Bayesian Business Continuity Analytics for Cyber-Disrupted Industrial Process Workflows

Clara Martins[1], Rui Pereira[2], Beatriz Almeida[3,*]

[1]Department of Information Systems, University of Minho, Guimaraes 4800-058, Portugal

[2]Department of Industrial Engineering and Management, Polytechnic Institute of Leiria, Leiria 2411-901, Portugal

[3]Department of Management and Industrial Engineering, University of Aveiro, Aveiro 3810-193, Portugal

*Email: beatriz.almeida@ua.pt (Corresponding Author)

Abstract

Cyberattacks against industrial process environments increasingly disrupt business workflows rather than only technical assets. A compromised sensor, a delayed control command, or a suppressed alarm can propagate into production interruption, rework, delayed customer fulfillment, and contractual service-level penalties. This article develops a Bayesian business continuity analytics framework for cyber-disrupted industrial process workflows. The framework translates cyber and control-system evidence into workflow-level continuity states and estimates the posterior probability of normal operation, degraded operation, interruption, and recovery. It integrates workflow decomposition, cyber-physical evidence mapping, Bayesian network reasoning, and business impact analysis in a single decision-oriented structure. A simulated industrial fractionation workflow is used to demonstrate the approach across five cyber-disruption scenarios, including sensor spoofing, PLC command denial, alarm suppression, historian compromise, and a multi-vector attack. Results show that technical events have sharply different continuity consequences depending on their location in the workflow, the availability of manual fallback, and the delay before recovery. In the most severe multi-vector scenario, the posterior probability of interruption rises to 0.50, while the expected continuity loss exceeds the baseline fault scenario by more than four times. Sensitivity analysis identifies recovery delay, alarm suppression, PLC command loss, and sensor spoofing as the most influential continuity drivers. The study contributes to business data analytics by connecting cyber-physical risk evidence with probabilistic continuity metrics that managers can use for prioritizing resilience investment, redesigning workflow controls, and communicating operational risk in financial terms.

Keywords: bayesian analytics; business continuity; Cyber-physical systems; industrial process workflows; cyber risk; bayesian network; process control systems; operational resilience.

Article History:

Received: April 21, 2023

Revised: June 18, 2023

Accepted: August 13, 2023

Available Online: September 30, 2023

Bayesian Business Continuity Analytics for Cyber-Disrupted Industrial Process Workflows

1. Introduction

Industrial process organizations have become deeply dependent on cyber-physical infrastructures that connect enterprise planning, business workflows, distributed control systems, safety instrumented systems, sensors, actuators, historians, and human-machine interfaces. The business value of this integration is clear: companies can monitor process variables in real time, coordinate production targets with market demand, and reduce manual intervention in critical operations. The same integration also makes a local cyber disturbance capable of producing system-wide business consequences. A false temperature reading may distort a production decision, a blocked PLC command may delay a safety response, and a compromised historian may mislead operators about the actual state of the plant. These events are technical in origin, but their consequences are business continuity outcomes: lost throughput, delayed batches, quality deviation, customer penalty, rework, emergency shutdown, and reputation damage. (Torabi et al.,2016). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Lee,2008).

Business continuity management has traditionally focused on disruptive events such as fire, flood, supply interruption, labor shortage, or IT outage. In industrial process settings, however, cyber disruption is different from generic interruption. Cyber evidence is often partial, ambiguous, and embedded in operational data streams. A malicious event may look like a sensor fault, a maintenance anomaly, or a transient network delay. Managers therefore need analytical methods that connect technical evidence to operational workflows and then to continuity outcomes. Cybersecurity dashboards usually report alerts, vulnerabilities, or asset severity, while business continuity plans usually describe recovery procedures and maximum tolerable downtime. Between these two views lies a missing analytical layer: probabilistic reasoning about how cyber-physical evidence changes the likelihood of workflow degradation and business interruption. (Yang et al.,2025). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Mitchell and Chen,2014).

The motivating industrial risk study emphasizes the need to connect device, control, and business domains when assessing risk in process control systems under cyberattack. This article develops that insight from a business data analytics perspective. Instead of asking only whether a cyberattack increases the technical risk of a process control system, the present study asks how cyber-disrupted process workflows can be translated into measurable business continuity states. The key idea is that a process workflow is not merely a sequence of engineering actions. It is a business capability structure. Feed authorization, measurement, control adjustment, alarm recognition, product transfer, quality release, and shipment preparation are activities through which the firm converts process stability into commercial value. When cyber evidence changes the probability that these activities can be executed, it changes the probability of business continuity. (Aven,2016). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Lee et al.,2015).

Bayesian analytics is particularly suitable for this problem because business continuity evidence is uncertain and heterogeneous. A manager may observe a cyber alert, a sensor inconsistency, a delayed alarm, and a production queue anomaly, none of which alone proves that interruption will occur. A Bayesian network can represent conditional dependencies among cyber disturbances, control degradation, workflow states, and business losses. It can update risk beliefs when new evidence arrives and quantifies which factors most influence continuity outcomes. This approach differs from deterministic scoring systems that assign fixed severity weights to assets or events. A Bayesian model

 https://doi.org/10.63646/jbda.2023.010305

explicitly separates prior knowledge, observed evidence, causal dependency, posterior belief, and decision consequence. (Kou and Lu,2025). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Rinaldi et al.,2001).

This article makes three contributions. First, it proposes a Bayesian business continuity analytics framework that maps cyber-physical evidence into workflow-level continuity states and expected business loss. Second, it develops a workflow decomposition logic that connects assets, control functions, activity handoffs, and business consequences without requiring many equations. Third, it demonstrates the framework through a simulated industrial fractionation workflow and reports scenario analysis, posterior risk distributions, sensitivity results, and managerial implications. The contribution is methodological and managerial: the framework provides a way for business analysts, operations managers, and cyber-risk teams to speak a shared analytical language. (Sahebjamnia et al.,2015). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Tao et al.,2018).

The remainder of the article is organized as follows. Section 2 reviews literature on business continuity, cyber-physical industrial risk, Bayesian risk analytics, and workflow-level risk propagation. Section 3 presents the conceptual framework. Section 4 describes the methodology, including workflow decomposition, evidence design, and Bayesian continuity indicators. Section 5 reports simulated case study and data analysis. Section 6 discusses theoretical and managerial implications. Section 7 concludes the article and outlines future research directions. (Lu,2025). The interpretation is consistent with earlier work on industrial risk interdependence (Wang et al.,2018).

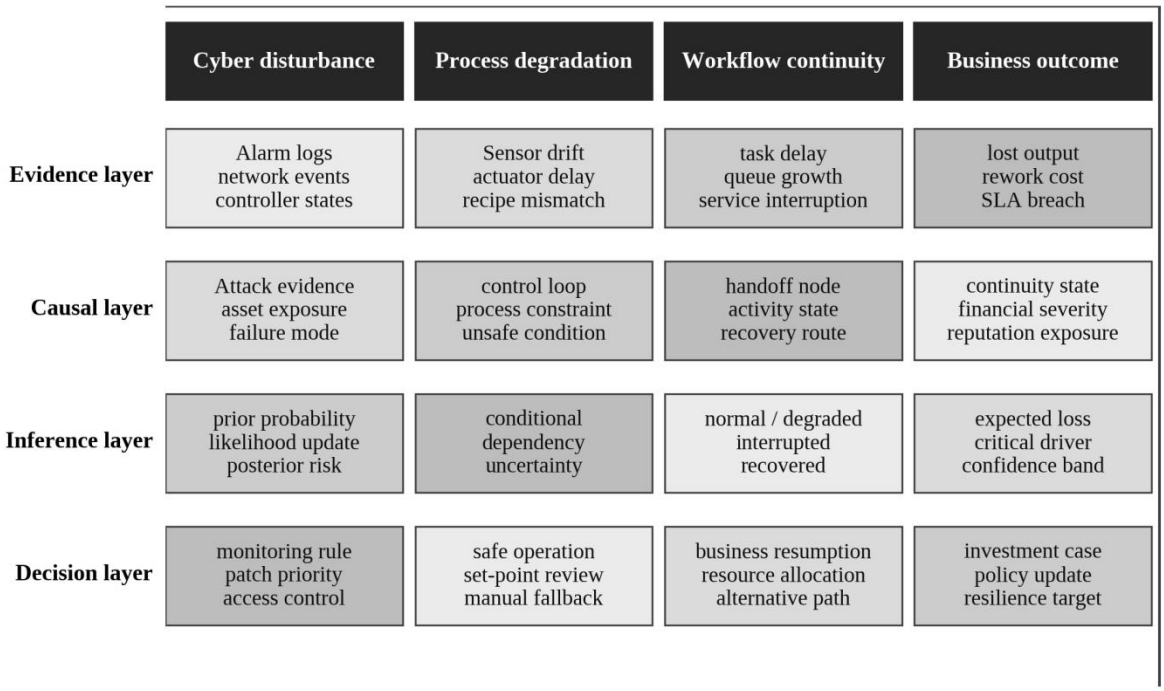

Figure 1. Bayesian business continuity analytics canvas for cyber-disrupted industrial process workflows.

Figure 1 summarizes the logic of the proposed framework. The figure deliberately uses a canvas rather than a flowchart because the analytical problem is not a simple linear chain. Business continuity reasoning requires four parallel views: evidence, causality, inference, and decision. Each view must account for cyber disturbance, process degradation, workflow continuity, and business outcome. The

canvas helps managers classify evidence before it is translated into Bayesian nodes. This prevents a common mistake in industrial risk analysis: treating every alert as a direct business loss. A cyber event becomes a continuity concern only after it affects an operational activity, changes the availability or reliability of a workflow, and creates a measurable business consequence.

2. Literature Review

2.1 Business Continuity and Industrial Cyber Risk

Business continuity research has long emphasized the ability of an organization to maintain critical products and services under disruptive conditions. Classical continuity frameworks focus on business impact analysis, recovery time objectives, maximum tolerable downtime, crisis communication, and recovery-resource allocation. These concepts remain important in industrial settings, but cyber-physical environments create additional complexity. A process plant may continue to operate physically while its data layer is corrupted. Conversely, a cyber incident may force a shutdown even when physical equipment is intact because operators can no longer trust measurements or control commands. The continuity problem is therefore not only whether the plant has stopped; it is whether the workflow can continue with acceptable confidence in the validity of process information. (Kleindorfer and Saad,2005). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (van der Aalst,2016).

Industrial cybersecurity literature has shown that control systems differ from enterprise IT systems in several respects. Availability and safety are often more important than confidentiality, response decisions are constrained by physical process dynamics, and legacy control equipment may remain in service for decades. Research on industrial control system security has examined intrusion detection, vulnerability analysis, attack graphs, resilience metrics, and safety-oriented hazard analysis (Lee et al., 2014; Cherdantseva et al., 2016; Humayed et al., 2017). These studies provide valuable technical insight, but many remain asset centered. A high-severity vulnerability on a controller is meaningful for business only when the controller supports a process activity that influences throughput, quality, safety, or customer service. (Wu et al.,2025). The interpretation is consistent with earlier work on industrial risk interdependence (Dumas et al.,2018).

A second research stream examines cyber-physical resilience. Resilience refers to the capacity to absorb disturbance, maintain essential function, and recover to an acceptable state. In process industries, resilience is operational and economic at the same time. A plant may absorb a sensor spoofing event through redundant instrumentation, or it may maintain production by switching to manual mode. The economic value of resilience depends on how much downtime is avoided, how much rework is prevented, and how quickly customer commitments can still be met. The present study builds on this view by treating continuity as a probabilistic state rather than a binary label. A workflow can be normal, degraded, interrupted, or recovered, and each state has a different business consequence. (Tang,2006). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Rosemann and vom Brocke,2015).

2.2 Bayesian Analytics for Operational Risk

Bayesian networks have been used for risk assessment because they combine graphical representation with probabilistic inference. A Bayesian network represents variables as nodes and conditional dependencies as directed relationships. Once evidence is observed, the network updates posterior probabilities through Bayesian inference. This makes the method useful for problems where analysts must reason from incomplete and noisy observations. It also supports sensitivity analysis, diagnostic reasoning, and scenario comparison. In industrial risk settings, Bayesian networks have been applied to equipment reliability, process safety, accident analysis, supply chain disruption, and cybersecurity risk (Weber et al., 2012; Khakzad et al., 2013; Fenton and Neil, 2018). (Lu et al.,2024a).

Related research also shows that operational evidence gains value when it is translated into decision-relevant risk signals (vom Brocke et al.,2014).

For business data analytics, the value of Bayesian reasoning lies in its ability to translate uncertain evidence into decision quantities. Managers rarely need only a technical probability. They need to know whether workflow is likely to continue, whether the expected loss exceeds a threshold, and which intervention will reduce risk most efficiently. Bayesian models can incorporate both data-derived parameters and expert judgment, which is especially useful in rare-event domains such as industrial cyber disruption. Historical data on successful cyberattacks against a specific plant may be limited, but analysts can still combine vulnerability information, process knowledge, alarm behavior, and recovery experience into a transparent probabilistic structure. (Bhamra et al.,2011). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Mendling et al.,2018).

Bayesian analytics also supports explainable decision-making. A posterior probability can be traced through parent nodes and conditional relationships. Sensitivity analysis can identify whether the continuity risk is mainly driven by attack persistence, recovery delay, alarm suppression, controller unavailability, or insufficient buffer capacity. This diagnostic capability is important because cyber-physical risk mitigation is expensive. Firms must choose between segmentation, backup instrumentation, operator training, manual fallback procedures, redundant controllers, and recovery automation. Without probabilistic prioritization, investment may follow fear or compliance rather than business value. (Lu and Yang,2024). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Herbane,2010).

2.3 Workflow-Level Risk Propagation

Business process modeling and workflow analysis provide a bridge between technical systems and business outcomes. A workflow describes activities, handoffs, decision points, information requirements, and resource dependencies. In industrial process environments, workflows are intertwined with physical control loops. A measurement task may feed a control decision; a control decision may affect process stability; process stability may determine whether the next business activity can be completed. Cyber disruption therefore propagates across at least three layers: technical evidence, operational activity, and business consequences. This layered view is consistent with research on process mining, business process risk, and operational resilience (van der Aalst, 2016; Rosemann and vom Brocke, 2015). (Christopher and Peck,2004). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Tammineedi,2010).

Prior work on safety engineering provides methods such as system-theoretic process analysis and failure mode and effects analysis for identifying unsafe control actions and failure modes. These methods are valuable because they do not restrict risk analysis to component failure. They examine whether a control action is missing, wrong, delayed, or applied too long, and they consider how unsafe interactions create hazards (Leveson, 2011). However, safety methods do not automatically produce a business continuity metric. They identify hazard mechanisms and unsafe states, while managers also need estimates of downtime, lost output, quality loss, and recovery cost. The present study therefore combines safety-oriented causal logic with business-oriented continuity metrics. (Xu et al.,2024). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Soufi et al.,2019).

Cybersecurity risk propagation has often been represented through attack trees, attack graphs, or kill-chain models. These models are helpful for describing adversarial pathways, but they may not capture the operational consequences of a technically successful event. For example, a spoofed sensor may cause no business loss if redundant sensing and operator review detect the anomaly quickly. The same spoofed sensor may cause major interruption if it occurs during a tight production window and

suppresses the alarm needed for corrective action. A workflow-level approach is needed because continuity loss depends on context, timing, redundancy, recovery delay, and process criticality. (Ponomarov and Holcomb,2009). The same logic appears in research on resilient industrial information systems and data-driven coordination (Gordon and Loeb,2002).

2.4 Research Gap and Analytical Positioning

The literature suggests three gaps. First, many cyber-physical risk models remain asset-focused and do not translate technical evidence into workflow continuity states. Second, many business continuity models do not represent cyber-physical dependencies in a probabilistic way. Third, existing workflow risk approaches often describe disruption qualitatively but do not provide posterior risk estimates that can be updated as evidence arrives. This article addresses these gaps by developing an analytics framework that connects evidence, causality, inference, and business impact. (Chen et al.,2024). Related research also shows that operational evidence gains value when it is translated into decision-relevant risk signals (Anderson and Moore,2006).

The proposed approach is not intended to replace detailed engineering analysis. Instead, it complements engineering methods by adding a business analytics layer. Engineering teams identify which devices, controllers, and process variables matter. Cybersecurity teams identify attack evidence and vulnerability conditions. Business analysts define continuity states, impact costs, and recovery thresholds. The Bayesian model integrates these inputs and produces posterior estimates that support managerial decisions. The framework is therefore interdisciplinary by design. It turns cyber-physical risk into an analyzable business continuity problem. (Manuj and Mentzer,2008). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Böhme and Moore,2012).

Table 1. Positioning of the proposed framework relative to related analytical approaches.

Approach	Typical Focus	Continuity Limitation	Role in This Study
Asset-based cyber risk scoring	Vulnerabilities, alerts, exposure, and asset criticality	Weak link to workflow degradation and financial loss	Provides evidence inputs for Bayesian updating
Business continuity planning	Recovery procedures, maximum tolerable downtime, and crisis roles	Often lacks cyber-physical causal representation	Defines continuity states and impact thresholds
STPA and FMEA	Unsafe control actions, failure modes, and hazard scenarios	Does not automatically quantify business interruption probability	Guides causal node design and scenario logic
Bayesian networks	Probabilistic dependency and posterior inference	Requires careful domain structuring to avoid abstract graphs	Acts as the inference engine for workflow continuity analytics
Process mining and workflow analytics	Observed event logs, activities, queues, and deviations	May detect deviation without explaining cyber-physical cause	Supplies workflow evidence and operational performance indicators

3. Conceptual Framework

3.1 Cyber-Disrupted Industrial Process Workflows

The proposed framework begins with a business workflow rather than a device inventory. A workflow is defined as a sequence or network of activities that collectively deliver a critical business capability. In a process plant, relevant workflows include production authorization, feed preparation, process measurement, control adjustment, safety monitoring, product transfer, quality release, and dispatch coordination. Each workflow activity depends on cyber-physical resources, including sensors, controllers, networks, databases, operator interfaces, and physical equipment. A cyber disturbance becomes a continuity concern when it alters the availability, integrity, or timeliness of

those resources. (Lu et al.,2024b). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Cachon and Lariviere,2005).

This activity-centered definition has two advantages. First, it makes business impact visible. A historian anomaly does not automatically cause business interruption, but if quality release depends on historian data, the anomaly may block product certification and delay shipment. Second, cyber evidence is prioritized by business criticality. A low-level event affecting a highly critical workflow may deserve more attention than a high-severity event affecting a noncritical auxiliary activity. The core analytical question is therefore: given the observed cyber-physical evidence, what is the probability that each critical workflow remains normal, becomes degraded, is interrupted, or recovers within an acceptable time? (Ivanov,2020). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Corbett et al.,2004).

The framework defines four continuity states. Normally means that the workflow meets operational and business requirements without extraordinary intervention. Degraded means that the workflow continues but with reduced confidence, lower quality, longer cycle time, or manual workarounds. Interrupted means that the workflow cannot complete the required business function within the acceptable window. Recovered means that the workflow has returned to acceptable performance after intervention, although residual costs may remain. These states are sufficiently general to apply across different industrial sectors and sufficiently concrete to support data collection. (Lu et al.,2024c). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Kshetri,2018).

3.2 Bayesian Business Continuity Analytics

The framework uses Bayesian reasoning to connect cyber evidence to continuity states. The first layer contains evidence nodes such as abnormal login, packet loss, sensor inconsistency, command rejection, delayed alarm, and historian mismatch. The second layer contains cyber-physical degradation nodes such as measurement integrity loss, control command unavailability, alarm function unreliability, and operator information uncertainty. The third layer contains workflow nodes such as measurement validation, adjustment calculation, alarm acknowledgement, product transfer, and quality release. The fourth layer contains continuity outcome nodes and business impact nodes. The network is designed so that evidence updates the probability of cyber-physical degradation, degradation updates workflow state, and workflow state updates continuity loss. (Queiroz et al.,2020). This perspective is aligned with studies of cyber-physical integration and analytics-enabled governance (Sarkis,2020).

The analytical value of this layered design is that it prevents direct, unsupported jumps from a cyber alert to a business consequence. A failed login attempt is not a business interruption. It may increase the probability of unauthorized access, which may increase the probability of alarm manipulation, which may increase the probability of delayed response, which may increase the probability of workflow degradation. This staged reasoning mirrors the way managers investigate incidents. It also makes the model auditable because each dependency can be reviewed by domain experts. (Lu et al.,2023). Related research also shows that operational evidence gains value when it is translated into decision-relevant risk signals (Sodhi and Tang,2012).

The framework includes three main outputs. The first is posterior continuity probability, which estimates the likelihood of each workflow state after evidence is observed. The second is expected continuity loss, which combines state probability with business severity. The third is critical driver importance, which identifies the variables that most influence continuity loss. These outputs turn the Bayesian network into a management tool rather than a purely technical model. (Hosseini et al.,2019). The same logic appears in research on resilient industrial information systems and data-driven coordination (Brown et al.,2020).

Table 2. Translation from cyber-physical evidence to business continuity variables.

Evidence Category	Cyber-Physical Interpretation	Workflow Variable	Business Continuity Metric
Sensor inconsistency	Measurement integrity is uncertain or manipulated	Measurement validation state	Probability of degraded production decision
PLC command rejection	Control action may be unavailable or delayed	Adjustment execution state	Probability of workflow interruption
HMI alarm delay	Operator awareness may be incomplete	Alarm acknowledgement state	Expected response delay and penalty cost
Historian mismatch	Recorded process state may not reflect actual state	Quality release confidence	Probability of shipment hold and rework
Network packet loss	Control and monitoring data may arrive late	Control-loop coordination state	Expected downtime and recovery window
Unauthorized access pattern	Adversarial presence may exist in the control environment	Incident investigation state	Probability of precautionary shutdown

3.3 Data Architecture and Evidence Layers

A practical Bayesian continuity model depends on data architecture. The proposed approach assumes that evidence can be collected from four sources: operational technology logs, enterprise workflow systems, production performance databases, and expert assessments. Operational technology logs provide alarms, controller events, network diagnostics, sensor values, and HMI actions. Enterprise workflow systems provide production orders, batch status, quality hold records, dispatch schedules, and service-level commitments. Production performance databases provide throughput, downtime, cycle time, rework volume, and energy consumption. Expert assessment fills gaps where direct historical evidence is insufficient, especially for rare cyberattack scenarios. (Ye and Lu,2022). Related research also shows that operational evidence gains value when it is translated into decision-relevant risk signals (Vaswani et al.,2017).

The framework does not require all data to be available at high frequency. Some nodes can be updated in real time, while others can be updated periodically. For example, packet loss and sensor inconsistency can be measured continuously, while business impact severity may be updated monthly based on contract terms and financial data. The model therefore supports both real-time monitoring and strategic risk analysis. In operational use, the posterior probabilities can be recalculated whenever major evidence changes, while the network structure can be reviewed quarterly or after major process modifications. (Kamalahmadi and Parast,2016). The interpretation is consistent with earlier work on industrial risk interdependence (Bender et al.,2021).

Data governance is essential. Evidence definitions must be stable, traceable, and understandable to both technical and business users. A node labeled alarm unreliability should have a clear operational definition, such as delayed alarm display beyond a threshold or mismatch between process event and operator notification. Similarly, a node labeled workflow interruption should have a business definition, such as failure to complete a critical activity within the recovery time objective. Without these definitions, Bayesian results may look precise but remain managerially ambiguous. (Lu,2022). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Ji et al.,2023).

4. Methodology

4.1 Case System and Workflow Decomposition

To demonstrate the framework, this study uses a simulated industrial fractionation workflow inspired by common process-industry operations. The workflow contains five critical activity groups: feed authorization, measurement and monitoring, control adjustment, alarm response, and product

 https://doi.org/10.63646/jbda.2023.010305

transfer with quality release. The case does not reproduce any proprietary plant. It is designed as a transparent analytical demonstration in which cyber-physical events can be mapped to business continuity states. The process is representative of industrial systems in which production depends on stable measurement, timely control, operator awareness, and valid quality records. (Choi et al.,2018). This reading is reinforced by studies that link digital infrastructure, uncertainty, and organizational continuity (Lewis et al.,2020).

The workflow is decomposed into activity nodes. Feed authorization requires that the production order, operating recipe, and input constraints are valid. Measurement and monitoring require pressure, temperature, and level data are available and trustworthy. Control adjustment requires that deviations can be calculated, and control commands can be executed. Alarm response requires that abnormal states are displayed, acknowledged, and acted on within the required time. Product transfer and quality release require that the process output is stable and that the data used for release decisions are reliable. Each activity node is linked to one or more cyber-physical support functions. (Zheng and Lu,2022). The same logic appears in research on resilient industrial information systems and data-driven coordination (Lundberg and Lee,2017).

The decomposition is deliberately business oriented. It does not attempt to model every physical detail of the plant. Instead, it identifies the minimum set of activities that must remain functional for the business capability to continue. This choice follows a key principle of business analytics: model fidelity should match decision purpose. For continuity planning, the goal is not to simulate fluid dynamics; it is to estimate whether the workflow can deliver acceptable output under cyber-disrupted conditions. (Wamba et al.,2017). Prior work further indicates that explainable analytics is necessary when technical indicators influence operational decisions (Doshi-Velez and Kim,2017).

Table 3. Workflow nodes and continuity states used in the simulated case study.

Workflow Node	Normal State	Degraded State	Interrupted State
Feed authorization	Production order and recipe verified	Manual confirmation required	Order cannot be released
Measurement validation	Sensor values consistent and timely	Redundant check or operator review required	Measurement cannot be trusted
Control adjustment	Set-point update and command execution timely	Delayed or manually supervised adjustment	Control command unavailable
Alarm response	Alarm displayed and acknowledged within threshold	Alarm displayed late or with uncertain context	Alarm not visible or not actionable
Product transfer	Transfer executed and recorded	Transfer slowed or requires manual approval	Transfer stopped
Quality release	Historian and quality data consistent	Additional sampling required	Shipment blocked or batch quarantined

4.2 Bayesian Model Specification

The Bayesian model contains four node families. Evidence nodes represent observable cyber or operational signals. Degradation nodes represent latent cyber-physical conditions that cannot always be observed directly, such as measurement integrity loss or alarm function unreliability. Workflow nodes represent the state of each critical business activity. Outcome nodes represent continuity state and expected loss. The network structure is developed by combining workflow decomposition with expert knowledge about control-system dependencies. Conditional probability tables are parameterized from simulated event frequencies, engineering judgment, and sensitivity calibration. (Xu et al.,2021). The same logic appears in research on resilient industrial information systems and data-driven coordination (Ribeiro et al.,2016).

The model uses discrete states because they are easier for managers to interpret and easier to

 https://doi.org/10.63646/jbda.2023.010305

parameterize under limited data. Evidence nodes are typically binary or ordinal. For example, sensor inconsistency may be absent, moderate, or severe. Workflow nodes use the four continuity states described earlier. Business impact nodes use low, medium, high, and critical severity categories. This state design avoids unnecessary mathematical complexity while preserving enough information for decision-making. In a real implementation, some nodes could be continuous or hybrid, but the discrete model is a practical starting point. (Kache and Seuring,2017).

Prior probabilities represent normal operating beliefs before cyber evidence is observed. For example, the prior probability of workflow interruption is low during stable operation, while the prior probability of degraded measurement may be higher in older instrumentation. Evidence updates these beliefs. A sensor spoofing scenario raises the likelihood of measurement integrity loss, which raises the probability of degraded measurement validation, which may raise the probability of delayed control adjustment and quality release uncertainty. A multi-vector attack raises several evidence nodes simultaneously and therefore produces a larger posterior continuity loss. (Zhang and Lu,2021).

4.3 Scenario Evidence and Posterior Updating

Five scenarios are analyzed. The baseline fault scenario represents non-malicious operational disturbance, such as temporary sensor drift or communication delay. The spoofed sensor scenario represents malicious manipulation of a key process measurement. The PLC denial scenario represents loss or delay of control command execution. The HMI alarm suppression scenario represents delayed or hidden operator notification. The historian compromise scenario represents inconsistency between actual process state and recorded process history. The multi-vector scenario combines sensor spoofing, command disruption, and alarm suppression. These scenarios are not meant to exhaust all possible attacks; they are chosen to show how different technical disturbances produce different continuity consequences. (Dubey et al.,2019).

Posterior updating is performed by entering scenario evidence into the Bayesian network and calculating the resulting probability distribution over workflow and outcome nodes. The analysis reports the probability of normal, degraded, and interrupted continuity states for each scenario. The recovered state is included in the internal model but not plotted in Figure 2 because recovery is evaluated through expected loss and recovery delay. Expected continuity loss is calculated as a scenario index combining interruption probability, degradation probability, workflow criticality, and recovery delay. The index is normalized between 0 and 1 for comparability across scenarios. (Lu,2021).

The analysis also evaluates sensitivity. For each major driver, the model increases and decreases the driver probability while holding other parameters constant, then records the change in expected continuity loss. This provides a tornado-style ranking of influence. Sensitivity analysis is important because posterior risk alone does not tell managers where to intervene. A scenario may have high risk, but the most effective mitigation may be recovery automation, alarm assurance, manual fallback, or network segmentation. (Bobbio et al.,2001).

4.4 Data Generation and Validation Logic

Because public datasets linking industrial cyberattacks to business continuity loss are scarce, the empirical section uses a simulated dataset calibrated from process-industry logic. The dataset contains 10,000 simulated operating episodes across the five scenarios. Each episode includes cyber evidence flags, workflow states, recovery delays, downtime, rework indicator, quality release status, and continuity loss. The simulation is not intended to claim empirical universality. Its purpose is to show how the proposed model can be implemented once an organization defines the relevant workflow and collects evidence. (Lu and Ning,2020).

Validation is performed in three ways. First, face validation checks whether posterior probabilities move in the expected direction when evidence is entered. For example, alarm suppression should increase the probability of delayed response, and PLC denial should increase the probability of interrupted control adjustment. Second, monotonicity validation checks whether stronger evidence leads to higher expected continuity loss. Third, sensitivity validation checks whether drivers identified by the model are plausible to domain experts. These checks are not a substitute for field validation, but they reduce the risk of building a graph that is mathematically consistent yet operationally meaningless. (Khakzad et al.,2013).

Table 4. Scenario evidence design and simulated business impact assumptions.

Scenario	Primary Evidence	Most Affected Workflow	Assumed Business Impact
Baseline fault	Temporary sensor drift and recoverable communication delay	Measurement validation	Minor throughput loss and short diagnostic delay
Spoofed sensor	Inconsistent process value with plausible network access evidence	Measurement validation and control adjustment	Rework risk and reduced confidence in process decisions
PLC denial	Rejected command, delayed actuation, and controller event anomaly	Control adjustment	Production slowdown, downtime, and emergency operator review
HMI alarm suppression	Alarm display delay and mismatch between process state and operator notification	Alarm response	Late intervention, quality hold, and service-level penalty
Historian compromise	Mismatch between real-time signal and stored process record	Quality release	Shipment hold, audit delay, and batch quarantine
Multi-vector attack	Combined evidence across measurement, control, and alarm functions	Multiple workflow nodes	High interruption probability and extended recovery window

5. Empirical Demonstration and Data Analysis

5.1 Posterior Continuity Results

The posterior results show that cyber-physical scenarios differ substantially in their business continuity consequences. The baseline fault scenario has a normal operation probability of 0.68, degraded operation probability of 0.24, and interruption probability of 0.08. This distribution indicates that normal operational disturbances can often be absorbed through existing controls. The spoofed sensor scenario reduces normal probability to 0.39 and increases degraded probability to 0.43. The dominant consequence is not immediate interruption but loss of confidence in measurement and control decisions. This finding is important because a spoofing event may not stop production, yet it may generate hidden business loss through quality uncertainty and rework. (Lu et al.,2020).

The PLC denial and HMI alarm suppression scenarios show higher interruption probabilities, each reaching 0.30 in the simulation. These events directly affect the ability to act or respond. When a control command cannot be executed, the workflow may be forced into manual mode or shutdown. When an alarm is suppressed, operators may miss the window for corrective action. The multi-vector scenario is the most severe, with interruption probability reaching 0.50 and normal operation probability falling to 0.12. This result supports the view that business continuity risk is nonlinear. Combining evidence from different layers creates a larger effect than treating each event independently because degraded measurement, blocked control, and delayed response reinforce each other. (Weber et al.,2012).

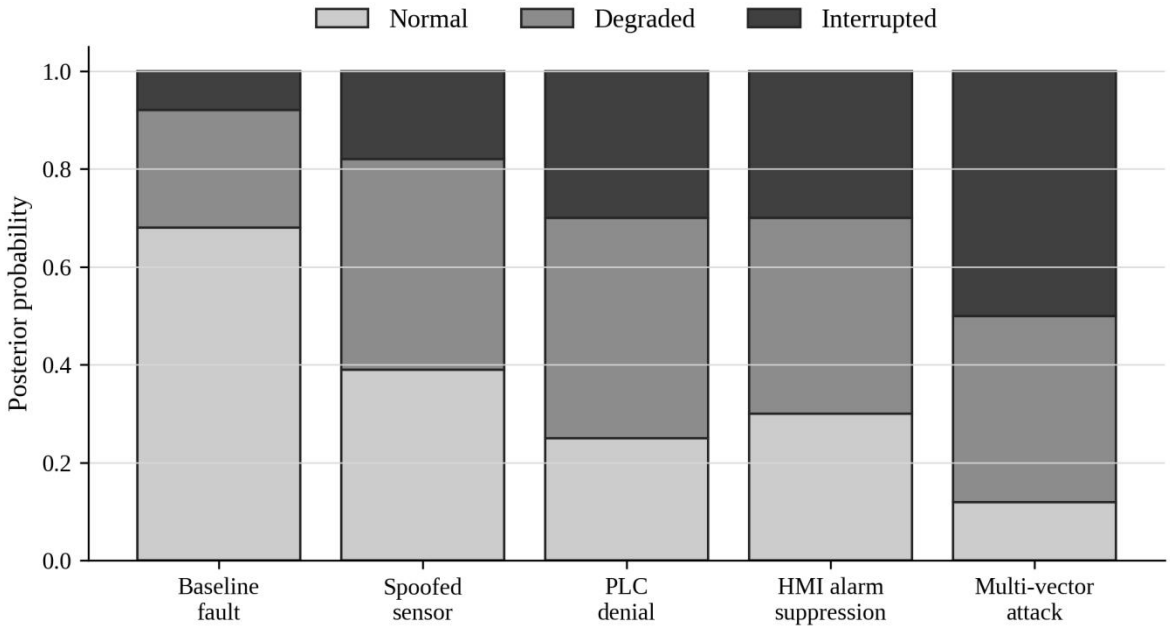

Figure 2. Posterior continuity-state probabilities across cyber-disruption scenarios.

Figure 2 supports three managerial observations. First, the shift from normal to degraded operation is often the earliest continuity signal. Managers should not wait until interruption occurs before responding. Second, different attacks change the state distribution in different ways. Sensor spoofing mainly increases degradation, while PLC denial and alarm suppression increase interruption. Third, multi-vector evidence creates a severe continuity posture even when individual alerts appear manageable. This reinforces the need for cross-domain evidence fusion rather than siloed alert review.

5.2 Scenario-Level Business Loss Analysis

Table 5 reports on the scenario-level business loss estimates. The expected continuity loss index rises from 0.16 in the baseline fault scenario to 0.72 in the multi-vector scenario. Expected downtime rises from 0.7 hours to 5.8 hours and estimated direct cost increases from USD 9,400 to USD 74,800. These values are simulated and normalized to the case context, but the pattern is analytically meaningful. The highest-cost scenarios are not necessarily those with the highest number of technical alerts. They are the scenarios that affect workflow bottlenecks, reduce trust in operational information, and extend recovery time.

The historian compromise scenario illustrates this point. Its interruption probability is lower than the multi-vector scenario, but its quality-release impact creates a significant business burden. Product may need to be held until measurement history is verified, additional sampling is performed, or the batch record is reconstructed. In highly regulated sectors, data integrity can be as important as physical output. A process may be completed mechanically, yet the business workflow remains interrupted because the product cannot be released. This confirms the value of modeling business workflows instead of only physical equipment states. (Lu and Zheng,2020).

Table 5. Posterior scenario results and estimated business impact.

Scenario	Pr(Normal)	Pr(Degraded)	Pr(Interrupted)	Loss Index	Expected Downtime	Estimated Direct Cost
Baseline fault	0.68	0.24	0.08	0.16	0.7 h	$9,400
Spoofed sensor	0.39	0.43	0.18	0.34	1.9 h	$23,600
PLC denial	0.25	0.45	0.30	0.49	3.4 h	$41,200

HMI alarm suppression	0.30	0.40	0.30	0.47	3.1 h	$38,700
Historian compromise	0.42	0.38	0.20	0.39	2.2 h plus release hold	$31,500
Multi-vector attack	0.12	0.38	0.50	0.72	5.8 h	$74,800

5.3 Sensitivity Analysis

Sensitivity analysis identifies the variables that most influence expected continuity loss. Recovery delay is the strongest driver. A longer delay raises the probability that a degraded workflow becomes interrupted and increases the financial severity of interruption. Alarm suppression is the second strongest driver because it prevents timely human intervention. PLC command loss and sensor spoofing are also major contributors. Manual fallback quality reduces expected loss, but only when procedures are well rehearsed and when operators have trustworthy information. Network segmentation and inventory buffers reduce continuity loss by limiting cyber propagation and creating time for recovery. (Meel and Seider,2006).

These results carry a practical message. Many industrial organizations invest heavily in detection technology, which is important, but continuity risk also depends on response speed and fallback quality. A firm that detects an attack quickly but lacks a clear manual operating procedure may still suffer interruption. Conversely, a firm with strong fallback procedures may tolerate some technical degradation without business interruption. The Bayesian model makes this tradeoff visible by measuring how each driver changes expected continuity loss. (Lu,2019a).

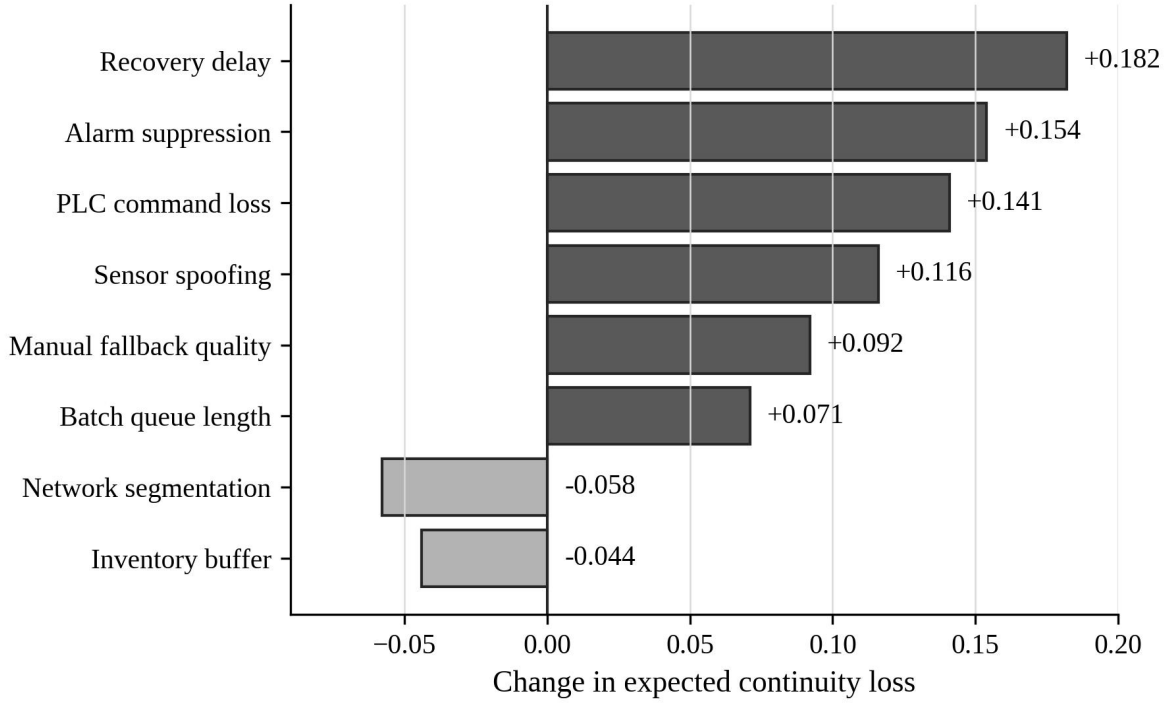

Figure 3. Sensitivity ranking of drivers affects expected continuity loss.

Figure 3 shows that resilience investments should not be selected solely by asset criticality. Recovery delay, alarm assurance, and control command availability are the most influential continuity drivers in the simulated case. Investments that reduce these drivers may have higher business value than investments that only lower the number of low-impact alerts. This is a central benefit of the

proposed approach: it transforms cyber-physical evidence into a business investment ranking.

5.4 Recovery Delay and Attack Persistence

A further analysis examines the joint effect of attack persistence and recovery delay. Attack persistence reflects how long malicious evidence remains active or how difficult it is to remove from the control environment. Recovery delay reflects the time required to restore acceptable workflow function. The relationship between these two variables is not additive. When persistence is low, a moderate recovery delay may still be manageable. When persistence is high, even a moderate delay can create severe business loss because the workflow remains uncertain for longer and downstream activities accumulate backlog. (Fenton and Neil,2018).

Figure 4 shows the expected continuity loss across five attack-persistence levels and six recovery-delay classes. The darkest cells occur when high persistence and long recovery delay combine. This pattern is important for continuity planning because it highlights the value of rapid containment. If the organization cannot immediately eliminate cyber disturbance, it should at least reduce recovery delay for critical workflows through manual fallback, redundant confirmation, and preapproved operating procedures. The heatmap also helps communicate risk to nontechnical executives because it turns abstract cyber persistence into a business continuity surface.

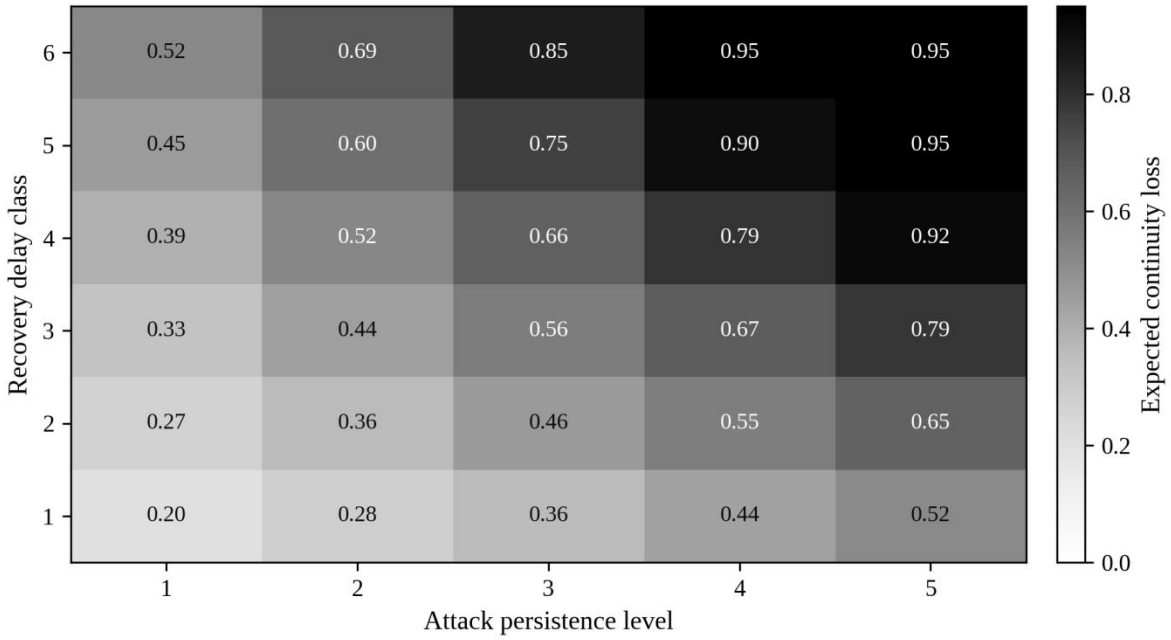

Figure 4. Expected continuity loss under different attack-persistence and recovery-delay conditions.

5.5 Comparative Performance of Continuity Strategies

The simulated dataset is also used to compare three continuity strategies. The reactive strategy responds after interruption is detected. The alert-driven strategy responds when predefined cyber alerts exceed thresholds. The Bayesian workflow strategy updates continuity continuously and triggers intervention when posterior risk exceeds a business threshold. The Bayesian strategy performs best because it uses both technical evidence and workflow context. It can respond before interruption occurs when degradation probability becomes high, and it can avoid unnecessary shutdown when evidence suggests that the workflow remains within acceptable limits. (Lu,2019b).

Table 6 reports the comparative results. The Bayesian workflow strategy reduces expected downtime by 34% relative to the reactive strategy and reduces estimated direct cost by 29%. It also

lowers false escalation compared with the alert-driven strategy because not every alert produces high continuity risk. This result is consistent with the overall argument of the article: business continuity analytics should not only count cyber events; it should evaluate what those events mean for critical workflows.

Table 6. Comparative performance of continuity response strategies in the simulated dataset.

Strategy	Trigger Logic	Average Downtime	False Escalation Rate	Estimated Cost per Severe Episode	Managerial Interpretation
Reactive response	Intervene after workflow interruption is confirmed	4.1 h	Low	$52,600	Least disruptive before incidents but costly after interruption
Alert-driven response	Intervene when cyber alert severity exceeds a fixed threshold	3.2 h	High	$45,300	Technically conservative but may overreact to low-continuity alerts
Bayesian workflow response	Intervene when posterior continuity loss exceeds business threshold	2.7 h	Moderate	$37,400	Best balance between early action and business relevance

6. Discussion

6.1 Theoretical Contributions

This study contributes to business data analytics by reframing cyber-physical risk as a continuity inference problem. Existing industrial cybersecurity studies often measure risk at the asset or vulnerability level. Existing continuity studies often define recovery objectives but do not infer workflow state from cyber-physical evidence. The proposed Bayesian framework connects these domains. It treats business continuity as a probabilistic state that can be updated using heterogeneous evidence. This perspective is especially relevant for process industries, where technical disturbances propagate through workflow activities before becoming financial consequences. (Pearl,2009).

The study also contributes to the literature on risk propagation. Rather than modeling propagation only as an attack path or a sequence of component failures, it models propagation as a transformation of evidence into workflow degradation and then into business impact. This shift is important because business consequences are mediated by activity context. The same technical event may have different effects depending on workflow timing, redundancy, recovery capability, and contractual exposure. A Bayesian workflow model can represent these contextual dependencies more explicitly than a static risk score. (Lu and Xu,2019).

A third contribution is methodological. The article demonstrates how simulated scenario data, expert knowledge, and workflow definitions can be combined into a decision model when real attack data are scarce. Rare-event domains often struggle with data limitations. The proposed approach does not require large, labeled attack datasets before analysis can begin. Instead, it supports staged model development: start with expert-structured priorities, calibrate with simulated or historical incidents, and update conditional probabilities as evidence accumulates. This is a practical path for organizations that need continuity analytics before they have extensive cyber-disruption histories. (Zio,2009).

6.2 Managerial Implications

The results offer several implications for managers. First, business continuity teams should define critical workflows before cyber incidents occur. If a firm does not know which activities create

business value and which technical resources support them, it cannot translate cyber evidence into continuity risk. Workflow decomposition should therefore be part of cyber resilience planning. Second, managers should monitor degraded workflow probability, not only confirmed interruption. The simulated results show that degradation is often the early signal of business risk, especially in sensor spoofing and historian compromise scenarios. Waiting for confirmed interruption may lead to avoidable downtime and rework. (Lu,2018).

Third, recovery delays should be treated as a major risk driver. The sensitivity analysis indicates that reducing recovery delay may be more valuable than reducing some low-impact technical vulnerabilities. This does not mean cybersecurity prevention is unimportant. It means continuity planning must integrate prevention, detection, response, and recovery. Fourth, alarm assurance deserves special attention. Suppressed or delayed alarms combine technical and human factors. They undermine operator awareness and weaken manual fallback. Organizations should test whether alarms remain visible, meaningful, and actionable during cyber-disrupted conditions. (Amin et al.,2009).

Fifth, the model can support investment decisions. A manager can compare the expected reduction in continuity loss from alternative interventions: redundant sensing, PLC backup, network segmentation, alarm verification, incident playbooks, operator training, or automated recovery scripts. The intervention with the largest reduction in expected continuity loss per unit cost should receive priority. This approach moves cyber resilience investment from compliance-driven budgeting toward evidence-based business analytics. (Lu,2017a).

Table 7. Managerial use cases for Bayesian business continuity analytics.

Use Case	Decision Question	Model Output	Practical Action
Incident triage	Which cyber alerts threaten business continuity?	Posterior probability of degraded or interrupted workflow	Escalate only when continuity threshold is exceeded
Resilience investment	Which control improvement gives the highest business value?	Sensitivity ranking and expected loss reduction	Prioritize recovery automation, alarm assurance, or segmentation
Continuity planning	Which workflows require manual fallback?	Workflow interruption probability under scenarios	Design and test alternative procedures
Executive reporting	How should cyber risk be explained financially?	Expected continuity loss and downtime estimate	Translate technical risk into business-impact language
Post-incident learning	Which evidence changed the risk estimate most?	Diagnostic probability trace and driver importance	Update conditional probabilities and response playbooks

6.3 Implementation Guidelines

Implementation should proceed in stages. The first stage is workflow selection. Organizations should begin with one high-value workflow rather than attempting to model the entire plant. The selected workflow should have clear business impact, available operational data, and identifiable cyber-physical dependencies. The second stage is evidence definition. Each evidence node must have a clear data source, threshold, and interpretation. The third stage is model construction. Domain experts should review the network structure and conditional probability assumptions. The fourth stage is validation with historical incidents, tabletop exercises, or simulated scenarios. The fifth stage is integration into decision routines. (Cardenas et al.,2008).

Human governance is as important as model design. Bayesian analytics should not become an opaque scoring system. Users should understand why a posterior risk estimate changes and which evidence drives the update. The model should include audit logs, version control, and explanation views. Model review should occur after major process changes, cyber incidents, or control-system upgrades. Because industrial processes evolve, a continuity model that is not maintained can become

misleading. Governance should therefore assign responsibility for evidence quality, probability calibration, and business impact assumptions. (Lu,2017b).

The framework also raises organizational questions. Cybersecurity, operations, and business continuity teams often use different metrics. Cybersecurity teams may focus on vulnerabilities and alerts. Operations teams may focus on downtime and process stability. Business continuity teams may focus on recovery objectives and crisis response. Bayesian continuity analytics can act as a shared interface among these groups. It does not eliminate the need for specialized expertise; it creates a common decision layer where evidence and business impact can be discussed consistently. (Humayed et al.,2017).

6.4 Limitations

This study has limitations. The empirical demonstration uses simulated data rather than proprietary plant records. Simulation allows transparent scenario analysis, but field validation is required before claims about specific industries or plants can be made. The Bayesian model is intentionally compact. Real deployment may require more detailed nodes for equipment, network zones, process variables, shift conditions, and recovery resources. The model also assumes that conditional relationships can be elicited and reviewed by experts. In practice, organizations may disagree about these relationships, and probability calibration may require several iterations. (Khan et al.,2015).

Another limitation is that the framework focuses on short-term continuity outcomes. Long-term consequences such as regulatory investigation, customer trust, insurance premium changes, and strategic market loss are not fully modeled. These effects may be substantial after severe cyber incidents. Future work should extend the model to multi-period analysis and include learning effects. As organizations collect more incident data, Bayesian priors can be updated, and the model can become increasingly data driven. Another extension is to combine the framework with process mining so that workflow deviations are learned automatically from event logs rather than defined manually. (Cherdantseva et al.,2016).

7. Conclusion

This article developed a Bayesian business continuity analytics framework for cyber-disrupted industrial process workflows. The study argued that cyber-physical events become business risks when they affect critical workflow activities and change the probability of normal operation, degradation, interruption, or recovery. The proposed framework connects cyber evidence, process degradation, workflow states, and business outcomes in a probabilistic decision structure. It allows managers to update continuity beliefs as evidence arrives, estimate expected continuity loss, and identify the drivers that most influence business impact.

The simulated industrial fractionation case demonstrated the value of this approach. Sensor spoofing mainly increased workflow degradation, while PLC denial and alarm suppression increased interruption probability. A multi-vector attack produced the most severe continuity posture, with interruption probability reaching 0.50 and expected continuity loss more than four times the baseline fault scenario. Sensitivity analysis showed that recovery delay, alarm suppression, PLC command loss, and sensor spoofing were the strongest drivers of continuity loss. Strategy comparison showed that a Bayesian workflow response can reduce downtime and cost compared with reactive or purely alert-driven response strategies.

The main implication is that business continuity analytics should move beyond static recovery plans and technical alert counts. Industrial organizations need probabilistic models that connect cyber-physical evidence to workflow consequences and financial severity. Bayesian reasoning provides a

transparent and adaptable method for this task. When combined with workflow decomposition, expert review, and business impact analysis, it can support risk-informed investment, incident triage, resilience planning, and executive communication. Future research should validate the framework using field data, integrate process mining for automated workflow evidence, and extend the model to multi-period learning and portfolio-level resilience optimization.

AUTHOR CONTRIBUTIONS

Author	Contribution
Clara Martins	Conceptualization, methodology, writing - original draft, visualization
Rui Pereira	Formal analysis, data curation, scenario design, validation
Beatriz Almeida	Supervision, writing - review and editing, project administration, correspondence

DECLARATIONS

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: The study uses a simulated dataset generated for methodological demonstration. Aggregated scenario values and model assumptions are reported in the article. No proprietary industrial data is redistributed.

Funding: This research received no external funding.

Ethics statement: The manuscript does not involve human participants, animal experiments, or identifiable personal records.

ABOUT THE AUTHORS

Clara Martins is affiliated with the Department of Information Systems at the University of Minho, Portugal. Her research focuses on business analytics, process modeling, and organizational resilience in digital industrial environments.

Rui Pereira is a researcher in industrial engineering and management at the Polytechnic Institute of Leiria, Portugal. His work examines production planning, cyber-physical operations, and data-driven decision support for manufacturing systems.

Beatriz Almeida is affiliated with the Department of Management and Industrial Engineering at the University of Aveiro, Portugal. Her research interests include Bayesian analytics, industrial risk management, and business continuity governance.

REFERENCES

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. Safety Science, 89, 201-218. https://doi.org/10.1016/j.ssci.2016.06.015

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2025.2541199

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13. https://doi.org/10.1016/j.ejor.2015.12.023

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster

recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273. https://doi.org/10.1016/j.ejor.2014.09.055

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. Production and Operations Management, 14(1), 53-68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451-488. https://doi.org/10.1016/j.ijpe.2005.12.006

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. International Journal of Production Research, 49(18), 5375-5393. https://doi.org/10.1080/00207543.2011.563826

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The International Journal of Logistics Management, 15(2), 1-14. https://doi.org/10.1108/09574090410700275

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), 124-143. https://doi.org/10.1108/09574090910954873

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. International Journal of Physical Distribution & Logistics Management, 38(3), 192-223. https://doi.org/10.1108/09600030810866986

Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

Ivanov, D. (2020). Viable supply chain model: Integrating agility, resilience and sustainability perspectives. International Journal of Production Research, 58(10), 2904-2915. https://doi.org/10.1080/00207543.2020.1742487

Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

Queiroz, M. M., Ivanov, D., Dolgui, A., & Wamba, S. F. (2020). Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review. Annals of Operations Research, 319, 1159-1196. https://doi.org/10.1007/s10479-020-03685-7

Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511

Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. Transportation Research Part E: Logistics and Transportation Review, 125, 285-307. https://doi.org/10.1016/j.tre.2019.03.001

Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383-402. https://doi.org/10.1080/23270012.2022.2089064

Kamalahmadi, M., & Parast, M. M. (2016). A review of the literature on the principles of enterprise and supply chain resilience. International Journal of Production Economics, 171, 116-133. https://doi.org/10.1016/j.ijpe.2015.10.023

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. https://doi.org/10.1111/poms.12838

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management. International Journal of Operations & Production Management, 37(1), 10-36. https://doi.org/10.1108/IJOPM-02-2015-0078

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Dubey, R., Gunasekaran, A., Childe, S. J., Roubaud, D., Wamba, S. F., Giannakis, M., & Foropon, C. (2019). Big data analytics and organizational culture as complements to swift trust and collaborative performance in the humanitarian supply chain. International Journal of Production Economics, 210, 120-136. https://doi.org/10.1016/j.ijpe.2019.01.023

Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering & System Safety, 71(3), 249-260. https://doi.org/10.1016/S0951-8320(00)00077-6

Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-320. https://doi.org/10.1080/23270012.2020.1802622

Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection, 91(1-2), 46-53. https://doi.org/10.1016/j.psep.2012.01.005

Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence, 25(4), 671-682. https://doi.org/10.1016/j.engappai.2010.06.002

Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

Meel, A., & Seider, W. D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science, 61(21), 7036-7056. https://doi.org/10.1016/j.ces.2006.07.007

Lu, Y. (2019a). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Fenton, N., & Neil, M. (2018). Risk Assessment and Decision Analysis with Bayesian Networks. CRC Press. https://doi.org/10.1201/b21982

Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information

Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

Pearl, J. (2009). Causality: Models, Reasoning, and Inference. Cambridge University Press. https://doi.org/10.1017/CBO9780511803161

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Zio, E. (2009). Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety, 94(2), 125-141. https://doi.org/10.1016/j.ress.2008.06.002

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523

Amin, S., Cardenas, A. A., & Sastry, S. S. (2009). Safe and secure networked control systems under denial-of-service attacks. Hybrid Systems: Computation and Control, 31-45. https://doi.org/10.1007/978-3-642-00602-9_3

Lu, Y. (2017a). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

Cardenas, A. A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. IEEE International Conference on Distributed Computing Systems Workshops, 495-500. https://doi.org/10.1109/ICDCS.Workshops.2008.40

Lu, Y. (2017b). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. IEEE Internet of Things Journal, 4(6), 1802-1831. https://doi.org/10.1109/JIOT.2017.2703172

Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection, 98, 116-147. https://doi.org/10.1016/j.psep.2015.07.005

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

Lee, E. A. (2008). Cyber physical systems: Design challenges. International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, 363-369. https://doi.org/10.1109/ISORC.2008.25

Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46(4), 1-29. https://doi.org/10.1145/2542049

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11-25. https://doi.org/10.1109/37.969131

Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48, 157-169. https://doi.org/10.1016/j.jmsy.2018.01.006

Wang, J., Ma, Y., Zhang, L., Gao, R. X., & Wu, D. (2018). Deep learning for smart manufacturing: Methods and applications. Journal of Manufacturing Systems, 48, 144-156. https://doi.org/10.1016/j.jmsy.2018.01.003

van der Aalst, W. M. P. (2016). Process Mining: Data Science in Action. Springer. https://doi.org/10.1007/978-3-662-49851-4

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). Fundamentals of Business Process Management. Springer. https://doi.org/10.1007/978-3-662-56509-4

Rosemann, M., & vom Brocke, J. (2015). The six core elements of business process management. In J. vom Brocke & M. Rosemann (Eds.), Handbook on Business Process Management 1 (pp. 105-122). Springer. https://doi.org/10.1007/978-3-642-45100-3_5

vom Brocke, J., Zelt, S., & Schmiedel, T. (2014). On the role of context in business process management.

International Journal of Information Management, 36(3), 486-495. https://doi.org/10.1016/j.ijinfomgt.2015.10.002

Mendling, J., Decker, G., Hull, R., Reijers, H. A., & Weber, I. (2018). How do machine learning, robotic process automation, and blockchains affect the human factor in business process management? Communications of the Association for Information Systems, 43(1), 297-320. https://doi.org/10.17705/1CAIS.04319

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. Business History, 52(6), 978-1002. https://doi.org/10.1080/00076791.2010.511185

Tammineedi, R. L. (2010). Business continuity management: A standards-based approach. Information Security Journal: A Global Perspective, 19(1), 36-50. https://doi.org/10.1080/19393550903551843

Soufi, H. R., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. International Journal of Production Research, 57(3), 779-800. https://doi.org/10.1080/00207543.2018.1483586

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992

Böhme, R., & Moore, T. (2012). The iterated weakest link: A model of adaptive security investment. Journal of Information Security, 3(2), 81-90. https://doi.org/10.4236/jis.2012.32010

Cachon, G. P., & Lariviere, M. A. (2005). Supply chain coordination with revenue-sharing contracts: Strengths and limitations. Management Science, 51(1), 30-44. https://doi.org/10.1287/mnsc.1040.0215

Corbett, C. J., Zhou, D., & Tang, C. S. (2004). Designing supply contracts: Contract type and information asymmetry. Management Science, 50(4), 550-559. https://doi.org/10.1287/mnsc.1030.0173

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Sarkis, J. (2020). Supply chain sustainability: Learning from the COVID-19 pandemic. International Journal of Operations & Production Management, 41(1), 63-73. https://doi.org/10.1108/IJOPM-08-2020-0568

Sodhi, M. S., & Tang, C. S. (2012). Managing Supply Chain Risk. Springer. https://doi.org/10.1007/978-1-4614-3238-8

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., et al. (2020). Language models are few-shot learners. Advances in Neural Information Processing Systems, 33, 1877-1901. https://doi.org/10.48550/arXiv.2005.14165

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1706.03762

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 610-623. https://doi.org/10.1145/3442188.3445922

Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Xu, Y., Ishii, E., Bang, Y. J., Madotto, A., & Fung, P. (2023). Survey of hallucination in natural language generation. ACM Computing Surveys, 55(12), 1-38. https://doi.org/10.1145/3571730

Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., et al. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. Advances in Neural Information Processing Systems, 33, 9459-9474. https://doi.org/10.48550/arXiv.2005.11401

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1705.07874

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. https://doi.org/10.48550/arXiv.1702.08608

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144. https://doi.org/10.1145/2939672.2939778