Street Art & Urban Creativity | Vol. 12, No. 4, 2026 | ISSN 2183-9956
Street Art & Urban Creativity. Scientific Journal

A Multi-Criteria, Risk-Informed Asset Integrity Framework for Power System Protection & Control Equipment: Bridging Reliability, Cybersecurity, Human Factors, and Lifecycle Economics

CHANDER VIJAY S SANBHI (CHANDER@CHEVRON.COM)[1]

Abstract

The protection and control equipment of a power system is easy to overlook, tucked away in substation cabinets and rarely noticed until something goes wrong, yet it is precisely this equipment that decides whether a fault becomes a contained, momentary event or cascades into a blackout affecting millions. Managing the integrity of these assets has traditionally been treated as an engineering reliability problem, but that framing has become too narrow, because modern protection and control equipment is digital, networked, operated by people under pressure, and expensive to own over its full life, so its integrity now depends on reliability, cybersecurity, human factors, and lifecycle economics together. This paper proposes a multi-criteria, risk-informed asset integrity framework for power system protection and control equipment that deliberately bridges these four dimensions rather than treating them in isolation. The framework scores each asset against the four dimensions, weights and combines them into an integrated, risk-informed integrity index that reflects both the condition of the asset and the consequence of its failure, and uses this index to prioritize maintenance, replacement, and investment decisions. Using a conceptual and analytical approach grounded in the relevant literature, we develop the framework, define its criteria and their aggregation, and demonstrate through analysis how integrating the four dimensions changes asset prioritization compared with reliability-only approaches. The analysis shows that assets ranking as low-priority on reliability alone can rank as high-priority once cybersecurity exposure, human-factors vulnerability, and lifecycle economics are included, so that the integrated framework surfaces risks that conventional approaches miss. The paper concludes that a multi-criteria, risk-informed approach provides a more complete and defensible basis for managing the integrity of protection and control assets, and it discusses the data, weighting, and organizational challenges of applying it.

Keywords: Asset integrity protection & control, multi-criteria decision analysis, risk-informed maintenance cybersecurity, lifecycle economics

1. Introduction

In the vast and intricate machine that is a modern power system, few components carry as much responsibility for so little recognition as the protection and control equipment. These are the relays, controllers, and associated systems that continuously watch over the grid and act, within milliseconds, to isolate faults, protect equipment, and maintain stability when something goes wrong [1]. Their role is fundamentally that of a guardian: when a fault occurs, it is the protection system that decides whether the fault is contained quickly and locally, causing minimal disruption, or whether it spreads, potentially cascading into the kind of large-scale blackout that can affect millions of people and cause enormous economic damage [2]. The integrity of this equipment, its ability to function correctly when called upon, is therefore central to the reliability and security of the entire power system, and managing that integrity is a matter of real consequence.

For much of the history of the field, managing the integrity of protection and control assets was understood primarily as a reliability engineering problem. The equipment was largely electromechanical, self-contained, and physical, and the central questions were about its condition, its ageing, and its likelihood of failing to operate correctly, addressed through inspection, testing, and maintenance aimed at keeping the hardware working [3]. This

reliability-centered view served reasonably well for the equipment of an earlier era, and it remains important, but it has become increasingly inadequate to the realities of modern protection and control equipment, whose nature has changed profoundly.

Several developments have transformed the problem. First, protection and control equipment has become digital and networked, with modern relays and controllers being sophisticated computers connected to communication networks, which introduces an entirely new dimension of risk, namely cybersecurity, since networked digital equipment can be attacked, compromised, or disrupted through cyber means in ways that physical equipment could not [4]. The security of protection and control assets against cyber threats has become a serious concern, particularly given their critical role and the growing threat to critical infrastructure. Second, the equipment is operated and maintained by people, and the correct functioning of protection and control depends not only on the equipment itself but on the humans who configure, test, and operate it, whose errors can compromise integrity as surely as equipment failure, making human factors an essential dimension [5]. Third, the equipment is expensive to own over its full life, and decisions about maintaining, upgrading, and replacing it involve substantial costs and long time horizons, so that lifecycle economics, the full cost of ownership over the asset's life, is a crucial consideration in managing its integrity [6].

These developments mean that the integrity of modern protection and control equipment depends not on reliability alone but on reliability, cybersecurity, human factors, and lifecycle economics together, and that managing it well requires considering all four. Yet these dimensions have traditionally been addressed separately, by different specialists using different methods, with reliability engineers focused on equipment condition, security specialists on cyber threats, human-factors experts on operator error, and asset managers on economics, and this fragmentation means that no single view captures the integrity of an asset in the round [7]. An asset might be judged sound on reliability grounds while carrying serious cybersecurity exposure, or economically due for replacement while remaining reliable, and considering each dimension in isolation risks missing the overall integrity picture and misdirecting resources.

The central argument of this paper is that managing the integrity of protection and control assets well requires a multi-criteria, risk-informed framework that deliberately bridges these four dimensions, integrating them into a single view that reflects both the condition of an asset across all four and the risk that its failure would pose. Such a framework would allow assets to be assessed and prioritized on the basis of their integrity in the round, surfacing risks that any single dimension would miss and directing maintenance, replacement, and investment where they are most needed. The gap this paper addresses is that while each dimension has been studied, an integrated framework that brings them together in a risk-informed way specifically for protection and control asset integrity is needed, and developing such a framework is the aim of the study.

Accordingly, the paper pursues several objectives. The first is to establish the four dimensions relevant to the integrity of modern protection and control equipment and the limitations of considering them separately. The second is to develop a multi-criteria, risk-informed framework that integrates the four dimensions into a single integrity index. The third is to demonstrate, through analysis, how integrating the dimensions changes asset prioritization compared with reliability-only approaches. The fourth is to consider the practical challenges of applying the framework. The remainder of the paper reviews the relevant literature, describes the analytical approach, sets out the framework and its aggregation, presents the analysis of how integration changes prioritization with supporting figures, discusses the implications and challenges, and concludes.

2. LITERATURE REVIEW

The literature relevant to this study spans asset integrity and reliability management for power system equipment, the cybersecurity of protection and control systems, human factors in their operation, lifecycle economics and asset management, and the multi-criteria decision methods that can integrate these dimensions.

The foundational literature concerns asset integrity and reliability management for power system protection and control. It documents the critical role of protection and control equipment in power system reliability and the traditional focus on managing the integrity of this equipment through condition assessment, testing, and maintenance aimed at ensuring correct

operation [1]. This literature establishes the reliability-centered approaches that have dominated the field, including condition-based and risk-based maintenance, which prioritize maintenance according to equipment condition and the consequence of failure, and it emphasizes the importance of the equipment functioning correctly when called upon [3]. A recurring theme is the shift from time-based to condition-based and risk-based approaches, reflecting a growing sophistication in how reliability is managed, though the focus remains largely on the reliability dimension.

The literature on cybersecurity of protection and control systems forms a second and increasingly prominent strand. It documents the transformation of protection and control equipment into digital, networked systems and the consequent emergence of cybersecurity as a critical concern, since these systems can now be targeted by cyber threats that could disrupt their operation with serious consequences for the power system [4]. This literature establishes cybersecurity as an essential dimension of the integrity of modern protection and control equipment, distinct from traditional reliability, and it describes the growing attention to securing critical infrastructure against cyber threats, while noting that cybersecurity has often been addressed separately from reliability-focused asset management [7].

The third strand concerns human factors in the operation and maintenance of protection and control systems. This literature recognizes that the correct functioning of protection and control depends not only on the equipment but on the people who configure, test, operate, and maintain it, and that human error is a significant contributor to protection and control problems [5]. It establishes human factors as a genuine dimension of integrity, since errors in setting, testing, or operating the equipment can compromise its correct functioning regardless of the equipment's own condition, and it argues that managing integrity well requires attention to the human element alongside the technical, an element that reliability-focused approaches have often underweighted.

The fourth strand concerns lifecycle economics and asset management for power system equipment. This literature frames the management of assets in terms of their whole-life cost and value, considering not only the immediate condition of equipment but the full economics of owning, maintaining, upgrading, and replacing it over its life, and it establishes lifecycle economics as central to sound asset management decisions [6]. It connects asset management to the balancing of cost and risk over time, arguing that decisions about maintenance and replacement should consider the economic dimension alongside the technical, and it reflects the broader development of asset management as a discipline that integrates condition, risk, and cost.

The fifth strand concerns the multi-criteria decision methods needed to integrate these dimensions. This literature documents methods for making decisions that involve multiple, sometimes conflicting criteria, allowing diverse dimensions to be weighted and combined into an integrated assessment that supports prioritization [8]. It establishes multi-criteria decision analysis as a suitable approach for problems where several distinct considerations must be balanced, and it has been applied to asset management and maintenance prioritization, providing the methodological basis for integrating reliability, cybersecurity, human factors, and lifecycle economics into a single framework. Reviews of asset management increasingly advocate integrated, risk-informed, multi-dimensional approaches, arguing that managing the integrity of critical assets well requires bringing together the several dimensions that bear on it rather than treating them in isolation, while noting the challenges of data, weighting, and integration [9]. The present study contributes to this direction, developing a multi-criteria, risk-informed framework that integrates the four dimensions for protection and control asset integrity.

3. METHODOLOGY

3.1. Research Approach

This study adopts a conceptual and analytical approach, drawing on the relevant literature to develop a multi-criteria, risk-informed asset integrity framework for protection and control equipment and to analyze how integrating the four dimensions affects asset prioritization. This approach is appropriate because the study's aim is to develop and demonstrate a framework that integrates several dimensions into a coherent decision-support tool, which is a task of framework construction and analysis rather than of primary data collection [9]. The approach allows the study to build on the established knowledge across the relevant fields, reliability,

cybersecurity, human factors, lifecycle economics, and multi-criteria decision analysis, while contributing the integrated framework that the fragmented state of that knowledge lacks.

3.2. The Four Integrity Dimensions

The framework rests on four dimensions established as relevant to the integrity of modern protection and control equipment. Reliability captures the condition of the equipment and its likelihood of functioning correctly, the traditional focus of integrity management [3]. Cybersecurity captures the exposure of the networked, digital equipment to cyber threats that could compromise its operation [4]. Human factors captures the vulnerability of the equipment's correct functioning to human error in its configuration, testing, operation, and maintenance [5]. Lifecycle economics captures the whole-life cost and economic position of the asset, including the costs of maintaining, upgrading, and replacing it [6]. Each dimension is assessed for an asset, and the framework integrates the four into a single view of the asset's integrity.

3.3. Risk-Informed Scoring

The framework is risk-informed, meaning that it considers not only the condition of an asset across the dimensions but the risk that its failure would pose, combining the likelihood of a problem with the consequence of that problem for the power system [1]. Risk in this sense can be represented as the product of a likelihood and a consequence,

R = L \times C

where R is the risk, L the likelihood of failure or compromise, and C the consequence of that failure for the power system. This risk-informed orientation ensures that the framework prioritizes not merely assets in poor condition but assets whose poor condition, across any of the dimensions, would pose the greatest risk, so that a highly critical asset with a moderate problem may warrant more attention than a less critical asset with a severe problem. The consequence term reflects the criticality of the asset within the power system, capturing the importance of its correct functioning.

3.4. Multi-Criteria Aggregation

The framework aggregates the four dimensions into a single integrated integrity index using a multi-criteria approach, in which each dimension is scored, weighted according to its importance, and combined [8]. The integrated integrity index for an asset can be expressed as a weighted combination of its risk-informed scores across the four dimensions,

$$I = \sum_{k=1}^{4} w_k , r_k$$

where I is the integrated integrity index, r_k is the risk-informed score for dimension k (reliability, cybersecurity, human factors, and lifecycle economics), w_k is the weight assigned to that dimension reflecting its relative importance, and the weights sum to one. This aggregation produces a single index that reflects an asset's integrity across all four dimensions in a risk-informed way, allowing assets to be assessed and prioritized on an integrated basis rather than on any single dimension. The weighting allows the relative importance of the dimensions to be reflected and adjusted according to the priorities and context of the organization applying the framework.

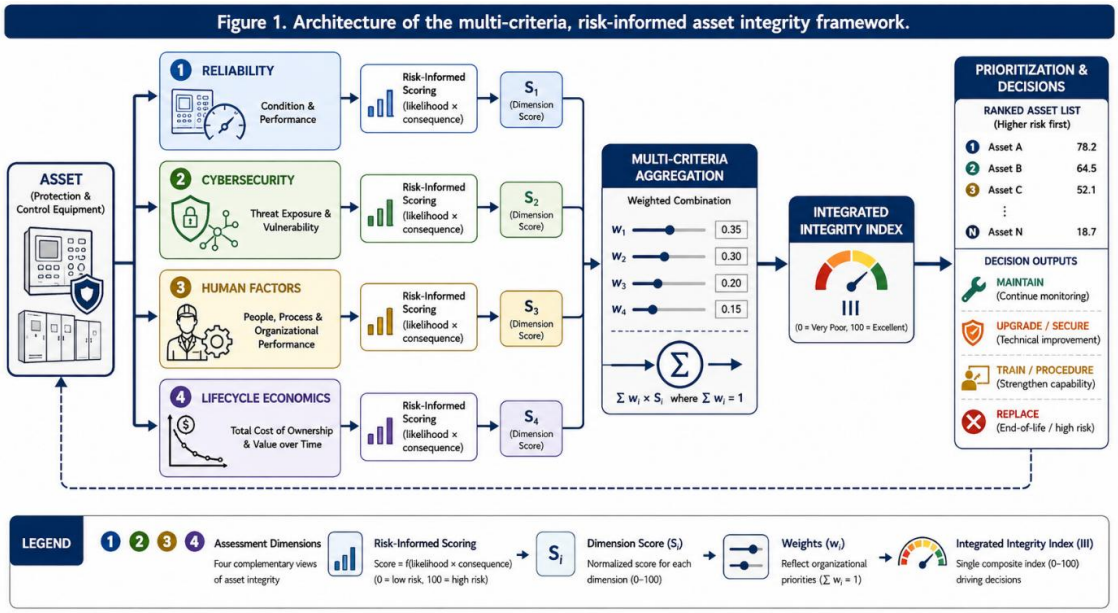

Figure 1. Architecture of the multi-criteria, risk-informed asset integrity framework

4. FRAMEWORK STRUCTURE AND CRITERIA

4.1 The Logic of Integration

The framework's central logic is that the integrity of a modern protection and control asset is a function of all four dimensions, so that assessing any one in isolation gives an incomplete and potentially misleading picture, whereas integrating them gives a complete one. The logic runs as follows. An asset's ability to fulfill its protective function correctly when needed depends on its being in good condition (reliability), secure against cyber compromise (cybersecurity), correctly configured and operated by people (human factors), and economically sound to retain (lifecycle economics), and a serious deficiency in any dimension threatens its integrity [7]. Because the dimensions are distinct and a deficiency in one may not be visible in another, only by assessing all four and integrating them can the true integrity and risk of an asset be understood. The framework therefore assesses each dimension, scores it in a risk-informed way, and aggregates the scores into an integrated index that captures the asset's integrity in the round, which is then used to prioritize decisions.

4.2 The Reliability Dimension

The reliability dimension assesses the condition of the equipment and its likelihood of functioning correctly, drawing on the established methods of condition and reliability assessment [3]. It considers factors such as the age and condition of the equipment, its maintenance and failure history, and indicators of its likely future performance, producing a score reflecting the risk that the equipment will fail to operate correctly. This dimension is the traditional focus of integrity management and remains essential, capturing the fundamental question of whether the equipment itself is in a condition to perform its function, but in the integrated framework it is one of four dimensions rather than the whole of the assessment.

4.3 The Cybersecurity Dimension

The cybersecurity dimension assesses the exposure of the digital, networked equipment to cyber threats that could compromise its operation [4]. It considers factors such as the equipment's connectivity and exposure, the security measures protecting it, and its vulnerability to known threats, producing a score reflecting the risk that the equipment could be compromised through cyber means. This dimension is essential for modern equipment precisely because it captures a risk entirely absent from traditional reliability assessment, since a relay in

perfect physical condition may nonetheless be highly vulnerable to cyber compromise, and its inclusion is one of the key ways the integrated framework surfaces risks that reliability-only approaches miss.

4.4 The Human Factors Dimension

The human factors dimension assesses the vulnerability of the equipment's correct functioning to human error in its configuration, testing, operation, and maintenance [5]. It considers factors such as the complexity of the equipment and its settings, the potential for and history of human error, and the procedures and training that guard against it, producing a score reflecting the risk that human error could compromise the equipment's correct functioning. This dimension recognizes that even sound, secure equipment can fail to protect correctly if it is misconfigured or mishandled by people, and its inclusion ensures that the framework accounts for the human element that reliability-focused approaches have often underweighted.

4.5 The Lifecycle Economics Dimension

The lifecycle economics dimension assesses the whole-life cost and economic position of the asset, considering the costs of maintaining, upgrading, and replacing it over its life [6]. It considers factors such as the ongoing cost of keeping the asset in service, its remaining economic life, and the economics of replacement or upgrade, producing a score reflecting the economic dimension of decisions about the asset. This dimension recognizes that integrity management is not only a technical but an economic matter, since decisions about maintaining, upgrading, or replacing equipment involve substantial costs and trade-offs, and its inclusion ensures that the framework supports decisions that are economically as well as technically sound.

5. ANALYSIS

5.1 How Integration Changes Asset Prioritization

The central analytical demonstration of the framework is that integrating the four dimensions changes asset prioritization compared with reliability-only approaches, surfacing risks that the conventional single-dimension view misses. Table 1 illustrates how a set of assets might be scored across the four dimensions and how their integrated ranking differs from their reliability-only ranking.

Table 1. Illustrative asset scores across dimensions and resulting rankings (higher score = higher risk/priority).

Asset	Reliability	Cybersecurity	Human factors	Lifecycle econ.	Integrated index	Reliability-only rank	Integrated rank
A	0.72	0.31	0.40	0.55	0.53	1	3
B	0.38	0.88	0.52	0.44	0.57	4	2
C	0.41	0.35	0.81	0.39	0.50	3	4
D	0.55	0.79	0.62	0.71	0.67	2	1

The illustration makes the framework's value concrete. Under a reliability-only view, asset A ranks highest priority because its reliability score is worst, and asset B ranks low because its reliability is good. But once the other dimensions are included, the picture changes: asset B, though reliable, carries a very high cybersecurity risk that makes it a serious concern the reliability-only view entirely missed, and it rises to second priority. Asset D, moderate on reliability, rises to top priority once its high cybersecurity, human-factors, and economic risks are combined. Asset A, meanwhile, falls in priority because its risks, though real on reliability, are lower across the other dimensions. This reordering demonstrates that the integrated framework directs attention differently, and more completely, than the reliability-only approach, surfacing high-risk assets that conventional assessment would overlook.

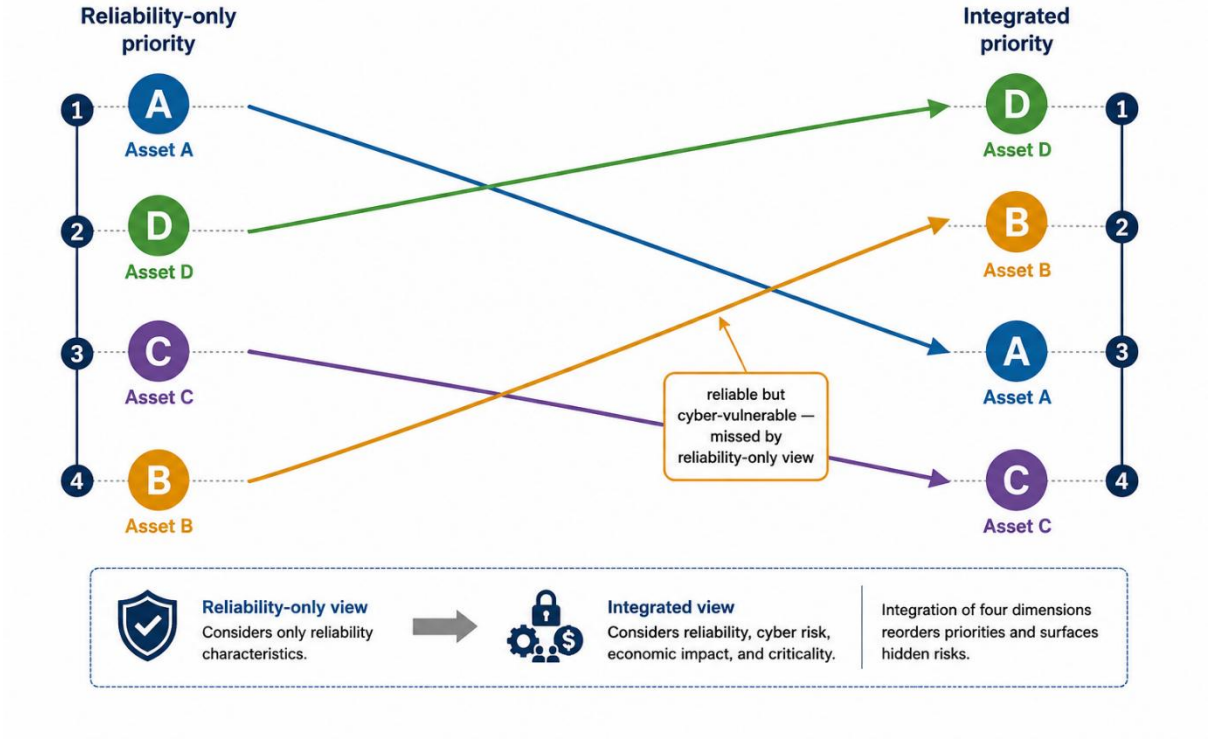

Figure 2. Reliability-only versus integrated asset prioritization.

5.2 The Contribution of Each Dimension

The analysis shows that each of the four dimensions contributes distinct information to the integrated assessment, capturing risks that the others do not, which is why integrating them yields a more complete picture than any single dimension. Table 2 summarizes the distinct contribution of each dimension and the risk it captures that the others miss.

Table 2. Distinct contribution of each integrity dimension.

Dimension	Risk it captures	Missed if omitted
Reliability	Equipment failing to operate	Physical/condition-based failure
Cybersecurity	Cyber compromise of operation	Attack on sound equipment
Human factors	Error in configuration/operation	Mishandling of sound, secure equipment
Lifecycle economics	Uneconomic retention	Cost-inefficient asset decisions

The table underscores why all four dimensions are needed. Each captures a genuinely distinct way in which an asset's integrity or the soundness of decisions about it can be compromised, and omitting any one leaves a blind spot: omit cybersecurity and cyber-vulnerable assets go unnoticed; omit human factors and error-prone configurations are missed; omit lifecycle economics and technically sound but uneconomic assets are retained wastefully. Because the dimensions are complementary rather than overlapping, integrating them provides coverage that no single dimension can, which is the fundamental rationale for the multi-criteria approach and the source of its advantage over reliability-only assessment.

5.3 The Effect of Weighting

The analysis also examines how the weighting of the dimensions affects the integrated assessment, since the weights reflect the relative importance assigned to each dimension and can be adjusted according to context and priorities. Table 3 illustrates how different weighting emphases shift the integrated priority of assets.

Table 3. Effect of weighting emphasis on integrated asset priority (illustrative top-priority asset).

Weighting emphasis	Emphasized dimension(s)	Resulting top-priority asset

Balanced	All equal	D
Reliability-focused	Reliability	A
Security-focused	Cybersecurity	B
Economics-focused	Lifecycle economics	D

The illustration shows that the weighting matters and that the framework accommodates different priorities. Under balanced weighting, asset D ranks top; under a security-focused weighting reflecting heightened concern about cyber threats, asset B, the most cyber-vulnerable, rises to top; under a reliability-focused weighting, asset A returns to top. This flexibility is a feature rather than a weakness, since it allows an organization to reflect its own priorities, risk appetite, and context in the assessment, emphasizing the dimensions it judges most important. It does, however, mean that the weighting must be chosen thoughtfully and transparently, since it influences the results, and the analysis highlights the importance of setting the weights in a considered, justifiable way rather than arbitrarily.

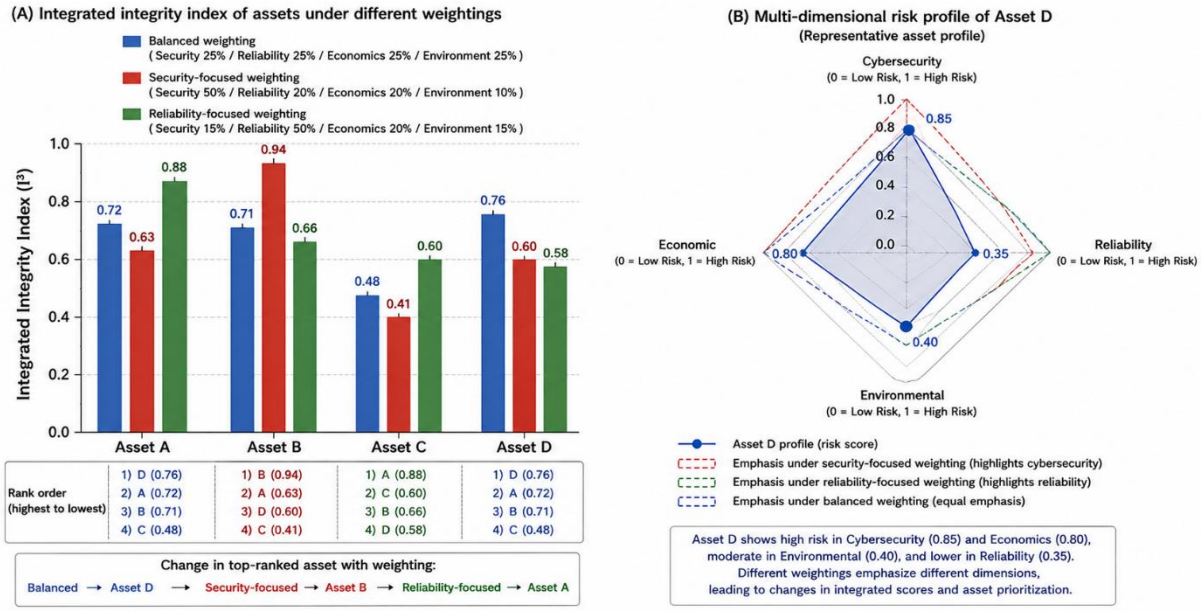

Figure 3. Sensitivity of asset prioritization to dimension weighting.

5.4 From Assessment to Decision

The analysis emphasizes that the framework's ultimate purpose is to support better decisions about protection and control assets, translating the integrated integrity assessment into prioritized action. The integrated index identifies which assets pose the greatest overall risk and therefore warrant the most attention, and the profile of an asset across the dimensions indicates what kind of action is needed: an asset high on cybersecurity risk needs security measures, one high on human-factors risk needs improved procedures or training, one high on reliability risk needs maintenance, and one high on lifecycle-economics risk may warrant replacement. The framework thus supports not only prioritization but the targeting of the appropriate response to the specific nature of each asset's risk, allowing maintenance, upgrade, security, training, and replacement decisions to be directed where they will most improve integrity. This linkage from integrated assessment to targeted decision is where the framework delivers its practical value, ensuring that limited resources are directed to the assets and the actions that most reduce risk.

6. DISCUSSION

The analysis presented here supports the study's central argument that managing the integrity of modern protection and control assets well requires a multi-criteria, risk-informed framework that bridges reliability, cybersecurity, human factors, and lifecycle economics, rather than treating these dimensions in isolation. This argument rests on the recognition that the integrity of modern protection and control equipment depends on all four dimensions, and that considering any one alone gives an incomplete and potentially misleading picture, whereas

integrating them gives a complete and more defensible basis for decisions.

The most important finding, demonstrated concretely in the analysis, is that integrating the four dimensions changes asset prioritization, surfacing high-risk assets that a reliability-only view misses. The illustration of an asset that ranks low on reliability but high on cybersecurity, and that rises sharply in priority once the integrated view is taken, captures the essential value of the framework: it reveals risks that the conventional single-dimension approach cannot see, and it directs attention and resources accordingly. This is significant because misdirected attention is costly in a domain where the consequences of asset failure can be severe, and because the reliability-only approach, though well established, is increasingly inadequate to equipment whose most serious vulnerabilities may lie outside the reliability dimension entirely. The framework's ability to surface these hidden risks is its principal contribution.

The finding that each dimension contributes distinct information reinforces the rationale for integration. Because reliability, cybersecurity, human factors, and lifecycle economics each capture a genuinely different way in which integrity or sound decision-making can be compromised, and because these are complementary rather than overlapping, integrating them provides coverage that no single dimension can. This means the framework is not merely adding detail to reliability assessment but bringing in whole categories of risk, cyber, human, and economic, that reliability assessment omits, which is why the integrated view can differ so substantially from the reliability-only view. The completeness of the coverage is what makes the integrated assessment more defensible and more useful.

The examination of weighting highlights both a strength and a responsibility. The framework's accommodation of different weightings allows it to reflect an organization's own priorities, risk appetite, and context, which is valuable because different organizations and circumstances legitimately weigh the dimensions differently, and because priorities shift, as when heightened cyber threats warrant greater emphasis on security. But this flexibility also means that the weighting must be chosen thoughtfully and transparently, since it influences the results, and the framework's outputs are only as sound as the judgments embedded in its weights. This places a responsibility on those applying the framework to set the weights in a considered, justifiable, and transparent way, and it is a genuine consideration in applying the approach rather than a mere technicality.

The framework's linkage from integrated assessment to targeted decision is where its practical value is realized. By identifying not only which assets pose the greatest overall risk but what kind of risk each poses, the framework supports the targeting of the appropriate response, security measures, procedures, maintenance, or replacement, to the specific nature of each asset's vulnerability. This ensures that the framework improves not just prioritization but the effectiveness of the actions taken, directing limited resources to the assets and interventions that most reduce risk. In a domain where resources are always constrained and the assets are critical, this targeted, risk-informed direction of effort is a substantial practical benefit.

Several practical challenges must nonetheless be acknowledged honestly. The most fundamental is data: the framework requires information to score each asset across four dimensions, and obtaining reliable, comparable data across such diverse dimensions, condition, cyber exposure, human-factors vulnerability, and economics, is genuinely difficult, since these are assessed in different ways by different specialists and may not be readily available or comparable. The challenge of scoring and normalizing the dimensions so that they can be meaningfully combined is real, since the dimensions are measured differently and must be brought to a common basis, which involves judgment. The setting of weights, as discussed, requires careful, transparent judgment and affects the results. And there is an organizational challenge, because the dimensions have traditionally been the province of different specialists and functions, so applying an integrated framework requires bringing these together and overcoming the fragmentation that the framework is designed to remedy, which is as much an organizational as a technical undertaking. Finally, the framework, like any decision-support tool, informs rather than replaces expert judgment, and its outputs must be interpreted by those with the expertise to apply them wisely.

These challenges define directions for realizing the value and for further work. Developing methods and data sources for scoring the dimensions reliably and comparably, and for normalizing and combining them soundly, would strengthen the framework's application. Establishing considered, transparent approaches to weighting would improve the defensibility of its outputs. Fostering the organizational integration of the reliability, security, human-factors, and asset-management functions would enable the framework to be applied as intended. And

validating the framework through application to real asset populations would confirm its practical value and refine it. The framework developed here provides a foundation and an agenda for such work.

7. CONCLUSION

This paper proposed a multi-criteria, risk-informed asset integrity framework for power system protection and control equipment that deliberately bridges reliability, cybersecurity, human factors, and lifecycle economics, integrating these four dimensions into a single, risk-informed integrity index to support asset prioritization and decisions. Motivated by the recognition that modern protection and control equipment is digital, networked, operated by people, and economically significant, so that its integrity depends on all four dimensions rather than reliability alone, the framework assesses each dimension in a risk-informed way, weights and aggregates them into an integrated index, and uses that index to prioritize maintenance, security, training, and replacement decisions. The analysis demonstrated that integrating the four dimensions changes asset prioritization compared with reliability-only approaches, surfacing high-risk assets, such as reliable but cyber-vulnerable equipment, that the conventional single-dimension view misses entirely, and it showed that each dimension contributes distinct, complementary information, that the weighting of the dimensions shapes the assessment and must be set thoughtfully, and that the framework supports the targeting of appropriate responses to the specific nature of each asset's risk.

The central contribution of this work is to bring together, in a single risk-informed framework, the four dimensions that bear on the integrity of modern protection and control assets but that have traditionally been managed in isolation, and to demonstrate that integrating them provides a completer and more defensible basis for managing that integrity than any single dimension allows. This matter because protection and control equipment is critical to the reliability and security of the power system, because its integrity now depends on dimensions well beyond traditional reliability, and because managing it dimension by dimension risks missing the serious risks that only an integrated view reveals. The study is candid that applying the framework faces real challenges of data, scoring, weighting, and organizational integration, and it identifies these as the priorities for realizing its value and for further work. With attention to these challenges and validation on real asset populations, the multi-criteria, risk-informed framework proposed here offers power system operators a more complete, defensible, and practically useful basis for safeguarding the integrity of the protection and control equipment on which the security of the grid ultimately depends.

References

1. Pawan Kumar Singh, Scaling Gate-All-Around (GAA) Transistor Architectures for Sub-2nm AI Accelerators Using Atomically Thin 2D Materials, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5713
2. Pawan Kumar Singh, Energy-Efficient Task Scheduling in Green Cloud Computing Using Neuromorphic Spiking Neural Networks, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5712
3. Rangavinay Teja Royal Jagga, 2026, DOI: 10.1109/GCWCN66157.2025.11448495, Date of Conference: 22-23 November 2025,Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448495
4. Rangavinay Teja Royal Jagga , 2026, Subtle Data Contamination in Visual AI: Covert Model Backdoors via Resampling Exploits, Date of Conference: 22-23 November 2025, Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448514
5. Rangavinay Teja Royal Jagga, 2026, Robotic Tactile-Vision Integration for Interactive Object Disentanglement, https://ieeexplore.ieee.org/document/11448337
6. Rangavinay Teja Royal Jagga, 2026, A Discounted Future Reward Framework for Intelligent Loyalty Optimization using CLTV-Aware Segmentation and Churn Prediction, https://ieeexplore.ieee.org/document/11497560
7. Anjaneyulu Gudla; Manish Kumar; Vamshi Jeksani; Kiran Kumar Reddy; Gayathri Band, Harnessing

Artificial Intelligence Cybersecurity: Cutting Edge Collaboration of SAP AWS to Safeguard Life Science Data. 2026 https://doi.org/10.1109/aiei69164.2026.11497833
8. G. Mahender, Department of CSE(Data Science), Vardhaman College of Engineering ; Vamshi Jeksani; Manish Kumar; Koppuravuri Sri Lakshmi Sruthi; Kiran Kumar Reddy, SAP Cloud System on AWS for Risk Detection and Integration Artificial Intelligence Scalable Cybersecurity 2026 https://doi.org/10.1109/aiei69164.2026.11497435
9. Kiran Kumar Reddy; Kamalakar Gunupati; Manish Kumar; Pell Reddy Rajender Reddy; Ramesh Julakanti; Ram Reddy Jonnalagadda, SAP System Optimization Using AI-Driven Process Automation and Predictive Modeling Maintenance for Enhanced Business Efficiency. 2025 https://doi.org/10.1109/computingcon64838.2025.11376613
10. A. Mahendra Vardhan and S. Sridhar, "Determining False Positive Analysis of Software Vulnerabilities with Predefined Scan Rules using Random Forest Classifier and Decision Tree Technique," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 622-625, DOI: https://doi.org/10.1109/ICAC3N56670.2022.10074458
11. Amilineni, M.V. 2025. Audit-Safe Agentic RAG Framework for Regulated Enterprise Systems: A Trustworthy AI Architecture for SAP, Finance, Healthcare, and Government Workflows. INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES. (Jan. 2025), 34–46. DOI: https://doi.org/10.29284/7fjzk883
12. Pawan Kumar Singh, ACCELERATING LARGE LANGUAGE MODEL TRAINING USING HYBRID QUANTUM-CLASSICAL VARIATIONAL AUTOENCODERS WITH INTEGRATED PHOTONIC QRAM, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/501, DOI: https://doi.org/10.46121/pspc.54.3.45
13. Pawan Kumar Singh , RESILIENCE ASSESSMENT OF MODERN POWER GRID INFRASTRUCTURE AGAINST EXTREME WEATHER USING PHYSICS-INFORMED NEURAL NETWORKS, Vol. 54 No. 1 (2026): January-March 2026, Power System Protection and Control, ISSN-1674-3415,https://pspac.info/index.php/dlbh/article/view/502, DOI: https://doi.org/10.46121/pspc.54.1.64
14. Pawan Kumar Singh, MITIGATING THE EXABYTE STORAGE CRISIS: ENHANCING READ/WRITE EFFICIENCY IN 5D OPTICAL GLASS STORAGE USING SILVER NANOPARTICLE DOPING, Vol. 38 No. 11s (2025), International Journal of Applied Mathematics (IJAM) , pISSN 1311-1728, eISSN 1314-8060 ,https://ijamjournal.org/ijam/publication/index.php/ijam/article/view/2153
15. Mr. Pawan Kumar Singh (Author), Miss. Pari Nidhi Singh (Author) ,Intelligent Bot, ASIN : B0DBGCQY8X,Publisher : Namya Press, Publication date : November 25, 2022,Language : English, Print length : 105 pages,ISBN-10 : 9390124867,ISBN-13 : 978-9390124862,Item Weight : 7.5 ounces, Dimensions : 6.24 x 0.43 x 9.24 inches,https://www.amazon.com/Intelligent-Bot-Pawan-Kumar-Singh/dp/B0DBGCQY8X/ref=sr_1_5?crid=2VAXN5BRN5SMS&dib=eyJ2IjoiMSJ9.v3OCQvHBpy20RIjfMWh0qbOl-RLOlUJIC8Xa0Pjeqilvo2sbZ_suN3LbSCw_OA_ZD_4lgjRLMGlBwZQQ1ehZEfDpt_MJiOUfVuqqzMav0I5_mb6pN5DQog0U7SA826n1DQQ3QAtWwopHy4lC5IfhZXttKj9faiyATwhdtDATSSV1-r7FmzM2VQyIA0jxcfq6E6hp9ECfH1fby0li9kUfGpLxMq4GktlzUIJO5ggrhsQ.G1AjQiVqU4HFsnSczvz-X6NXCNs3EFSn-RI8mcWWGOc&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book&qid=1787815741&sprefix=pawan+kumar+singh%2C+bo%2Caps%2C450&sr=8-5
16. Mr. Pawan Kumar Singh (Author), STORAGE CRISES DUE TO RISE OF AI: A Comprehensive Guide to Managing the Storage Challenges in the Age of Artificial Intelligence, ASIN : B0HFK12ZCT Publisher : EB1 Profile, Accessibility : Learn more, Publication date : August 17, 2026,Edition : 1st Language : English, File size : 1.7 MB, Screen Reader : Supported, Enhanced typesetting : Enabled X-Ray : Not Enabled, Word Wise : Not Enabled ,Print length : 261 pages ,ISBN-13 : 979-8951479112,Page Flip : Enabled, https://www.amazon.com/STORAGE-CRISES-DUE-RISE-Comprehensive-ebook/dp/B0HFK12ZCT/ref=sr_1_1?crid=9MF6C4WDVJR5&dib=eyJ2IjoiMSJ9.DQ8fesBch7ELmRnilDt-YA.NBSCHLmetvnbhkxwIpOoj3s0IVsCV8y6-ZCfCP6Ul1c&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book%2C+eb1+Profile&qid=1787816040&sprefix=pawan+kumar+singh%2C+book%2C+eb1+profile%2Caps%2C420&sr=8-1
17. Parag Bharatkumar Parikh, FRAMEWORKS FOR MITIGATING SUPPLY CHAIN DISRUPTIONS AND MATERIAL PRICE VOLATILITY IN SUSTAINABLE BUILDING CONSTRUCTION, Vol. 53 No. 2 (2025): April-June 2025 , , Power System Protection and Control, ISSN-1674-3415,

https://pspac.info/index.php/dlbh/article/view/447, DOI: https://doi.org/10.46121/pspc.53.2.34
18. Parag Bharatkumar Parikh, IMPLEMENTING DIGITAL INSPECTION PROTOCOLS FOR ENHANCED QUALITY CONTROL MANAGEMENT IN HIGH-RISE CONSTRUCTION, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/439, DOI: https://doi.org/10.46121/pspc.54.3.12
19. Parag Bharatkumar Parikh , EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/issue/view/30, DOI: https://doi.org/10.46121/pspc.54.1.61
20. Parag Bharatkumar Parikh, EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Vol. 54 No. 1 (2026): January-March 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/440, DOI: https://doi.org/10.46121/pspc.54.1.61
21. Ronakkumar shah, REDEFINING BUSINESS PROCESS MANAGEMENT: THE SYNERGY OF AI AND INTELLIGENT AUTOMATION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/448, DOI: https://doi.org/10.46121/pspc.54.3.14
22. Ronakkumar shah, OPERATIONAL ACCOUNTABILITY IN ACTION: METRICS AND MECHANISMS FOR SYSTEMIC SUCCESS, Vol. 53 No. 4 (2025): October-December 2025, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/452, DOI: https://doi.org/10.46121/pspc.53.4.40
23. Ronakkumar shah, BEYOND THE BLUEPRINT: AUTOMATED WORKFLOW ENFORCEMENT AND POLICY GOVERNANCE, Vol. 53 No. 2 (2025): April-June 2025 , System Protection and Control, ISSN-1674-3415 ,https://pspac.info/index.php/dlbh/article/view/451, DOI: https://doi.org/10.46121/pspc.53.2.35
24. Ronakkumar shah , Cognitive Process Intelligence: Integrating Generative AI and Automated Workflow Discovery, Vol. 33 No. 08 (2024): JOCAAA, Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5676
25. Ronakkumar shah, research Trends in Smart Workflow Automation: A Bibliometric Analysis of Emerging Themes, Home / Archives / Vol. 33 No. 05 (2024): JOCAAA, Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5675
26. Tushita Agarwal; Swaminathan Sethuraman, Mapping Customer Behavior: Visual Analysis of Online Retail Interactions, DOI: https://doi.org/10.1109/IC2NC67409.2025.11376261
27. Tushita Agarwal, Efficient Data Summarization and Comparison via Grid-Based Statistical Proxies for Large-Scale Datasets, DOI: https://doi.org/10.1109/ICBATS66542.2025.11258564
28. Dip Bharatbhai Pate, Dynamic vs. Static visualizations: Understanding their use cases in big data analysis, International Journal of Science and Research Archive, 2022, 05(02), 392-395., DOI https://doi.org/10.30574/ijsra.2022.5.2.0077
29. Dip Bharatbhai Patel, Building scalable business intelligence systems in the cloud: A technical approach, International Journal of Science and Research Archive, 2021, 02(01), 212-215., Received on 03 February 2021; revised on 17 April 2021; accepted on 19 April 2021,DOI: https://doi.org/10.30574/ijsra.2021.2.1.0047
30. Dip Bharatbhai Patel, Understanding the Impact of Text Analytics on Social Media Sentiment Analysis, Vol. 5 No. 5 (2019) ,September-October, DOI: https://doi.org/10.32628/CSEIT1936413
31. Dip Bharatbhai Patel, Real-Time Data Streaming in BI Dashboards: Opportunities and Challenges, Archives / Vol. 5 No. 4 (2019) : July-August, DOI: https://doi.org/10.32628/CSEIT192142
32. Dip Bharatbhai Patel, the Role of Data Visualization in Modern Intelligence, Archives / Vol. 2 No. 2 / Research Article, DOI: https://doi.org/10.32996/jcsts.2020.2.2.4
33. Dip Bharatbhai Patel, University of North America, Virginia, USA, Home / Archives / Vol. 5 No. 02 (2025): Volume 05 Issue 02 / Articles, https://www.academicpublishers.org/journals/index.php/ijdsml/article/view/5958
34. Sai Akshara Vemuri , KINEMATIC OPTIMISATION OF SOFT ROBOTIC MANIPULATORS FOR MEDICAL INTERVENTION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/450
35. Sai Akshara Vemuri, https://www.periodicos.ulbra.org/index.php/acta/article/view/528
36. A. Srivastava, "Securing PHI in cloud-based healthcare systems: Challenges, frameworks, and future

directions," J. Comput. Anal. Appl., vol. 33, no. 2, Aug. 2024. [Online]. Available: https://www.eudoxuspress.com/index.php/pub/article/view/4349/3190
37. A. Srivastava, "AI-assisted cloud migration of healthcare claims data from legacy systems: A metadata-driven framework," Int. J. Commun. Networks Inf. Secur., vol. 14, no. 3, Nov. 2022. [Online]. Available: https://ijcnis.org/index.php/ijcnis/article/view/8682
38. A. Srivastava, "Enhancing provider and claims data accuracy using artificial intelligence on cloud-native data platforms," J. Comput. Anal. Appl., vol. 31, no. 4, Nov. 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4347/3189
39. A. Srivastava, "A unified framework for secure cloud data management: Integrating governance, metadata intelligence, and privacy controls," J. Inf. Syst. Eng. Manage., vol. 9, no. 2, Apr. 2024. [Online]. Available: https://www.jisem-journal.com/download/45_A_Unified_Framework.pdf
40. A. Srivastava, "Optimizing large-scale data migration for cloud-native architectures," J. Comput. Anal. Appl., vol. 31, no. 2, pp. 652–662, May 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4603
41. Aziz, A., Chandusha, K., Naga Kiran, B., Prasad, M. L. M., Golla, K., Rajeswari, S., & Katta, S. K. R. (2026). Exploring Machine Learning Applications for Genomic Data Analysis in Personalized Medicine. International Journal of Drug Delivery Technology, 16(38s), 1166-1173. https://doi.org/10.25258/ijddt.16.38s.127,https://www.periodicos.ulbra.org/index.php/acta/article/view/687
42. Abdul Aziz. “Intelligent Health Analytics: Mastering AI in Healthcare Data”. Acta Scientiae, vol. 25, no. 4, Aug. 2024, pp. 544-55, https://www.periodicos.ulbra.org/index.php/acta/article/view/687. https://doi.org/10.5281/zenodo.21699886
43. Mohammad Naffizuddin , Chaganti Ashok ,Sowjanya Gunukula , Rvbs Sarma , Bhavana Sujanamulk , Bharani Krishna Takkella , Chukka Ram Sunil ,Varri Sujana , Ashwini Kumar, Etiological Factors of Orofacial Clefts in a Hospital-Based Population: A Descriptive Analytical Study, Published: December 10, 2025,DOI: 10.7759/cureus.98868,DOI : https://doi.org/10.7759/cureus.98868
44. Event-Aware Multi-Layer Storage Risk Forecasting for Oracle Database Estates Using HAPF, Raghu Gollapudi, International Journal of Computational and Experimental Science and Engineering, 10(4), 2024 ,10.22399/ijcesen.5183
45. Backup Integrity and Recovery Readiness Assessment for High-Availability Databases
Raghu Gollapudi, Computer Fraud & Security, Vol. 2023, Issue 8, pp. 35-48, 10.52710/cfs.1031
46. Data-Driven Risk Scoring For Grid Assets Using Centralized Production Databases ,Raghu Gollapudi, International Journal of Advances in Signal and Image Sciences, 11(3s), 2025, pp. 50-87 ,10.29284/y6m4p915
47. Risk-Controlled Near-Zero-Downtime Oracle Database Migration Using GoldenGate
Raghu Gollapudi, International Journal of Computational and Experimental Science and Engineering, 8(3), 2022 ,10.22399/ijcesen.5382
48. An Automated Risk Scoring Framework for SQL Execution Plan Analysis and Performance Regression Detection in Oracle Database Systems, Raghu Gollapudi ,2026 International Conference on Multidisciplinary Innovations For Smart & Sustainable Future (MISSF), pp. 1-6 ,10.1109/MISSF68264.2026.11521893
49. An Optimization-Based Framework for Database-Level Fraud Detection in Real-Time Financial Systems, Raghu Gollapudi ,2026 IEEE 15th International Conference on Communication Systems and Network Technologies (CSNT), pp. 1304-1310 , 10.1109/CSNT69054.2026.11502505
50. Latency-Bound Online Consistency Verification for Always-on Financial Databases
Raghu Gollapudi, 2026 IEEE Madhya Pradesh Section Conference (MPCON), pp. 1597-1603
10.1109/MPCON69668.2026.11508277
51. AI-Driven Stability Classification of Database Workloads in Regulated Systems
Raghu Gollapudi,2026 IEEE 15th International Conference on Communication Systems and Network Technologies (CSNT), pp. 1005-1010,10.1109/CSNT69054.2026.11502278
52. SHIELD-DBOps: An Admissibility-and-Verification Framework for Guardrail-Based Database Operations , Raghu Gollapudi, Engineering, Technology & Applied Science Research, 16(4), 2026, pp. 37239-37244, 10.48084/etasr.19469
53. ARDA-GATE: Auditable Recovery Decision Architecture for Unsafe-Promotion Prevention in Hybrid Oracle Database Failover, Raghu Gollapudi, Journal of Intelligent Decision Making and Information Science, 3(5s), 2026, pp. 957-992, 10.59543/jidmis.v3.1229
54. Manoj Kumar Kagitha, Automated Security Compliance in Ci/Cd: A Natural Language Processing (NLP) Approach to Detecting Vulnerabilities in Infrastructure-As-Code (Terraform/Bicep),Publication year 2021, Volume 2021, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/970

55. Manoj Kumar Kagitha, Hybrid Quantum-Classical Resource Scheduling: A Proposed Architecture for Next-Generation Hyperscale Data Centers, Publication year 2024, Volume 2024, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/969
56. Manoj Kumar Kagitha, Self-Healing Cloud Infrastructure: A Hybrid Reinforcement Learning Framework for Predicting Microservice Failures in Azure Kubernetes Service (AKS),Publication year 2023, Volume 2023, Issue 12,https://computerfraudsecurity.com/index.php/journal/article/view/971
57. Manoj Kumar Kagitha, LOAD BALANCING TECHNIQUES IN DISTRIBUTED CLOUD ENVIRONMENTS, (IJESMR - 2017), D.O.I:10.53555/jcr.v6:i1.13380, https://jcreview.com/archives/volume-6/issue-1/13380
58. Manoj Kumar Kagitha, AI-DRIVEN OBSERVABILITY FOR HYPERSCALE COLOCATION DATA CENTERS: A CASE STUDY OF LOG ANALYTICS AND ANOMALY DETECTION PIPELINES, Archives / Vol. 27 No. 7 (2019): JOCAAA,https://www.eudoxuspress.com/index.php/pub/article/view/5053
59. Manoj Kumar Kagitha, GREENOPS IN THE CLOUD: AN AI-DRIVEN TELEMETRY ANALYSIS MODEL FOR REDUCING CARBON FOOTPRINT IN HIGH-AVAILABILITY CLUSTERS, Vol. 28 No. 6 (2020): JOCAAA, https://www.eudoxuspress.com/index.php/pub/article/view/5054
60. Narula, U. (2006). Communication models. Atlantic Publishers & Dist.
61. Padín Otero, R. (2017). La articulación de la moda en el espacio museístico en el cambio de milenio.Universidad de Vigo.
62. Pagani, G., & Stellato, F. (2020). El director de comunicación (Dircom)y su rol de guardián de marca. Proceso de Brand Guardian. Anuario De Investigación USAL, (7). https://p3.entendiste.ar/index.php/anuarioinvestigacion/article/view/5239
63. Pérez, L. (2021). La moda en el museo. El caso de la moda argentina. Cuaderno, 127, 107-117. Phillips, N (2022). Hablemos de las nuevas viejas zapatillas de Balenciaga. Vogue.es. https://acortar.link/YrzBZl
64. Pratt, M., Sarmiento, O. L., Montes, F., Ogilvie, D., Marcus, B. H., Perez, L. G., & Brownson, R. C. (2012). The implications of megatrends in information and communication technology and transportation for changes in global physical activity. The Lancet, 380(9838), 282-293. https://doi.org/10.1016/S0140-6736(12)60736-3
65. Puyuelo Cazorla, M. (2021). Exposiciones: comunicación, cultura y diseño. Todo sobre diseño. Una década de exposiciones de diseño en la Sala Hall, 11.
66. Freeman, M. & Rampazzo Gambarato, R. (2018). The Routledge Companion to transmedia studies. New York. https://doi-org.eur.idm.oclc.org/10.4324/9781351054904
67. Robledo Dioses, K., Atarama Rojas, T., & Palomino Moreno, H. (2017). De la comunicación multimedia a la comunicación transmedia: una revisión teórica sobre las actuales
68. narrativas periodísticas. Estudios sobre el Mensaje Periodístico, 23(1), 223-240. http://dx.doi.org/10.5209/ESMP.55593
69. Romeu, C. (2017). Los vínculos ocultos (o no) entre Demna Gvasalia y Cristóbal Balenciaga. Vein.es. https://acortar.link/pko09i
70. Sáez-Angulo, J. (2019) Balenciaga y la pintura española. Asmoda.com. https://acortar.link/xqP3SJ Steele, V. (1998). A museum of fashion is more than a clothes bag. Fashion Theory, 4(2), 327–335. https://doi.org/10.2752/136270498779476109
71. Steele, V. (2018). Fashion Theory. Hacia una transformación cultural de la moda. Editorial Ampersand.
72. Navarrete Hernández, T. (2019). Digital heritage tourism: innovations in museums. World Leisure Journal, 61, 200-214. https://doi.org/10.1080/16078055.2019.1639920
73. Villena Alarcón, E. (2014). La narrativa transmedia en el modelo de comunicación de las empresas de moda internacionales: un estudio de caso. Communication Papers, 3(4), 15-21. https://doi.org/10.33115/udg_bib/cp.v3i04.22122
74. Wallenberg, L. (2020). Art, life, and the fashion museum: for a more solidary exhibition practice.
75. Fashion and Textile, 7(17), 1-16. https://doi.org/10.1186/s40691-019-0201-5
76. Walls Ramírez, M. (2020). Aportes De La comunicación Para La difusión Del Patrimonio Cultural. Revista De Ciencias De La Comunicación E Información, 25(1), 49-55. https://doi.org/10.35742/rcci.2020.25(1).49-55.
77. We are Social & Meltwater (2023). Global Digital Report—the essential guide to the latest connected behav*iours.* http://bit.ly/3k43tRq