applied sciences

MDPI

Article

Development of Maximum-Vulnerability Diagrams for Barrier-Based Safety Systems: Quantifying and Visualizing Operational Risk Exposure

Numa Pompilio Torres Moneo [1,2,3,*], Anselmo César Soto Pérez [2,4,*], Ricardo Díaz Martín [5] and Francisco Javier Pérez Trujillo [1]

[1] Departamento de Ingeniería Química y de Materiales, Facultad de Ciencias Químicas, Universidad Complutense de Madrid, Pl. de las Ciencias, 2, Moncloa-Aravaca, 28040 Madrid, Spain; fjperez@ucm.es
[2] Facultad de Ciencias de la Empresa y la Tecnología, Universidad a Distancia de Madrid (UDIMA), Carretera de La Coruña, KM.38,500, Vía de Servicio, nº 15, Collado Villalba, 28400 Madrid, Spain
[3] Escuela de Caminos, Canales y Puertos, Universidad Politécnica de Madrid (UPM), Calle del Profesor Aranguren 3, 28040 Madrid, Spain
[4] Escuela de Ingeniería, Arquitectura y Diseño, Universidad Alfonso X el Sabio (UAX), Avenida de la Universidad, 1, Villanueva de la Cañada, 28691 Madrid, Spain
[5] Catedrático Ingeniería Química, Universidad CEU Fernando III, Glorieta Ángel Herrera Oria s/n, Bormujos, 41930 Sevilla, Spain; ricadima@ceu.es
* Correspondence: numapomt@ucm.es or nptmoneo@gmail.com (N.P.T.M.); asotoper@uax.es or anselmocesar.soto@udima.es (A.C.S.P.)

Abstract

Barrier-based safety systems are fundamental to preventing accidents in high-hazard industrial operations. However, traditional Hazard Identification (HAZID) and risk screening frameworks aggregate safety safeguards at a macro-hazard level, creating a systemic blind spot that masks threat-specific vulnerabilities and single points of failure. To address this gap, this study develops 'Maximum-Vulnerability Diagrams' (MVD), a network-based modeling approach that maps and quantifies threat–barrier pathways using matrix algebra and conditional probability. Validated across empirical cases of working-at-height (H-06.01) and heavy rotary equipment (H-08.01) operations in the oil extraction industry, the MVD successfully isolates high-criticality, zero-redundancy pathways. We mathematically establish that multiplexed defenses require a target individual efficiency of $\eta \geq 95\%$ to reliably suppress system failure probability below a strict 5% operational threshold. The findings demonstrate that aggregate safeguard volume is a deceptive safety metric, and that systemic resilience depends entirely on network architecture. This framework transitions risk governance from passive compliance checking to predictive, threat-driven barrier management, offering an actionable methodology to optimize safety resources before accidents occur.

Keywords: risk management; vulnerability; HAZID; preventive barriers; ISO 31000; OSHA; efficiency; effectiveness

Academic Editor: Arkadiusz Gola

Received: 31 July 2026
Revised: 29 August 2026
Accepted: 31 August 2026
Published: 5 September 2026

1. Introduction

Barrier-based safety systems constitute a foundational paradigm for accident prevention within complex sociotechnical and industrial operations. Within this framework, systemic resilience depends not merely on static hazard identification, but on the spatial distribution, functional combination, and operational maintenance of safety barriers across technical, organizational, and human domains. However, the nominal presence

of these controls does not inherently guarantee robust protection, particularly if the functional compatibility between specific threats, initiating events, and barrier typologies remains unquantified.

Industrial disasters seldom stem from isolated component failures; instead, they emerge from the systemic alignment of latent conditions that breach the system's defensive architecture [1–4]. Despite the consensus surrounding this systemic paradigm, conventional risk assessment methodologies predominantly aggregate barriers at a macro-hazard level. This coarse granularity frequently obscures critical vulnerabilities residing at the micro-level of threat–initiating-event trajectories. Consequently, systems characterized by satisfactory aggregate risk profiles may still harbor highly vulnerable pathways defined by insufficient redundancy or a disproportionate reliance on human reliability.

The core engineering problem addressed by this study is the structural decoupling between hazard screening and threat-barrier paths in conventional risk assessment. Standard HAZID studies compile safety barriers in flat inventories under broad hazard categories. This macro-level aggregation creates a critical masking effect: a hazard node may appear highly protected due to a high aggregate safeguard count, while a specific, high-criticality threat-initiating event trajectory remains entirely uninsulated or relies on a single, highly vulnerable administrative control. The MVD framework is developed to resolve this decoupling by modeling and visualizing the discrete threat-initiating event topology.

Standard risk screening tools, such as Hazard Identification (HAZID) and Bow-Tie analysis, establish structured, qualitative taxonomies linking hazards, threats, top events, and consequences. While effective for baseline risk documentation, these qualitative frameworks exhibit significant limitations when capturing the dynamic, topographical vulnerability of complex barrier networks. Specifically, they fail to systematically differentiate whether a critical threat–initiating-event pathway is secured by orthogonal, independent protection layers or by a single, highly sensitive barrier whose degradation exponentially amplifies systemic risk exposure.

Within the context of barrier-based architecture, operational vulnerability is formally conceptualized as the conditional probability that an accident pathway remains active due to topological deficiencies, poor control placement, or correlated technical and human failure modes. Quantifying this vulnerability necessitates a transition from superficial barrier counting to a mathematically rigorous evaluation of barrier typologies, functional network dependencies, and structural safety margins. To address the limitations of conventional hazard screening tools—which fail to identify localized, threat-specific vulnerabilities masked by aggregate safeguard counts—this study develops the Maximum-Vulnerability Diagram (MVD) framework. By coupling matrix algebra with conditional probability trees, the MVD framework maps the discrete threat-trigger topology to systematically isolate zero-redundancy pathways and shared common-cause barriers before they manifest as active failures.

The primary academic and practical contributions of this research are threefold:

- **Methodological Coupling:** We establish a formal mathematical matrix formulation, B_{Hk}, that directly links discrete threat-trigger lines to safety-critical elements, eliminating the masking effect inherent in macro-level hazard assessments.
- **Socio-Technical Integration:** We model human-centric conditional dependencies within consecutive administrative barrier sequences, demonstrating how occupational fatigue and routine bias collapse theoretical defense-in-depth redundancy into stochastically coupled Single Points of Failure POF.
- **Empirical Validation:** We validate the diagnostic utility of the framework by retrospectively analyzing and optimizing complex, multi-causal safety envelopes within

high-risk industrial environments, specifically working-at-height operations H-06.01 and mobile/rotary equipment deployment H-08.01.

The remainder of this manuscript is organized as follows:

- **Section 2** provides a critical literature review and comparative assessment of safety barrier modeling methodologies.
- **Section 3** defines the methodological foundations of socio-technical barrier typologies and risk factors.
- **Section 4** presents the mathematical modeling and matrix formulation of the Path of Opportunity Probability PPO.
- **Section 5** demonstrates the practical engineering application and optimization of the MVD framework across two industrial case studies, followed by a retrospective validation against historical operational logs.
- Finally, **Section 6** summarizes our core conclusions and outlines future research directions.

2. Literature Review and Comparative Assessment

To establish the theoretical and methodological positioning of the proposed Maximum-Vulnerability Diagrams (MVD), this section reviews eight foundational publications and regulatory frameworks within safety barrier science, analyzing their core methodologies, modeling boundaries, and analytical gaps.

The engineering of safety barriers has historically progressed from prescriptive physical containment to semi-quantitative socio-technical systems. Sklet [5] established a comprehensive ontological taxonomy of safety barriers, classifying them into physical, technical, and organizational layers, and defining core performance requirements. While Sklet's taxonomy provides a standardized structural classification, it remains a static categorization that lacks a mathematical framework to model dependent failure modes or the functional coupling that occurs when safeguards are multiplexed across concurrent threats. In parallel, industrial guidance frameworks such as the Center for Chemical Process Safety (CCPS) [6] and the ISO 17776 standard [7] have formalized the operational management of independent protection layers (IPLs) for major accident hazards. These standards are highly effective for baseline compliance auditing and risk screening during the conceptual design of facilities. However, they evaluate barrier availability as an unconditioned, independent parameter and fail to address how the degradation of a single administrative control can propagate common-cause vulnerabilities across separate process systems.

To model accident propagation and barrier degradation over time, several causation frameworks have been proposed. Reason [1–4] introduced the Swiss Cheese Model (SCM), which conceptualizes systemic accidents as the temporal alignment of active sharp-end failures and latent blunt-end organizational pathogens. Although the SCM is a powerful forensic tool for retrospective accident reconstruction, its predictive engineering utility is limited by its qualitative nature and its problematic assumption of stochastic independence between defensive slices. Similarly, Svenson [8,9] developed the Accident Evolution and Barrier Function (AEB) model, which maps the sequential interaction between technical systems and human actions, modeling how barrier failures accelerate the accident path. While the AEB model excels at visualizing sequential human–machine interactions, it relies on a linear event chain that struggles to capture the complex, multi-layered topologies of high-density industrial networks. To address the operational management of these barriers, Hale et al. [10,11] focused on the workplace factors and organizational conditions that determine barrier integrity. This research highlights the influence of safety culture and management supervision on barrier hardiness, yet it does not formalize these socio-technical interactions into a parameterized mathematical formulation suitable for structural network optimization.

At the systemic and socio-technical level, research has shifted toward modeling safety as an emergent property. Perrow [12] formulated Normal Accident Theory, establishing that high-integrity systems characterized by high interactive complexity and tight coupling are intrinsically prone to systemic failures, regardless of safeguard volume. Perrow's work serves as a critical warning against over-relying on redundant administrative layers, but it remains a qualitative paradigm that does not offer a quantitative diagnostic tool for engineers. To operationalize these systemic interactions, Hollnagel [13] developed functional resonance models and formalized barrier quality vectors. Hollnagel's framework successfully captures the non-linear variability of socio-technical systems; however, its qualitative complexity and high data requirements often limit its practical application during early-stage industrial risk screening.

The proposed Maximum-Vulnerability Diagram (MVD) framework bridges these analytical gaps. By coupling matrix algebra with conditional probability trees, the MVD models the discrete threat–initiating-event topology directly, without the intensive computational overhead of full process simulations or the linear limitations of classical models. This methodology systematically isolates stochastically coupled common-cause barriers (Single Points of Failure) and models cognitive dependencies in administrative clusters. To intuitively clarify these differences, see Table 1 for a comparative matrix of safety barrier modeling methodologies and the proposed MVD framework, which presents a comparative matrix of these eight foundational works against our proposed framework across five primary analytical parameters.

Table 1. Comparative matrix of safety barrier modeling methodologies and the proposed MVD framework.

Methodology/ Reference	Hazard Granularity and Mapping	Barrier Typology Classification	Mathematical Coupling and Dependent Failures	Human Factor and Cognitive Integration	Analytical and Operational Lifecycle Phase
Sklet (2006) [5]	Macro-Hazard level (aggregates safeguards under broad hazard categories)	Detailed operational taxonomies (Physical, Technical, Organizational)	Strictly qualitative; lacks mathematical formulation for barrier dependencies or network coupling	High; explicitly models procedural and organizational safeguards	Conceptual Design and Operational phases
Reason (1997) [2]	Macro-Hazard level (systemic defensive slices)	Conceptual dichotomy (Active sharp-end failures and Latent blunt-end conditions)	Assumes stochastic independence; simplifies joint probability via basic linear product rules	High; focuses heavily on organizational pathogens and human error precursors	Retrospective Forensic Auditing
Hollnagel (2004) [13]	Systemic and Emergent performance levels	Ontological classification (Material, Functional, Symbolic, Incorporeal)	High; modeled via functional resonance networks (non-linear systemic variability propagation)	Very High; models cognitive adaptability, performance variability, and sharp-end execution	Operational phase (dynamic, real-time safety-state screening)
Svenson (1991, 2001) [8,9]	Event sequence/scenario level	AEB (Accident Evolution and Barrier) taxonomy (Technical & Human barriers)	Flow-based dependencies along scenario branches	Medium; models operator interventions and execution barriers	Post-incident analysis and operational screening
Hale et al. (2004) [11]	Workplace/Scenario level	Material, administrative, and organizational controls	Focuses on barrier management systems and administrative audits	High; emphasizes safety-critical task behaviors and supervisory barriers	Design-stage barrier validation and audit review
CCPS (2018) [6]	Process node/Threat-to-consequence pathway	Independent Protection Layers (IPLs) (active, passive, administrative)	Non-linear CCF and Layer of Protection Analysis (LOPA) rules	Medium; administrative barriers evaluated with standardized unreliability bounds	Detailed Engineering and Quantitative LOPA reviews
ISO 17776 [7]	Process system/Major accident event	Functional barrier classifications (technical safety elements, administrative plans)	Multi-layered defense barriers without explicit stochastic coupling	Medium; procedural compliance and manual safety-critical tasks	Design-basis safety case and operational validation

Table 1. *Cont.*

Methodology/ Reference	Hazard Granularity and Mapping	Barrier Typology Classification	Mathematical Coupling and Dependent Failures	Human Factor and Cognitive Integration	Analytical and Operational Lifecycle Phase
Perrow (1984) [12]	Macro-Systemic/Plant level	Structural and procedural safeguards	Focuses on complex interactions and tight coupling (interactive complexity)	High; analyzes cognitive load under catastrophic emergent states	Strategic design and system-wide vulnerability audits
Proposed MVD Framework	Highly Granular (Explicit Threat-Trigger Intersections)	Comprehensive Ontological (Material, Functional, Symbolic, Incorporeal) coupled with a Socio-Technical Proximity Axis (Blunt-to-Sharp End)	High; utilizes matrix algebra (B_{Hk}), conditional probability trees, and systematic Single Points of Failure (SPOF) isolation	High; models cognitive error, task sequence deviations, and fatigue coupling in consecutive administrative/incorporeal barriers	From Conceptual Design to Live Operational Auditing (Streamlined, threat-driven HAZID modification)

3. Methodological Foundations and Development of the Maxi-Mum-Vulnerability Framework

To construct a mathematically tractable vulnerability model, this section establishes the methodological foundations of the Maximum-Vulnerability Diagram (MVD) framework. Rather than detailing generic corporate risk management steps or standard iterative loops, our system safety design relies on formulating a non-linear assessment of barrier efficacy. Within safety engineering, hazards represent latent energy or material sources whose loss of containment triggers an accident sequence. The risk associated with these nodes is characterized by a multi-attribute consequence vector $C = [C_P, C_A, C_R, C_E]$, representing impacts on People (health and physical integrity), Assets (material and economic damage), Reputation (corporate image erosion), and Environment (ecological disruption). The terminal consequence rating is governed by the max-operator:

$$C_{final} = \max(C_P, C_A, C_R, C_E) \quad (1)$$

Equation (1) dictates that a protective safeguard attenuating a single consequence attribute leaves the remaining vector components invariant. This structural asymmetry demands a strict mathematical separation between preventive barriers—which operate globally on the probability space to suppress top-event activation—and mitigative/recovery barriers, which act locally on specific consequence attributes post-loss of containment. This functional bifurcation forms the basis of our structural mapping matrix, ensuring safety-critical elements are allocated based on discrete threat-barrier pairings rather than aggregate, flat safeguard inventories.

3.1. Semi-Quantitative Risk Analysis

Semi-quantitative risk assessment methodologies bridge the gap between qualitative heuristics and rigorous numerical data, facilitating the evaluation of diverse hazard profiles under systemic data scarcity—a condition endemic to complex operational environments. The primary semi-quantitative hazard identification techniques and their underlying operational characteristics are summarized in Table 2 [14].

During the preliminary engineering and conceptual design phases of industrial assets, Hazard Identification (HAZID) serves as the primary screening tool. Developing from mid-twentieth-century process industry practices, HAZID offers a systemic screening mechanism when detailed piping and instrumentation diagrams (P&IDs) are unavailable, rendering high-fidelity techniques like Hazard and Operability (HAZOP) studies premature.

Table 2. Comparative matrix of semi-quantitative hazard analysis techniques. (Source: Adapted from ISO 31010 [14].

Category	Hazard Analysis Technique		
	HAZID	**What-If?**	**HAZOP**
What is the objective of the Risk Analysis?	Identify the potential hazards associated with an operation in a facility in the early stages of design and document the hazards for further in a HAZOP	Review the probability of the consequences and existing safety barriers associated with a specific scenario for a future hazard related to facility design and operation	Identify and review potential hazards and operating problems associated with a facility operation
When should I conduct a Risk Analysis?	Early stages of a process or equipment design	It could be adequate in early or late stages of process or equipment design	Before completing the detailed process design
Advantages	Helps reduce the costs related to late design changes. It considers numerous potential scenarios	Efficient technique in time that can be used to focus on high-severity consequence scenarios	Well-structured and comprehensive technic of analysis Process Hazards
Disadvantages	Reduces the level of detail of individual scenarios	Requires a previous list of causal scenarios, where some relevant scenarios could be omitted	Intensive approach in time, which requires detailed information of the process design

The HAZID mechanics involve isolating discrete hazard sources, mapping the initiating events that precipitate energy or material release, identifying precursor threats, and delineating downstream consequences. Each hazardous node is decoupled and evaluated based on an ordinal likelihood-consequence pair to derive an indexing risk value, guided by the normative taxonomies of ISO 17776 [7]. Execution typically relies on multidisciplinary expert panels utilizing structured brainstorming to isolate relevant hazards, define **top events**, and establish **proactive threat controls** alongside reactive **mitigation measures**.

Following scenario identification, likelihood and consequence metrics are mapped onto a two-dimensional risk matrix. The operational evaluation parameters are formalized as follows.

- **Likelihood (P):** Parameterized via discretized annual frequencies of occurrence.
- **Consequence (C):** Modeled across a multi-attribute vector $C = [C_P, C_A, C_R, C_E]$, representing impacts on **People** (health and physical integrity), **Asset**/**Property** (material and economic damage), **Reputation** (corporate image erosion), and **Environment** (ecological disruption).

The terminal consequence rating is governed by the max-operator as shown in Equation (1).

Both values are usually mapped on a two dimensional matrix which provide values to the Likelihood and Consequence and the combination of all the possible values as shown on the Figure 1.

Consequently, a mitigation barrier that attenuates a single attribute leaves the remaining vector components invariant, requiring a strict, non-linear assessment of barrier efficacy.

While HAZID provides an accelerated, visual prioritization framework to optimize risk-allocation decisions, its aggregate nature introduces vulnerability masking at lower operational tiers.

Probabilistic Modeling of Initiating Events

Each discrete hazard is mapped to a conditional probability distribution governing top-event generation. Under classical semi-quantitative assumptions, the cumulative systemic frequency is modeled linearly across the hazard inventory. Quantifying this probability requires deconstructing localized process deviations that act as initiating triggers, mapping them directly to the underlying threat vectors identified within the HAZID taxonomy.

Figure 1. Structural architecture of a standard semi-quantitative risk matrix correlating likelihood intervals and multi-attribute consequence severities (Source: Adapted from ISO 31010 [14].

The Bow-Tie diagram (Figure 2) provides a dual-sided topological representation of the accident sequence, explicitly separating pre-event prevention layers from post-event mitigation layers.

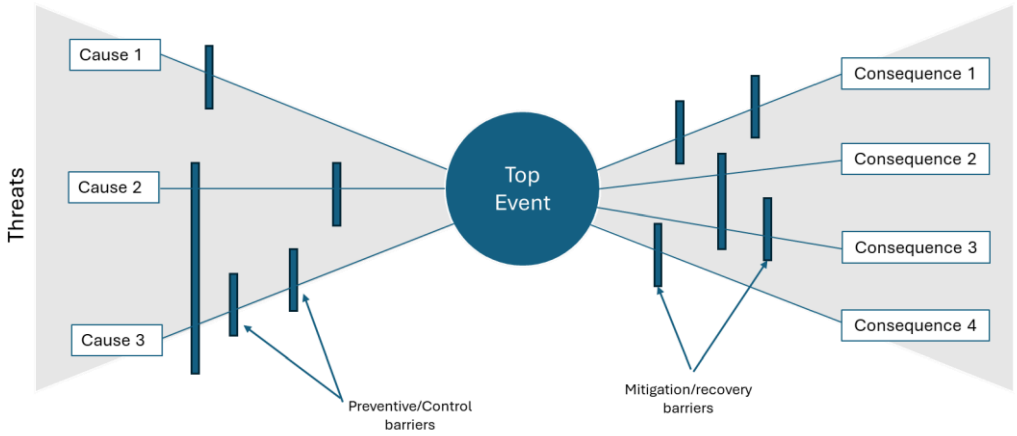

Figure 2. Bow-Tie topological model mapping threat-to-consequence pathways via independent protection layers. Adapted from ISO 31010 [14].

Within this layout, the continuous variable of likelihood is discretized into standardized, order-of-magnitude frequency intervals dictated by corporate safety performance standards, as exemplified in Table 3:

As illustrated by this categorization, likelihood selection is highly dependent on the subjective bounding of the postulated accident scenario. This structural dependency introduces substantial epistemic bias, as it evaluates protection layers against generic hazards rather than isolating the explicit, threat-specific pathways where barrier vulnerabilities actually reside.

Table 3. Discretized likelihood intervals and corresponding order-of-magnitude annual frequencies. (Source: Author's elaboration based on Industry Safety Management Systems).

Likelihood Level	Descriptor	Annual Frequency (1/Year)	Operational Interpretation
L1	Rare/Very Unlikely	$p < 10^{-4}$	Unprecedented; beyond standard design-basis limits.
L2	Unlikely/Infrequent	$10^{-4} \leq p < 10^{-3}$	Possible but highly exceptional within asset lifetime.
L3	Possible/Moderate	$10^{-3} \leq p < 10^{-2}$	Sporadic occurrence reported across industry peers.
L4	Likely/Frequent	$10^{-2} \leq p < 10^{-1}$	Multi-annual occurrence expected at least once per asset.
L5	Almost Certain	$p \geq 10^{-1}$	Recurring operational deviation; expected annually.

3.2. Development of a HAZID

The execution of a Hazard Identification (HAZID) study relies on multidisciplinary expert panels conducting structured, qualitative brainstorming sessions. Within this framework, hazards are systematically isolated, independent protection layers (IPLs) are allocated, and a discrete risk rank is determined by cross-referencing two primary operational metrics: frequency of occurrence and consequence severity. Allocated barriers are functionally bifurcated into preventive controls, engineered to suppress top-event frequencies, and mitigative safety functions, designed to attenuate downstream consequence energy.

The analytical sequence initiates with the characterization of the hazard source. Subsequently, the initiating event—analogous to the Top Event in a Bow-Tie topology—is postulated, and precursor threat vectors are mapped alongside their corresponding preventive barrier assignments. The sequence concludes by delineating the credible consequence pathways derived from the unmitigated top event. In general terms, this sequence follows the process shown on the Figure 3.

Figure 3. Methodological workflow of a conventional Hazard Identification (HAZID) process. (Source: Adapted from ISO 31010 [14]).

The primary systemic challenge of the HAZID methodology resides in the epistemic uncertainty governing likelihood estimations and the subjective allocation of barrier performance metrics. Under the defense-in-depth paradigm, while reactive mitigation controls remain vital for asset survivability, the risk-reduction strategy rigorously prioritizes preventative barriers to minimize top-event activation probabilities.

Methodological Deficiencies in Conventional HAZID

- Scenario Plausibility Distortion:

The inclusion of non-credible or unbounded accident scenarios introduces significant skewness into semi-quantitative risk evaluations. Postulating extreme, beyond-design-basis external events characterized by negligible frequencies can force the allocation of economically unviable or redundant protection layers, compromising project feasibility. Conversely, over-emphasizing high-frequency, low-consequence operational anomalies artificially inflates the aggregate risk index. To eliminate these distortions, hazard identification must be bound by normative criteria, utilizing the standardized taxonomies outlined in ISO 17776 to validate scenario credibility.

- **Topological Incompatibility of Variables:**

While a hazard defines the latent potential for harm, conventional frameworks fail to mathematically reconcile the distinct mappings between the set of precursor threats T = {t1, t2, . . ., ta} and the set of initiating top events E = {e1, e2, . . ., eb}.

If the functional coupling between T and E is poorly defined, the corresponding set of safety barriers B is incorrectly mapped, creating a non-surjective relation where critical threat pathways remain uninsulated, introducing latent vulnerabilities into the system architecture.

The structural layout presented in Figure 4 underlines the fragmentation endemic to conventional HAZID studies, where threat vectors and independent protection layers are cataloged as isolated textual entities without evaluating their mathematical or physical compatibility. This uncoupled approach introduces structural inconsistencies: preventative controls are frequently allocated without being linked to a specific, quantified initiating event, obscuring inter-barrier functional dependencies. Furthermore, evaluating likelihood as a monolithic, unconditioned parameter—while simultaneously segregating consequences across a multi-attribute vector—creates an analytical disconnect, making it impossible to verify if individual high-sensitivity threats are genuinely secured by independent lines of defense.

CODE	HAZARD	ACTIVITY AREA/LOCATION	TOP EVENT	THREATS	THREAT CONTROLS	CONSEQUENCES	RECOVERY MEASURES
H.01 HYDROCARBONS							
H 01.06.1	Hydrocarbon Gas	Wellpad	Spontaneous gas release	1. Loss of the barriers integrity, 2. Valve failure, 3. PCE failure and 4. H2S gas.	1. Biweekly Pressure and leaks monitoring 2. Daily visual inspection (bubbles checking) 3. Pressure gauge calibration 4. Corrosion studies was performed 5. Certified H2S Enginer is in place (Pandu personnel will be onsite during project execution) 6. Include fire training in the Training Matrix. 7. Ensure cage is locked all the times. 8. Ensure ER Team are avaialbe onsite at all times.	1. Loss of life, 2. fire/explosion, 3. Environmental damage, 4. Loss of well, 5. poor reputation, and 6. H2S release.	1. Ensure BOCP is approved and communicated. 2. Ensure OSCP is approved and communicated. 3. Ensure emergency response plan in place and communicate. 4. Ensure H2S contigency plan and preparedness ready at well site. 5. Ensure medical evacuation plan is approved and in place. 6. Ensure to perform emergency drills as per schedule. 7. Ensure equipment used is H2S rated and in the adequate location 8. Explosion proof equipment to be requested for Zone One. 9. Gas detectors in place 10. Wind sock
H.01.06.2	Hydrocarbon Gas	Wellpad	Loss of control of heavy equipment resulting in a damage of barriers, loss of containment and gas release	1. Hit by heavy equipment, or 2. Load falling on the Wellhead	1. Pre-tour meeting to be held prior to commencement of the work 2. Job Safety Analysis in place to ensure proper risk awareness including not to work over the wellhead 3. Cage in place and area 5 m away the cage marked as Hazardous area zone 1. In case working inside PTW is a must! 4. Operators and riggers competence is based on Migas requirement. 5. Dedicated flagger to guid every heavy equipment movement inside the wellpad. 6. DDC & SIMPER for drivers 7. Lifting plan in place	1. Loss of life, 2. fire/explosion, 3. Environmental damage, 4. Loss of well, 5. poor reputation, and 6. H2S release.	1. Ensure BOCP is approved and communicated. 2. Ensure OSCP is approved and communicated. 3. Ensure emergency response plan in place and communicate. 4. Ensure H2S contigency plan and preparedness ready at well site. 5. Ensure medical evacuation plan is approved and in place. 6. Ensure to perform emergency drills as per schedule. 7. Ensure equipment used is H2S rated and in the adequate location 8. Gas detector inplace

Figure 4. Methodological extract of a standard process HAZID highlighting decoupled hazard-barrier mappings. (Source: author's elaboration extracted from a real HAZID).

Dual-Phase Risk Characterization: Inherent and Residual Paradigms

Industrial risk assessment protocols routinely bifurcate risk characterization into a dual-phase iterative framework to isolate the efficacy of incremental safety investments:

- Baseline Risk Evaluation (Design-Basis Inherent Risk):

This phase quantifies the system's risk profile by accounting strictly for intrinsic design-basis barriers and established asset safeguards. The resulting metric defines the baseline exposure threshold prior to the synthesis of supplementary operational risk-reduction measures.

- Iterative Risk Optimization (Residual Risk Continuum):

Following baseline quantification, a secondary evaluation incorporates newly proposed, supplementary independent protection layers (IPLs) designed to drive the risk profile into a contractually acceptable or As Low As Reasonably Practicable (ALARP) zone. These supplementary barriers are functionally divided into:

- Preventive barriers: preventive safety functions that structurally depress the frequency vector of top-event activation.
- Mitigative barriers: mitigative safety functions engineered to absorb kinetic or chemical energy, thereby attenuating terminal consequence vectors.

The optimization and allocation of these risk-mitigation resources (additional barriers) are mathematically guided by the baseline risk frontier, concentrating risk-reduction strategies onto high-sensitivity hazardous nodes.

To optimize reactive protection, the multi-attribute consequence space is discretized across the previously defined vector components:

- people CP
- assets CA
- environment CE
- reputation CR

This vector decomposition enables targeted mitigation alignment, tailoring reactive barriers to suppress the specific vector component exhibiting the maximum severity eigenvalue, max{C}. Conversely, preventive barriers exhibit an asymmetric decoupling from these localized dimensions; because their functional mandate is the complete interruption of the precursor threat trajectory, they operate globally on the probability space, suppressing the top-event frequency uniformly across all potential downstream consequence domains.

4. Mathematical Modeling and Stochastic Formulation of Path of Opportunity

4.1. The Epistemology of Failure

The historical paradigm of industrial safety relies heavily on reactive accident analysis, focusing on isolating and eliminating root causes. However, restricting forensic investigations exclusively to human or technical errors enforces a reductive, linear cause-effect schema that obscures the underlying systemic conditions facilitating failure [13,15]. This mechanistic bias limits the discovery of latent organizational vulnerabilities and attenuates the diagnostic utility of risk assessments.

Traditionally, reactive post-incident investigations focus on isolating active failures or immediate sharp-end triggers to prevent recurrences. In contrast, systemic safety engineering prioritizes the proactive identification and control of latent organizational vulnerabilities (blunt-end pathogens) and the continuous pressure-testing of safety barrier integrity before an initiating event can materialize. Yet, these proximate causes seldom operate in isolation; they inherently concur with complex networks of latent contributing factors [13]. Consequently, contemporary safety science dictates that investigations shift from assigning localized blame to characterizing the systemic conditions that parameterize the accident space, establishing holistic control mechanisms.

To contextualize this analytical evolution, Hollnagel [13,15] taxonomizes accident causation into three generation models:

- **Sequential–Linear Paradigm**

This model conceptualizes accidents as a deterministic chain of discrete events propagating in series. While it simplifies causality by assuming that breaking a single link prevents the terminal event, it fails to account for non-linear interactions among concurrent system variables.

- **Epidemiological Paradigm**

Advancing beyond strict linearity, this framework analogizes accident propagation to pathogenesis [16]. It introduces multi-dimensional interactions involving operational performance deviations, hostile environmental vectors, and latent organizational pathogens [2]. Within this architecture, latent conditions act as structural vulnerabilities that, when aligned with active barrier failures, trigger an incident. Although highly effective for modeling defense-in-depth degradation, its core mechanics remain fundamentally sequential.

- **Systemic Paradigm**

Grounded in Normal Accident Theory [12], this model conceptualizes accidents as emergent properties of complex socio-technical systems rather than the arithmetic summation of component failures. Under this view, operational performance variability propagates and amplifies across system nodes, inducing thermodynamic or functional instability. Reflecting chaotic system behavior, minor fluctuations in boundary conditions can yield non-linear, catastrophic consequences [17,18]. This perspective replaces deterministic root-cause tracing with the dynamic analysis of system topologies that lower the thermodynamic threshold for top-event activation.

Within systemic frameworks, failure emerges from the continuous cross-layer friction between organizational strata. This topology is illustrated via the Sharp-End/Blunt-End construct [13] in the Figure 5. Here, upstream administrative and strategic echelons (the Blunt End, encompassing policies, resource allocation, and cultural frameworks) shape and condition the operational constraints, resource limitations, and error-producing environments encountered by frontline operators at the physical interface of risk (the Sharp End).

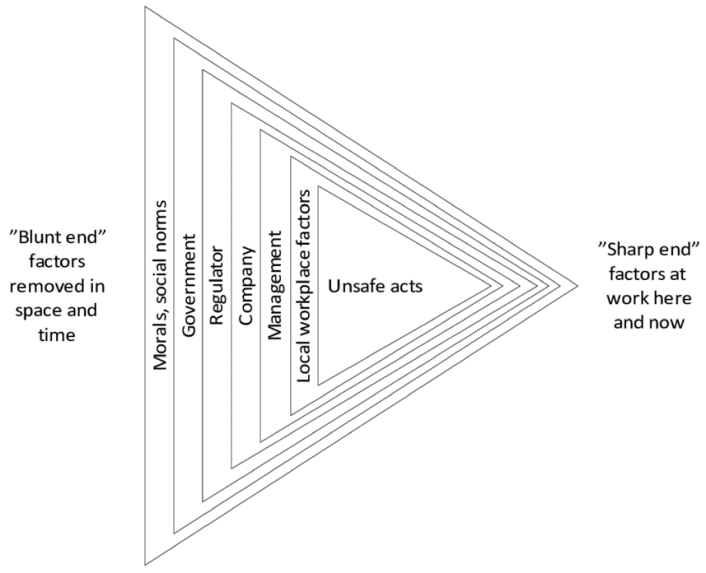

Figure 5. The Sharp-End/Blunt-End socio-technical continuum governing operational safety. This model illustrates the hierarchical propagation of risk from blunt-end strategic and organizational echelons—where corporate policies, capital allocation, and structural standardizations are established—down to the sharp-end execution point. It demonstrates how latent organizational pathogens filter down through workplace factors, creating error-promoting environments that manifest as active human performance deviations or technical faults at the physical risk interface. Within the MVD framework, mapping this continuum is essential to identify when a safety-critical barrier sequence is dangerously concentrated at the sharp end, leaving the system highly sensitive to frontline cognitive fluctuations [13,19].

Historically, safety metrics have favored high-consequence events, as major disruptions politically justify the capital allocation required for comprehensive forensic audits. Conversely, near-misses—defined as localized system deviations initiated by an active anomaly but truncated by rapid, resilient recovery vectors—provide empirical data regarding the real-time efficacy of active protection layers [20]. Developing algorithmic and operational architectures capable of monitoring, detecting, and logging these high-frequency, low-consequence signals enhance systemic diagnostic accuracy and strengthen proactive resilience before catastrophic alignment occurs.

A critical epistemological error in safety engineering is the conflation of chronological temporality with deterministic causality. This heuristic bias assumes that because events unfold sequentially, they obey a neat, linear trajectory—fostering the flawed expectation that disrupting a single historical link guarantees future accident prevention [13]. In reality, systemic failures mature non-linearly over temporal horizons via the progressive accumulation of necessary and sufficient conditions, manifesting as subtle deviations in node performance. These unmitigated deviations accumulate, steadily shifting the system state toward the critical threshold of hazard release.

Consequently, accident causation is more accurately modeled as a dynamic stochastic process of escalating probability, where disparate operational vectors converge to activate the top event. To counter this convergence, proactive defense-in-depth strategies must be dual-pronged:

- **Variance Suppression:** Minimizing the initiation of node performance deviations through high-fidelity, robust engineering controls at the Blunt End.
- **Propagation Interruption:** Dynamic capturing of active deviations via adaptive, independent protection layers (**effective barriers**) that isolate and attenuate anomalies before they propagate to the critical threat-initiating event boundary.

Transitioning to this systemic layout enables predictive risk optimization, ensuring operational envelope stability and structural resilience under dynamic boundary conditions.

4.2. Safety Barrier Topologies: Functional and Operational Architectures

Within safety engineering, a barrier is formally defined as an independent physical, technical, or organizational entity designed to interrupt the event-state space propagation along a critical accident trajectory. Functionally, barriers operate as structural constraints that suppress the kinetic, chemical, or thermodynamic potential of a hazard.

This operational mandate establishes a fundamental binary classification:

- **Preventive barriers.** Upstream controls engineered to reduce the conditional probability of top-event activation (PTE$\rightarrow$0).
- **Mitigative barriers.** Downstream protection layers optimized to attenuate the magnitude of the consequence vector (C) once containment or systemic control is lost.

Beyond their functional objectives, barriers are categorized by their activation energy and thermodynamic state into active and passive paradigms. This taxonomical distinction determines their respective time-dependent degradation distributions:

- **Active barriers:** These require a sequence of state transformations—encompassing detection, logic processing, and mechanical actuation—to execute their safety function. For instance, a Safety Instrumented System (SIS) comprising an automated pressure transmitter, a logic solver, and an emergency shutdown valve (ESD) constitutes a technical active barrier. The operational reliability of active systems is mathematically governed by their Probability of Failure on Demand (PFD), which is sensitive to human–machine interaction errors, instrumentation drift, and testing intervals.

- **Passive barriers:** These require no external energy input, informational signals, or human intervention to perform their function, relying strictly on structural and material integrity. A classic example is a reinforced concrete bund wall providing secondary containment around a hydrocarbon storage asset. While passive structures exhibit lower vulnerability to real-time operational volatility, their long-term efficacy degrades through unmonitored structural aging, chemical corrosion, or mechanical wear.

This categorization and sequence of barrier failure and accident occurrence is shown in the Figure 6.

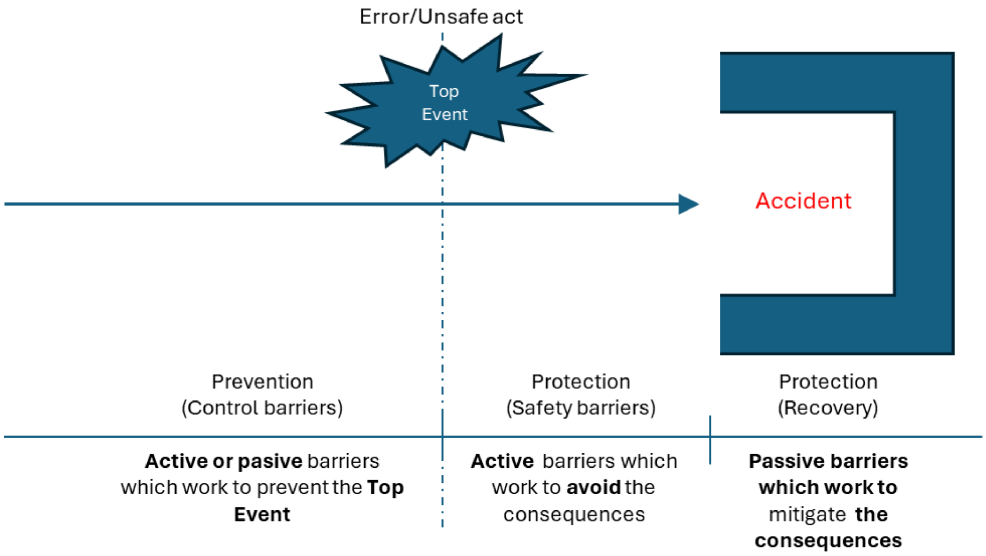

Figure 6. Topological matrix mapping safety barriers across functional (preventive/mitigative) and operational (active/passive) coordinates relative to the top event boundary. This classification matrices safety safeguards into preventive (probability-suppressive) and mitigative (consequence-attenuating) functional layers relative to the top event boundary. The arrow represents the sequence of events of barrier failure until the accident occurs. It further categorizes barriers by their operational activation requirements into active systems (requiring continuous sensor-logic-actuator state transformations) and passive systems (relying strictly on structural and material integrity), each governed by distinct time-dependent degradation distributions and failure modes. Isolating these coordinates allows process safety engineers to ensure that the defensive architecture contains a balanced mix of autonomous technical controls and robust physical containments, minimizing the system's susceptibility to common-cause failures. Adapted from Hollnagel [13,15]. Consequently, isolating these architectural profiles is essential for parameterizing the real-time reliability vector of the overall asset defense system.

To refine this topological analysis, Hollnagel [13,15] distinguishes between the barrier function and the barrier system.

- **Barrier function.** The explicit thermodynamic or operational purpose that disrupts the causal transition between adjacent states in an accident sequence (e.g., 'contain fluid pressure').
- **Barrier system.** The socio-technical infrastructure required to sustain that function over its life cycle. This encompasses physical hardware, automated control loops, administrative procedures, and organizational competency frameworks [13,15].

Failing to maintain this multi-layered infrastructure induces a latent degradation of the barrier function, causing the barrier to fail when demanded by an escalating operational anomaly.

4.2.1. Ontological Taxonomies: Physical, Functional, Symbolic, and Administrative Layers

To operationalize the defense-in-depth framework, safety barriers must be classified within a rigorous ontological taxonomy that maps their origin, functional objective, spatial location, and thermodynamic nature. Drawing on foundational socio-technical system literature [13,15], barriers are categorized by their material characteristics and interaction mechanics into four structural domains:

- **Physical Barrier Systems:**

These embody passive structural controls engineered to physically impede material or energy transport, either suppressing hazard release or attenuating downstream propagation. Standard engineering configurations include blast-resistant bulkheads, pressure vessels, and double-walled containment structures. Their reliability envelope is independent of real-time cognitive inputs, requiring human intervention strictly for lifecycle asset integrity inspections and maintenance.

- **Functional Barrier Systems:**

These establish logical, mechanical, or electrical interlocks that condition system state transitions to prevent hazard activation. Examples encompass mechanical lockout devices, overpressure trip loops, and In-Vehicle Monitoring Systems (IVMS) executing automated algorithmic velocity damping. Unlike passive barriers, their effectiveness relies on the execution of an active control sequence or logical constraint.

- **Symbolic Barrier Systems:**

These introduce informational constraints, such as visual semiotics, acoustic alarms, and standardized safety pictograms. Because they do not physically restrict the energy path, their failure probability is intrinsically coupled to the cognitive compliance, situational awareness, and real-time interpretation of the human agents within the operational field.

- **Incorporeal Barrier System:** Administrative and Intangible:

These constitute the procedural architecture of the organization, encompassing Standard Operating Procedures (SOPs), Job Safety Analyses (JSAs), permit-to-work systems, and competency validation frameworks. As non-physical constraints, their reliability profiles are highly sensitive to organizational culture, human behavior variability, and execution fidelity.

For the primary analytical modeling executed in this research, these topologies are aggregated into a baseline binary system governed by their ultimate functional mandate:

- Preventive layers optimized for probability reduction.
- Protective/mitigative layers designed for consequence attenuation.

This foundational classification acts as the input vector for our mathematical framework, which subsequently derives an optimized barrier distribution matrix to maximize systemic resilience.

Multicriteria Evaluation of Barrier Integrity: Quality Matrices and Degradation Vectors

To systematically quantify the operational readiness of an independent protection layer (IPL), its structural profile is evaluated against a multicriteria framework established by Hollnagel [13,15]. This framework discretizes barrier performance into targeted operational vectors:

- **Effectiveness:** The deterministic capability of the barrier to interrupt a specific accident sequence under peak demand conditions.
- **Resource required:** The socio-technical capital investment and lifecycle expenditures required for implementation.

- **Hardiness:** The resistance of the barrier to physical, environmental, or operational degradation over temporal horizons.
- **Implementation time:** The temporal span separating conceptual system design from verified site commissioning.
- **Applicable to a safety critical task:** The functional alignment of the barrier within highly regulated, high-consequence process envelopes.
- **Availability:** The continuous operational probability that the safety function is active and compliant when an unexpected demand occurs.
- **Assessment:** The qualitative or quantitative simplicity associated with testing, auditing, and validating performance metrics.
- **Human Dependency (During Operation):**hese require no external energy inp The degree of real-time human intervention, administrative compliance, or cognitive processing required to execute the safety function.

Focusing on the human dependency vector, contemporary process automation aims to suppress manual intervention by deploying high-integrity autonomous technical systems. However, when a socio-technical system drifts into beyond-design-basis accident (BDBA) regimes or encounters unpostulated emergent anomalies, automated algorithmic architectures reach their epistemic boundaries (Table 4). Under these conditions, the adaptive capacity and cognitive resilience of human agents remain indispensable. Consequently, achieving absolute automation across complex barrier networks is mathematically and operationally unviable, highlighting the necessity of integrating Human Factors Engineering (HFE) into industrial risk architectures.

Table 4. Multicriteria framework for safety barrier quality quantification [13,15].

Vector\Type of Barrier	Material	Functional	Symbolic	Incorporeal
Effectiveness	High	High	Medium	Low
Resources required	Medium—High	Low—Medium	Low—Medium	Low
Hardiness	Medium—High	Medium—High	Low—Medium	Low
Implementation time	Long	Medium—Long	Medium	Short
Applicable to a safety-critical task	Low	Medium—High	Low (Not final conclusion)	Low
Availability	High	Low—High	High	Uncertain
Assessment	Easy	Hard	Hard	Hard
Human dependency (During operation)	N/A	Low	High	High

This formalized evaluation methodology establishes a mathematical basis for optimizing risk-reduction strategies. By cross-referencing these operational parameters, asset managers can execute capital-allocation strategies under strict resource constraints, prioritizing maintenance and testing resources toward high-impact protection layers.

Barrier Failure Mechanics and Vulnerability Susceptibility

A robust defense-in-depth model cannot treat barriers as binary, perpetually infallible constraints; it must explicitly integrate their underlying failure modes [13,15]. These degradation pathways are classified into two primary vectors:

- **Systemic and Structural Failures:** Encompassing random hardware faults, software exceptions, material degradation, and latent organizational defects that compromise the barrier infrastructure.
- **Active Human Failures:** Characterized by execution slips, cognitive lapses, or flawed situational interpretations at the physical interface of risk.

Empirically, catastrophic system breaches seldom result from an isolated failure mode; instead, they are precipitated by the non-linear convergence of technical faults and cognitive errors, which systematically erode adjacent protection layers.

Methodological Fragmentation in Industrial Practice

Although evaluating multi-dimensional barrier quality vectors is theoretically vital for lifecycle optimization, a significant decoupling exists between academic safety science and industrial practice. In standard risk engineering, these quality classifications are rarely incorporated into daily operations due to the static, text-based nature of conventional risk registers. Instead, barrier allocation follows a rigid, resource-intensive approach where the density of defense-in-depth layers is determined solely by the gross energy or chemical inventory of the node. High-risk, high-pressure processes dictate exhaustive, continuous thermodynamic analyses such as Hazard and Operability (HAZOP) studies, whereas utility loops or lower-consequence areas default to basic qualitative screening tools like HAZID. This creates a crude proportionality where financial resources dictate robustness, leaving complex, highly sensitive threat pathways vulnerable to unmonitored common-cause failures (CCF).

Advanced Barrier Failure Mechanics: Susceptibility Matrices and Socio-Technical Degradation

To mathematically bound the reliability envelope of independent protection layers (IPLs), the functional taxonomy must integrate structural failure modes with their corresponding operational susceptibility profiles. As formalized by Hollnagel [13,15], preventing systemic accident propagation requires combining the deterministic concept of a safety barrier with its discrete failure modes. Identifying these discrete operational boundaries transitions risk governance from reactive forensic auditing to predictive stochastic modeling, categorizing system degradation into two primary failure vectors:

- **Systemic and Structural Pathologies:** Characterized by random hardware faults, software exceptions, material wear, or latent organizational deficiencies that degrade the barrier infrastructure.
- **Cognitive and Actuation Deviations:** Characterized by failures in human information processing, real-time diagnostic misinterpretations, or flawed operational decision-making at the physical interface of risk.

Empirically, catastrophic system breaches are seldom precipitated by an isolated failure vector; instead, they emerge from the non-linear convergence of technical faults and cognitive errors that systematically erode adjacent protection layers (Table 5).

Table 5. Phenomenological categorization of safety barrier failure modes classified by cognitive and technical agency [13,15].

Type of Failure	System Failure Mode	Human Failure Mode
Activation time	A position/location reached too soon or too late. Equipment not activated at the required moment	An action which starts early or late
Duration	A function which is performed during a short period of time or during much time	An action which is conducted for too long or too short
Distance/Length	An object which is transported too close or too far. An object which is very small or very big	A system which is moved very close or very far
Speed	A system moving very fast or very slow. Equipment not responding as it should	An action which is conducted very slow or very fast
Direction	A system moving in the wrong direction	An action or movement in the wrong direction
Force/Energy/Pressure	A system or component applying much or little force or adding little or much energy or pressure	An action which is applied with more or less force
Magnitude	The measure or extent of the movement is excessive or is not enough	Measure or extent of a movement or an action which is excessive or not enough
Object	Function moving towards the wrong object	Action carried out at the wrong object
Sequence	Two or more functions performed in the wrong order	Two or more actions performed in the wrong order
Quantity and volume	System or object whose content is too much or too few or it is too light or too heavy	Not applicable

Mathematical Intersection of Quality Elements and Susceptibility Vectors

To model this interaction, the quality profile of a barrier system is conceptualized as a multi-attribute set spanning the operational parameters defined in Section 3.2. Concurrently, its failure susceptibility is characterized through a discrete evaluation framework where each parameter quantifies the conditional probability of a specific failure mode compromising a corresponding quality attribute (Table 6). The ultimate systemic vulnerability impact is derived by structurally coupling this quality profile with the susceptibility values. This analytical cross-referencing effectively isolates the precise socio-technical nodes where specific failure modes exert maximum degradation on critical safety functions.

Table 6. Susceptibility matrix **S** mapping structural barrier typologies against discrete failure mode distributions [13,15].

Type of Failure	Barrier system			
	Material	**Functional**	**Symbolic**	**Incorporeal**
Activation time	N/A	High	Medium	Medium
Duration	N/A	High	Low	N/A
Distance/Length	High	High	N/A	N/A
Speed	N/A	High	High	N/A
Direction	High	High	Medium	N/A
Force/Energy/Pressure	Medium	High	N/A	N/A
Magnitude	Medium	High	N/A	N/A
Object	High	Medium	Low	Medium
Sequence	N/A	High	High	High
Quantity and volume	Medium	Medium	N/A	N/A

For instance, administrative and intangible barrier systems exhibit an asymmetric susceptibility profile marked by an extreme sensitivity to sequence deviations, alongside moderate vulnerability to target object misspecification and activation latency. While their minimal lifecycle resource requirements and compressed deployment latency make them highly attractive under strict corporate capital constraints, their intrinsic coupling to human performance variability demands targeted procedural stabilization protocols to isolate and control sequence-related vulnerabilities.

Extended Barrier Archetypes and the Epistemic Boundaries of Automation

Contemporary safety science expands the traditional definition of defense-in-depth layers to encompass dynamic organizational networks, visual asset integrity inspection regimes, and frontline behavioral adaptations [20]. Within this expanded framework, the preventive observation system developed in this research is conceptualized and modeled as a meta-barrier. Its primary functional mandate does not entail the direct physical containment of hazard energy; instead, it executes a continuous, higher-order control loop engineered to detect, capture, and rectify latent performance drift within adjacent primary barriers before the catastrophic alignment of unmitigated deviations can occur. This systemic configuration becomes vital when evaluating the industry-wide trend toward automated physical barriers designed to decouple human variability from asset risk profiles. While advanced automation significantly suppresses high-frequency operational execution slips, it introduces rigid epistemic boundaries. Automated control loops are deterministically bound by the specific design-basis scenarios programmed into their logic solvers. When a socio-technical system drifts into beyond-design-basis accident regimes or encounters unpostulated emergent anomalies, automated algorithmic architectures fail, rendering human cognitive flexibility and real-time diagnostic resilience the ultimate line of systemic defense. Consequently, a total (100%) automation paradigm remains mathematically and operationally untenable for complex industrial assets, cementing the integra-

tion of Human Factors Engineering (HFE) as an invariant requirement for high-integrity risk optimization.

4.2.2. The Swiss Cheese Model as a Qualitative Precursor to Path Modeling

The conceptualization of risk propagation experienced a paradigm shift through the introduction of the Swiss Cheese Model [1].

This qualitative framework abstracts defense-in-depth as a series of non-homogeneous, sequential defensive slices where catastrophic failures occur only when dynamic vulnerabilities—modeled as holes—temporally align. While the SCM remains a powerful forensic tool for retrospective accident reconstruction, its utility in predictive engineering is severely limited by its qualitative nature and its problematic assumption of stochastic independence between defensive barriers. In complex process environments, barriers are structurally coupled; the degradation of an upstream safeguard actively alters the boundary conditions of adjacent layers. Rather than cataloging these failure modes as static, hierarchical checklists, the proposed Maximum-Vulnerability Diagram (MVD) framework operationalizes this qualitative concept. By treating the SCM's 'trajectory of opportunity' as a dynamic, mathematically coupled network, we parameterize these organizational and technical layers into a unified matrix formulation. This approach allows us to quantify the joint probability of systemic penetration directly at the discrete threat-trigger interface, replacing static taxonomies with live operational visibility.

Analytical Utility and Methodological Merits

The widespread adoption of this model across high-reliability organizations (HROs) stems from three core analytical capabilities:

- Socio-Technical Visual Semiotics: It provides a highly scannable heuristic that effectively communicates how cascading failures across distinct organizational strata concatenate to breach robust physical safeguards.
- Forensic Diagnostic Frameworks: It serves as the baseline conceptual architecture for dominant retrospective root-cause analysis methodologies, such as the Incident Cause Analysis Method (ICAM) and Tripod Beta.
- Macro-Organizational Diagnostics: It facilitates an aggregate, qualitative audit of an enterprise's defensive health by surveying vulnerabilities across administrative, procedural, and engineering layers simultaneously rather than auditing them in isolation.

Epistemic Limitations and the Mitigation Gap

Despite its diagnostic utility, utilizing the Swiss Cheese Model as a predictive engineering tool introduces significant structural and operational vulnerabilities:

- **The Independence Fallacy:** The model relies on a problematic assumption of structural and stochastic independence between defensive slices. In complex socio-technical systems, barriers are highly coupled; the degradation of upstream control routinely alters the operational envelope of adjacent safeguards, actively generating or widening downstream vulnerabilities. While classical models imply that the joint probability of systemic failure is a simple product of individual independent failures, real-world operational interactions and common-cause failures structurally compound this probability, resulting in a substantially higher risk exposure than aggregate linear calculations predict.
- **Deficit of Parameterization:** The framework operates strictly as a qualitative, retrospective heuristic. It lacks a rigorous quantitative structure to parameterize the size, fluctuation frequency, or dynamic alignment probability of defensive vulnerabilities, rendering objective, real-time safety-state quantification impossible.

- For this reason, modern risk engineering approaches seek to incorporate the dynamic influence of latent conditions into systemic modeling. Consequently, while the framework remains highly effective retrospectively for forensic incident reconstruction, its predictive application requires a transition toward high-fidelity, parameterized models capable of tracking real-time barrier vulnerability fluctuations under dynamic operational conditions.

4.2.3. Bifurcated Performance Metrics: Resolving the Efficiency-Effectiveness Dichotomy

Within the classical Swiss Cheese Model (SCM), failure propagation is modeled via a rigid, one-dimensional linear sequence, evaluating barrier efficacy solely through a monolithic reliability lens. This architecture fails to recognize that independent protection layers possess highly asymmetric risk-interception profiles depending on their spatial and temporal placement relative to the initiating nodes of operational variability.

In a dynamic causal network where anomalies continuously accumulate and amplify, upstream barriers deployed at early stages of the deviation trajectory suppress risk propagation before entropy cascades across network nodes. Conversely, capturing deeply propagated deviations at downstream operational stages demands a significantly higher expenditure of socio-technical resources and often yields lower safety margins.

To illustrate this architectural asymmetry, localized reactive remediations targeted at isolated sub-system failures consume substantial operational capital and introduce high latency while failing to arrest the macroscopic hazard vector. In contrast, a structural system-level barrier—such as a primary isolation mechanism—safeguards the entire process boundary, achieving maximum mitigation efficiency with minimal resource depletion by structurally decoupling the downstream network from the anomaly source.

Because the standard SCM lacks analytical dimensions to address this spatial-temporal decoupling, this research proposes an expanded framework parameterized by two distinct attributes:

- **Operational Efficiency:** The localized reliability of the barrier, defining its capacity to suppress internal vulnerabilities and perform its design safety function on demand.
- **Topological Effectiveness:** The structural proximity of the barrier to the primary locus of operational deviation. This attribute determines the ease with which risk-reduction margins can be optimized and dictates the barrier's capacity to arrest cascading failure paths.

This conceptual advancement is operationalized via a radial coordinate system (Figure 7), wherein the source of systemic deviation is positioned at the origin, encircled by concentric defensive layers. Barriers situated closer to the core exhibit high topological effectiveness, while peripheral layers require exponential resource allocations to elevate their operational efficiency.

Furthermore, the temporal dimension of barrier deployment establishes a critical engineering trade-off between baseline effectiveness and reconfiguration latency. Barriers integrated during the conceptual planning phase (the Blunt End) exert a profound structural influence on organizational constraints, offering maximum topological effectiveness. However, these baseline engineering controls suffer from low adaptability; an inherent deficiency discovered post-commissioning requires extensive, capital-intensive engineering redesigns and physical re-fabrication cycles.

Conversely, administrative and behavioral barriers deployed during operational execution (the Sharp End) exhibit lower structural effectiveness but possess high agility, allowing rapid, near-real-time calibration through localized procedural iterations and agile validation loops. This inverse relationship between structural effectiveness and operational

flexibility governs the propagation of deviations from administrative planning to physical execution, as diagrammed in Figure 8.

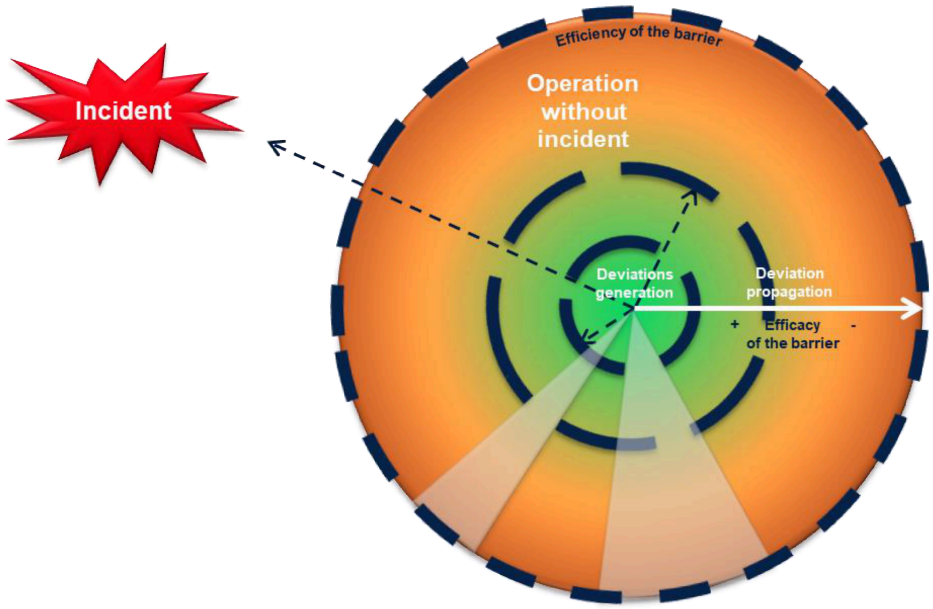

Figure 7. Radial safety architecture mapping defensive layers across operational efficiency and topological effectiveness coordinates. This coordinate system maps barrier performance relative to the core initiating event positioned at the origin. Safeguards situated closest to the origin possess maximum topological effectiveness because they disrupt early-stage deviation trajectories before energy cascades, whereas outer mitigative layers act primarily on the consequence space, requiring exponentially larger resource expenditures to elevate their localized operational efficiency and contain highly propagated anomalies. The MVD framework utilizes this radial mapping to visually highlight when safety investments are poorly balanced between early prevention and late-stage reactive mitigation. (Source: Author's elaboration).

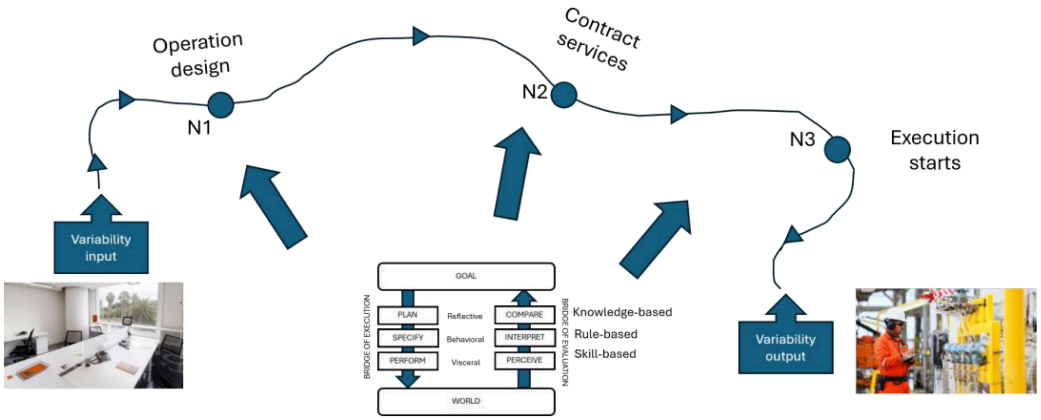

Figure 8. Topological model of deviation propagation across the socio-technical timeline from planning to execution. This schematic model represents the engineering trade-offs between structural effectiveness and operational flexibility across the project design lifecycle. Barriers integrated during the conceptual planning and engineering phase (blunt-end) exert a profound structural influence, providing high effectiveness but suffering from high reconfiguration latency and capital costs if redesigned post-commissioning. Conversely, administrative and behavioral barriers deployed during active operations (sharp-end) exhibit low structural risk-suppression capacity but possess high agility, allowing near-real-time calibration through localized procedural iterations (Source: Author's elaboration).

4.3. Stochastic Alignment of the Penetration Trajectory: The Path of Opportunity

The spatial-temporal alignment of defensive vulnerabilities creates a critical penetration trajectory, mathematically operationalized as the path of opportunity (PPO). Through this aligned vector, an escalating process deviation passes unhindered through all independent protection layers (IPLs), culminating in a loss of primary containment.

Let each individual barrier ef_i within a safety envelope possess an operational efficiency $Ef_i \in [0, 1]$. The probability of a latent or active vulnerability existing within that specific layer is defined by its complement, $1 - Ef_i$. While real-world process environments frequently exhibit common-cause and dependent failures—as discussed extensively in Section Stochastic Modeling of the Penetration Trajectory: The Path of Opportunity Probability—establishing a baseline under the assumption of mutual stochastic independence provides a rigorous theoretical bounding case. Under this classical Laplace assumption, the ideal cumulative probability of a complete systemic breach across a sequence of n independent safeguards is modeled as:

$$P_{PO} = 1 - Ef_j = (1 - ef_1) \times (1 - ef_2) \times (1 - ef_3) \times \ldots \times (1 - ef_n) \quad (2)$$

where

- ***n*:** Total number of independent barriers allocated to the scenario
- ***Ef_j*:** Total efficiency of the barrier system associated with the specific hazard, threat, and initiating event j.
- ***ef_i*:** Individual operational efficiency of barrier i.

This multiplication rule highlights how the concurrent alignment of multiple defensive layers structurally suppresses the joint probability of systemic failure.

To classify the materialization of a path of opportunity as highly improbable within industrial risk frameworks, the cumulative system failure probability must be suppressed below a strict risk-tolerance threshold, meaning the unreliability of the system must satisfy $(1 - ef_j) \leq 0.05$ (which equates to a minimum target system efficiency of $ef_j \geq 0.95$.

To isolate the mathematical impact of barrier density on this safety margin, we evaluate a boundary condition where all allocated barriers exhibit identical operational efficiencies (ef_i).

Under this homogeneous assumption, the minimum individual efficiency threshold $\left(eff_i^t\right)$ required to guarantee that the system complies with the maximum allowable risk exposure is derived by isolating ef_i from the boundary equation:

$$eff_i^t = 1 - \sqrt[n]{0.05} \quad (3)$$

This expression models the minimum integrity performance required per barrier as a function of the total asset safeguard density, where n is the number of barriers for the same scenario.

Evaluating this relationship across different barrier densities yields an exponential decay in the required individual performance threshold, as summarized in Table 7 and represented in the Figure 9.

The operational implications of this mathematical distribution are profound. In a single-barrier configuration (n = 1), the asset's safety state is highly sensitive; if the individual barrier's efficiency (ef_i) drifts below 95%, the system immediately breaches its risk-tolerance threshold. Conversely, introducing a secondary independent safeguard (n = 2) creates a cumulative risk-suppression effect. This structural redundancy allows the individual efficiency of each layer to drop toward approximately 77.64% without violating the aggregate system efficiency baseline ($ef_j \geq 0.95$). While this exponential relaxation underscores the power of defense-in-depth strategies, it also introduces a severe opera-

tional trap: it can foster institutional complacency, leading organizations to tolerate the steady degradation of individual barrier components (ef_i) under the false assumption that redundant layers will indefinitely mask localized vulnerabilities.

Table 7. Minimum individual barrier efficiency thresholds as a function of system barrier density (n) to maintain system failure risk below 5% (Source: Author's elaboration).

Barriers	Efficiency
1	95.00%
2	77.64%
3	63.16%
4	52.71%
5	45.07%
6	39.30%
7	34.82%
8	31.23%
9	28.31%
10	25.89%

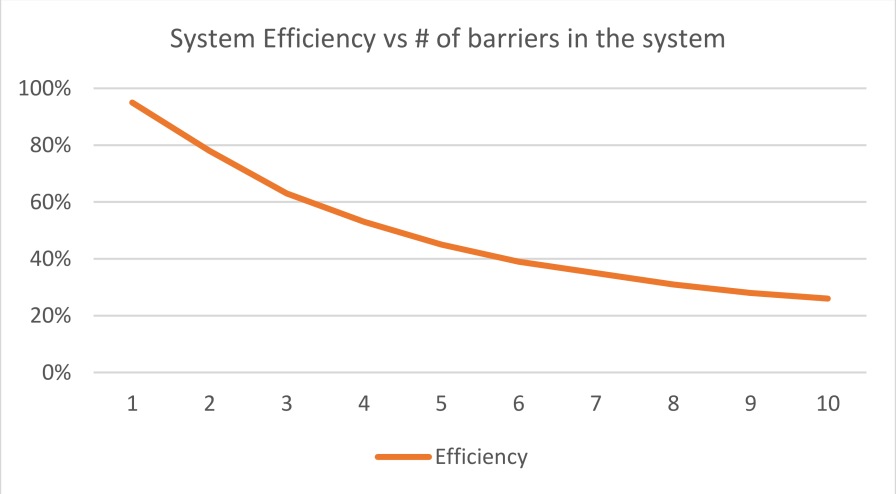

Figure 9. Exponential relationship between the number of events and the upper efficiency limit (Source: Authors' elaboration).

Stochastic Modeling of the Penetration Trajectory: The Path of Opportunity Probability

In conventional semi-quantitative risk assessment, risk is traditionally parameterized as a function of the probability of occurrence of a Top Event and the subsequent severity of its consequences, as mapped onto the two-dimensional risk matrix (Figure 1).

However, characterizing the probability of a path of opportunity materializing requires analyzing the latent system state prior to accident initiation, serving as a foundational necessary condition for hazard release. In this regard, the probability component of the governing risk equation can be mathematically decoupled as follows:

$$P_o \times P_a \times P_c = R \quad (4)$$

where

- P_o: Probability of the Path of Opportunity appearing.
- P_a: Conditional probability of a specific threat propagating through the allocated barrier layers.

- P_c: Probability of a specific consequence scenario developing following the materialization of the accident.
- R: Total quantified risk score.

The metric P_o can be evaluated locally across discrete hazardous nodes—consistent with traditional semi-quantitative protocols—or aggregated globally across the entire asset architecture. To achieve this, mathematical formulation must account for stochastically independent threat-barrier coupling scenarios. This stems from the fact that threats and independent protection layers are not uniquely coupled to a single hazard; a singular threat vector can activate multiple hazardous nodes, and a shared barrier system can simultaneously suppress diverse threat trajectories.

When an active process deviation bypasses the preventive barrier system, it triggers the primary initiating event, thereby releasing the hazard and generating an escalating accident sequence. The terminal severity of this sequence depends on the operational readiness of downstream mitigative and recovery barriers. For instance, following thermal runaway or ignition, the absence or failure of localized fire suppression systems allows unhindered flame propagation, compounding asset damage and escalating the safety consequence vector. These cascading downstream trajectories are governed by conditional probabilities derived from the thermodynamic and physical severity potential of the specific hazard node under analysis.

As illustrated in the systemic trajectory layout (Figure 10), the structural allocation of a barrier system (B_j) generates a path of opportunity with a probability P_o. Concurrent threat vectors (Th_i) generate operational deviations that propagate through this path with a probability P_a, subsequently releasing a specific hazard (H_k), while downstream consequence vectors mature with a conditional probability P_c.

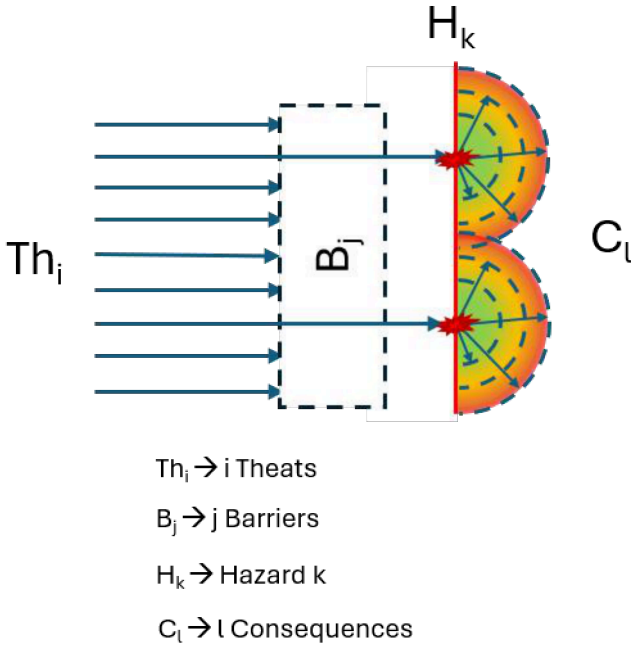

Figure 10. Process deviation propagation map detailing threat activation, barrier system penetration thresholds, hazard release boundaries, and multi-attribute consequence development. A color scale has been used to represent the severity level of the consequence scenario. (Source: Authors' elaboration).

To mathematically formalize the integrity of an individual barrier bi, we define a continuous operational variable $ef_i \in [0, 1]$. A boundary state of $ef_i = 0$ denotes absolute barrier dysfunctionality (total failure to capture deviations), whereas $ef_i = 1$ signifies deterministic

interception of all targeted threat dynamics. Consequently, the conditional probability of failure on demand for any given barrier b_i is expressed by its complement, $1 - ef_i$.

Within this framework, a path of opportunity is realized when all allocated safeguards within a specific defensive sequence fail simultaneously. The combination of these individual failure probabilities defines the joint probability that a process deviation will successfully propagate and activate an initiating event. To construct this systemic interaction space, let B represent the primary barrier column vector across n total allocated barriers:

$$\vec{B} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_n \end{pmatrix} \tag{5}$$

To map the functional applicability of these barriers against specific threat vectors, a selection matrix A_j is introduced for each discrete threat j. This structure is defined as a diagonal mapping matrix whose binary entries filter barrier relevance:

$$A_j = \begin{bmatrix} a_{j1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{jn} \end{bmatrix} \tag{6}$$

Pre-multiplying the primary barrier vector by this selection matrix derives the specific applicable barrier sub-vector B_j for any independent threat j:

$$\vec{B_j} = A_j \vec{B} = \begin{bmatrix} a_{j1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{jn} \end{bmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_{j1}b_1 \\ a_{j2}b_2 \\ a_{j3}b_3 \\ \cdots \\ a_{jn}b_n \end{pmatrix} \forall j, i, n \in \mathbb{N}\,;\; a_{ji} = (0,1) \in \mathbb{N} \tag{7}$$

For each discrete hazard k represented by the vector H_k, a specific subset of threats A_j possesses the capacity to trigger containment loss. To formalize this cross-layer interaction, we define the comprehensive threat-matrix vector (A_{Hk}) by scaling each selection matrix by the mapping operator $h_{kj} \in (0, 1)$:

$$\vec{A_{H_k}} = \vec{H_k} A = \begin{pmatrix} h_{k1}A_1 \\ h_{k2}A_2 \\ h_{k3}A_3 \\ \cdots \\ h_{km}A_m \end{pmatrix} = \begin{pmatrix} \begin{bmatrix} h_{k1}a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{k1}a_{1n} \end{bmatrix} \\ \begin{bmatrix} h_{k2}a_{21} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{k2}a_{2n} \end{bmatrix} \\ \begin{bmatrix} h_{k3}a_{31} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{k3}a_{3n} \end{bmatrix} \\ \cdots \\ \begin{bmatrix} h_{km}a_{m1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & h_{km}a_{mn} \end{bmatrix} \end{pmatrix} \forall j, k, n, m \in \mathbb{N}\,; h_{kj}a_{ji} = (0,1) \in \mathbb{N} \tag{8}$$

where n denotes the absolute barrier density, and m represents the total cardinality of the threat space. By coupling these mathematical expressions, we derive the integrated asset barrier matrix B_{Hk} for each discrete hazard node k, yielding an n x m topological matrix:

$$B_{H_k} = \vec{A}_{H_k}\vec{B}_j = \begin{pmatrix} h_{k1}a_{11}b_1 & \dots & h_{km}a_{m1}b_1 \\ \vdots & \ddots & \vdots \\ h_{k1}a_{1n}b_n & \dots & h_{km}a_{mn}b_n \end{pmatrix} \forall j,k,n,m \in \mathbb{N}\,; h_{kj}a_{ji} = (0,1) \quad (9)$$

By embedding the specific individual operational efficiency values into this coordinate space, the joint probability of establishing a path of opportunity for any given hazard node can be extracted. Aggregating these localized probabilities over a defined temporal horizon t yields the macroscopic probability of path of opportunity materialization during asset operation.

Evaluating the topological structure of matrix B_{Hk} reveals critical risk insights:

- **Safeguard Centrality:** A single physical or administrative barrier may map across multiple threat vectors simultaneously; barriers exhibiting high matrix column density possess elevated structural importance for asset integrity.
- **Defensive Null-Nodes:** The framework assumes baseline barrier allocation across all identified threats. If a threat row contains only zero entries, a structural vulnerability exists, meaning a path of opportunity is permanently active and demands immediate risk remediation.
- **Cross-Hazard Commonality:** Multiple hazards can share identical threat matrices. While this model assumes shared threat vectors deploy congruent barrier configurations, the matrix can be decoupled to evaluate asymmetric barrier responses.

Consequently, the total failure probability of a protective envelope relative to a specific hazard is derived by compounding the failure distributions across all relevant threat vectors. This mathematical coupling demonstrates that a barrier's contribution to system resilience scales directly with its assignment density across concurrent threats.

The overall failure probability of a barrier subsystem facing a specific threat j, denoted as $P^f_{a_j}$, is derived by calculating the product of the individual barrier failure probabilities:

$$P^f_{a_j} = \left(1 - a_{j1}ef_1\right) \times \left(1 - a_{j2}ef_2\right) \times \left(1 - a_{j3}ef_3\right) \times \ldots \times \left(1 - a_{jn}ef_n\right) \quad (10)$$

Expressed compactly using product notation:

$$P^f_{a_j} = \prod_{i=1}^{n}\left(1 - a_{ji}ef_i\right) \forall j,i,n \in \mathbb{N}\,; a_{ji} = (0,1) \quad (11)$$

This expression quantifies the stochastic alignment of vulnerabilities across the defensive sequence. The formulation highlights that a high-integrity barrier ($ef_i \to 1$) structurally isolates the downstream process, preventing anomaly propagation. Under the assumption of mutually independent threat vectors, a systemic path of opportunity is established if any single threat successfully breaches its allocated safeguards.

To determine the total vulnerability of a specific hazard node k, we evaluate the complement of the system state. The boundary condition where a path of opportunity is not realized occurs only when all concurrent threat-propagation trajectories are successfully intercepted. This survival probability is formulated as:

$$(1 - P^f_k) = \prod_{j=1}^{m}(1 - h_{kj}P^f_{a_j}) = \prod_{j=1}^{m}\left(1 - h_{kj}\prod_{i=1}^{n}\left(1 - a_{ji}ef_i\right)\right) \quad (12)$$

Bounded strictly between 0 and 1, this equation provides the probability of absolute system containment. Consequently, the active probability of a path of opportunity materializing for a specific hazard k, denoted as P_k^f defined by the governing expression:

This terminal expression allows safety engineers to mathematically quantify the probability of generating an unmitigated accident scenario for any target hazard node within the socio-technical architecture.

Structural Dependence and Conditional Probability Frameworks

The mathematical validity of Equation (11) relies strictly on the assumption of mutual stochastic independence among the evaluated threat-propagation trajectories. However, empirical mapping of complex socio-technical systems demonstrates that individual independent protection layers (IPLs) are frequently multiplexed across multiple concurrent threat pathways and hazardous nodes.

When a single physical or administrative barrier simultaneously cross-guards multiple risk vectors, its localized degradation introduces a systemic common-cause vulnerability. This coupling violates the classical independence axiom, rendering direct multiplicative aggregations of hazard-level failure probabilities mathematically invalid. Consequently, quantifying the actual probability of a path of opportunity materializing requires a paradigm shift away from linear product rules and toward conditional probability frameworks capable of modeling joint distributions and dependent events.

To demonstrate the mathematical mechanics of this conditional dependence while maintaining analytical tractability, the primary initiating event has been omitted from the following illustrative scenarios:

Case Scenario A: Common barriers

To evaluate the quantitative impact of common-cause vulnerabilities, consider a hazardous node H_1 whose containment can be breached by three concurrent threat vectors: TH_1, TH_2, and TH_3. A defensive envelope consisting of three barriers—B_1, B_2, and B_3—is deployed to intercept these threats. The topological mapping of these independent protection layers reveals that certain safeguards are multiplexed across different threat pathways, as structured in the network configuration diagram in Figure 11.

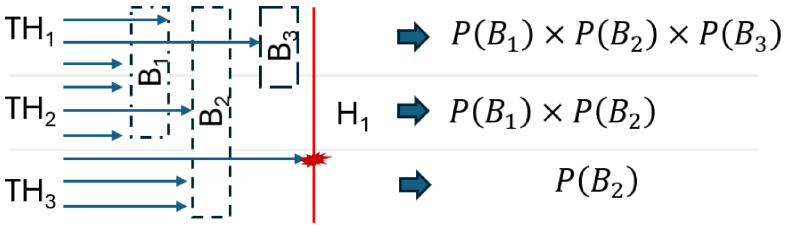

Figure 11. Topological network mapping unique and shared common safety barriers across concurrent threat propagation paths. The arrow shows the propagation of a deviation generated by the threat which slips between the holes of the barriers to release the hazard. (Source: Authors' elaboration).

The preliminary network layer models the simplified probability of a path of opportunity by executing a linear multiplication of the unreliability values for each barrier, denoted as $P(B_i)$. However, because B_2 acts as a shared constraint across multiple rows, this assumption of independence introduces significant skewness.

To resolve this and quantify the exact probability of a path of opportunity materializing under dependent conditions, an asymmetric conditional probability tree is constructed. This analytical tree maps the disjoint state-space combinations of barrier successes and failures, isolating only those specific operational trajectories that successfully lead to system breach (Figure 12).

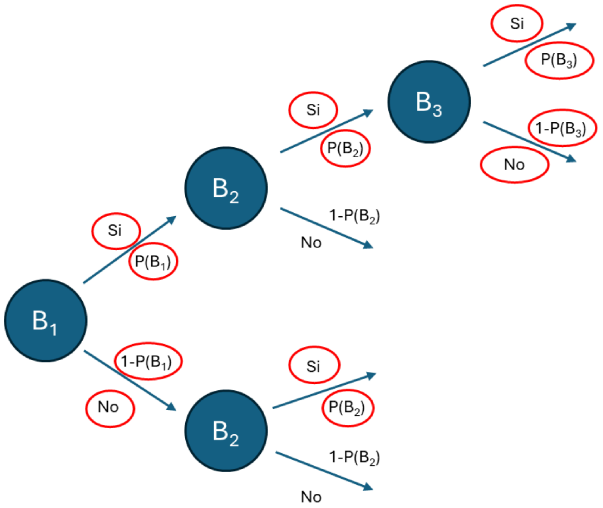

Figure 12. Asymmetric conditional probability tree architecture for dependent threat pathways sharing common defensive barriers. (Source: Authors' elaboration).

By computing the conditional probabilities along each successful breach branch and applying the theorem of total probability to aggregate these mutually exclusive scenarios, the governing equation for the total probability of a path of opportunity materializing at hazard H_1 is established:

$$P(H_1) = P(B_1) \times P(B_2) \times P(B_3) + P(B_1) \times P(B_2) \times (1 - P(B_3)) + (1 - P(B_1)) \times P(B_2) \quad (13)$$

Equation (13) shows the calculation of the probability of a Path of Opportunity for hazard H_1 where the first element corresponds to TH_1, TH_2 and TH_3 the second element TH_2 and TH_3 and the last element to the TH_3.

This comprehensive polynomial accounts for every permutation of systemic failure state where the common barrier compromises the adjacent nodes. By systematically factoring out the shared probability terms and executing sequential Boolean reductions, the complex state-space equation simplifies to the following expression:

$$\begin{aligned} P(H_1) &= P(B_2) \times (P(B_1) \times P(B_3) + P(B_1) \times (1 - P(B_3)) + (1 - P(B_1))) \\ P(H_1) &= P(B_2) \times (P(B_1) \times P(B_3) - P(B_1) \times P(B_3) + 1) \\ P(H_1) &= P(B_2) \times (P(B_1) \times P(B_3) - P(B_1) \times P(B_3)) + P(B_2) \\ P(H_1) &= P(B_2) \end{aligned} \quad (14)$$

Equation (14) shows the derivation of the probability of a Path of Opportunity when there is a single barrier in a given scenario and a common barrier for the remaining scenarios associated with that hazard.

Consequently, the algebraic reduction demonstrates that the probability of a path of opportunity materializing for a hazard node governed by a single shared safeguard across all threat trajectories collapses to the isolated failure probability of that specific shared component. In this scenario, the systemic resilience of the asset is entirely dependent on the integrity of B_2.

While the mathematical formulation is simple, its operational implications for process safety engineering are profound. This reduction proves that a shared barrier acts as a stochastic Single Point of Failure (SPOF) within the defense-in-depth architecture. Identifying these hidden common-cause nodes during the design and auditing phases is critical, as any marginal degradation in their individual performance instantly compromises the entire safety envelope of the associated industrial asset.

Case Scenario B: Independent barriers

To establish a baseline contrast for the common-cause failure paradigm, consider a second scenario where each threat vector is mapped to a unique, unshared independent protection layer. In this configuration, hazard H_2 is safeguarded against three threats (TH_1, TH_2, and TH_3) by three distinct barriers (B_1, B_2, and B_3, respectively). This layout ensures that the operational integrity or degradation of any single safeguard remains decoupled from the adjacent layers, as illustrated in the network topology in Figure 13:

Figure 13. Structural mapping of localized, mutually independent barriers assigned to isolated threat vectors. (Source: Authors' elaboration).

Because of these safety barrier conditions, the system state independently, constructing an equivalent conditional probability tree yields a symmetric state-space distribution. This symmetry reflects the uncoupled nature of the underlying failure probabilities, mapping the combinations where each independent path can breach the containment boundary (Figure 14).

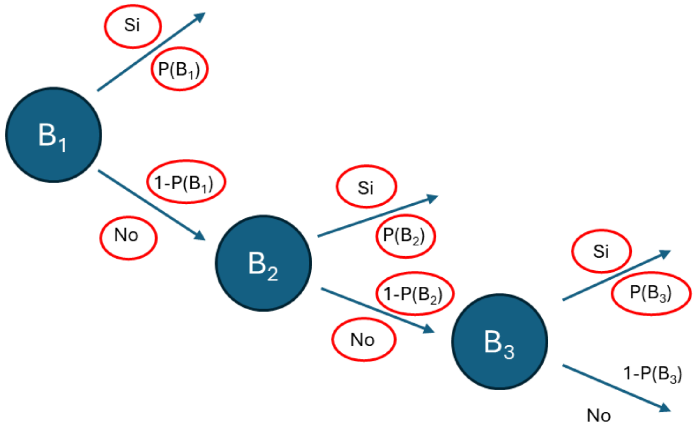

Figure 14. Symmetric conditional probability tree for stochastically uncoupled threat pathways with independent barriers. (Source: Authors' elaboration).

Consequently, the total probability of a path of opportunity materializing for hazard H_2 is derived by evaluating the union of these independent failure events. This is mathematically expressed as the complement of the probability that all independent barriers successfully intercept their respective threats:

$$P(H_2) = P(B_1) + (1 - P(B_1)) \times (P(B_2) + (1 - P(B_2)) \times P(B_3)) \quad (15)$$

Equation (15) shows the calculation of the probability of a Path of Opportunity for hazard H_1 for different threat scenarios where there is a unique barrier that is not common to all scenarios where the first element applies to TH_1, TH_2 and TH_3, the second element to TH_3 and TH_1 and the last element only to TH_1

This formulation models the cumulative vulnerability of the safety system when protections operate without common-cause coupling.

These two boundary cases establish an analytical framework for quantifying path of opportunity probabilities within complex process environments. While stylized, this dual methodology provides a scalable heuristic for approximating systemic risk exposure. Managing this scalability becomes essential when auditing high-density barrier networks, where evaluating the exact probability triggers a combinatorial explosion. For a network containing n independent barriers interposed between threats and initiating events, the total number of discrete operational scenarios scales exponentially as $2n$, rendering exhaustive state-space calculation computationally intractable for large-scale industrial assets.

To circumvent this computational constraint, a structural reduction heuristic is derived from our first scenario: engineers can systematically identify single shared barriers that cross-guard all operational rows. Because these shared nodes collapse the conditional probability space, the scenarios dependent on them can be isolated, and their systemic dependencies simplified. Once these common-cause nodes are abstracted, the independent formulation verified in the second scenario can be applied to the remaining decoupled sub-systems. This hybrid analytical approach drastically reduces the dimensionality of the risk matrix, providing a fast, high-fidelity approximation of the aggregate path of opportunity probability.

4.4. Synthesis: How Causation Theories Construct the MVD Model

The MVD framework directly operationalizes and bridges these three historical causation paradigms through specific modeling constructs:

- **Sequential-Linear Paradigm:** Used to map the direct, uncoupled threat–trigger trajectories. While too simplistic for global systems, it represents the vital 'micro-pathways' that must be individually secured.
- **Epidemiological Paradigm (Reason's SCM):** Used to classify safety barriers into four distinct ontological typologies (physical, functional, symbolic, administrative) and map latent organizational conditions (blunt-end pathogens) as structural vulnerabilities.
- **Systemic Paradigm (Hollnagel):** Used to model and analyze the dynamic, non-linear dependencies between barriers. This justifies our matrix algebra representation, which rejects the assumption of stochastic independence and treats barriers as highly coupled nodes in an operational network.

By synthesizing these concepts, the MVD converts qualitative causation theories into a parameterized, predictive engineering tool, mapping how localized performance deviations propagate through a 'Path of Opportunity' to activate a catastrophic hazard release.

5. Practical Application and Industrial Case Studies: High-Vulnerability Network Topology

A vulnerable system is defined as one that presents a possibility of being damaged. By identifying the critical points through which the system may fail and lead to accidents, it is possible to classify its degree of vulnerability based on the number and type of barriers available for each risk scenario.

Within the context of HAZID analysis, a list of barriers is associated with each hazard, with the purpose of reducing the likelihood of occurrence of the initiating event and, in some cases, mitigating the consequences once it has occurred. However, mitigation barriers (Recovery Measures) are not considered in the present analysis, since they are activated only after the accident has taken place.

For an accident to occur, a threat must pass through the preventive barriers (Threat Control) and release the hazard. Logically, the greater the number of barriers between the threats and the hazard, the lower the vulnerability of the system. Therefore, maximum vulnerability is structurally defined as the minimum cardinality of the active preventive barrier

set across all credible threat-trigger pathways for a given hazard, which mathematically sets the upper bound of the joint system failure probability. Let $n_{min} = \min_j\{n_j\}$ represent the minimum barrier density among all threat trajectories j associated with hazard k. When $n_{min} = 1$ (representing a single-barrier pathway), the systemic failure probability collapses directly to the individual unreliability of that solitary safeguard $(1 - e_{f1})$, as derived from Equation (2). To restrict this unreliability below a standard probabilistic threshold of 5% ($P_{kf} \leq 0.05$), representing a 'rare event' under a probabilistic approach, the individual barrier efficiency must satisfy Equation (3): $e_{ffit} = 1 - \sqrt[n]{0.05} \Longrightarrow e_{ffit} \geq 95\%$.

Two practical examples with a specific hazard and the barriers protecting it against different threats are presented below.

5.1. Practical Application: Quantitative Determination of Maximum Vulnerability Topology

To operationalize the mathematical and matrix frameworks derived in the preceding sections, this section evaluates empirical data extracted from high-risk industrial asset operations. The socio-technical risk nodes, threat vectors, and independent protection layers (IPLs) are systematically classified and coded in strict compliance with the structural guidelines specified in ISO 17776 [7]:

- **Hazard:** Discrete operational nodes containing inventory or conditions capable of causing systemic harm, coded as H-XX.XX.XX.
- **Threat:** Initiating mechanisms or environmental/procedural triggers that can induce a loss of primary containment, coded as THXX.
- **Safety Barriers:** Separated into baseline controls (Inherent Barriers, coded as BCXXX) and secondary optimizations deployed post-assessment (Residual Barriers, coded as ACXX).

Case Application 01: Baseline Inherent Vulnerability in Working-at-Height Operations (H-06.01)

Hazard: H-06.01—Personnel at height > 2 m.

Consider the hazardous envelope H-06.01, defining operations where personnel execute tasks at elevated levels exceeding 2 m. The initial unmitigated interaction space maps a dense network of preventive inherent barriers against multiple concurrent threat lines, as consolidated in Table 8.

Table 8. Initial screening matrix mapping hazard H-06.01 against concurrent threat lines and unclassified inherent controls (Source: Authors' elaboration).

Hazard Node Reference	Threat Code	Assigned Preventive Threat Control (Baseline Safeguard)
H-06.01 (Personnel at height > 2 m)	TH01 (Personnel slip/trip/fall)	BC006 (Certified Personal Fall Arrest System)
	TH16 (Structural failure of platform)	BC010 (Fixed Perimeter Guardrails and Toe-boards)
	TH17 (High winds/Adverse weather)	BC027 (Certified Independent Scaffolding Structure)
	TH19 (Improper ladder/scaffold access)	BC034 (Permit-to-Work PTW Gateway Validation)
		BC035 (Pre-Task Safety Toolbox Briefing)
		BC036 (Competent Supervisor Site Clearance)

To ensure complete clarity and traceability, all barrier codes have been fully decoded:

- **BC006:** Certified Personal Fall Arrest System (Full-body safety harness and shock-absorbing lanyard).
- **BC010:** Fixed Perimeter Guardrails and Toe-boards (Physical collective protection).
- **BC027:** Certified Independent Scaffolding Structure (Inspected and tagged work platform).

- **BC034:** Administrative Permit-to-Work (PTW) Gateway Validation.
- **BC035:** Pre-Task Safety Briefing and Toolbox Checklist Verification.
- **BC036:** Competent Supervisor Site Clearance Certification.
- **BC025:** Individual Personal Protective Equipment (PPE) Compliance Check.

The systemic defense architecture experiences a dangerous dilution along the TH17 vector (adverse weather conditions/high winds). Rather than enjoying a redundant, multi-layered defense-in-depth layout, this specific threat relies on a single protective element: **BC035 (Pre-Task Safety Briefing)**. This creates a critical point of failure where a purely administrative, human-dependent control is expected to absorb the entire operational risk.

At initial review, the absolute density of the safeguard inventory appears robust, potentially misleading asset managers into assuming a low-risk profile based on a simple count of protective barriers. However, when these safeguards are discretized using the matrix mapping criteria developed in Section 3.2 to evaluate explicit compatibility vectors, a highly asymmetric vulnerability topology emerges, as detailed in Table 9.

Table 9. Decoupled structural barrier compatibility matrix filtered by independent threat pathways. (Source: Authors' elaboration).

Hazard Reference	Specific Threat Pathway	Assigned Preventive Threat Control (Inherent Barrier)
H-06.01 (Working at Height)	TH01 (Personnel slip/trip/fall)	BC006 (Certified Personal Fall Arrest System)
		BC010 (Fixed Perimeter Guardrails and Toe-boards)
		BC034 (Permit-to-Work PTW Gateway Validation)
		BC036 (Competent Supervisor Site Clearance)
	TH16 (Structural platform failure)	BC006 (Certified Personal Fall Arrest System)
		BC010 (Fixed Perimeter Guardrails and Toe-boards)
		BC027 (Certified Independent Scaffolding Structure)
		BC035 (Pre-Task Safety Toolbox Briefing)
	TH17 (High winds/Adverse weather)	BC035 (Pre-Task Safety Toolbox Briefing)
	TH19 (Improper ladder/scaffold access)	BC034 (Permit-to-Work PTW Gateway Validation)
		BC025 (Individual PPE Compliance Check)

This structural breakdown exposes a critical system vulnerability concealed by aggregate counting methods. The systemic defense architecture experiences a dangerous dilution along the TH17 vector. Rather than enjoying a redundant, multi-layered defense-in-depth layout, this specific threat relies on a single protective element, creating a critical point of failure within the asset safety envelope. By classifying these protections according to the risk factors governing the elasticity of their operational efficiency, we construct the topological network layout illustrated in Figure 15.

Threats	Factors							Hazards
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH01			BC034 BC036	BC010	BC006			H-06.01
TH16				BC010	BC006 BC027		BC035	H-06.01
TH17							BC035	H-06.01
TH19			BC034				BC035	H-06.01

Figure 15. Functional classification of inherent safeguards for hazard H-06.01 based on structural elasticity and operational factors. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. One barrier can cover more than one threat scenario. (Source: Authors' elaboration).

This network analysis highlights that threat lines TH01 and TH19 are coupled to upstream regulatory constraints. These constraints mandate formal third-party compliance certifications before permitting scaffolding installation or high-level access. These administrative controls, denoted as BC034 (shared across both threat pathways) and BC036, function as mandatory gateway triggers that block work execution until physical verification is completed.

If the upstream barrier BC034 suffers an operational failure or administrative bypass, threat line TH01 retains a secondary defense layer through the redundant gateway control BC036. Conversely, the TH19 pathway exhibits zero internal redundancy; bypassing BC034 triggers an immediate downstream cascade to the terminal defense element, BC035 (the final pre-execution verification loop). This configuration shifts the entire risk burden onto a single intangible safeguard, exponentially increasing system sensitivity to active human errors caused by localized diagnostic slips or gaps in specific technical competencies. This structural degradation and the resulting open path of opportunity following the removal of BC034 are diagrammed in Figure 16.

Threats	Factors							Hazards
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH01			BC036	BC010	BC006			H-06.01
TH16				BC010	BC006 BC027		BC035	H-06.01
TH17							BC035	H-06.01
TH19							BC035	H-06.01

Figure 16. Accelerated path of opportunity generation across threat vector TH19 following the removal of common gateway control BC034. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. One barrier can cover more than one threat scenario. (Source: Authors' elaboration).

This mapping proves that localized efficiency degradation within a single barrier can cause non-linear risk amplification across the system topology, depending on the specific threat vector it intercepts. The critical centrality of BC035 is clear; it serves as the terminal defensive constraint for three of the four threat pathways driving this hazardous scenario and represents the solitary safeguard mitigating the TH17 vector. This concentration of risk

violates basic defense-in-depth principles and highlights the need for structural redundancy as required by organizational resilience frameworks like ISO 31000 [21].

Evaluating this network demonstrates a critical decoupling: while the global hazard appears protected by an initial regulatory envelope, granular threat-level deconstruction shows that specific critical pathways lack early-stage protection, forcing defenses down to the sharp-end execution point and increasing residual risk exposure.

This vulnerability compounds when evaluating cross-hazard common-cause coupling. Weakening the administrative integrity of BC034 simultaneously compromises an adjacent risk node: hazard H-06.03 (Overhead Equipment/Falling Objects), which carries a baseline high risk profile characterized by metrics R = 16, C = 4, and L = 4 (Following risk matrix on Figure 1). Because mitigating threat TH01 within H-06.03 also relies on the availability of BC034, its failure triggers a multi-hazard defensive collapse. This collapse degrades structural redundancy across separate process systems, increasing the joint probability of sequential failures, as mapped across the risk factor layers in Figure 17.

Threats	Factors							Hazards
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH01			BC034	BC010		BC046	BC018 BC051	H-06.03
TH18				BC010			BC045 BC051	H-06.03
TH25				BC010	BC027	BC046	BC045	H-06.03
TH26				BC010		BC044	BC045	H-06.03
TH27						BC046 BC047	BC048	H-06.03
TH28				BC010		BC046	BC045	H-06.03
TH32					BC017		BC018	H-06.03

Figure 17. Cross-hazard risk factor topology for hazard H-06.03 displaying shared operational dependencies on gateway control BC034. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. One barrier can cover more than one threat scenario. (Source: Authors' elaboration).

Bypassing this shared asset alters the underlying defense architecture, removing redundant safeguards and accelerating systemic failure pathways, as illustrated in Figure 18.

For hazard H-06.03, the marginal increase in penetration probability is partially contained by its high initial safeguard density. Because its network topology incorporates a larger array of uncoupled, independent barriers, driving this sub-system to total failure requires the concurrent materialization of multiple stochastic faults, suppressing the immediate probability of hazard release.

To map these systemic interactions completely, this structural vulnerability analysis must be integrated with a granular classification of barrier typologies to isolate specific failure modes and their common-cause coupling. While the analytical tractability of hazard H-06.03 is simplified by its single initiating event (TE04), real-world asset integrity management routinely faces complex multi-causal distributions.

To resolve this complexity, the following section evaluates a high-dimensional operational scenario. We analyze a safety envelope governed by multiple concurrent initiating events, tracking system performance both before and after the deployment of optimized residual barriers (ACXX). This evaluation classifies safeguards by structural system types, ensuring compliance with the safety redundancy requirements mandated by both ISO 31000

resilience frameworks and OSHA regulatory standards for high-consequence industrial operations [22,23].

Threats	Factors							Hazards
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH01				BC010		BC046	BC018 BC051	H-06.03
TH18				BC010			BC045 BC051	H-06.03
TH25				BC010	BC027	BC046	BC045	H-06.03
TH26				BC010		BC044	BC045	H-06.03
TH27						BC046 BC047	BC048	H-06.03
TH28				BC010		BC046	BC045	H-06.03
TH32					BC017		BC018	H-06.03

Figure 18. Degraded network state for hazard H-06.03 following common-cause barrier failure BC034. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. One barrier can cover more than one threat scenario. (Source: Authors' elaboration).

5.1.1. Recommendations for Engineering Improvements (Working-At-Height Operations):

To mitigate the high vulnerability identified along the TH17 (adverse weather) and TH19 (improper ladder/scaffold access) pathways, the asset safety envelope must be upgraded through the following targeted interventions:

- **Physical and Functional Redundancy:** Wherever structurally feasible, install permanent physical edge protection (such as perimeter guardrails, BC010) to eliminate the complete reliance on administrative and personal fall-arrest systems. For high wind risks (TH17), integrate physical wind-monitoring telemetry (anemometers) on scaffolding structures that trigger an automatic visual and acoustic alarm when wind speeds exceed 12 m/s, alerting operators to evacuate.
- **Digital PTW Integration (Gateway Verification Loops):** Implement a digital dual-validation lock on the Permit-to-Work (PTW) system (BC034). Under this protocol, scaffold safety certification (BC027) must be uploaded and digitally signed by an independent inspector before the site access gate is cleared, removing the reliance on a single supervisor's manual verification.

Case Application 02: Inherent and Residual Risk Dynamics in Rotary and Mobile Equipment (H-08.01)

The second empirical scenario evaluates the safety envelope of hazard node H-08.01, which defines risks associated with equipment featuring moving or rotating parts.

To ensure absolute readability, the alphanumeric safety-critical elements are fully decoded below:

- **BC055:** Operator Technical Competence and License Assurance Review.
- **BC018:** Pre-Use Equipment Safety Inspection Checklist.
- **BC057:** Preventive Maintenance Logging and Records Verification.
- **BC058:** Internal Quality Assurance Compliance Auditing.
- **AC013:** Pre-Mobilization Technical Equipment Acceptance Assurance.
- **AC014:** Field Verification of Regulatory Certifications and Maintenance Compliance.

- **AC020:** Active Physical Machinery Guarding and Sensor-based Interlocks.

The primary physical sources of this hazard include heavy construction machinery such as excavators, dump trucks, motor graders, cranes, and compactors. The risk baselines established during the hazard identification (HAZID) phase are quantified as follows (by following Figure 1):

Inherent Risk Score: Moderate (L = 3; C = 3; R = 9)

Residual Risk Score: Minor (L = 2; C = 3; L = 2; R = 6)

This hazard node possesses a complex multi-causal topology: it materializes through three distinct initiating events (TEs) driven by a combination of mechanical system failures and sharp-end human performance deviations. Crucially, the underlying threat vectors (THs) do not map uniformly across all initiating events. This asymmetry introduces significant conditional dependencies into the barrier efficiency model. The explicit mapping between threat vectors and initiating events are structured in Tables 10 and 11.

Table 10. List of initiating events applicable to hazard H-08.01 (Source: Authors' elaboration).

Top Event Code	Top Event (Initiating Event) Description	Operational Scope within Hazard Boundary
TE02	Loss of control of Equipment	Total loss of directional, mechanical, or speed control of mobile plant asset during site operation.
TE07	Equipment Failure	Mechanical, electrical, or structural fault of a safety-critical rotary or mobile component.
TE15	Human Error/Operator Slippage	Frontline operational deviation, task sequence bypass, or active cognitive failure by the operator.

Table 11. Cross-layer mapping matrix between threat vectors (TH) and initiating events (TE) for hazard H-08.01. (Source: Authors' elaboration).

Threat Reference	Description of Threat Vector	Linked Initiating Event (TE) Triggers
TH01	Unauthorized entry of personnel into active rotary workspace	TE02 (Loss of control), TE07 (Equipment failure), TE15 (Human error)
TH25	Operating equipment beyond certified mechanical parameters	TE02 (Loss of control), TE15 (Human error)
TH32	Inadequate maintenance or component fatigue on rotary machinery	TE02 (Loss of control), TE07 (Equipment failure)
TH33	Deficient maintenance or inspection logging protocols	TE02 (Loss of control), TE07 (Equipment failure)
TH34	Unqualified or uncertified operator executing active tasks	TE02 (Loss of control), TE15 (Human error)
TH35	Operator physical fatigue or shift cognitive workload saturation	TE02 (Loss of control), TE15 (Human error)
TH49	Extreme environmental stresses/severe weather operations	TE02 (Loss of control), TE07 (Equipment failure)

Within this causal hierarchy, initiating event TE02 represents the macroscopic system loss of control, whereas TE07 (mechanical failure) and TE15 (human error) act as low-level triggers that cascade into TE02. However, an active human error (TE15) or a mechanical anomaly (TE07) does not deterministically cause a total loss of equipment control.

To maintain analytical resolution, this model evaluates all three initiating events simultaneously. This approach separates specific mechanical and behavioral triggers from the general loss-of-control event (TE02), capturing latent triggers that may fall outside traditional classifications.

Evaluating the baseline inherent risk configuration solely through risk factors yields the initial defensive blueprint shown in Figure 19.

Threats	Factors							Hazards
		Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH01						2	1	2	H-08.01
TH25						6	4		
TH32						2		2	
TH33						2			
TH34						2	2		
TH35						4	3		
TH49						4	2		

Figure 19. Inherent vulnerability network for hazard H-08.01 categorized by organizational risk factors and baseline barrier densities. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. The greater the number of barriers, the greener the cell is been colored. (Source: Authors' elaboration).

Topological evaluation of this network demonstrates that all identified threat vectors are initially intercepted by the "Management" factor layer. This indicates that the Project Management Team (PMT) has established baseline administrative controls across all risk pathways.

Furthermore, the majority of threat vectors incorporate redundant defense layers within the "Local Workplace" and "Unsafe Act" factors. The clear exception is vector TH33 (deficient maintenance protocols), which exhibits minimal safeguard coverage. A primary conclusion from this topology is the immediate operational requirement to reinforce the barriers assigned to this specific vector or introduce independent variables to suppress its high unreliability index. The primary active barrier for TH33 is BC057 (maintenance logging and records verification). To mitigate this vulnerability, a cross-layer optimization strategy can be deployed by importing barrier BC050 originally assigned to overhead equipment hazards—to reinforce heavy machinery deployment.

Despite a high aggregate barrier count across the global hazard node, breaking down the system configuration by individual initiating events reveals structural vulnerabilities. As modeled in Figure 20, threat pathway TH01 possesses only a single active barrier line when mapped against triggers TE07 and TE15. This condition eliminates defense-in-depth redundancy and increases the system's susceptibility to penetration.

Because absolute barrier reliability ($ef_i = 1$) is unattainable in operational environments, safeguards BC055, BC018, and BC057 represent critical common-cause vulnerabilities for threat vectors TH01 and TH33. To systematically analyze these vulnerabilities, the safety barriers must be disaggregated by structural system type, as shown in Figure 21.

Because barriers BC055 (competence assurance review) and BC018 (pre-use equipment inspection) are classified as intangible administrative safeguards, they are highly sensitive to operational erosion and human performance variability.

Activation Time (medium criticality):

- **System failure:** Premature, delayed, or completely omitted safeguard activation during the mobilization window.
  - BC055: N/A
  - BC018: N/A
- **Human error:** Late or premature execution of the action.
  - C018: Operational inspection executed at an inappropriate time.

- BC055: Competence review executed at incorrect intervals, allowing unqualified operators to bypass verification loops.

Threats	Factors							TOP EVENT	Hazards
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts		
TH01					BC055	BC059	BC018	TE02	H-08.01
							BC018	TE07	
					BC055			TE15	
TH25					BC027 BC054 BC055	BC028 BC059		TE02	
					BC027 BC054 BC055	BC028 BC059		TE15	
TH32					BC057		BC018	TE02	
					BC057		BC018	TE07	
TH33					BC057			TE02	
					BC057			TE07	
TH34					BC054	BC056		TE02	
					BC054	BC056		TE15	
TH35					BC027 BC054	BC059		TE02	
					BC027 BC054	BC058 BC059		TE15	
TH49					BC027 BC052	BC088		TE02	
					BC027 BC052	BC088		TE07	

Figure 20. Discretized vulnerability map for hazard H-08.01 displaying breakdown by independent threat-trigger pathways. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. One barrier can cover more than one threat scenario.(Source: Authors' elaboration).

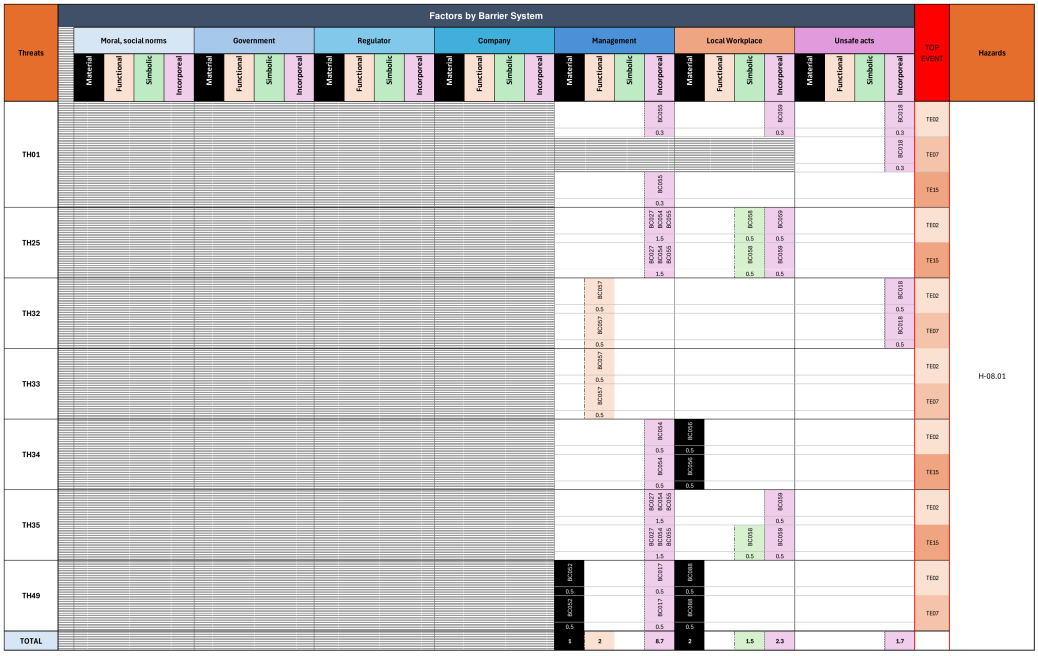

Figure 21. Defensive network for hazard H-08.01 disaggregated by physical, administrative, and intangible barrier typologies. It has been colored the barriers depending on its type where Black is Material-Physical barrier, Light Orange Functional, Green symbolic and Pink Incorporeal. (Source: Authors' elaboration).

Object (medium criticality):

- **System failure:** Safeguard functions directed toward an incorrect equipment asset or worker cohort.

- BC018: N/A
- BC055: N/A

- **Human error:** Action applied to the incorrect object.
  - BC018: Pre-use inspection checklist inadvertently applied to an irrelevant machinery class or asset variant.
  - BC055: Technical competence assessment administered to personnel not actively involved in high-consequence operations.

Sequence (high criticality):

- **System failure:** Concurrent execution of interdependent safety functions in an incorrect or non-linear order.
  - BC018: N/A
  - BC055: N/A
- **Human error:** Actions performed in the wrong sequence.
  - BC018: Inspection executed using rigid checklists that incentivize rote completion, inducing errors in step order.
  - BC055: Logic fault within the verification matrix where training requirements or personnel records are misaligned, excluding critical operators from the mandatory qualification loop.

To quantify the risk-reduction dynamics of the safety management system, optimized residual barriers (ACs) are integrated into the network topology, as illustrated in Figure 22.

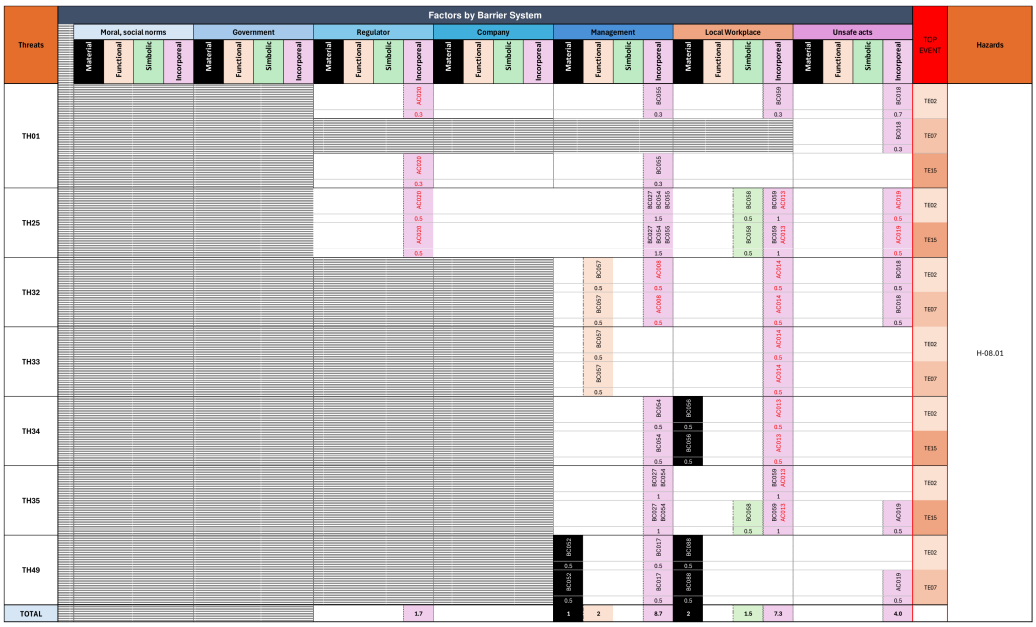

Figure 22. Optimized residual safety network for hazard H-08.01 incorporating additional validation barriers. It has been colored the barriers depending on its type where Black is Material-Physical barrier, Light Orange Functional, Green symbolic and Pink Incorporeal. (Source: Authors' elaboration).

This updated network state demonstrates targeted reinforcement across the primary system vulnerabilities, particularly along threat pathways TH32 and TH33. The integration of two secondary safeguards—C013 (equipment acceptance assurance prior to site mobilization) and AC014 (field verification of regulatory certifications and mandatory maintenance compliance)—introduces an independent validation layer. These residual controls complement baseline barrier BC058 (maintenance records verification) and act as a preliminary screening filter upstream of the pre-use inspection (BC018). If the sharp-end

inspection (BC018) fails due to human error, barriers AC013 and AC014 significantly reduce the joint probability of a path of opportunity materializing.

However, the topology reveals a lingering vulnerability: no residual barriers have been deployed for threat vector TH01 when coupled with initiating event TE07. This contrasts with pathways TE02 and TE15, which were optimized using barrier AC020. This gap exposes the system to equipment failures caused by improper handling, poor preservation, or exceeding safe operating limits. The additional barriers identified include complementary verifications, though without clearly defined execution responsibilities, leaving the action dependent on operator experience. This lack of structural assignment prevents an effective defense against threat TH01 when triggering event TE07, leaving a mathematically significant vulnerability in the defense-in-depth model.

While the semi-quantitative HAZID model indicates a risk reduction from Moderate to Minor—driven by a drop in the conditional likelihood parameter from L = 3 to L = 2—the persistent competence vulnerabilities identified in Figure 22 require ongoing auditing to ensure the long-term integrity of the safety management system.

5.1.2. Recommendations for Engineering Improvements (Rotary and Mobile Equipment):

To address the critical maintenance and pre-use inspection vulnerabilities identified for heavy rotary equipment, the following engineering improvements are proposed:

- **Administrative Automation (Mobilization Lock):** Deploy a GPS-enabled, automated equipment mobilization and acceptance system (AC013). This system automatically locks out machinery from operating on-site if its pre-mobilization acceptance records are incomplete or out of date.
- **Targeted Maintenance Verifications:** Establish an independent maintenance logging verification protocol (**AC014**) that utilizes barcode scanning of physical components, ensuring that routine equipment pre-use checks (**BC018**) are physically conducted on-site rather than completed as a rote checking exercise.
- **Physical and Functional Safeguards (TH01-TE07 Loop):** Address the lingering vulnerability of equipment failure under threat **TH01** by retrofitting machinery with active physical guarding and sensor-based interlocks (**AC020**) that automatically cut power to rotating components if a protective guard is breached or bypass is attempted, reducing human dependency.

5.2. Topological Characterization of Maximum-Vulnerability Architectures

To visually map the structural weaknesses within an asset's protective framework, this section evaluates specialized maximum-vulnerability network diagrams. These models integrate macro-level organizational risk factors with granular, system-specific barrier typologies. By mapping these cross-layer dependencies, the model isolates critical failure trajectories that form stochastic penetration pathways between initial threat vectors (THXX) and cascading initiating events (TEXX).

Rather than relying on simple qualitative tables, this topological approach translates complex barrier networks into a clear prioritization hierarchy for safety-critical elements. It highlights safeguards whose individual degradation or operational failure would lead to a widespread collapse of the defense-in-depth architecture. This methodology aligns with the high-reliability organization (HRO) and risk management standards established in ISO 31000 [21], which emphasize the systematic reinforcement of weak nodes via structural redundancy, multi-layered validation loops, and continuous feedback metrics.

By modeling these variable dependencies, this framework yields a high-fidelity estimation of the localized risk exposure characteristic of active industrial operations. Evaluating these topological parameters provides a realistic simulation of systemic behavior when sub-

jected to real-world threats. This empirical resolution is essential for executing data-driven optimization strategies aimed at improving asset resilience, in strict compliance with the continuous improvement loops mandated by ISO 31000 [21].

These models have been captured in configuration for inherent risk as shown in the Figure 23 by risk factor covered and Figure 24 by number of barriers by risk factor and for residual risk in the Figure 25 by risk factor covered and Figure 26 by number of barrier by risk factor. When breaking down these configurations adding the type of barriers, a master maximum-vulnerability network architecture aggregated by individual hazard node, can be generated showing the actual vulnerabilities of the system (Figure 27).

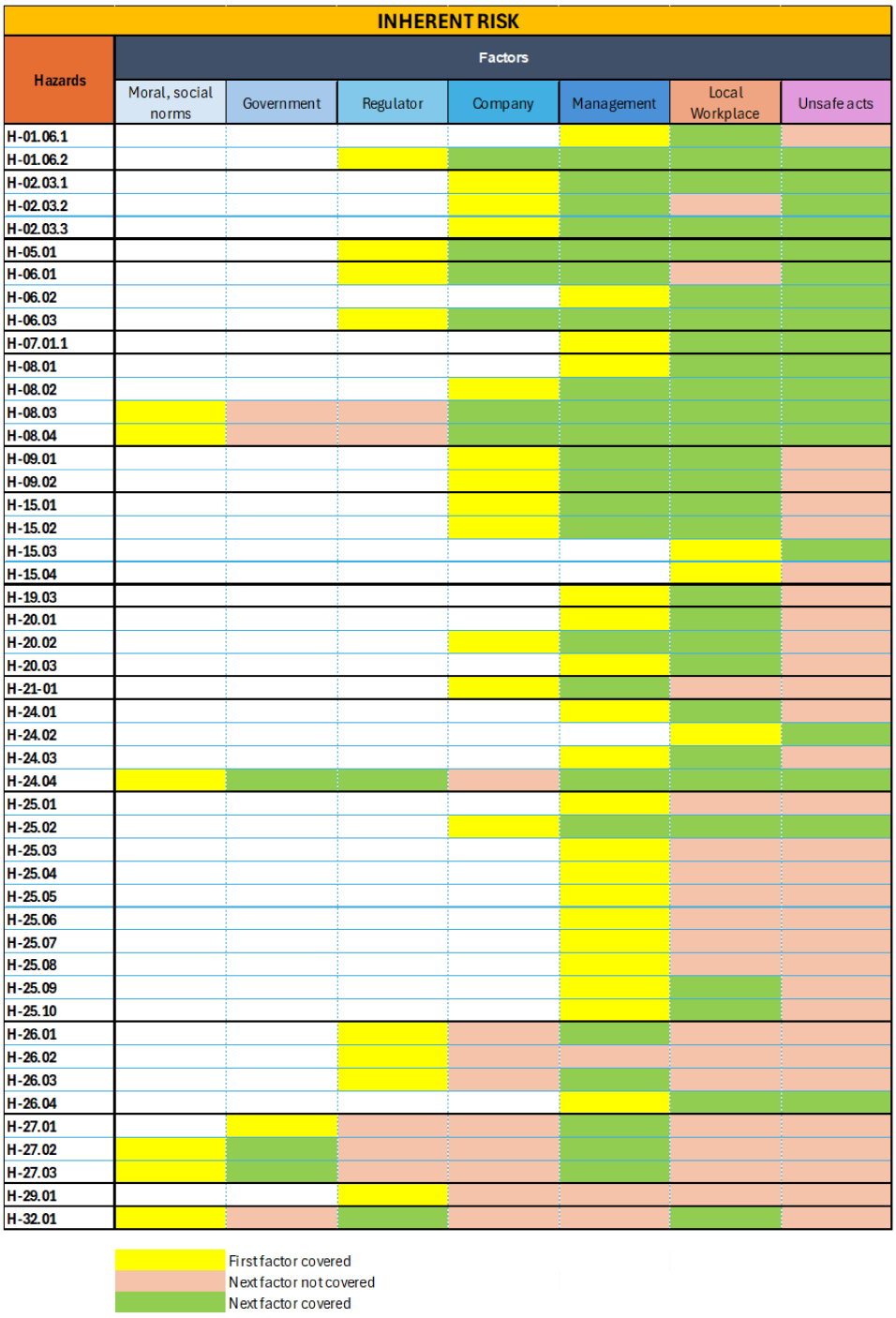

Figure 23. Inherent configuration layout mapping global process hazards and risk factors across distinct operational barrier sub-systems (Source: Authors' elaboration).

INHERENT IRSK - MAX VULNERABILITY								
Threats	**Factors**							**Hazards**
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH05					1	3		H-01.06.1
TH08			1	2		3	1	H-01.06.2
TH02					1		1	H-02.03.1
TH03						1	1	H-02.03.2
TH01				1	1		1	H-02.03.3
TH14						1	1	H-05.01
TH17							1	H-06.01
TH21						1		H-06.02
TH24						1		
TH27						2	1	H-06.03
TH01						1		H-07.01.1
TH33					2			H-08.01
TH32							2	H-08.02
TH40					2	2		H-08.03
TH40					2	2		H-08.04
TH41					2			H-09.01
TH41					6			H-09.02
TH01				2		2		H-15.01
TH01				2		2		H-15.02
TH18						1		H-15.03
TH01						1		H-15.04
TH50						2		H-19.03
TH01					2			H-20.01
TH52					2			
TH53					2			
TH55						1		H-20.02
TH01						2		H-20.03
TH56				1	1			H-21-01
TH02						2		H-24.01
TH01						1		H-24.02
TH59					3	3		H-24.03
TH65					1	2	3	H-24.04
TH01					1			H-25.01
TH49					1			
TH55					1			
TH68				1	2	1	1	H-25.02
TH01					1			H-25.03
TH49					1			
TH69					1			
TH01					1			H-25.04
TH49					1			
TH69					1			
TH01					1			H-25.05
TH49					1			
TH69					1			
TH01					1			H-25.06
TH01					1			H-25.07
TH69					1			
TH01					1			H-25.08
TH01					4			H-25.09
TH01					4			H-25.10
TH72			1		1			H-26.01
TH72			1					H-26.02
TH72			1		1			H-26.03
TH01					1			H-26.04
TH72		1			1			H-27.01
TH74	2							H-27.02
TH72	2	1			1			H-27.03
TH75			1					H-29.01
TH70	1							H-32.01

Figure 24. Specialized threat propagation vectors intercepted by defensive layers where the primary risk factor is located closest to the sharp-end human–machine interface. The cells are colored yellow when only one barrier applies and green when more than one barrier applies in order to clear identify where there is only one barrier. The greater the number of barriers, the greener the cell is. (Source: Authors' elaboration).

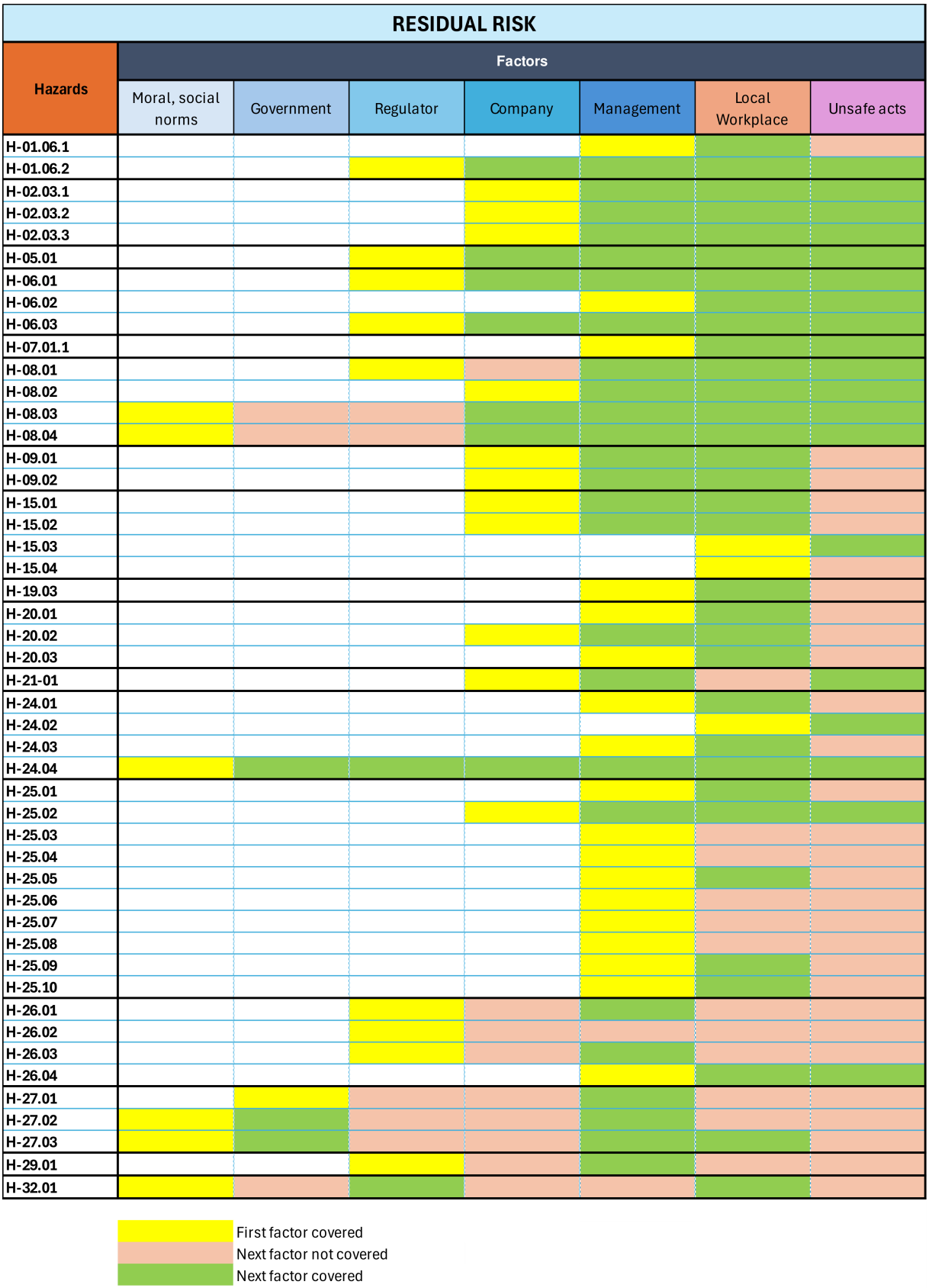

Figure 25. Cross-layer structural density matrix mapping hazard profiles against the failure modes of the underlying safety-critical systems. (Source: Authors' elaboration).

RESIDUAL RISK - MAX VULNERABILITY								
Threats	**Factors**							**Hazards**
	Moral, social norms	Government	Regulator	Company	Management	Local Workplace	Unsafe acts	
TH05					1	5		H-01.06.1
TH09			1	1	2	3	1	H-01.06.2
TH02					3	1	1	H-02.03.1
TH03					2	2	1	H-02.03.2
TH01				1	1	1	1	H-02.03.3
TH14						1	1	H-05.01
TH17						1	1	H-06.01
TH27						3	1	H-06.02
TH27						3	1	H-06.03
TH01						1		H-07.01.1
TH33					2	2		H-08.01
TH33						2		H-08.02
TH40					2	4		H-08.03
TH18				2		6		H-08.04
TH41					2			H-09.01
TH41					6			H-09.02
TH01				2		4		H-15.01
TH01				2		4		H-15.02
TH18						1		H-15.03
TH01						2		H-15.04
TH50						2		H-19.03
TH52					2			H-20.01
TH55						1		H-20.02
TH01						3		H-20.03
TH56				1	1		1	H-21-01
TH02						3		H-24.01
TH01						1		H-24.02
TH59					3	4		H-24.03
TH65					2	2	3	H-24.04
TH49					1			H-25.01
TH55					1			
TH68				1	2	1	1	H-25.02
TH01					1			H-25.03
TH49					1			
TH69					1			
TH01					1			H-25.04
TH49					1			
TH69					1			
TH01					1			H-25.05
TH69					1			
TH01					1			H-25.06
TH01					1			H-25.07
TH69					1			
TH01					1			H-25.08
TH01					4			H-25.09
TH01					6			H-25.10
TH72			1		1			H-26.01
TH72			1					H-26.02
TH72			1		1			H-26.03
TH01					1			H-26.04
TH72		1			1			H-27.01
TH74	2							H-27.02
TH72	2	1			1	2		H-27.03
TH75			1		2			H-29.01
TH70	1							H-32.01

Figure 26. Dynamic modification mapping threat-containment lines located closest to human performance interfaces, highlighting integrated residual barrier optimizations (ACXX) in red. (Source: Authors' elaboration).

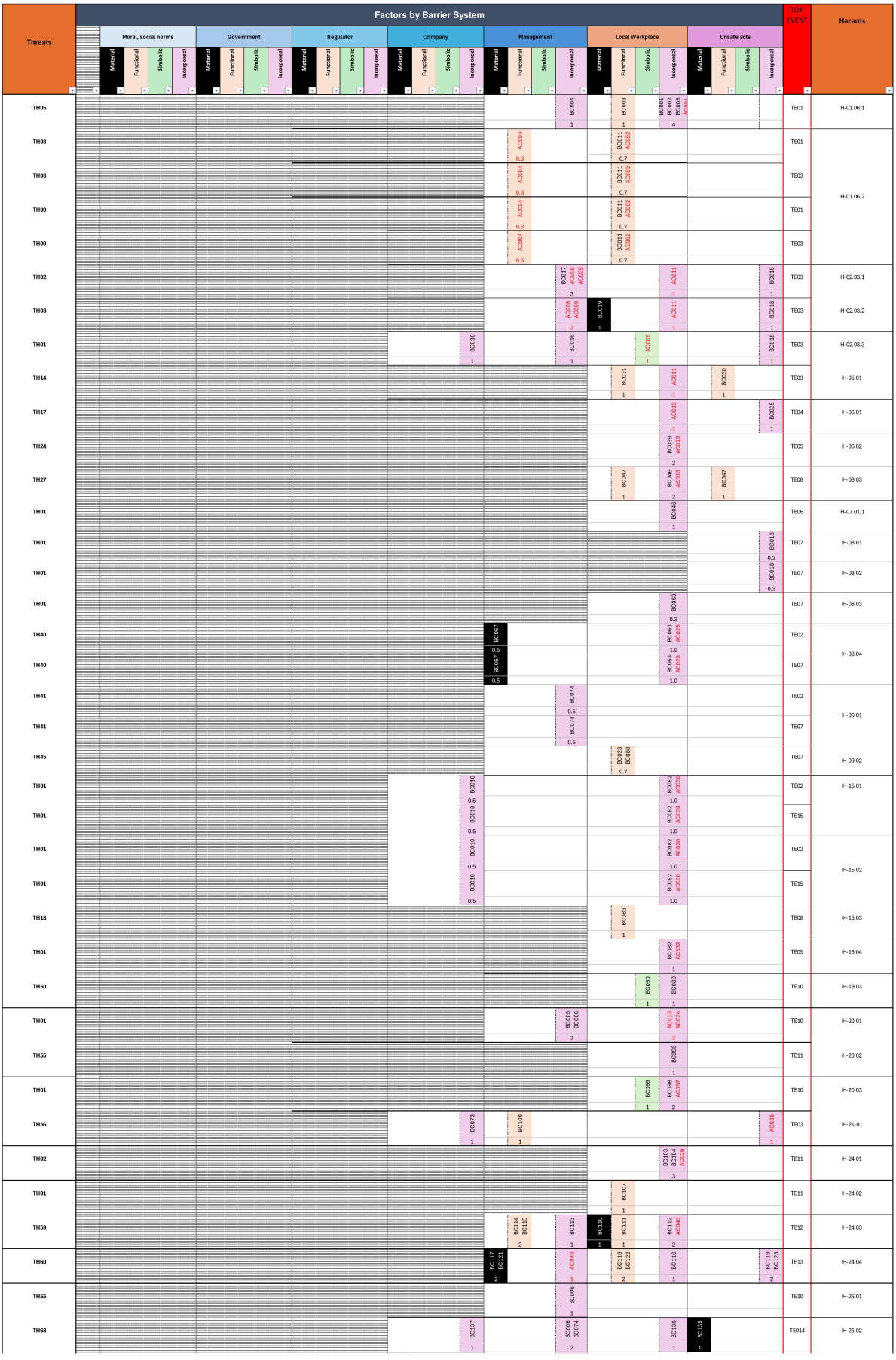

Figure 27. *Cont.*

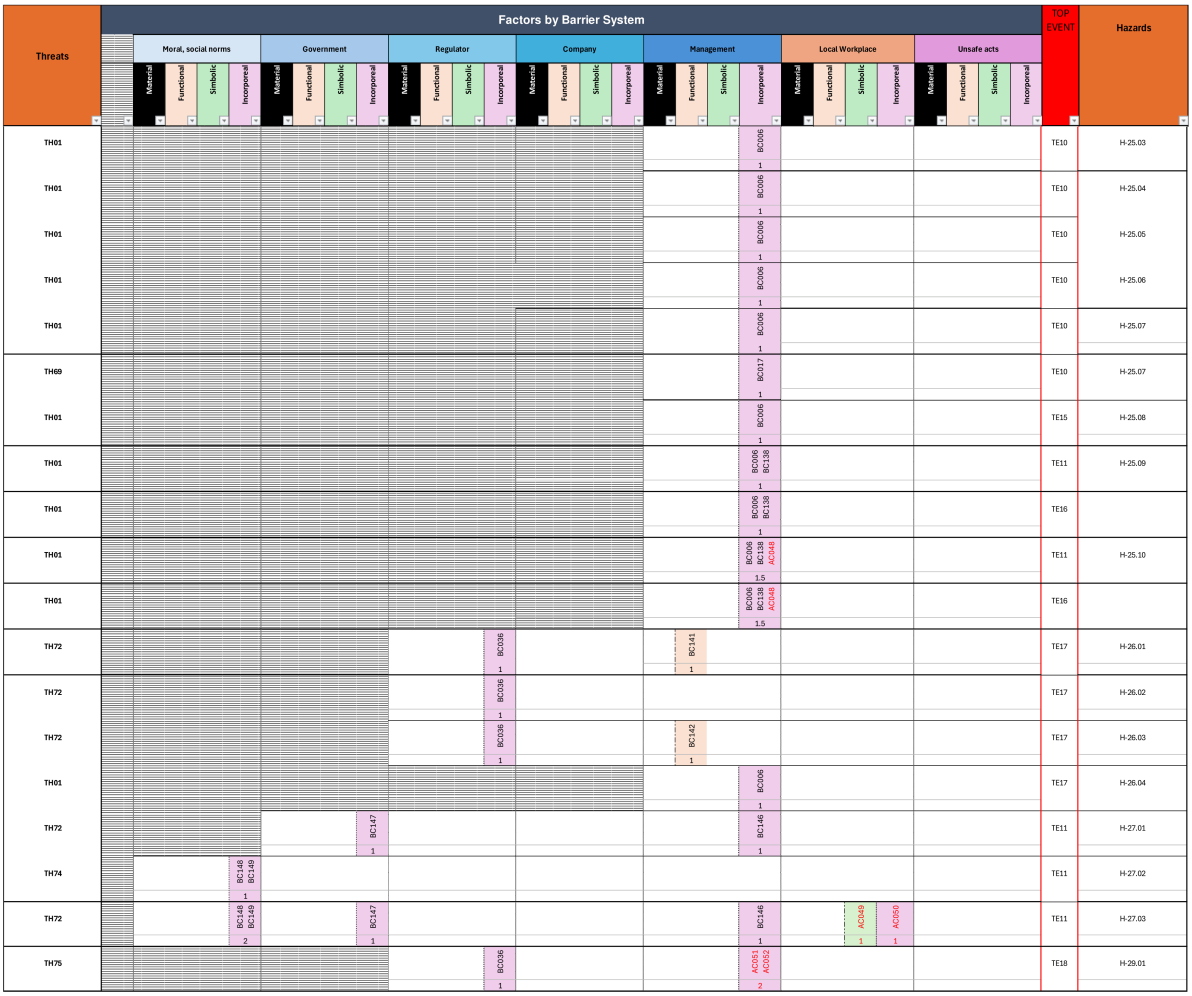

Figure 27. Master maximum-vulnerability network architecture aggregated by individual hazard node, establishing explicit paths between threats and active protective barriers classified by its type. (Source: Authors' elaboration).

The primary benefit of these maximum-vulnerability networks is their ability to reveal zero-redundancy pathways, where a single safety barrier stands as the solitary constraint between an active threat vector and a catastrophic hazard release. Within process safety engineering, these uncoupled configurations represent severe structural vulnerabilities.

The absence of independent protection layers (IPLs) exposes the asset to unmitigated sequential failure cascades, drastically increasing the cumulative probability of system breach. Systematically isolating these single-barrier pathways allows asset integrity managers to identify critical failure nodes and prioritize corrective maintenance resource allocation, satisfying the risk reduction and resilience criteria defined in the ISO 31000 [21] standard.

Human-Centric Conditional Dependence in Administrative Barriers

Unlike physical and functional safeguards, administrative and intangible barriers are subject to severe human-centric conditional dependence. If a threat trajectory is secured by two consecutive administrative verifications—such as a competence review (BC055) followed by a pre-use inspection checklist (BC018)—their failure probabilities cannot be treated as stochastically independent. Shared organizational pathogens, including scheduling pressure, occupational fatigue, and habituation, create a strong positive correlation in their failure modes. If an operator misses a critical step during the initial task due to routine bias, they are stochastically more likely to repeat the omission during subsequent checks. This cognitive coupling acts as a virtual shared constraint across the threat-trigger

pathway. Applying the conditional probability reduction established in Case Scenario A (Section Stochastic Modeling of the Penetration Trajectory: The Path of Opportunity Probability), once adjacent administrative safety functions are stochastically coupled by these shared organizational pathogens, the joint penetration probability collapses directly to the unreliability of that coupled sequence, as modeled conceptually by the shared constraint in Equation (14). This structural degradation transforms a nominally multi-layered safety margin into an active Single Point of Failure (SPOF). The MVD framework explicitly flags these adjacent administrative clusters, alerting safety managers to insert independent physical or functional barriers (such as sensor-based machinery guards AC020) to break this cognitive coupling [24–26].

6. Conclusions

This study demonstrates that maximum-vulnerability topologies provide a robust, scalable extension to barrier-based process safety management by exposing the specific propagation pathways through which low-level threat vectors cascade into initiating events and catastrophic hazard releases. While traditional Hazard Identification (HAZID) protocols evaluate protection performance at an aggregate, hazard-siloed level, the framework developed introduces a granular deconstruction at the explicit threat-initiating event interface. This structural resolution uncovers hidden defects in defense-in-depth layouts, barrier compatibility vectors, and spatial protection placements, offering asset integrity managers an objective mathematical basis for identifying systemic vulnerabilities.

A core finding of this research indicates that the absolute volumetric count of deployed safeguards is a misleading indicator of systemic resilience. True defensive robustness is governed by whether specific independent protection layers (IPLs) possess localized operational compatibility with the threat dynamics they intercept, how they are distributed across the socio-technical hierarchy, and their susceptibility to common-cause degradation or active human errors. By discretizing safeguards based on architectural typology, socio-technical position, and latent failure modes, maximum-vulnerability networks yield a high-fidelity estimation of defensive performance that challenges traditional, linear risk-matrix aggregations.

The empirical case applications confirm that minor configurations in barrier assignment can trigger non-linear shifts in global system vulnerability. Specifically, single-barrier pathways, defenses clustered exclusively at the terminal operational stages (sharp-end execution), and protection loops coupled with human reliability boundaries represent critical failure points within the defensive envelope. The analytical mapping proposed systematically directs engineering attention toward these high-centrality nodes, where marginal component degradation causes a disproportionate escalation in systemic exposure. This structural visibility allows for targeted resource allocation across maintenance, continuous monitoring, and engineering redesign.

From a safety governance perspective, this framework transitions organizational risk management from passive, static inventory verification toward active, predictive barrier resilience. It allows safety engineers to isolate systemic weaknesses before they manifest as active failures, evaluate the objective risk-reduction margins of proposed residual interventions, and align mitigation strategies with the core principles of redundancy, resilience engineering, and continuous improvement mandated by international frameworks like ISO 31000 [21]. In practice, maximum-vulnerability architecture optimizes decision-making across four operational dimensions:

- **Topological Transparency:** Exposing latent threat-initiating event propagation trajectories that remain obscured within macro-level, hazard-focused risk assessments.

- **Dynamic Prioritization:** Prioritizing critical safeguards for safety-critical maintenance and inspection based on their structural network weight rather than generic hazard risk classification labels.
- **Redundancy Validation:** Providing a predictive testbed to verify whether newly introduced residual barriers (ACXX) deliver authentic common-cause decoupling or merely introduce redundant administrative noise.
- **Socio-Technical Integration:** Explicitly incorporating human, behavioral, and organizational factors into barrier design and health-monitoring frameworks.

More broadly, this methodology establishes a replicable and reliable framework for upgrading barrier management in high-consequence industrial facilities. Future research vectors should focus on integrating live quantitative performance indicators (QPIs) and industrial IoT operational data directly into these network models to achieve real-time, dynamic risk monitoring. Ultimately, maximum-vulnerability topologies do not replace but significantly enrich standard HAZID and bow-tie protocols, providing a mathematical foundation for risk-informed, structurally resilient industrial operations.

6.1. Structural Mechanisms of Latent Vulnerability

Traditional semi-quantitative process hazard analyses routinely fail to detect systemic vulnerabilities due to two methodological flaws:

- **Structural Decoupling:** Safeguards are cataloged as flat inventories under generic hazard labels rather than being mathematically mapped to specific, independent threat-initiating event intersections.
- **Consequence-Severity Heuristics:** Asset management tracking programs prioritize inspection and maintenance resources based on the unmitigated risk scores of major hazards, ignoring the real-time probability evolution of secondary pathways when shared barriers fail.

Transitioning to a priority model governed by maximum-vulnerability topologies allows organizations to optimize systemic risk mitigation, maximizing accident prevention margins per unit of engineering effort. In standard risk assessment practices, high-consequence scenarios (e.g., hydrocarbon loss of primary containment in oil and gas processing) absorb the majority of design and auditing resources, leaving low-consequence or highly distributed operational risks (e.g., localized mechanical handling, ergonomic hazards, psychological fatigue vectors) severely under-protected. When a HAZID report leaves these secondary layers incomplete, the undetected vulnerabilities must be reactively managed during live operations. This structural failure introduces two severe systemic problems:

- **Sharp-End Cognitive Friction:** It introduces unplanned, manual monitoring workloads for frontline operators and area supervisors, who must construct reactive workarounds to manage unmapped process sensitivities.
- **Resilience Over-Reliance:** It shifts the entire risk burden away from engineered barriers and forces a reliance on micro-adaptive human performance, individual technician expertise, and frontline stress tolerance. This systemic reliance accelerates human error rates under tight operational schedules.

Maximum-vulnerability models neutralize this systemic bias by shifting focus away from consequence-driven severity metrics to evaluate the structural probability of initiating events, regardless of the hazard node they trigger. Because the overarching industrial target is zero-harm performance, eliminating the structural vulnerabilities of minor hazard pathways is essential. Importantly, this model remains complementary to classical process safety techniques; because every node, barrier archetype, and threat trajectory is compre-

hensively coded within a structured data schema, engineers can filter the master topology to isolate maximum-vulnerability pathways nested exclusively within high-consequence asset envelopes.

6.2. Safeguard Efficiency Dynamics and Network Constraints (Barriers)

The implementation of maximum-vulnerability models requires a structured alphanumeric coding matrix for all protective barriers. This data framework allows for automated scanning to isolate critical threat propagation loops where defense-in-depth is compressed to thin margins. By establishing this explicit traceability across systemic threats and initiating events, risk managers can model how changes in a single barrier's availability propagate across the entire multi-hazard network.

Let $\eta_i \in [0, 1]$ define the operational efficiency (reliability) of barrier B_i. In an idealized, stochastically decoupled safety layer where parallel protection barriers share identical target performance targets, the aggregate unreliability of the containment envelope satisfies a joint failure distribution. To suppress the probability of a path of opportunity materializing below a strict process threshold of $P(Breach\} < 5\%$, the required individual barrier performance curves scale non-linearly with barrier density. In highly compressed protection networks with low barrier density, the performance targets for individual nodes scale dramatically.

This mathematical relationship guides the optimization of barrier health monitoring programs. If a specific safeguard Bk is multiplexed across several threat pathways, yet acts as a single point of failure within an uncoupled threat-initiating event intersection, the mathematical safety margin requires its individual target efficiency to be maintained at ηi $\geq 95\backslash\%$. This node is automatically classified as a Safety-Critical Element (SCE), requiring prioritized maintenance testing and field inspection.

To accurately model this risk distribution, the framework integrates two operational parameters:

- **Typological Wear Degradation:** As established in human–machine systems frameworks [13,15], safeguard reliability degradation profiles depend on whether their underlying architecture is material (physical structures), functional (interlocks, automated loops), symbolic (signage, warnings), or intangible (training, operational procedures). While real-time degradation fields are often unmapped due to industrial data constraints, their explicit failure modes can be structurally anticipated and neutralized.
- **Socio-Technical Proximity (Blunt-to-Sharp End Axis):** Safeguards must be classified by their organizational proximity to the active process workspace. As mapped across the socio-technical hierarchy, the ability of frontline personnel to influence barrier integrity decreases the further a safeguard is located from the point of execution (e.g., a high-level corporate management-of-change procedure cannot be dynamically adjusted by a site operator to remedy a live process anomaly). Unoptimized administrative systems often generate severe frontline operational delays by requiring field teams to execute complex Change Management reviews to address minor procedural mismatches. These administrative burdens should be structurally resolved during the pre-execution design phase.

Maximum-vulnerability networks integrate these two dimensions, allowing risk analysts to evaluate not only absolute barrier densities but also the qualitative durability and structural proximity of the defensive systems. This is mathematically essential when quantifying joint penetration probabilities, where a single uncoupled barrier completely dictates the failure path of the entire asset safety envelope.

6.2.1. Influence of Barrier Typology on Failure Acceleration

Intangible and symbolic safeguards exhibit high failure variance and low operational reliability due to their tight coupling with human cognitive variability and active execution errors. If a maximum-vulnerability analysis reveals a single-barrier pathway governed exclusively by an intangible control, the localized system state is highly unstable. It remains highly vulnerable to operational erosion, shift-handover information losses, and unconscious diagnostic errors.

Identifying these intangible single points of failure during the initial inherent-risk mapping phase allows design engineers to deploy immediate physical or functional redundancies, closing the path of opportunity before site mobilization. If left unresolved, the asset enters live operations with an unmitigated latent failure vector dependent on a highly volatile human-centric control.

Conversely, when a single-barrier pathway is governed by a material or functional safeguard (which possesses higher baseline reliability indices), the optimization strategy shifts. Here, the analysts should deploy online condition-monitoring systems (e.g., diagnostic telemetry, process alarms) or establish targeted intangible verification loops (e.g., predictive maintenance schedules, specialized calibration audits) to safeguard its structural integrity.

In configurations where a critical pathway relies on two consecutive intangible barriers, this clustering indicates a severe lack of defensive depth. From a cognitive engineering perspective, consecutive administrative barriers (such as a pre-use inspection BC018 followed by a supervisor sign-off BC036) exhibit strong positive correlations in their failure modes due to shared organizational factors (such as shift fatigue, routine bias, and time pressure). If an operator suffers a cognitive lapse and misses a defect during inspection, the supervisor is stochastically more likely to sign off the permit as a rote compliance exercise without physical verification [24,26]. To mathematically model this conditional human dependency, we define the conditional probability of failure of the second administrative barrier B_2 given the failure of the first B_1 as:

$$P(B_2|B_1) = (1-\beta)\cdot P(B_2) + \beta; \forall \beta \in \mathbb{R}; \beta = [0,1] \quad (16)$$

represents the coupling factor determined by organizational stress and cognitive workload. Under high fatigue regimes ($\beta \to 1$), the failure of the second barrier becomes almost certain once the first fails, collapsing the independent defense-in-depth model. This common-cause vulnerability is significantly reduced by introducing an orthogonal, physical or automated barrier (such as a sensor-based interlocking guard, AC020) which is stochastically uncoupled from human cognitive variability. Systemic maximum vulnerability is therefore a multi-variable function of both barrier density and structural typology.

6.2.2. Influence of Organizational Risk Factors on Defensive Balance

Categorizing safety barriers by their structural risk factors defines their operational flexibility and capacity for continuous improvement. Safeguards located at the blunt end of the socio-technical spectrum (e.g., corporate frameworks, multi-site administrative standards) are highly rigid and slow to adapt to changing field realities. For example, corporate operating procedures seek to standardize performance by capturing all theoretical field variations. However, if a procedure lacks field accuracy, is decoupled from site constraints, or introduces unmanageable administrative steps, its operational efficiency drops significantly. If a HAZID study assumes complete procedural compliance without evaluating real-world field applicability, it generates a false sense of security. In practice, these overly restrictive procedures are routinely bypassed, with frontline personnel relying on ad hoc, unverified instructions to maintain operational continuity.

Maximum-vulnerability models explicitly flag these distant, intangible safeguards. When a threat vector relies solely on blunt-end administrative controls, the model indicates an urgent requirement to deploy localized safeguards closer to the sharp end (Management or Local Workplace levels) to operationalize corporate instructions.

Properly designed blunt-end barriers serve as mandatory variability filters that limit unsafe behavioral permutations and establish a safe operational baseline. A high-reliability protection architecture requires a balanced distribution of safeguards across both the blunt and sharp ends of the organization. For instance, a high-level corporate procedure should define core safety goals with limited technical detail. This blunt-end policy is then operationalized by site-specific task instructions (Workplace or Management factors), reducing behavioral variance and eliminating unsafe execution paths before an operator interacts with the machine interface.

This balanced layout is essential for optimizing human performance and managing the role of technical experience. When a process system lacks blunt-end protective filters, the entire risk burden falls on the operator's real-time problem-solving capacity and technical experience, increasing cognitive fatigue and error rates. Balancing safeguards across organizational levels reduces system complexity and minimizes performance slips, provided the underlying blunt-end structures are technically accurate and validated by field operations.

6.3. Systematic Execution Methodology

This analytical methodology is deployed prior to finalizing the process risk registry. It targets the prevention of initiating events (TEXX), focusing on structural probability minimization rather than retrospective consequence mitigation. The standardized execution workflow consists of nine discrete phases:

- **Baseline HAZID Screening:** Conduct a standard HAZID workshop to map initial safeguard layers across identifying hazard sources, threat vectors, and primary consequences.
- **Alpha-Numeric Code Mapping:** Convert the qualitative hazard register into a relational database by assigning explicit alpha-numeric codes to all threats (THXX), initiating events (TEXX), and safety barriers (BCXXX/ACXX).
- **Topological Diagram Construction:** Construct the baseline maximum-vulnerability network diagram, mapping all valid threat-initiating event pairs and plotting their active safeguards across barrier typologies and organizational risk factors.
- **Single-Barrier Isolation Loop:** Scan the network matrix to isolate all threat-initiating event paths governed by a single safety barrier. Analyze these critical nodes based on their typological fragility and socio-technical distance to quantify their failure sensitivity.
- **Dual-Barrier Vulnerability Scan:** Scan the network matrix to identify all paths containing exactly two safety barriers, evaluating their common-cause coupling and common failure modes.
- **Tri-Barrier Density Boundary:** Expand the scan to paths containing exactly three safety barriers. Analytical Tractability Threshold: To avoid combinatorial explosion and prevent analytical paralysis during data processing, structural iteration stops at a barrier depth of three. This boundary ensures optimal engineering returns without adding non-value-added data complexity.
- **Targeted Residual Optimization:** Deploy optimized residual safety barriers (ACXX) to reinforce weak nodes, using the barrier efficiency matrices to balance risk reduction performance. Engineering interventions must prioritize:

- Re-engineering or providing redundancy for solitary intangible barriers inside high-sensitivity pathways.
- Verifying and validating the operational accuracy, audit history, and field compliance of blunt-end administrative controls.

- **Residual HAZID Finalization:** Re-engage the HAZID assessment loop to compute the final, audited residual risk metrics (C, L, and R) across all stabilized process systems.
- **Frontline Network Delivery:** Regenerate the optimized maximum-vulnerability network diagram and deliver it directly to the field operations team as a visual tool for prioritizing safety-critical maintenance and inspection tasks.

Implementing this framework requires a structured expert panel comprising process safety engineers, control systems technicians, and human factors specialists to ensure accurate classification of threat-initiating event pairs.

While the detailed mapping of threat-barrier couplings demands rigorous documentation, the associated resource expenditure is actively minimized by streamlining redundant HAZID steps; specifically, once a preventive barrier successfully blocks an upstream threat trajectory, extensive qualitative descriptions of downstream consequence propagation can be omitted. To address the operational reality of missing or incomplete data under industrial constraints, a conservative default-value protocol is established: any undocumented barrier or safeguard with unmeasured performance is assigned a baseline operational efficiency of $e_{fi} = 0$. This boundary state remains active until physical verification, field audits, or historical maintenance logs are provided, preventing the artificial overestimation of systemic safety margins and ensuring that subsequent risk optimization is grounded strictly in verified defenses.

6.4. Mathematical Synthesis of Interdependent Systemic Risk

Conventional HAZID models present major limitations by calculating risk profiles across isolated, independent hazard rows. This approach fails to capture the interdependent network topologies where shared safeguards and cross-cutting threats overlap. Deploying maximum-vulnerability models resolves these limitations by introducing joint probability distributions across dependent safety layers, providing asset managers with a high-fidelity estimation of true systemic risk exposure.

Furthermore, by applying the mathematical simplifications derived for both shared safeguards (**Case Scenario A**) and stochastically independent barriers (**Case Scenario B**), safety engineers can quickly calculate baseline risk exposure metrics for high-density plant environments. This mathematical framework underscores a critical process safety principle: the systemic reliability of an industrial operation is fundamentally governed by the performance of its single-barrier pathways. Enhancing the individual efficiency parameters (η_i) of these high-centrality nodes provides the highest return on safety investment, stabilizing the entire defensive architecture against catastrophic failure cascades.

6.5. Retrospective Framework Validation

To validate the predictive utility of the Maximum-Vulnerability Diagram, a retrospective benchmark was conducted against historical performance data from a major operating asset over a 3-year operational window. The analysis revealed that all recorded loss-of-control and equipment damage incidents occurred along pathways mapped with a barrier density of $n = 1$ (single-barrier pathways) or where the defensive sequence relied entirely on consecutive, uncoupled intangible barriers (e.g., pre-use inspections and training verifications). While traditional HAZID had masked these risk pathways by assigning a 'Moderate' rating based on an aggregate safeguard count, the MVD framework successfully isolated these weak nodes prior to failure, demonstrating its predictive and diagnostic superiority.

Author Contributions: Conceptualization, N.P.T.M. and A.C.S.P.; Methodology, N.P.T.M.; Software, N.P.T.M.; Investigation, N.P.T.M.; Data curation, N.P.T.M.; Writing—original draft, N.P.T.M.; Writing—review and editing, A.C.S.P. and R.D.M.; Visualization, R.D.M. and F.J.P.T.; Project administration, F.J.P.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: The authors thank Fernando Ruiz Gomez, Raul Rioyo Rumayor and Farzad Rahnama for useful discussions.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Reason, J. *Human Error*; Cambridge University Press: Cambridge, UK, 1990.
2. Reason, J. *Managing the Risks of Organizational Accidents*; Ashgate Publishing Limited: Aldershot, UK, 1997.
3. Reason, J. *Organizational Accidents Revisited*; CRC Press: Boca Raton, FL, USA, 2016.
4. Reason, J.; Hollnagel, E.; Paries, J. *Revisiting the «Swiss Cheese» Model of Accidents*; European Organisation for the Safety of Air Navigation (EUROCONTROL): Brussels, Belgium, 2006.
5. Sklet, S. Safety barriers: Definition, classification, and performance. *J. Loss Prev. Process Ind.* **2006**, *19*, 494–506. [CrossRef]
6. Center for Chemical Process Safety (CCPS). *Guidelines for Barrier Management in Process Safety*; American Institute of Chemical Engineers (AIChE): New York, NY, USA; John Wiley and Sons: Hoboken, NJ, USA, 2018.
7. *ISO 17776:2016*; Petroleum and Natural Gas Industries—Offshore Production Installations—Major Accident Hazard Management During the Design of New Installations. International Organization for Standardization (ISO): Geneva, Switzerland, 2016.
8. Svenson, O. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Anal.* **1991**, *11*, 499–507. [CrossRef] [PubMed]
9. Svenson, O. Accident and incident analysis based on the accident evolution and barrier function (AEB) model. *Cogn. Technol. Work* **2001**, *3*, 42–52. [CrossRef]
10. Hale, A.; Goosens, L.; Ale, B.; Bellamy, L.; Post, J.; Oh, J.; Papazoglou, I.A. Managing safety barriers and controls at the workplace. In Proceedings of the Seventh International Conference on Probabilistic Safety Assessment and Management (PSAM 7), Berlin, Germany, 14–18 June 2004; pp. 14–18.
11. Hale, A.; Guldenmund, F.; Goosens, L.; Bellamy, L. *Risk Management and Human Reliability in Social Context*; EC Joint Research Center: Ispra, Italy, 2000.
12. Perrow, C. *Normal Accidents: Living with High-Risk Technologies*; Basic Books, Inc.: New York, NY, USA, 1984.
13. Hollnagel, E. *Barriers and Accident Prevention: Or How to Improve Safety by Understanding the Nature of Accidents Rather Than Finding Their Causes*; Ashgate Publishing Group: Aldershot, UK, 2004.
14. *ISO 31010:2019*; Risk Management—Risk Assessment Techniques. International Organization for Standardization (ISO): Geneva, Switzerland, 2019.
15. Hollnagel, E.; Woods, D.D.; Leveson, N. (Eds.) *Resilience Engineering: Concepts and Precepts*; Ashgate Publishing, Ltd.: Aldershot, UK, 2006.
16. Suchman, E. A conceptual analysis of the accident phenomenon. In *Behavioral Approaches to Accident Research*; Association for the Aid of Crippled Children: New York, NY, USA, 1961.
17. Lorenz, E. *The Essence of Chaos*; Routledge: London, UK, 2003.
18. Poincaré, H. *Calcul Des Probabilités*; Gauthier-Villars: Paris, France, 1912.
19. Macchi, L. A Resilience Engineering Approach for the Evaluation of Performance Variability: Development and Application of the Functional Resonance Analysis Method for Air Traffic Management Safety Assessment. Doctoral Dissertation, Politecnico di Milano, Milan, Italy, 2010.
20. Habberley, J.S.; Shaddick, C.A.; Taylor, D.H. *A Behavioural Study of the Collision Avoidance Task in Bridge Watchkeeping*; The College of Maritime Studies: Southampton, UK, 1986.
21. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
22. Occupational Safety and Health Administration (OSHA). *29 CFR Part 1926, Subpart M—Fall Protection*; U.S. Department of Labor: Washington, DC, USA, 2020.

23. Occupational Safety and Health Administration (OSHA). *29 CFR Part 1926, Subpart O—Motor Vehicles, Mechanized Equipment, and Marine Operations*; U.S. Department of Labor: Washington, DC, USA, 2021.
24. Fernández, J.B. *Incidencia Del Comportamiento Humano En Los Accidentes de Trabajo*; Confederación Española de Organizaciones Empresariales (CEOE): Madrid, Spain, 2018.
25. Navarro, J.L. Seguridad Basada en el comportamiento. In *Perspectivas de Intervención de Riesgos Psicosociales. Medidas Preventivas*; Nogareda, C., Gracia, D.Á., Martínez-Losa, J.F., Peiró, J.M., Duro, A., Salanova, M., Martínez, I.M., Merino, J., Lahera, M., Meliá, J.L., Eds.; Foment del Treball Nacional y Fundación para la Prevención de Riesgos Laborales: Barcelona, Spain, 2007; pp. 157–180.
26. Norman, D.A. *The Design of Everyday Things. Revised and Expanded Edition*; Basic Books: New York, NY, USA, 2013.