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.