Volume-06|Issue-09|September|Year-2026 ISSN: 3049-2343

International Journal of Academic and Industrial Research Innovations(IJAIRI)

Research Paper Title :Fault-Tolerant Distributed Quantum Intelligence with Photonic Circuit Emulation and AI-Augmented Control for Autonomous Cyber-Physical Networks

[1]Murali Krishna Pasupuleti

[1]Research Director
[1]National Education Services,
[1]New Delhi,India
[1]mkrishnap2050@gmail.com

Abstract:
Autonomous cyber-physical networks increasingly combine distributed sensing, edge intelligence, networked control, and safety-critical actuation, yet their reliability is constrained by correlated cyber faults, communication loss, model drift, hardware degradation, and the fragility of emerging quantum resources. This paper develops a fault-tolerant distributed quantum-intelligence architecture that couples photonic circuit emulation, quantum error-aware computation, AI-augmented control, distributed consensus, and deterministic safety fallback. The purpose is to formalize how heterogeneous quantum, photonic, AI, and control subsystems can jointly preserve mission-level stability when individual components fail or become uncertain. The study adopts a model-based systems methodology, synthesizes the supplied literature on fault-tolerant photonic quantum computing, distributed autonomous control, cyber-physical resilience, AI-native edge systems, and quantum-assisted optimization, and formulates a multi-layer state-space and reliability model. A composite Fault-Tolerant Quantum Intelligence Resilience Index (FTQIRI) integrates quantum reliability, photonic emulation fidelity, AI robustness, network resilience, closed-loop stability, and cyber assurance. An illustrative 0–10 numerical model yields an integrated score of 8.49 for the proposed architecture versus 6.34 for a conventional hybrid baseline, indicating the expected value of cross-layer redundancy and adaptive orchestration rather than empirical superiority. The paper further specifies an invention-oriented architecture, independent system and method claim drafts, and dependent claim concepts around digital-twin emulation, syndrome-informed control, consensus-based failover, cryptographic verification, and safety envelopes. The principal contribution is a unified mathematical and engineering framework that treats quantum fault tolerance and cyber-physical fault tolerance as coupled control problems, thereby connecting photonic quantum hardware, distributed intelligence, and autonomous network safety within one verifiable decision loop.

Keywords: fault-tolerant quantum computing; distributed quantum intelligence; photonic circuit emulation; autonomous cyber-physical systems; AI-augmented control; quantum error correction; resilient edge intelligence; distributed consensus; safe reinforcement learning; digital twin; quantum–classical co-design; cyber resilience; multi-agent control; reliability optimization; verifiable AI

Copyright:

© 2026 by Murali Krishna Pasupuleti.

1. Introduction

The next generation of autonomous cyber-physical systems (CPS) will not be defined by a single algorithm or computing substrate. They will be heterogeneous systems in which physical sensing, classical edge computing, AI inference, networked control, photonic acceleration and, where technically justified, quantum information processing coexist within closed decision loops. Such systems appear in autonomous mobility, smart grids, industrial robotics, resilient cities, advanced communications, and distributed scientific infrastructures. Their common engineering requirement is not merely high computational performance but dependable operation under compound disturbances. A safe architecture must continue to estimate, decide and control when sensors fail, packets are lost, adversaries inject perturbations, AI models drift, photonic components deviate from calibration, or quantum circuits experience noise and decoding errors.

The supplied literature establishes several parts of this problem but mostly in separate disciplinary layers. Fault-tolerant quantum computing research examines architectural and memory-level mechanisms for suppressing or correcting quantum errors, including photonic approaches and low-depth coding strategies (Ostmann, Nunn & Jones 2026; Nelson et al. 2025; Renault et al. 2025). Autonomous control research develops robust and distributed fault-tolerant control for vehicles, multi-UAV systems and power CPS (Zhang, Ifqir & Puig 2025; Yu et al. 2025; Qi et al. 2026). AI-native network research addresses distributed intelligence and terminal–edge–cloud collaboration (Karachalios et al. 2023; Wang et al. 2026), while photonic and quantum-AI work explores high-speed AI processing, optimization and photonic neural architectures (Beghriche et al. 2026; Daneshzad & Parsanasab 2026; Boras, Ewaniuk & Rotenberg 2026). The central gap is architectural: these advances require a common state, risk and control language before they can be orchestrated as one fault-tolerant autonomous system.

This paper therefore treats fault tolerance as a cross-layer control objective. The proposed architecture continuously estimates both physical state and computational trust state. Photonic circuit emulation provides a fast digital or hardware-in-the-loop surrogate of the quantum/photonic path; quantum syndrome or reliability indicators become control variables rather than isolated hardware diagnostics; AI policies are constrained by safety envelopes; and distributed agents use consensus and failover

rules to preserve bounded operation. The design extends the concept of nonfragile CPS control under cyberattack (Qi et al. 2026) toward heterogeneous quantum-enabled infrastructure and complements resilient edge architectures (Xu, Nagothu & Chen 2024) with an explicit quantum-photonic assurance layer.

The global relevance of the problem follows from the diffusion of autonomy into energy, mobility, manufacturing and communications. In such settings, a local computational failure can propagate into physical consequences, while an apparently minor physical deviation may destabilize an AI policy or invalidate a quantum-assisted optimization result. Secure V2X, post-quantum IoT–edge–cloud security and AI-driven grid reliability research show that resilience has become a system property spanning computation, communications and control rather than a narrowly local hardware property (Li, Xie & Iqbal 2026; Alrowaili et al. 2026; Ahmadi, Aly & Gu 2026). A formal framework that integrates these layers can help researchers specify failure modes, compare architectures and design validation experiments before expensive hardware deployment.

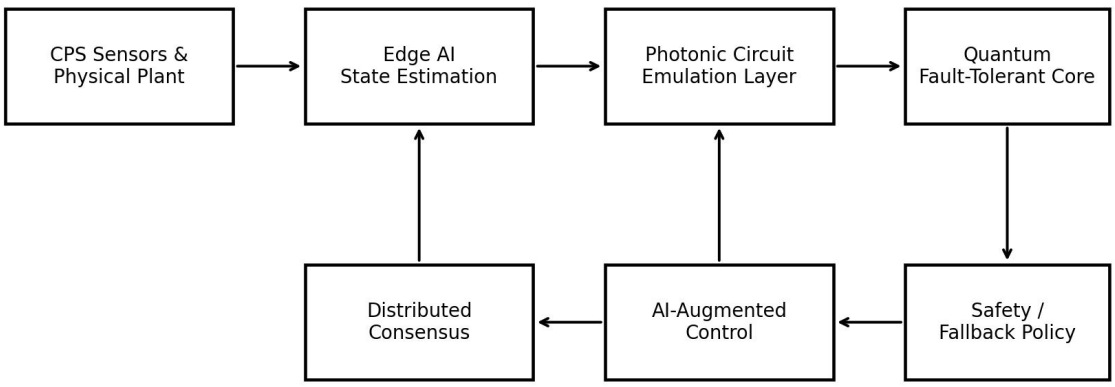


Figure 1. Proposed fault-tolerant distributed quantum-intelligence architecture.

1.1 Research Questions

- RQ1. How can quantum-computing reliability, photonic emulation fidelity, AI robustness, network resilience and physical-control stability be represented within a unified cross-layer state model?
- RQ2. How can photonic circuit emulation be used as a predictive validation and failover mechanism for distributed quantum-assisted control?
- RQ3. Which control and consensus mechanisms can prevent local computational faults or cyber disturbances from propagating into unsafe physical states?
- RQ4. How should AI-augmented control switch among quantum-assisted, photonic-emulated and deterministic safe modes under uncertainty?
- RQ5. Which measurable indicators can be combined into a mission-level resilience index suitable for simulation, digital-twin testing and later empirical validation?
- RQ6. What invention-oriented architecture and method elements emerge from the integration of fault-tolerant quantum computing, photonic emulation and autonomous CPS control?

1.2 Research Objectives

- To synthesize the supplied literature into a cross-layer architecture for fault-tolerant distributed quantum intelligence.
- To formulate state-space, matrix, dynamic, reliability and optimization models for quantum-photonic-AI cyber-physical operation.
- To define a photonic circuit emulation layer that supports prediction, verification, anomaly localization and safe failover.
- To construct an illustrative resilience index and numerical model for transparent comparative reasoning.
- To establish validation metrics for simulation, hardware-in-the-loop and distributed autonomous-system experimentation.
- To articulate an invention-oriented technical problem, architecture, and claim concepts suitable for subsequent specialist patent drafting and prior-art assessment.

2. Literature Review

Fault-tolerant quantum computing addresses the gap between noisy physical operations and reliable logical computation. In the supplied corpus, Ostmann, Nunn and Jones (2026) investigate a nonlinear photonic architecture directed toward fault-tolerant quantum computing, while Renault et al. (2025) present an end-to-end switchless architecture for fault-tolerant photonic quantum computing. Nelson et al. (2025) focus on low-depth random circuit codes for quantum memory. Together these works establish that fault tolerance is inseparable from architecture: topology, switching, coding depth, loss pathways and measurement structure determine whether logical reliability can scale. The implication for autonomous CPS is that the quantum layer should expose operational health variables—such as syndrome rate, logical error estimate, loss probability and resource margin—to the higher-level controller instead of remaining opaque.

The supplied IJAIRI literature extends this architectural view. Pasupuleti (2026a) frames photonic-interconnected quantum chiplets as a modular and networked computing approach, while Pasupuleti (2026b) links topological quantum error correction with tensor-network optimization in photonic quantum computing. Pasupuleti (2026c) connects quantum signal processing with fault-tolerant photonic computing, and Pasupuleti (2026d) links topological photonics to neuromorphic computing and low-power edge intelligence. These contributions support the paper's decision to model the photonic subsystem not simply as an interconnect but as an emulation, signal-conditioning and confidence-estimation layer between quantum computation and CPS actuation.

A second literature stream concerns fault-tolerant control. Zhang, Ifqir and Puig (2025) examine robust LPV fault-tolerant tracking control for autonomous vehicles, and Yu et al. (2025) develop distributed fault-tolerant control for multi-UAVs using dynamic event triggering. Qi et al. (2026) directly address nonfragile fault-tolerant control for power CPS under cyberattacks. Li and Zhang (2026) integrate cyberattack detection, fault estimation and fault-tolerant control in smart-grid CPS. Across these studies, a common principle is visible: resilient autonomy requires state estimation, fault diagnosis, bounded control and reconfiguration. The current paper generalizes that principle to include computational trust variables associated with AI and quantum-photonic execution.

A third stream concerns distributed AI and edge resilience. Karachalios et al. (2023) discuss distributed machine learning and native-AI enablers for end-to-end resource management in 6G, while Wang et al. (2026) formulate terminal–edge–cloud collaboration for AI-native networks. Xu, Nagothu and Chen (2024) emphasize autonomous and resilient edge architecture for smart cities. Asim et al. (2023) review AI-based secure edge systems for IoT devices and cities. These works motivate a layered deployment model in which local agents retain minimum safe autonomy even when access to remote intelligence degrades.

A fourth stream concerns quantum–AI optimization and photonic acceleration. Gu et al. (2026) discuss hybrid quantum-classical reinforcement learning for scheduling systems and Bożejko et al. (2026) study manufacturing scheduling with autonomous AI and quantum computing. Daneshzad and Parsanasab (2026) consider photonic quantum hardware for AI optimization, while Beghriche et al. (2026) examine photonic AI accelerators for ultra-fast wireless signal processing. Boras, Ewaniuk and Rotenberg (2026) and Saffer et al. (2026) further demonstrate photonic neural and memory/signal-processing directions. This stream suggests that quantum and photonic resources should be scheduled dynamically according to task criticality, latency, error rate and energy cost rather than treated as continuously available accelerators.

Security research adds another dimension. Anchuri et al. (2026) develop lightweight cryptographic proofs of inference for verifiable AI. Li, Xie and Iqbal (2026) propose a quantum-enabled resilient and secure V2X framework, while Alrowaili et al. (2026) evaluate post-quantum cryptography across IoT–edge–cloud layers. These works support integrity attestation for model outputs, messages and control decisions. In a safety-critical distributed setting, fault tolerance without provenance can mask adversarial failure; conversely, cryptographic assurance without control-theoretic fallback cannot guarantee safe physical behavior.

Finally, the supplied IJAIRI papers offer complementary safety and validation concepts: quantum-limited sensing-to-action for autonomous robots (Pasupuleti 2025b), quantum machine-learning test oracles for mobile robots (Pasupuleti 2021a), control-theoretic AI safety (Pasupuleti 2021b), QML-based edge anomaly detection (Pasupuleti 2023a), and safe reinforcement learning within digital-twin/HIL control (Pasupuleti 2023b). These strands collectively motivate a digital assurance loop in

which faults are detected, emulated, predicted, verified, contained and recovered across computational and physical layers.

Table 1. Literature-to-architecture synthesis.

Literature stream	Representative supplied sources	Contribution to proposed framework
Fault-tolerant photonic quantum computing	Ostmann et al. (2026); Renault et al. (2025); Nelson et al. (2025)	Logical reliability, photonic architecture, memory/error management
Distributed fault-tolerant control	Zhang et al. (2025); Yu et al. (2025); Qi et al. (2026)	Reconfiguration, event triggering, nonfragile control under faults/attacks
AI-native distributed edge	Karachalios et al. (2023); Wang et al. (2026); Xu et al. (2024)	Hierarchical intelligence placement, resilient edge operation
Quantum–AI / photonic acceleration	Gu et al. (2026); Bożejko et al. (2026); Beghriche et al. (2026)	Adaptive resource scheduling, low-latency inference/optimization
Cyber assurance and verification	Anchuri et al. (2026); Alrowaili et al. (2026); Li et al. (2026)	Proofs, post-quantum security, resilient communication
Digital-twin and safe autonomy	Pasupuleti (2021a, 2021b, 2023a, 2023b, 2025b)	Test oracles, safe RL, anomaly detection, sensing-to-action assurance

2.1 Conceptual Framework

The conceptual framework defines six interacting constructs. Quantum Reliability (QR) represents logical error suppression, syndrome stability and usable quantum resource margin. Photonic Emulation Fidelity (PEF) represents the agreement between predicted/emulated photonic circuit behavior and observed hardware behavior. AI Robustness (AIR) captures inference stability, uncertainty calibration, adversarial tolerance and policy consistency. Network Resilience (NR) represents connectivity, consensus continuity, packet-loss tolerance and secure routing. Control

Stability (CS) represents bounded state error, robust tracking and safe-mode controllability. Cyber Assurance (CA) represents authentication, integrity, post-quantum protection and, where available, verifiable inference.

The mechanism is explicitly cross-layer. QR and PEF influence the trust assigned to a quantum-assisted decision. AIR converts sensor state into predicted outcomes and control actions. NR determines whether distributed agents can share trust evidence and reach consensus. CS constrains every candidate action through a safety envelope, while CA protects the evidence and command path. The expected outcome is mission resilience: the probability that the network preserves a defined safe and useful operating region despite faults, disturbances or attacks.

The framework assumes that no single subsystem is unconditionally trusted. Instead, each subsystem provides a confidence score and an uncertainty estimate. A supervisory policy then allocates computation and control among three modes: quantum-assisted mode when quantum/photonic confidence is high; photonic-emulated/classical mode when quantum execution is degraded but the surrogate remains trustworthy; and deterministic safe mode when uncertainty or attack indicators exceed a threshold. This architecture converts fault tolerance from a passive redundancy feature into an active decision process.

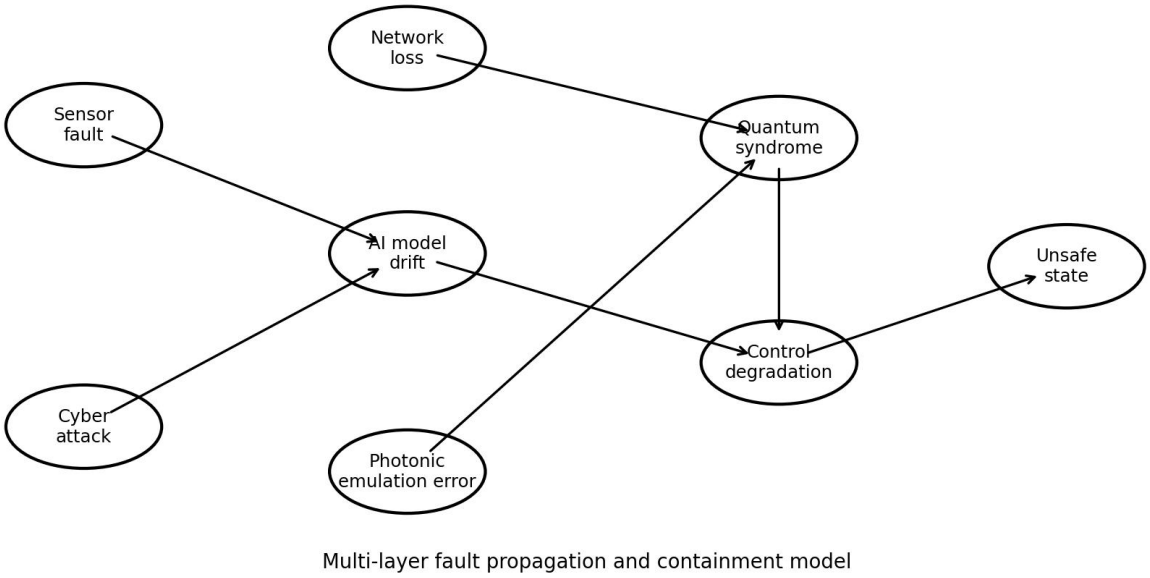


Figure 2. Cross-layer fault-propagation and containment model.

2.2 Research Gap

The theoretical gap is the absence, within the supplied literature, of a single resilience model that couples logical quantum reliability with autonomous CPS stability. Existing quantum fault-tolerance studies primarily optimize logical computation, while control studies primarily assume classical computational substrates. The methodological gap concerns co-simulation: there is limited integration of photonic circuit emulation, quantum health indicators, AI uncertainty and physical plant dynamics in one closed-loop validation environment. The empirical gap is that representative studies address specific platforms—vehicles, UAVs, grids, smart-city edge systems or photonic quantum architectures—without a general cross-domain validation protocol.

The sectoral gap concerns transferability. Safety-critical sectors increasingly use similar edge-to-cloud and multi-agent patterns, but resilience metrics remain domain-specific. A normalized cross-layer index can support comparative engineering without pretending that all domains have identical safety thresholds. The policy and governance gap concerns accountability in autonomous hybrid systems: when a control decision depends on a quantum-assisted optimization or AI inference, designers need auditable evidence about model confidence, computational mode, failover trigger and final safety filter. The proposed framework addresses these gaps conceptually, while recognizing that empirical confirmation requires hardware and field data.

3. Methodology

The study uses a design-science and model-based systems methodology. The unit of analysis is a distributed autonomous node embedded in a wider CPS network. Each node is represented by a physical plant, sensing layer, edge estimator, AI policy, photonic circuit emulator, optional quantum processing module, network/consensus module, cyber-assurance layer and safety controller. The paper does not report a field experiment. This paper proposes a model-based analytical framework and uses numerical scoring for demonstration; empirical validation requires real-world data collection.

Data sources for future validation should include synchronized sensor telemetry, actuator commands, packet traces, AI uncertainty measures, photonic device telemetry, quantum execution logs, error-syndrome or logical error estimates, energy consumption, latency and safety events. Sampling should be episode-based, covering normal operation and designed fault-injection scenarios. Recommended scenarios include sensor bias, actuator saturation, packet loss, Byzantine or compromised agents, AI distribution shift, photonic phase/amplitude drift, quantum-resource degradation and simultaneous multi-layer faults. Stratified scenario sampling should ensure that rare but severe compound faults are not diluted by normal operating episodes.

The analytical strategy comprises: (i) state-space modelling of physical and computational states; (ii) a reliability layer based on component and correlated-fault probabilities; (iii) Bayesian or uncertainty-aware fusion of health indicators; (iv) constrained optimization for mode selection and control; (v) graph-based consensus for distributed agents; and (vi) simulation/HIL validation against safety, reliability, latency and resource metrics. The architecture can be implemented with Python/Qiskit for quantum experimentation, photonic simulation or circuit-emulation tools, MATLAB/Simulink for plant and controller modelling, and NS-3 or equivalent network simulation. These software examples are implementation pathways rather than evidence of empirical execution in this paper.

Table 2. Proposed data and variables.

Variable	Definition	Scale / indicator	Expected effect	Relevance
QR	Quantum reliability	0–10; logical-error margin, syndrome stability	Positive	Determines trust in quantum-assisted computation
PEF	Photonic emulation fidelity	0–10; emulator–hardware agreement	Positive	Enables predictive validation and failover
AIR	AI robustness	0–10; calibrated confidence, drift tolerance	Positive	Reduces unstable or adversarial decisions
NR	Network	0–10; availability,	Positive	Maintains distributed

Variable	Definition	Scale / indicator	Expected effect	Relevance
	resilience	consensus continuity		coordination
CS	Control stability	0–10; bounded tracking/state error	Positive	Direct physical-safety determinant
CA	Cyber assurance	0–10; integrity, authentication, PQ protection	Positive	Prevents malicious fault masquerading
FI	Fault intensity	0–1; weighted fault severity	Negative	Stress variable for resilience testing
L	Control-cycle latency	ms	Negative beyond deadline	Real-time feasibility constraint
E	Energy cost	normalized or J/cycle	Negative in constrained setting	Resource/sustainability constraint
MR	Mission resilience	0–1 or 0–10	Outcome	Probability/score of safe useful operation

3.1 Mathematical Framework

Let x(t) denote the physical plant state, z(t) the computational health state, u(t) the applied control action, d(t) an exogenous disturbance, a(t) a cyber-adversarial input and m(t) the selected computational mode. The cross-layer system is represented as an augmented hybrid state model. The physical state evolves continuously or at a fast sampled rate, while m(t) switches among quantum-assisted, emulated/classical and deterministic-safe modes.

$$\xi(t) = [x(t)^T, z(t)^T]^T, \quad \xi(t) = F_m \xi(t) + G_m u(t) + D d(t) + H a(t) + w(t) \quad (1)$$

Here $\xi(t)$ is the augmented state; F_m and G_m are mode-dependent system and input matrices; D and H map environmental and adversarial disturbances; and w(t) is process uncertainty. The computational health vector may be written as z(t) = [q(t),

p(t), rAI(t), rN(t), rC(t)]^T for quantum, photonic, AI, network and cyber-health indicators.

For a distributed network of N autonomous nodes, the stacked state X(k) can be expressed using graph coupling. Let A be the adjacency matrix and Lg = Dg − A the graph Laplacian. Consensus and state alignment are modelled by:

$$X(k+1) = (I_N \otimes A_o - \eta L_g \otimes K_c)X(k) + (I_N \otimes B_o)U(k) + \Omega(k) \quad (2)$$

where A_0 and B_0 are local dynamics, η is the consensus gain, Kc is the coupling/control matrix, ⊗ is the Kronecker product and Ω(k) aggregates faults, noise and attacks. Stability can be studied through eigenvalue or Lyapunov conditions on the switched closed-loop matrices.

Photonic circuit emulation is treated as a surrogate mapping from control/configuration θ and input s to a predicted observable ŷp. The mismatch ep between emulator and measured photonic/quantum output becomes a diagnostic signal:

$$\hat{y_p}(k) = P_\varphi(s(k), \theta(k)), e_p(k) = y_p(k) - \hat{y_p}(k) \quad (3)$$

where φ is the calibrated photonic emulation model parameterized by φ. A persistent increase in ||ep|| signals drift, component degradation or unmodelled operating conditions and lowers PEF.

The AI-augmented controller selects both action and computational mode by minimizing expected multi-objective cost under safety constraints:

$$min_{u,m} E[\Sigma_{\tau=0}^{T}(x^T Q x + u^T R u + \lambda_1 C_q(m) + \lambda_2 L(m) + \lambda_3 E(m) + \lambda_4 R_f(m))] \quad (4)$$

$$\text{subject to } x(k) \in S_safe, P(failure|z(k), m(k)) \leq \varepsilon, L(m) \leq L_max \quad (5)$$

Q and R penalize state deviation and control effort; Cq is quantum-resource cost; L is latency; E is energy; Rf is fault risk; λi are policy weights; safe is the certified safety set; and ε is the maximum acceptable conditional failure probability.

A risk-adjusted mission outcome can be represented by a logistic prediction equation:

$$P(MR=1)=\sigma(\beta_0+\beta_1 QR+\beta_2 PEF+\beta_3 AIR+\beta_4 NR+\beta_5 CS+\beta_6 CA-\beta_7 FI-\beta_8 L) \quad (6)$$

where $\sigma(v) = 1/(1 + e^{(} - v))$. For descriptive scoring before empirical calibration, the paper uses a weighted index rather than estimated β coefficients:

$$FTQIRI = 0.20QR + 0.15PEF + 0.17AIR + 0.15NR + 0.20CS + 0.13CA \quad (7)$$

All component values in Equation (7) are normalized to 0–10. The weights sum to one and intentionally emphasize quantum reliability and physical control stability. They are normative demonstration weights, not empirically estimated parameters.

A simple reliability block approximation for partially redundant computational pathways is:

$$R_path = 1 - (1 - R_qR_p)(1 - R_e)(1 - R_s) \quad (8)$$

where RqRp is the usable quantum-photonic path reliability, Re is the emulated/classical fallback reliability and Rs is the deterministic safe-controller reliability. Equation (8) assumes conditional independence for illustration; real systems should model common-cause failures with copulas, Bayesian networks or fault trees.

Finally, a Lyapunov safety condition can be imposed for each admissible mode. With $V(x)=x^TPx$, $P > 0$, the controller seeks a mode/action such that $\Delta V \leq -\alpha\|x\|^2$ outside a small invariant set. This makes AI or quantum optimization advisory unless the selected action passes the stability filter.

3.2 Numerical Model for Better Insight

An illustrative normalized example demonstrates the FTQIRI calculation. The proposed architecture is assigned QR=8.7, PEF=8.5, AIR=8.2, NR=8.3, CS=8.8 and CA=8.4. These numbers are illustrative and do not represent measured performance. Substituting into Equation (7):

$$FTQIRI = 0.20(8.7)+0.15(8.5)+0.17(8.2)+0.15(8.3)+0.20(8.8)+0.13(8.4) \quad (9)$$

$$FTQIRI = 1.740 + 1.275 + 1.394 + 1.245 + 1.760 + 1.092 = 8.506 \approx 8.51 \quad (10)$$

Using the baseline illustrative values QR=6.2, PEF=6.8, AIR=6.5, NR=6.0, CS=6.6 and CA=5.9 gives FTQIRI≈6.34. The difference of approximately 2.17 points should be interpreted as the model's expected architectural benefit under the chosen assumptions, not as an observed experimental effect. The main insight is structural: redundancy alone is insufficient unless the system can estimate confidence, switch modes and enforce safety constraints across layers.

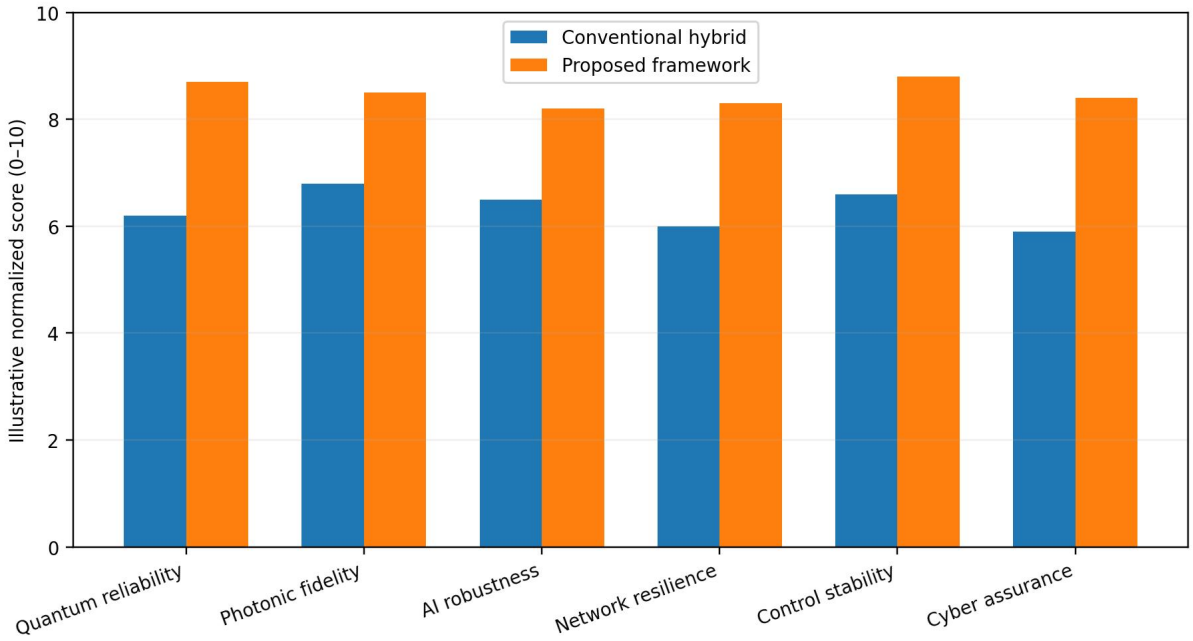


Figure 3. Illustrative cross-layer resilience scores for baseline and proposed architectures.

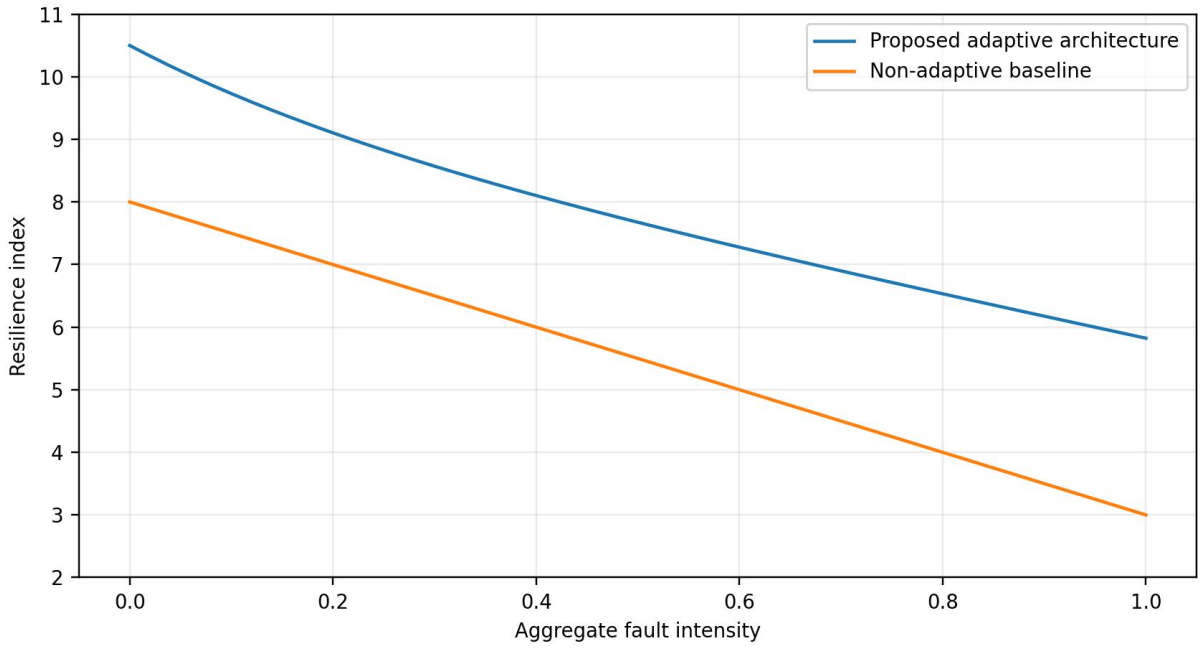


Figure 4. Illustrative sensitivity of resilience to aggregate fault intensity.

3.3 Data and Variables

The empirical dataset should be multi-rate and timestamp-aligned. Physical variables may be sampled at millisecond or sub-millisecond rates, while quantum calibration and network-security indicators may update more slowly. A common event clock should map every control action to the state estimate, computational mode, confidence vector and safety-filter outcome that produced it. Missingness should be treated as information: loss of quantum telemetry or consensus messages is itself a potential health indicator.

Measurement scales should preserve both raw engineering units and normalized analysis variables. For example, latency should remain in milliseconds for deadline analysis, but it can also be mapped to a 0–10 timeliness score. Quantum reliability can be represented by logical error probability, syndrome-event rate or successful-circuit probability depending on the implementation. Photonic fidelity may be based on phase/amplitude error, transfer-matrix distance or task-level agreement between emulation and hardware. AI robustness should include calibration error and out-of-distribution detection rather than accuracy alone.

3.4 Proposed Model / Framework

The proposed framework is named the Photonic-Emulated Fault-Tolerant Quantum Intelligence Control Framework (PEFT-QIC). PEFT-QIC is a supervisory architecture that transforms heterogeneous health evidence into a computational-mode decision and a safety-filtered control action. Its essential loop is Sense → Estimate → Emulate → Quantum/AI Decide → Verify → Safety Filter → Actuate → Audit.

At each cycle k, the framework constructs a health vector h(k)=[QR,PEF,AIR,NR,CS,CA]. It computes a risk score ρ(k), predicts candidate outcomes using the photonic/digital emulator, and chooses the least-cost admissible mode. If quantum reliability falls below τq, or emulation mismatch exceeds τp, quantum-assisted control is suspended. If AI uncertainty exceeds τAI or network consensus is unreliable, control authority is reduced or localized. When the safety barrier indicates a constraint violation, the deterministic safety controller overrides all learned or quantum-assisted actions.

$$m*(k), u*(k) = argmin_{m,u \in U_safe} J(x,h,m,u) subject to \rho(x,h,m,u) \leq \rho_max \quad (11)$$

Table 3. PEFT-QIC mode selection logic.

Operating condition	Selected mode	Primary mechanism	Fallback
Healthy quantum/photonic + high confidence	Quantum-assisted	Quantum/AI optimization with photonic verification	Emulated/classical
Quantum degradation; emulator trusted	Photonic-emulated/classical	Surrogate prediction + classical robust control	Deterministic safe
AI uncertainty or model drift	Constrained classical	Robust estimator and certified controller	Deterministic safe
Network partition	Local autonomous	Local safe policy + cached consensus state	Graceful degradation
Cyber integrity failure	Isolated safe mode	Quarantine compromised path; verified commands only	Manual/safe shutdown
Compound severe fault	Deterministic safe	Invariant-set controller; minimum-risk action	Controlled stop

3.5 Invention-Oriented Technical Structure

3.5.1 Invention Title

Fault-Tolerant Distributed Quantum Intelligence Control System with Photonic Circuit Emulation and Adaptive Safety-Constrained Failover for Autonomous Cyber-Physical Networks.

3.5.2 Research Problem

Existing autonomous CPS architectures can separately tolerate selected hardware faults, cyber disturbances or computational uncertainty, but they lack a unified mechanism that detects quantum-photonic degradation, predicts its effect on downstream AI/control decisions, and safely reallocates computational authority across distributed nodes before physical instability occurs. A further problem is that high-performance quantum-assisted or AI-generated decisions may be difficult to trust in real time because computational confidence, photonic drift and physical safety are monitored by different subsystems. The invention-oriented problem is therefore to maintain bounded and auditable autonomous control under simultaneous computational, communication, cyber and physical faults without requiring continuous availability of the quantum path.

3.5.3 Novel Architecture

The proposed architecture combines: (a) a distributed sensing and state-estimation layer; (b) a photonic circuit emulation layer that predicts quantum/photonic behavior and computes mismatch; (c) a fault-tolerant quantum processing layer exposing syndrome-derived reliability indicators; (d) an AI controller that produces candidate actions and uncertainty; (e) a distributed consensus layer for cross-node health and task allocation; (f) a cyber-assurance layer for authenticated and optionally verifiable inference/control evidence; and (g) a deterministic safety kernel that can override, degrade or isolate higher-level computation. Novelty is claimed conceptually in the closed-loop orchestration and cross-layer trust-state use, not in any individual generic component considered alone. Formal patentability requires jurisdiction-specific prior-art searching beyond this supplied corpus.

3.5.4 Independent System

A distributed autonomous cyber-physical control system comprising: a plurality of autonomous nodes each including at least one physical sensor, a state estimator and an actuator interface; a photonic circuit emulation module configured to generate an expected photonic or quantum-processing response for a candidate computational configuration; a quantum-processing module configured to execute at least one

optimization, inference or state-processing operation and output a quantum reliability indicator; an artificial-intelligence control module configured to generate a candidate control action and an uncertainty indicator; a distributed health-consensus module configured to combine node-level physical, network, artificial-intelligence, photonic and quantum health indicators; and a safety-constrained supervisory controller configured to compare an observed photonic or quantum response with the expected response, determine a computational trust state, select among a quantum-assisted operating mode, an emulated or classical operating mode, and a deterministic safe operating mode, and authorize an actuator command only when a predicted system state satisfies a predefined safety constraint.

3.5.5 Independent Method

A computer-implemented method for fault-tolerant control of a distributed autonomous cyber-physical network, the method comprising: acquiring physical-state and computational-health telemetry from a plurality of networked autonomous nodes; estimating a current physical state and a cross-layer health state; emulating, by a photonic circuit emulation module, an expected response of a selected photonic or quantum computational pathway; executing or receiving a quantum-assisted computational result and an associated reliability indicator; generating, by an artificial-intelligence controller, a candidate control action and uncertainty indicator; calculating a mismatch between an observed response and the emulated expected response; updating a fault risk value using the mismatch and the cross-layer health state; selecting a computational operating mode according to the fault risk value, latency constraint and safety constraint; filtering the candidate control action through a deterministic safety controller; distributing health or mode information to one or more peer nodes for consensus or failover; and actuating the physical system using the filtered control action while storing an auditable record of the selected mode, reliability indicators, mismatch and safety decision.

3.5.6 Dependent System

- The system/method wherein the quantum reliability indicator includes a syndrome-event rate, logical error estimate, loss estimate or resource-margin metric.

- The system/method wherein the photonic circuit emulator is continuously calibrated from measured phase, amplitude, timing or transfer-function telemetry.
- The system/method wherein a quantum-assisted result is accepted only when both a quantum-reliability threshold and an emulator-mismatch threshold are satisfied.
- The system/method wherein distributed nodes perform dynamic event-triggered health consensus to reduce communication overhead while preserving fault awareness.
- The system/method wherein a Byzantine-resilient or trust-weighted consensus rule excludes a node whose cyber-integrity or physical-health score falls below a threshold.
- The system/method wherein the AI controller uses calibrated predictive uncertainty and out-of-distribution detection to reduce or revoke control authority.
- The system/method wherein cryptographic proof or authenticated provenance is associated with an AI inference, quantum result, model version or control command.
- The system/method wherein the supervisory controller optimizes latency, energy, reliability and fault risk using a constrained multi-objective policy.
- The system/method wherein the deterministic safety controller applies a control-barrier, Lyapunov, reachability or invariant-set constraint before actuation.
- The system/method wherein a network partition causes automatic transition from distributed optimization to a local minimum-risk policy.
- The system/method wherein photonic-emulated execution is used as a shadow mode to compare against the active quantum or AI decision path before failover.
- The system/method wherein the audit record stores cross-layer health scores, selected mode, failover reason, safety-filter intervention and resulting physical state.
- The system/method wherein task scheduling allocates quantum, photonic and classical resources according to mission criticality and computational trust state.
- The system/method wherein multiple autonomous vehicles, robots, grid controllers or industrial agents share fault evidence and coordinate recovery actions.

- The system/method wherein post-quantum cryptographic protection is applied to node authentication, health telemetry or control-message integrity.

4. Results and Analysis

Because no experimental dataset was supplied, the results are analytical and scenario-based. The principal result is a set of testable propositions derived from the PEFT-QIC model. First, resilience should improve when computational health is explicitly included in control-state estimation. A controller that knows only the physical state cannot distinguish a genuine physical disturbance from a corrupted or low-confidence computational recommendation. Second, photonic emulation should reduce unsafe mode-switch delay by providing a precomputed or rapidly evaluated shadow estimate of quantum/photonic behavior. Third, distributed consensus should improve fault localization when multiple agents observe overlapping environment and network conditions, provided that consensus itself is protected against compromised agents.

The illustrative FTQIRI comparison gives 8.51 for the proposed architecture and approximately 6.34 for the conventional baseline. Decomposing the increase shows that no single factor dominates; the architecture benefits from jointly raising quantum reliability, photonic observability, AI robustness, network continuity, control stability and cyber assurance. This is consistent with the supplied literature, which treats fault tolerance and resilience as multi-mechanism problems rather than single-point corrections (Qi et al. 2026; Li & Zhang 2026; Xu, Nagothu & Chen 2024).

Sensitivity analysis in Figure 4 models increasing aggregate fault intensity. The proposed architecture retains a higher resilience trajectory because it can reconfigure computational mode and control authority. The baseline degrades approximately linearly because it lacks explicit adaptive failover. This curve is illustrative, but it defines an empirical hypothesis: under controlled fault injection, a cross-layer supervisory architecture should have a lower resilience-loss slope than a fixed-path architecture.

Latency creates a countervailing trade-off. More verification, consensus and emulation can increase decision time. Figure 5 therefore depicts an illustrative reliability–latency frontier. Very low latency may require reduced assurance, while very high assurance may exceed real-time deadlines. The optimization problem in

Equation (4) is intended to locate an application-specific compromise. In hard real-time systems, the deterministic safe controller must remain faster than the high-level quantum/AI optimization path.

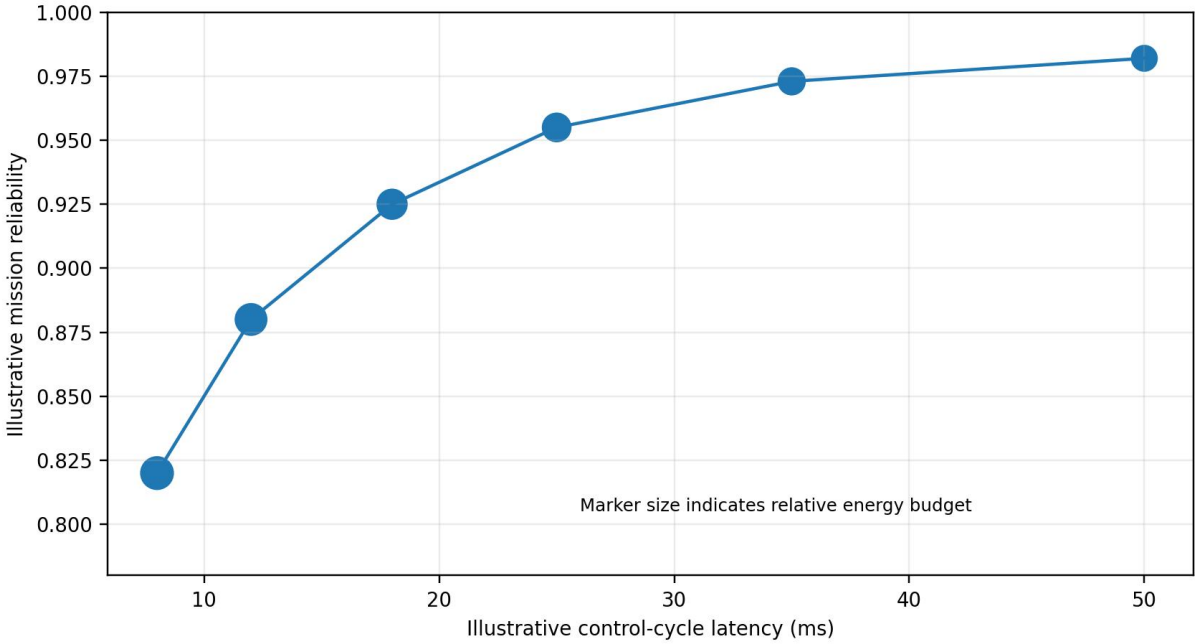


Figure 5. Illustrative latency–reliability frontier for cross-layer verification and control.

Table 4. Scenario-based analytical results and validation metrics.

Scenario	Baseline expected response	PEFT-QIC expected response	Key metric
Photonic drift	Undetected bias until task error	Emulator mismatch lowers PEF; reconfigure/calibrate	Detection delay, unsafe-action rate
Quantum error spike	Potentially degraded optimization output	QR threshold suspends quantum-assisted mode	Logical-error rate, mode-switch time
AI distribution shift	Overconfident action possible	Uncertainty threshold restricts AI authority	Calibration error, OOD detection rate
Network partition	Loss of centralized coordination	Local minimum-risk mode; later consensus	Mission continuity,

Scenario	Baseline expected response	PEFT-QIC expected response	Key metric
		recovery	consensus recovery time
Cyber command injection	Potential control corruption	Integrity check + isolation + safety filter	False-command acceptance rate
Compound sensor + network fault	Escalating state uncertainty	Cross-layer risk aggregation + controlled degradation	Maximum state deviation, recovery time

Table 5. Proposed validation metrics.

Metric	Definition	Suggested experimental calculation	Desired direction
Safe mission completion	Fraction of episodes completed without safety violation	safe completed / total episodes	Higher
Unsafe action acceptance	Candidate unsafe actions reaching actuator	unsafe actuated / unsafe proposed	Lower
Fault detection latency	Time from fault onset to confident detection	$t_{detect} - t_{fault}$	Lower
Mode-switch latency	Time from trigger to safe-mode activation	$t_{mode} - t_{trigger}$	Lower
Resilience-loss slope	Change in MR per change in fault intensity	$\Delta MR/\Delta FI$	Less negative
Control error	Tracking/state deviation under	RMSE or max norm	Lower

Metric	Definition	Suggested experimental calculation	Desired direction
	faults		
Computational trust calibration	Agreement between confidence and correctness	ECE/Brier-type score	Lower error
Energy per safe episode	Energy normalized by successful safe mission	J / safe episode	Lower subject to safety

4.1 Discussion

The theoretical contribution is the coupling of two historically separate ideas: quantum fault tolerance and cyber-physical fault-tolerant control. Quantum error correction normally seeks reliable logical operations, whereas CPS control seeks stable physical trajectories. PEFT-QIC makes logical reliability a measurable input to physical-control authority. This shifts the design question from “Is the quantum computation correct?” to “Is the computational pathway sufficiently trustworthy, timely and useful to participate in this control cycle?” Such a formulation is compatible with modular photonic architectures (Renault et al. 2025; Ostmann, Nunn & Jones 2026) and with robust CPS control under attacks (Qi et al. 2026).

The practical contribution is graceful degradation. A deployable architecture should not equate loss of quantum capability with loss of mission capability. Instead, quantum resources should enhance optimization, prediction or coordination when trustworthy, while photonic emulation and classical robust control preserve functionality during degradation. This principle is consistent with hybrid quantum-classical scheduling (Gu et al. 2026) and with distributed autonomous control where event-triggered and local decisions reduce dependence on continuous centralized communication (Yu et al. 2025).

For industry, the framework is relevant to autonomous vehicles, robotics, smart grids, industrial control, distributed sensing and future communications. The exact

safety constraints differ by domain, but the architecture supplies a transferable pattern: health-aware computation, shadow emulation, multi-path decision making, safety filtering and auditability. AI-native networks and edge architectures further support distributed placement of these functions (Karachalios et al. 2023; Wang et al. 2026; Xu, Nagothu & Chen 2024).

Policy and governance implications concern accountability. Hybrid autonomous systems may combine probabilistic AI, experimental quantum resources and safety-critical actuators. Regulators and operators may require evidence of which computational mode was active, what confidence was available, why failover occurred and whether a safety mechanism overrode an AI decision. Verifiable AI concepts (Anchuri et al. 2026) and post-quantum security across IoT–edge–cloud layers (Alrowaili et al. 2026) can support such evidence, but they do not replace engineering validation.

Ethically, designers should avoid using quantum or AI complexity as a reason to obscure responsibility. Safety-critical deployment requires explainable failure modes, human override where appropriate, cybersecurity controls, documented model limitations and conservative fallback. The architecture should be evaluated for disparate physical risks across operating environments and for systemic effects when many autonomous agents share similar models or vulnerabilities.

4.2 Supplied-Corpus Prior-Art Mapping

A structured mapping of the supplied corpus indicates that the constituent technologies are individually represented, but the specific combination proposed here should be evaluated at the claim-element level. The matrix below is not a patentability opinion; it identifies where the supplied sources appear most relevant and where the proposed combination requires further professional search.

Table 6. Preliminary prior-art mapping based only on the supplied corpus.

Claim element / feature	Closest supplied-corpus themes	Preliminary differentiation to investigate
Fault-tolerant photonic quantum execution	Ostmann et al. (2026); Renault et al. (2025);	Use of quantum/photonic health as real-time control-

Claim element / feature	Closest supplied-corpus themes	Preliminary differentiation to investigate
	Nelson et al. (2025)	authority input
Distributed CPS fault-tolerant control	Yu et al. (2025); Qi et al. (2026); Li & Zhang (2026)	Coupling with quantum reliability and emulator mismatch
Photonic circuit shadow emulation	Pasupuleti (2026c, 2026d); Beghriche et al. (2026)	Closed-loop shadow verification preceding CPS actuation
AI uncertainty + safe fallback	Pasupuleti (2021b, 2023b); Xu et al. (2024)	Three-mode supervisory selection driven by cross-layer trust state
Distributed health consensus	Karachalios et al. (2023); Wang et al. (2026)	Consensus over computational trust and physical safety variables
Verifiable / PQ-secured decision path	Anchuri et al. (2026); Alrowaili et al. (2026)	Binding provenance to mode selection and safety-filter audit record

5. Conclusion

This paper has developed a unified framework for fault-tolerant distributed quantum intelligence in autonomous cyber-physical networks. The architecture integrates fault-tolerant quantum processing, photonic circuit emulation, AI-augmented control, distributed health consensus, cyber assurance and deterministic safety filtering. Its central proposition is that computational trust must become part of the control state: quantum reliability, photonic mismatch, AI uncertainty and network integrity should directly influence how much authority a high-performance decision path receives.

The mathematical framework formalizes this idea through augmented state-space dynamics, graph-coupled distributed control, emulator mismatch, constrained multi-objective optimization, probabilistic mission resilience and an illustrative FTQIRI

index. The numerical example demonstrates transparent scoring rather than empirical proof. The invention-oriented structure identifies a technical problem—maintaining safe autonomous control under heterogeneous computational and physical faults—and proposes a supervisory architecture that can move among quantum-assisted, emulated/classical and deterministic-safe modes while retaining an auditable decision trail.

The framework's future value lies in testability. It can be instantiated in simulation, hardware-in-the-loop platforms and multi-agent testbeds, then evaluated under reproducible fault injection. The most important empirical question is whether cross-layer trust-aware failover reduces unsafe action rates and resilience-loss slopes without violating real-time latency and energy constraints. If validated, the approach could provide a common systems-engineering pattern for resilient quantum-enabled autonomy across mobility, energy, manufacturing, sensing and advanced communications.

5.1 Limitations

The principal limitation is the absence of a supplied empirical dataset or hardware experiment. All numerical scores, sensitivity curves and performance comparisons are illustrative. The weighted FTQIRI is a normative construct whose weights require expert elicitation or empirical calibration. The state-space model simplifies nonlinear, asynchronous and non-Markovian behaviors that may dominate real systems. The reliability expression assumes independence for illustration and therefore does not capture common-cause failures. Generalizability across sectors is conceptual rather than demonstrated. Quantum and photonic implementations vary substantially in hardware maturity, noise sources and timing constraints. Finally, the prior-art mapping is restricted to the supplied reference corpus and is not a substitute for a comprehensive patent database search, legal claim chart or jurisdiction-specific patentability analysis.

5.2 Future Research Directions

- Build a hardware-in-the-loop PEFT-QIC demonstrator coupling physical plant simulation, photonic emulation, quantum-circuit execution and real-time safety filtering.

- Estimate FTQIRI weights using Delphi expert elicitation, Bayesian hierarchical modelling or multi-criteria decision analysis across sectors.
- Develop common-cause fault models linking photonic loss, network congestion, power disturbance and AI model drift rather than assuming independent failures.
- Investigate formal verification of mode switching using hybrid automata, control barrier functions, reachability analysis and temporal logic.
- Benchmark quantum-assisted scheduling and optimization against classical heuristics under strict latency, energy and reliability budgets.
- Develop Byzantine-resilient health-consensus protocols that distinguish malicious nodes from legitimately degraded nodes.
- Integrate verifiable inference and post-quantum identity mechanisms into the audit chain for safety-critical distributed autonomy.

Conduct domain-specific validation in multi-UAV coordination, smart-grid control, industrial robotics and autonomous mobility with standardized fault-injection suites.

References

Ostmann, M, Nunn, J & Jones, AE 2026, 'Nonlinear photonic architecture for fault-tolerant quantum computing', Physical Review A, vol. 114, no. 1, accessed <http://dx.doi.org/10.1103/s3dr-tsbg>.

Zhang, S, Ifqir, S & Puig, V 2025, 'Robust LPV Fault Tolerant Tracking Control Using Set-Based Approaches for Autonomous Vehicles', 2025 6th International Conference on Control and Fault-Tolerant Systems (SysTol), pp. 240–245, accessed <http://dx.doi.org/10.1109/systol66549.2025.11267365>.

Yu, Z, Hu, Y, Wang, Y, He, Y, Zhang, X, Yang, H & Yu, Z 2025, 'Distributed Fault-Tolerant Control for Multi-UAVs Based on Dynamic Event-Triggered Mechanism', 2025 Joint International Conference on Automation-Intelligence-Safety (ICAIS) & International Symposium on Autonomous Systems (ISAS), pp. 1–6, accessed <http://dx.doi.org/10.1109/icaisisas64483.2025.11051601>.

Nelson, J, Bentsen, G, Flammia, ST & Gullans, MJ 2025, 'Fault-tolerant quantum memory using low-depth random circuit codes', Physical Review Research, vol. 7, no. 1, accessed <http://dx.doi.org/10.1103/physrevresearch.7.013040>.

Renault, P, Yard, P, Pooser, RC, Eaton, M & Zaidi, HA 2025, 'End-to-end switchless architecture for fault-tolerant photonic quantum computing', Quantum, vol. 9, p. 1796, accessed <http://dx.doi.org/10.22331/q-2025-07-14-1796>.

Qi, W, Shen, F, Zong, G, Su, S-F, Cao, J & Sun, K 2026, 'Nonfragile Fault-Tolerant Control for Power Cyber-Physical Systems With Cyber Attacks', IEEE Transactions on Cybernetics, vol. 56, no. 4, pp. 2402–2407, accessed <http://dx.doi.org/10.1109/tcyb.2025.3634154>.

Anchuri, P, Campanelli, M, Cesaretti, P, Gennaro, R, Jois, TM, Kayman, HS & Ozdemir, T 2026, 'Towards Verifiable AI with Lightweight Cryptographic Proofs of Inference', 2026 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), pp. 955–977, accessed <http://dx.doi.org/10.1109/satml68715.2026.00058>.

Wang, Q, Dan, D, Li, Z, Wu, C & Wang, J 2026, 'Terminal-Edge-Cloud Collaborative AI-Native Network Towards 6G', 2026 Global 6G Conference (Global 6G), pp. 1–6, accessed <http://dx.doi.org/10.1109/global6g69473.2026.11566897>.

Karachalios, OA, Zafeiropoulos, A, Kontovasilis, K & Papavassiliou, S 2023, 'Distributed Machine Learning and Native AI Enablers for End-to-End Resources Management in 6G', Electronics, vol. 12, no. 18, p. 3761, accessed <http://dx.doi.org/10.3390/electronics12183761>.

Gu, Y, Dai, S, Liu, C, Wang, Q-L & Cheng, L 2026, 'Hybrid quantum-classical reinforcement learning for scheduling systems', Quantum Computational AI, pp. 117–133, accessed <http://dx.doi.org/10.1016/b978-0-44-330259-6.00015-3>.

Bożejko, W, Trotskyi, S, Uchroński, M & Wodecki, M 2026, 'Optimizing two-machine scheduling in flexible manufacturing systems using autonomous AI and quantum computing', Neurocomputing, vol. 664, p. 132067, accessed <http://dx.doi.org/10.1016/j.neucom.2025.132067>.

Chen, H, Zhang, Y, Zhou, H, Park, T, Sun, W, Kim, K-N, Huang, H, Park, Y-L & Lee, T-W 2026, 'Self-adaptive all-photonic synapse for autonomous neuromorphic robots', Nano Energy, vol. 154, p. 111983, accessed <http://dx.doi.org/10.1016/j.nanoen.2026.111983>.

Xu, R, Nagothu, D & Chen, Y 2024, 'AR-Edge: Autonomous and Resilient Edge Computing Architecture for Smart Cities', Edge Computing Architecture - Architecture and Applications for Smart Cities, accessed <http://dx.doi.org/10.5772/intechopen.1005876>.

Asim, M, Junhong, C, Wenyin, L & Abd El-Latif, AA 2023, 'Artificial Intelligence-Based Secure Edge Computing Systems for IoTDs and Smart Cities: A Survey', Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities, pp. 155–173, accessed <http://dx.doi.org/10.1007/978-3-031-51097-7_13>.

Li, S, Xie, Y & Iqbal, M 2026, 'QuanReS: A Hybrid Quantum-Enabled Resilient and Secure V2X Communications Framework in Smart Cities', IEEE Transactions on Consumer Electronics, vol. 72, no. 2, pp. 3940–3948, accessed <http://dx.doi.org/10.1109/tce.2025.3647004>.

Alrowaili, A, Ozmen, SC, Kazim, M & Rehman, MU 2026, 'Post-Quantum Cryptography for Smart City Cybersecurity: An Evaluation of PQC Algorithms Across IoT–Edge–Cloud Layers', IET Smart Cities, vol. 8, no. 1, accessed <http://dx.doi.org/10.1049/smc2.70040>.

Li, J & Zhang, Y 2026, 'Cyberattack Detection, Fault Estimation, and Fault-Tolerant Control of Smart-Grid Cyber-Physical Systems', IET Smart Energy Systems, vol. 2, no. 2, pp. 102–119, accessed <http://dx.doi.org/10.1049/ses2.70028>.

Ahmadi, M, Aly, H & Gu, J 2026, 'A comprehensive review of AI-driven approaches for smart grid stability and reliability', Renewable and Sustainable Energy Reviews, vol. 226, p. 116424, accessed <http://dx.doi.org/10.1016/j.rser.2025.116424>.

Beghriche, A, Bouaita, B, Benmessahel, B, Berrhail, F & Seghir, F 2026, 'Photonic AI Accelerators for Ultra-Fast Wireless Signal Processing in 6G Networks', Traitement du Signal, vol. 43, no. 1, pp. 27–51, accessed <http://dx.doi.org/10.18280/ts.430103>.

Daneshzad, S & Parsanasab, G-M 2026, 'Photonic Quantum Hardware for AI Optimization Tasks', 2026 International Interdisciplinary Conference on Artificial Intelligence: Engineering, Health, Finance and Humanities (IICAI), pp. 1–6, accessed <http://dx.doi.org/10.1109/iicai70155.2026.11620969>.

Boras, I, Ewaniuk, J & Rotenberg, N 2026, 'Quantum photonic neural networks in time', Optica Quantum, accessed <http://dx.doi.org/10.1364/opticaq.603710>.

Saffer, O, Marines Cabello, JH, Slinkov, G, Becker, S, Geilen, A & Stiller, B 2026, 'Brillouin-based memory and signal processing for photonic neuromorphic computing', in M Notomi & T Zhou (eds.), AI and Optical Data Sciences VII, p. 61, accessed <http://dx.doi.org/10.1117/12.3077887>.

Pasupuleti, MK 2026a, 'Photonic-Interconnected Quantum Chiplets for Modular and Networked Quantum Computing', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 06, no. 05, pp. 264–300, accessed <http://dx.doi.org/10.62311/nesx/rp9-30052026>.

Pasupuleti, MK 2026b, 'Topological Quantum Error Correction with Tensor-Network Optimization for Scalable Photonic Quantum Computing Architectures', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 06, no. 06, pp. 1–35, accessed <http://dx.doi.org/10.62311/nesx/rpj1-30062026>.

Pasupuleti, MK 2026c, 'Quantum Signal Processing for Fault-Tolerant Photonic Computing and Quantum-Enhanced Scientific Intelligence', International Journal

of Academic and Industrial Research Innovations (IJAIRI), vol. 06, no. 07, pp. 1–48, accessed <http://dx.doi.org/10.62311/nesx/rp1jy-30072026>.

Pasupuleti, MK 2026d, 'Topological Photonics for Neuromorphic Computing, Quantum Communications and Ultralow-Power Edge Intelligence', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 06, no. 07, pp. 92–141, accessed <http://dx.doi.org/10.62311/nesx/rp3jy-30072026>.

Pasupuleti, MK 2025a, 'Fault-Tolerant Quantum Computing via Macroscopic Quantum Tunnelling in Superconducting Circuits', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 05, no. 12, National Education Services, pp. 1–21, viewed <http://dx.doi.org/10.62311/nesx/rp-dec-p1-2025>.

Pasupuleti, MK 2025b, 'Quantum-Limited Sensing-to-Action for GPS-Denied Navigation in Autonomous Robots', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 05, no. 12, National Education Services, pp. 264–290, viewed <http://dx.doi.org/10.62311/nesx/rp-dp1225>.

Pasupuleti, MK 2023a, 'QML for Edge Anomaly Detection: Variational Circuits on MQTT/NS-3 Stream', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 03, no. 12, National Education Services, pp. 174–188, viewed <http://dx.doi.org/10.62311/nesx/rp-301223-174-188>.

Pasupuleti, MK 2023b, 'AI Digital Twins in Simulink: Safe RL for Hardware-in-the-Loop Control', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 03, no. 06, National Education Services, pp. 114–125, viewed <http://dx.doi.org/10.62311/nesx/rp-30623-114-125>.

Pasupuleti, MK 2021a, 'Verifying Autonomous Mobile Robots with Quantum Machine Learning Test Oracles', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 01, no. 01, National Education Services, pp. 259–272, viewed <http://dx.doi.org/10.62311/nesx/rp-1-03-25>.

Pasupuleti, MK 2021b, 'A Control-Theoretic Framework for AI Safety: Stability, Robustness, and Assurance', International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 01, no. 01, National Education Services, pp. 303–315, viewed <http://dx.doi.org/10.62311/nesx/rp-1-06-2021>.