International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 06, Issue 3-4, (July- December 2020), www.ijtmh.com

A Unified Conceptual Model for Integrating Hardware Reliability and Software-Based Fault Diagnostics

Eromosele Asibor[1], Emmanuel Chukwuma Okeke[2*], Enoch Ogunnowo[3], Oluranti Ogundapo[4], Precious Nnamdi Ibe[5]

[1] Nigeria National Exploration and Production (NEPL) Ltd, Benin City, Nigeria

[2] IDEX Corporation, USA

[3] McNeese State University, Lake Charles, LA, USA

[4] Airtel Networks, Nigeria

[5] University of Port Harcourt, Port Harcourt, Nigeria

* Corresponding author: Emmanuel Chukwuma Okeke, emmanuelokeke68@gmail.com

Abstract

Hardware reliability engineering and software-based fault diagnostics have matured as largely separate disciplines. Reliability engineering predicts how often and when physical components will fail, using population statistics, physics-of-failure models and design-time analyses such as FMEA and fault trees. Fault diagnostics, increasingly implemented in software, detects, isolates and identifies faults in individual systems at run time from sensor data, error counters and logs. Because the two communities use different vocabularies, time scales and units of analysis, their outputs are rarely combined. This paper addresses that gap through a conceptual research design that combines an integrative literature review with model building. A corpus of 120 sources published to date, spanning reliability foundations, fault diagnosis and prognostics, industrial integrity management, power systems, security monitoring, IT service reliability, risk analytics and human factors, was screened and synthesized thematically. The synthesis identifies eight dimensions on which the two disciplines diverge and four integration gaps. From these, the paper develops a unified conceptual model of five layers (physical reliability, observation, software diagnosis, integration, and decision) linked by bottom-up evidence flows and top-down prior and context flows, and anchored in a shared fault ontology based on the fault, error and failure chain. A probabilistic formalization treats design-time reliability models as priors, diagnostic outputs as likelihoods with explicit coverage and false-alarm characteristics, and the integration layer as the producer of posterior hazard rates and remaining useful life estimates, while a fleet feedback loop recalibrates both reliability and diagnostic parameters. An illustrative server memory scenario shows moderate and strong diagnostic evidence reducing predicted median life from about 47,000 hours to about 33,000 and 23,000 hours respectively. The paper discusses theoretical and practical implications, states its limitations, and sets out an agenda for empirical validation.

Keywords: hardware reliability; fault diagnosis; prognostics and health management; dependability; Bayesian inference; conceptual model; integrative literature review; condition-based maintenance

DOI: https://doi.org/10.21590/ijtmh.2020063-414

1. INTRODUCTION

Modern engineered systems, from data center servers and automotive electronic control units to avionics and industrial controllers, depend on hardware whose failure behaviour is increasingly shaped by software. Processors log machine-check exceptions, memory controllers correct and count bit errors, storage devices report self-monitoring attributes, and embedded controllers run continuous built-in tests. A substantial and growing share of the intelligence that determines whether a hardware fault becomes a system failure now resides in diagnostic and recovery software (Avizienis et al., 2004; Sorin, 2009).

The same pattern recurs across sectors. In oil and gas, reliability-centred and condition-based maintenance concepts govern the upkeep of static equipment, bearings and swivels, fired heaters and mooring systems (Obetta & Ninduwezuor-Ehiobu, 2018; Obetta & Ninduwezuor-Ehiobu, 2019; Obetta, 2019; Obetta, 2020). In electric power systems, predictive maintenance and condition monitoring of critical infrastructure rely on software that interprets sensor data (Adaramola et al., 2018), and unmanned aerial vehicles now support grid inspection programmes (Dagodzo, 2018a). In computing infrastructure, machine learning drives resource scaling (Ahmed et al., 2020) and automated log analytics drives incident response (Mbonu, Iwuanyanwu, et al., 2019). In each case hardware condition and software interpretation are inseparable, yet the methods used to reason about them are seldom brought together in one framework.

Despite this convergence in practice, the theory that supports it has remained divided. Hardware reliability engineering, rooted in probability theory and the physics of failure, answers population questions: what is the failure rate of a component type, what fraction of units will survive a mission, and which failure modes dominate risk (Birolini, 2017; Pearl, 1988; Rausand & Høyland, 2004). Fault diagnostics, rooted in control theory, signal processing and artificial intelligence, answers instance questions: is this particular unit faulty now, where is the fault, and what kind of fault is it (Isermann, 2006; Lei et al., 2020; Venkatasubramanian et al., 2003). The first discipline works mainly at design time and in aggregate; the second works at run time and for individual units.

The separation has practical costs. Reliability predictions made during design are seldom updated with the rich evidence that diagnostic software collects in the field, so maintenance plans and spare-part provisioning rest on assumptions that may be years out of date. Conversely, diagnostic reasoners often

treat all candidate faults as equally plausible, or rely on ad hoc thresholds, ignoring the prior knowledge about failure modes and their relative frequencies that a reliability analysis already contains. Field studies of large computing fleets have shown that observed error and failure behaviour can differ markedly from vendor datasheets and from simple constant-rate assumptions (Schroeder & Gibson, 2007; Schroeder et al., 2009), which strengthens the case for models that learn from diagnostic evidence.

Prognostics and health management (PHM) has made important progress in linking condition monitoring to remaining useful life estimation (Jardine et al., 2006; Lee et al., 2014; Pecht, 2008; Si et al., 2011). However, PHM frameworks are usually presented as processing pipelines for specific equipment classes, and they rarely make explicit how classical reliability artefacts such as FMECA tables, fault trees and failure-rate handbooks should interact with software diagnostic outputs, or how imperfect diagnosis should be represented. What is missing is a conceptual model: a technology-neutral description of the entities, relationships and information flows that any integration must respect.

This paper therefore asks three research questions. RQ1: On which conceptual dimensions do hardware reliability engineering and software-based fault diagnostics diverge, and what gaps prevent their integration? RQ2: What layers, entities and information flows should a unified conceptual model contain to bridge them? RQ3: How can the outputs of the two disciplines be combined formally so that reliability knowledge and diagnostic evidence each improve the other?

The paper makes four contributions in answering them. It synthesizes the relevant literature and identifies the mismatches and gaps that keep the two disciplines apart. It proposes a five-layer unified conceptual model with a shared fault ontology and explicit bidirectional information flows. It provides a probabilistic formalization in which reliability models supply priors, diagnostics supply likelihoods and an integration layer computes posterior health states and hazard rates. Finally, it demonstrates the model on an illustrative scenario. The remainder of the paper is organized as follows. Section 2 describes the research method. Section 3 presents the results and discussion: the literature synthesis, the conceptual model and its probabilistic formalization, an illustrative application, a discussion of the research questions, and the implications, limitations and directions for future research. Section 4 concludes.

2. RESEARCH METHOD

2.1 Research Design

The study follows a conceptual research design, which is appropriate when the aim is to integrate existing knowledge into a new explanatory structure rather than to test hypotheses on primary data (Jaakkola, 2020; Jabareen, 2009). Among the approaches to conceptual research, it adopts the model type, which develops a framework that predicts relationships among constructs and can later be tested empirically (Jaakkola, 2020). The design proceeds in three stages: an integrative literature review to establish the knowledge base, a thematic synthesis to identify mismatches and gaps, and a model-building stage in which the conceptual model is specified, formalized and illustrated. Integrative reviews are suited to topics that span several research communities with different traditions, because they allow mature and emerging literatures to be combined into new perspectives (Snyder, 2019; Torraco, 2005).

2.2 Literature Identification and Selection

Two complementary sources were used. The first was the foundational literature of the two disciplines: standard texts and widely cited reviews on reliability theory, dependability, fault diagnosis, prognostics and fault-tolerant computing, identified by backward and forward reference tracing from core works (Webster & Watson, 2002). The second was a consolidated corpus of peer-reviewed applied studies spanning engineering, computing, security, analytics and safety, which was screened for relevance to the integration problem.

Three inclusion criteria were applied. First, a source had to be published in or before 2020, the reference year of the study. Second, it had to address at least one element of the integration problem: failure mechanisms or life modelling, condition monitoring or observation, detection and diagnosis, risk estimation, or decisions and actions that depend on asset condition. Third, it had to be a peer-reviewed article, conference paper, scholarly book or recognized standard. Sources whose subject matter had no plausible link to hardware condition, monitoring or risk-based decisions were excluded. The screening produced a final corpus of 120 sources, of which 24 are foundational works and 96 are applied studies. Methodological sources cited in this section are not counted in the corpus.

2.3 Analysis and Synthesis

The corpus was analysed by thematic synthesis. Each source was read for its contribution to five analytical questions: what it assumes about how hardware fails, what it observes, how it infers condition,

how it represents uncertainty, and what decision it supports. Codes arising from these questions were grouped iteratively into themes following established guidance on thematic analysis (Braun & Clarke, 2006), and a concept-centric matrix was used to organize the literature by theme rather than by author (Webster & Watson, 2002). Table 1 lists the nine resulting themes, the number of sources in each and the part of the model to which each theme mainly contributes.

Table 1. Thematic structure of the review corpus

Theme	**Sources**	**Role in the model**
Reliability and dependability foundations	9	Ontology, life models, standards (L1, shared ontology)
Fault diagnosis, prognostics and failure prediction	15	Detection, isolation, prognosis methods (L3, L4)
Industrial reliability, integrity and maintenance	15	Failure-mode knowledge and maintenance practice (L1, L5)
Remote inspection and diagnostic quality systems	8	Observation channels and diagnostic accuracy (L2, L3)
Power and energy systems	14	Operating stresses and environmental context (L1)
Operational technology and enterprise security	15	Detection pipelines and false-alarm management (L3)
IT operations and service reliability	14	Telemetry, outcome records, fleet feedback (L2, feedback loop)
Risk analytics and early warning	15	Calibrated alerting and data-limited inference (L4)
Human factors, safety and maintenance logistics	15	Operator decisions and spare-part logistics (L5)
Total	120	

2.4 Model Development and Evaluation

Model development followed the procedure for building conceptual frameworks from multidisciplinary literature: concepts were identified and deconstructed, integrated where they overlapped, and synthesized into a coherent structure (Jabareen, 2009). The mismatches identified in the synthesis were translated into design principles; the principles were used to specify layers, a shared ontology and information flows; and the qualitative model was then formalized probabilistically so that its claims are precise and testable. Because the study is conceptual, the model is evaluated analytically rather than empirically, through internal consistency, coverage of the identified gaps, and an illustrative scenario that demonstrates its behaviour with plausible parameters. Empirical validation is identified as future work in Section 3.8.

3. RESULTS AND DISCUSSION

This section reports the results of the study in the order in which they were produced: the synthesis of the review corpus, the conceptual model derived from it, the model's probabilistic formalization and an illustrative application. It then discusses the findings against the research questions and sets out their implications, limitations and directions for future research.

3.1 Literature Synthesis

3.1.1 Hardware Reliability Engineering

Reliability is classically defined as the probability that an item performs its required function under stated conditions for a stated period of time (Birolini, 2017). For a component with lifetime T, the reliability function is $R(t) = P(T > t)$ and the hazard rate $h(t)$ gives the instantaneous failure intensity conditional on survival. Design-time practice combines several tools. Failure-rate handbooks such as MIL-HDBK-217F (U.S. Department of Defense, 1991) provide base rates adjusted by stress factors; life distributions such as the Weibull capture infant mortality, random failures and wear-out; and structural methods such as failure mode, effects and criticality analysis (FMECA) and fault tree analysis relate component failures to system-level consequences (Rausand & Høyland, 2004). Physics-of-failure approaches model specific mechanisms such as electromigration, thermal cycling fatigue and dielectric breakdown (Pecht, 2008). Functional safety standards such as IEC 61508 (International Electrotechnical Commission, 2010) further require quantified diagnostic coverage, which is one of the few places where reliability engineering already acknowledges diagnostics explicitly.

The strength of this tradition is its rigour about uncertainty at the population level. Its weakness, from the perspective of an individual operating system, is that its parameters are static and generic. A Weibull model fitted to a component family says little about whether the particular unit in a given rack is degrading faster than its peers.

Industrial practice illustrates both the reach and the limits of this tradition. Reliability engineering and failure analysis frameworks for complex engineering systems (Gideon et al., 2019) and risk-based process engineering for natural gas infrastructure (Asibor & Isong, 2019) formalize how failure modes are ranked and controlled. In offshore and upstream operations, risk-based inspection and fitness-for-service assessment of ageing pressure vessels (Obetta, 2018), integrity management of fired heaters, boilers and furnaces (Obetta, 2019), reliability-centred maintenance of static mechanical equipment (Obetta, 2020), condition-based maintenance of buoy bearings and swivels (Obetta & Ninduwezuor-Ehiobu, 2018) and integrity assurance of turret mooring systems (Obetta & Ninduwezuor-Ehiobu, 2019) all encode detailed knowledge of how equipment degrades. Related work addresses automated risk assessment for regulatory deliverables in upstream operations (Uchechi & Ominyi, 2020), operational integrity in high-risk drilling (Nwangwu et al., 2018) and inventory availability as a driver of plant uptime (Okonkwo et al., 2018b). These studies are rich in failure-mode knowledge but typically treat run-time diagnostic evidence as an input to periodic review rather than as a continuous update to reliability estimates.

Degradation mechanisms set the baseline hazard on which such programmes rest. Corrosion management and material selection for export equipment in marine environments (Obetta et al., 2020), NDT-based integrity management and corrosion risk assessment for refinery equipment (Atta et al., 2020) and green corrosion inhibitors for mild steel (Atta et al., 2018) show how environmental and material factors shape life distributions, while the documented transition from reactive to predictive maintenance in mechanical systems (Sunday et al., 2020) shows how organizations have begun to act on degradation information before failure occurs.

3.1.2 Software-Based Fault Diagnostics

Fault diagnosis is conventionally decomposed into detection (deciding that something is wrong), isolation (locating the faulty component) and identification (determining the type, size and time of the fault) (Isermann, 2006). Three families of methods dominate. Model-based methods compare measured behaviour with the output of an analytical or simulation model and analyse the resulting residuals (Isermann, 2006; Venkatasubramanian et al., 2003). Knowledge-based methods use expert rules, fault

dictionaries, signed directed graphs or case libraries. Data-driven methods learn the mapping from observations to fault classes using statistical or machine learning techniques, a field that has expanded rapidly with deep learning (Lei et al., 2020). In computing systems, a closely related body of work addresses online failure prediction from error logs and system telemetry (Salfner et al., 2010), and autonomic computing has framed self-diagnosis as part of a monitor, analyse, plan and execute loop (Kephart & Chess, 2003).

Diagnostic software is powerful precisely because it operates on individual units in real time. Yet its outputs are typically categorical alarms or anomaly scores without a calibrated probabilistic meaning, and they are seldom traced back to the failure modes that the reliability analysis enumerated. Moreover, diagnostic software is itself fallible: it has finite coverage, nonzero false-alarm rates, and its own software faults (Grottke & Trivedi, 2007; Lyu, 1996).

Applied work shows how far software-based diagnosis has spread in practice. Predictive maintenance and condition monitoring are established in critical power and energy infrastructure (Adaramola et al., 2018) and are central to the shift away from run-to-failure maintenance (Sunday et al., 2020). Remote sensing extends observation to dispersed assets: unmanned aerial vehicles are used for national power grid inspection (Dagodzo, 2018a), transmission line inspection (Dagodzo, 2018b) and pipeline and corridor monitoring (Dagodzo & Ahiaeke Patrick, 2020), and satellite image interpretation demonstrates how spectral data can be turned into diagnostic classifications (Dagodzo, 2018c). Clinical laboratory research offers an instructive parallel, because diagnostic accuracy there has been shown to depend on integrated information systems (Abdulrazaq et al., 2019), formal quality systems (Yusuf & Abdulrazaq, 2018), multi-site reporting networks (Yusuf et al., 2020) and the quality of surveillance data (Ekemezie et al., 2018). The same dependencies, on data integration, quality assurance and fleet-wide reporting, apply to the software that diagnoses hardware.

3.1.3 Prior Integration Efforts

Several research lines have partially bridged the gap. The dependability taxonomy of Avizienis et al. (2004) provides a common vocabulary of faults, errors and failures that spans hardware and software, but it is descriptive rather than computational. Bayesian networks have been applied to reliability analysis and to diagnosis separately and occasionally together (Langseth & Portinale, 2007; Weber et al., 2012). Condition-based maintenance and PHM research has shown how degradation signals can drive remaining useful life estimates (Jardine et al., 2006; Lee et al., 2014; Zhang & Jiang, 2008), and proportional hazards

models with condition covariates provide a principled way to modulate a baseline hazard with monitored data (Jardine et al., 2006). Fault tolerant computer architecture has studied detection, diagnosis and recovery mechanisms inside processors and memories (Mukherjee, 2008; Sorin, 2009). Each line contributes building blocks; none supplies a general conceptual model that tells a designer which artefacts to connect, in which direction, and with which semantics.

3.1.4 Evidence from Adjacent Monitoring and Detection Domains

Beyond the core reliability and diagnosis literatures, applied research in neighbouring domains bears on the integration problem. It is grouped below by the part of the proposed model to which it contributes most directly.

Power and energy systems. Grid and machine research describes the stresses under which hardware operates and the control software that manages them. Examples include grounding system design for medium-voltage networks (Adeniji et al., 2020), voltage control with distributed generation (Oshevire et al., 2017), multi-algorithm optimization of single-phase induction motors (Amayo & Popoola, 2017a; Amayo et al., 2015; Amayo, 2017) and telecommunication network quality (Amayo & Popoola, 2017b). Work on solar power in small-scale manufacturing (Sunday & Omoegun, 2018), load distribution for hybrid solar installations (Sunday & Omoegun, 2019), residential air-conditioning control (Sunday et al., 2019), smart solar microgrids (Komi & Adeniji, 2020), hydrogen integration in national grids (Shittu et al., 2019), solar radiation estimation (Odejobi & Ahmed, 2018b), large-scale solar programme strategy (Yeboah & Ike, 2020) and multimodal long-term production forecasting (Nwangwu et al., 2020) supplies the operating-profile and environmental information from which reliability priors are derived.

Operational technology and enterprise security. Security monitoring is a close methodological relative of fault diagnosis, because both infer abnormal states from network, log and sensor data. Relevant work covers NERC CIP compliance and OT network architecture in electric utilities (Adegbite et al., 2020), insider threat classification (Akeju et al., 2018), security audit and enterprise risk assessment (Dosunmu & Ogundele, 2019), intrusion detection and prevention (Dosunmu & Ogundele, 2020), risk-based assurance of data availability (Fadayomi et al., 2019), log analytics and automated incident response (Mbonu, Iwuanyanwu, et al., 2019), privacy-centric security engineering (Okoruwa et al., 2020), identity and access management in federated and hybrid environments (Mbonu, Aliliele, et al., 2020; Oshoba et al., 2019), directory service assessment and administration (Ladapo et al., 2018; Ladapo et al., 2019), secure cloud implementation across jurisdictions (Mbonu, Aliliele, et al., 2019), data protection risk

modelling (Mbonu et al., 2018), infrastructure-as-code governance (Mbonu, Iwuanyanwu, et al., 2020) and security awareness (Onche et al., 2020). Because a cyber attack and a hardware fault can produce similar symptoms, the shared ontology must allow both hypotheses to be considered, and the calibration and false-alarm problems documented in this literature mirror those of hardware diagnostics.

IT operations and service reliability. Service reliability research supplies the data and organizational processes that the fleet feedback loop in Section 3.2.4 depends on. Examples include scalable cloud architectures (Ahmed & Odejobi, 2018a), energy-efficient virtual machine placement (Ahmed & Odejobi, 2018b), cloud network resource allocation (Ahmed et al., 2019), predictive cloud scaling (Ahmed et al., 2020), multi-tenant performance evaluation (Odejobi & Ahmed, 2018a), database optimization (Odejobi et al., 2019), blockchain-based configuration audit trails (Oshoba et al., 2020), IT support maturity and continuity (Anyanwu, 2019; Anyanwu, 2020), DevOps tooling and continuous delivery pipelines (Badmus et al., 2018; Badmus et al., 2020), data integration architectures (Badmus et al., 2019a), platform governance (Badmus et al., 2019b) and business continuity and disaster recovery preparedness (Fadero et al., 2020).

Risk analytics and early warning. Analytical work outside engineering contributes transferable techniques for calibrated alerting and data-limited inference. These include data-driven risk evaluation models (Akomolafe & Agu, 2019), technology-enabled risk assessment (Akomolafe & Agu, 2018), data-driven executive decision systems (Lawal & Oduleye, 2019), automation and analytics in operations management (Agboada et al., 2018), standard operating procedures as change infrastructure (Agboada et al., 2019), predictive demand forecasting (Aifuwa et al., 2020), lifecycle and churn prediction (Oziri et al., 2020), data-driven and spatially explicit risk modelling under limited data (Azeez & Badmus, 2018; Lamidi & Olamide, 2018), predictive compliance monitoring in aviation (Adeyelu, 2018), AI-based wildlife strike risk quantification (Adeyelu, 2020), adaptive safety management systems (Adeyelu, 2019), near-miss and hazard observation analytics (Arumosoye & Obriki, 2019), risk-based decisions in regulated manufacturing (Aneke & Adesemoye, 2020) and traceability and chain-of-custody integrity (Aneke & Adesemoye, 2019). Taken together, these domains confirm the demand for calibrated, explainable alerts and the absence of a shared model that connects such alerts to the physical reliability of the underlying assets.

3.1.5 Conceptual Mismatches and Integration Gaps

Table 2 summarizes the mismatches between the two disciplines that a unified model must reconcile. The mismatches are not merely terminological. They concern the unit of analysis, the treatment of time, the representation of uncertainty and the intended consumer of results.

Table 2. Contrasting perspectives of hardware reliability engineering and software-based fault diagnostics

Dimension	**Hardware reliability engineering**	**Software-based fault diagnostics**
Central question	How likely is failure, and when?	Is there a fault now, where, and of what kind?
Unit of analysis	Component population or design	Individual operating unit
Time scale	Design life, missions, years	Milliseconds to days, at run time
Primary inputs	Handbook rates, test data, stress profiles, physics of failure	Sensor signals, error counters, logs, residuals
Typical outputs	R(t), MTTF, failure-mode criticality, fault trees	Alarms, fault classes, anomaly scores
Uncertainty treatment	Explicit and probabilistic at population level	Often implicit, thresholds or uncalibrated scores
Main consumer	Designers, safety assessors, logistics planners	Operators, recovery software, technicians
Update cycle	Revised at design reviews or after field studies	Continuous

Reading these mismatches across the nine themes of the corpus yields four integration gaps, which the conceptual model is designed to close.

- **G1, Semantic gap.** Reliability artefacts and diagnostic outputs refer to failure modes and components using different identifiers and vocabularies, so their results cannot be joined without manual interpretation.

- **G2, Uncertainty gap.** Reliability models express uncertainty probabilistically, whereas diagnostic outputs are usually thresholded alarms or uncalibrated scores, so they cannot be combined by standard inference.
- **G3, Feedback gap.** Field evidence collected by diagnostic software seldom returns to update design-time reliability parameters or the measured performance of the diagnostics themselves.
- **G4, Decision gap.** Maintenance and operational decisions rarely draw on a single calibrated estimate of asset risk that reflects both prior knowledge and current evidence, and human and logistical constraints are seldom modelled alongside it.

3.2 The Unified Conceptual Model

3.2.1 Design Principles

The model was developed around five principles derived from the mismatches and gaps in Section 3.1.5.

- **Shared semantics.** Every artefact in either discipline must refer to the same component identifiers and failure-mode definitions, so that a diagnostic conclusion can be mapped to a reliability entity without manual interpretation.
- **Probabilistic interfaces.** Information crossing a layer boundary is expressed as a probability distribution, a likelihood, or a quantity with stated uncertainty, rather than as a bare alarm.
- **Bidirectionality.** Evidence flows upward from physical phenomena to decisions, while priors, context and expectations flow downward to guide observation and diagnosis.
- **Fallible diagnosis.** The diagnostic layer is treated as an imperfect sensor characterized by coverage, false-alarm probability and latency, and its own reliability is part of the model.
- **Two time scales.** The model operates both at run time for individual units and over longer periods for fleets, with a feedback loop that converts accumulated diagnostic evidence into recalibrated reliability parameters.

3.2.2 Shared Fault Ontology

The model adopts the fault, error and failure chain of Avizienis et al. (2004) as its backbone. A *fault* is the adjudged or hypothesized cause of an error, such as a degraded DRAM cell or a cracked solder joint.

An *error* is the part of the system state that may lead to a failure, such as a flipped bit in a cache line. A *failure* is an event in which the delivered service deviates from correct service. Reliability engineering mainly quantifies faults and failures, whereas diagnostics mainly observes errors and symptoms. Making the chain explicit clarifies that diagnostics observes the middle of the causal chain and must reason backwards to faults and forwards to failures.

On top of this chain the ontology defines four further concepts: a *component* with a unique identifier and position in the system structure; a *failure mode* attached to a component, carrying its FMECA attributes; a *symptom signature* describing which observable patterns each failure mode is expected to produce; and *confidence semantics*, a rule that every diagnostic statement carries either a probability or a likelihood ratio. The symptom signature is the critical bridge: it extends each FMECA row with the observations by which that failure mode can be recognized, converting a design-time document into a diagnostic knowledge base.

3.2.3 The Five Layers

Figure 1 shows the model. Its layers are ordered from physical phenomena at the bottom to decisions at the top, with the shared ontology spanning all of them.

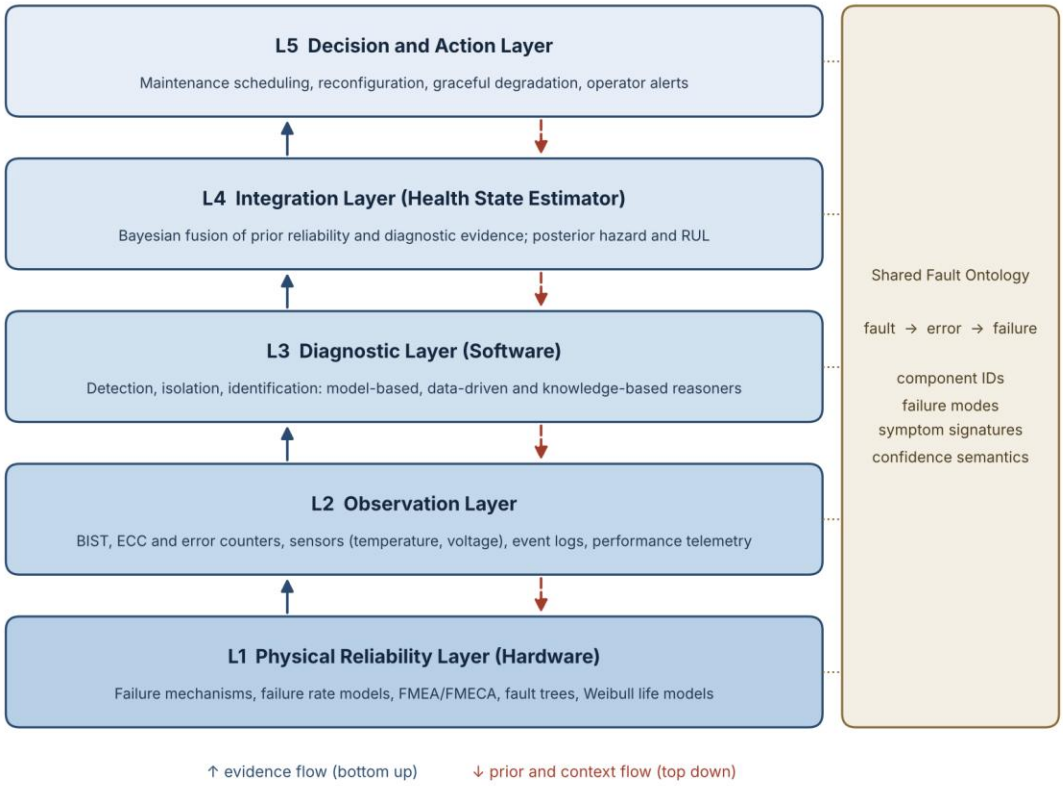


Figure 1. The unified conceptual model: five layers linked by bottom-up evidence flow and top-down prior and context flow, anchored in a shared fault ontology.

L1, Physical Reliability Layer. This layer holds the hardware and the models that describe how it fails: failure mechanisms, life distributions, failure-rate predictions, FMECA tables and fault trees. Its outputs are prior distributions over component health and over the time to each failure mode, conditioned on known stresses such as temperature and duty cycle.

L2, Observation Layer. This layer comprises the instrumentation through which hardware condition becomes visible to software: built-in self-test, error-correcting code counters, parity checks, watchdogs, environmental sensors, performance counters and event logs. Each observation channel is characterized by what it can see (its coverage of failure modes), how noisy it is, and its sampling rate. The top-down flow allows higher layers to request additional tests or raise sampling rates when suspicion increases. Remote inspection by unmanned aerial vehicles extends this layer to geographically dispersed assets (Dagodzo & Ahiaeke Patrick, 2020; Dagodzo, 2018b).

L3, Diagnostic Layer. Here software reasoners perform detection, isolation and identification. The model is deliberately agnostic about technique: model-based residual generators, rule engines and trained

classifiers may coexist. What the model prescribes is the interface. Each reasoner must report its conclusions against the shared ontology, as likelihoods of the observed evidence under each candidate failure mode, together with its calibrated coverage and false-alarm characteristics. Detection pipelines from operational technology security (Adegbite et al., 2020) and enterprise intrusion detection and log analytics (Dosunmu & Ogundele, 2020; Mbonu, Iwuanyanwu, et al., 2019) already exhibit much of this structure and could be adapted to it.

L4, Integration Layer. The integration layer, or health state estimator, is the core contribution of the model. It fuses the L1 priors with the L3 likelihoods to produce a posterior health state for each component, a posterior hazard rate and a remaining useful life distribution. It also propagates component-level posteriors through the system structure, for example a fault tree or reliability block diagram, to obtain system-level risk.

L5, Decision and Action Layer. This layer turns posterior risk into actions: proactive replacement, workload migration, reconfiguration to spare resources, graceful degradation or operator notification. Because decisions are taken on calibrated probabilities rather than raw alarms, they can be optimized against explicit cost and risk criteria, consistent with the reconfigurable fault-tolerant control literature (Zhang & Jiang, 2008).

Decisions at this layer are made by people as well as software, so human factors matter. Studies of operational integrity in high-risk drilling (Nwangwu et al., 2018), data-driven occupational risk control (Obriki & Arumosoye, 2018), safety walkthroughs and culture (Obriki & Arumosoye, 2019), leadership-driven safety culture (Obogo, Ozobu, et al., 2019a), construction safety risk governance (Obogo, Ozobu, et al., 2019b), hazard identification practice (Obogo, Uduokhai, et al., 2019), human error causation (Obriki & Arumosoye, 2020), heat stress in extreme environments (Arumosoye & Obriki, 2018), contractor safety governance (Arumosoye & Obriki, 2020), QHSE audit systems (Obogo et al., 2020a), heavy-lift risk management (Obogo et al., 2020b) and safety management in maintenance projects (Obogo et al., 2020c) show that well-calibrated risk estimates help only if they are presented in a form that operators trust and can act on. Maintenance actions also depend on the availability of spares, which links L5 to supply chain risk management for gas processing projects (Agbabiaka et al., 2019), procurement optimization in oil and gas (Okonkwo et al., 2018a), inventory availability and plant uptime (Okonkwo et al., 2018b), demand forecasting (Aifuwa et al., 2020), contractual resilience in energy supply chains (Uchechi et al., 2020) and capital equipment financing (Okoli et al., 2020).

3.2.4 Information Flows and the Fleet Feedback Loop

Two flows run through the layers. The bottom-up evidence flow carries observations, diagnostic likelihoods and posterior estimates toward decisions. The top-down prior and context flow carries failure-mode priors to diagnostic reasoners, so that rare failure modes require stronger evidence than common ones, and carries attention requests to the observation layer. A third flow operates on the longer time scale: outcomes recorded at L5, such as confirmed failures after component removal, are returned to L1 to recalibrate life distributions and to L3 to recalibrate diagnostic coverage. This fleet feedback loop is what allows the model to correct inaccurate design-time assumptions over the service life of a product line. In practice, maintenance programme records (Obetta, 2020), near-miss and hazard observation databases (Arumosoye & Obriki, 2019) and IT support processes (Anyanwu, 2019) are natural sources of these outcome records. Table 3 lists the principal constructs exchanged across each interface.

Table 3. Principal constructs exchanged at each layer interface

Interface	**Downward (prior and context)**	**Upward (evidence)**
L1 to L2	Expected failure modes and their observable symptoms; recommended monitoring points	Raw physical phenomena made observable by instrumentation
L2 to L3	Requests for additional tests or higher sampling rates	Time-stamped observations with channel identifiers and noise characteristics
L3 to L4	Prior probabilities of failure modes for each component	Likelihoods P(evidence | mode), coverage c, false-alarm probability f
L4 to L5	Risk tolerances, cost models, mission profile	Posterior health state, posterior hazard, remaining useful life distribution, system-level risk
L5 to L1 (fleet loop)	Not applicable	Confirmed failure times and modes, censored survival data, diagnostic outcome records

3.3 Probabilistic Formalization

3.3.1 Health State

Let each component i have a discrete health state $S_i(t)$ taking values in $\{H, D_1, ..., D_m, F\}$, where H denotes healthy, D_k denotes a latent or degraded condition associated with failure mode k, and F denotes failed. Discrete states are chosen because they map directly onto FMECA rows and fault tree basic events; continuous degradation variables can be accommodated by discretization or by replacing the states with a continuous latent variable without changing the structure of the model.

3.3.2 Reliability Priors from L1

The physical reliability layer supplies, for each component, a baseline hazard $h_0(t)$ and a prior distribution over latent states at time t. For a Weibull life model with shape β and scale η, the baseline reliability and hazard are

$$R_0(t) = \exp[\, -(t / \eta)^{\beta} \,], \quad h_0(t) = (\beta / \eta)(t / \eta)^{\beta - 1} \tag{1}$$

The prior probability of a degraded state, $\pi_k(t) = P(S_i(t) = D_k)$, is obtained from the FMECA mode apportionment and, where available, from physics-of-failure models of degradation onset. These priors encode the design-time knowledge that pure diagnostic reasoners usually discard.

3.3.3 Diagnostic Evidence from L3

Let e denote the evidence produced by the diagnostic layer over an observation window. Rather than a binary alarm, each reasoner provides the likelihood of the evidence under each state, $L_k = P(e \mid S = D_k)$ and $L_H = P(e \mid S = H)$. For a simple detector these likelihoods follow directly from its coverage c_k, the probability of raising an alarm given mode k, and its false-alarm probability f:

$$P(\text{alarm} \mid D_k) = c_k, \quad P(\text{alarm} \mid H) = f \tag{2}$$

Richer reasoners, such as classifiers producing probability vectors, can be converted into likelihoods by dividing their posterior outputs by the class priors used during training. This conversion is important: it prevents the training-set class frequencies from silently replacing the reliability priors of Section 3.3.2.

3.3.4 Posterior Health State in L4

The integration layer combines priors and likelihoods by Bayes' rule (Pearl, 1988):

$$P(D_k \mid e) = L_k \, \pi_k \, / \, (\, L_H \, \pi_H + \Sigma_j \, L_j \, \pi_j \,) \tag{3}$$

Expressed in odds form for a single degraded state, the posterior odds equal the prior odds multiplied by the likelihood ratio $\Lambda = L_D / L_H$. The odds form makes the role of each discipline transparent: reliability engineering contributes the prior odds, and diagnostics contributes the likelihood ratio. A diagnostic alarm with a high likelihood ratio for a failure mode that reliability analysis rates as very rare may still yield a modest posterior, which is the formal expression of the principle that extraordinary claims require extraordinary evidence.

3.3.5 Posterior Hazard and Remaining Useful Life

Each latent state carries a hazard multiplier $\kappa_k \geq 1$ relative to the baseline, estimated from accelerated tests, field data or expert judgement, with $\kappa_H = 1$. Following the proportional hazards approach widely used in condition-based maintenance (Jardine et al., 2006), the posterior hazard after evidence arrives at time t_e is

$$h(t \mid e) = h_0(t) \cdot \rho(e), \quad \rho(e) = P(H \mid e) + \Sigma_k \kappa_k P(D_k \mid e), \quad t > t_e \tag{4}$$

and the conditional reliability given survival to t_e becomes

$$R(t \mid e, T > t_e) = \exp\{ -\rho(e) [(t / \eta)^{\beta} - (t_e / \eta)^{\beta}] \} \tag{5}$$

The remaining useful life distribution follows directly, and its median or a chosen percentile can be passed to L5. Component posteriors are propagated to system level by substituting posterior unreliabilities for basic-event probabilities in the system fault tree or reliability block diagram (Langseth & Portinale, 2007; Rausand & Høyland, 2004).

3.3.6 Fleet-Level Recalibration

Over the longer time scale, the fleet feedback loop treats confirmed failure times as observed data and units removed without failure as right-censored data, and updates the life distribution parameters by Bayesian or maximum likelihood estimation (Rausand & Høyland, 2004; Si et al., 2011). Simultaneously, each diagnostic alarm that is followed by a confirmed fault, or by a no-fault-found finding, is used to update the estimates of c_k and f. The model therefore learns both how the hardware actually fails and how well the diagnostic software actually sees those failures. This dual recalibration addresses a recurring finding of field studies, namely that real-world failure behaviour can deviate substantially from datasheet predictions (Schroeder & Gibson, 2007; Schroeder et al., 2009).

3.4 Illustrative Application: Server Memory Subsystem

To show how the model operates, consider a DRAM module in a data center server. The example is illustrative: its parameters are chosen to be plausible and to expose the mechanics of the model, not to report measured values. Large-scale field studies have shown that DRAM errors are more frequent than once assumed, that they are strongly correlated within modules, and that the presence of correctable errors substantially raises the probability of future uncorrectable errors (Schroeder et al., 2009). This makes memory a natural case for integrating reliability priors with diagnostic evidence.

L1. The design-time model assigns the module a Weibull life with $\beta = 1.5$ (mild wear-out) and $\eta =$ 60,000 hours, giving a prior median life of about 47,000 hours. FMECA identifies a dominant latent mode D, progressive cell or row degradation, with a prior probability of 0.05 at 15,000 hours of operation and a hazard multiplier $\kappa = 6$.

L2 and L3. The memory controller counts corrected ECC errors and reports their addresses. A diagnostic reasoner classifies the pattern. A few scattered corrected errors are consistent with both transient soft errors and early degradation, giving a moderate likelihood ratio of about 4.75. Repeated corrected errors at the same row, which are far more typical of a permanent fault, give a strong likelihood ratio of about 76.

L4. Applying Equation (3) in odds form, the prior odds of 0.05/0.95 yield posterior probabilities of degradation of 0.20 for moderate evidence and 0.80 for strong evidence. Equation (4) then gives hazard multipliers of $\rho = 0.80 + 6(0.20) = 2.0$ and $\rho = 0.20 + 6(0.80) = 5.0$. Figure 2 shows the resulting reliability curves and Table 4 summarizes their key values.

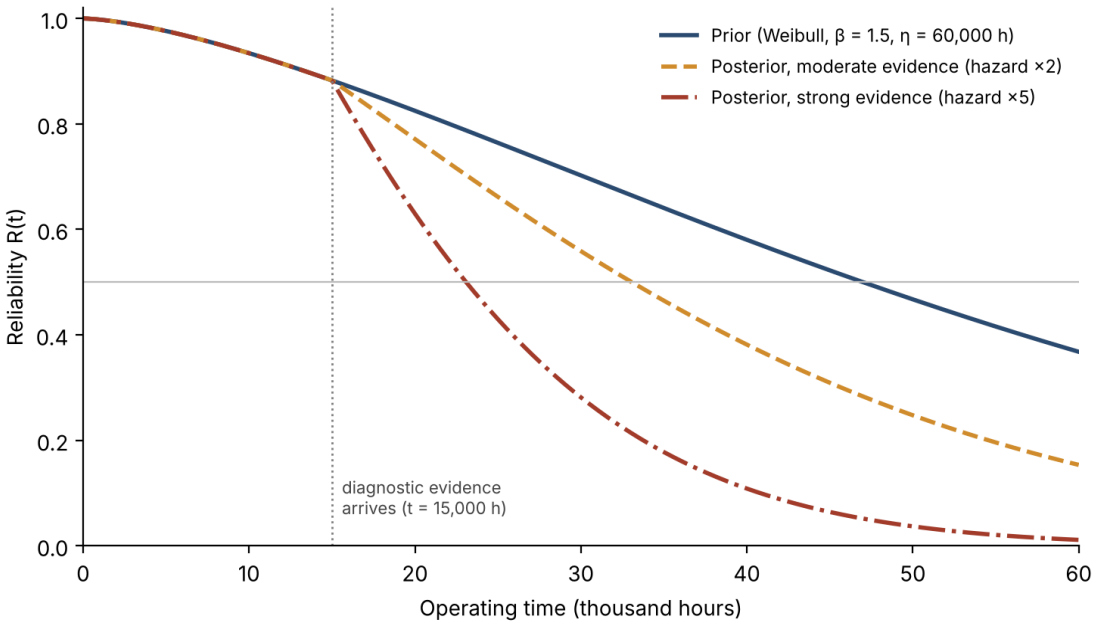


Figure 2. Prior and posterior reliability of the illustrative memory module after diagnostic evidence arrives at 15,000 hours.

Table 4. Effect of diagnostic evidence on predicted reliability (illustrative values)

Scenario	**P(D | e)**	**Hazard multiplier ρ**	**R(30,000 h)**	**Median life (h)**
Prior only (no evidence)	0.05	1.0	0.70	about 47,000
Moderate evidence (Λ ≈ 4.75)	0.20	2.0	0.56	about 33,100
Strong evidence (Λ ≈ 76)	0.80	5.0	0.28	about 23,000

L5. The decision layer can now act on calibrated risk. Under moderate evidence, a reasonable action is to raise the ECC scrubbing rate and schedule replacement at the next planned maintenance window. Under strong evidence, migrating workloads and retiring the affected pages or module promptly is justified, because the predicted probability of surviving to 30,000 hours has fallen from 0.70 to 0.28. Neither the reliability model alone nor the diagnostic classifier alone could produce this graded response: the former cannot distinguish this module from its peers, and the latter cannot express how much its alarm should change the expected lifetime.

Fleet loop. As modules are removed, their confirmed failure modes and times update β, η and κ, while alarm outcomes update the likelihood ratios. If the fleet shows that repeated same-row errors precede failure even more reliably than assumed, the strong-evidence likelihood ratio rises and future decisions become more decisive.

3.5 Discussion

3.5.1 Answering the Research Questions

With respect to RQ1, the synthesis shows that the two disciplines diverge on eight dimensions, from their central question and unit of analysis to their treatment of uncertainty and update cycle (Table 2), and that these divergences produce four integration gaps: semantic, uncertainty, feedback and decision. The applied literature reviewed confirms that the gaps are practical rather than theoretical. Integrity and maintenance programmes in oil and gas encode rich failure-mode knowledge yet update it periodically (Obetta, 2019; Obetta, 2020), while monitoring and detection systems in power, security and IT operations generate continuous evidence that is rarely expressed in probabilistic terms (Adaramola et al., 2018; Ahmed et al., 2020; Dosunmu & Ogundele, 2020).

With respect to RQ2, the model answers with five layers, a shared ontology and three information flows. Each element is traceable to a gap: the shared ontology and symptom signatures address G1; probabilistic interfaces at every layer boundary address G2; the fleet feedback loop addresses G3; and the decision layer, informed by calibrated posteriors and by human-factors and logistics considerations, addresses G4. With respect to RQ3, the probabilistic formalization shows that combination is principled and computationally light: reliability knowledge enters as prior odds, diagnostic evidence as a likelihood ratio, and their product as a posterior that modulates a baseline hazard. The illustrative scenario shows the practical value of this combination, producing graded actions that neither discipline could justify alone.

3.5.2 Relationship to Existing Frameworks

The model is intended to complement rather than replace existing frameworks. It specializes the dependability taxonomy of (Avizienis et al., 2004) into a computational structure; it places PHM pipelines (Lee et al., 2014; Pecht, 2008) within a broader context that includes design-time artefacts; and it can host Bayesian network formulations (Langseth & Portinale, 2007; Weber et al., 2012) as concrete implementations of the integration layer. Its distinctive contribution is the insistence on a shared ontology and on explicit, bidirectional, probabilistic interfaces between the reliability and diagnostic worlds.

The model also differs from the security and IT operations frameworks reviewed in Section 3.1.4. Those frameworks share the detection structure of the diagnostic layer but rarely connect alerts to physical failure mechanisms (Adegbite et al., 2020; Dosunmu & Ogundele, 2019). Placing them within the model would let a single integration layer weigh hardware degradation and malicious activity as competing explanations for the same symptoms.

3.6 Implications

3.6.1 Theoretical Implications

The study has three theoretical implications. First, it reframes hardware reliability and software diagnostics as two estimators of the same latent quantity, component health, operating at different time scales, rather than as separate disciplines with separate outputs. Second, it extends the dependability taxonomy of Avizienis et al. (2004) from a descriptive vocabulary into a computational structure, showing how the fault, error and failure chain can carry probabilities between layers. Third, it positions diagnostic software as a fallible sensor whose coverage and false-alarm rates are themselves parameters to be estimated, which integrates software reliability concerns (Grottke & Trivedi, 2007; Lyu, 1996) into hardware reliability modelling.

3.6.2 Practical Implications

For practitioners, the model has four implications. First, FMECA documents should be extended with symptom signatures and observation channels, turning a compliance artefact into a living diagnostic asset. Second, diagnostic software should report calibrated likelihoods rather than bare alarms, which requires that diagnostic coverage and false-alarm rates be measured, not merely asserted, consistent with the diagnostic coverage concepts in IEC 61508 (International Electrotechnical Commission, 2010). Third, the integration layer should be treated as an explicit architectural component with its own requirements, verification and ownership, instead of an implicit function scattered among monitoring tools, maintenance spreadsheets and operator judgement; experience with integrity management programmes (Obetta & Ninduwezuor-Ehiobu, 2019; Obetta, 2019) and automated risk assessment frameworks (Uchechi & Ominyi, 2020) suggests that such a component is organizationally feasible. Fourth, maintenance records, near-miss databases and IT service tickets should be structured so that they can feed the fleet feedback loop (Anyanwu, 2019; Arumosoye & Obriki, 2019).

3.6.3 Implications for Standards and Governance

For standards bodies and asset owners, the model suggests that reliability prediction and diagnostic coverage requirements, which are currently specified separately, could be linked through common failure-mode identifiers and reporting formats. Governance frameworks for safety, integrity and IT service management could then require that risk-based decisions cite a calibrated estimate of asset health and its sources, improving traceability and auditability of maintenance decisions (Akomolafe & Agu, 2018; Obogo et al., 2020a).

3.7 Limitations

Several limitations should be acknowledged. The formalization assumes that diagnostic evidence is conditionally independent given the health state; correlated evidence from multiple reasoners observing the same symptom will overstate confidence unless dependencies are modelled. The proportional hazards assumption may not hold for all failure mechanisms, particularly those with abrupt onset. Hazard multipliers and likelihood ratios require data that may be scarce for new designs, so early in a product's life the model will lean heavily on expert judgement. The illustrative application uses chosen rather than measured parameters, and the model has not yet been validated empirically on field data. Finally, the model addresses hardware faults diagnosed by software; it treats software faults in the diagnostic layer only through its coverage and false-alarm parameters, and a fuller treatment of software aging and software reliability (Grottke & Trivedi, 2007; Lyu, 1996) remains outside its scope. Research on human error causation (Obriki & Arumosoye, 2020) further cautions that actions taken at the decision layer remain subject to human error, however well calibrated the estimates that inform them.

The study also has methodological limitations. As a conceptual paper, it develops and illustrates the model but does not test it. The review corpus was restricted to sources published to date and drawn from foundational texts and a consolidated applied corpus, so relevant work outside these sources may have been missed, and the thematic coding was performed by a single analyst without inter-rater checks. The illustrative scenario covers one subsystem in one domain; other domains, such as rotating machinery or power electronics, may expose requirements the model does not yet address.

3.8 Future Research

A research agenda follows from these limitations. Empirical validation on fleet data, such as server telemetry or automotive diagnostic trouble codes, is the most urgent need, with prediction accuracy

assessed using established prognostic metrics (Si et al., 2011). Methods for learning dependency structures among diagnostic reasoners would relax the conditional independence assumption. Extending the ontology to include software faults and their interaction with hardware faults would move the model toward a full system-level dependability framework. Finally, the rapid growth of deep learning in fault diagnosis (Lei et al., 2020) raises the question of how to obtain calibrated likelihoods from such models; calibration techniques and uncertainty-aware architectures deserve study specifically in the context of the integration layer. Spatially explicit risk modelling under limited data (Lamidi & Olamide, 2018) and machine learning for predictive resource scaling (Ahmed et al., 2020) are useful starting points.

Four further directions follow from the methodology. Case studies in at least two contrasting domains, for example offshore static equipment and data centre hardware, would test whether the five layers and four gaps generalize. Delphi studies with reliability engineers, diagnosticians and maintenance managers could refine the ontology and the design principles. Structured systematic reviews with explicit search strings and multiple coders would strengthen the evidence base. Finally, simulation studies comparing decisions made with and without the integration layer would quantify its economic value in terms of avoided failures, unnecessary replacements and spare-part inventory.

4. CONCLUSION

Hardware reliability engineering and software-based fault diagnostics describe the same underlying reality, the progression from faults through errors to failures, from complementary vantage points. Through an integrative review of 120 sources published to date, this paper has shown that their separation produces semantic, uncertainty, feedback and decision gaps, and has proposed a unified conceptual model to close them. The model organizes the problem into five layers bound by a shared fault ontology, defines probabilistic interfaces through which reliability priors and diagnostic likelihoods meet, and closes a fleet feedback loop that lets field evidence correct design assumptions. The formalization shows that the combination is principled and computationally simple, and the illustrative memory example shows that it produces graded, risk-based decisions that neither discipline can produce alone. Validating and extending the model on real systems is the natural next step.

REFERENCES

Abdulrazaq, K., Yusuf, H. D., Osinem, H. E., & Eribenne, F. (2019). A model for improving infection detection accuracy through integrated laboratory information systems. *Iconic Research and Engineering Journals*, *3*(6), 650-675. https://doi.org/10.64388/IREV3I6-1723089

Adaramola, T. S., Fadero, S., & Gideon, E. N. (2018). Predictive maintenance and condition monitoring in critical power and energy infrastructure. *Iconic Research and Engineering Journals*, *2*(5), 454-477. https://doi.org/10.64388/IREV2I5-1722489

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2020). Securing operational technology networks in electric utilities: A systematic review of NERC CIP compliance and architectural threat mitigation. *International Journal of Engineering and Modern Technology*, *6*(3), 103-146. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg103.146

Adeniji, I. O., Shittu, H., Opara, I. S., & Shittu, M. A. (2020). Grounding system design optimization for medium-voltage distribution networks in emerging power markets. *Iconic Research and Engineering Journals*, *3*(11), 547-565. https://doi.org/10.64388/IREV3I11-1714040

Adeyelu, O. O. (2018). A predictive compliance monitoring framework for detecting systemic safety risks through aviation consumer complaint data. *Iconic Research and Engineering Journals*, *1*(8), 250-276. https://doi.org/10.64388/IREV1I8-1718478

Adeyelu, O. O. (2019). An adaptive safety management system implementation model for aerodromes in developing economy contexts. *Iconic Research and Engineering Journals*, *3*(4), 628-654. https://doi.org/10.64388/IREV3I4-1718479

Adeyelu, O. O. (2020). An artificial intelligence-driven conceptual model for wildlife strike risk quantification and aircraft airworthiness impact assessment at high-traffic African airports. *Iconic Research and Engineering Journals*, *4*(1), 339-368. https://doi.org/10.64388/IREV4I1-1718482

Agbabiaka, J., Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2019). Supply chain risk management model for EPC and gas processing projects. *Iconic Research and Engineering Journals*, *3*(2), 968-980. https://doi.org/10.64388/IREV3I2-1713124

Agboada, P., Ezeako, R., Okoli, I. E., & Uzondu, C. S. (2018). Digital transformation in operations management: A review of advances in automation, analytics, and process redesign. *International Journal of Engineering Technology Research & Management*, *2*(11), 109-134.

Agboada, P., Ezeako, R., Okoli, I. E., & Uzondu, C. S. (2019). Standard operating procedures as change infrastructure: A conceptual framework for sustaining operational improvement. *Iconic Research and Engineering Journals*, *3*(6), 706-730. https://doi.org/10.64388/IREV3I6-1723313

Ahmed, K. S., & Odejobi, O. D. (2018a). Conceptual framework for scalable and secure cloud architectures for enterprise messaging. *IRE Journals*, *2*(1), 1-15.

Ahmed, K. S., & Odejobi, O. D. (2018b). Resource allocation model for energy-efficient virtual machine placement in data centers. *IRE Journals*, *2*(3), 1-10.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2019). Algorithmic model for constraint satisfaction in cloud network resource allocation. *IRE Journals*, *2*(12), 516-532.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2020). Predictive model for cloud resource scaling using machine learning techniques. *Journal of Frontiers in Multidisciplinary Research*, *1*(1), 173-183.

Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., Ike, P. N., Nnabueze, S. B., & Olatunde-Thorpe, J. (2020). Predictive analytics models enhancing supply chain demand forecasting accuracy and reducing inventory management inefficiencies. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(3), 171-181. https://doi.org/10.54660/.IJMRGE.2020.1.3.171-181

Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. *Iconic Research and Engineering Journals*, *1*(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778

Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. *Iconic Research and Engineering Journals*, *1*(9), 458-475.

Akomolafe, O., & Agu, M. U. (2019). A review of data-driven risk evaluation models for emerging market financial institutions. *Iconic Research and Engineering Journals*, *3*(6), 433-448.

Amayo, E. B. (2017). Multi algorithm of loss objective function of a single phase induction motor. *International Journal of Development Research*, *7*(5), 12805-12810.

Amayo, E. B., & Popoola, T. T. (2017a). Multi algorithm of weight objective function of a single phase induction motor. *International Journal of Trend in Research and Development*, *4*(2), 184-188.

Amayo, E. B., & Popoola, T. T. (2017b). Scientific study of telecommunication deployment in achieving quality network. *International Journal of Trend in Research and Development*, *4*(5), 311-314.

Amayo, E. B., Ubeku, E., & Oshevire, P. (2015). Multi algorithm of a single objective function of a single phase induction motor. *Journal of Multidisciplinary Engineering Science and Technology*, *2*(12), 3400-3403.

Aneke, O. B., & Adesemoye, A. C. (2019). Toward an integrated conceptual framework for traceability and chain-of-custody integrity in pharmaceutical distribution. *Iconic Research and Engineering Journals*, *3*(4), 655-672.

Aneke, O. B., & Adesemoye, A. C. (2020). A conceptual framework for risk-based decision-making in good manufacturing practice environments. *Iconic Research and Engineering Journals*, *4*(6), 325-341.

Anyanwu, K. C. E. (2019). Developing a maturity model for standardizing IT support operations across geographically distributed multi-office organizations. *Iconic Research and Engineering Journals*, *3*(5), 580-598.

Anyanwu, K. C. E. (2020). Balancing cost and operational continuity in hybrid remote and on-site IT support for multi-branch SMEs. *International Journal of Economics and Financial Management*, *5*(2), 132-148. https://doi.org/10.56201/ijefm.v5.no2.2020.pg132.148

Arumosoye, O. M., & Obriki, O. D. (2018). Development of an integrated heat stress risk conceptual model for industrial operations in extreme environments. *Iconic Research and Engineering Journals*, *1*(12), 141-160. https://doi.org/10.64388/IREV1I12-1714415

Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. *Iconic Research and Engineering Journals*, *3*(2), 981-999. https://doi.org/10.64388/IREV3I2-1714417

Arumosoye, O. M., & Obriki, O. D. (2020). A governance-oriented conceptual model for contractor safety performance in multi-contract industrial projects. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 728-740. https://doi.org/10.54660/.IJMRGE.2020.1.5.728-740

Asibor, E., & Isong, D. E. (2019). Risk-based process engineering framework for strengthening reliability across complex natural gas infrastructure systems. *Iconic Research and Engineering Journals*, *3*(2), 1020-1060. https://doi.org/10.64388/IREV3I2-1723153

Atta, S., Asomani, E., & Adenuga, O. M. (2018). A systematic review of green corrosion inhibitors from agricultural extracts for mild steel protection in acidic and alkaline media. *International Journal of Engineering and Modern Technology*, *4*(1), 64-97. https://doi.org/10.56201/ijemt.vol.4.no1.2018.pg64.97

Atta, S., Tofah, P., Kankam, M. A., & Adenuga, O. M. (2020). A critical review of NDT-based integrity management and corrosion risk assessment strategies for refinery process equipment. *International Journal of Engineering and Modern Technology*, *6*(2), 19-46. https://doi.org/10.56201/ijemt.vol.6.no2.2020.pg19.46

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11-33.

Azeez, L. O., & Badmus, O. B. (2018). Data-driven framework for predicting subsurface contamination pathways in complex remediation projects. *Iconic Research and Engineering Journals*, *2*(5), 312-335.

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2018). A systematic review of CI/CD pipeline strategies in Salesforce DevOps: Tools, practices, and deployment outcomes. *Iconic Research and Engineering Journals*, *2*(6).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019a). A conceptual model for ETL design and data integration in Salesforce-centric enterprise architectures. *Iconic Research and Engineering Journals*, *3*(5).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019b). A governance framework for Salesforce platform management in regulated healthcare environments. *Iconic Research and Engineering Journals*, *3*(6).

Badmus, O., Dosunmu, A. A., Ozowara, D. E., & Anunagba, C. O. (2020). A comparative framework for Salesforce DevOps tooling: Evaluating Copado, Flosum, and Salesforce DX across enterprise deployment contexts. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 1021-1031. https://doi.org/10.54660/.IJMRGE.2020.1.5.1021-1031

Birolini, A. (2017). *Reliability engineering: Theory and practice* (8th ed.). Springer.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Dagodzo, D. (2018a). A conceptual framework for UAV integration into national power grid inspection programs. *Iconic Research and Engineering Journals*, *2*(5), 391-412. https://doi.org/10.64388/IREV2I5-1716082

Dagodzo, D. (2018b). A review of UAV applications in electrical transmission line inspection: Methods, technologies, and challenges. *Iconic Research and Engineering Journals*, *2*(6), 234-254. https://doi.org/10.64388/IREV2I6-1716083

Dagodzo, D. (2018c). Hydrothermal alteration interpretation of LANDSAT and ASTER data. Lambert Academic Publishing.

Dagodzo, D., & Ahiaeke Patrick, M. C. (2020). UAV-based pipeline and corridor monitoring: A review of current practices and emerging technologies. *Iconic Research and Engineering Journals*, *3*(10), 574-597. https://doi.org/10.64388/IREV3I10-1716084

Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. *Iconic Research and Engineering Journals*, *3*(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225

Dosunmu, A. A., & Ogundele, P. O. (2020). Intrusion detection and prevention models for enhancing organizational cyber defense effectiveness. *Iconic Research and Engineering Journals*, *4*(6), 310-324. https://doi.org/10.64388/IREV4I6-1713226

Ekemezie, U. C., Ohunyon, G., & Sydney, E. (2018). Evaluating IDSR implementation in Benue State, Nigeria: DHIS2 data quality and surveillance capacity. *Iconic Research and Engineering Journals*, *2*(6).

Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. *Iconic Research and Engineering Journals*, *2*(12), 602-617. https://doi.org/10.64388/IREV2I12-1713779

Fadero, S., Jooda, D., Oyesiji, S. O., & Nwakamma, S. (2020). Business continuity and disaster recovery preparedness in African financial services: Lessons from the COVID-19 pandemic. *Iconic Research and Engineering Journals*, *3*(9), 525-544. https://doi.org/10.64388/IREV3I9-1722620

Gideon, E. N., Adaramola, T. S., & Fadero, S. (2019). Reliability engineering and failure analysis in complex engineering systems. *Iconic Research and Engineering Journals*, *2*(11), 703-727. https://doi.org/10.64388/IREV2I11-1722490

Grottke, M., & Trivedi, K. S. (2007). Fighting bugs: Remove, retry, replicate, and rejuvenate. *Computer*, *40*(2), 107-109.

International Electrotechnical Commission. (2010). *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems* (2nd ed.).

Isermann, R. (2006). *Fault-diagnosis systems: An introduction from fault detection to fault tolerance*. Springer.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, *10*(1-2), 18-26. https://doi.org/10.1007/s13162-020-00161-0

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, *8*(4), 49-62. https://doi.org/10.1177/160940690900800406

Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, *20*(7), 1483-1510.

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer*, *36*(1), 41-50.

Komi, N. M., & Adeniji, I. O. (2020). Co-optimizing technical performance and community affordability in smart solar microgrids for underserved regions. *International Journal of*

Engineering and Modern Technology, *6*(3), 173-212. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg173.212

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. *Iconic Research and Engineering Journals*, *2*(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. *Iconic Research and Engineering Journals*, *3*(4), 608-627. https://doi.org/10.64388/IREV3I4-1717206

Lamidi, O. B. A., & Olamide, A. (2018). Spatially explicit risk modeling framework for tracking subsurface contaminant migration in data-limited remediation sites. *Iconic Research and Engineering Journals*, *2*(6), 178-198.

Langseth, H., & Portinale, L. (2007). Bayesian networks in reliability. *Reliability Engineering & System Safety*, *92*(1), 92-108.

Lawal, O. A., & Oduleye, T. E. (2019). Conceptualizing data driven executive decision systems for strategic financial planning. *Iconic Research and Engineering Journals*, *3*(3).

Lee, J., Wu, F., Zhao, W., Ghaffari, M., Liao, L., & Siegel, D. (2014). Prognostics and health management design for rotary machinery systems: Reviews, methodology and applications. *Mechanical Systems and Signal Processing*, *42*(1-2), 314-334.

Lei, Y., Yang, B., Jiang, X., Jia, F., Li, N., & Nandi, A. K. (2020). Applications of machine learning to machine fault diagnosis: A review and roadmap. *Mechanical Systems and Signal Processing*, *138*, Article 106587.

Lyu, M. R. (Ed.). (1996). *Handbook of software reliability engineering*. McGraw-Hill.

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. *Iconic Research and Engineering Journals*, *2*(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2020). A review of identity and access management integration strategies in hybrid and multi cloud environments. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 795-810. https://doi.org/10.54660/.IJMRGE.2020.1.5.795-810

Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. *Iconic Research and Engineering Journals*, *2*(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. *International Journal of*

Multidisciplinary Research and Growth Evaluation, *1*(5), 811-828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828

Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. *Iconic Research and Engineering Journals*, *3*(2), 1000-1019. https://doi.org/10.64388/IREV3I2-1714915

Mukherjee, S. (2008). *Architecture design for soft errors*. Morgan Kaufmann.

Nwangwu, C. V., Duvbiama-Owasanoye, O. A., & Onwumere, A. (2018). A framework for operational integrity in high-risk drilling: Balancing productivity and safety compliance. *Iconic Research and Engineering Journals*, *2*(5), 436-453.

Nwangwu, C. V., Duvbiama-Owasanoye, O. A., & Onwumere, A. (2020). High-fidelity reservoir forecasting: A technical review of multimodal modeling for long-term production estimates. *Iconic Research and Engineering Journals*, *4*(5), 390-409.

Obetta, P. C. (2018). A risk-based inspection concept for fitness-for-service assessment of ageing pressure vessels on offshore joint venture facilities. *Iconic Research and Engineering Journals*, *2*(5), 497-520. https://doi.org/10.64388/IREV2I5-1722578

Obetta, P. C. (2019). Reliability and integrity management of fired heaters, boilers and furnaces in upstream oil and gas: A review. *Iconic Research and Engineering Journals*, *3*(5), 599-626. https://doi.org/10.64388/IREV3I5-1722580

Obetta, P. C. (2020). A reliability-centered maintenance (RCM) concept for static mechanical equipment in offshore oil and gas operations. *International Journal of Multidisciplinary Futuristic Development*, *1*(1), 74-91. https://doi.org/10.54660/IJMFD.2020.1.1.74-91

Obetta, P. C., & Ninduwezuor-Ehiobu, N. (2018). A condition-based maintenance concept for CALM buoy bearings and swivels to improve offshore crude export availability. *Iconic Research and Engineering Journals*, *2*(6), 385-410. https://doi.org/10.64388/IREV2I6-1722579

Obetta, P. C., & Ninduwezuor-Ehiobu, N. (2019). Integrity assurance of FSO turret mooring systems: A review of inspection, monitoring and life-extension strategies. *Iconic Research and Engineering Journals*, *3*(6), 599-629. https://doi.org/10.64388/IREV3I6-1722581

Obetta, P. C., Ninduwezuor-Ehiobu, N., & Olisakwe, H. C. (2020). Corrosion management and material selection for crude oil export equipment in marine environments: A review. *International Journal of Multidisciplinary Futuristic Development*, *1*(1), 92-110. https://doi.org/10.54660/IJMFD.2020.1.1.92-110

Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020a). Advances in internal QHSE audit systems for industrial engineering operations. *Iconic Research and Engineering Journals*, *4*(4), 399-417. https://doi.org/10.64388/IREV4I4-1715499

Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020b). Conceptual risk management model for heavy lifting and crane installation engineering operations. *Shodhshauryam, International Scientific Refereed Research Journal*, *3*(4), 122-144. https://doi.org/10.32628/SHISRRJ214441

Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020c). Critical review of occupational safety management systems in oil and gas maintenance projects. *Shodhshauryam, International Scientific Refereed Research Journal*, *3*(4), 145-166. https://doi.org/10.32628/SHISRRJ214442

Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019a). Advances in leadership driven safety culture transformation in large construction workforces. *Iconic Research and Engineering Journals*, *3*(5), 507-523. https://doi.org/10.64388/IREV3I5-1715497

Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019b). Development of a construction safety risk governance model for multi contractor high rise projects. *Iconic Research and Engineering Journals*, *2*(9), 502-522. https://doi.org/10.64388/IREV2I9-1715495

Obogo, S. F., Uduokhai, D. O., & Ozobu, C. O. (2019). Systematic review of hazard identification and risk control practices in urban construction projects. *Iconic Research and Engineering Journals*, *2*(12), 666-681. https://doi.org/10.64388/IREV2I12-1715496

Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. *Iconic Research and Engineering Journals*, *1*(7), 169-189. https://doi.org/10.64388/IREV1I7-1714414

Obriki, O. D., & Arumosoye, O. M. (2019). A conceptual framework linking management safety walkthrough frequency and coverage to safety culture outcomes in mega projects. *Iconic Research and Engineering Journals*, *2*(8), 355-374. https://doi.org/10.64388/IREV2I8-1714416

Obriki, O. D., & Arumosoye, O. M. (2020). Conceptual framework for human error causation in high-risk construction and industrial activities. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 715-727. https://doi.org/10.54660/.IJMRGE.2020.1.5.715-727

Odejobi, O. D., & Ahmed, K. S. (2018a). Performance evaluation model for multi-tenant Microsoft 365 deployments under high concurrency. *IRE Journals*, *1*(11), 92-107.

Odejobi, O. D., & Ahmed, K. S. (2018b). Statistical model for estimating daily solar radiation for renewable energy planning. *IRE Journals*, *2*(5), 1-12.

Odejobi, O. D., Hammed, N. I., & Ahmed, K. S. (2019). Approximation complexity model for cloud-based database optimization problems. *IRE Journals*, *2*(9), 1-10.

Okoli, I., Agboada, P., Kinyanjui, A., Akintobi, A., & Pedro, O. (2020). Capital equipment financing and risk management in healthcare technology procurement. International Journal of Humanities and Information Technology(Special Issue 2), 12-54. https://doi.org/10.21590/ijhit.spcl.02.02

Okonkwo, C. S., Ogunwole, O., & Okeke, O. T. (2018a). Framework for strategic procurement optimization in oil and gas operations. *Iconic Research and Engineering Journals*, *1*(7), 153-168. https://doi.org/10.64388/IREV1I7-1713119

Okonkwo, C. S., Ogunwole, O., & Okeke, O. T. (2018b). Model for inventory availability and plant uptime improvement in energy facilities. *Iconic Research and Engineering Journals*, *2*(4), 160-172. https://doi.org/10.64388/IREV2I4-1713120

Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(5), 371-389.

Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 1032-1044. https://doi.org/10.54660/.IJMRGE.2020.1.5.1032-1044

Oshevire, P., Eyenubo, O. J., & Amayo, B. (2017). Voltage control in the presence of distributed generation. *ATBU Journal of Science, Technology and Education*, *5*(2), 165-173.

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2019). Secure identity and access management model for distributed and federated systems. *IRE Journals*, *3*(4), 550-567.

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. *Journal of Frontiers in Multidisciplinary Research*, *1*(1), 193-201.

Oziri, S. T., Arowogbadamu, A. A. G., & Seyi-Lande, O. B. (2020). Predictive analytics applications in reducing customer churn and enhancing lifecycle value in telecommunications markets. *International Journal of Multidisciplinary Futuristic Development*, *1*(2), 40-49.

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: Networks of plausible inference*. Morgan Kaufmann.

Pecht, M. (2008). *Prognostics and health management of electronics*. Wiley.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Wiley.

Salfner, F., Lenk, M., & Malek, M. (2010). A survey of online failure prediction methods. *ACM Computing Surveys*, *42*(3), Article 10.

Schroeder, B., & Gibson, G. A. (2007). Disk failures in the real world: What does an MTTF of 1,000,000 hours mean to you? In *Proceedings of the 5th USENIX Conference on File and Storage Technologies (FAST 07)*. USENIX Association.

Schroeder, B., Pinheiro, E., & Weber, W.-D. (2009). DRAM errors in the wild: A large-scale field study. In *Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems* (pp. 193-204). ACM.

Shittu, H., Opara, I. S., Elumilade, R. A., & Adeniji, I. O. (2019). Hydrogen as a secondary energy carrier: Modeling its integration in national grids. *Iconic Research and Engineering Journals*, *3*(1), 628-643. https://doi.org/10.64388/IREV3I1-1713909

Si, X.-S., Wang, W., Hu, C.-H., & Zhou, D.-H. (2011). Remaining useful life estimation: A review on the statistical data driven approaches. *European Journal of Operational Research*, *213*(1), 1-14.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sorin, D. J. (2009). *Fault tolerant computer architecture*. Morgan & Claypool.

Sunday, E. A., & Omoegun, G. O. (2018). Integrating solar power solutions in small-scale manufacturing industries in Nigeria. *International Journal of Scientific Research in Science, Engineering and Technology*, *4*(8), 832-853.

Sunday, E. A., & Omoegun, G. O. (2019). Optimizing electrical load distribution for hybrid solar installations in developing economies. *International Journal of Scientific Research in Mechanical and Materials Engineering*, *3*(6), 27-47.

Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2019). Thermodynamic efficiency and control strategies in residential air conditioning systems. *International Journal of Scientific Research in Civil Engineering*, *3*(3), 52-76.

Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2020). Transitioning from reactive to predictive maintenance in mechanical systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(6), 425-447.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356-367. https://doi.org/10.1177/1534484305278283

U.S. Department of Defense. (1991). *MIL-HDBK-217F: Reliability prediction of electronic equipment*.

Uchechi, N., & Ominyi, M. (2020). Advances in automated risk assessment frameworks for regulatory deliverables in upstream energy operations. *International Journal of Multidisciplinary Evolutionary Research*, *1*(2), 158-175. https://doi.org/10.54660/IJMER.2020.1.2.158-175

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2020). Force majeure and contractual resilience in global energy supply chains: A systematic review. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(5), 1247-1264. https://doi.org/10.54660/.IJMRGE.2020.1.5.1247-1264

Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003). A review of process fault detection and diagnosis: Part I: Quantitative model-based methods. *Computers & Chemical Engineering*, *27*(3), 293-311.

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.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii-xxiii.

Yeboah, B. K., & Ike, P. N. (2020). Programmatic strategy for renewable energy integration: Lessons from large-scale solar projects. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(3), 306-315. https://doi.org/10.54660/.IJMRGE.2020.1.3.306-315

Yusuf, H. D., & Abdulrazaq, K. (2018). A conceptual framework for strengthening diagnostic quality systems in resource-limited clinical laboratories. *Iconic Research and Engineering Journals*, *1*(11), 145-179. https://doi.org/10.64388/IREV1I11-1723090

Yusuf, H. D., Abdulrazaq, K., Osinem, H. E., & Eribenne, F. (2020). Advances in antimicrobial resistance surveillance using multi-laboratory national reporting networks. *International Journal of Multidisciplinary Evolutionary Research*, *1*(2), 176-194. https://doi.org/10.54660/IJMER.2020.1.2.176-194

Zhang, Y., & Jiang, J. (2008). Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, *32*(2), 229-252.