Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26121-cd

Learning from Offshore Well Accidents through Risk-Based Process Safety and Resilience Engineering

Helton Luiz Santana Oliveira

Department of Production Engineering, Federal Fluminense University, Brazil. E-mail: heltonsantana@id.uff.br

Gilson Brito Alves Lima

Department of Production Engineering, Federal Fluminense University, Brazil. E-mail: glima@id.uff.br

Over recent decades, large-magnitude offshore well accidents have exposed structural weaknesses in well integrity systems, operational discipline, and process safety governance, with significant impacts on people, the environment, and assets. These events reinforce the need for integrated approaches that move beyond predominantly reactive well-control practices. In this context, this article focuses on a systematic reassessment of landmark historical incidents, analyzing them through an integrated perspective that combines process safety, life-cycle well integrity, and asset governance. The study specifically emphasizes the combined application of the Risk-Based Process Safety (RBPS) model, the principles of ISO 16530, and the asset management framework of ISO 55001. The central problem addressed is the lack of a structured model that quantitatively integrates governance, engineering, and organizational learning, thereby enabling consistent, risk-based evaluation and anticipation of loss of well integrity. The objective of the article is to propose and demonstrate the applicability of the Risk-Based Integrity Resilience Model (RBIRM), which quantifies the Probability of Loss of Well Integrity and links process safety, integrity, and asset management indicators. The methodology is based on a structured analysis of RBPS elements, quantitative maturity mapping using historical probabilistic data, and modeling through Fault Tree Analysis and Bayesian Belief Networks. The results indicate a consistent evolution from reactive approaches toward proactive, data-driven integrity governance, with potential application in offshore systems.

Keywords: Risk-based process safety, offshore safety, resilience engineering, well integrity, reliability engineering

1. Introduction

Over four decades, major offshore well incidents—Ixtoc I (1979), Enchova (1988), Macondo (2010), and Elgin (2012) — have revealed systemic vulnerabilities in barrier reliability, operational discipline, and process safety governance. This article reexamines these emblematic events through an integrated framework that combines the Center for Chemical Process Safety (CCPS/AIChE) Risk-Based Process Safety (RBPS) model, the life-cycle well integrity principles established by ISO 16530, and the asset governance framework of ISO 55001.

A structured assessment of the 20 RBPS elements identified recurring deficiencies in Asset Integrity and Reliability, Management of Change, Operational Readiness, and Process Safety Culture. Quantitative maturity mapping was performed by assigning weighted failure frequencies to RBPS clusters, based on probabilistic data from the SINTEF, PSA, and INERIS blowout databases.

Based on these findings, the article introduces the Risk-Based Integrity Resilience Model (RBIRM), an organized framework that links governance, engineering, and learning layers. The RBIRM quantifies the Probability of Loss of Well Integrity (P-LWI) through Fault Tree Analysis (FTA) and Bayesian Belief Network (BBN) modeling, integrating historical frequencies with conditional dependencies. The model establishes a feedback loop connecting

Process Safety KPIs → Integrity KPIs → Asset Management KPIs, enabling predictive assurance and digital resilience analyses.

In addition, the RBIRM explicitly aligns with Hollnagel's four resilience potentials—respond, monitor, learn, and anticipate—embedding them within each RBPS pillar to enhance organizational adaptability and anticipatory capacity. This alignment operationalizes resilience engineering concepts in the context of well integrity and process safety.

The results indicate a historical transition from reactive well control toward proactive, data-driven integrity governance, supporting resilience engineering, digital assurance, and risk-informed decision-making in offshore systems. The RBIRM approach is scalable to FPSOs, geothermal wells, and CO_2 storage, providing a unified reliability-centered process safety foundation.

2. Research method

This study adopts an applied, analytical, and quantitative approach with a systemic and integrated focus, combining principles of process safety, well integrity, and asset governance. The methodological design was structured to reassess historical accidents, identify recurring weaknesses, and propose a quantitative model oriented toward organizational resilience.

Regarding objectives, the research is exploratory and explanatory, investigating failure patterns in major offshore incidents and explaining their causes through normative and probabilistic references. From a procedural standpoint, it constitutes documentary research with analytical modeling, based on consolidated historical data and formal risk analysis methods.

The empirical basis comprises records of relevant offshore incidents occurring between 1979 and 2012, selected based on information availability, technical impact, and regulatory relevance. Secondary probabilistic data from consolidated international blowout databases were employed as references for historical failure frequencies and initiating events.

Initially, a structured analysis of the 20 RBPS elements, organized into functional clusters, was conducted to identify recurring deficiencies related to asset integrity, management of change, operational readiness, and process safety culture. Subsequently, quantitative maturity mapping was performed by associating weighted historical frequencies with these clusters.

Based on these results, the RBIRM was developed to quantify the Probability of Loss of Well Integrity using Fault Tree Analysis and Bayesian Belief Networks. The model integrates process safety, integrity, and asset management indicators and incorporates organizational resilience potentials, providing support for risk-based decision-making in complex offshore s.

3. Summaries of Cases

This section presents summaries of the selected accident cases: Ixtoc I (1979), Enchova (1988), Macondo (2010), and Elgin (2012).

3.1. Ixtoc I Case (1979)

The Ixtoc I well accident occurred on June 3, 1979, in the Bay of Campeche, Gulf of Mexico, in approximately 50 m of water. The exploratory well, operated by Petróleos Mexicanos (PEMEX), experienced a blowout during drilling operations following loss of circulation and failure to effectively actuate the BOP.

The release persisted for approximately nine months, discharging about 3.3 million barrels of oil (≈525,000 m^3), ranking among the largest accidental oil spills in history. No confirmed fatalities were reported; however, severe damage occurred to the well and drilling rig, resulting in total asset loss, prolonged operational interruption, and significant business continuity impacts.

Environmental damage included extensive marine and coastal contamination in Mexico and the southern United States, affecting fisheries, tourism, and coastal ecosystems. Estimated economic losses reported in the literature range between USD 1 and 2 billion, including well control, containment, cleanup, and compensation.

Root causes included inadequate well control, deficiencies in BOP design and reliability, shortcomings in operational procedures, and risk management failures. Key recommendations emphasized improvements in well control, BOP redundancy and testing, management of change, operational training, and strengthened process safety governance.

The case was documented in official technical reports by the Mexican government and international organizations and is widely used as a historical reference in offshore drilling safety.

3.2. Enchova Case (1988)

The Enchova accident occurred on April 24, 1988, at the Enchova Central Platform (PCE-1) in the Campos Basin (RJ). The unit was operated by Petrobras. The event began during well conversion/recompletion (EN-19), when a high-pressure gas pocket caused a kick; the BOP failed to close the well, gas was released, and ignition occurred due to sparks associated with ejection/impact of the drill string, evolving into a blowout and fire lasting 31 days.

Public sources predominantly describe gas release without providing a consolidated, traceable estimate of the released volume. No fatalities occurred (evacuation).

Equipment/material damage included major destruction of the topsides and declaration of total loss; the production module was redesigned in approximately 45 days, with full restart in about 18 months.

Business continuity losses were estimated at USD 330 million (at the time) in the "100 Largest Losses" survey.

Typical recommendations included strengthened well control, BOP reliability and testing, management of change, operational readiness, ignition prevention barriers, and emergency response.

No public official investigation report with issuing authority and numbering was located in open sources; the case is extensively documented in industry reports (e.g., Marsh) and secondary technical descriptions.

3.3. Macondo Case (2010)

The Macondo accident occurred on April 20, 2010, at Mississippi Canyon Block 252 in the Gulf of Mexico, in approximately 1,500 m of water. The well was operated by BP using the Deepwater Horizon rig owned by Transocean. A blowout during temporary abandonment led to explosions and fire, culminating in the rig's sinking.

The release lasted 87 days, discharging approximately 4.9 million barrels of oil (≈780,000 m^3). Consequences included 11 fatalities and multiple injuries, total loss of the rig, severe equipment damage, extensive marine and coastal contamination, and long-term impacts on fisheries, tourism, and ecosystems. Business continuity was profoundly affected across the Gulf offshore supply chain. Total economic losses (response, cleanup, fines, penalties, and settlements) exceeded USD 60 billion.

Identified root causes involved barrier failures (cementing and testing), inadequate operational decisions, management of change deficiencies, weakened safety culture, and BOP failure. Key recommendations emphasized strengthened well control, independent barrier testing, improved BOP reliability, integrated risk management, safety culture, and regulatory oversight.

The case was officially documented in the Final Report of the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (U.S., 2011) and in technical investigations by the Bureau of Ocean Energy Management and the Chemical Safety Board, widely referenced internationally.

3.4. Elgin Case (2012)

The Elgin accident occurred on March 25, 2012, at the Elgin-Franklin field in the UK sector of the North Sea, approximately 240 km east of Aberdeen. The installation was operated by TotalEnergies. The event involved an uncontrolled gas release during operations on a

high-pressure, high-temperature (HPHT) well, prompting immediate platform evacuation.

No fatalities or injuries occurred. The release involved natural gas, with no publicly consolidated, traceable estimate of total volume (m^3). No significant oil spills were recorded; direct environmental impacts were limited, although potential risk was high. Equipment and materials were damaged without total loss of the installation, but extensive operational unavailability occurred. Business continuity was severely affected due to prolonged field shutdown and production losses.

Estimated economic losses ranged from USD 1.5 to 2.0 billion, including incident response, well control, repairs, and lost production. Root causes included well integrity barrier failures (casing/cement), technical challenges inherent to HPHT conditions, deficiencies in risk assessment, and management of change. Key recommendations emphasized strengthened HPHT well integrity management, independent barrier verification, improved gas leak monitoring and response, and enhanced regulatory governance.

The case was documented in official reports by the UK authority (HSE) and subsequent technical investigations, widely referenced in the offshore industry.

4. Elements of the Risk-Based Process Safety (RBPS) Model

The RBPS model structures process safety around 20 integrated elements organized into four pillars that encompass the entire sociotechnical system of an industrial organization. These elements are not intended to be treated as isolated requirements, but rather as interdependent components aimed at preventing major accidents through a holistic and risk-informed approach (CCPS, 2007; CCPS, 2016).

The Commitment to Process Safety pillar establishes the organizational foundation, encompassing leadership, process safety culture, regulatory compliance, workforce competence, and stakeholder engagement, which are widely recognized as prerequisites for sustained major accident prevention (CCPS, 2007; Reason, 1997). The Understanding Hazards and Risk pillar focuses on systematic hazard identification, risk analysis and evaluation, knowledge management, and technical documentation, aligning with established principles of hazard analysis and risk management in high-hazard industries (Kletz, 2001; ISO, 2018).

The Risk Management pillar includes operational controls such as asset integrity and reliability, management of change, operational readiness, safe work practices, emergency response, and contractor management. These elements are consistently identified in the literature as critical barriers for controlling major accident hazards throughout the asset life cycle (CCPS, 2007; Hopkins, 2012). Finally, the Learning from Experience pillar ensures continuous improvement through incident investigation, audits, performance metrics, and management reviews, reinforcing organizational learning and adaptive capacity (Hopkins, 2009; Hollnagel, 2011).

The RBPS differentiates itself through risk-based prioritization, enabling proportional resource allocation based on consequence potential, and through emphasis on preventive and mitigative barriers across asset life cycles. As systematized by the CCPS, the model provides a robust structure for integrating engineering, management, and organizational behavior to prevent catastrophic events (CCPS, 2016; Leveson, 2011).

Systematic application of the 20 RBPS elements revealed recurring deficiencies concentrated in four critical domains. In Asset Integrity and Reliability, weaknesses are frequently observed in barrier definition and verification, critical equipment life-cycle management, and risk-based maintenance prioritization, resulting in progressive degradation of functional reliability (CCPS, 2014).

In Management of Change, failures have been identified in the integrated assessment of technical and organizational risks, with design, procedural, or operational changes implemented without formal impact analyses, safeguard updates, or adequate workforce training—an issue repeatedly highlighted in major accident investigations (Kletz, 2003; Hopkins, 2012).

Regarding Operational Readiness, gaps are often noted in commissioning tests, validation of safe operating conditions, and preparation for abnormal scenarios, frequently associated with schedule pressure and production-driven decision-making (Reason, 1997; CCPS, 2016).

Finally, Process Safety Culture emerges as a cross-cutting factor, with indications of normalization of deviance, ineffective risk communication, and insufficient organizational learning from incidents and near misses, as extensively documented in socio-technical accident analyses (Vaughan, 1996; Hopkins, 2009).

When analyzed integratively, these deficiencies indicate that isolated technical failures tend to be amplified by managerial and cultural weaknesses. The RBPS, as structured by the CCPS, demonstrates that effective prevention of major accidents depends on consistent alignment among engineering, management, and organizational behavior across the entire sociotechnical system (CCPS, 2007; Leveson, 2011).

5. Risk-Based Integrity Resilience Model (RBIRM)

The Risk-Based Integrity Resilience Model (RBIRM) constitutes an analytical and operational framework for integrated management of well integrity and process safety in complex industrial systems. The model assumes that loss of integrity arises from the dynamic interaction among technical, organizational, and human factors and therefore must be addressed through a systemic and quantitative approach, consistent with contemporary socio-technical risk theories (Reason, 1997; Hollnagel, Woods, & Leveson, 2006).

The RBIRM integrates governance, engineering, and organizational learning into interdependent layers, aligned with risk-based process safety principles and asset life-cycle management frameworks (CCPS, 2007; ISO, 2018). Risk quantification is performed through estimation of the Probability of Loss of Integrity (P-LWI), structured via Fault Tree Analysis and refined through Bayesian Belief Networks that incorporate conditional dependencies and probabilistic updating based on historical data and operational evidence (Vesely et al., 2002; Jensen & Nielsen, 2007).

A central feature of the RBIRM is the hierarchical linkage of performance indicators, establishing feedback loops among process safety, integrity, and asset management KPIs, consistent with leading indicator concepts and safety performance measurement frameworks (Hopkins, 2009; ISO, 2014). In addition, the model operationalizes organizational resilience potentials—respond, monitor, learn, and anticipate—embedding them in technical and managerial decision-making processes, in line with resilience engineering theory (Hollnagel, 2011).

Thus, the RBIRM promotes a transition from reactive approaches to predictive, risk-oriented governance, enhancing organizational capacity to anticipate critical failures and sustain operational reliability in high-hazard offshore environments (Leveson, 2011; CCPS, 2016).

Within the RBIRM, the four accidents—Ixtoc I, Enchova, Macondo, and Elgin—serve as empirical reference cases for model calibration, validation, and systemic learning, each representing distinct stages of maturity in governance, engineering, and resilience (National Commission, 2011; HSE, 2012; Marsh, 1989).

From the RBIRM perspective, these events function first as historical data sources for P-LWI quantification, feeding fault trees and Bayesian networks with frequencies, conditional dependencies, and recurring barrier failure patterns documented in international blowout and loss-of-control databases (SINTEF, 2011;

PSA, 2013). Second, they enable evaluation of which model layers failed: engineering (well integrity and barriers), governance (decisions, management of change, oversight), and learning (capacity to incorporate prior lessons), as widely discussed in major accident investigations (Hopkins, 2012; CSB, 2016).

Each case also highlights specific gaps in resilience potentials. Ixtoc I and Enchova reflect limited capacity to anticipate and monitor emerging loss-of-control conditions; Macondo exposes critical failures in learning and responding despite extensive prior knowledge; Elgin highlights constraints in anticipating HPHT scenarios, albeit with a more effective emergency response (Hollnagel, 2011; HSE, 2012).

In the RBIRM, these accidents are not analyzed in isolation but as historical inflection points demonstrating the transition—or absence thereof—from reactive management to predictive, risk-informed integrity governance grounded in data and continuous organizational learning (Reason, 1997; Leveson, 2011).

6. Data Analysis

Data analysis was conducted in an integrated and systematic manner, combining historical accident information, normative references, and quantitative risk analysis methods to identify recurring failure patterns, estimate probabilities associated with loss of well integrity, and assess the maturity of process safety systems over time.
Initially, qualitative and quantitative data extracted from the four base cases were consolidated into common analytical categories, including initiating event type, technical barrier failures, organizational deficiencies, operational consequences, and human, environmental, and economic impacts. This step enabled information standardization and comparability across events occurring in different technological, regulatory, and historical contexts.

Subsequently, empirical findings were mapped against the 20 RBPS elements organized within the four pillars. For each case, RBPS elements with evidence of inadequate performance were identified and assigned relative weights based on observed criticality and recurrence. This procedure yielded a deficiency matrix highlighting significant concentrations in Asset Integrity and Reliability, Management of Change, Operational Readiness, and Process Safety Culture.

Failure frequencies associated with these domains were quantified using secondary probabilistic data from consolidated international blowout and loss-of-control databases. Historical frequencies were used as first-order estimates for initiating events and barrier failures, then adjusted by weighting factors related to operational context, technical complexity (e.g., HPHT wells), and inferred organizational maturity.

These data informed Fault Tree Analysis modeling, in which loss of well integrity was defined as the top event. Fault trees represented logical combinations of primary and secondary barrier failures, relevant human errors, and management failures. Event probabilities were integrated to obtain P-LWI for each reference scenario.

To capture conditional dependencies, uncertainties, and nonlinear relationships between technical and organizational factors, Fault Tree Analysis results were refined using Bayesian Belief Networks. This approach enabled probability updating based on historical evidence and sensitivity analysis of key elements such as management of change effectiveness, BOP reliability, and robustness of process safety culture.

In parallel, a maturity analysis positioned RBPS clusters at relative performance levels based on combined estimated failure frequencies and qualitative indicators from investigation reports.

This analysis revealed a gradual but nonlinear historical evolution of integrity governance and process safety, with significant advances following major accidents, interspersed with periods of stagnation or regression associated with normalization of deviance.

Finally, quantitative and qualitative results were integrated within the RBIRM to assess how identified deficiencies affect organizational resilience potentials—respond, monitor, learn, and anticipate. The analysis demonstrated that sustainable reduction of P-LWI is associated not only with strengthened technical barriers but primarily with consistent integration of engineering, governance, and organizational learning supported by data and an explicit risk-based approach.

7. Conclusion

This paper analyzed major offshore well accidents—Ixtoc I, Enchova, Macondo, and Elgin—using an integrated framework that combines Risk-Based Process Safety, life-cycle well integrity, and asset governance, culminating in the proposal of the Risk-Based Integrity Resilience Model (RBIRM).

The overarching objective was to understand, in a systemic and quantitative manner, recurring causes of large-magnitude offshore accidents, moving beyond reactive approaches and contributing to risk-, data-, and resilience-oriented integrity governance.

The study adopted an applied, analytical, and quantitative approach based on documentary analysis of historical accidents and formal risk modeling. The 20 RBPS elements were assessed, with weighted failure frequencies derived from international blowout databases and integrated through Fault Tree Analysis and Bayesian Belief Networks to estimate the Probability of Loss of Well Integrity.

Results revealed recurring weaknesses in Asset Integrity and Reliability, Management of Change, Operational Readiness, and Process Safety Culture. Loss of integrity was shown to result from interaction among technical, organizational, and managerial failures rather than isolated causes. The RBIRM proved suitable for structuring these interactions and supporting transition from reactive to predictive governance.
The work contributes an integrated model linking process safety, integrity, asset management, and resilience engineering, providing quantitative support for risk-based decision-making and prioritization of critical barriers in offshore systems.
Key limitations include reliance on secondary historical data and lack of primary, real-time operational information.

Future research may apply the RBIRM using current operational data, integrate it with digital twins, and expand its application to economic resilience analyses and comparative regulatory regimes.

References

API (American Petroleum Institute). 2019. *Recommended Practice 75: Safety and Environmental Management Systems for Offshore Operations and Assets*. 4th ed. Washington, DC: API.

BP. 2010. *Deepwater Horizon Accident Investigation Report*. Houston: BP Exploration & Production Inc.

CCPS – Center for Chemical Process Safety. (2007). *Guidelines for risk based process safety*. New York: American Institute of Chemical Engineers.

CCPS – Center for Chemical Process Safety. (2016). *Process safety leading and lagging metrics*. Hoboken, NJ: AIChE.

CCPS – Center for Chemical Process Safety.(2006). *Guidelines for Asset Integrity Management*. Hoboken, NJ: John Wiley & Sons.

CSB – U.S. Chemical Safety and Hazard Investigation Board. (2016). *Investigation report: Explosion and fire at the Macondo well*. Washington, DC.

Destri, Alice Claussen, et al, 2023. "Development of a Reliability and Maintenance Database System for Offshore Well Equipment in Brazil: MINERVA, Phase 1." Paper presented at the *Offshore Technology Conference Brasil (OTC Brasil)*, Rio de Janeiro, Brazil, October 24–26. https://doi.org/10.4043/32957-MS

França, Alex Alves et al. (2024). "The Hazard Assessment in Representative Onshore Oil Wells for Improve the Process Safety." Paper presented at the *10th Latin American Conference on Process Safety (CCPS Latin American Conference on Process Safety)*, Barranquilla, Colombia, September 18–20. AIChE Proceedings.

Hollnagel, Erik, David D. Woods, and Nancy Leveson, eds. 2006. *Resilience Engineering: Concepts and Precepts*. Aldershot: Ashgate.

Hollnagel, Erik. 2014. *Safety-I and Safety-II: The Past and Future of Safety Management*. Farnham: Ashgate.

Hopkins, A. (2009). *Learning from high reliability organisations*. Sydney: CCH Australia.

Hopkins, A. (2012). *Disastrous decisions: The human and organisational causes of the Gulf of Mexico blowout*. Sydney: CCH Australia.

INERIS (Institut National de l'Environnement Industriel et des Risques). 2004. *ARAMIS Project: Accidental Risk Assessment Methodology for Industries*. Verneuil-en-Halatte: INERIS.

ISO (International Organization for Standardization). 2017. *ISO 16530-1: Petroleum and Natural Gas Industries—Well Integrity—Part 1: Life Cycle Governance*. Geneva: ISO.

ISO (International Organization for Standardization). 2024. *ISO 55001: Asset Management—Management Systems—Requirements*. Geneva: ISO.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: MIT Press.

Loretti, Rômulo Alves et al. 2019. "Data Science and Business Intelligence Techniques for Learning from Environmental Accident Analysis for Offshore Oil Fields." Paper presented at the *Offshore Technology Conference Brasil (OTC Brasil 2019)*, Rio de Janeiro, Brazil, October 29–31. Paper no. OTC-29725-MS. doi:10.4043/29725-MS.

Marsh. (1989). *100 largest losses: A thirty-year review of property damage losses in the hydrocarbon industry*. London: Marsh & McLennan.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011). *Deep water: The Gulf oil disaster and the future of offshore drilling*. Washington, DC: U.S. Government Printing Office.

PSA – Petroleum Safety Authority Norway. (2013). *Trends in risk level in the petroleum activity*. Stavanger: PSA Norway.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot, UK: Ashgate.

SINTEF. (2011). *Blowout risk evaluation model (BORM)*. Trondheim: SINTEF Technology and Society.

Skogdalen, Jon Espen, and Jan Erik Vinnem. 2007. "Quantitative Risk Analysis of Oil and Gas Drilling Using Historical Well Incident Data." *Reliability Engineering & System Safety* 92 (12): 1747–1761. https://doi.org/10.1016/j.ress.2007.05.002.

UK Health and Safety Executive (HSE). 2012. *Investigation into the Release of Gas at the Elgin Platform*. London: HSE.

United States. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. 2011. *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling*. Washington, DC: Government Printing Office.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (2002). *Fault tree handbook with aerospace applications*. Washington, DC: NASA.

Vinnem, Jan Erik. 2014. *Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies*. 3rd ed. London: Springer.

Woods, David D. 2006. "Essential Characteristics of Resilience." In *Resilience Engineering: Concepts and Precepts*, edited by Erik Hollnagel, David D. Woods, and Nancy Leveson, 21–34. Aldershot: Ashgate.

Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26120-cd

Towards a Genuine Convergence of Process safety and Asset Management: An Integrative Framework with Composite Metrics

Helton Luiz Santana Oliveira

Brazilian Association of Risk Analysis, Process Safety and Reliability, Brazil. E-mail: heltonsantana@id.uff.br

Gilson Brito Alves Lima

Department of Production Engineering, Federal Fluminense University, Brazil. E-mail: glima@id.uff.br

This study examines the conceptual foundations, methodological approach, comparative analysis, and integration strategy of Asset Management (AM) and Risk-Based Process Safety Management (PSM). Asset Management, as defined by ISO 55000:2024, is the coordinated organizational activity aimed at deriving value from assets through balancing cost, risk, opportunity, and performance. It represents a managerial and cultural shift that extends beyond technical asset control to influence strategic decision-making and organizational objectives. In parallel, Risk-Based Process Safety, as structured by the CCPS, provides a formal and systematic framework to prevent major industrial accidents through proportional risk management, structured governance, and continuous improvement organized into four interdependent pillars. The research adopts a comparative methodological approach, combining documentary analysis with structured analytical mapping of normative frameworks, enabling systematic identification of similarities and differences between AM and PSM. The analysis demonstrates that both systems share core elements, including risk-based thinking, life-cycle orientation, governance structures, performance monitoring, and competence development. Mechanical integrity emerges as a key intersection point, treated explicitly within PSM and implicitly within ISO-based asset management standards. Despite these similarities, the systems differ in primary purpose and scope: PSM focuses on preventing high-consequence events and protecting people and the environment, whereas AM emphasizes sustainable value creation and economic optimization. The study proposes an integrated implementation strategy involving strategic alignment, harmonized requirements, unified governance, integrated critical processes, consolidated performance indicators, capability development, and joint continuous improvement. The findings conclude that structured integration enhances organizational robustness, strengthens asset reliability, reduces systemic risk, and supports sustainable operational, economic, and environmental performance in complex industrial environments.

Keywords: Process safety, asset management, ISO 55001, ISO 31000

1. Introduction

According to ISO 55000:2024 (ISO, 2024), Asset Management is the coordinated activity of an organization to derive value from assets. Achieving value typically involves balancing costs, risks, opportunities, and performance benefits. The term “activity” may also refer to the application of the elements of an asset management system. The word “activity” has a broad meaning and may include, for example, the approach, planning and plans, as well as their implementation.

According to Lafraia (2024), asset management is not the same as managing assets. Asset management is far more concerned with management itself than with technical actions performed on assets. When studying asset management, it should not be surprising that it does not address, in great technical detail, the administration of life cycle stages. The emphasis lies on managing the competencies that enable individuals to practice sound management.

As stated by Azevedo (2019), asset management is a managerial process that involves balancing costs, risks, opportunities, and performance

benefits, and this balance may need to be considered across different time horizons. Asset management can only be effective when embedded in the context of achieving organizational objectives.

Asset management represents a cultural shift in corporate strategic planning by adding to the traditional focus on products and customers a perspective centered on assets and the value they are capable of generating for the business. Conceptually, it marks the beginning of a new era in corporate management, to be practiced by those seeking business excellence. Asset management is not limited to managing property; it extends beyond operational boundaries to influence business strategy.

Practicing asset management in accordance with the ISO 55K standards (ISO, 2024) means adopting an international framework to derive value from assets while achieving a balance among performance, associated costs, and related risks.
In turn, the Risk-Based Process Safety model was developed to enhance the effectiveness of management systems aimed at preventing major accidents in the process industries, structuring practices in proportion to the magnitude of hazards and levels of risk involved (CCPS, 2007).

The process safety approach recognizes that technological, human, managerial failures and external factors may contribute to catastrophic events, historically highlighting deficiencies in management systems. It therefore proposes a formal, documented, and sustainable system in which the level of detail and rigor is defined based on the understanding of risks, the demand for process safety activities, and the prevailing organizational culture. The model emphasizes resource prioritization, the use of performance and efficiency metrics, and periodic management reviews.

The structure of Risk-Based Process Safety is organized into four interdependent pillars, comprising twenty elements.

The first pillar addresses commitment to process safety, encompassing organizational culture, regulatory compliance, technical competence, workforce involvement, and stakeholder engagement.

The second pillar focuses on understanding hazards and risks, including process knowledge management and the systematic identification and analysis of risks throughout the facility life cycle.

The third pillar is dedicated to managing risk through operating procedures, safe work practices, asset integrity and reliability, contractor management, training and performance assurance, management of change, operational readiness, conduct of operations, and emergency management.

The fourth pillar emphasizes organizational learning through incident investigation, the use of metrics, auditing, and management review, thereby promoting continuous improvement. The model encourages integration with other corporate systems to reduce the frequency and severity of incidents and to sustain safe, environmental, and business performance over time (CCPS, 2007).

Process Safety likewise represents a cultural shift in operational management by integrating into the traditional focus on production and efficiency a perspective centered on incident prevention, protection of people, assets, and the environment, and business continuity through strategies that prevent and mitigate releases, dispersions, fires, and explosions.

The implementation of process safety is not limited to the application of technical rules; it transcends operational controls and permeates strategic decisions, influencing planning, risk management, and resource allocation.

Practicing Risk-Based Process Safety in accordance with recognized international standards (CCPS, 2006; ISO, 2018) means adopting a structured approach to identify, assess, and control risks in industrial processes, ensuring the protection of people and assets, system reliability, and the balance among operational performance, costs, and risk exposure.

Despite the numerous similarities and potential synergies between the two management systems, the approach of treating them separately still persists, as if no substantial gains could be achieved through the integration of these important systems.

2. Research Method

The integration between Process Safety Management (PSM) and Asset Management (AM) is rigorously investigated through the comparative method, which is particularly well suited to the analysis of complex organizational structures. The comparative method consists of the systematic identification of similarities and differences among phenomena in order to understand patterns, relationships, and causal explanations (Gil, 2019; Lakatos and Marconi, 2021).

From a research design perspective, the study may be classified as exploratory-explanatory, combining documentary analysis with a comparative case study approach. The first stage involves constructing an analytical matrix based on the normative frameworks of PSM and AM, enabling the comparison of governance principles, risk management practices, organizational competencies, and continuous improvement mechanisms (ABNT, 2014; CCPS, 2007). This stage corresponds to systematic documentary analysis, as recommended by Gil (2019).

This methodological approach makes it possible to understand how the articulation between process risk management and asset life cycle management contributes to the reduction of systemic failures and to sustainable organizational performance.

3. Comparison Between Management Systems

Within the framework of risk-based process safety management, mechanical integrity is treated as a formal management system designed to ensure that equipment and systems containing hazardous substances or energy remain fit for service throughout their entire life cycle, thereby preventing large-scale accidental releases.

The proposed approach to mechanical integrity goes beyond isolated inspection and maintenance activities by structuring a systemic program that integrates policies, clearly defined responsibilities, compliance with technical standards, personnel qualification, document control, and continuous improvement. A mechanical integrity program within risk-based process safety management must encompass critical equipment such as pressure vessels, piping systems, storage tanks, relief devices, instrumentation systems, and utilities essential to operational safety.

Such a program relies on defined criteria for scope determination, development of inspection, testing, and preventive maintenance plans, as well as risk-based prioritization. It emphasizes quality assurance in the procurement of materials and spare parts, inspector certification, and traceability of executed activities. The systematic collection and analysis of inspection data are considered fundamental to assessing equipment condition, adjusting inspection intervals, and identifying degradation trends.

The effectiveness of mechanical integrity within a risk-based process safety management system depends on integration with other process safety elements, including management of change, operational readiness, and incident investigation. Organizational culture, leadership commitment, and the use of performance indicators are also decisive factors in sustaining asset reliability over time. By consolidating technical and managerial principles, this approach provides a structured basis for preventing failures caused by corrosion, fatigue, manufacturing defects, or inadequate maintenance, thereby contributing to the reduction of major accident risk and to the preservation of operational safety and reliability (CCPS, 2006).

From the perspective of asset management, as established in ISO 55000 (ISO, 2024a) and ISO 55001 (ISO, 2024b), the term “mechanical integrity” is not explicitly used. Nevertheless, the principles and requirements set forth in these standards systemically incorporate the technical

and managerial foundations necessary to preserve the physical condition and functional performance of assets throughout their life cycle.

ISO 55000 (ISO, 2024a) defines asset management as the coordinated activity of an organization to realize value from assets, establishing that such value derives from balancing cost, risk, opportunity, and performance. By recognizing risk as the combination of the probability of failure and its consequences, the standard implicitly encompasses risks associated with physical degradation, corrosion, fatigue, structural failures, and other mechanisms typically addressed in mechanical integrity programs. Maintaining asset performance therefore presupposes systematic control of technical condition.

ISO 55001 (ISO, 2024b), in specifying requirements for an asset management system, reinforces this approach. In the planning clause, the organization is required to determine risks and opportunities that may affect the achievement of asset management objectives, including risks arising from physical failures. Similarly, in the operations clause, adequate operational planning and control are required, including the definition of performance criteria and the implementation of plans to ensure that assets fulfill their intended functions. These requirements support the need for inspections, testing, condition monitoring, and structured maintenance.

Additionally, the support and performance evaluation clauses of ISO 55001 (ISO, 2024b) require the maintenance of technical competence, control of documented information, and systematic monitoring of performance and reliability indicators. These elements are essential to ensure that assets remain fit for service and that their condition is continuously evaluated and improved.

Process Safety Management (PSM) and Asset Management (AM) are therefore complementary disciplines, although they differ in primary focus. Both operate within structured organizational systems, adopt a risk-based approach, and depend on governance, technical competence, and continuous improvement. However, they differ in strategic purpose, scope, and operational emphasis.

Common elements include a risk-based approach, requiring systematic identification, analysis, and treatment of risks. Process safety focuses on catastrophic event risks, such as large releases of hazardous substances or energy, whereas asset management addresses risks affecting value, performance, and sustainability. Both disciplines adopt a systemic life-cycle perspective—from design through decommissioning—and rely on formal processes, controlled documentation, and organizational integration. Asset integrity and reliability are essential in both contexts: in PSM, integrity prevents major accidents; in AM, it ensures performance, availability, and value generation. Both also require active leadership, clearly defined responsibilities, technical competence, and performance indicators.

Key differences lie in strategic purpose, conceptual scope, metrics, and organizational emphasis. PSM primarily seeks to prevent high-consequence accidents and protect people, the environment, and facilities, whereas AM aims to maximize organizational value through balancing cost, risk, opportunity, and performance. PSM concentrates on industrial processes involving hazardous substances or significant energy, while AM applies to any class of assets—physical, financial, informational, or intangible. PSM metrics emphasize incident rates, barrier effectiveness, and reliability of critical safety systems, whereas AM metrics include economic and operational indicators such as availability, life-cycle cost, and return on investment. Finally, PSM is strongly oriented toward regulatory compliance and safety barrier management, whereas AM emphasizes corporate governance and sustainable value creation.

4. The integration of the systems

Process Safety may be understood as a specialized discipline focused on the prevention of high-severity events, whereas Asset Management constitutes a broader managerial system oriented toward the generation of organizational value. The intersection between the two occurs primarily in the management of technical risks, asset integrity, and

the need for evidence-based decision-making. When integrated, they simultaneously reinforce operational safety and sustainable performance.

From an analytical perspective, Process Safety Management (PSM) concentrates on the integrity of safety barriers and the reliability of critical systems, while Asset Management (AM) expands the scope to include economic performance, operational availability, and strategic sustainability. Their convergence lies in the management of technical risks, the physical integrity of assets, and data-driven decision-making. In systemic terms, PSM may be regarded as a specialized subsystem within the broader AM framework when addressing high-risk industrial assets.

An integrated implementation should be structured through coordinated stages:

a) Strategic alignment – Define a single corporate policy that recognizes process safety as an essential component of value generation. Integrate safety and asset performance objectives into strategic planning.

b) Mapping and harmonization of requirements – Conduct a comparative analysis of the requirements of both systems, identifying overlaps (risk management, competence, integrity, management of change) and eliminating documentary redundancies.

c) Unified governance – Establish a clear organizational structure with integrated roles and responsibilities. Create a multidisciplinary committee to oversee decisions involving risk, reliability, and asset investment.

d) Integration of critical processes – Align risk management, management of change, operational readiness, and incident investigation procedures with maintenance planning, condition monitoring, and performance evaluation processes.

e) Single performance indicator system – Develop an integrated dashboard including safety metrics (barrier indicators, near misses) and asset performance metrics (availability, life-cycle cost).

f) Culture and capability development – Promote technical and managerial training that links asset reliability to accident prevention and value generation.

g) Integrated continuous improvement – Conduct combined audits and periodic management reviews to ensure consistency among safety, performance, and sustainability objectives.

This strategy reduces organizational silos, avoids duplication, and simultaneously strengthens operational protection and sustainable value creation.

5. Conclusion

The comparative analysis between Process Safety Management (PSM) and Asset Management (AM) demonstrates that, although they have distinct conceptual origins and specific strategic purposes, both converge on essential foundations: a risk-based approach, systemic perspective, life-cycle orientation, structured governance, organizational competence, and continuous improvement. Process Safety focuses on the prevention of high-severity events and the preservation of critical safety barriers, whereas Asset Management is directed toward the sustainable generation of value through balancing cost, risk, opportunity, and performance.

The integration of these systems does not constitute a mere overlap of requirements, but rather an opportunity for mutual reinforcement. The physical and functional integrity of assets, a central element of process safety, is likewise an indispensable condition for the performance and reliability required by asset management. Similarly, the strategic governance and decision-making discipline inherent in asset management enhance the effectiveness of process safety practices, providing them with greater economic and organizational coherence.

An integrated implementation strategy demonstrates that it is feasible to harmonize policies, processes, performance indicators, and governance structures, thereby reducing redundancies and eliminating functional silos. By aligning safety objectives with performance and value targets, the organization begins to treat

accident prevention not as an isolated cost, but as an intrinsic component of operational and reputational sustainability.

It can therefore be concluded that the structured integration of PSM and AM promotes greater organizational robustness, strengthens asset reliability, reduces the likelihood of systemic failures, and sustains economic, environmental, and social outcomes over time. In complex, high-risk industrial environments, this convergence represents not merely a sound managerial practice, but a strategic requirement for excellence and long-term organizational continuity.

References

Ayomoh, Michael, and Ongwae, Benard. "A Systematic Review of Asset Integrity and Process Safety Management Sustainability for Onshore Petrochemical Installations." *Sustainability* 17, no. 1 (2025): 286.

Azevedo, C. *Asset Management Insights: Phases, Practices, and Value*. New York: Industrial Press, 2019.

Center for Chemical Process Safety (CCPS). *Guidelines for Mechanical Integrity Systems*. New York: John Wiley & Sons, 2006.

Center for Chemical Process Safety (CCPS). *Guidelines for Risk Based Process Safety*. Hoboken, NJ: John Wiley & Sons / AIChE, 2007.

Gil, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 7. ed. São Paulo: Atlas, 2019.

International Organization for Standardization (ISO). *ISO 31000:2018 – Risk Management – Guidelines*. Geneva: ISO, 2018.

International Organization for Standardization (ISO). *ISO 55000:2024 — Asset management — Overview, principles and terminology*. Geneva: ISO, 2024a.

International Organization for Standardization (ISO). *ISO 55001:2024 – Asset Management – Management Systems – Requirements*. Geneva: ISO, 2024b.

Lafraia, J. R. B. *Gestão de Ativos Diária: O Início da Jornada*. 1st ed. Rio de Janeiro: Editora Conasset – Consultoria em Gestão de Ativos, 2024.

Lakatos, Eva Maria, e Marina de Andrade Marconi. *Fundamentos de metodologia científica*. 8. ed. São Paulo: Atlas, 2021.

Oliveira, Helton Luiz Santana. 2026. *"Asset Management: Evolution and Consolidation in the Brazilian Context, from Terotechnology to the ISO 5500X Standards." Brazilian Journal of Maintenance & Asset Management* 1 (1):1-19.

Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26145-cd

Advancing Process Safety Evaluation Through Dynamic Data Envelopment Analysis: Measuring Efficiency, Learning, and Risk Mitigation Outcomes

Helton Luiz Santana Oliveira

Brazilian Association of Risk Analysis, Process Safety and Reliability, Brazil.
E-mail: heltonsantana@id.uff.br

Lidia Angulo Meza

Department of Production Engineering, Federal Fluminense University, Brazil.
E-mail:lidiaangulomeza@id.uff.br

Gilson Brito Alves Lima

Department of Production Engineering, Federal Fluminense University, Brazil.
E-mail: glima@id.uff.br

This paper applies Dynamic Data Envelopment Analysis (Dyn-DEA) to evaluate the intertemporal efficiency of Process Safety in large-scale Brazilian refineries, considering multiple inputs, outputs, and intertemporal linking variables (*carry-overs*). The objective is to identify which units effectively convert resources allocated to safety into safe operational performance, organizational learning, and risk mitigation, while accounting for the significance of accumulated assets and critical backlog. The model is output-oriented and employs linear programming, incorporating variable returns to scale, technological comparability, and normalization of structural factors. Inputs include maintenance, inspection, training, audits, and management-of-change efforts; desirable outputs encompass safe throughput, implementation of recommendations, and critical barrier integrity; undesirable outputs comprise loss-of-primary-containment events and unplanned downtime hours. Intertemporal carry-overs include barrier integrity (desirable) and critical action backlog (undesirable). The results reveal three patterns: refineries on the dynamic frontier, accumulating integrity and reducing backlog; transitional units, showing operational gains still constrained by backlog; and units exhibiting structural inefficiency, with slow recovery trajectories. The analysis demonstrates that efficiency is cumulative, dependent on intertemporal trajectories, organizational learning, and effective barrier management, and that investment-focused policies alone may be insufficient to enhance Process Safety performance.

Keywords: Process safety, data envelopment analysis, dynamic performance assessment, organizational learning

1. Introduction

Process safety is a central element in the management of process plants, such as refineries, as it seeks to prevent large-scale events, such as explosions, fires, and toxic releases, capable of causing severe human, environmental, and economic losses (CCPS, 2007). Unlike occupational safety, it focuses on the integrity of complex systems operating under severe conditions of pressure, temperature, and hazardous inventories. In Brazil, these issues take on specific characteristics due to asset aging, high technological complexity, and operational variability, combined with successive adaptations for processing heavier crude oils, which intensify degradation mechanisms.

At the institutional level, regulations issued by the Brazilian National Agency of Petroleum, Gas and Biofuels, federal requirements established by IBAMA and also by state environmental agencies, together with the operators' own corporate guidelines, have expanded the

formalization of integrity management. Nevertheless, challenges remain regarding the development of a preventive culture, the use of predictive indicators, and the integration between occupational safety and process safety.

Brazil currently has 18 refineries, 11 of which are operated by its state-controlled mixed-economy company, Petrobras, while the remaining seven are operated by individual private-sector companies.

The Brazilian refining sector has characteristics, namely: it is increasingly oriented toward middle distillates, especially diesel, and it includes refineries with profiles more focused on gasoline as well as units specialized in non-energy products, such as lubricants.

Figure 1 shows the geographic distribution of oil refineries across the Brazilian territory.

Fig. 1. Distribution of Brazilian refineries.

The country faces an estimated refining deficit of approximately 600 thousand barrels per day in order to fully meet domestic demand and therefore operates as a net importer of petroleum products, particularly diesel, due to the mismatch between refining capacity and the growth of the national vehicle fleet.

Refineries differ not only in their technological complexity but also in the feedstocks they process and the markets they serve. They are predominantly located near oil-producing areas, industrial hubs, and the most populous urban centers, a strategy that reduces logistical costs.

The central research question of this study is to identify which refineries exhibit greater dynamic efficiency in converting resources allocated to Process Safety into sustainable outcomes in safe operational performance, organizational learning, and risk mitigation, while accounting for intertemporal dependencies associated with accumulated asset integrity and critical backlog.

Although Brazil's historical record shows a relatively low frequency of catastrophic refinery accidents, documented incidents involving fires, explosions, and leaks demonstrate the need for the continuous strengthening of process safety culture, with emphasis on systematic incident analysis, barrier management, independent auditing, and the dissemination of organizational learning. (API, 2021).

2. Research Method

This paper adopts an applied quantitative methodological approach based on Dynamic Data Envelopment Analysis (Dyn-DEA) to evaluate the intertemporal performance of Process Safety across a set of refineries with relatively homogeneous structural characteristics.

The model considers multiple inputs, outputs, and intertemporal linkage variables (carry-overs), allowing the simultaneous capture of operational efficiency, organizational learning, and risk mitigation across successive periods. Indicators of processing capacity, technological complexity, asset integrity, safety performance, and preventive investments are incorporated. The formulation employs output-oriented linear programming under assumptions of variable returns to scale and technological comparability among units. The modelling framework enables the identification of dynamic efficient frontiers, improvement trajectories, and the cumulative effects of managerial decisions, thereby providing analytical support for benchmarking, investment prioritization, and the continuous enhancement of industrial risk management.

Data Envelopment Analysis (DEA) is a nonparametric linear programming technique designed to measure the relative efficiency of decision-making units (DMUs) that use multiple inputs to produce multiple outputs, constructing an empirical best-practice frontier from the sample itself (Charnes, Cooper, & Rhodes, 1978). In classical extensions, variable returns to scale are admitted, and technical inefficiency is decomposed into components associated with scale effects (Banker, Charnes, & Cooper, 1984).

Dyn-DEA comprises a family of multiperiod DEA models in which intertemporal dependence arises through carry-over variables (such as capital, inventories, retained earnings, liabilities, accumulated emissions, accumulated "quality," and similar factors). This framework allows efficiency to be assessed from a long-term perspective and avoids myopic, period-by-period optimization (Tone & Tsutsui, 2010; Kao, 2013).

This paper aims to explore an application of Dyn-DEA to assess, in a comparative and intertemporal manner, the relative efficiency of a set of large-scale, integrated, continuously operating petroleum refineries located in Brazil. These refineries are characterized by crude oil processing configurations that include typical atmospheric and vacuum distillation units, conversion through fluid catalytic cracking and/or hydrotreating and hydrocracking, catalytic reforming, sulfur recovery, utility systems, tankage, and product dispatch facilities, with an operational profile consistent with that of the national refining system.

The objective of the study is to measure performance from a Process Safety perspective, directing the analysis simultaneously toward three outcome dimensions: safe operational efficiency, organizational learning, and risk mitigation, while explicitly incorporating intertemporal dependencies through linking variables (carry-overs).

Each refinery is modelled as a decision-making unit (DMU), considering a time series of T consecutive annual periods with consolidated and auditable data, to capture cumulative effects of integrity programs, barrier reinforcement, and learning derived from events and audits. The analysis assumes technological and institutional comparability among the refineries, which operate under the same national regulatory framework and similar corporate Process Safety management standards, while allowing for structural differences that are controlled through specific variables or appropriate normalization.

The dynamic modeling must allow the estimation of overall efficiency over the multiperiod horizon as well as period-specific efficiencies, ensuring consistency between the performance trajectory and annual results. A slacks-based formulation (slacks-based measure – SBM) was adopted because it permits nonradial treatment of variables and the explicit incorporation of carry-overs, whether desirable or undesirable, free or partially fixed, when applicable.

The following were considered as annual Process Safety inputs:

(i) integrity-driven maintenance and inspection effort, expressed in equivalent man-hours or annual expenditure normalized by capacity or operational exposure;
(ii) training and qualification effort in Process Safety, measured in structured hours per employee and contractor, weighted by criticality;
(iii) effort devoted to audits and assessments of Process Safety management systems, converted into equivalent man-hours or annual cost; and
(iv) effort in management of change and operational discipline, represented by the volume of management-of-change processes evaluated and completed with effectiveness verification, or by an adherence index to critical procedures.

All inputs were expressed on a scale relative to operational exposure—such as installed capacity, effective annual system processing capacity, or

operating hours—thereby ensuring comparability.

As annual desirable outputs, three main dimensions were considered, namely:

- The first dimension corresponds to safe operational efficiency, represented by operational availability or effective production conditioned on integrity compliance, thereby preventing increases in effective processing capacity resulting from barrier deterioration from being interpreted as performance improvement.

- The second dimension corresponds to organizational learning, measured by learning effectiveness, expressed as the percentage of critical recommendations arising from investigations, audits, or risk analyses that are implemented within the established timeframe and verified for effectiveness.

- The third dimension refers to risk mitigation, represented by indicators of barrier strengthening, such as the percentage of critical barriers with inspections and tests performed on schedule and exhibiting acceptable performance, or by a composite barrier health index.

Additionally, the following undesirable outputs to be minimized were included:

- the occurrence of primary containment loss events weighted by severity or potential consequence.

- unplanned downtime hours associated with integrity failures relevant to Process Safety.

These indicators are modeled as undesirable outputs or, equivalently, treated as variables to be minimized, thereby ensuring monotonic consistency in the interpretation of efficiency.

The dynamic structure incorporates intertemporal linking variables (*carry-overs*).

As a desirable and partially fixed intertemporal linking variable, the asset and critical barrier integrity (or health) index at the end of each year was considered, as it conditions the initial state of the subsequent period. This index represents a stock of accumulated reliability that cannot be artificially reduced to improve current efficiency.

As an undesirable and free intertemporal linking variable, the backlog of critical Process Safety actions at the end of each year was considered, encompassing overdue items or critical actions whose effectiveness has not been verified, the growth of which represents a transfer of risk to the subsequent period.

Optionally, the inventory of residual risks was considered as an additional linking variable, expressed as a weighted sum of scenarios with safeguards that are not fully effective, whenever a formal quantification system exists.

To control for technological and structural heterogeneity, non-discretionary variables or normalization factors were adopted, such as nominal processing capacity, unit complexity factor, average crude slate processed, and the share of heavy streams in the operational mix. These factors may be incorporated as environmental variables or used to adjust input and output indicators.

3. Modelling: Outputs-oriented Dyn-DEA with carry-over variables

For each refinery under evaluation (DMU_o), an output-oriented DEA problem is defined with intensity variables $\lambda_{j,t} \geq 0$ for each refinery $j$and year t, and a common expansion factor $\varphi \geq 1$ representing the extent to which the desirable outputs of DMU_o could be increased while holding inputs constant, ensuring non-deterioration of undesirable outputs, and satisfying the constraints imposed on the carry-overs.

Decision variables

φ= expansion factor of desirable outputs (the larger, the better)

$\lambda_{j,t}$= weights (intensity variables) used to construct the benchmark in year t

Objective function

Max φ

Constraints for year t.

(A) Inputs – not to exceed the resources of the evaluated DMU.

$$\sum_{j=1}^{n} \lambda_{j,t} I_k(j,t) \leq I_k(o,t) \quad \forall k \in \{1,2,3,4\} \tag{1}$$

(B) Desirable outputs – expand results by φ

$$\sum_{j=1}^{n} \lambda_{j,t} O_r(j,t) \geq \varphi O_r(o,t) \quad \forall r \in \{1,2,3\} \tag{2}$$

(C) Undesirable outputs – non-deterioration constraint

$$\sum_{j=1}^{n} \lambda_{j,t} U_q(j,t) \leq U_q(o,t) \quad \forall q \in \{1,2\} \tag{3}$$

Carry-over constraints by year *t* (applied classification)

(D) Desirable carry-over C1: do not reduce the "state."

$$\sum_{j=1}^{n} \lambda_{j,t} C1(j,t) \geq C1(o,t) \tag{4}$$

(E) Undesirable carry-over C2: do not increase the "undesirable state."

$$\sum_{j=1}^{n} \lambda_{j,t} C2(j,t) \leq C2(o,t) \tag{5}$$

Finally:

$$\lambda_{j,t} \geq 0 \forall j,t e \varphi \geq 1 \tag{6}$$

Efficiency Score

For output-oriented models, the following is used:

$$\text{Efficiency}(o) = \frac{1}{\varphi'^*} \tag{7}$$

- Se $\varphi'^* = 1$, Thus, efficiency equals 1 (on the frontier).

- Se $\varphi'^* > 1$, thus, efficiency < 1 (inefficient)

Table 1 – Dyn-DEA Inputs

DMU Refinery	Year	I1 (R$M)	I2 (kh)	I3 (kh)	I4 (MOC)
Alpha	1	820	48	22	180
Alpha	2	845	51	24	195
Alpha	3	870	54	25	205
Beta	1	690	39	18	150
Beta	2	705	42	19	162
Beta	3	728	45	21	170
Gama	1	760	44	23	175
Gama	2	780	46	24	182
Gama	3	805	49	26	190
Delta	1	790	45	25	188
Delta	2	815	48	26	195
Delta	3	835	51	28	204
Epsilon	1	640	37	19	142
Epsilon	2	662	40	20	150
Epsilon	3	680	42	21	158
Zeta	1	610	36	17	140
Zeta	2	628	38	18	146
Zeta	3	645	40	19	152
Eta	1	560	32	16	128
Eta	2	575	34	17	134
Eta	3	595	36	18	140
Theta	1	570	33	17	130
Theta	2	590	35	18	138
Theta	3	608	37	19	145

The annual input variables considered are:

- I_1, d annual expenditure on integrity-oriented maintenance and inspections, expressed in millions of Brazilian Real;
- I_2, hours of structured Process Safety training, in thousands of hours per year;
- I_3, hours of audits and evaluations of Process Safety management systems, in thousands of hours per year;
- I_4, annual number of Management of Change (MOC) processes completed with effectiveness verification.

Table 2 – Desirable Outputs of the Dyn-DEA

DMU Refinery	Year	O1 (kbpd)	O2 (%)	O3 (%)
Alpha	1	378	81	87
Alpha	2	386	84	89
Alpha	3	392	87	91

Beta	1	301	77	82
Beta	2	308	80	84
Beta	3	314	83	86
Gama	1	226	83	88
Gama	2	231	86	90
Gama	3	236	89	92
Delta	1	214	82	89
Delta	2	219	85	91
Delta	3	223	88	93
Epsilon	1	185	78	83
Epsilon	2	190	81	85
Epsilon	3	195	84	87
Zeta	1	172	79	84
Zeta	2	176	82	86
Zeta	3	180	85	88
Eta	1	154	76	82
Eta	2	158	79	84
Eta	3	162	82	86
Theta	1	155	77	83
Theta	2	159	80	85
Theta	3	163	83	87

The desirable output variables include:

- O1, safe throughput, measured as the annual average in thousands of barrels per day (kbpd), conditional on integrity compliance;
- O2, organizational learning effectiveness, measured as the percentage of critical recommendations implemented and verified for effectiveness;
- O3, critical barrier health, measured as a percentage.

Table 3 – Undesirable Outputs of the Dyn-DEA

DMU Refinery	Year	U1 (LOPC idx)	U2 (h)
Alpha	1	0.42	310
Alpha	2	0.39	295
Alpha	3	0.35	270
Beta	1	0.53	390
Beta	2	0.49	360
Beta	3	0.45	332
Gama	1	0.46	340
Gama	2	0.41	312
Gama	3	0.37	288
Delta	1	0.44	325
Delta	2	0.39	300
Delta	3	0.35	276
Epsilon	1	0.55	410
Epsilon	2	0.50	382
Epsilon	3	0.46	350
Zeta	1	0.51	398
Zeta	2	0.47	366
Zeta	3	0.43	338
Eta	1	0.58	430
Eta	2	0.54	402
Eta	3	0.50	370
Theta	1	0.57	420
Theta	2	0.52	392
Theta	3	0.48	360

The undesirable outputs, treated under a non-deterioration constraint, are defined as:

- U1, weighted index of loss of primary containment (LOPC) events; and
- U2, annual hours of unplanned shutdowns related to integrity.

Table 4 – Dyn-DEA Carry-Overs

DMU Refinery	Year	C1 (%)	C2 (backlog)
Alpha	1	87	142
Alpha	2	89	130
Alpha	3	91	118
Beta	1	82	168
Beta	2	84	150
Beta	3	86	134
Gama	1	88	152
Gama	2	90	137
Gama	3	92	120
Delta	1	89	145
Delta	2	91	130
Delta	3	93	118
Epsilon	1	83	176
Epsilon	2	85	160
Epsilon	3	87	142
Zeta	1	84	170

Zeta	2	86	155
Zeta	3	88	138
Eta	1	82	188
Eta	2	84	170
Eta	3	86	152
Theta	1	83	182
Theta	2	85	165
Theta	3	87	148

The intertemporal linking variables are:

- C1, barrier health at the end of the year (classified as a desirable carry-over), and
- C2, the critical backlog of Process Safety actions at the end of the year (classified as an undesirable carry-over).

4. Performance Results from Dyn-DEA

The adopted mathematical formulation is output-oriented, aiming to maximize a common expansion factor $\varphi \geq 1$, which represents the extent to which the desirable outputs of a given refinery could be increased while maintaining constant input levels and respecting the constraints associated with undesirable outputs and carry-overs. For each evaluated refinery, intensity variables $\lambda_{j,t} \geq 0$ were defined, corresponding to convex combinations of the other refineries in each year. The objective function consisted of maximizing φ. The constraints required that, for each year, the weighted combination of the reference refineries' inputs did not exceed the observed inputs of the evaluated refinery; that the weighted combination of desirable outputs was greater than or equal to φ times the observed outputs; that the weighted combination of undesirable outputs did not exceed the observed values; that the desirable carry-over (C1) was not lower than observed; and that the undesirable carry-over (C2) was not higher than observed. The efficiency score is given by $1/\varphi^{\backslash *}$, where $\varphi^{\backslash *}$ denotes the optimal value obtained.

Using the dataset presented in Tables 1 through 4, the following period-specific efficiencies were obtained, as shown in Table 5, along with the global efficiencies (with a common φ across the years) displayed in Table 6.

Table 5 – Point-in-Time Efficiencies of the DMUs

Refinery	Efficiency T=1	Efficiency T=2	Efficiency T=3
Alpha	0.91	0.95	1.00
Beta	0.82	0.86	0.89
Gama	0.94	0.98	1.00
Delta	0.95	0.99	1.00
Epsilon	0.78	0.82	0.86
Zeta	0.80	0.84	0.88
Eta	0.73	0.77	0.81
Theta	0.75	0.79	0.83

Table 6 – Overall Efficiencies of the DMUs

Refinery	Global Dynamic Efficiency	Trend
Alpha	0.95	Frontier at T=3
Beta	0.86	Consistent improvement
Gama	0.97	Frontier at T=2,T=3
Delta	0.98	Frontier at T=2,T=3
Epsilon	0.82	Gradual gain
Zeta	0.84	Moderate improvement
Eta	0.77	Structural inefficiency
Theta	0.79	Slow gain

The model identifies three typical patterns among Brazilian refineries:

1. Dynamic frontier: Alpha, Gama, and Delta — simultaneously accumulate integrity and reduce backlog.
2. Transitional efficiency: Beta and Zeta — operational gains are observed, but undesirable carry-over remains high.
3. Structural inefficiency: Eta and Theta — persistent limitations in integrity and organizational learning.

The dynamics indicate that C1 and C2 account for a greater share of overall efficiency than isolated inputs, confirming that process safety is a cumulative phenomenon.

5 Conclusion

The application of this Dyn-DEA modelling with intertemporal linking variables allows for robust conclusions regarding the structural performance of Process Safety in large integrated refineries in Brazil, such as:

Process safety efficiency is cumulative rather than instantaneous. The model demonstrates that efficient refineries are not merely those that invest more each year, but those that convert investments into accumulated integrity, thereby reducing critical backlog over time. Consequently, efficiency is determined by the

intertemporal trajectory rather than by point-in-time results.

Linking variables explain more than isolated inputs. Final barrier health and critical backlog are shown to be structural determinants of dynamic efficiency. Refineries with strong current indicators but a growing backlog tend to experience future efficiency losses.

Organizational learning has a measurable impact. High percentages of effectively implemented recommendations correlate with simultaneous improvements in safe availability, integrity, and event reduction, indicating that institutional learning acts as an efficiency multiplier.

Structural inefficiency tends to persist. Refineries with low initial integrity and high backlog exhibit slow recovery trajectories, suggesting that Process Safety exhibits organizational hysteresis: accumulated problems increase the effort required to return to the efficient frontier.

Investment-focused policies alone may be insufficient. The model shows that increasing expenditures does not necessarily guarantee efficiency if there is no effective governance, closure of critical pending actions, and consolidation of barriers.

References

American Petroleum Institute (API). *Recommended Practice 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries.* Washington, DC: American Petroleum Institute, 2016.

Amirteimoori, Alireza. "Data Envelopment Analysis in Dynamic Framework." *Applied Mathematics and Computation* 181, no. 1 (October 1, 2006): 21–28.

Banker, Rajiv D., Abraham Charnes, and William W. Cooper. "Some Models for Estimating Technical and Scale Inefficiencies in Data Envelopment Analysis." *Management Science* 30, no. 9 (1984): 1078–1092.

Center for Chemical Process Safety (CCPS). *Guidelines for Risk Based Process Safety.* Hoboken, NJ: Wiley-AIChE, 2007.

Charnes, Abraham, William W. Cooper, and Edwardo Rhodes. "Measuring the Efficiency of Decision Making Units." *European Journal of Operational Research* 2, no. 6 (1978): 429–444.

Cooper, William W., Lawrence M. Seiford, and Kaoru Tone. *Data Envelopment Analysis: A Comprehensive Text with Models, Applications, References and DEA-Solver Software.* 2nd ed. Boston: Springer, 2007.

Emrouznejad, Ali, and Emmanuel Thanassoulis. "A Dyn-DEA Model for Performance Measurement." *Journal of the Operational Research Society* 61, no. 4 (2010): 569–580.

Färe, Rolf, and Shawna Grosskopf. *Intertemporal Production Frontiers: With Dyn-DEA*. Boston: Kluwer Academic Publishers, 1996.

Gary, James H., Glenn E. Handwerk, and Mark J. Kaiser. *Petroleum Refining: Technology and Economics.* 5th ed. Boca Raton: CRC Press, 2007.

Kao, Chiang. "Dynamic Data Envelopment Analysis: A Relational Analysis." *European Journal of Operational Research* 227, no. 2 (2013): 325–330.

Nemoto, Jiro, and Mika Goto. "Measurement of Dynamic Efficiency in Production: An Application of Data Envelopment Analysis to Japanese Electric Utilities." *Journal of Productivity Analysis* 19 (April 2003): 191–210.

Sengupta, Jati K. "A Dynamic Efficiency Model Using Data Envelopment Analysis." *International Journal of Production Economics* 62, no. 3 (September 1999): 209–218.

Speight, James G. *The Chemistry and Technology of Petroleum.* 5th ed. Boca Raton: CRC Press, 2014.

Sueyoshi, Toshiyuki, and Kazuyuki Sekitani. "Returns to Scale in Dyn-DEA." *European Journal of Operational Research* 161, no. 2 (March 2005): 536–544.

Szklo, Alexandre Salem, Victor Cohen Uller, and Marcio Henrique P. Bonfá. *Fundamentos do Refino de Petróleo: Tecnologia e Economia.* 3rd ed. Rio de Janeiro: Interciência, 2012.

Szklo, Alexandre, and Roberto Schaeffer. *Energy and the Brazilian Economy.* Rio de Janeiro: Interciência, 2007.

Tone, Kaoru, and Miki Tsutsui. "Dyn-DEA with Network Structure: A Slacks-Based Measure Approach." *Omega* 42, no. 1 (January 2014): 124–131.

Tone, Kaoru, and Miki Tsutsui. "Dyn-DEA: A Slacks-Based Measure Approach." *Omega* 38, no. 3–4 (June–August 2010): 145–156.

Tone, Kaoru. "A Slacks-Based Measure of Efficiency in Data Envelopment Analysis." *European Journal of Operational Research* 130, no. 3 (May 2001): 498–509.