International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Governing Cyber Physical Systems Under Conditions of Complexity: A Framework for Integrated Oversight in Adaptive Governance Architectures

Dr. Robb Shawe

Departments of Cyber Leadership, Sustainability and Critical Infrastructure, Capitol Technology University, 11301 Springfield Road, Laurel, MD, USA

doi.org/10.51505/ijaemr.2026.11329 URL: http://dx.doi.org/10.51505/ijaemr.2026.11329

Received: May 23, 2026 Accepted: Jun 01, 2026 Online Published: Jun 10, 2026

Abstract

Cyber-physical systems (CPS) form the backbone of modern infrastructure, integrating computational intelligence with physical processes across energy, transportation, healthcare, manufacturing, and public services. These systems operate in dynamic, interconnected environments where disruptions propagate rapidly and unpredictably. Traditional governance models—designed for siloed, linear systems—are insufficient for managing the complexity, interdependence, and real-time operational demands of CPS. This manuscript introduces the Cyber-Physical Governance Framework (CPGF), a cross-sector governance architecture that integrates adaptive oversight, AI-enabled sensing, event-validated learning, and executive decision translation. The CPGF extends the Adaptive Governance Systems Framework (AGSF), the AI-Enabled Governance Oversight Model (AIGOM), the Governance Maturity Model (GMM), and the Event-Validated Governance (EVG) Framework by specifying governance mechanisms tailored to CPS environments. The model supports resilience, accountability, and real-time performance alignment across critical cyber-physical domains. The framework further establishes cyber-physical governance as a convergence architecture that integrates real-time operational intelligence, adaptive oversight, event-validated learning, executive synchronization, and resilience-oriented governance modernization across interconnected cyber-physical ecosystems operating amid complexity and rapid change.

Keywords: cyber-physical governance; CPS oversight; adaptive governance; real-time monitoring; socio-technical systems; resilience engineering; AI-enabled governance

1. Introduction

Cyber-physical systems (CPS) integrate computational intelligence with physical processes, enabling real-time sensing, automated control, and dynamic system adaptation. These systems underpin critical infrastructure, industrial automation, healthcare delivery, transportation networks, and public services (National Institute of Standards and Technology [NIST], 2024). Their complexity, interdependence, and speed of operation create governance challenges that exceed the capabilities of traditional oversight models.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

These conditions create governance convergence challenges in which operational intelligence, AI-enabled decision systems, cyber-physical observability, executive oversight, and resilience coordination must function as a synchronized governance architecture rather than as isolated oversight domains. As CPS environments become increasingly autonomous and interconnected, governance systems require integrated orchestration capabilities that operate continuously across dynamic cyber-physical ecosystems (Dekker, 2011; Endsley, 2017; Woods, 2018).

Governance systems must evolve to manage CPS environments characterized by:

- nonlinear system behavior
- rapid propagation of failures
- AI-enabled decision loops
- cross-domain interdependencies
- real-time operational demands

This manuscript introduces the **Cyber-Physical Governance Framework (CPGF)**, which extends AGSF (Shawe, 2026), AIGOM, GMM, EVG, and GTF to define governance mechanisms tailored to CPS environments.

1.1 Methodological Orientation

This manuscript employs a conceptual integrative methodology grounded in cyber-physical governance synthesis, adaptive governance orchestration theory, resilience-engineering analysis, interdisciplinary socio-technical framework integration, and operational convergence modeling (Jabareen, 2009; Torraco, 2005). The Cyber-Physical Governance Framework (CPGF) was developed through structured evaluation of cyber-physical governance architectures, AI-enabled operational intelligence systems, adaptive oversight models, resilience coordination frameworks, human-AI teaming structures, and executive governance synchronization mechanisms across energy, transportation, healthcare, manufacturing, and smart-city operational environments.

Rather than functioning as an empirical CPS field study, the manuscript integrates a cyber-physical governance convergence synthesis approach designed to establish a continuously adaptive governance architecture through which operational intelligence, AI-enabled analytics, event-validated learning, resilience coordination, human oversight, and executive governance synchronization operate collectively across interconnected cyber-physical ecosystems (Meadows, 2008; von Bertalanffy, 1968).

Sources were selected for their relevance to cyber-physical systems governance, adaptive oversight, resilience engineering, AI-enabled operational intelligence, human-AI collaboration, executive governance coordination, systems integration, and real-time decision support processes. Priority was given to peer-reviewed scholarship, foundational systems theory literature, resilience engineering research, governance modernization studies, cyber-physical systems governance frameworks, and authoritative guidance addressing complex operational

Vol. 11, No. 03; 2026

ISSN: 2456-3676

ecosystems across energy, transportation, healthcare, manufacturing, and smart-city environments.

The framework-development process employed explicit inclusion and exclusion criteria. Included sources were required to address cyber-physical governance, adaptive oversight, resilience coordination, operational intelligence integration, AI-enabled decision systems, governance synchronization, organizational adaptation, or executive governance decision-making. Sources that focused exclusively on isolated technical implementation issues, on narrowly defined engineering performance measures without governance implications, or on domain-specific operational procedures unrelated to governance oversight were excluded from the synthesis.

Comparative analysis of the selected literature identified recurring governance challenges associated with cyber-physical complexity, operational interdependence, AI-enabled control, real-time risk emergence, resilience coordination, governance observability, and executive synchronization. Particular attention was given to research examining how organizations maintain governance effectiveness as operational environments evolve more rapidly than traditional governance structures can adapt to.

The Cyber-Physical Governance Framework (CPGF) emerged through the synthesis of recurring governance capabilities consistently represented throughout the reviewed literature. Comparative evaluation revealed a common governance progression through which operational sensing, AI-enabled analytics, human oversight, adaptive learning, and executive governance coordination function collectively to maintain resilience, accountability, and operational continuity within dynamic cyber-physical environments.

The resulting framework conceptualizes cyber-physical governance as a convergence architecture rather than a collection of independent oversight activities. By organizing governance around recurring processes of sensing, interpretation, adaptation, learning, and executive synchronization, the CPGF provides a systematic pathway for organizations to sustain adaptive governance modernization across increasingly interconnected cyber-physical ecosystems.

2. Results of Cyber-Physical Governance Synthesis

2.1 Emergent Cyber-Physical Governance Themes

The cyber-physical governance synthesis identified five recurring governance challenges that are consistently represented across resilience engineering, adaptive governance, cyber-physical systems management, operational intelligence, human-AI teaming, and socio-technical systems literature (Endsley, 2017; Hollnagel, 2014; Leveson, 2011; Woods, 2018). Although terminology varied across disciplines, substantial convergence emerged regarding the governance challenges organizations face in managing increasingly interconnected cyber-physical environments.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

The first recurring challenge involved operational complexity, characterized by nonlinear interactions among technological, organizational, environmental, and human-system components. The second challenge centered on interdependence, reflecting the tight coupling of cyber and physical systems in which localized disruptions may propagate rapidly across operational ecosystems. The third challenge involved adaptive oversight, emphasizing the need for governance mechanisms that can respond to evolving operational conditions and emerging risks in real time. The fourth challenge focused on resilience coordination, highlighting the importance of maintaining continuity, recovery capability, and adaptive capacity amid uncertainty and disruption. The fifth challenge involved executive synchronization, emphasizing the need to align operational intelligence, governance observability, and strategic decision-making across multiple organizational levels.

Collectively, these recurring governance themes suggest that effective cyber-physical governance requires integrated oversight architectures that synchronize sensing, analytics, human judgment, adaptive learning, resilience management, and executive governance coordination across complex socio-technical ecosystems.

2.2 Cyber-Physical Governance Development Outcome

The identification of these recurring governance challenges informed the development of the Cyber-Physical Governance Framework (CPGF). Comparative analysis revealed a consistent governance progression through which cyber-physical systems generate operational intelligence, AI-enabled analytics evaluate evolving conditions, human oversight contextualizes emerging risks, adaptive governance mechanisms facilitate organizational learning, and executive leadership synchronizes resilience-oriented decision-making.

The resulting framework organizes cyber-physical governance into five interconnected adaptive layers: Real-Time Cyber-Physical Sensing, AI-Enabled Analytics and Control, Human Oversight and Intervention, Event-Validated Governance, and Executive Decision Translation. Each layer contributes to a continuously adaptive governance lifecycle through which organizations maintain operational awareness, resilience coordination, governance accountability, and strategic synchronization across dynamic cyber-physical environments.

The synthesis further revealed that cyber-physical governance functions as a convergence capability rather than a collection of isolated governance activities. Effective governance requires integrating operational intelligence, adaptive oversight, human intervention, event-driven learning, and executive coordination mechanisms that sustain resilience and institutional effectiveness amid increasing complexity, interdependence, and technological change.

These findings provide the conceptual foundation for the Cyber-Physical Governance Framework presented in the following sections and establish the basis for the convergence of governance across diverse cyber-physical operational ecosystems.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

3. Theoretical Foundations for Cyber-Physical Governance

3.1 Socio-Technical Systems Theory

CPS governance must account for interactions among human, organizational, and technological subsystems (Carayon, 2006).

3.2 Resilience Engineering

CPS requires adaptive capacity to absorb disruptions and maintain operational continuity (Hollnagel, 2014).

3.3 Human-AI Teaming

Governance must integrate AI-enabled sensing and control with human oversight and accountability (Wickens et al., 2015).

3.4 Event-Validated Learning

CPS generates high-frequency events that support continuous recalibration of governance (Shawe, 2026). Collectively, these theoretical foundations support the reconceptualization of cyber-physical governance as an adaptive convergence architecture that continuously integrates operational intelligence, AI-enabled control, human oversight, event-validated learning, and executive governance synchronization within dynamic socio-technical ecosystems (Leveson, 2011; Meadows, 2008).

4. The Cyber-Physical Governance Framework (CPGF)

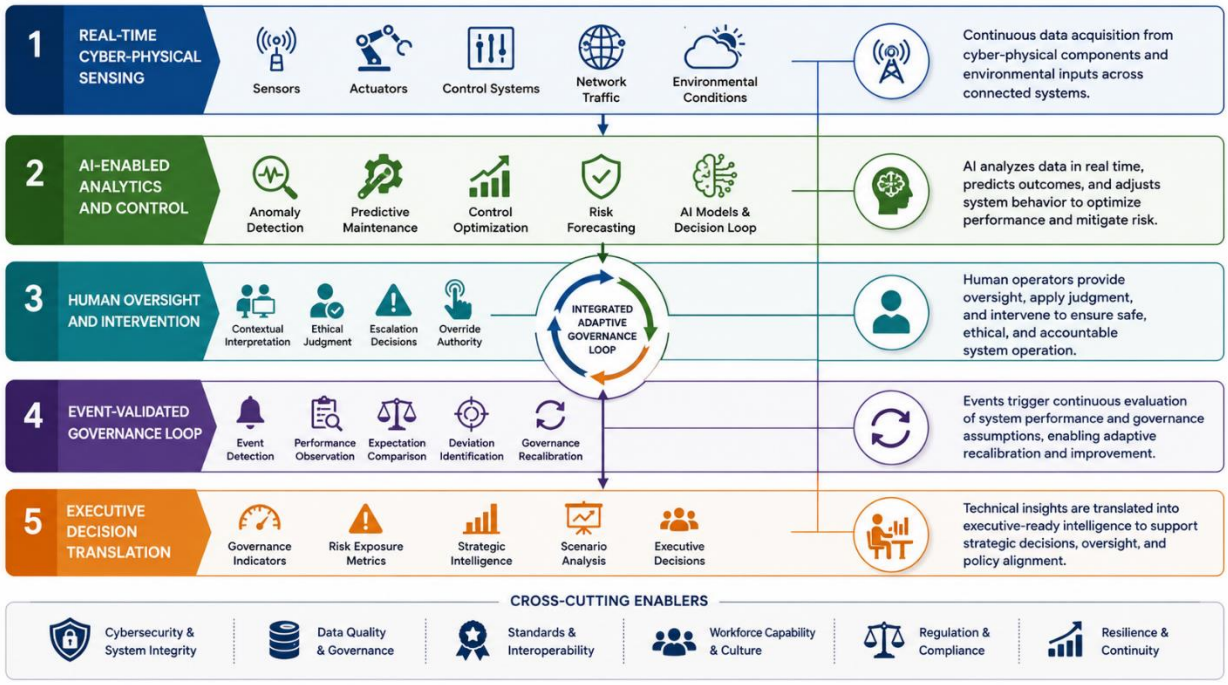
Building upon the constitutional governance architecture established through the Adaptive Governance Systems Framework (AGSF), the operational intelligence architecture operationalized through the AI-Enabled Governance Oversight Model (AIGOM), the governance evolution architecture formalized through the Governance Maturity Model (GMM), the adaptive governance-learning architecture operationalized through Event-Validated Governance (EVG), the comparative governance ecosystem analysis examining cross-domain governance variability across critical operational sectors, and the executive governance synchronization architecture established through the Governance Translation Framework (GTF), the Cyber-Physical Governance Framework (CPGF) establishes the operational convergence layer through which adaptive governance systems function across dynamic cyber-physical ecosystems (Leveson, 2011; Dekker, 2011). Figure 1 illustrates the integrated governance convergence architecture through which real-time sensing, AI-enabled analytics, human oversight, event-validated learning, and executive governance synchronization operate as continuously adaptive governance layers within interconnected CPS environments.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

Cyber-Physical Governance Framework (CPGF)



Note. Author created. The figure illustrates the cyber-physical governance convergence architecture, in which real-time sensing, AI-enabled analytics, human oversight, event-validated learning, and executive governance synchronization operate as integrated, adaptive governance layers within interconnected cyber-physical ecosystems.

As illustrated in Figure 1, cyber-physical governance emerges through the continuous synchronization of operational intelligence, AI-enabled oversight, human intervention, adaptive learning, and executive governance coordination processes that collectively transform fragmented oversight structures into integrated resilience-oriented governance ecosystems capable of operating under conditions of complexity, interdependence, and rapid operational change.

The CPGF establishes cyber-physical governance convergence through **five integrated adaptive governance layers** that collectively synchronize operational observability, AI-enabled analytics, human oversight, resilience adaptation, and executive governance orchestration across interconnected CPS ecosystems.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

4.1 Layer 1 — Real-Time Cyber-Physical Sensing

CPS generates continuous telemetry from:

- sensors
- actuators
- control systems
- network traffic
- environmental conditions

This layer aligns with AGSF's sensing architecture and AIGOM's AI-enabled monitoring.

4.2 Layer 2 — AI-Enabled Analytics and Control

AI systems support:

- anomaly detection
- predictive maintenance
- control optimization
- risk forecasting

These capabilities enhance CPS performance but require governance oversight to ensure transparency and accountability (Shneiderman, 2022; Parasuraman et al., 2000).

Effective cyber-physical governance requires that AI-enabled analytics and control functions operate within clearly defined governance boundaries. Although AI systems may enhance anomaly detection, predictive assessment, operational optimization, and real-time decision support, governance responsibility remains vested in institutional oversight structures rather than autonomous technologies.

Governance mechanisms supporting AI-enabled control may include model-validation protocols, algorithmic performance monitoring, explainability requirements, escalation thresholds, override authorities, and continuous audit processes. These controls help ensure that AI-generated recommendations remain transparent, accountable, and aligned with organizational objectives, regulatory obligations, resilience priorities, and operational risk tolerances.

Within cyber-physical environments, governance oversight must further address the potential consequences of automation bias, model drift, inaccurate predictions, and unintended operational outcomes. Human operators, governance analysts, and executive leadership therefore maintain responsibility for validating significant AI-generated actions, evaluating emerging risks, and ensuring that automated decision-support systems remain aligned with institutional governance expectations.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Through these governance mechanisms, AI-enabled analytics function not as autonomous governance authorities but as adaptive decision-support capabilities operating within a broader cyber-physical governance architecture designed to preserve accountability, resilience, and executive oversight.

4.3 Layer 3 — Human Oversight and Intervention

Human operators provide:

- contextual interpretation
- ethical judgment
- escalation decisions
- override authority

This layer ensures that AI-enabled control remains aligned with governance expectations (Argyris & Schön, 1978; Senge, 2006).

Human oversight functions as the primary governance safeguard within cyber-physical environments characterized by increasing levels of automation, AI-enabled decision support, and autonomous system behavior. Although operational intelligence and predictive analytics may enhance situational awareness, governance accountability remains dependent on human interpretation, judgment, and intervention capabilities to evaluate operational conditions within broader organizational, ethical, regulatory, and strategic contexts.

Effective cyber-physical governance therefore requires clearly defined escalation pathways, decision authorities, override mechanisms, and accountability structures that specify when human intervention becomes necessary. Governance personnel may be required to evaluate conflicting operational priorities, assess resilience implications, interpret emerging risks, validate AI-generated recommendations, and determine whether operational conditions warrant executive notification, governance review, or immediate corrective action.

Human oversight further serves as a protection mechanism against automation bias, overreliance on predictive systems, algorithmic misclassification, and governance complacency. By maintaining active human participation in critical decision-making processes, organizations preserve adaptive judgment capabilities that may not be fully captured by automated analytics or machine-driven optimization.

Within the Cyber-Physical Governance Framework, human oversight operates as the convergence layer through which operational intelligence, AI-enabled recommendations, organizational objectives, resilience priorities, and governance obligations are integrated into accountable institutional decision-making. This role ensures that cyber-physical governance remains aligned with organizational values, stakeholder expectations, regulatory requirements, and executive governance responsibilities.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

4.4 Layer 4 — Event-Validated Governance Loop

Events—including failures, anomalies, and deviations—trigger:

- performance observation
- expectation comparison
- deviation identification
- governance recalibration

This layer integrates EVG within CPS environments.

4.5 Layer 5 — Executive Decision Translation

Technical signals are translated into:

- governance indicators
- risk exposure metrics
- strategic decision intelligence

This layer aligns with the Governance Translation Framework (GTF) and supports the synchronization of governance intelligence, resilience coordination, and executive decision orchestration across interconnected cyber-physical ecosystems (Shneiderman, 2022; Woods, 2018).

5. Cross-Sector Applications of the CPGF

The CPGF provides a scalable cyber-physical governance convergence architecture that synchronizes operational intelligence, AI-enabled analytics, adaptive oversight, resilience coordination, and executive governance orchestration across critical infrastructure, healthcare, transportation, manufacturing, smart cities, and other interconnected CPS ecosystems (Perrow, 1984; Woods, 2018).

5.1 Energy and Utilities

CPS governs grid stability, load balancing, and fault detection (NIST, 2024).

5.2 Transportation Systems

Autonomous vehicles, rail systems, and air traffic control rely on CPS oversight.

5.3 Healthcare Delivery

Medical devices, robotic surgery, and clinical automation require CPS governance (Carayon et al., 2015).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

5.4 Industrial Automation

Manufacturing systems depend on CPS for precision, safety, and efficiency.

5.5 Smart Cities

Urban infrastructure integrates CPS for traffic, utilities, and public safety.

5.6 Illustrative Cyber-Physical Governance Convergence Scenario

To illustrate the operationalization of the Cyber-Physical Governance Framework (CPGF), consider a regional smart-grid ecosystem integrating AI-enabled energy distribution systems, autonomous infrastructure controls, predictive maintenance architectures, and executive governance oversight across interconnected utility networks.

During routine operations, cyber-physical sensing systems detect abnormal voltage fluctuations affecting multiple substations within a regional distribution network. Simultaneously, predictive analytics identify early indicators of infrastructure instability associated with a critical transformer cluster that supplies approximately 22% of the region's power distribution **capacity**.

Layer 1: Real-Time Cyber-Physical Sensing

Telemetry systems continuously collect operational data from:

- substations,
- grid controllers,
- environmental monitoring systems,
- network traffic architectures,
- infrastructure-health monitoring platforms.

Operational sensing identifies:

- voltage fluctuation variance: +18% above baseline,
- transformer thermal-stress increase: +27%,
- network-load imbalance: +14%,
- infrastructure anomaly score: 8.9/10,
- projected instability probability: 45% within 48 hours.

At this stage, the information remains operationally significant but does not yet provide sufficient governance context for executive action.

Layer 2: AI-Enabled Analytics and Control

Predictive analytics systems evaluate anomaly patterns, infrastructure dependencies, and potential cascading effects across the smart-grid ecosystem.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

AI-enabled assessment identifies:

- projected probability of localized transformer failure: 45%,
- probability of cascading service interruption: 28%,
- estimated customer impact: 165,000 service accounts,
- projected operational disruption window: 8–12 hours,
- estimated infrastructure recovery cost: $3.4 million.

These outputs provide early-warning intelligence but require governance interpretation before organizational response decisions can be initiated.

Layer 3: Human Oversight and Intervention

Governance analysts, infrastructure engineers, and operational leadership evaluate the AI-generated assessments within the context of:

- resilience-management priorities,
- regulatory obligations,
- critical-service dependencies,
- emergency-response capabilities,
- executive escalation criteria.

Human review confirms that multiple healthcare facilities, transportation systems, and public safety organizations depend on the affected infrastructure corridor. Analysts determine that the projected disruption exceeds established resilience-risk thresholds and warrants escalation to governance.

Layer 4: Event-Validated Governance Loop

Governance teams compare observed operational conditions against established performance expectations and resilience objectives.

Evaluation identifies:

- resilience-capability degradation,
- elevated infrastructure-dependency exposure,
- increased probability of regional service disruption,
- misalignment with continuity-performance targets.

The event is therefore classified as a governance-significant resilience deviation requiring adaptive governance recalibration and executive review.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Layer 5: Executive Decision Translation

Translated governance intelligence is presented to executive leadership via resilience dashboards, governance heat maps, infrastructure risk projections, and decision-support summaries. Executive reporting includes:

- projected disruption probability: 45%,
- estimated customer impact: 165,000 accounts,
- projected financial exposure: $3.4 million,
- resilience-impact rating: High,
- regulatory-reporting implications,
- recommended mitigation alternatives.

Leadership evaluates multiple response options, including preventive infrastructure maintenance, controlled load redistribution, emergency-response activation, and contingency resource deployment. Based on the translated governance intelligence, executives authorize proactive intervention and infrastructure stabilization measures to reduce the risk of disruption and preserve regional resilience.

This scenario demonstrates how the Cyber-Physical Governance Framework synchronizes operational sensing, AI-enabled analytics, human oversight, adaptive governance learning, and executive decision coordination into a unified cyber-physical governance architecture. Rather than treating operational anomalies as isolated technical events, the framework transforms cyber-physical complexity into resilience-oriented governance intelligence that supports adaptive leadership decisions across interconnected critical infrastructure ecosystems.

6. Implications for Governance Modernization

The CPGF enables organizations to modernize governance processes by establishing integrated cyber-physical oversight architectures capable of synchronizing operational observability, AI-enabled decision support, resilience coordination, adaptive governance learning, and executive oversight across rapidly evolving CPS environments (Organisation for Economic Co-operation and Development [OECD], 2024; World Economic Forum, 2023).

6.1 Real-Time Governance Capability

CPS requires governance systems capable of operating at machine speed.

6.2 Integrated Oversight Across Domains

Governance must unify cybersecurity, engineering, operations, and executive leadership.

6.3 Enhanced Accountability Mechanisms

AI-enabled control loops require transparent oversight structures.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

6.4 Institutional Resilience

Event-validated learning strengthens CPS resilience and adaptability.

6.5 Governance Implementation Implications

The CPGF provides organizations with a structured cyber-physical governance convergence architecture capable of synchronizing operational intelligence, AI-enabled oversight, resilience coordination, adaptive governance learning, and executive decision orchestration across rapidly evolving CPS environments. Executive leadership may use the framework to strengthen operational observability, improve resilience coordination, enhance adaptive governance responsiveness, and establish integrated governance synchronization pathways that support cyber-physical modernization initiatives.

Regulators and governance authorities may apply the CPGF to improve governance transparency, strengthen cyber-physical oversight capability, modernize adaptive governance coordination mechanisms, and support resilience-oriented governance synchronization across interconnected AI-enabled operational ecosystems (OECD, 2024).

Operational governance teams may utilize the framework to improve cyber-physical observability integration, strengthen event-driven governance coordination, institutionalize adaptive governance convergence processes, and synchronize operational intelligence with resilience-oriented governance modernization objectives.

7. Conclusion

The Cyber-Physical Governance Framework (CPGF) advances governance scholarship by establishing an integrated oversight architecture that synchronizes real-time sensing, AI-enabled analytics, human intervention, adaptive governance learning, resilience coordination, and executive decision support across complex cyber-physical environments. As organizations increasingly rely on interconnected technologies to support critical operations, governance systems must evolve beyond fragmented oversight structures toward adaptive architectures that can operate amid complexity, interdependence, and rapid change.

The framework contributes to cyber-physical governance research by demonstrating that effective governance depends not only upon technological capability but also upon the ability to coordinate operational intelligence, human judgment, resilience management, organizational learning, and executive oversight within a unified governance structure. By conceptualizing governance as a convergence architecture rather than a collection of isolated control mechanisms, the CPGF provides a systematic pathway for organizations to strengthen accountability, improve operational observability, enhance resilience performance, and support adaptive institutional decision-making across dynamic socio-technical ecosystems.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

The framework further illustrates how governance modernization can be achieved through the continuous integration of cyber-physical sensing, AI-enabled decision support, human oversight, event-validated learning, and executive governance synchronization. This integrated approach enables organizations to identify emerging risks more effectively, evaluate operational consequences more accurately, and implement governance responses that remain aligned with strategic objectives, resilience priorities, regulatory obligations, and stakeholder expectations.

Although conceptual in nature, the framework establishes a foundation for future empirical investigation and practical implementation. Future research should examine the effectiveness of cyber-physical governance architectures across critical infrastructure sectors, evaluate the influence of AI-enabled governance systems on executive decision quality, assess resilience outcomes associated with adaptive governance convergence, and investigate how cyber-physical governance capabilities contribute to organizational performance under conditions of operational uncertainty and disruption.

The Cyber-Physical Governance Framework therefore provides a theoretically grounded and operationally relevant model through which organizations can strengthen governance coordination, enhance adaptive oversight, improve resilience-oriented decision-making, and support governance modernization across increasingly interconnected cyber-physical ecosystems. By integrating technological observability, human accountability, organizational learning, and executive leadership into a unified governance architecture, the framework offers a practical pathway for sustaining effective governance in the cyber-physical environments that increasingly define modern organizational operations.

References

Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.

Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics, 37*(4), 525–535.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Flatley Brennan, P. (2006). Work system design for patient safety: The SEIPS model. *Quality and Safety in Health Care, 15*(Suppl. 1), i50–i58. https://doi.org/10.1136/qshc.2005.015842

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*.

Dekker, S. (2011). *Drift into failure: From hunting broken components to understanding complex systems*. Ashgate Publishing.

Endsley, M. R. (2017). From here to autonomy: Lessons learned from human-automation research. *Human Factors, 59*(1), 5–27. https://doi.org/10.1177/0018720816681350

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

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

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors, 46*(1), 50–80.

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

Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Organisation for Economic Co-operation and Development. (2024). *Framework for anticipatory governance of emerging technologies*. OECD Publishing.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30*(3), 286–297. https://doi.org/10.1109/3468.844354

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2–3), 183–213.

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

Senge, P. M. (2006). *The fifth discipline: The art and practice of the learning organization* (Rev. ed.). Doubleday.

Shawe, R. (2026). *From probabilistic compliance to event-validated resilience*. International Journal of Advanced Engineering and Management Research.

Shneiderman, B. (2022). *Human-centered AI*. Oxford University Press.

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

von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Wickens, C. D., Lee, J. D., Liu, Y., & Gordon-Becker, S. (2015). *An introduction to human factors engineering* (2nd ed.). Pearson.

Woods, D. D. (2018). The theory of graceful extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions*, *38*(4), 433–457. https://doi.org/10.1007/s10669-018-9708-3

World Economic Forum. (2023). *The Global Risks Report 2023* (18th ed.). World Economic Forum.