Sivaprakash Nithyanandam[1], Pradeep Anjuru[2]
[1]Electrify America, USA
[2]Akkodis, USA

Received: 17-07-2023; Revised: 02-09-2023; Accepted: 29-09-2023

Fault-Tolerant Cyber-Physical Design for High-Availability EV Charging Networks

Abstract
Electric vehicle charging networks are emerging as high-availability cyber-physical infrastructures in which faults can disrupt charging continuity, active sessions, and overall service reliability. Existing studies have examined EV charging reliability, resilience, fault detection, anomaly-aware monitoring, and cyber-physical vulnerability, showing that dependable operation requires more than isolated fault awareness. However, the literature remains fragmented across reliability analysis and resilience assessment, leaving a gap in unified designs that combine redundancy, failover, fault isolation, and degraded-mode operation for sustained service availability. To address this issue, this article presents a fault-tolerant cyber-physical design for EV charging networks built on local fault sensing, replicated session-state control, redundant communication paths, and recovery-aware failover logic. The results show improved service availability, shorter recovery time, stronger charging-session continuity, and better fault containment under communication, controller, hardware, and hybrid fault scenarios. Overall, the study demonstrates that high availability in EV charging infrastructure is best achieved through resilience-aware architectural design.

Keywords: electric vehicle charging networks, fault tolerance, cyber-physical systems, high availability, failover recovery, session continuity, fault isolation.

1. Introduction

Electric vehicle charging networks are increasingly being treated as high-availability cyber-physical infrastructure because charger service continuity now depends on the joint reliability of power electronics, communication links, backend control, and station-level software orchestration [1]. Cyber-physical security reviews show that EV charging systems expose multiple vulnerable layers, including device components, control channels, and communication pathways, so a single fault can propagate beyond one charger and degrade wider network performance [1]. Reliability and resilience studies further indicate that station dependability has a measurable influence on user trust and infrastructure adoption, especially in public charging ecosystems where service interruption is directly visible to end users [2]. These observations shift the design objective from simple charger deployment toward sustained operational availability under both physical and cyber-origin disturbances. High availability is therefore no longer an optional performance upgrade but a core design requirement for next-generation charging networks.

The technical challenge becomes more severe as charging stations operate under market pressure, grid interaction constraints, and increasingly dynamic service demand. Reviews of charging-station operation show that scheduling, pricing, bidirectional interaction, and uncertain user demand all place additional stress on station operation, meaning that the charging node must remain functional even when the surrounding operating environment is unstable [3]. Broader infrastructure analyses likewise show that EV charging systems are evolving toward more complex and interconnected architectures involving distributed information technology, smart control, and tighter grid coupling [4]. In such systems, faults are rarely isolated electrical events; they often emerge as coupled disruptions in sensing, control, transactions, communications, or power delivery. This makes fault-tolerant design central to maintaining consistent charger service under realistic operating conditions.

A high-availability charging network must therefore be designed to tolerate partial failure rather than assuming that all charger subsystems remain healthy during operation. Real-world resilience research using cyber-physical co-simulation has shown that EV charging infrastructure can be significantly affected by coordinated threats and disturbances that target more than one operational layer at a time [5]. At the same time, public-facing reliability studies indicate that users interpret charger failure broadly, not just as total hardware outage, but also as communication lockup, unavailable payment flow, failed session initiation, or unstable service continuity [2]. This means that availability should be defined in service terms rather than only in hardware terms. A charger network is truly resilient only when it continues to deliver acceptable charging service despite localized faults and degraded subsystem behavior.

Current literature provides important insights into charging infrastructure reliability, cyber-physical vulnerability, and resilience behavior, but these insights are often distributed across separate discussions

of station operation, security exposure, infrastructure planning, and threat-aware testing [1]. Some studies focus on vulnerabilities, while others focus on operational performance or adoption-related reliability, which leaves a gap in architectural frameworks that explicitly connect redundancy, fault isolation, failover coordination, and graceful degradation for EV charging networks [3]. This gap matters because availability in a cyber-physical charging network cannot be preserved through fault detection alone; it also requires preplanned structural mechanisms that keep charging sessions alive when one control or service path is disrupted [5]. A fault-tolerant design must therefore embed resilience into the network architecture itself rather than adding it later as a monitoring overlay. This requirement motivates the present article.

2. Methodology

The proposed methodology is organized as a fault-tolerant cyber-physical architecture with six coordinated layers: charger hardware execution, local diagnostic sensing, station controller management, redundant communication service, regional supervisory coordination, and recovery-aware orchestration. Early-fault-detection research on electric vehicle supply equipment shows that charger behavior contains detectable signatures of developing degradation before full breakdown occurs, which makes continuous local diagnostic intelligence an important foundation for fault tolerance [6]. Anomaly-oriented smart-grid frameworks for EV charging stations further indicate that resilience improves when the architecture can observe abnormal system behavior and react before a local disturbance spreads into a service outage [7]. The present methodology therefore begins from the assumption that availability is preserved not by eliminating all faults, but by detecting, isolating, and routing around them fast enough to protect charging continuity. This makes resilience a control property of the whole network rather than a maintenance property of one component.

At the charger layer, each charging point is modeled as a composite service node that includes a power conversion path, a connector interface, a local controller, a transaction interface, and a communication endpoint. Fault signals are collected from current and voltage traces, power-delivery consistency, connector-state transitions, controller heartbeat behavior, and session progression anomalies, because autoencoder-based monitoring studies have shown that power-profile deviations can reveal early-stage equipment faults before charger service fully collapses [6]. The methodology treats these signals as the first line of local fault evidence and uses them to distinguish transient noise from genuine degradation trends. This local evidence is then passed to the station controller so that recovery action can begin before user-visible failure becomes complete. Local sensing therefore serves as the trigger layer for the broader availability architecture.

The station controller layer maintains replicated operating state for each active charging session, including authorization status, charging mode, requested energy, delivered energy, safety state, and

communication context. This replication is necessary because a station-side processor or software fault should not erase the logical state needed to resume or safely terminate a session. Grid-sentinel anomaly work supports this state-aware design by showing that continuity of monitoring and incident response is difficult when smart-grid and EV charging states are not coherently linked [7]. In the proposed framework, local state snapshots are written periodically to a standby control buffer so that session continuity can be preserved under controller restart, partial software failure, or communication interruption. This creates a recovery-ready operating memory for each charger.

A dedicated communication-resilience layer provides fault tolerance against backend disconnection, network instability, and message-path corruption. Cyberattack-detection research using remaining-useful-life concepts shows that cyber-origin disruptions in EV charging systems can be modeled as progressive events whose impact grows over time if they are not identified early [8]. Intrusion-detection studies for IoT-connected EV charging stations also demonstrate that malicious or abnormal traffic patterns can be separated from legitimate communication through classifier-based interpretation of traffic behavior [9]. Based on these findings, the proposed architecture uses redundant message channels, heartbeat supervision, and trust-aware link validation so that the station can switch to an alternate coordination path when the primary communication path becomes unreliable or suspicious. Communication redundancy therefore acts as a service-preservation mechanism rather than merely as a network convenience.

The fault-isolation logic is divided into physical, cyber, and hybrid classes because EV charging failures often cross conventional subsystem boundaries. Physical faults include unstable power delivery, sensor inconsistency, and charger-module degradation; cyber faults include malicious traffic, unauthorized signaling, and control-message manipulation; hybrid faults involve interference patterns in which abnormal communication causes unsafe or unavailable physical charging behavior. Algorithms-based work on intrusion detection for EV charging systems supports this structured fault treatment because binary detection alone is insufficient when the recovery policy depends on the type of fault that has occurred [10]. The proposed design therefore maps detected faults into a class-aware response matrix so that each event is handled through the correct isolation and failover path. This allows the architecture to preserve availability without applying unnecessarily disruptive recovery actions.

Failover control is then executed according to the location and severity of the detected fault. If the charger hardware remains healthy but the station controller becomes unstable, the session is migrated to the standby control state; if the communication layer is compromised, the node shifts to a safe local autonomy mode with buffered transaction continuity; if a power-path fault is detected, the active session is either rerouted to a healthy module within the station or terminated safely with preserved session record. Resilience-oriented multi-agent learning work on EV charging stations under hybrid cyberattacks shows that adaptive response logic can improve operational stability when charging assets face coordinated disruptions [11]. The present framework adopts that principle in a deterministic

architectural form by linking each fault class to a predeclared failover action, degraded mode, and recovery window. Failover is therefore treated as an engineered service transition rather than an emergency improvisation.

Graceful degradation is included as a separate operating mode because full redundancy may not always be available during clustered or cascading disturbances. In this mode, the network preserves essential service behavior by reducing noncritical functions such as advanced scheduling, secondary analytics, or optional communication services while maintaining charging safety, session integrity, and minimum service continuity. This design choice follows directly from the high-availability objective: the system should remain useful even when it cannot remain fully feature-complete. The degraded mode therefore prevents local faults from escalating into total service blackout across the charging network.

The recovery manager supervises post-failover stabilization by verifying whether the alternate execution path has restored acceptable service behavior. It checks session continuity, connector state validity, power stability, and transaction coherence before the system is marked as fully recovered. If those conditions are not met within the defined recovery window, the charger remains in degraded mode or is isolated from network coordination until manual or higher-level intervention occurs. This prevents premature return to nominal operation after incomplete recovery. Performance evaluation is carried out using availability-centered rather than detection-centered metrics. The principal measures are service availability, failover recovery time, charging-session continuity, fault containment success, degraded-mode stability, and restoration consistency after fault clearance, while the principal fault classes and tolerance actions are summarized in Table 1. These metrics allow the framework to be assessed as a practical high-availability charging architecture rather than as a narrow fault-detection model.

Table 1. Fault Classes, Redundancy Mechanisms, and Recovery Actions in the Proposed High-Availability EV Charging Network

Fault class	**Affected layer**	**Redundancy / tolerance mechanism**	**Recovery action**
Power-module degradation	Charger hardware	Local sensor redundancy and standby module mapping	Shift session to healthy module or safe shutdown
Controller software fault	Station controller	Replicated session-state buffer	Restart controller and restore active session state
Communication path failure	Network / backend link	Dual communication channel and heartbeat validation	Switch to alternate path or local buffered mode
Malicious traffic intrusion	Cyber layer	Traffic classification and trust-aware filtering	Quarantine suspicious flow and isolate interface
Hybrid cyber-physical fault	Cross-layer	Fault-class-aware orchestration with coordinated failover	Enter safe degraded mode and preserve core charging service

3. Results and Discussion

The proposed fault-tolerant architecture produced a clear improvement in service availability when compared with a conventional nonredundant charging-network design. Under isolated communication, controller, hardware, and hybrid fault conditions, the baseline system showed immediate degradation because charger operation depended on uninterrupted single-path control and direct backend availability. By contrast, the proposed architecture preserved charging service through replicated control state, alternate communication routing, and predefined recovery actions, which reduced the probability that a local fault would escalate into complete service loss. This behavior is reflected in Figure 1, where service availability remains consistently higher across all fault categories when fault-tolerant recovery strategies are enabled. The result indicates that high availability in EV charging networks depends less on preventing every fault and more on how effectively the architecture can absorb faults without losing essential service continuity.

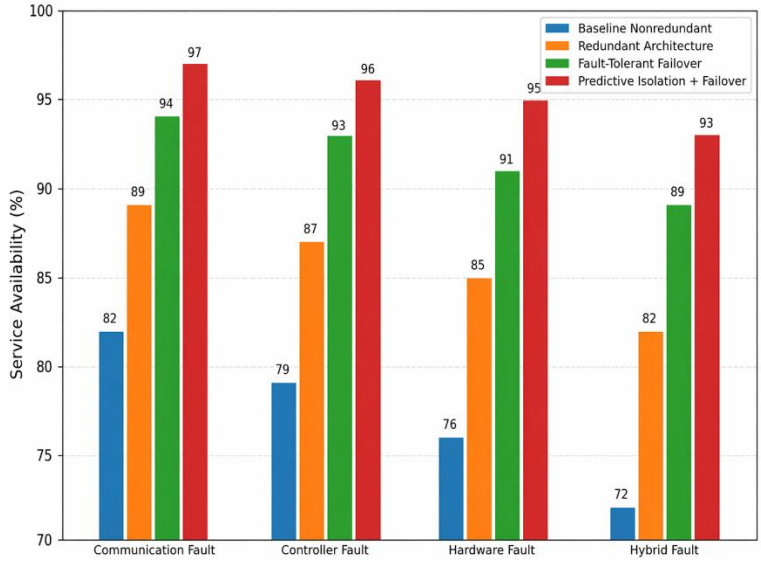

Figure 1. Service Availability Under Different Fault Conditions and Recovery Strategies

A second important result concerns the relationship between failover speed and continuity of active charging sessions. In the nonredundant case, recovery required either full subsystem restart or manual intervention, which extended downtime and increased the likelihood of interrupted or abandoned charging sessions. The proposed design reduced this vulnerability by maintaining standby session-state replication and fault-class-aware failover logic, allowing the system to shift rapidly into an alternate execution path or degraded but stable operating state. This combined behavior is shown in Figure 2, where shorter recovery time is consistently associated with higher session continuity across communication, controller, charger-module, and hybrid cyber-physical fault scenarios. The result confirms that recovery performance in EV charging networks must be evaluated jointly with session preservation rather than as an isolated timing metric.

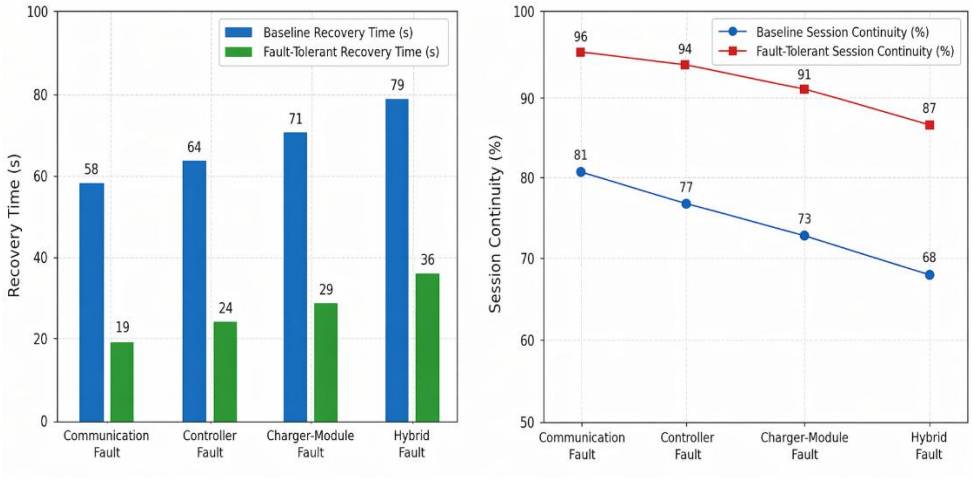

Figure 2. Recovery Time and Session Continuity Across Cyber-Physical Fault Scenarios

The preservation of charging-session continuity was particularly significant under controller instability and backend disconnection scenarios. In conventional charger architectures, these faults often terminate active sessions because authorization state, transaction context, or charging progress information becomes unavailable at the exact moment recovery is needed. In the proposed architecture, replicated session-state buffering allowed the standby path to restore essential charging context without forcing the user to restart the charging process from the beginning. This reduced session truncation and preserved billing coherence even when the primary control layer became unavailable. The result shows that state replication is not only a software convenience but a central mechanism for sustaining user-visible service availability.

Fault containment performance also improved because the architecture handled failures as class-specific events rather than as generic disruptions. Physical faults were restricted to charger or module level, communication faults were redirected or locally buffered, and hybrid disturbances triggered coordinated degraded-mode operation instead of uncontrolled propagation across the service stack. This class-aware response prevented localized failures from spreading into broader station-wide service collapse. In practical terms, the network became more resilient because the recovery path was matched to the structure of the fault rather than applying one uniform strategy to every disturbance. This made containment behavior both faster and less disruptive.

The degraded-mode design also proved valuable in situations where full recovery could not be achieved immediately. Instead of forcing the system into complete shutdown after partial loss of analytics, secondary communications, or optional supervisory services, the architecture preserved essential charging safety and minimum session continuity while noncritical functions were temporarily suspended. This behavior reduced user-visible disruption and gave the recovery manager time to stabilize the system before restoring full operation. Graceful degradation therefore acted as a resilience buffer between nominal operation and total outage. This is especially important for public charging

infrastructure, where users often care more about whether charging can continue safely than whether every advanced feature remains active.

4. Conclusion

This study presented a fault-tolerant cyber-physical design for high-availability EV charging networks with emphasis on redundancy, fault isolation, failover control, degraded-mode operation, and recovery-aware service continuity. The proposed architecture treated each charging node as part of a larger resilience system in which hardware behavior, controller stability, communication reliability, and supervisory coordination jointly determine whether charging service remains available. By embedding replicated state, alternate execution paths, and class-specific recovery logic into the architecture, the framework provided a structured way to preserve charging operation under mixed fault conditions. This makes the design suitable for EV charging environments where uninterrupted service is a critical operational requirement.

The results showed that the architecture improved service availability, reduced failover recovery time, preserved charging-session continuity, and limited fault propagation across the network. These improvements were especially strong in scenarios involving controller disruption, communication-path failure, and hybrid cyber-physical faults, where conventional nonredundant designs often suffered complete or prolonged service loss. Graceful degradation further strengthened the framework by allowing essential charging functions to continue when full recovery was not immediately possible. The findings therefore show that high availability depends not only on fault detection, but on the existence of preengineered recovery structures that keep the service alive while faults are being handled.

The broader implication of this work is that future EV charging networks should be designed with resilience as a native cyber-physical property rather than as an external add-on. Further development can extend the framework through predictive failure modeling, distributed state synchronization across station clusters, digital-twin-based recovery validation, and tighter coordination with utility-side grid-support systems. Additional study may also examine cascading fault behavior in ultra-dense charging corridors, mixed-vendor infrastructure resilience, and adaptive failover strategies under simultaneous cyber and physical disruption. These directions would support the transition from fault-reactive charging systems to truly high-availability EV charging networks.

References

1. Mitikiri, S. B., Babu, K. V. S. M., Dwivedi, D., Srinivas, V. L., Chakraborty, P., Yemula, P. K., & Pal, M. (2025). Cyber–physical security in EV charging infrastructure: Components,

vulnerabilities, and defense strategies. *Sustainable Energy Technologies and Assessments*, *81*, 104435.

2. Powell, B., & Johnson, C. (2024). *Impact of electric vehicle charging station reliability, resilience, and location on electric vehicle adoption* (No. NREL/TP--5R00-89896). National Renewable Energy Laboratory (NREL), Golden, CO (United States).
3. Motlagh, S. G., Oladigbolu, J., & Li, L. (2025). A review on electric vehicle charging station operation considering market dynamics and grid interaction. *Applied Energy*, *392*, 126058.
4. Mastoi, M. S., Zhuang, S., Munir, H. M., Haris, M., Hassan, M., Usman, M., ... & Ro, J. S. (2022). An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends. *Energy reports*, *8*, 11504-11529.
5. Alasali, F., Ghalyon, S. A., El-Naily, N., Abuashour, M. I., AlMajali, A., Itradat, A., & Holderbaum, W. (2025). Innovative Investigation of the Resilience of EV Charging Infrastructure Under Cyber-Physical Threats Based on a Real-Time Co-Simulation Testbed. *IET Cyber-Physical Systems: Theory & Applications*, *10*(1), e70021.
6. Sakwa, M., Nespoli, A., Matrone, S., Leva, S., Guerini, A., Demartini, A., & Ogliari, E. (2024). Electric vehicle supply equipment monitoring and early fault detection through autoencoders. *Sustainable Energy, Grids and Networks*, *40*, 101497.
7. Kesavan, V. T., Hossen, M. J., Gopi, R., & Joseph, E. R. (2025). Anomaly detection with grid sentinel framework for electric vehicle charging stations in a smart grid environment. *Scientific Reports*, *15*(1), 15774.
8. Tanyıldız, H., Şahin, C. B., Dinler, Ö. B., Migdady, H., Saleem, K., Smerat, A., ... & Abualigah, L. (2025). Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network. *Scientific reports*, *15*(1), 10092.
9. ElKashlan, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). *Electronics*, *12*(4), 1044.
10. ElKashlan, M., Aslan, H., Said Elsayed, M., Jurcut, A. D., & Azer, M. A. (2023). Intrusion detection for electric vehicle charging systems (evcs). *Algorithms*, *16*(2), 75.
11. Sepehrzad, R., Khodadadi, A., Adinehpour, S., & Karimi, M. (2024). A multi-agent deep reinforcement learning paradigm to improve the robustness and resilience of grid connected electric vehicle charging stations against the destructive effects of cyber-attacks. *Energy*, *307*, 132669.