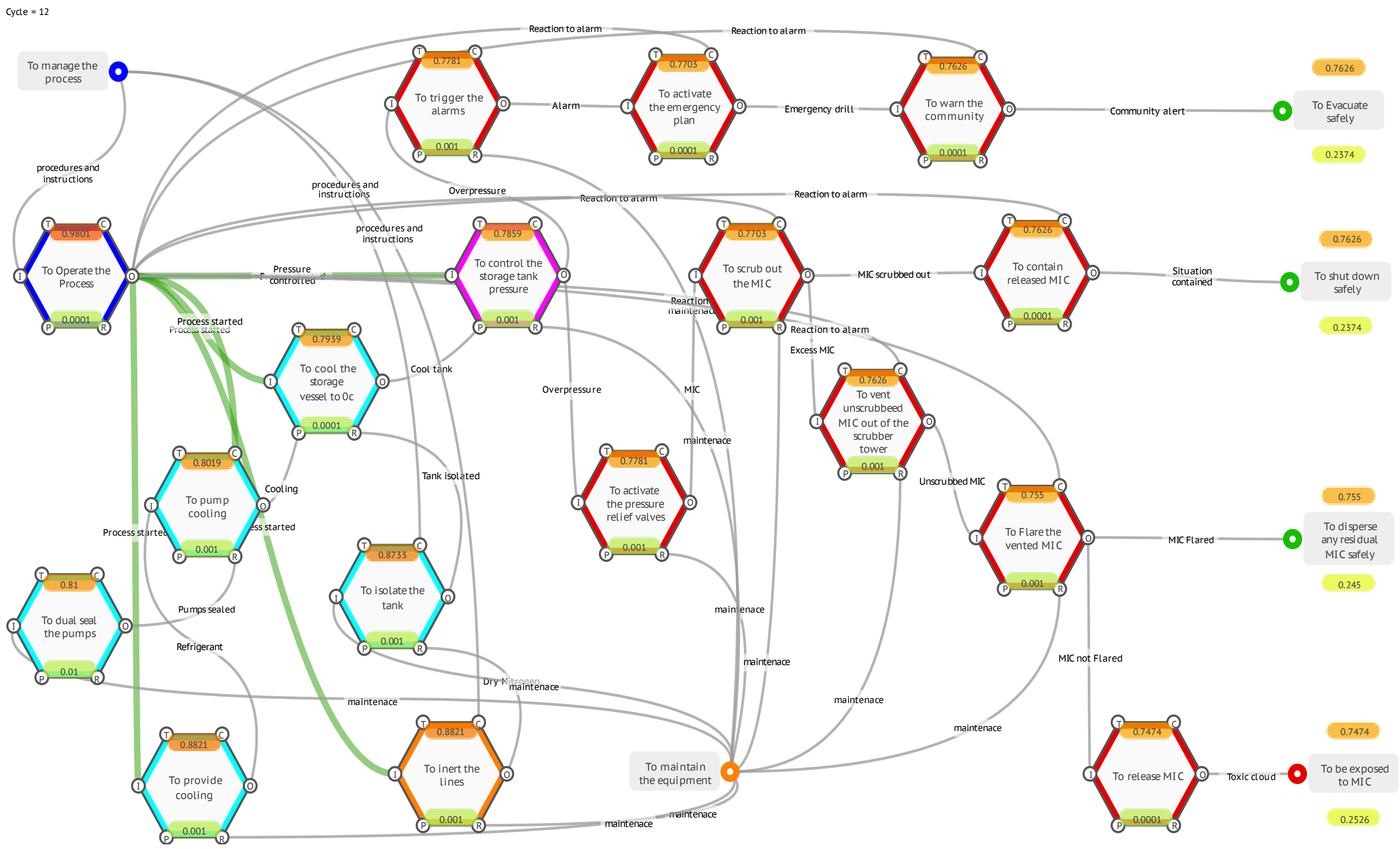
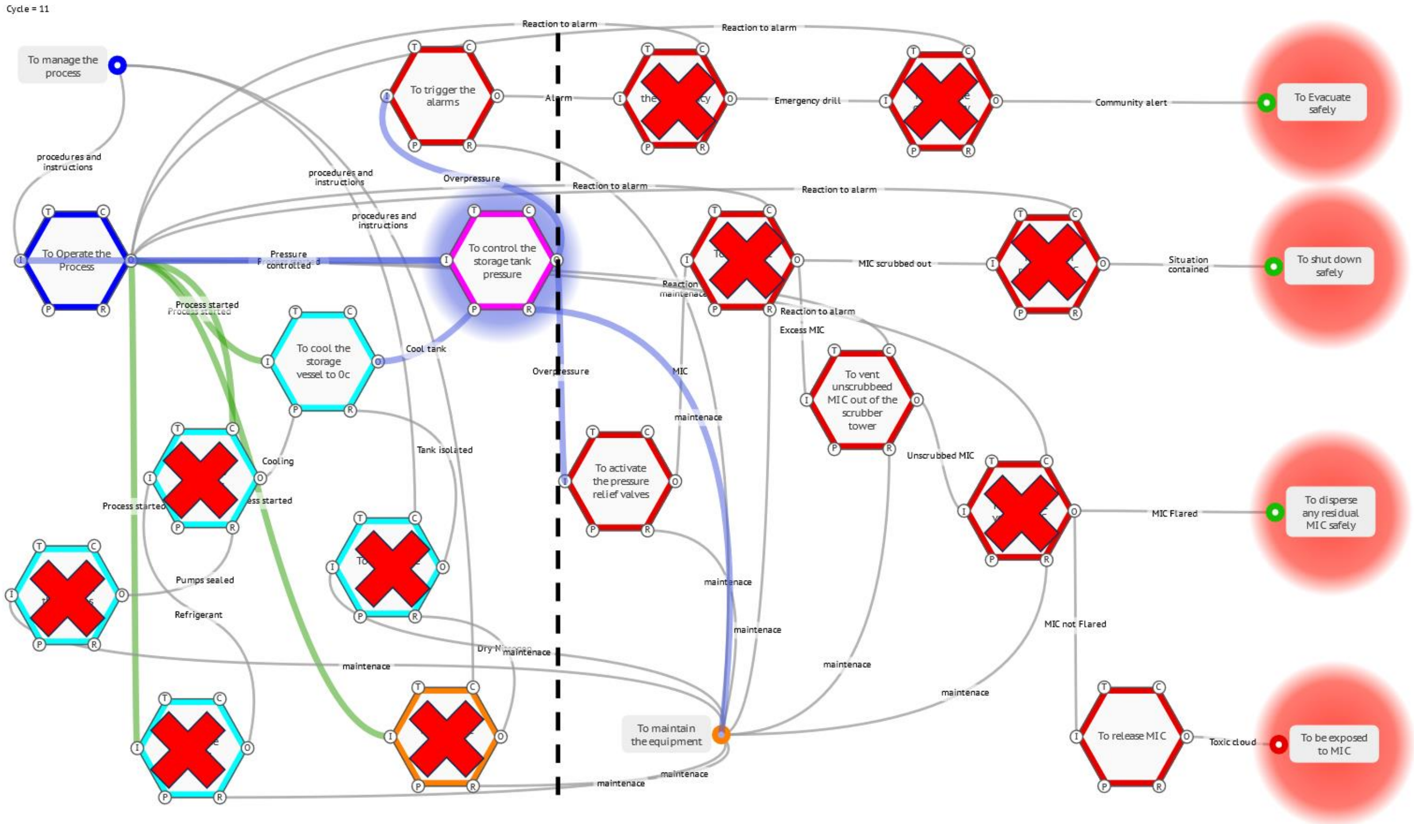


Fig. 2. – The "as designed" performance probabilities of the safety barriers at Bhopal

But “as done” at Bhopal many of these barriers were missing



And the calculated probabilities of failure for Bhopal conditions become certain-

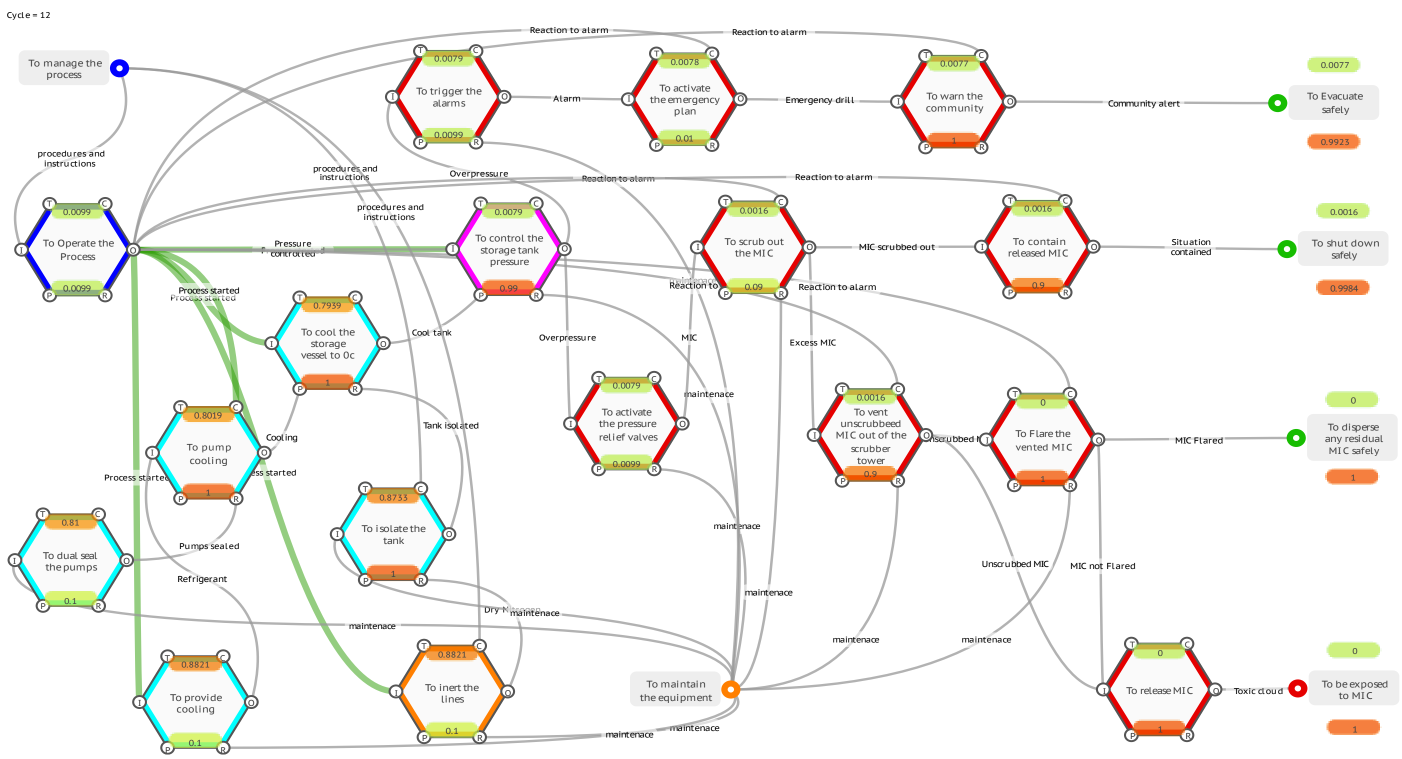


Fig. 3 – Calculated probabilities of failure for the Bhopal conditions

From this we can calculate the tabulated probabilities for Bhopal conditions-

Table 1 – The calculated probabilities of Failure on demand (Pfail) and overall expected failure (Pfd) and success (Pso) for the Bhopal situation.

IDNr	IDName	Pfun	Pfail	Psd	Pfd	Pir	Pic
0	To Operate the Process	0.99	0.010000000000000009	0.0099	0.00990000000000001		
1	To cool the storage vessel to 0c	0.99	1	0.7938810000000001	1		
2	To pump cooling	0.99	1	0.8019000000000001	1		
3	To control the storage tank pressure	0.01	0.99	0.007938810000000001	0.99		
4	To isolate the tank	0.99	1	0.8732691	1		
5	To inert the lines	0.99	1	0.88209	0.09999999999999998		
6	To dual seal the pumps	0.9	1	0.81	0.09999999999999998		
7	To provide cooling	0.99	1	0.88209	0.09999999999999998		
8	To trigger the alarms	0.99	0.010000000000000009	0.007859421900000002	0.00990000000000001		
9	To activate the pressure relief valves	0.99	0.010000000000000009	0.007859421900000002	0.00990000000000001		
10	To maintain the equipment	0.9	0.09999999999999998	0.9	0.09999999999999998		
11	To scrub out the MIC	0.2	0.8	0.0015718843800000004	0.07999999999999999		
12	To Flare the vented MIC	0.99	1	0	1		
14	To vent unscrubbeed MIC out of the scrubber tower	0.99	1	0.0015561655362000004	0.8		
15	To disperse any residual MIC safely			0	1		
16	To shut down safely			0.0015561655362000004	0.9984438344638		
17	To contain released MIC	0.99	1	0.0015561655362000004	0.8		
18	To activate the emergency plan	0.99	1	0.007780827681000002	0.010000000000000009		
19	To warn the community	0.99	1	0.007703019404190002	1		0
20	To Evacuate safely			0.007703019404190002	0.99229698059581		
21	To release MIC	0.99	1	0	1		
22	To prevent exposure to MIC			0	1		
23	To manage the process	0.9	0.09999999999999998				

Conclusion

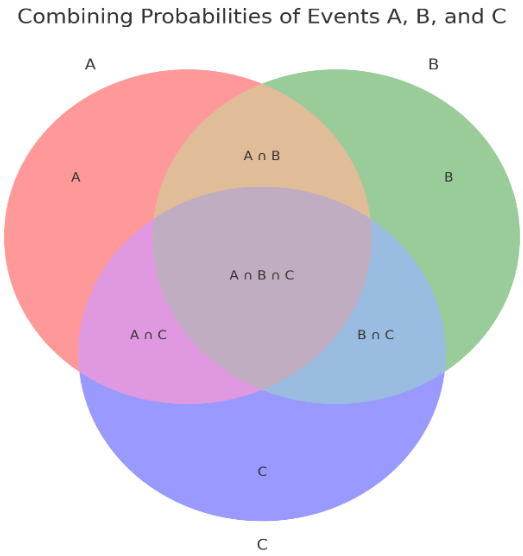
The **Bhopal disaster** occurred due to a **cascade of barrier failures**. The preventive barriers (e.g., refrigeration, nitrogen blanketing, proper maintenance) were either disabled, poorly maintained, or bypassed due to operational decisions. The mitigative barriers (e.g., vent gas scrubber, flare tower, emergency response) also failed to function when needed. This **systemic breakdown** underscores the importance of maintaining **robust safety culture**, rigorous adherence to **process safety management (PSM)**, and continuous evaluation of both **preventive and mitigative controls** to prevent similar tragedies.

The **Bow Tie approach** effectively highlights where these barriers were intended to function and where they ultimately failed, offering critical lessons for industries handling hazardous chemicals.

Adding the FRAM analysis enables the interactions and interdependencies to be tracked and the local effect of these interactions on the propagation of the failure to be highlighted.

But it is clear that without any analysis, that the plant could not be run safely with all these barriers missing. Once there was a large ingress of water the process was doomed to fail to contain the released MIC.

Appendix B – The LOPA approach - Independent probabilities



This Venn diagram represents the probabilities of events A, B, and C and their combinations.

1. $P(A \cup B)$: The probability of A or B occurring is:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

2. $P(A \cup B \cup C)$: To include a third event C, the combined probability is:

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

- $P(A)$, $P(B)$, and $P(C)$ represent the probabilities of each individual event.
- $P(A \cap B)$, $P(A \cap C)$, and $P(B \cap C)$ represent the probabilities of two events occurring together.
- $P(A \cap B \cap C)$ accounts for the probability that all three events happen simultaneously.

The diagram visually shows how these regions overlap, making it easier to understand which parts to include or subtract when calculating combined probabilities.

In the Layers of Protection Analysis (LOPA) a risk assessment technique used to estimate the probability of a hazardous event occurring by sequentially considering independent layers (or barriers) of protection. Each layer reduces the likelihood of failure, and by multiplying these probabilities of failure on demand (PFD), we can quantify the overall effectiveness of 1, 2, or 3 barriers.

1. **Single Barrier (1 Layer of Protection):**
   - If we have one protective barrier with a probability of failure on demand (PFD) denoted as $P(A)$, the effectiveness of this single layer is:
   $$P_{\text{Failure}} = P(A)$$
   - The probability that the system *does not fail* is $1 - P(A)$.
2. **Two Barriers (2 Layers of Protection):**
   - If two independent barriers A and B are in place, each with PFDs of $P(A)$ and $P(B)$, the combined probability of both barriers failing is:
   $$P_{\text{Failure}} = P(A) \times P(B)$$
   - The effectiveness improves because both barriers need to fail for the hazard to occur.
3. **Three Barriers (3 Layers of Protection):**
   - When three independent barriers A, B, and C are present, each with PFDs $P(A)$, $P(B)$, and $P(C)$, the overall probability of all three barriers failing is:
   $$P_{\text{Failure}} = P(A) \times P(B) \times P(C)$$
   - This significantly reduces the likelihood of failure because all three barriers must fail simultaneously for the hazardous event to occur.

Suppose the probabilities of failure on demand for three barriers are:

- **Barrier 1:** $P(A) = 0.1$ (10% chance of failure)
- **Barrier 2:** $P(B) = 0.05$ (5% chance of failure)
- **Barrier 3:** $P(C) = 0.02$ (2% chance of failure)

Effectiveness of Each Scenario:

1. **One Barrier:**
   $P_{\text{Failure}} = 0.1$ (10%)
2. **Two Barriers:**
   $P_{\text{Failure}} = 0.1 \times 0.05 = 0.005$ (0.5%)
3. **Three Barriers:**
   $P_{\text{Failure}} = 0.1 \times 0.05 \times 0.02 = 0.0001$ (0.01%)

Each additional layer of protection dramatically reduces the probability of failure. In practice, these layers can represent safety instruments, physical containment systems, or human intervention. LOPA helps ensure that the risk of failure is reduced to an acceptable level by quantifying the cumulative effectiveness of these barriers through sequential multiplication of PFDs.

In the Venn diagram, the regions where events overlap (intersections) illustrate where multiple events occur together. In LOPA, the multiplication of probabilities can be thought of as isolating those regions where **all the independent barriers fail** — analogous to the innermost intersection where all events occur simultaneously. However, in LOPA, this is simplified by assuming independence, which eliminates the need for inclusion-exclusion adjustments.

For dependent probabilities we can use a **Bayesian Approach.** And to calculate the combination of probabilities using **Bayes' Theorem**, we need to frame the problem in terms of **conditional probabilities**. Bayes' Theorem helps us update the probability of an event based on new evidence, and it can be particularly useful when events are **dependent** or when we want to understand how one event influences the likelihood of another.

Bayes′ Theorem Formula

For two events A and B, Bayes′ Theorem states:

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

Where:

- $P(A \mid B)$ is the **posterior probability**: the probability of A given that B has occurred.
- $P(B \mid A)$ is the **likelihood**: the probability of B given that A has occurred.
- $P(A)$ is the **prior probability** of A.
- $P(B)$ is the total probability of B.

Imagine you have three barriers (A, B, and C) that are designed to prevent a hazardous event. We want to calculate the probability that all three barriers fail, but we'll explore two cases:

1. **Independent Barriers**: The failures of A, B, and C are independent.
2. **Dependent Barriers**: The failure of one barrier increases the likelihood that another barrier fails.

Let's use the following probabilities:

- $P(A)$: Probability that Barrier A fails = 0.1 (10%)
- $P(B)$: Probability that Barrier B fails = 0.05 (5%)
- $P(C)$: Probability that Barrier C fails = 0.02 (2%)

For the **dependent case**, let's assume:

- $P(B \mid A)$: Probability that B fails given that A has failed = 0.2 (20%)
- $P(C \mid A \cap B)$: Probability that C fails given that A and B have both failed = 0.5 (50%)

For **independent Barriers (LOPA)**

The same probability that all barriers fail was simply = 0.1 x 0.05 x 0.02 = 0.0001

This means there is a **0.01%** chance that all three independent barriers fail. (on demand)

Comparison of Results

Scenario	Probability of All Three Failures
Independent Barriers	0.0001 (0.01%)
Dependent Barriers	0.01 (1%)

In the Context of FRAM

If we have a FRAM system model of interacting functions (say barriers), we can estimate the probability of a single successfully executing depending on the probabilities of its Aspects. (the probabilities of successful operation of upstream function.)

In a FRAM model, each function's execution depends on the successful provision of its aspects. By quantifying the probability of failure for each upstream function and propagating these probabilities, you can better understand the overall variability and potential points of failure in the system. This approach enhances the ability to anticipate and mitigate risks, ultimately improving system resilience.

Scenario:

Consider a FRAM system model where a function F (e.g., "Activate Safety Barrier") depends on the following upstream functions:

1. **Function A**: "Sensor Detects Hazard"
   Probability of success: $P(A) = 0.9$ (90%)
2. **Function B**: "Control System Processes Signal"
   Probability of success: $P(B) = 0.8$ (80%)
3. **Function C**: "Power Supply Available"
   Probability of success: $P(C) = 0.95$ (95%)

Case 1: Independent Functions

Assume A, B, and C are independent. The probability that F executes successfully is:

$$P(F) = P(A) \times P(B) \times P(C)$$

Substitute the values:

$$P(F) = 0.9 \times 0.8 \times 0.95 = 0.684$$

This means there is a **68.4% chance** that F ("Activate Safety Barrier") will execute successfully.

Case 2: Dependent Functions (Using Conditional Probabilities)

Suppose the success of B depends on A, and C depends on both A and B. Let's assign:

- $P(B \mid A) = 0.85$: Probability that B succeeds given A succeeds.
- $P(C \mid A \cap B) = 0.9$: Probability that C succeeds given both A and B succeed.

To find $P(F)$ (probability that F succeeds), we use:

$$P(F) = P(A) \times P(B \mid A) \times P(C \mid A \cap B)$$

Substitute the values:

$$P(F) = 0.9 \times 0.85 \times 0.9 = 0.6885$$

This means there is a **68.85% chance** that F will execute successfully when the upstream functions are dependent.

Probability of Failure

1. **Independent Case**:

$$P(F^c) = 1 - P(F) = 1 - 0.684 = 0.316$$

   The probability that the function (barrier) fails is **31.6%**.

2. **Dependent Case**:

$$P(F^c) = 1 - P(F) = 1 - 0.6885 = 0.3115$$

   The probability that the function (barrier) fails is **31.15%**.

So, for our initial analysis we can use the LOPA independent PFD's but use the FRAM method to link those aspects that the function is dependent on and use their probability of failure to calculate the resulting probability of failure. As the difference is marginal (0.4%).

We can then therefore also **propagate the probability of failure on demand** to calculate the probability of failure of a **downstream function** in a FRAM model. This is particularly useful when modeling the dependencies between functions and understanding how failures in upstream functions affect downstream outcomes.