

Article

Dynamic Risk Assessment Framework for Concurrent Cyber–Physical Attacks in DER-Integrated Power Grids

Cen Chen ¹, Jinghong Lan ¹, Ying Zhang ², Zheng Zhang ¹, Nuannuan Li ¹ and Yubo Song ^{2,3,*} 

¹ State Grid Henan Electric Power Research Institute, Zhengzhou 450052, China; sunshinecen@163.com (C.C.); lanjh08@163.com (J.L.); zszhere@gmail.com (Z.Z.); 18339231859@163.com (N.L.)

² School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China; iamzyyyy@seu.edu.cn

³ Key Laboratory of Green and Intelligent Development and Efficient Utilization of Strategic Mineral Resources of Xinjiang Production and Construction Corps, Xinjiang University of Technology, Hotan 848000, China

* Correspondence: songyubo@seu.edu.cn

Abstract

Distributed Energy Resource (DER)-integrated power grids are vulnerable to cascading effects under concurrent cyber–physical attacks, where even minor disruptions in system states accumulate and amplify over time, leading to significant system failures. Traditional static risk assessment methods are insufficient for modeling these time-varying, dynamic scenarios, particularly in the context of concurrent attacks. This paper presents a dynamic risk assessment framework leveraging time-synchronized co-simulation, which integrates power system and communication network simulations within a unified time framework. Cyber-attack actions in the communication layer are mapped to corresponding physical disturbances in the distribution network, including voltage, frequency, and power variations. Using the resulting system state evolution trajectories, a Markov Decision Process (MDP)-based state transition tree captures the progression of system risk under concurrent attacks. This framework accounts for cumulative risk across different attack paths and identifies critical nodes and high-risk propagation paths within the network. By incorporating a concurrent event detector into the MDP model, the method quantifies evolving risk dynamics, overcoming the limitations of traditional static methods. Case studies on the IEEE 13-node test feeder and IEEE 14-bus system demonstrate that concurrent attacks result in a security risk metric 2.3 times higher than single-point attacks, validating the effectiveness of the proposed approach in identifying vulnerable nodes whose compromise could lead to cascading failures, supporting the risk-aware prioritization of defensive resources.

Keywords: new-type power system; distributed resource network; co-simulation; attack simulation; risk assessment



Academic Editor: José Matas

Received: 29 January 2026

Revised: 27 February 2026

Accepted: 8 March 2026

Published: 11 March 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The increasing penetration of Distributed Energy Resources (DERs) is reshaping the operational structure of modern power grids, particularly at the distribution level. Distributed photovoltaics, energy storage systems, controllable loads, and electric vehicle charging infrastructures are being deployed at scale, introducing a large number of actively controlled nodes into traditionally passive networks [1]. As a result, power grid operation is no longer governed solely by physical power flow constraints but increasingly depends on real-time coordination enabled by information and communication technologies [2].

In China, this transformation is closely associated with the development of DER-integrated power grids within the broader framework of the new-type power system,

which emphasizes high renewable penetration, extensive interconnection, and coordinated operation across source, network, load, and storage [3,4]. Aggregation mechanisms such as virtual power plants enable geographically dispersed DERs to participate in coordinated control and market operation through communication and control infrastructures [5]. While these mechanisms enhance flexibility and resource utilization, they also introduce strong cyber–physical coupling, making system operation sensitive to disturbances originating in either domain.

Early research on power grid security primarily addressed physical contingencies caused by equipment failures or environmental disturbances. Risk assessment and protection strategies were therefore developed based on static fault analysis and redundancy planning. With the increasing reliance on communication-based monitoring and control, cybersecurity threats targeting measurement, communication, and control layers have become an integral part of power system security analysis [6]. In many existing studies, cyber incidents are treated as isolated events, and their impacts are evaluated independently of the evolving physical system state.

Such separation becomes increasingly inadequate in DER-integrated power grids. Cyber intrusions targeting communication channels, control logic, or measurement data can directly influence DER control actions and distribution network operating conditions. Previous studies have shown that carefully crafted cyber actions, such as false data injection, are sufficient to manipulate system estimation and control outcomes even in the absence of direct physical damage [7]. Due to the tight feedback loops between DER control and network operation, cyber disturbances can propagate into the physical domain, leading to voltage violations, power oscillations, and protection misoperations.

A critical challenge arises when multiple cyber–physical attack actions occur concurrently. In DER-integrated power grids, coordinated attacks targeting multiple components can introduce small but temporally correlated disturbances across different system states. These disturbances do not remain localized but accumulate along the system evolution trajectory, progressively amplifying operational stress. Even minor deviations in voltage, frequency, or power balance can trigger cascading effects when concurrent events interact over time. This dynamic accumulation mechanism makes system risk fundamentally time-dependent rather than event-specific.

Existing risk assessment approaches for cyber–physical power systems are predominantly static or quasi-static. Attack graph-based models and vulnerability scoring methods have been widely used to enumerate potential attack paths and identify critical components [8,9]. While effective in representing structural dependencies, these methods abstract system behavior into discrete states and transitions, limiting their ability to capture time-dependent interactions between cyber actions and physical responses. In particular, coordinated or concurrent attacks, often described as N–k events, introduce dynamic coupling effects that static representations fail to characterize [10–12].

Recent efforts have attempted to incorporate dynamic factors into cyber–physical security analysis of distribution networks with high DER penetration. A recent comprehensive survey [13] underscores that while probabilistic models and vulnerability scoring have evolved, most existing methodologies still represent system dynamics through abstract state transitions. Dynamic Bayesian network models have been employed to describe probabilistic propagation of cyber risks into physical system states [14]. While cutting-edge research has begun to utilize Deep Reinforcement Learning (DRL) to identify critical nodes and complex attack paths in cyber–physical power systems [15], these approaches often treat the physical grid as a static reward provider. Coordinated attack scenarios targeting multiple DER components have also been investigated to reflect increasingly complex threat patterns [16]. Although these approaches introduce temporal awareness,

system dynamics are still frequently represented through simplified or discrete transitions. This limits the ability to capture the recursive feedback between the attacker's knowledge gain and the resulting contraction of physical security margins, especially the continuous, fine-grained interactions between malicious cyber actions and circuit-level power behavior under coordinated and concurrent attack conditions.

Simulation-based analysis provides an alternative pathway for capturing cyber–physical interactions. Early co-simulation platforms integrating power system and communication network simulators demonstrated the feasibility of joint modeling [17]. Subsequent work extended co-simulation toward cybersecurity analysis in smart grids [18]. However, many existing platforms rely on loosely coupled architectures, where cyber events and physical responses are exchanged at coarse time scales. Such configurations limit the ability to reproduce fine-grained feedback and event-driven interactions under concurrent attack conditions [19].

These limitations highlight the need for a dynamic risk assessment framework tailored to DER-integrated power grids, in which cyber attack actions, physical system dynamics, and their mutual interactions are explicitly represented within a unified temporal context. Addressing this need requires a tightly coupled co-simulation environment capable of mapping cyber actions in the communication layer to circuit-level physical disturbances, together with a formal risk modeling approach that captures cumulative risk evolution under concurrent events.

Based on this motivation, this paper develops a dynamic risk assessment framework for concurrent cyber–physical attacks in DER-integrated power grids. The framework integrates time-synchronized co-simulation of communication networks and power system dynamics with a Markov Decision Process-based state evolution model. By constructing system state trajectories under concurrent attack actions and expanding state transitions through a concurrent event detection mechanism, the proposed approach quantifies risk accumulation over time and identifies critical nodes and high-risk propagation paths under dynamic operating conditions. The main contributions of this paper are as follows:

- A dynamic cyber–physical risk assessment framework is developed for DER-integrated power grids, combining time-synchronized co-simulation of communication networks and power system dynamics to support risk analysis under event-driven and concurrent attack conditions.
- A state evolution modeling approach based on a Markov Decision Process is introduced to characterize cumulative risk progression under concurrent cyber–physical attacks. By extending state transitions to account for simultaneous attack actions, the model represents how interacting events propagate through coupled cyber and physical system states over time.
- Case studies on the IEEE 13-node test feeder and IEEE 14-bus system provide quantitative evidence of risk amplification under concurrent attacks. The results demonstrate that concurrent attack scenarios lead to substantially higher security risk levels than single-point attacks and reveal critical nodes and high-risk propagation paths associated with cascading failures.

2. Related Work

2.1. Cyber–Physical Simulation for DER-Integrated Power Grids

Simulation technologies play a critical role in analyzing cyber–physical interactions in DER-integrated power grids, where direct experimentation on operational systems is infeasible. Early real-time simulation platforms, such as the All-Digital Power System Real-time Simulator (ADPSS), were developed to model large-scale power system dynamics with high fidelity [20]. While effective for physical system analysis, these platforms are

characterized by high cost and limited scalability, which restrict their applicability to large-scale security studies involving distributed resources. Bouslimani et al. [21] provided a comprehensive review of 100 survey papers, highlighting the surge in research regarding cyber–physical security and the complexity of modern smart grid structures.

To address these limitations, co-simulation frameworks that integrate power system simulators with communication network simulators have been proposed. The EPOCHS platform developed by Hopkinson et al. [17] represents an early effort to jointly model electromechanical behavior and communication processes. Although EPOCHS demonstrated the feasibility of coordinated simulation, it was primarily designed to study communication impacts on system performance and did not explicitly support cyber attack execution or security analysis. Subsequent studies explored interdependent network modeling to analyze cascading failures across power and communication infrastructures [22], providing insight into system vulnerability from a network topology perspective.

Security-oriented simulation tools have since been developed to incorporate attack modeling and defensive evaluation. NeSSi2 [23] and its successor HOLEG [24] focus on network-level attack scenarios and resilience evaluation using agent-based and time-discrete simulation techniques. ASTORIA [25] further extends this line of work by enabling attack injection and consequence assessment in simulated power system infrastructures. These platforms provide valuable capabilities for cybersecurity experimentation; however, their primary focus remains on network behavior and sampled system responses. The coupling between cyber events and physically consistent distribution network dynamics, which is essential for DER-integrated grids, is typically abstracted or simplified.

Recent advances in cybersecurity simulation have attempted to combine engineering safety simulation with cyber attack modeling through hardware-in-the-loop, numerical, and semi-physical approaches [26]. To enhance modularity, Diao et al. [27] proposed a modular probabilistic risk assessment framework that simulates interactions between protection systems, operators, and attackers using the IEEE 14-bus system. Similarly, Pasiadis et al. [28] leveraged Software Defined Networking (SDN) within a cyber-resilience framework to accurately detect attacks and perform network path re-allocation to maintain Quality of Service (QoS). Despite improved realism, existing platforms still face challenges in scalability and coupling depth. In particular, support for event-driven and concurrent attack execution remains limited, constraining the analysis of coordinated cyber–physical attacks on DER-integrated power grids.

2.2. Dynamic Risk Assessment of Cyber–Physical Attacks in DER-Enriched Systems

Quantitative risk assessment has become the dominant approach for evaluating cybersecurity threats due to its ability to provide probabilistic and comparable metrics. A recent survey by Arjmand et al. [29] analyzed dynamic security risk assessment (DRA) techniques from 2016 to 2025, revealing a significant trend toward integrated methodologies that combine AI/ML with mathematical modeling to maintain real-time assessment capabilities. In general cybersecurity research, attack graph-based models have been widely adopted to represent possible attack paths and quantify system exposure. Probabilistic attack graphs and related extensions combine vulnerability information with transition probabilities to estimate attack likelihoods [8,30]. Hierarchical models such as HARM further integrate attack graphs and attack trees to improve scalability and computational efficiency [31]. Hybrid approaches combining attack trees and graphs have also been proposed to visualize attacker behavior and goal progression [32].

These methods have been extended to power system security analysis to account for cyber–physical interactions. Bayesian Attack Graphs have been used to assess attack success probabilities in power grid environments by incorporating vulnerability scores and

system topology [33]. More recent studies focus on distribution networks and monitoring systems, modeling cyber–physical dependencies to identify critical components and attack paths [34]. Dynamic Bayesian Networks have been employed to describe probabilistic risk propagation from the cyber layer to physical system states in distribution networks [35]. Cheimonidis and Rantos [36] further extended this by integrating open-source intelligence with Bayesian networks and Fuzzy Cognitive Maps to proactively estimate threat probabilities and suggest mitigation strategies. Other approaches infer attack likelihoods through correlation networks or continuous-time stochastic models to capture interdependencies among system components [37,38].

Markov-based models provide a formal framework for representing sequential attacker behavior under uncertainty. Markov Decision Processes have been applied to model attacker actions and evaluate security risk in cyber–physical systems [39]. Furthermore, Zhang and Ni [40] developed a security-oriented risk assessment method for cyber–physical distribution systems (CPPDSs) using MDP to calculate a specific cyber–physical risk index (CPRI), while considering finite defense resource allocation through an attack–defense game. While these approaches introduce temporal structure into risk assessment, system states are often defined at an abstract level, and the evolution of physical system dynamics is not explicitly represented. In DER-integrated power grids, where coordinated attacks on multiple distributed resources can trigger nonlinear and state-dependent responses, such abstractions limit the ability to capture concurrent events and physically driven risk amplification.

Existing risk assessment methods for DER-integrated power grids either rely on static representations or employ dynamic models with limited coupling to physical system behavior. This gap motivates the development of dynamic risk assessment approaches that explicitly integrate cyber attack evolution with physically consistent power system responses, particularly under event-driven and coordinated attack scenarios.

3. Methodology

3.1. Framework Design

The proposed framework characterizes the evolution of system risk in DER-integrated power grids under concurrent cyber–physical attacks by explicitly modeling the interaction between cyber events and physical system dynamics over time. The framework integrates time-synchronized co-simulation with a state-based risk assessment mechanism, enabling the analysis of how cyber-induced disturbances propagate through the power grid and accumulate across multiple attack paths.

Figure 1 illustrates the time-synchronized co-simulation framework used to generate system state trajectories under attack conditions. Power system dynamics and communication network behavior are executed on a unified time axis, allowing cyber events in the communication layer to be directly associated with their physical consequences in the distribution network. Attack actions are produced by an attacker behavior model and mapped to physical disturbances, which are reflected as variations in observable system states such as voltage profiles, frequency responses, and power flows. This synchronized execution captures the temporal dependence between attack actions and system responses, producing continuous state trajectories rather than isolated operating points.

The system state trajectories generated by the co-simulation framework constitute the input to the risk assessment component shown in Figure 2. Instead of evaluating security impacts at individual time steps, the framework organizes system evolution into a structured representation that reflects feasible transitions between states under different attack actions. This representation enables the analysis of how risk propagates across time and across interconnected components of the network.

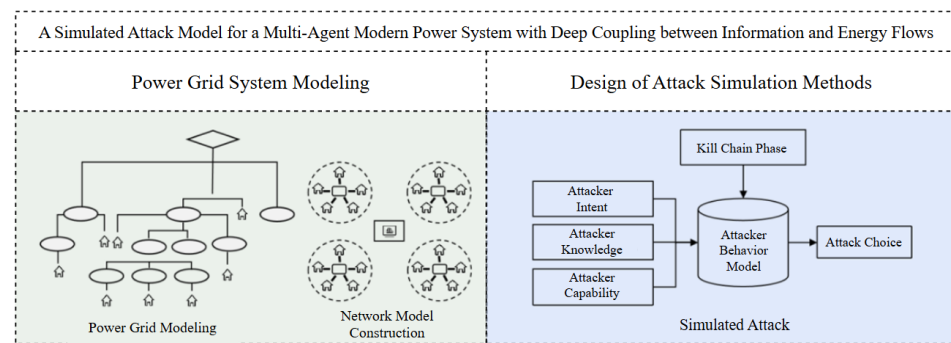


Figure 1. Time-Synchronized Co-Simulation Framework for Cyber-Physical State Generation.

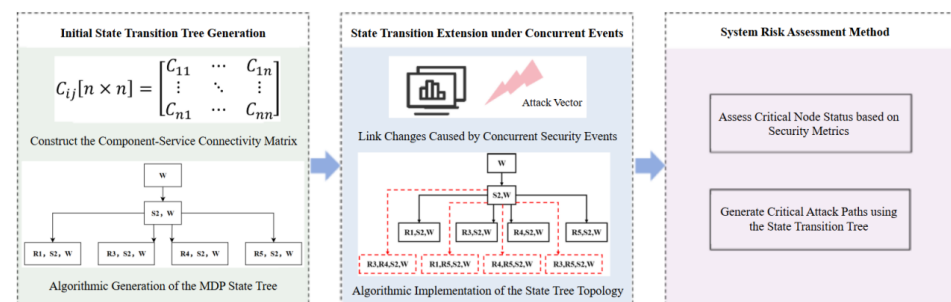


Figure 2. MDP State Tree-Based Dynamic Risk Assessment Framework for Distribution Networks

As illustrated in Figure 2, the risk assessment module constructs a state transition tree based on a Markov Decision Process formulation. Tree nodes correspond to system states derived from co-simulation outputs, while edges represent feasible transitions driven by attack actions and system dynamics. Network connectivity and attack reachability jointly constrain the expansion of the state tree, ensuring that only physically and logically attainable states are considered. This structure explicitly represents the temporal progression of risk and the branching of attack-induced state evolution paths.

The framework incorporates a concurrent event detection mechanism to account for the interaction of multiple attack events occurring within overlapping time intervals. When concurrent events introduce state changes that cannot be captured through sequential transitions, additional states are incorporated into the transition tree to reflect their combined impact. This extension allows the state-based representation to capture non-linear risk amplification effects arising from concurrent cyber-physical interactions, which are not adequately described by static or single-event models.

By integrating time-synchronized co-simulation with a state transition tree representation, the framework enables the systematic analysis of cumulative risk evolution under concurrent attack conditions. The resulting structure supports the identification of critical system states and high-risk propagation paths, which are examined in detail in the subsequent methodological sections.

3.2. Time-Synchronized Co-Simulation

The dynamic interaction between cyber events and physical system responses requires that power system simulation and communication network simulation evolve on a consistent temporal basis. In DER-integrated distribution networks, cyber actions such as command manipulation, data injection, or communication disruption do not instantaneously translate into physical consequences. Their impacts unfold over time through control loops, protection mechanisms, and power flow dynamics. To capture this temporal dependence, the proposed framework adopts a time-synchronized co-simulation approach

in which power system dynamics and communication network behavior are executed under a unified simulation clock.

Within the co-simulation environment, the power grid simulator and the communication network simulator advance in discrete time steps that are aligned through a synchronization interface. Cyber events are generated in the communication domain as time-stamped actions and are injected into the power system simulator at the corresponding simulation instants. This alignment preserves the temporal order between attack execution, control signal propagation, and physical response, allowing cyber-induced disturbances to affect the physical system state in a causally consistent manner. The simulation therefore captures delayed and cumulative system responses rather than isolated event-triggered changes.

The co-simulation framework supports bidirectional information exchange between the cyber and physical domains. Measurements from the power system, such as node voltages, frequencies, power injections, and line flows, are periodically reported to the communication layer and may influence subsequent cyber actions. Conversely, cyber-layer events modify control inputs or data availability in the power system simulator, leading to observable changes in physical states. This bidirectional coupling represents feedback mechanisms that are essential for modeling attack escalation and cross-domain propagation under dynamic conditions.

A primary output of the time-synchronized co-simulation is a sequence of system states describing the evolution of the distribution network under attack. Each state corresponds to a specific simulation time step and reflects both intrinsic system dynamics and externally induced cyber disturbances. This representation preserves temporal continuity and provides a structured description of how localized perturbations propagate through interconnected components of the network over time.

The resulting state trajectories constitute the data basis for constructing state-based representations of system evolution under attack conditions. Their temporal consistency and causal alignment enable subsequent analysis of state transitions and risk propagation without relying on static assumptions or single-event abstractions.

3.3. Cyber-to-Physical Action Mapping

Cyber-to-physical action mapping describes how attack actions generated in the communication domain are translated into disturbances acting on the physical distribution network. In the proposed framework, cyber attacks are not treated as predefined fault events with fixed consequences. Instead, each attack action is interpreted through its effect on control signals, data availability, or device behavior, and its physical impact is reflected through the dynamic evolution of power system states over time.

Attack actions are generated by an attacker behavior model that formalizes the interaction between the attacker and the communication network. The information network is represented by a set of nodes and exploitable vulnerabilities, and a single attack action is defined as a triplet $a = (s, t, e)$, where s denotes the source node initiating the action, t denotes the target node, and e denotes the vulnerability exploited on the target. An attack scenario is represented as a sequence of such actions $\{a_k\}$ executed over time. This formulation provides a structured description of feasible attack actions at a given system state without attempting to enumerate all possible attack strategies.

Within the attacker behavior model, the selection of attack actions follows a staged decision process aligned with the concept of a network kill chain. At each simulation step t_k , the attacker evaluates its current intent I_k and accumulated network knowledge Ω_k to determine the active kill chain stage K_k , which can be expressed as

$$K_k = \mathcal{F}(I_k, \Omega_k), \quad (1)$$

where $\mathcal{F}(\cdot)$ denotes a fuzzy inference mapping. The selected stage constrains the admissible set of attack actions available at that time step, ensuring that action selection reflects situational context rather than random choice. The overall decision flow for kill chain stage selection is illustrated in Figure 3.

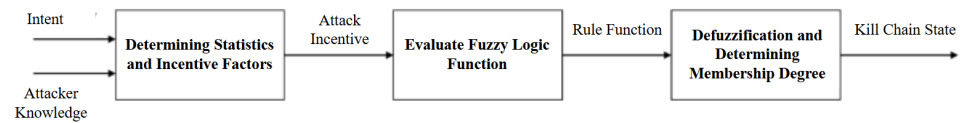


Figure 3. Decision Flow for Kill Chain Stage Selection in the Attacker Behavior Model.

The physical impact of a cyber attack action is determined by how compromised communication behavior alters power system operation. This relationship is represented through a mapping operator that converts a cyber action into a physical disturbance applied to the system state. For an attack action a_k executed at time t_k , the induced disturbance can be written as

$$\Delta x(t_k) = \mathcal{M}(a_k, x(t_k^-)), \quad (2)$$

where $x(t_k^-)$ denotes the system state immediately before the attack, and $\mathcal{M}(\cdot)$ captures the cyber-to-physical mapping mechanism.

Load-related disturbances constitute one of the most direct mappings from cyber actions to physical effects. When control over smart loads or switching devices is compromised, coordinated load connection or disconnection leads to variations in nodal power injections. For node i , the active power under attack is expressed as

$$P_i(t_k) = P_i^0(t_k) + \Delta P_i(t_k), \quad (3)$$

where $P_i^0(t_k)$ denotes the nominal load and $\Delta P_i(t_k)$ represents the attack-induced load deviation. These deviations propagate through the network and modify line power flows and nodal voltage profiles over subsequent simulation steps.

Cyber actions targeting measurement data or control signals affect the physical system through delayed, incorrect, or absent control responses. In such cases, the power system evolves under altered control inputs, and the resulting state transition is governed by the system dynamics

$$x(t_{k+1}) = f(x(t_k), \Delta u(t_k)), \quad (4)$$

where $\Delta u(t_k)$ represents the control deviation induced by cyber interference.

All cyber-induced disturbances are injected into the time-synchronized co-simulation at discrete simulation instants. The power system simulator computes the resulting system states according to its dynamic model, producing a sequence of time-indexed states that capture voltage levels, power injections, and line flows under attack conditions. These state trajectories preserve both the temporal ordering and magnitude of disturbances, providing a consistent description of how cyber actions translate into physical system evolution.

By representing cyber attacks through their induced physical disturbances and embedding these disturbances into continuous state trajectories, the mapping process establishes a direct connection between communication-layer actions and observable power system behavior. This representation enables subsequent state-based analysis of risk propagation under concurrent cyber–physical attack conditions without relying on predefined impact categories or static contingency assumptions.

3.4. MDP-Based State Transition Tree for Dynamic Risk Propagation

The evolution of system risk under cyber–physical attacks is represented through a state transition structure that captures how attack-induced disturbances propagate across

system components and over time. This structure is formulated using a Markov Decision Process (MDP), in which system states encode the cumulative impact of attack actions and transitions represent feasible attack-driven state evolutions constrained by network connectivity and system dynamics. Rather than focusing on policy optimization, the MDP formulation is used to organize reachable system states into a state transition tree that supports quantitative risk aggregation along different attack paths.

Let S denote the finite set of system states. Each state $s \in S$ corresponds to a specific configuration of compromised cyber components together with the associated physical operating condition of the distribution network derived from co-simulation. The initial state s_0 represents normal operation with no compromised components. As attack actions are executed, the system transitions to states that reflect both newly compromised components and the resulting physical disturbances captured in the state trajectory.

For each state s , a finite set of admissible actions $A(s)$ is defined. An action represents the exploitation of a vulnerability that is reachable under the current connectivity and access conditions. Feasible state transitions are determined jointly by the communication network connectivity and the attack action definition introduced in Section 3.3. A transition from state s to state s' under action $a \in A(s)$ is denoted by the conditional probability $P_a(s, s')$, which reflects the likelihood that the exploitation succeeds and leads to the corresponding system configuration. In this work, transition probabilities are parameterized using normalized vulnerability severity scores, such that

$$P_a(s, s') = \frac{\text{CVSS}(a)}{10}, \quad (5)$$

where $\text{CVSS}(a) \in [0, 10]$ denotes the severity score associated with the exploited vulnerability.

The transition probability $P_a(s, s')$ is constrained by the attacker's capability K_k ; an action is only executable when K_k satisfies the stage requirements of the specific attack path, thus capturing the adaptive feedback loop.

The reachability between components is encoded in a connectivity matrix $C \in \{0, 1\}^{n \times n}$, where n is the number of cyber-accessible components. An entry $C_{ij} = 1$ indicates that a compromised service on component i enables access to component j , while $C_{ij} = 0$ indicates no direct access path. This matrix constrains the expansion of the state transition tree by restricting admissible actions to those consistent with the underlying communication topology and access control relationships.

Based on the state definition, action set, and connectivity constraints, the state transition tree is constructed by enumerating all reachable states starting from s_0 . Each node in the tree corresponds to a system state, and each directed edge represents a feasible transition under a specific attack action. The construction process iteratively expands newly discovered states until no additional reachable states exist. The resulting structure explicitly represents all attack propagation paths permitted by the system topology and vulnerability configuration.

To quantify the security impact associated with each state, a risk-based reward function is defined based on the physical operating condition of the power system. Let L denote the set of distribution lines, and let $f_s(l)$ and $f_{\max}(l)$ denote the power flow and thermal limit of line l under state s , respectively. The physical impact of state s is measured as

$$F(s) = \sum_{l \in L} \left[\max \left(\frac{f_s(l)}{f_{\max}(l)} - 1, 0 \right) \right]^2, \quad (6)$$

which penalizes line overload conditions while assigning zero contribution to normal operating states. The immediate reward associated with a transition from s to s' under action a is defined as

$$R_a(s, s') = F(s') - F(s), \quad (7)$$

reflecting the marginal increase in physical stress induced by the attack action. While system security involves multiple dimensions, we utilize line overloads as the primary indicator because they serve as a critical proxy for system-wide risk in DER-integrated networks. Branch overloads are the immediate physical consequence of coordinated attacks and the fundamental triggers for cascading failures; exceeding thermal limits lead to relay tripping, which reconfigures the topology and further stresses the remaining branches. Thus, the penalty on line flows effectively captures the non-linear transition from localized stress to systemic vulnerability.

Risk propagation along attack paths is evaluated using a Bellman-type value iteration over the state transition tree. The risk value $I(s)$ associated with state s satisfies

$$I_{k+1}(s) = \max_{a \in A(s)} \sum_{s' \in S} P_a(s, s') [R_a(s, s') + \gamma I_k(s')], \quad (8)$$

where $\gamma \in (0, 1)$ is a discount factor that controls the relative influence of future states. This formulation aggregates cumulative risk along feasible attack paths and assigns higher values to states that are both reachable with high probability and associated with severe physical impact.

The resulting state transition tree, together with the corresponding risk values, provides a structured representation of dynamic risk propagation under cyber–physical attacks. By tracing high-value paths and states within the tree, critical components and attack sequences that contribute disproportionately to overall system risk can be identified.

The evaluation of risk propagation is performed directly on the state transition tree generated from the MDP formulation. Let $\mathcal{T} = (S_{\mathcal{T}}, E_{\mathcal{T}})$ denote the state transition tree, where $S_{\mathcal{T}} \subseteq S$ represents the set of reachable states starting from the initial state s_0 , and $E_{\mathcal{T}}$ represents directed edges corresponding to feasible transitions (s, a, s') . The tree is constructed by iteratively expanding reachable states under the connectivity constraints and action set $A(s)$ until no new states can be discovered.

Risk propagation is evaluated by assigning an initial risk value $I_0(s)$ to each state in $S_{\mathcal{T}}$, where $I_0(s) = 0$ for all non-terminal states and $I_0(s) = F(s)$ for terminal states. Terminal states are defined as states for which no further admissible actions exist under the connectivity and vulnerability constraints. The risk value of non-terminal states is then updated through backward iteration along the tree structure.

At iteration $k + 1$, the risk value of each state $s \in S_{\mathcal{T}}$ is updated according to

$$I_{k+1}(s) = \max_{a \in A(s)} \sum_{s' \in \text{Succ}(s, a)} P_a(s, s') [R_a(s, s') + \gamma I_k(s')], \quad (9)$$

where $\text{Succ}(s, a)$ denotes the set of successor states of s under action a in the state transition tree. This update propagates risk information from downstream states toward upstream states, reflecting the accumulation of physical impact along feasible attack paths.

The iteration proceeds until convergence, defined by $\max_{s \in S_{\mathcal{T}}} |I_{k+1}(s) - I_k(s)| < \epsilon$ for a predefined tolerance ϵ . The converged value $I(s)$ represents the cumulative risk associated with state s , accounting for both immediate physical impact and expected future risk along all reachable attack paths. By construction, states closer to the root capture upstream risk exposure, while states deeper in the tree reflect localized but potentially severe physical consequences.

The complete procedure for constructing the state transition tree and evaluating risk propagation is summarized in Algorithm 1. The resulting risk values enable the identification of critical states and high-risk propagation paths, which form the basis for subsequent analysis of concurrent attack effects.

Algorithm 1 State Transition Tree Construction and Risk Propagation Evaluation

Require: Connectivity matrix C , initial state s_0 , admissible action generator $A(\cdot)$, transition model $P_a(s, s')$, reward increment $R_a(s, s')$, discount factor $\gamma \in (0, 1)$, tolerance ϵ

Ensure: Reachable state set $S_{\mathcal{T}}$, transition edge set $E_{\mathcal{T}}$, converged risk value $I(s)$ for all $s \in S_{\mathcal{T}}$

```

1: Initialize  $S_{\mathcal{T}} \leftarrow \{s_0\}$ ,  $E_{\mathcal{T}} \leftarrow \emptyset$ 
2: Initialize queue  $Q \leftarrow [s_0]$ 
3: while  $Q$  is not empty do
4:   Pop  $s$  from  $Q$ 
5:   for all  $a \in A(s)$  do
6:     Determine successor candidates  $\text{Succ}(s, a)$  using connectivity constraint  $C$ 
7:     for all  $s' \in \text{Succ}(s, a)$  do
8:       Add edge  $(s, a, s')$  to  $E_{\mathcal{T}}$ 
9:       if  $s' \notin S_{\mathcal{T}}$  then
10:        Add  $s'$  to  $S_{\mathcal{T}}$  and push  $s'$  into  $Q$ 
11:       end if
12:     end for
13:   end for
14: end while
15: Initialize  $I^{(0)}(s) \leftarrow 0$  for all  $s \in S_{\mathcal{T}}$ 
16: repeat
17:    $I^{(k+1)} \leftarrow I^{(k)}$ 
18:   for all  $s \in S_{\mathcal{T}}$  do
19:      $I^{(k+1)}(s) \leftarrow \max_{a \in A(s)} \sum_{s' \in \text{Succ}(s, a)} P_a(s, s') [R_a(s, s') + \gamma I^{(k)}(s')]$ 
20:   end for
21:    $\Delta \leftarrow \max_{s \in S_{\mathcal{T}}} |I^{(k+1)}(s) - I^{(k)}(s)|$ 
22:    $k \leftarrow k + 1$ 
23: until  $\Delta < \epsilon$ 
24: return  $S_{\mathcal{T}}$ ,  $E_{\mathcal{T}}$ ,  $I(s) = I^{(k)}(s)$ 

```

3.5. State Transition Extension Under Concurrent Attack Events

In distribution networks with high penetration of distributed energy resources, system risk cannot be fully characterized by isolated component failures. Due to the topological interdependence of power delivery paths and the temporal overlap of cyber attack actions, multiple components may be compromised within the same simulation interval, giving rise to system states that do not appear in single-action state transition models. To address this limitation, the proposed framework extends the MDP state transition structure by incorporating states induced by concurrent attack events.

The extension procedure is motivated by the fact that the physical impact of multiple simultaneous component failures can be super-additive due to nonlinear power-flow redistribution, constraint activation, and protection-induced topology changes. Let T denote a set of power system components, such as transmission lines or their associated protective relays, and let P represent the current grid topology. We quantify the system impact of a failure set T under topology P by a trajectory-level reward function $RF(T, P)$, defined as the cumulative line-overload penalty over a finite simulation horizon:

$$RF(T, P) = \sum_{k=1}^H \sum_{\ell \in \mathcal{L}} \left[\max(0, f_{\ell}^{(T, P)}(k) - f_{\ell}^{\max}) \right]^2. \quad (10)$$

Here, $\mathcal{L}$ is the set of monitored lines, H is the number of discrete simulation steps in the evaluation horizon, and $f_{\ell}^{(T,P)}(k)$ is the active power flow on line ℓ at step k after applying the simultaneous failure set T under topology P . The parameter $f_{\ell}^{\max}$ represents the predefined thermal limit of line ℓ , serving as a physical design constraint. Since the simulation is conducted on the IEEE 14-bus test system, these thresholds are strictly adopted from the standard technical specifications of the IEEE 14-bus benchmark dataset. If the power flow exceeds this predefined limit ($f_{\ell} > f_{\ell}^{\max}$), it indicates a severe physical impact—meaning the line cannot operate normally due to thermal stress—which may trigger protection mechanisms and lead to power outages. The squared penalty in the formula emphasizes that larger overloads are disproportionately more harmful and reflects the nonlinear risk escalation inherent in concurrent cyber–physical failures.

A subset of components $\{t_i, t_j\} \subset T$ is identified as a concurrent event set if

$$RF(\{t_i\}, P) + RF(\{t_j\}, P) < RF(\{t_i, t_j\}, P), \quad (11)$$

which indicates that the joint failure produces a physical consequence that cannot be explained as a simple superposition of two isolated failures. In practice, this condition captures cases where the simultaneous outage activates different binding constraints or triggers additional protective actions, leading to a qualitatively different system evolution within the horizon H .

Based on this criterion, the power network is analyzed to identify small clusters of components whose concurrent compromise leads to amplified service disruption. In practical implementation, the detector enumerates candidate component pairs or small subsets and evaluates the corresponding reward function values under the current topology. Higher-order combinations are not exhaustively explored, as empirical analysis shows that simultaneous failures of a limited number of critical components are sufficient to isolate load areas or trigger cascading effects.

Figure 4 illustrates a representative example. In the shown network, individual failures of relays controlling lines L_1 or L_2 do not interrupt power delivery to Load Area A. However, when both relays are compromised within the same time interval, all supply paths to that area are disconnected, resulting in a large-scale outage. This system state cannot be inferred from single-failure transitions and therefore must be introduced explicitly.

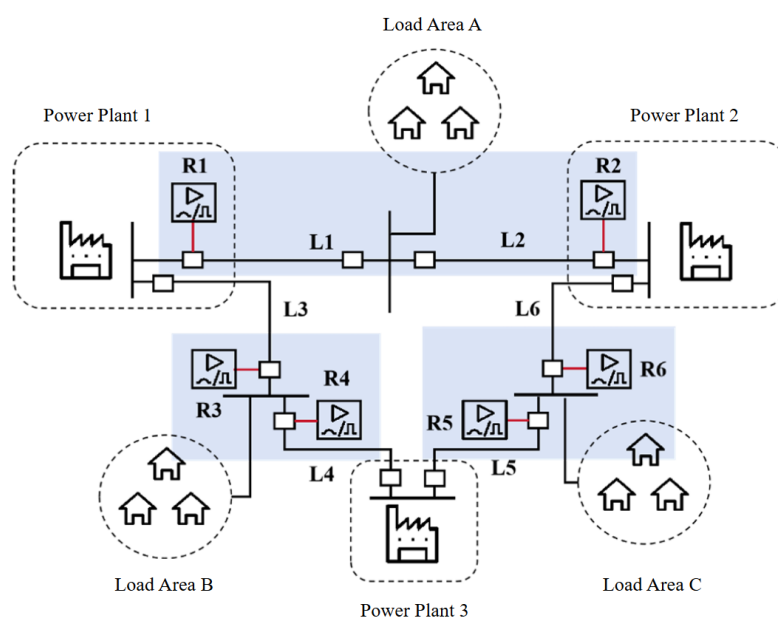


Figure 4. Example of concurrent event state identification in a multi-link distribution network.

The concurrent event sets identified above are used to extend the original MDP state transition tree. Let $\mathcal{S}$ and $\mathcal{A}$ denote the state set and action set generated from single-action attack paths. For each concurrent event set, all state paths in the original tree that correspond to the individual component failures are extracted. These paths are then aggregated to form composite transition sequences terminating at newly introduced states that represent simultaneous failures.

The resulting extended state set is given by

$$\mathcal{S}' = \mathcal{S} \cup \mathcal{S}_{\text{concurrent}} \quad (12)$$

where $\mathcal{S}_{\text{concurrent}}$ contains only states induced by concurrent events satisfying (11). Transition probabilities associated with concurrent transitions are computed under the assumption that attack actions on distinct components are conditionally independent within a simulation step. Accordingly, the probability of a concurrent transition is obtained by multiplying the probabilities of the corresponding individual transitions.

The state extension process is summarized in Algorithm 2, which takes the original MDP state tree and the detected concurrent event sets as inputs and augments the tree by introducing only those composite states that meet the concurrency condition. This selective extension avoids uncontrolled state space growth while preserving the ability to represent non-additive system impacts.

Algorithm 2 MDP State Transition Extension under Concurrent Events

Require: Concurrent event sets, original MDP state tree

Ensure: Extended state set and transition set

- 1: **for** each concurrent event set **do**
 - 2: extract single-failure paths from the original state tree
 - 3: aggregate paths into composite transition sequences
 - 4: introduce concurrent states into the state set
 - 5: assign transition probabilities via multiplicative composition
 - 6: **end for**
-

Figure 5 shows an example of the extended state transition tree generated for a general distribution network topology. Compared with the original structure, the extended tree explicitly includes branches corresponding to concurrent attack-induced states, enabling the representation of cascading effects that arise only under simultaneous failures.

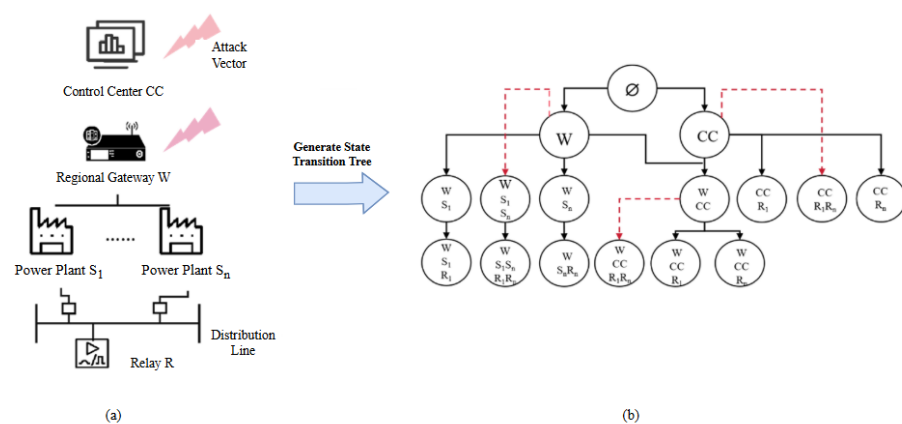


Figure 5. (a) General topology of the distribution network. (b) Extended MDP state transition tree incorporating concurrent events.

By embedding concurrent attack-induced states into the MDP framework through a reproducible detection-and-extension procedure, the resulting state transition tree captures

system behaviors that remain hidden under single-event assumptions. This extended structure provides the basis for quantifying cumulative risk under concurrent cyber–physical attacks in subsequent analysis.

4. Experiments Evaluation

4.1. Experimental Setup

The experimental setup is designed to validate the proposed dynamic risk assessment framework under concurrent cyber–physical attack conditions, with particular emphasis on time-dependent state evolution and cross-domain interactions. To this end, a time-synchronized co-simulation environment is constructed to integrate power system dynamics and communication network behavior within a unified temporal framework. This configuration enables cyber-layer attack actions to be consistently mapped to physical-layer disturbances and allows system risk to be evaluated along evolving state trajectories rather than at isolated operating points.

All experiments are conducted using open-source simulation tools on commodity computing platforms to ensure reproducibility. The hardware environment consists of two computing systems operating under Windows 10 and Ubuntu 22.04.2, respectively. The Windows platform is equipped with an Intel Core i5-12500H processor running at 3.10 GHz and 16 GB LPDDR4 memory at 2666 MHz, while the Linux platform uses a 64-bit Ubuntu 22.04.2 operating system with Linux kernel version 5.19.0-35-generic and 32 GB DDR4 memory at 2400 MHz. A summary of the hardware configuration is provided in Table 1. All simulations are executed in non-real-time mode without hardware-in-the-loop acceleration.

Table 1. Experimental Hardware Environment Configuration.

Operating System	CPU/Kernel	Memory
Windows 10	Intel Core i5-12500H 3.10 GHz	16 GB LPDDR4 2666 MHz
Ubuntu 22.04.2	Linux Kernel 5.19.0-35-generic	32 GB DDR4 2400 MHz

The software environment is built entirely on open-source components. Power system behavior is modeled using GridLAB-D, while communication network dynamics are simulated using NS-3. Cross-domain coordination is achieved through the Framework for Network Co-Simulation (FNCS), which provides centralized time management and event synchronization. Simulation control logic and attack configuration are implemented in Python 3.7, and all experiments are executed under a 64-bit Linux runtime environment to ensure compatibility with FNCS and NS-3. The software configuration is summarized in Table 2.

Table 2. Experimental Software Environment Configuration.

Component	Configuration Information
Programming Language	Python 3.7
Power System Simulator	GridLAB-D
Communication Simulator	NS-3
Co-simulation Framework	FNCS (https://github.com/FNCS/fncs , accessed 10 March 2026)
Runtime Environment	Linux 64-bit

The co-simulation mechanism relies on FNCS to enforce strict temporal consistency between simulators. Each simulator registers with the FNCS broker and advances simulation time only after receiving global synchronization permission. Cyber events generated

in the communication network are transmitted to the power system simulator through a publish–subscribe mechanism, where they are interpreted as control or load disturbances. This design ensures that cyber-induced effects are applied to the physical system at precisely aligned simulation time steps, allowing the resulting voltage, frequency, and power responses to be attributed to specific attack actions. The overall time-synchronized co-simulation workflow is illustrated in Figure 6.

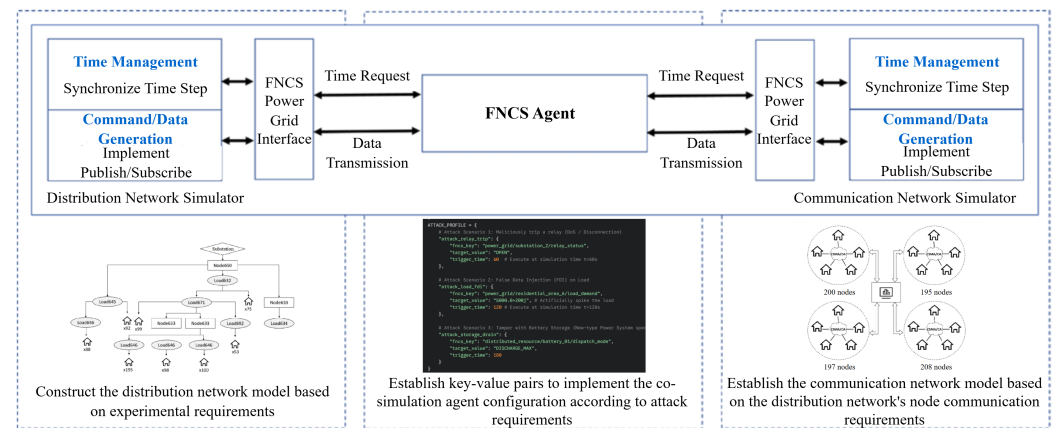


Figure 6. Time-synchronized cyber–physical co-simulation architecture based on FNCS.

Distribution-level physical experiments are conducted using the IEEE 13-node test feeder, which represents a medium-voltage distribution network operating at 10 kV. The feeder configuration is selected to examine how cyber-layer attacks targeting user-side devices propagate through the distribution network and accumulate into observable physical disturbances. Based on standard distribution capacity constraints, the feeder is populated with 800 residential loads, each corresponding to a single household device with a nominal power demand of 4 kW. The resulting baseline operating power of the feeder is 3200 kW, remaining within the thermal and current limits of a typical 10 kV distribution line.

Each residential load in the power system model is explicitly mapped to a corresponding communication node in the cyber domain, establishing a one-to-one relationship between physical consumption behavior and smart meter communication activity. The user-side communication network is divided into four Home Area Network groups to reflect realistic access network coverage. Each group contains approximately 200 nodes and employs carrier-sense multiple-access mechanisms to simulate shared-medium communication behavior. Point-to-point and local area network links are configured with a data rate of 4 Mbps and a fixed transmission delay of 3 ms. The integrated cyber–physical attack scenario constructed on the IEEE 13-node feeder is shown in Figure 7.

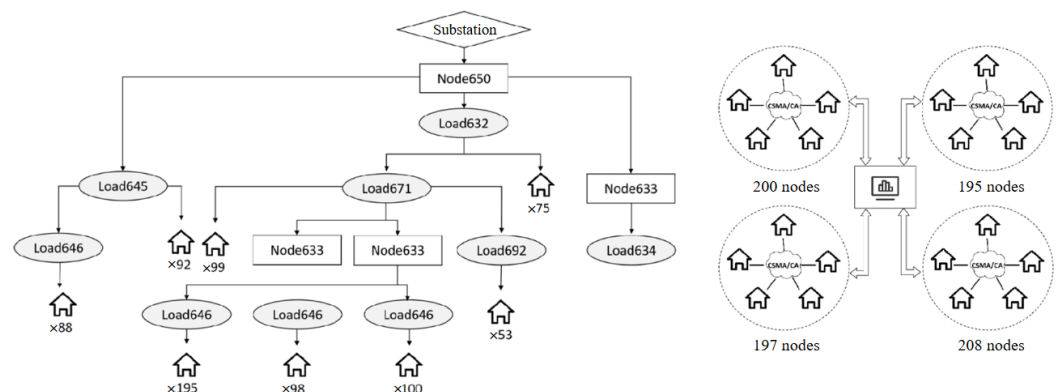


Figure 7. Cyber–physical attack scenario based on the IEEE 13-node test feeder.

To support dynamic risk assessment based on state transition modeling, additional experiments are conducted using the IEEE 14-bus test system. This system provides a standardized transmission-level topology suitable for representing system states, attack paths, and concurrent event interactions within a manageable state space. Substations, relays, regional gateways, and the control center are modeled as interconnected cyber–physical components. Each transmission line is protected by relays located at substations, where compromising a single relay is sufficient to interrupt line operation. Communication flows between user devices, gateways, and the control center create multiple potential intrusion paths, forming the structural basis for concurrent attack scenarios. The corresponding attack topology is illustrated in Figure 8.

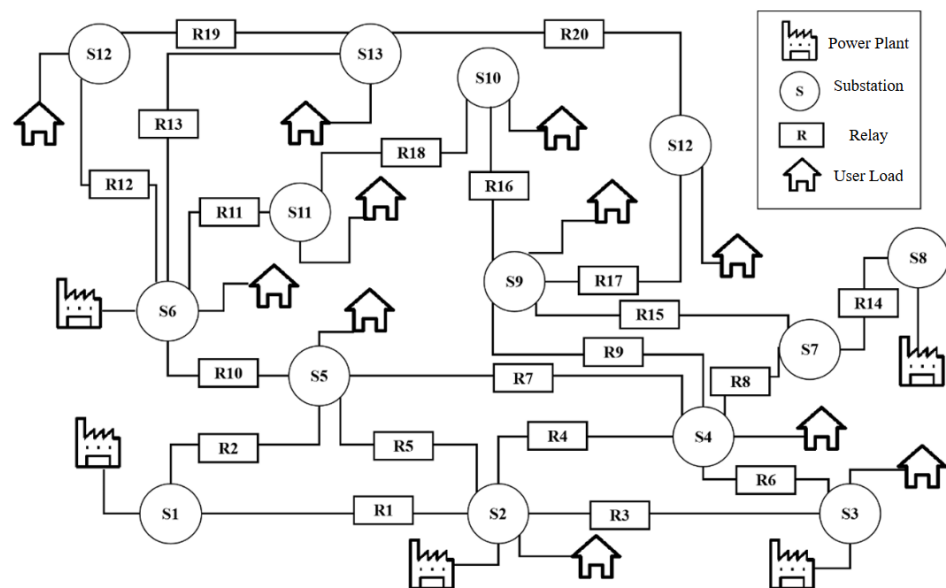


Figure 8. Attack scenario construction based on the IEEE 14-bus test system.

Across all experiments, attack behaviors are abstracted as cyber events that degrade communication quality, alter control commands, or modify load states, rather than as specific exploit implementations. This abstraction allows the experimental setup to emphasize system-level state evolution and risk accumulation mechanisms. State transition probabilities required by the MDP-based risk assessment model are derived from representative vulnerability severity information associated with relays, substations, gateways, and control center components, and are applied consistently across single-event and concurrent attack scenarios to enable comparative analysis of dynamic risk behavior.

4.2. System State Evolution Under Cyber–Physical Attacks

Figure 9 shows the evolution of total feeder load over a 24 h period under normal operation and under sustained channel interference. During low-demand periods, the difference between the two operating conditions remains limited, indicating that moderate communication latency does not immediately affect system regulation when sufficient control margins are available. As system demand increases toward daytime peak hours, the divergence between normal and attacked load trajectories becomes progressively more pronounced.

Between 12:00 and 16:00, the feeder load under channel interference exhibits a delayed response to rising demand. This delay reflects the impact of increased communication latency on the propagation of control signals and on the execution of load regulation actions. After 16:00, delayed control responses accumulate, leading to a pronounced load overshoot. During the late afternoon and evening period, the total feeder load under attack exceeds

the corresponding normal operating level. Even after demand begins to decline after 21:00, the load under attack remains elevated, indicating that the system continues compensating for previously unaddressed demand. The resulting trajectory demonstrates that communication-layer disruptions can induce persistent deviations in physical operating states through temporal accumulation rather than through instantaneous disturbances.

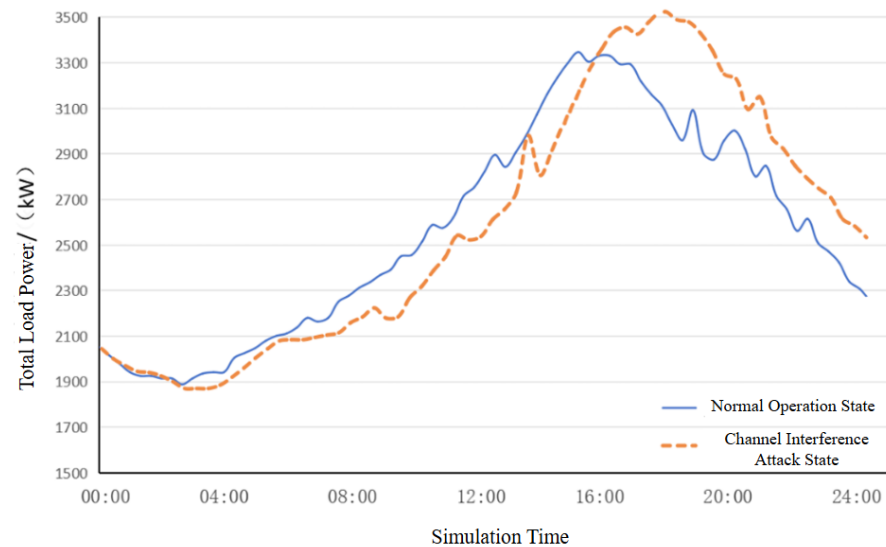


Figure 9. Total feeder load evolution under channel interference attack.

The spatial distribution of voltage deviations induced by channel interference is illustrated in Figure 10, which presents nodal voltage levels at 18:00, corresponding to the period of maximum load divergence. Under normal operation, voltages follow a gradual decline along the feeder and remain within acceptable operating limits. Under attack conditions, voltage levels increase at all nodes, with several nodes exceeding standard regulation bounds. The voltage at Node 7 increases from 0.912 p.u. to 0.956 p.u., surpassing the allowable deviation range and indicating degraded power quality. The non-uniform voltage response across nodes suggests that communication-induced control delays amplify local sensitivities associated with network topology and load distribution.

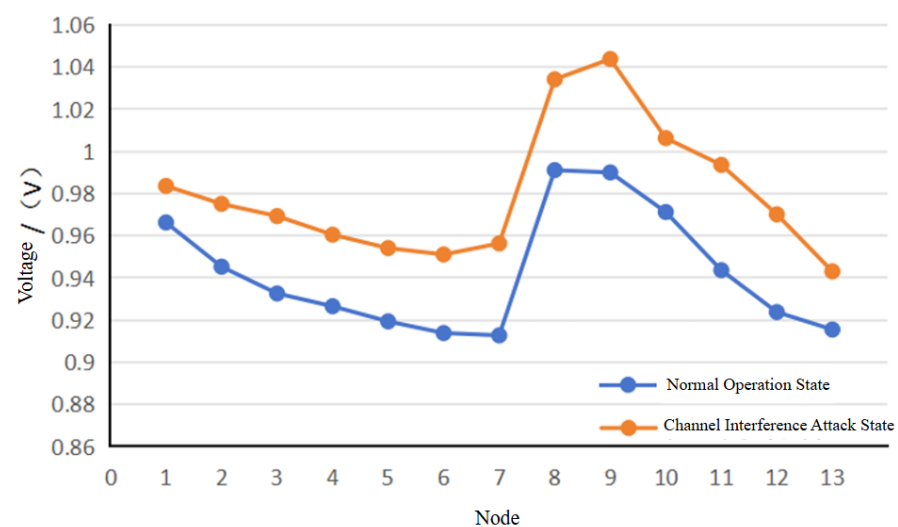


Figure 10. Nodal voltage distribution under channel interference at peak impact time.

Figure 11 presents the total feeder load trajectory under malicious code injection attacks, where load values reported to or controlled by the system are directly manipulated.

At 08:00, a load connection attack induces an instantaneous power increase of 1617 kW, causing the total feeder load to surge to 6874 kW and exceed the predefined operating threshold. This abrupt deviation triggers protective responses and illustrates how cyber manipulation of edge devices can generate sharp physical transients.

A load disconnection attack executed at the same time produces an abrupt reduction in feeder load to approximately 4900 kW. Although the direction of change differs, both cases demonstrate that data integrity attacks can drive the system into abnormal operating regions by creating false representations of demand or supply. Compared with channel interference, these attacks produce immediate state jumps rather than delayed accumulation, yet both mechanisms reduce operational margins and increase the likelihood of cascading effects.

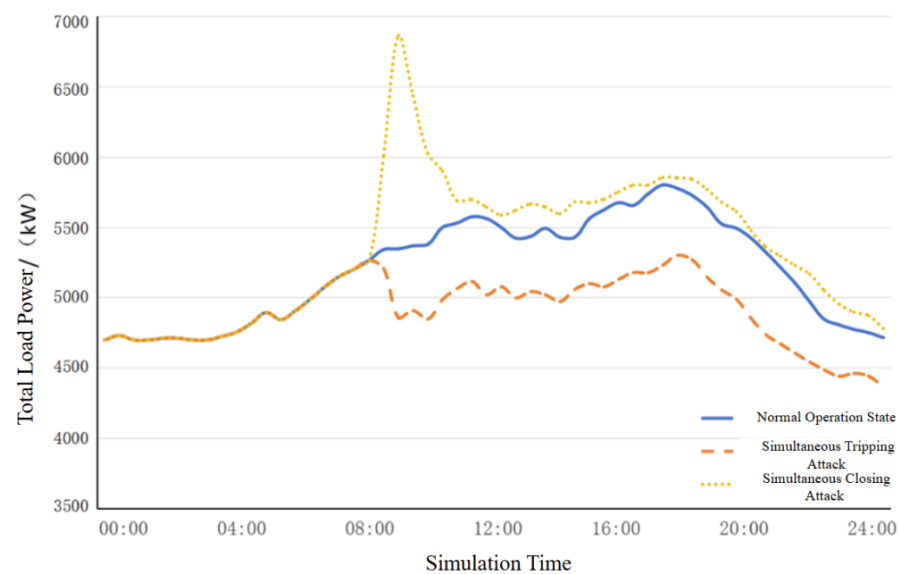


Figure 11. Total feeder load evolution under malicious code injection attacks.

The observed load and voltage trajectories indicate that cyber–physical attacks affect power system behavior through distinct dynamic pathways. Communication disruptions primarily introduce delayed responses and accumulated deviations, while data integrity attacks induce instantaneous state transitions. In both cases, deviations persist over extended time horizons and alter subsequent system responses, forming state trajectories that differ fundamentally from normal operation. These evolving trajectories constitute the basis for state transition modeling and dynamic risk quantification in the following analysis.

4.3. Dynamic Risk Assessment Based on MDP State Transitions

The state transition structure of the IEEE 14-bus system is first examined under the assumption that no attack has yet occurred. Starting from the initial secure system state ϕ , all reachable system states and their transition relationships are enumerated based on component connectivity and feasible attack actions. The resulting Markov Decision Process state transition tree is shown in Figure 12, where gateways (W), substations (S), and relays (R) are represented as discrete cyber–physical states. This baseline state tree characterizes the complete set of potential attack progressions under single-event conditions.

Under single-event assumptions, the system complies with the $(N - 1)$ security criterion, where the failure or compromise of any single component does not induce structural changes in the remaining state space. This property is reflected in the security metric results reported in Table 3. For substations S_2 and S_4 , identical security metric values

are obtained across all discount factor settings, indicating that both substations exhibit equivalent security importance when considered in isolation.

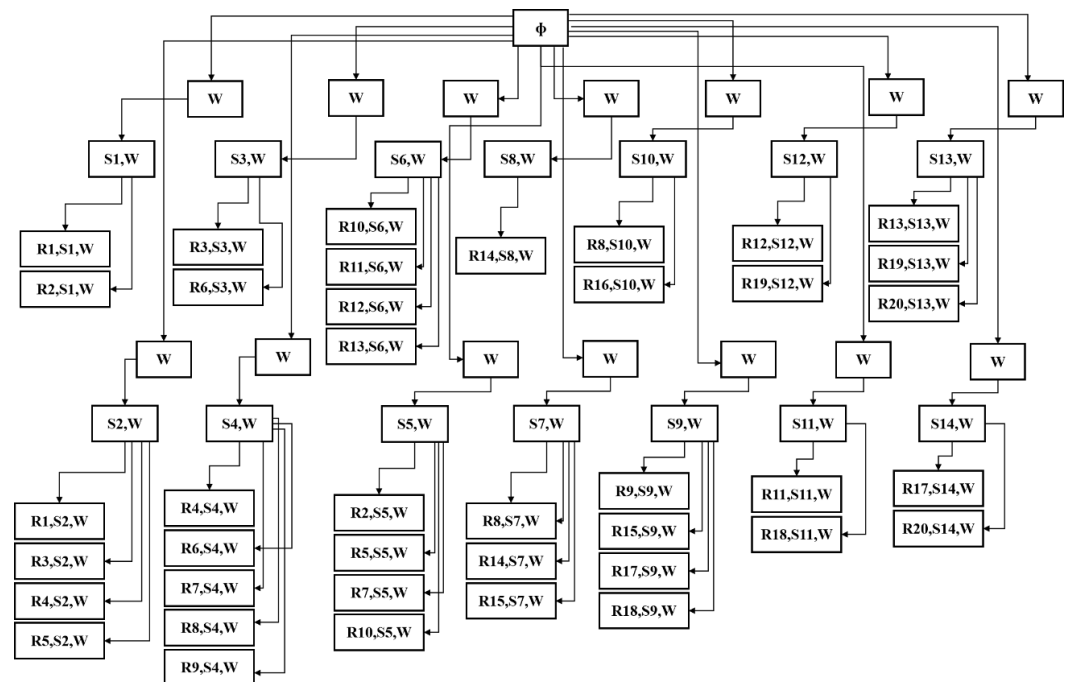


Figure 12. State transition tree for the IEEE 14-bus system under single-event conditions.

The discount factor γ plays a critical role in the dynamic risk assessment, reflecting the decision-maker's preference trade-off between near-term and forward risks. Specifically, a low value like $\gamma = 0.1$ represents a “short-sighted” perspective, focusing on the immediate physical impact of an attack. A moderate value of $\gamma = 0.5$ balances current damage with potential future consequences. In contrast, $\gamma = 0.9$ represents a forward-looking perspective, where the assessment accounts for long-term cascading effects and the accumulation of risks over time. While variations in γ affect the absolute magnitude of the security metric, they do not alter the relative ranking of nodes under single-event conditions.

Table 3. Security metric results under single-event conditions (dimensionless).

Attack Intention	$\gamma = 0.1$	$\gamma = 0.5$	$\gamma = 0.9$
Substation S_2	2.11	4.70	5.67
Substation S_4	2.11	4.70	5.67

Once an initial attack event is introduced, the system state no longer remains static. The occurrence of a compromised relay alters circuit operating conditions and enables additional attack opportunities along the same electrical path. To capture the nonlinear interaction between near-simultaneous events, a concurrent event detector is incorporated into the MDP formulation. This detector defines the temporal resolution of “concurrency” based on the primary protection clearing time (typically 100 ms to 500 ms in the IEEE 14-bus system). If multiple attacks occur within this window—before the grid can reach a new steady-state equilibrium—they are aggregated into a single simultaneous failure set T . This allows new system states to be generated when multiple attack events coexist, reflecting the physical reality that near-simultaneous disturbances collectively drive power flow redistribution. The resulting state transition extension is illustrated in Figure 13, where newly introduced states are highlighted. With concurrent events considered, the total number of reachable system states increases from 48 to 117, substantially expanding

the set of feasible attack paths and capturing the synergistic risk escalation that single-event models overlook. Sensitivity tests on the window size (ranging from 50 ms to 1 s) indicate that while the state space size varies, the identified critical attack paths remain consistent, demonstrating the robustness of the detector against minor variations in protection settings or communication jitters.

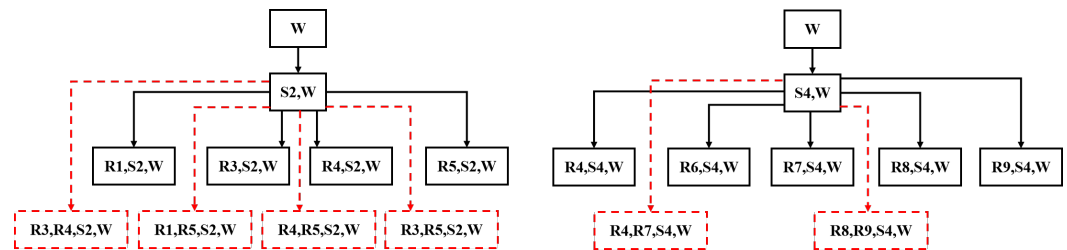


Figure 13. State transition tree extension under concurrent security events.

The expansion of the state space directly affects the distribution of security risk across system components. As shown in Table 4, the security metric values under concurrent-event conditions differ markedly from those obtained under single-event assumptions. After substation S_2 is compromised, the security importance of substation S_4 increases across all discount factor settings. For $\gamma = 0.9$, the security metric associated with S_4 rises to 13.3, compared with 6.23 for S_2 , indicating a pronounced shift in system risk concentration.

Table 4. Security metric results under concurrent-event conditions (dimensionless).

Attack Intention	$\gamma = 0.1$	$\gamma = 0.5$	$\gamma = 0.9$
Substation S_2	3.41	5.81	6.23
Substation S_4	6.20	11.20	13.30

This change in relative security importance does not arise from additional attacks on S_4 itself, but from the altered system state induced by prior events. The results indicate that concurrent attack conditions modify the structure of the state transition tree and redistribute risk toward components that are not initially critical under single-event analysis. These observations motivate the identification of high-risk propagation paths and critical nodes based on cumulative risk, which is examined in the subsequent analysis.

The proposed security metric I serves as a dynamic risk indicator by integrating the stochastic cyber-attack transition probability (P_a) with the deterministic physical impact (R_a) through the recursive Bellman equation. As summarized in Table 5, under the representative setting of $\gamma = 0.9$, the security metric for substation S_4 escalates from 5.67 in the single-event scenario to 13.30 in the conditional concurrent scenario ($S_4|S_2$). This represents a risk enhancement of approximately 2.35 times, a result that is statistically significant as confirmed by the 95% confidence intervals [12.63, 13.97]. It is essential to clarify that this 2.3-fold risk escalation is rooted in nonlinear cyber–physical coupling rather than a simple temporal accumulation of independent events. In the IEEE 14-bus system, the initial failure at S_2 reconfigures the network topology, causing power flow to deviate toward neighboring corridors and narrowing the security margins of the remaining branches. When S_4 is subsequently attacked, the system is already in a “pre-stressed” state. This causal interaction is captured by the Bellman-based metric, where the synergistic impact of S_2 and S_4 on line flows, combined with the attacker’s knowledge gain, leads to a disproportionate and non-linear increase in the overall risk index.

Table 5. Comparative Analysis of Security Metrics: Single vs. Conditional Events.

Attack Scenario	Coupling γ	Mean I	95% CI	SD	Escalation Ratio
Single (S_2)	0.1	2.11	[1.96, 2.26]	0.08	1.00×
	0.5	4.70	[4.42, 4.98]	0.14	1.00×
	0.9	5.67	[5.33, 6.01]	0.17	1.00×
Concurrent ($S_2 S_4$)	0.1	3.41	[3.17, 3.65]	0.12	1.62×
	0.5	5.81	[5.46, 6.16]	0.18	1.24×
	0.9	6.23	[5.92, 6.54]	0.16	1.10×
Concurrent ($S_4 S_2$)	0.1	6.20	[5.83, 6.57]	0.19	2.94×
	0.5	11.20	[10.53, 11.87]	0.34	2.38×
	0.9	13.30	[12.63, 13.97]	0.34	2.35×

Note: $S_i|S_j$ denotes the security metric of S_i under the condition that S_j has already been attacked.

4.4. Identification of Critical Nodes and High-Risk Propagation Paths

The expanded state transition tree obtained under concurrent-event conditions enables explicit identification of attack propagation paths and their associated risks. Each path represents a feasible sequence of state transitions from an initial cyber–physical access point to a target relay or substation. To quantify the likelihood of successful attack progression along a given path, the success probability of an attack path r is defined as the product of state transition probabilities associated with all transitions along that path,

$$P_r = \prod P_a(s_i, s_j), \quad (13)$$

where $P_a(s_i, s_j)$ denotes the transition probability from state s_i to state s_j . This formulation captures the cumulative effect of multiple vulnerabilities exploited along a single attack route.

Based on the IEEE 14-bus system topology and the state transition probabilities derived from component vulnerabilities, a complete set of feasible attack paths is generated from the state transition tree. Table 6 summarizes representative attack paths, their lengths, and corresponding success probabilities. The results indicate that attack paths with fewer transition steps tend to exhibit higher success probabilities, reflecting reduced exposure to defensive interruption. Among the enumerated paths, the path $W \rightarrow S_2 \rightarrow R_2$ achieves the highest success probability of 0.528 with only three attack steps, identifying it as a dominant high-risk propagation path.

Table 6. Attack path information derived from the state transition tree.

Path ID	Attack Path	Number of Steps	Success Probability
Path 1	$W \rightarrow S_1 \rightarrow R_1$	3	0.499
Path 2	$W \rightarrow S_2 \rightarrow S_1 \rightarrow R_1 \rightarrow R_2$	5	0.412
Path 3	$W \rightarrow S_2 \rightarrow R_2$	3	0.528
Path 4	$CC \rightarrow W \rightarrow R_1 \rightarrow R_2$	4	0.264
Path 5	$CC \rightarrow W \rightarrow R_1$	3	0.275
Path 6	$CC \rightarrow W \rightarrow R_2$	3	0.264
Path 7	$CC \rightarrow R_1$	2	0.430
Path 8	$CC \rightarrow R_1 \rightarrow R_2$	3	0.413
Path 9	$CC \rightarrow R_2$	2	0.413

Although several attack paths exhibit comparable success probabilities, their structural characteristics differ substantially. For instance, Paths 8 and 9 achieve identical success probabilities while involving different numbers of intermediate states. Longer paths introduce additional components whose compromise may alter subsequent system states, increasing uncertainty in downstream risk propagation. This observation indicates that

attack path length alone is insufficient to characterize system risk, and that the interaction between intermediate states and concurrent events must be considered.

Critical nodes are identified by examining how attack paths intersect and how their compromise alters the distribution of risk across the state transition tree. Nodes such as substations S_2 and S_4 appear in multiple high-probability paths and act as convergence points for attack propagation. Under concurrent-event conditions, compromise of these nodes not only enables additional attack routes but also modifies the system operating state, thereby increasing the vulnerability of other components that are not directly targeted. This mechanism explains the observed shift in security importance reported in the dynamic risk assessment results.

The identification of high-risk propagation paths and critical nodes provides a structural basis for risk-aware defense prioritization. Components that lie on short, high-probability attack paths or serve as convergence points for multiple paths contribute disproportionately to cumulative system risk. Protecting these components can reduce both the likelihood of successful attack progression and the extent of risk amplification under concurrent cyber–physical events.

4.5. Computational Efficiency and Convergence Analysis

To address the practical applicability of the proposed framework, we evaluate its computational burden and convergence behavior. The security metric I is obtained through a value iteration process. Figure 14 illustrates the convergence characteristics under different scenarios and discount factors ($\gamma = 0.1, 0.5, 0.9$).

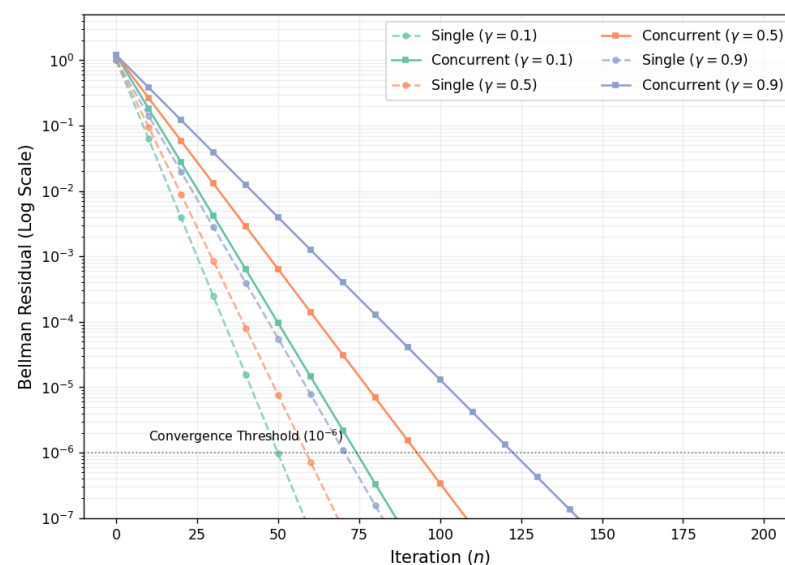


Figure 14. Convergence behavior of the security metric I (Bellman residual) for single and concurrent attack scenarios across varying γ .

As shown in the figure, the Bellman residual—representing the maximum change in the metric I between successive iterations—demonstrates consistent exponential decay. For $\gamma = 0.9$, the process converges within approximately 170 iterations to a tolerance of 10^{-6} . While the concurrent attack scenario (solid lines) involves a more complex state space (117 states) compared to the single event (48 states), the convergence rate remains robust. In terms of execution time, the computation for the IEEE 14-bus system completes in approximately 3.2 s on a standard i7 CPU, confirming that the framework can support near-real-time risk monitoring in practical power grids.

5. Conclusions

A dynamic risk assessment framework for DER-integrated power grids under concurrent cyber–physical attacks is presented. Time-synchronized co-simulation couples power system dynamics with communication network behavior, enabling cyber-layer attack actions to be consistently mapped to physical-layer state disturbances. Based on these trajectories, an MDP-based state transition tree models the evolution of system risk under both single-event and concurrent attack conditions. Experimental results show that the cumulative risk under concurrent conditions is approximately 2.3 times that of single-event scenarios, highlighting the synergistic escalation of multi-node compromises.

Beyond theoretical assessment, this framework provides a quantitative foundation for real-world grid resilience. By identifying high-risk propagation paths and state-dependent critical nodes, the model enables operators to prioritize defense resources (e.g., firewall hardening and intrusion detection) on nodes that exhibit the highest risk-escalation potential rather than just static vulnerability. Furthermore, the recursive nature of the proposed metric allows for proactive operational decision-making, such as triggering pre-emptive DER re-dispatch or load shedding before localized disturbances cascade into systemic failures under evolving concurrent threats.

6. Discussion

In this section, we discuss the technical extensibility and the inherent limitations of the proposed dynamic risk assessment framework, specifically focusing on FDI attacks, communication interruptions, and the refinement of vulnerability modeling.

6.1. Generalization to FDI Attacks

FDI attacks typically aim to compromise the integrity of state estimation or control commands by injecting malicious data into the feedback loop. While our current case studies focus on direct physical disruptions, the mathematical backbone of our MDP-based framework is inherently compatible with FDI scenarios. In our model, an FDI attack can be characterized as a malicious perturbation $\Delta u(t_k)$ to the control input or a bias in the observed state s . Since our security metric $I(s)$ is derived from the physical deviation of the grid, any FDI-induced instability will be quantitatively captured as an elevated risk value.

6.2. Impact of Communication Interruptions

Communication interruptions, such as packet loss or latency, affect data availability and can severely degrade the performance of event-triggered control systems. Within our framework, such interruptions can be modeled by adjusting the state transition probability $P_a(s, s')$. Specifically, a communication failure increases the uncertainty of the system transitions, potentially leading the system into a “vulnerable” state where the controller’s visibility is diminished. By incorporating an availability-aware factor into the MDP reward function, our framework can evaluate the risk of cascading failures triggered by the loss of critical control signals during concurrent attack events.

6.3. Limitations and Refinement of Vulnerability Modeling

It is essential to acknowledge that while our framework utilizes CVSS-based scores to determine the exploitation probability P_e , this approach primarily reflects the inherent severity of vulnerabilities rather than the actual likelihood in a defended environment. In practical grid operations, compensating controls—such as industrial firewalls between the Wide Area Network (W) and Substation (S_2)—can effectively reduce the actual exploitation probability below the theoretical CVSS base score. Although our current analysis provides a conservative risk upper bound, future work will focus on incorporating a dynamic

“defense correction factor” to quantify the effectiveness of specific security perimeters. This refinement will allow the framework to distinguish between theoretical vulnerability and the residual risk present under multi-layered defense-in-depth strategies.

It also should be noted that the current transition probability $P_a(s, s')$ is modeled based on vulnerability severity and an assumption of conditional independence between certain attack steps. While this provides a tractable mathematical framework, it may not fully capture the strategic interplay between a sophisticated attacker and proactive defense mechanisms (e.g., moving target defense or automated isolation). In reality, coordinated attackers may exhibit strategic dependencies that deviate from direct proportionality to static vulnerability scores. However, our inclusion of the Knowledge Gain coefficient K_k serves as a first step to relax this independence by dynamically adjusting success rates. Future work will incorporate game-theoretic models to better characterize the adversarial interactions and strategic interdependencies in cyber–physical attack–defense games.

6.4. Comparative Analysis with Existing Methods

To further demonstrate the superiority of the proposed framework, we compare its methodological logic with established studies. Specifically, [41] adopted a static attack tree transformation model that primarily focuses on the stochastic propagation time of attack steps within cyber space. However, it neglects the dynamic bi-directional feedback between the attack process and physical power grid states. Similarly, [39] utilized Markov Decision Processes (MDPs) to simulate the non-deterministic behavior of attackers, but their evaluation logic is largely confined to discrete cyber-component attack processes, failing to account for the continuous evolution of system physics and the adaptive knowledge gain of attackers.

In contrast, our framework bridges these gaps by integrating a fuzzy-logic-based capability factor and a physics-aware security index. This multi-dimensional coupling allows our model to capture the “synergistic effect” inherent in concurrent scenarios—a phenomenon where physical constraints and cyber actions reinforce each other. Unlike traditional cyber-only or static models that treat risk as a linear summation of isolated events, our approach identifies the non-linear risk escalation triggered by physical security margin contractions. This comparison highlights the necessity of considering cyber–physical interdependencies to prevent the significant underestimation of cascading risks in DER-integrated grids.

Author Contributions: Conceptualization, C.C. and Y.Z.; methodology, C.C.; software, C.C.; validation, J.L., Z.Z. and N.L.; formal analysis, Y.S.; investigation, C.C.; resources, J.L.; data curation, N.L.; writing—original draft preparation, C.C.; writing—review and editing, Y.Z.; visualization, Y.S.; supervision, J.L.; project administration, Z.Z.; funding acquisition, C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the Science and Technology Project of State Grid Henan Electric Power Company: Research on the Network and Data Security Protection System and Key Technologies for Distributed Resources in the New Power System (52170225000H).

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: We thank the reviewers for their valuable comments.

Conflicts of Interest: Authors Cen Chen, Jinghong Lan, Zheng Zhang and Nuannuan Li were employed by the company State Grid Henan Electric Power Research Institute. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Sani, S.B.; Celvakumaran, P.; Ramachandaramurthy, V.K.; Walker, S.; Alrazi, B.; Ying, Y.J.; Dahlan, N.Y.; Rahman, M.H.A. Energy storage system policies: Way forward and opportunities for emerging economies. *J. Energy Storage* **2020**, *32*, 101902. [\[CrossRef\]](#)
2. Said, D. A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities. *IEEE Eng. Manag. Rev.* **2022**, *51*, 76–107. [\[CrossRef\]](#)
3. Zhang, M.; Yang, X. Administrative framework barriers to energy storage development in China. *Renew. Sustain. Energy Rev.* **2021**, *148*, 111297. [\[CrossRef\]](#)
4. Wang, L.; Zhang, Q.; Liu, J.; Wang, G. Science mapping the knowledge domain of electrochemical energy storage technology: A bibliometric review. *J. Energy Storage* **2024**, *77*, 109819. [\[CrossRef\]](#)
5. Saha, P.; Akash, F.A.; Shovon, S.M.; Monir, M.U.; Ahmed, M.T.; Khan, M.F.H.; Sarkar, S.M.; Islam, M.K.; Hasan, M.M.; Vo, D.V.N.; et al. Grey, blue, and green hydrogen: A comprehensive review of production methods and prospects for zero-emission energy. *Int. J. Green Energy* **2024**, *21*, 1383–1397. [\[CrossRef\]](#)
6. Henderson, M.I.; Novosel, D.; Crow, M.L. Electric power grid modernization trends, challenges, and opportunities. In *IEEE Power Energy*; IEEE: Piscataway, NJ, USA, 2017.
7. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 1–33. [\[CrossRef\]](#)
8. Singhal, A.; Ou, X. Security risk analysis of enterprise networks using probabilistic attack graphs. In *Network Security Metrics*; Springer: Cham, Switzerland, 2017; pp. 53–73.
9. Presekal, A.; Ștefanov, A.; Rajkumar, V.S.; Palensky, P. Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Trans. Smart Grid* **2023**, *14*, 4007–4020. [\[CrossRef\]](#)
10. Schäfer, B.; Witthaut, D.; Timme, M.; Latora, V. Dynamically induced cascading failures in power grids. *Nat. Commun.* **2018**, *9*, 1975. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Yang, Y.; Guan, X.; Zhai, Q. Fast grid security assessment with N- k contingencies. *IEEE Trans. Power Syst.* **2016**, *32*, 2193–2203. [\[CrossRef\]](#)
12. Le, T.D.; Nguyen, H.P.T.; Huynh, K.T.; Beuran, R. Smart grid cyber-attack analysis and countermeasures. In Proceedings of the 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 20–22 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 590–595.
13. Khalaf, M.; Ayad, A.; Tushar, M.H.K.; Kassouf, M.; Kundur, D. A survey on cyber-physical security of active distribution networks in smart grids. *IEEE Access* **2024**, *12*, 29414–29444. [\[CrossRef\]](#)
14. Lu, Q.; Zhang, W. Integrating dynamic Bayesian network and physics-based modeling for risk analysis of a time-dependent power distribution system during hurricanes. *Reliab. Eng. Syst. Saf.* **2022**, *220*, 108290. [\[CrossRef\]](#)
15. Li, Y.; Zhang, H. Deep Reinforcement Learning-Based Approach for Identifying Critical Nodes in Cyber Physical Power Systems. *IEEE Trans. Reliab.* **2026**, *75*, 464–477. [\[CrossRef\]](#)
16. Li, Q.; Zhang, J.; Zhao, J.; Ye, J.; Song, W.; Li, F. Adaptive hierarchical cyber attack detection and localization in active distribution systems. *IEEE Trans. Smart Grid* **2022**, *13*, 2369–2380. [\[CrossRef\]](#)
17. Hopkinson, K.; Wang, X.; Giovanini, R.; Thorp, J.; Birman, K.; Coury, D. EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Trans. Power Syst.* **2006**, *21*, 548–558. [\[CrossRef\]](#)
18. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access* **2020**, *8*, 151019–151064. [\[CrossRef\]](#)
19. Abdelrahman, M.S.; Kharchouf, I.; Nguyen, T.L.; Mohammed, O.A. A hybrid physical co-simulation smart grid testbed for testing and impact analysis of cyber-attacks on power systems: Framework and attack scenarios. *Energies* **2023**, *16*, 7771. [\[CrossRef\]](#)
20. Wang, K.; Xu, J.; Li, G.; Tai, N.; Tong, A.; Hou, J. A generalized associated discrete circuit model of power converters in real-time simulation. *IEEE Trans. Power Electron.* **2018**, *34*, 2220–2233. [\[CrossRef\]](#)
21. Bouslimani, M.; Benbouzid-Si Tayeb, F.; Amirat, Y.; Benbouzid, M. Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures. *Appl. Sci.* **2025**, *15*, 12367. [\[CrossRef\]](#)
22. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Grunewald, D.; Lützenberger, M.; Chinnow, J.; Bye, R.; Bsufka, K.; Albayrak, S. Agent-based network security simulation. In Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems (AAMAS), Taipei, Taiwan, 2–6 May 2011; pp. 1325–1326.
24. Egert, R.; Cordero, C.G.; Tundis, A.; Mühlhäuser, M. HOLEG: A simulator for evaluating resilient energy networks based on the Holon analogy. In Proceedings of the 2017 IEEE/ACM 21st International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Rome, Italy, 18–20 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.

25. Wermann, A.G.; Bortolozzo, M.C.; da Silva, E.G.; Schaeffer-Filho, A.; Gaspary, L.P.; Barcellos, M. ASTORIA: A framework for attack simulation and evaluation in smart grids. In Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS), Istanbul, Turkey, 25–29 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 273–280.
26. Wang, X.; Liu, Y.; Jiao, K.; Liu, P.; Luo, X.; Liu, T. Intrusion device detection in fieldbus networks based on channel-state group fingerprint. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 4012–4027. [[CrossRef](#)]
27. Diao, X.; Zhao, Y.; Li, R.; Chakhchoukh, Y.; Johnson, B.; Le Blanc, K.; Smidts, C. A Modular Dynamic Probabilistic Risk Assessment Framework for Electric Grid Cybersecurity. *Eng. Rep.* **2025**, *7*, e70377. [[CrossRef](#)]
28. Pasiadis, A.; Kotsiopoulos, T.; Lazaridis, G.; Drosou, A.; Tzovaras, D.; Sarigiannidis, P. Cyber-resilience enhancement framework in smart grids. In *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*; Springer: Cham, Switzerland, 2023; pp. 363–386.
29. Arjmand, M.; Akbari, B.; Ghaeini, H.R. From voltage to vulnerability: A comprehensive survey of dynamic security risk assessment techniques in smart grids. *Int. J. Inf. Secur.* **2026**, *25*, 7. [[CrossRef](#)]
30. Khosravi-Farmad, M.; Ghaemi-Bafghi, A. Bayesian decision network-based security risk management framework. *J. Netw. Syst. Manag.* **2020**, *28*, 1794–1819. [[CrossRef](#)]
31. Eom, T.; Hong, J.B.; An, S.; Park, J.S.; Kim, D.S. A Framework for Real-Time Intrusion Response in Software Defined Networking Using Precomputed Graphical Security Models. *Secur. Commun. Netw.* **2020**, *2020*, 7235043. [[CrossRef](#)]
32. Al-Eiadeh, M.R.; Abdallah, M. Genigraph: A genetic-based novel security defense resource allocation method for interdependent systems modeled by attack graphs. *Comput. Secur.* **2024**, *144*, 103927. [[CrossRef](#)]
33. Wadhawan, Y.; AlMajali, A.; Neuman, C. A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronics* **2018**, *7*, 249. [[CrossRef](#)]
34. Lu, Q.; Li, J.; Peng, Z.; Wu, L.; Ni, M.; Luo, J. Detecting the cyber-physical-social cooperated APTs in high-DER-penetrated smart grids: Threats, current work and challenges. *Comput. Netw.* **2024**, *254*, 110776. [[CrossRef](#)]
35. Cheimonidis, P.; Rantos, K. A novel proactive and dynamic cyber risk assessment methodology. *Comput. Secur.* **2025**, *154*, 104439. [[CrossRef](#)]
36. Cheimonidis, P.; Rantos, K. A dynamic risk assessment and mitigation model. *Appl. Sci.* **2025**, *15*, 2171. [[CrossRef](#)]
37. Yao, P.; Yang, Q.; Wang, W. Dynamic cross-layer security risk assessment and mitigation for cyber-physical power systems. *Reliab. Eng. Syst. Saf.* **2025**, *261*, 111027. [[CrossRef](#)]
38. Duo, W.; Wang, S.; Zhou, M. Multi-step Sensor Attackability in Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2025**, *70*, 4794–4800. [[CrossRef](#)]
39. Bashar, A.; Muhammad, S.; Mohammad, N.; Khan, M. Modeling and analysis of MDP-Based security risk assessment system for smart grids. In Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 8–10 January 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 25–30.
40. Zhang, Y.; Ni, M. Security-oriented cyber-physical risk assessment for cyberattacks on distribution system. *Appl. Sci.* **2023**, *13*, 11569. [[CrossRef](#)]
41. Sadu, A.; Stevic, M.; Wirtz, N.; Monti, A. A stochastic assessment of attacks based on continuous-time Markov chains. In Proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon), Gammarth, Tunisia, 28 September–1 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 11–16.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.