**Global Multidisciplinary Journal**
eISSN: 2791-173X pISSN: 2791-2760

VOLUME04 ISSUE11
*Published 30-11-2025* *Page No. 120-127*

# AI-Enabled Resilience in Cyber-Physical and Financial Systems: Integrating Secure Intelligence across Clinical Trials, IoMT, Supply Chains, and FinTech

**Dr. Amina R. Laurent**

**Global Institute for Cyber-Physical Systems, University of Geneva**

## ABSTRACT

**Background: Rapid convergence of artificial intelligence (AI), cyber-physical systems (CPS), and distributed ledger technologies has created both unprecedented capabilities and complex vulnerabilities across domains that include clinical research, Internet of Medical Things (IoMT), agri-food supply chains, and financial services. The disparate literatures on AI-driven protection mechanisms, secure blockchain topologies, and CPS design patterns demand integrated theorization to inform both academic inquiry and practical governance (Syed & Faiza, 2024; Voulgaris et al., 2020).**

**Objective: This research article synthesizes theoretical and applied knowledge from the provided references to present a unifying conceptual and methodological framework for AI-enabled resilience in cyber-physical and financial systems. The framework explicates how AI models, secure architectures, and CPS design patterns can act synergistically to mitigate cyber threats, preserve data integrity, and enable trustworthy automation.**

**Methods: Using a rigorous integrative review approach grounded in the supplied references, the methodology reconstructs causal pathways between system components (AI agents, sensors, ledgers, network topologies) and adversarial threats. The paper uses systematic cross-domain mapping of threat vectors, defenses, and design principles, supported by close textual analysis of theory and applied studies in the corpus (Lee & Seshia, 2006; Khaitan & Mohan, 2021).**

**Results: The synthesis yields a layered resilience architecture: (1) sensing and verification at the edge (IoMT & RFID-enabled traceability), (2) secure transaction and provenance layers (hierarchical blockchain topologies), (3) AI-driven anomaly detection and adaptive response, and (4) governance and auditability mechanisms for human oversight. This architecture addresses confidentiality, integrity, availability, and non-repudiation across domains, and demonstrates how finance-specific requirements for transactional integrity align with CPS safety constraints (Singh, 2025; Rajkumar & Lee, 2010).**

**Conclusions: The integrated framework demonstrates that AI is not merely a detection tool but a coordinating agent that—if designed with CPS principles, embedded assurance, and secure ledger topologies—can materially enhance system resilience. Implementation requires domain-specific model assurance, explainability, and regulatory alignment. Future research should empirically validate cross-domain transferability, quantify trade-offs between model complexity and interpretability, and operationalize governance mechanisms for adaptive, AI-mediated security.**

## KEYWORDS

**Global Multidisciplinary Journal**
eISSN: 2791-173X pISSN: 2791-2760

VOLUME04 ISSUE11
*Published 30-11-2025* *Page No. 120-127*

**Artificial intelligence, cyber-physical systems, IoMT security, blockchain traceability, fintech cybersecurity, clinical trial privacy, hierarchical topologies**

## INTRODUCTION

The digitalization of physical systems and institutional processes has produced an interdependent ecosystem in which computational intelligence, sensing hardware, networked infrastructures, and distributed transactional systems interact to create new socio-technical capabilities and vulnerabilities (Lee & Seshia, 2006; Rajkumar & Lee, 2010). The convergence is particularly salient in four interrelated domains: clinical trials and medical data protection, Internet of Medical Things (IoMT), agri-food supply chain traceability, and financial services including fintech and core banking systems. Each domain has its own operational norms, regulatory constraints, and technological affordances; yet they share fundamental challenges: securing sensitive data, ensuring transactional integrity, enabling reliable automation, and maintaining human oversight in the face of adaptive adversaries (Syed & Faiza, 2024; Muhammad et al., 2023; Tian, 2016).

Clinical trial data represent a high-value target due to the sensitivity of health information and the criticality of integrity for medical evidence. AI systems have begun to be applied for protecting such data—through anomaly detection, privacy-preserving analytics, and secure access controls—but academic and practitioner accounts emphasize gaps in rigor, explainability, and integration with legal safeguards (Syed & Faiza, 2024). Simultaneously, IoMT devices proliferate in hospitals and clinical research settings, amplifying the attack surface and blending cyber risk with physical safety risk (Syed & Faiza, 2024). The challenges multiply when supply chain provenance and financial transaction integrity must be assured alongside clinical privacy—thereby requiring interoperable technologies and coherent governance.

Blockchain and hierarchical topologies have been proposed as mechanisms for traceability and tamper-evidence across supply chains, yet their application to quality control and dynamic environments requires careful mapping to system design patterns of CPS and rigorous understanding of latency, scalability, and consensus trade-offs (Voulgaris et al., 2020; Tian, 2016). In finance, AI-driven portfolio management and other algorithmic decision systems create both opportunity for performance enhancement and new classes of systemic risk, demanding cybersecurity practices that preserve transactional integrity and regulatory compliance (Bi & Lian, 2024; Singh, 2025).

Despite parallel developments in the literature, there remains a research gap: studies tend to be domain-specific and either strongly technical (focusing on cryptographic or control-theoretic solutions) or strongly managerial/regulatory (focusing on governance and policy). Few works systematically integrate AI's role as both analytic engine and control agent with CPS design principles and secure ledger topologies to offer prescriptive frameworks that span clinical research, IoMT, supply chains, and financial systems. This article addresses that gap by synthesizing the provided references into an integrated theoretical and methodological contribution that reconciles AI, CPS design, blockchain topologies, and domain-specific cybersecurity practices.

The problem statement is threefold: (1) how can AI be architected to protect sensitive clinical trial data and IoMT devices while preserving interpretability and compliance? (2) how can blockchain and hierarchical ledger designs be integrated with CPS design patterns to secure supply chain quality control and transaction provenance? (3) how should cybersecurity practices in fintech and core banking adapt to AI-driven decision-making and CPS integration? The research aims to construct a cross-domain framework, to explicate the theoretical rationale behind each component, and to provide a roadmap for practical implementation and future empirical testing.

**Global Multidisciplinary Journal**
eISSN: 2791-173X pISSN: 2791-2760

VOLUME04 ISSUE11
*Published 30-11-2025* *Page No. 120-127*

## Methodology

This study adopts an integrative theoretical synthesis methodology that carefully analyzes, triangulates, and builds upon the supplied corpus of domain-specific and foundational references. The methodological rationale is threefold: first, to remain strictly grounded in the supplied materials; second, to map conceptual overlaps across domains; and third, to produce an actionable layered architecture that respects the engineering, data-science, and governance constraints evident in the literature.

Selection and scope. The corpus provided includes applied studies on AI in clinical trials and IoMT security (Syed & Faiza, 2024; Syed & Faiza, 2024), AI for finance and portfolio management (Bi & Lian, 2024), practical system design for virtual assistants and NLP in cloud apps (Peta et al., 2023), blockchain security for decentralized transactions (Muhammad et al., 2023), hierarchical blockchain topologies for supply chains (Voulgaris et al., 2020), RFID/blockchain traceability for agri-food chains (Tian, 2016), and foundational CPS theory and design patterns (Lee & Seshia, 2006; Rajkumar & Lee, 2010; Khaitan & Mohan, 2021; Wolf & Jasper, 2022; Gill & Siddharth, 2023). A recent practical treatment of cybersecurity practices in fintech provides a specific institutional perspective (Singh, 2025). Together these works allow for cross-domain mapping.

**Analytic approach. The synthesis proceeds in several steps:**

1. Thematic extraction: identify recurring constructs (e.g., data integrity, provenance, anomaly detection, edge verification, hierarchical ledgers, CPS safety) across the corpus and distill domain-specific problem statements (clinical trials privacy, IoMT device security, supply chain traceability, transactional integrity). The corpus's applied and theoretical works inform these constructs (Syed & Faiza, 2024; Voulgaris et al., 2020; Lee & Seshia, 2006).
2. Cross-domain mapping: create conceptual correspondences between constructs (e.g., "provenance" in supply chains and "auditability" in clinical trials), revealing shared architectural requirements such as tamper-evidence, low-latency verification, and model explainability (Tian, 2016; Bi & Lian, 2024).
3. Layered architecture design: synthesize a layered resilience architecture grounded in CPS design patterns and ledger topologies, deploying AI functions at appropriate layers (Khaitan & Mohan, 2021; Rajkumar & Lee, 2010).
4. Elaboration of mechanisms: specify how AI techniques (anomaly detection, federated learning, explainable AI) align with edge-sensing, ledger synchronization, and governance processes—drawing explicitly from domain studies (Syed & Faiza, 2024; Peta et al., 2023; Muhammad et al., 2023).
5. Normative and operational recommendations: generate practical guidance for implementation, incorporating cybersecurity best practices for finance and core banking (Singh, 2025).

The methodology is deliberately text-based and conceptual, not empirical. It leverages close reading, logical inference, and theory-building anchored in the supplied references. Because the article synthesizes across disciplines, it prioritizes conceptual clarity and engineering plausibility over simulation or field data.

Analytic assumptions and limitations. The study assumes that the supplied corpus captures representative technical and managerial perspectives from the relevant domains. It further assumes that AI methods cited in the corpus (such as deep learning in finance or AI-driven security in medical contexts) can be adapted across domains with appropriate domain-aware constraints (Bi & Lian, 2024; Syed & Faiza, 2024). Limitations include the lack of primary empirical datasets and the absence of interactive testing; therefore, the recommendations

are framed as a theoretical and design-oriented contribution that requires later empirical validation (Gill & Siddharth, 2023).

## RESULTS

The synthesis produces a coherent, layered architecture and a set of domain-bridging findings that articulate how AI, CPS design, and ledger technologies can jointly enable resilient and secure digital-physical systems. The results are descriptive and analytic, as follows.

Layered resilience architecture. Across the corpus, four interdependent layers emerge as necessary for systemic resilience:

### 1. Edge Sensing and Local Verification Layer.

This layer includes sensors, IoMT devices, RFID tags, and embedded controllers that generate raw data and execute immediate control loops. CPS literature emphasizes the importance of robust embedded systems design, real-time constraints, and formal verification techniques to ensure safety and determinism at the edge (Lee & Seshia, 2006; Rajkumar & Lee, 2010). In healthcare, IoMT devices require security hardening and anomaly detection, because device compromise can directly impact patient safety (Syed & Faiza, 2024). In agri-food supply chains, RFID-enabled sensing provides provenance data that must be authenticated at the point of capture (Tian, 2016). AI's role at this layer is to perform lightweight, explainable anomaly detection and to validate data before it is promoted upstream (Khaitan & Mohan, 2021).

### 2. Secure Transaction and Provenance Layer (Ledger Topologies).

The second layer focuses on tamper-evidence, transactional integrity, and provenance through ledger technologies. Hierarchical blockchain topologies—where local or domain-specific ledgers interoperate with higher-level consensus layers—offer a way to balance scalability, latency, and trust relationships across stakeholders in supply chains and distributed research consortia (Voulgaris et al., 2020). For clinical trials, ledger-based audit trails can provide immutable records of data access and transformations, thereby strengthening regulatory compliance and reproducibility (Syed & Faiza, 2024). In finance, ledger architectures must preserve transactional integrity while meeting throughput demands of core banking, which implies hybrid ledger configurations and strong cryptographic primitives (Singh, 2025; Muhammad et al., 2023).

### 3. AI-driven Analytics and Adaptive Response Layer.

This core analytical layer deploys advanced machine learning and deep learning models for tasks such as portfolio management, anomaly detection, predictive maintenance, and dynamic risk scoring (Bi & Lian, 2024). Importantly, AI here is envisioned not as an isolated predictive tool but as an adaptive agent coordinating responses across edge and ledger layers—for example, triggering quarantines of compromised devices, flagging suspicious transactions for human review, or initiating automated provenance validation workflows. AI must be designed with model assurance, interpretability, and domain constraints to maintain trust (Peta et al., 2023; Syed & Faiza, 2024).

### 4. Governance, Auditability, and Human Oversight Layer.

The top layer ensures transparency, policy enforcement, and human-in-the-loop controls. The CPS literature emphasizes that engineered automation must include fail-safes and verifiable interfaces for human operators (Rajkumar & Lee, 2010; Gill & Siddharth, 2023). For clinical trials and financial systems, regulatory mandates demand auditable records, provenance, and explainable decision-making. Governance mechanisms include role-based access controls, cryptographic auditing, policy engines, and compliance workflows that interface with the

ledger and AI layers (Singh, 2025; Syed & Faiza, 2024).

**Cross-domain correspondences and transferability. The mapping highlights several transferable constructs:**

- Provenance and auditability are central both to agri-food quality control and to clinical trial data integrity; ledger topologies can be designed to support both contexts when coupled with domain-aware metadata standards (Tian, 2016; Voulgaris et al., 2020; Syed & Faiza, 2024).

- Real-time safety requirements in CPS (e.g., control loops in industrial systems) parallel safety-critical IoMT constraints; design patterns that enforce timing guarantees and formal verification on the edge can be adapted to healthcare contexts (Lee & Seshia, 2006; Khaitan & Mohan, 2021).

- Finance demands transactional throughput and non-repudiation; hierarchical ledger designs that decouple local consensus from global reconciliation can reconcile these requirements with CPS-style safety and latency constraints (Bi & Lian, 2024; Singh, 2025).

Model assurance and explainability. A crucial result is that AI's efficacy depends on aligning model complexity with the requirement for interpretability and regulatory scrutiny. In clinical trials and healthcare, explainable models are preferred to allow investigators and regulators to validate outcomes (Syed & Faiza, 2024). In finance, regulatory compliance and auditability necessitate models whose decision paths can be reconstructed for forensic analysis (Bi & Lian, 2024; Singh, 2025). The framework therefore prescribes tiered AI models: lightweight, interpretable models at the edge for immediate decisions; more complex centralized models for pattern discovery and optimization, paired with robust logging and explainability protocols (Peta et al., 2023).

Security posture for decentralized transactions. The synthesis identifies concrete security measures for blockchain-integrated systems: hierarchical topologies reduce attack surfaces by localizing consensus and establishing trusted gateway nodes; cryptographic signing of sensor data at capture prevents upstream tampering; and cross-layer attestation ensures that data promoted to higher layers meet policy checks (Voulgaris et al., 2020; Muhammad et al., 2023). For finance, transactional integrity must be augmented with anomaly detection on transaction metadata and adaptive response mechanisms that can isolate suspicious flows (Singh, 2025).

Operational implications and design patterns. The CPS design patterns literature (Khaitan & Mohan, 2021; Wolf & Jasper, 2022) provides concrete templates—such as controller redundancy, watchdog monitors, and secure bootstrapping—that can be instantiated within the proposed layered architecture. The results enumerate how each pattern supports resilience: redundancy mitigates device failure or compromise; watchdogs enable timely detection and rollback; secure bootstrapping ensures device identity and chain-of-trust from manufacture to deployment.

## DISCUSSION

This section elaborates the theoretical implications, evaluates potential counter-arguments, and outlines limitations and future research imperatives. The discussion revolves around four major themes: the role of AI as a coordinating agent, the reconciliation of ledger properties with CPS constraints, the sociotechnical imperatives of governance, and the domain-specific adaptations necessary for healthcare, supply chains, and

finance.

AI as a coordinating agent: opportunities and constraints. The framework positions AI as a coordination mechanism that maps sensor signals to ledger operations and to human actions. This reconceptualizes AI from a narrow predictive tool to an orchestrator of resilience: AI can prioritize alerts, adjudicate conflicting data, and propose remediation actions across system layers (Bi & Lian, 2024; Peta et al., 2023). The opportunity here is clear: AI can compress human managerial workload while enabling faster responses to complex, cross-domain incidents. However, significant constraints arise. First, model errors in safety-critical contexts can have dire consequences—ranging from misclassification of a compromised IoMT device to erroneous modification of a clinical trial dataset. The CPS literature cautions that automated control must be accompanied by formal verification and fail-safe design to preserve safety margins (Lee & Seshia, 2006; Rajkumar & Lee, 2010). Second, reliance on AI coordination raises explainability and accountability issues: when an AI-offered remediation is enacted, audit trails must clearly capture the model input, internal reasoning (to the extent feasible), and the decision outcome to support post-hoc analysis (Syed & Faiza, 2024; Singh, 2025).

Reconciling ledger properties with CPS constraints. Blockchains provide tamper-evidence and immutable provenance, yet classic public ledger properties—high latency, eventual consistency, and resource-intensive consensus—conflict with CPS requirements for predictability and low-latency control signals (Voulgaris et al., 2020; Tian, 2016). Hierarchical ledger topologies address this tension by creating local trusted ledgers that maintain immediate consistency for control functions, while periodically anchoring summaries to a higher-level consensus network for global auditability. This hierarchical approach offers a principled compromise: local determinism for safety, global immutability for provenance. Critics may argue that such hybridization reintroduces centralization trade-offs or trusted third-party dependencies. The response is that the design must specify clearly audited gateway nodes, cryptographic attestations, and redundancy to prevent single points of failure—a recommendation grounded in CPS redundancy patterns (Khaitan & Mohan, 2021; Wolf & Jasper, 2022).

Sociotechnical governance and human oversight. The literature stresses that technical solutions are necessary but not sufficient; governance, policy, and organizational culture determine practical resilience (Syed & Faiza, 2024; Singh, 2025). For instance, securely designed IoMT devices will still be vulnerable if procurement and patching practices are lax or if clinical workflows bypass security controls for expediency. Therefore, the architecture includes governance mechanisms—role-based access, policy engines, and audit interfaces—that are interoperable with the ledger and AI layers. Importantly, the governance layer must embed regulatory reporting requirements, informed consent management for clinical data, and compliance controls for financial regulation (Syed & Faiza, 2024; Singh, 2025). The sociotechnical challenge is to design user-centered interfaces and processes that minimize friction while ensuring accountability.

**Domain-specific considerations and adaptations.**

Clinical trials and IoMT. Clinical trials require protecting participant privacy, ensuring data integrity, and providing audit trails for regulatory agencies. AI can help by detecting anomalous access patterns, automating de-identification, and facilitating secure federated analyses that preserve privacy (Syed & Faiza, 2024). However, federated learning for clinical datasets must be deployed with cryptographic protections (e.g., secure aggregation) and robust outlier detection to prevent model poisoning. Device-level protections—secure boot, attestation, and monitoring—are essential for IoMT devices that can affect patient safety; these requirements mirror CPS safety constraints (Lee & Seshia, 2006; Khaitan & Mohan, 2021).

Agri-food supply chains. Traceability efforts using RFID and blockchain provide provenance and quality control

(Tian, 2016). Hierarchical blockchains can map well to supply chain structures—local farm or processor ledgers feeding regional registries with audits at national or international layers (Voulgaris et al., 2020). AI can analyze supply chain telemetry to detect anomalies (e.g., temperature excursions) and predict contamination risks. Notably, supply chain participants vary in technical sophistication; thus, low-barrier edge verification mechanisms and standardized metadata schema are essential to ensure data quality at capture (Tian, 2016).

Finance and fintech. Finance requires throughput, low-latency settlement, and strong regulatory compliance. AI-driven portfolio management offers enhanced optimization but introduces risks (e.g., model-driven market impact, adversarial manipulation). Cybersecurity practices in finance must therefore incorporate anomaly detection on transaction streams, model audit trails, and robust access controls (Bi & Lian, 2024; Singh, 2025). The framework advocates hybrid ledger topologies and AI-based fraud detection with human escalation, balanced against the need for rapid settlement and reconciliation.

Counter-arguments and risk trade-offs. A plausible counter-argument is that adding AI, ledgers, and governance layers increases system complexity and thus attack surfaces. Complexity indeed can create novel vulnerabilities if not managed. The framework mitigates this by advocating modular design patterns, minimal trusted computing bases, explicit interface contracts, and staged deployment with strong monitoring—approaches consistent with CPS design patterns and industrial best practices (Khaitan & Mohan, 2021; Wolf & Jasper, 2022). Another criticism is that auditability can conflict with privacy. The architecture addresses this by combining cryptographic techniques (selective disclosure, zero-knowledge proofs where applicable) with governance policies to ensure that auditability does not imply uncontrolled data exposure, particularly for clinical trial participants (Syed & Faiza, 2024).

Limitations of the current synthesis. The primary limitation of this study is its conceptual and non-empirical nature. While the layered architecture and recommendations are grounded in the provided literature, the absence of implementation case studies or field experiments means the claims are primarily theoretical. Additionally, because the corpus is pre-specified, it may omit emergent solutions or critiques outside the supplied references. Finally, operationalization in constrained resource environments (e.g., small farms or low-income healthcare settings) requires additional socio-technical interventions not fully addressed here.

Future research directions. The next stage should translate the framework into empirical prototypes and pilot deployments across domains, using mixed-methods evaluation to test resilience metrics (detection latency, false positive/negative rates, transactional throughput, governance compliance). Comparative studies should evaluate hierarchical ledger topologies against monolithic and fully centralized alternatives in terms of latency, security, and auditability. Model assurance research should quantify trade-offs between explainability and predictive performance in regulated settings like clinical trials and finance. Finally, policy-oriented research should examine how regulatory frameworks can foster cross-domain interoperability without undermining competition or data protection.

## CONCLUSION

The integrated synthesis presented in this article articulates how AI, cyber-physical systems design patterns, and hierarchical ledger topologies can jointly strengthen resilience across clinical trials, IoMT ecosystems, agri-food supply chains, and financial services. The proposed layered architecture—spanning edge sensing and verification, secure transaction and provenance layers, AI-driven analytics and adaptive response, and governance and auditability—provides a coherent blueprint for practice and research. Key insights include the necessity of model assurance and explainability, the value of hierarchical ledgers to reconcile CPS constraints with tamper-evidence requirements, and the centrality of governance and human oversight to operational

resilience. This cross-domain perspective demonstrates that technical integration must be accompanied by socio-technical design and regulatory alignment. Future work should empirically validate the architecture through cross-domain pilots, investigate trade-offs between complexity and robustness, and develop practical toolkits for implementers. The convergence of AI and CPS offers a path to resilient automation—but realizing this potential demands careful engineering, rigorous oversight, and sustained interdisciplinary collaboration.

## REFERENCES

1. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "AI in Protecting Clinical Trial Data from Cyber Threats." International Journal of Advanced Engineering Technologies and Innovations 1, no. 2 (2024): 567-592.
2. Bi, Shuochen, and Yufan Lian. "Advanced Portfolio Management in Finance using Deep Learning and Artificial Intelligence Techniques: Enhancing Investment Strategies through Machine Learning Models." Journal of Artificial Intelligence Research 4, no. 1 (2024): 233-298.
3. Peta, Venkata Phanindra, Sai Krishna Reddy Khambam, and Venkata Praveen Kumar Kaluvakuri. "Designing Smart Virtual Assistants for Cloud Apps: Utilizing Advanced NLP and AI." Available at SSRN 4927242 (2023).
4. Muhammad, Shafi, Fatima Meerjat, Amna Meerjat, Aryendra Dalal, and Samad Abdul. "Enhancing Cybersecurity Measures for Blockchain: Securing Transactions in Decentralized Systems." Unique Endeavor in Business & Social Sciences 2, no. 1 (2023): 120-141.
5. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "AI-Powered Security for Internet of Medical Things (IoMT) Devices." Revista de Inteligencia Artificial en Medicina 15, no. 1 (2024): 556-582.
6. S. Voulgaris, N. Fotiou, V. A. Siris, G. C. Polyzos, A. Tomaras and S. Karachontzitis, "Hierarchical Blockchain Topologies for Quality Control in Food Supply Chains," 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 2020, pp. 139-143, doi: 10.1109/EuCNC48522.2020.9200913.
7. Singh, V. (2025). Securing Transactional Integrity: Cybersecurity Practices in Fintech and Core Banking. QTanalytics Publication (Books), 86–96.
8. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1-6). IEEE.
9. Lee, E. A., & Seshia, S. A. (2006). Introduction to embedded systems: A cyber-physical systems approach. Lexington, MA: The MIT Press.
10. Rajkumar, R., & Lee, E. A. (2010). Cyber-physical systems: The next revolution in computing and control. In Proceedings of the 49th IEEE Conference on Decision and Control (pp. 738-743).
11. Khaitan, S. K., & Mohan, S. (2021). Design patterns for industrial cyber-physical systems. Cambridge University Press.
12. Wolf, M., & Jasper, D. (2022). Industrial cyber-physical systems: Theory and applications. Springer International Publishing.
13. Gill, K. P., & Siddharth, A. (Eds.). (2023). Cyber-physical systems: Advances in design, modeling, analysis, and control. Academic Press.