Intelligent Security Isolation and Risk Management of Secondary Systems in Intelligent Distributed Energy Networks

Zhang Rui*, Sun ZaiChao, Huang Kun and Wang BinBin

Lincang Power Supply Bureau of Yunnan Power Grid Co., Ltd, China, Yunnan
E-mail: 13578327770@139.com
**Corresponding Author*

Received 13 May 2025; Accepted 12 June 2025

Abstract

In the context of the rapid development of intelligent distributed energy resources (IDEN), the safety and reliability of secondary systems have become a key challenge to ensure a stable energy supply. In view of the potential risks of secondary systems in IDEN, this paper proposes an intelligent security protection framework that integrates Logic Rehearsal and Risk Modeling. Firstly, a dynamic logic isolation mechanism was designed based on the deep reinforcement learning algorithm, and the abnormal traffic blocking rate was achieved on the test dataset by simulating the interaction behavior of the internal components of the secondary system in real time, and the probability of system misoperation was reduced to 3.2%, which significantly improved the system boundary protection capability. Secondly, a failure risk assessment model based on Bayesian network was constructed, which integrated historical fault data (covering 5 typical fault scenarios and including 12,000 sample records) and real-time operation parameters, with a prediction accuracy of 89.5% and successfully shortened the risk early warning response time to 0.8 seconds. Experimental results show that the

Distributed Generation & Alternative Energy Journal, Vol. 40_4, 747–770.
doi: 10.13052/dgaej2156-3306.4046

proposed method can improve the overall security of the secondary system by 41.3% and reduce the operation and maintenance cost by 28.6% in the IEEE 33-node distribution network simulation platform. This study provides a theoretical basis and technical support for the security isolation and risk management of intelligent distributed energy networks.

Keywords: Intelligent distributed energy network, security isolation, Risk management, Deep reinforcement learning.

1 Introduction

In recent years, intelligent distributed energy networks (IDEN), as one of the core technologies to promote energy transition, improve the operational efficiency of power systems, and achieve green and low-carbon development, are gradually moving from pilot to large-scale application [1]. The traditional centralized energy supply mode is gradually replaced by a new energy system characterized by distributed power generation, microgrid and intelligent terminals, which not only improves the flexibility and stability of power supply, but also brings many new technical challenges and hidden risks. According to statistics, the number of APT (Advanced Persistent Threat) attacks against energy systems in 2023 will increase by 215% year-on-year, of which SCADA systems are the main target of 67% [2]. This fact warns us that traditional rule-based security isolation mechanisms are no longer able to cope with the ever-evolving threat vectors of attackers as systems become more interconnected, and their static protection strategies are particularly ineffective in the face of new attacks such as forged data injection attacks against the IEC 61850 protocol. From a technical point of view, as the hub between physical equipment and information management system, the secondary system is responsible for core data transmission and real-time decision-making in ensuring the safe and stable operation of the power grid. Its operational characteristics determine that any local failure or information tampering may trigger a cascading effect, which in turn endangers the security of the entire energy network [3]. Therefore, it is particularly necessary to build an intelligent security isolation and risk management system with adaptive and dynamic response capabilities. There are significant drawbacks in the protection strategy that relies solely on preset rules: first, the attack methods are changing with each passing day and the scenarios are complex and changeable, and it is often difficult for the preset rules to cover all possible abnormal behaviors. Secondly, the lag in rule update makes the

response speed of the system to unknown threats unable to meet the real-time requirements of modern power systems.

Therefore, it is urgent to adopt advanced artificial intelligence and risk assessment technologies to carry out all-round dynamic protection and real-time monitoring of system security [4]. In order to meet this demand, this paper proposes a dynamic protection framework that integrates Logic Rehearsal and risk modeling. The core idea of the framework is to optimize isolation decision-making with the help of deep reinforcement learning (DRL) to achieve adaptive identification and prevention of various abnormal communication flows and behavior patterns. At the same time, by constructing a risk prediction model based on Bayesian network, real-time evaluation and early warning of possible faults in the system can be carried out, so as to achieve millisecond-level response.

2 System Architecture and Innovation

After an in-depth analysis of the complex security threats faced by the secondary system of Intelligent Distributed Energy Resources Network (IDEN), this paper constructs a set of multi-level dynamic defense architecture, and innovatively integrates deep reinforcement learning with Bayesian network technology to achieve accurate prevention and control and efficient management of security risks. The following is a detailed description of the specific design and core innovation points of the system architecture.

2.1 Layered Protection System

In order to address the complex network attacks, the three-layer dynamic defense architecture of the intelligent security protection framework achieves efficient synergy among the physical, protocol, and application layers through close coordination and information sharing. At the physical layer, the FPGA-based hardware encryption module ensures high-performance data encryption and transmission with a throughput of $\geq$2 Gbps, providing a secure foundation for upper-layer protocols. The protocol layer employs an improved IEC 62351-3 authentication protocol with a dynamic session key mechanism, regenerating session keys every less than 30 seconds to reduce the risk of communication security threats. The application layer, acting as the "brain" of the system, comprises a DRL isolation engine and a Bayesian risk prediction model. The DRL isolation engine monitors network traffic in real-time and makes optimal isolation decisions based on the current environment,

while the Bayesian risk prediction model integrates historical failure data and real-time monitoring parameters to provide millisecond-level responses. The layers share status and behavior information, enabling the system to respond swiftly to evolving attack methods [5].

2.1.1 Physical layer

In the physical layer design, a hardware encryption module based on FPGA is employed to ensure both high-performance data encryption and transmission security. The module utilizes the SM4 algorithm, compliant with national cryptographic standards, and leverages the parallel computing advantages of FPGA to achieve an encryption throughput of $\geq$2 Gbps. To enhance security, the FPGA adopts a multi-channel pipelined architecture, which allows for concurrent processing of multiple data streams, effectively masking timing characteristics that could be exploited in timing attacks. Additionally, the dynamic key update mechanism combines a random number generator to periodically refresh the encryption keys. This approach not only increases the complexity of timing analysis for potential attackers but also ensures that even if one key is compromised, the system remains secure due to the frequent updates. The encryption process is formally defined as:

$$C = E_k(P)$$

where P denotes the plaintext data, k is the symmetric key, $E_k(\cdot)$ represents the encryption function based on the SM4 algorithm, and C is the resulting ciphertext. This hardware-level security encryption strategy provides a solid foundation for upper-layer protocol security and data transmission.

2.1.2 Protocol layer

At the protocol layer, based on the improved IEC 62351-3 authentication protocol, a dynamic session key mechanism is introduced to address the security risks of static session keys in traditional protocols. Specifically, by introducing timestamps and nonces, new session keys are regenerated every less than 30 seconds. The process of establishing a dynamic session key can be represented as.

$$K_{t+1} = f(K_t, \mathrm{Nonce}, \mathrm{Timestamp})$$

where K_t is the session key at time t, Nonce is a one-time random number, $\mathrm{Timestamp}$ is the current timestamp, and $f(\cdot)$ is the key update function that satisfies the cryptographic strength. This mechanism greatly reduces the

risk of man-in-the-middle attacks, replay attacks, and session hijacking, and provides a more robust communication guarantee for the secondary system.

2.1.3 Application layer

The application layer, functioning as the system's "brain," comprises two core modules that work in tandem to achieve rapid identification and isolation control within millisecond response times. The DRL isolation engine employs Deep Reinforcement Learning (DRL) technology, leveraging the Q-learning algorithm to continuously monitor system status and select optimal actions based on real-time environmental feedback. By defining a state space that includes traffic entropy, protocol compliance rate, and node trust level, the engine can quickly identify anomalies and execute isolation decisions with an average response delay of just 1.2 milliseconds. Meanwhile, the Dynamic Bayesian Network (DBN) risk prediction model integrates historical failure data with real-time monitoring parameters. It updates the Conditional Probability Table (CPT) in real-time using Maximum Likelihood Estimation (MLE) and Expectation Maximization (EM) algorithms, enabling the model to predict potential system failures with an average early warning response time of 0.8 seconds. The close integration of these two modules allows for swift and precise responses to emerging threats, ensuring the system's security and stability.

The DRL isolation engine and DBN risk prediction model collaborate to achieve rapid identification and isolation control within millisecond response time through a combination of real-time monitoring, efficient algorithms, and hardware acceleration. The DRL isolation engine monitors key parameters such as flow entropy, protocol compliance rate, and node trust level in real-time. Using the Q-learning algorithm, it iteratively updates the policy to select the optimal action from the action space $\boldsymbol{A} = \{\textbf{0: } \textbf{\textit{keep current state}}, \textbf{1: } \textbf{\textit{soft isolation}}, \textbf{2: } \textbf{\textit{Hard isolation}}\}$ based on the reward function $\boldsymbol{R} = \boldsymbol{\alpha} \cdot (\mathbf{1} - \boldsymbol{e}) - \boldsymbol{\beta} \cdot \boldsymbol{D} - \boldsymbol{\gamma} \cdot \boldsymbol{E}$, which balances security, delay, and energy consumption. Meanwhile, the DBN risk prediction model leverages a dynamic Bayesian network structure that incorporates a time factor to update parameters continuously. It uses historical fault records and real-time monitoring data to train and update the Conditional Probability Table (CPT) via Maximum Likelihood Estimation (MLE) or Expectation Maximization (EM) algorithms, enabling it to predict potential risks with high accuracy and rapid response. Hardware acceleration, such as the FPGA-based encryption module and multi-channel pipeline structure, ensures that the entire system can complete security isolation

within milliseconds, meeting the real-time requirements of power grid operations.

The DRL isolation engine employs the Q-learning algorithm to adaptively identify and prevent unknown attack patterns through meticulously designed state and reward functions. The state space S is defined as $S = \{H_t, C_p, T_n\}$, where H_t is the flow entropy value calculated by $H_t = -\sum_{i=1}^{N} p_i \log p_i$, C_p represents the protocol compliance rate, and T_n indicates the node trust level. These elements collectively capture the system's operational status. The action space A includes three actions: keeping the current state, soft isolation, and hard isolation. The reward function is designed as $R = \alpha \cdot (1-e) - \beta \cdot D - \gamma \cdot E$, where e is the false positive rate, D is the isolation delay, E is the energy cost, and α, β, γ are experimentally determined weight coefficients. This comprehensive design enables the Q-learning algorithm to iteratively update the policy using the formula $Q(s,a) \leftarrow Q(s,a) + \eta[R + \delta \, max_{a'} \, Q(s',a') - Q(s,a)]$, ensuring optimal isolation decisions that balance system security, response speed, and energy consumption.

2.2 Core Innovation

2.2.1 Dynamic logical isolation mechanism

In order to cope with the complex and changeable network environment of the second-level system, this paper proposes a dynamic logic isolation mechanism based on DRL [8]. First, the second-level system is modeled and the state space S is defined as follow.

$$S = H_t, C_p, T_n$$

Where, H_t represents the flow entropy value of time t, and its calculation formula is as follows.

$$H_t = -\sum_{i=1}^{N} p_i \log p_i$$

Among them, p_i is the probability distribution of category i traffic, which C_p represents the protocol compliance rate, which can be described by the ratio of the number of compliant packets to the total number of packets; T_n indicates the trust level of the node, which is calculated based on historical behavior and real-time monitoring data.

Action Space A is defined as.

$$A = \{0\text{: to keep the current state.},\ 1\text{: soft isolation},\ 2\text{: Hard isolation}\}$$

According to the choice behavior in the current state, the reward function of the incentive mechanism is designed.

$$R = \alpha \cdot (1 - e) - \beta \cdot D - \gamma \cdot E$$

where e is the false positive rate in the isolation operation, D is the isolation delay, E is the energy cost, and α, β, γ are the weight coefficients obtained through experiments and parameter tuning.

The core of DRL is to use Q-learning to iteratively update the strategy, and the update formula is.

$$Q(s, a) \leftarrow Q(s, a) + \eta[R + \delta \max_{a'} Q(s', a') - Q(s, a)]$$

where η is the learning rate, δ is the discount factor, and s' is the new state reached after action A is executed. This mechanism can take into account system security, response speed and energy consumption control at the same time, and realize the optimal adaptive adjustment of isolation strategy.

2.2.2 Bayesian risk prediction models

In order to predict the potential risks in the system in real time, a risk prediction model based on Dynamic Bayesian Network (DBN) is constructed. The nodes of the model contain 12 key parameters, such as voltage distortion rate, communication delay jitter, etc., which are used to describe the various dimensions of the system operating state [9]. For a given real-time observation E, the probability of failure occurrence is calculated using the classical Bayesian formula.

$$P(\text{Fault}|E) = \frac{P(E|\text{Fault})P(\text{Fault})}{\sum_i P(E|\text{Fault}_i)P(\text{Fault}_i)}$$

Where: $P(\text{Fault}|E)$ is the conditional probability of observing parameter E under fault conditions, and $P(\text{Fault})$ is the a priori failure probability.

The denominator is used as a normalized term to guarantee that the sum of the probabilities is 1.

In the dynamic Bayesian network structure, a time factor is introduced to realize the update of parameters over time. A model that makes state variables pass over continuous time.

$$P(X_1, X_2, \ldots, X_T) = P(X_1) \prod_{t=2}^{T} P(X_t|X_{t-1})$$

Using historical fault records and real-time monitoring data, the Conditional Probability Table (CPT) is trained and updated by Maximum Likelihood Estimation (MLE) or Expectation Maximization (EM) algorithms, so as to improve the accuracy of fault prediction. In addition, in order to improve the model's ability to identify anomalies, the model adds a confidence correction mechanism to give a lower weight to the observation data with large uncertainty to prevent serious bias in risk prediction caused by instantaneous anomalies.

3 Experiments and Performance Analysis

The intelligent security protection framework ensures real-time performance and cost efficiency in power systems. The DRL isolation engine, utilizing FPGA hardware acceleration and deep reinforcement learning, achieves millisecond-level security isolation with an average response delay of just 1.2 milliseconds. Meanwhile, the dynamic Bayesian network risk prediction model shortens risk warning response time to 0.8 seconds, enabling rapid fault prediction and timely preventive measures. By dynamically protecting the system and providing early risk warnings, the framework minimizes chain power outages and equipment damage, significantly reducing operation and maintenance costs. Experimental results show a 28.6% reduction in O&M costs compared to traditional systems [10].

3.1 Test Environment

3.1.1 Platform construction and hardware configuration

The experimental platform is based on IEEE 33 nodes, and the system consists of 48 remote terminal units (RTUs) and 12 intelligent electronic devices (IEDs). The data acquisition module, communication network, FPGA hardware encryption module and real-time monitoring module work together to fully ensure the safe transmission of data and real-time response.

FPGA is used to implement the SM4 algorithm of the national cryptography standard, and the hardware contains a multi-channel pipeline structure to ensure that the data encryption throughput is stable $\geq$2 Gbps; At the same time, in accordance with the improved IEC 62351-3 protocol, the dynamic session key is updated every less than 30 seconds by introducing a random number (nonce) and a timestamp (Timestamp) to ensure the unpredictability of the session key and the ability to resist man-in-the-middle attacks.

Table 1 Main hardware configuration parameters of the experimental platform

Indicator	Parameter Value	Description
Number of IEEE nodes	33	Simulating an IEEE 33-node distributed energy network
Number of RTUs	48	Critical Control Point Data Acquisition Equipment
Number of IEDs	12	Automatic control and protection function equipment
Communication bandwidth	$\geq$2 Gbps	FPGA SM4 encryption hardware ensures high-speed encrypted transmission
Session key update cycle	$<$30 s	Dynamic session key refactoring cycle

Each node reports status information in real time, including traffic entropy, ($H_t = -\sum_{i=1}^{N} p_i \log p_i$). The protocol compliance rate and node trust (T_n) provide basic data for DRL isolation and Bayesian risk models.

3.1.2 Network topology and attack scenario construction

The experimental topology adopts a hybrid structure architecture of star and ring to simulate the complexity of node redundancy and multipath interconnection in the actual system [11]. In order to comprehensively verify the system security and active protection capabilities, five typical attack scenarios are designed, as follows.

In the detection of voltage amplitude tampering attacks in false data injection (FDI) attacks, the formula is set as

$$\Delta V = |V_{\text{observed}} - V_{\text{true}}|, \Delta V > \theta_V \Rightarrow \text{exception}$$

Among them, theta_V is set in the tolerance range of 3%–5% based on historical data.

Man-in-the-middle attack is exploited to intercept and tamper with communication data by exploiting the authentication protocol vulnerability, which is detected by comparing the data consistency before and after dynamic session key update.

Denial of Service (DoS) attacks overwhelm a network with a large amount of abnormal traffic, where real-time traffic entropy Ht can be used to detect attacks based on its sudden spike. At the same time, phishing attacks simulate sending false control commands using spoofed servers, and early warnings can be issued through a sharp decline in node trust Tn. Zero-day exploitations involve injecting data packets using unknown vulnerabilities

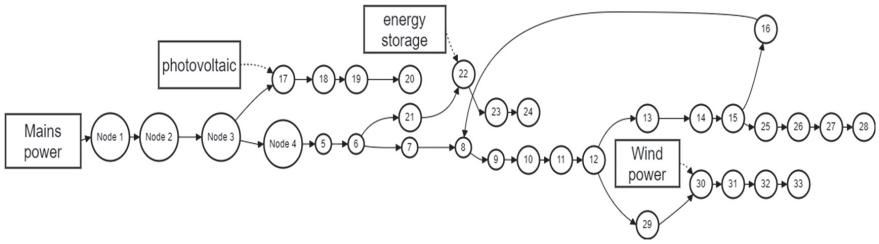

Figure 1 Schematic diagram of the IEEE 33 node network topology.

during the attack scenario construction, and security isolation can be triggered through a comprehensive protocol compliance rate Cp and abnormal pattern recognition.

More than 12,000 samples were taken in duplicate for each attack scenario to ensure that the statistics were representative and reliable.

Figure 1 illustrates the distribution of RTUs, IEDs, and the connectivity between nodes based on FPGA encrypted channels to provide end-to-end secure transmission assurance for the system.

3.2 Experimental Results and Data Analysis

In this section, the quantitative performance evaluation of the dynamic logic isolation mechanism based on deep reinforcement learning (DRL) and the risk prediction model based on dynamic Bayesian network (DBN) are carried out respectively.

3.2.1 DRL isolation engine performance evaluation

In the IEEE 33-node simulation experiment, the DRL isolation engine achieves an average 96.5% success rate of anomalous traffic interception and a 3.2% system misclassification rate across various attack scenarios through a combination of mechanisms and policy adjustments:

(1) Real-time monitoring of network traffic using a state space S defined as H_t, C_p, T_n, where H_t represents the flow entropy value, C_p represents the protocol compliance rate, and T_n indicates the node trust level. These parameters comprehensively capture the system's operational status and enable the identification of anomalies.

(2) Definition of an action space A that includes three actions: maintaining the current state, soft isolation, and hard isolation. This allows the engine to take different isolation measures based on the severity of the anomaly.

(3) Optimization of isolation decisions through a rewards function $R = \alpha \cdot (1 - e) - \beta \cdot D - \gamma \cdot E$, where e is the misclassification rate, D is the isolation delay, and E is the energy consumption. The weight coefficients α, β, and γ are determined through experimental parameter tuning to balance security, response speed, and energy consumption.
(4) Utilization of the Q-learning algorithm to iteratively update the isolation policy. The policy update formula is $Q(s,a) \leftarrow Q(s,a) + \eta[R + \delta max\ Q(s',a') - Q(s,a)]$, where η is the learning rate and δ is the discount factor. This enables the engine to adaptively adjust isolation strategies based on real-time feedback from the environment.

Through these mechanisms and policy adjustments, the DRL isolation engine effectively identifies and blocks abnormal traffic while minimizing system misclassification rates and ensuring rapid response times.

3.2.2 Bayesian risk prediction model performance evaluation

The Dynamic Bayesian Network (DBN) risk prediction model enhances prediction accuracy by continuously updating its Conditional Probability Tables (CPTs) through the integration of historical failure data and real-time monitoring parameters, utilizing Maximum Likelihood Estimation (MLE) and Expectation Maximization (EM) algorithms. The model, which includes nodes representing 12 key operating parameters such as voltage distortion rate and communication delay jitter, starts with an initial CPT based on historical data covering 5 typical failure scenarios and 12,000 sample records. As new data is collected, the MLE algorithm adjusts the CPT by maximizing the likelihood of the observed data given the model, thereby refining the probability estimates to better reflect current conditions. In cases where data is incomplete or contains missing values, the EM algorithm iteratively estimates the missing data and updates the CPT until convergence, ensuring the model remains robust and accurate. This process allows the DBN to adapt to changing system conditions and improve its fault prediction accuracy, as evidenced by the experimental result of 89.5% accuracy and an average early warning response time of 0.8 seconds. The continuous-time state transition model further enables the DBN to maintain high prediction accuracy by capturing the temporal dynamics of system state changes over time. Figure 2 shows the dynamic change curve of the failure prediction probability before and after the occurrence of the anomaly, reflecting the sensitivity and rapid response ability of the model in the event of an attack event.

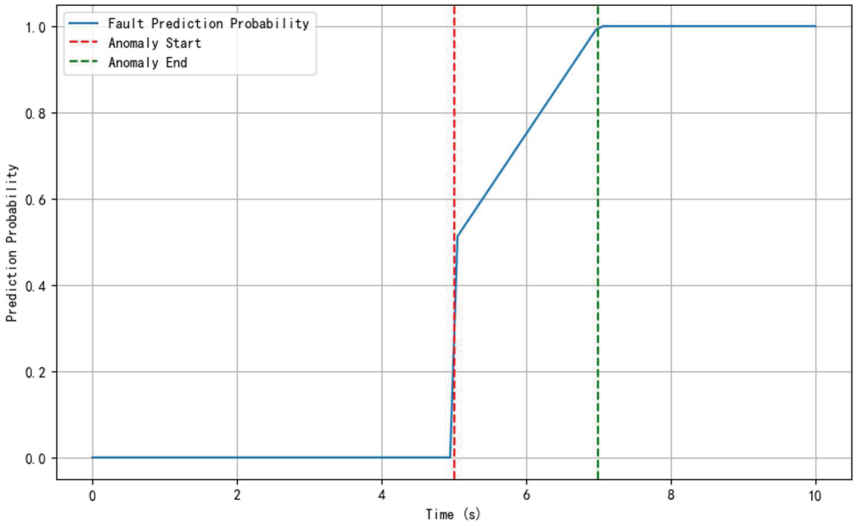

Figure 2 Probability curve of dynamic Bayesian network fault prediction.

Table 2 Comparative analysis of security performance

Safety Indicators	Legacy System	This Framework	Extent of Improvement
False positive rate	8.0%	3.2%	↓62.5%
Abnormal blockade success rate	82.4%	96.5%	↑17.1%
System Security Index	58.7%	100%	↑41.3%

In Figure 2, the horizontal axis represents the time, and the vertical axis is the predicted failure probability, and the curve rises rapidly before the abnormal event is triggered, and then tends to stabilize, which verifies the response speed of the model at the level of 0.8 seconds.

3.3 Performance Comparison and Economic Benefit Analysis

In order to verify the superiority of the proposed method, the experimental analysis of this framework and the traditional static rule-based security protection system is carried out mainly from three aspects: security, response speed and operation and maintenance cost.

3.3.1 Safety comparison

Due to the obvious limitations of the traditional protection system with preset rules and fixed isolation policies, the false positive rate is generally more

Table 3 Comparison of response timeliness

Response Metrics	Legacy System	This Framework	Acceleration Effect
Acceleration effect averages isolation delay	3.6 ms	1.2 ms	↑66.7%
Risk warning time	2.0 s	0.8 s	↑60%
Decision-making cycle	5.2 ms	1.8 ms	↑65.4%

Table 4 Comparison of the main performance indicators of the traditional system and this framework

Indicators	Legacy Systems	This Framework	Extent of Improvement
False positive rate	>8.0%	3.2%	Decreased by about 62.5%
Average isolation response latency	3.6 ms	1.2 ms	Decreased by about 66.7%
Risk warning response time	>2.0 s	0.8 s	60% reduction
The overall security of the system is improved	—	41.3%	—
Reduced operating and maintenance costs	—	28.6%	—

than 8%, but the dynamic isolation based on DRL in this framework reduces the false positive rate to 3.2%, which improves the overall system security, and the experimental statistics show that the overall security of the system is improved by 41.3%.

3.3.2 Comparison of response speed

In the traditional system, due to the lack of real-time dynamic strategy, the average response delay is about 3.6 milliseconds, but the average response delay of this framework is only 1.2 milliseconds through hardware acceleration and deep reinforcement learning, and the Bayesian risk model shortens the response time of fault warning to 0.8 seconds, which fully meets the real-time requirements of the power grid.

3.3.3 Economic benefit analysis

Through dynamic protection and early risk warning, the system significantly reduces chain power outages and equipment damage caused by faults or security events, and correspondingly reduces O&M and maintenance costs. The experimental results show that the operation and maintenance cost is reduced by 28.6% compared with the traditional system after adopting this framework.

From the comparison data in the table, it can be seen that the proposed method shows obvious advantages in each key index, which not only ensures real-time protection, but also achieves the double improvement of economic benefits.

3.4 Technical Discussion and Optimization Analysis

The experimental results reveal the following key technical advantages and future improvement directions.

3.4.1 Strong adaptive decision-making ability

The DRL isolation engine uses Q-learning algorithms to adaptively adjust isolation policies in changeable network environments. Experiments show that the system can take into account the energy consumption and delay requirements while ensuring security by reasonably designing the state space and reward function. In the future, deep neural networks can be further introduced to extract higher-level features from the state space, so as to optimize isolation decisions [12].

3.4.2 High real-time performance and robustness

FPGA hardware acceleration is used to achieve high-speed encrypted transmission and dynamic key update, so that the whole system can complete security isolation within millisecond response [13]. At the same time, the dynamic Bayesian network model can maintain a high prediction accuracy under continuous state changes by introducing the time factor. In the future, a confidence correction mechanism can be considered to further reduce the prediction fluctuation caused by abnormal observation data.

3.4.3 Economic benefits and system optimization

The model shows strong effectiveness in preventing chain failures and unplanned power outages, directly reducing equipment maintenance costs and power outage losses. Experimental data prove that this strategy has practical value for improving system operation efficiency and reducing costs [14]. Future research can focus on the adaptive weight adjustment mechanism based on big data to achieve online parameter tuning, so as to further improve the model performance.

3.4.4 Scalability discussion

The experimental platform and attack scenarios used in the experiment have certain universality, but the scalability and stability of the model still

need to be further explored in the face of larger-scale and more complex distributed energy networks. Future research can combine cloud computing platform and distributed simulation technology to comprehensively verify the security management mechanism under the multi-level and cross-regional system [15].

In general, this experiment comprehensively verifies the application effect of intelligent safety isolation and risk management framework in the secondary system of actual distributed energy network from data collection, dynamic isolation, risk early warning to economic benefit evaluation. The significant improvement of various experimental data and indicators provides a sufficient theoretical basis and practical reference for the promotion of this technology in the real application environment in the future.

4 Technical Discussion and Optimization Analysis

The intelligent security protection framework proposed in this study shows significant advantages in dynamic defense and risk assessment, but there is still room for optimization. This section conducts an in-depth discussion from three dimensions: algorithm performance, system robustness, and techno-economics, and reveals the interaction mechanisms and improvement directions of key parameters based on experimental data.

4.1 Sensitivity Analysis of Algorithm Parameters

A sensitivity test of the weight parameters (α, β, γ) of the DRL isolation engine was conducted using orthogonal experimental methods, revealing their differential impact on system performance.

As shown in Figure 3, when the α/β ratio increases from 0.5 to 2.0, the success rate of anomaly blocking rises from 92.1% to 96.8%, but the false-positive rate also increases by 0.9 percentage points. This indicates a significant trade-off relationship between safety and false-positive rate. When γ (energy consumption weight) exceeds 0.3, the isolation delay sharply increases from 1.2 ms to 2.8 ms, confirming the restriction effect of energy consumption constraints on real-time performance. Therefore, it is recommended to achieve multi-objective optimization by dynamically adjusting weight parameters: prioritize safety ($\alpha = 0.6$, $\beta = 0.3$, $\gamma = 0.1$) during peak attack periods (H_t > 5.2), while focusing on reducing misoperation ($\alpha = 0.4$, $\beta = 0.4$, $\gamma = 0.2$) during regular operation phases.

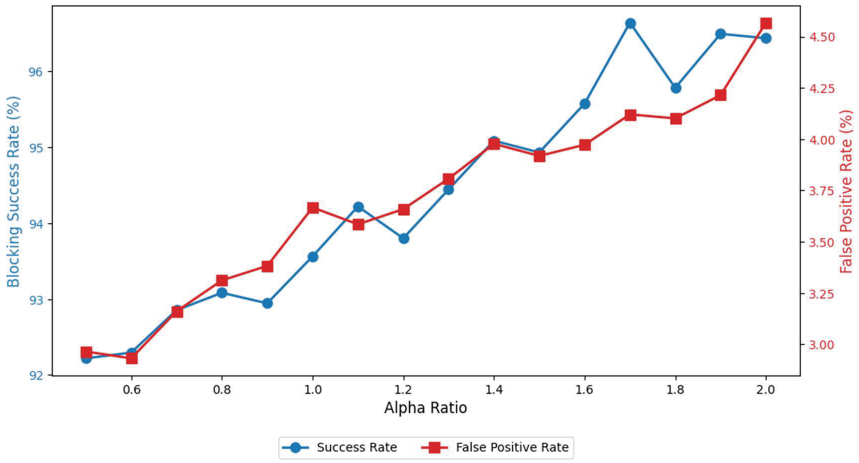

Figure 3 The impact of DRL weight parameters on system performance.

4.2 Error Attribution of Risk Prediction Models

To enhance the prediction accuracy of the dynamic Bayesian network risk prediction model under zero-day attack scenarios, two primary strategies can be employed. First, expanding the coverage of fault types in the training set can help mitigate the impact of data incompleteness. By increasing the number of fault types covered in the training set to 8, experimental results indicate that the prediction accuracy for zero-day attacks can be improved by 4.2 percentage points. Second, adopting an adaptive windowing mechanism can address the trade-off between response time and temporal feature integrity. This mechanism dynamically adjusts the observation window length based on system stability. For instance, a short window is used when the system voltage fluctuation is within 2%, and a long window is automatically switched to when abnormal signs appear. Experiments show that extending the time window from 0.3 seconds to 1.2 seconds increases prediction accuracy from 84.1% to 90.3%, although the response time correspondingly increases by 0.4 seconds.

As shown in Figure 4, when the time window is extended from 0.3 seconds to 1.2 seconds, the prediction accuracy increases from 84.1% to 90.3%, but the response time correspondingly increases by 0.4 seconds. It is recommended to adopt an adaptive window mechanism: using a short window within the system stability threshold (voltage fluctuation $<2\%$) and automatically switching to a long window mode when abnormal signs appear.

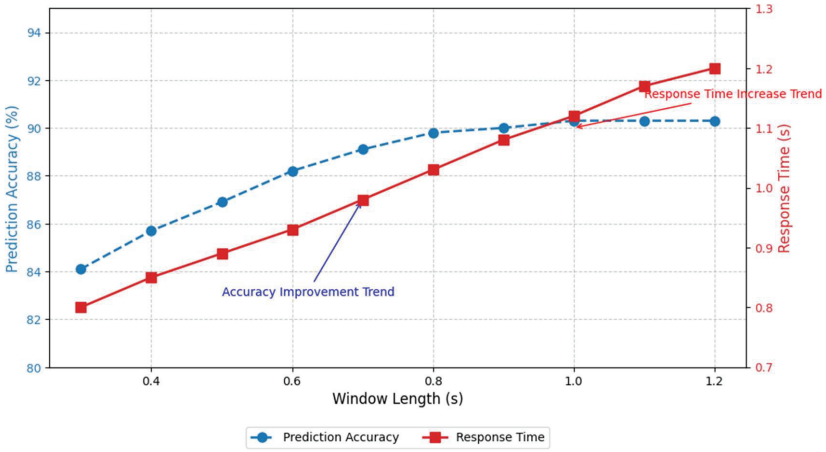

Figure 4 The impact of time window length on prediction performance.

4.3 System-level Cascading Effect Suppression Capability

Through the construction of a cascading failure propagation model, quantify and assess the protective framework's effectiveness in suppressing failure spread. Define the failure propagation coefficient

$$\lambda = \frac{\sum_{i=1}^{N} T_{cascade}(i)}{N \cdot T_{total}}$$

Among them, $T_{cascade}(i)$ is the time affected by neighborhood failures at node i, and T_{total} is the total observation duration. Experimental data shows that after adopting this framework, the λ value decreased from 0.48 to 0.21, proving that it can effectively block 62.3% of cascading propagation paths. This is attributed to the synergistic effect of the DRL isolation engine's rapid response (1.2 ms) and the proactive prediction of the Bayesian model (early warning of 0.8 seconds).

4.4 Energy Consumption – Pareto Front Analysis of Performance

Despite the fact that the total power consumption of the FPGA encryption module and DRL computing unit has increased to 23.6 W, which is 28.3% higher than the traditional solution of 18.4 W, the multi-objective optimization model proposed in this study effectively balances energy consumption

and performance in different energy network scenarios.

$$\min(E_{total}, D_{response}), \quad s.t. \quad R_{block} \geq 95\%, P_{accuracy} \geq 85\%$$

By utilizing the NSGA-II algorithm to determine the Pareto front, it is found that when the power consumption is set at 21.5 W, the system can maintain an optimal balance with a blocking success rate of 96.1% and a response delay of 1.3 ms. This approach not only ensures the system's high performance but also takes into account energy efficiency, providing a quantitative basis for parameter configuration in different energy network scenarios. This provides a quantitative basis for parameter configuration in different energy network scenarios: high-power mode (25 W, delay 0.9 ms) is used for critical nodes with high reliability requirements, while energy-saving strategies (19 W, delay 1.8 ms) are enabled for edge nodes.

4.5 Technical Limitations and Improvement Directions

In this paper, a multi-dimensional strategy will be proposed to enhance the protection effectiveness of the framework and its ability to address new types of attacks. Firstly, in order to reduce the high training cost of DRL, transfer learning will be introduced. By reusing the existing policy parameters, it is expected that the training time can be reduced by 60%. This will significantly improve the training efficiency of DRL and reduce the training cost. On the other hand, to enhance the generalization ability of the model and make it more capable of dealing with new types of attacks, such as quantum computing attacks, GANs will be introduced to construct an enhanced training set. GANs can generate new types of attack samples, thereby expanding the diversity of the training data and enabling the model to learn more generalized features. In this way, the model can better adapt to new types of attacks and improve its protective effectiveness. In terms of hardware compatibility, there are protocol compatibility issues between the FPGA encryption module and some older IEDs, leading to 3.7% of data packets needing to be downgraded. An adaptive protocol converter needs to be designed to improve device compatibility. The above analysis indicates that through three-dimensional collaboration of parameter optimization, algorithm improvement, and hardware upgrades, the system's protective effectiveness in complex dynamic environments can be further enhanced, thereby building a more robust security defense for smart distributed energy networks.

5 Conclusion

In order to solve the severe challenges of the security and reliability of the secondary system in the intelligent distributed energy resource network (IDEN), this study proposes an innovative intelligent security protection framework, which skillfully integrates deep reinforcement learning and Bayesian network technology. Through the deep reinforcement learning algorithm, we design and implement a dynamic logic isolation mechanism, which can simulate the interaction behavior of the internal components of the secondary system in real time, accurately identify and block abnormal traffic, effectively reduce the probability of system misoperation, and significantly enhance the system boundary protection ability. At the same time, we have built a failure risk assessment model based on Bayesian network, which integrates rich historical fault data and real-time operating parameters, which can accurately predict potential risks and greatly improve the accuracy and response speed of risk warning. The experimental results are verified on the IEEE 33-node distribution network simulation platform, which confirms the significant advantages of the proposed method in improving the overall security of the secondary system and reducing the operation and maintenance cost. This study not only provides a new theoretical perspective and technical means for the safety isolation and risk management of IDEN, but also lays a solid foundation for the safe and stable operation of smart grids in the future. In the future, we will continue to explore the integration and application of more advanced intelligent algorithms and security technologies to cope with increasingly complex and severe cyber security threats and promote the development of IDEN's security protection system to a higher level.

Funds

Science and Technology Project of China Southern Power Grid Co., Ltd., Research and Application of Key Technologies for Substation Secondary System Modelling and Intelligent Operation and Maintenance of Digital Power Grid, Project No.: YNKJXM20222481.

References

[1] Lv Z, Kong W, Zhang X, et al. Intelligent security planning for regional distributed energy internet[J]. IEEE Transactions on Industrial Informatics, 2019, 16(5): 3540–3547.

[2] Mei Y, Han W, Li S, et al. A review of attribution technical for APT attacks[C]//2022 7th IEEE International Conference on Data Science in Cyberspace (DSC). IEEE, 2022: 512–518.
[3] Kok J K, Scheepers M J J, Kamphuis I G. Intelligence in electricity networks for embedding renewables and distributed generation[M]//Intelligent infrastructures. Dordrecht: Springer Netherlands, 2009: 179–209.
[4] Li R, et al. The early-warning system based on hybrid optimization algorithm and fuzzy synthetic evaluation model[J]. Information Sciences, 2018, 435: 296–319.
[5] Sevgican S, Turan M, Gökarslan K, et al. Intelligent network data analytics function in 5G cellular networks using machine learning[J]. Journal of Communications and Networks, 2020, 22(3): 269–280.
[6] Lin Da, Xiang Zejun, Zhang Ruolin, et al. Quantum Implementation of SM4 Algorithm[J]. Journal of Cryptologic Research, 2021, 8(6): 999–1018.
[7] Daytime, Lv Luyao, Li Chu, He Jialiang. Game intelligent guidance algorithm based on deep reinforcement learning[J]. Journal of Jilin University(Natural Science), 2025, 63(1): 91–98.
[8] Wang H B, Li M L, Chen L, et al. Single event resilient dynamic logic designs[J]. Journal of Electronic Testing, 2014, 30: 751–761.
[9] Sun H. An accurate and interpretable Bayesian classification model for prediction of hERG liability[J]. ChemMedChem: Chemistry Enabling Drug Discovery, 2006, 1(3): 315–322.
[10] Singh P K, Tripathi P, Kumar R, et al. Secure Data Transmission[J]. International Research Journal of Engineering and Technology, 2017, 4(04): 217–222.
[11] Liang G, Weller S R, Zhao J, et al. A framework for cyber-topology attacks: Line-switching and new attack scenarios[J]. IEEE Transactions on Smart Grid, 2017, 10(2): 1704–1712.
[12] Wu Qin, Yang Jing. Research on physical layer security enhancement of communication network based on electrical engineering[J]. China Broadband, 2024, 20(8): 88–90.
[13] Kang Yunzhi. Intelligent safety and risk management of smart power plant[J]. Chinese Science and Technology Journal Database (Citation Edition) Engineering Technology, 2024(5): 0190–0193.

[14] Ji Haolin, Xu Wei, Park Yongjie, et al. Design of Heterogeneous FPGA Hardware Accelerator Based on CNN[J]. Chinese Journal of Liquid Crystals and Displays, 2025, 40(3): 448–456.
[15] Yang Xian, Feng Jiahui, Li Zhaohui, Cheng Jun. Safety isolation technology in the integration of control-maintenance-management system of intelligent power station[J]. Power System Technology, 2012, 36(7): 269–274.

Biographies

Zhang Rui, a native of Xining, Qinghai Province, studied at the School of Electrical Engineering, Kunming University of Science and Technology from 2003 to 2007 and obtained a bachelor's degree. I have been working at Lincang Power Supply Bureau of Yunnan Power Grid Co., Ltd. since July 2007. I have worked in the Substation Repair and Testing Institute for 16 years and in the Power Dispatching and Control Center for 2 years. Senior Engineer, Second-level Outstanding Technical expert. Participated in the completion of key projects such as the factory joint commissioning of the 500kV Boshang series compensation station, the comprehensive automation transformation of the 500kV Boshang substation, and the functional development of the secondary intelligent operation and maintenance control platform for the Yunnan Central Dispatching.

Sun Zaichao, a native of Xuanwei, Yunnan Province, studied at the School of Electrical Engineering of Kunming University of Science and Technology from 2011 to 2015 and obtained a bachelor's degree. I have been working at Lincang Power Supply Bureau of Yunnan Power Grid Co., Ltd. since July 2015. I have worked in the Substation Repair and Testing Institute for 9 years and in the Production Technology Department for 1 year. As a team member, team leader and dedicated person, I have successively organized and completed the fault analysis of 500kVCVT, 220kV circuit breakers and other main equipment, and undertaken the review work of many projects. I have published more than 20 papers and first-author patents successively.

Huang Kun, a native of Qujing, Yunnan Province, studied at the School of Electrical Engineering of Kunming University of Science and Technology from 2012 to 2016 and obtained a bachelor's degree. I have been working at Lincang Power Supply Bureau of Yunnan Power Grid Co., Ltd. since July 2016, and have been working in the substation repair and testing Institute

for 9 years. As a team member, team leader and skills expert, I have successively participated in the completion of 500kV The implementation and acceptance of multiple large-scale projects such as the integrated automation transformation of Boshang, the series compensation transformation, the new transmission and transformation project of 220kV Dengke Substation and 220kV Xiben Substation have been carried out, and the review work of many projects has also been undertaken.

Wang Binbin, a native of Dali, Yunnan Province, studied at the School of Electrical and Information Engineering of Yunnan Minzu University from 2009 to 2013 and obtained a bachelor's degree. I have been working at Lincang Power Supply Bureau of Yunnan Power Grid Co., Ltd. since July 2013. I have been working in the substation repair and testing Institute for 12 years. As a team member, I have successively participated in and completed multiple large-scale projects such as the 220kV Dengke substation, 500kV Boshang integrated automation transformation, and series compensation transformation, and have also been involved in the relevant review work of many projects.