Software and Hardware Decoupling of 10 kV Line Safety Protection Measurement and Control Device Based on Independent Chips

Jialin Bai[1,*], Shengguo Han[2], Jing Niu[1], Weixiang Qiao[1] and Wuzhi Zhao[1]

[1]*Guizhou Power Grid Co., Ltd. Electric Power Dispatching and Control Center, Guiyang, 550000, China*
[2]*Guiyang Power Supply Bureau of Guizhou Power Grid Co., Ltd, Guiyang, 550000, China*
E-mail: jialin-bai@outlook.com
[*]*Corresponding Author*

Received 01 July 2025; Accepted 23 July 2025

Abstract

The performance and security of 10 kV line protection and control devices are crucial given the quick expansion of the smart grid and industrial Internet of things. The traditional devices mostly use foreign chips, which have the risk of technology dependence and information security. Therefore, the research constructs a high-performance, autonomous and controllable 10 kV line protection and control device by means of independent chip selection and software and hardware decoupling method. The research utilizes the Longchip 3C6000/S chip, combined with key function modules, to build a hardware platform. The software adopts layered design to realize the separation of interface, service and application. YOLOv7 and software and hardware decoupling technology are utilized to enhance system performance and security. The experimental results indicated that the research method

Distributed Generation & Alternative Energy Journal, Vol. 40_5&6, 1049–1072.
doi: 10.13052/dgaej2156-3306.40566
© 2025 River Publishers

operated efficiently and stably on the test dataset. The initial loss value of YOLOv7 was in the range of 0.99-1.02, and approached 0 after 25–53 iterations. The training loss of YOLOv7 converged quickly, and the recognition accuracies reached 98.87% and 98.46%, respectively, with a peak hardware occupancy of 39%. The results show that the research-designed measurement and control device provides strong support for the stable operation and safe development of the power system. This method promotes the evolution of electric power secondary equipment towards autonomy, control, intelligence, and agility. It enhances the intelligence and information security capabilities of power systems.

Keywords: Measurement and control device, independent chip, secure encryption, YOLOv7, hardware and software decoupling.

Introduction

The degree of intelligence and informationization of the power system (PS) is continuously increasing against the backdrop of the deep integration of industrial Internet of things (IoT) and PS intelligence. The performance and dependability of 10 kV line protection and control devices (10 kV-LPCDs), a crucial link in power transmission, are closely tied to the PS's stable and safe operation [1, 2]. The traditional 10 kV-LPCD mostly adopts foreign chips. There are many problems such as technology constraints and information security risks. It is difficult to meet the development of smart grid and industrial IoT on the requirements of autonomous and controllable, safe and reliable equipment [3]. Most of the existing studies have not fully considered the software and hardware co-optimization, resulting in the device still has performance bottlenecks and safety hazards in practical applications. In the face of complex fault scenarios, there are still problems such as slow fault recognition speed and low accuracy. It is difficult to adapt to the requirements of smart grid for fast and accurate fault processing [4, 5]. Faults in PSs exhibit distinct, recognizable abnormal patterns in electrical waveform characteristics, such as amplitude abrupt changes, waveform distortion, and increased specific harmonic components. These patterns form unique "feature patterns" in time series data. By applying the principles of object detection in computer vision, it is possible to treat preprocessed electrical waveform data as target objects for identifying fault patterns. YOLOv7 is an efficient, single-stage object detection algorithm that excels at processing entire datasets and directly outputting the fault type, location, and confidence

level. This enables high-precision, rapid end-to-end fault detection. Therefore, the research combines the software and hardware decoupling with the quantitative target detection method you only look once version 7 (YOLOv7) through the methods of independent chip selection, hardware construction, software development, hardware and software adaptation, data processing, safety assurance, and test verification. A 10 kV-LPCD based on independent chip is constructed innovatively. It can not only realize efficient fault detection and protection functions, but also effectively resist various security threats and protect data privacy. This provides strong support for the stable operation and safe development of the PS, thus meeting the development needs of smart grid and industrial IoT.

1 Related Work

Line protection, measurement, and control devices monitor PS operation. They collect and analyze real-time parameters, such as current and voltage, to detect faults, isolate them, and protect equipment. This prevents blackout accidents and safeguards power equipment and lines. Munkhbaatar B et al. proposed a scheme to support the reliability of relay protection in this scenario for the reliability of relay protection of 110 kV high-load, short-distance transmission lines under the ring network structure. According to experimental data, the plan might successfully increase protection's accuracy and response time while lowering the possibility of erroneous and rejected acts. This provided an important technical reference for relay protection under similar grid structures [6]. Yasui S et al. proposed an effective lightning overvoltage protection scheme for outdoor low-voltage equipment facing lightning overvoltage issues. Experimental results showed that this scheme could significantly reduce the impact of lightning overvoltage on outdoor low-voltage equipment and improve the safety and reliability of the equipment in lightning environments [7]. Cao J et al. addressed the issue of lightning energy suppression for surge arresters used in 10 kV overhead distribution line transformers, employing a hybrid partial element equivalent circuit-multiconductor transmission line model for evaluation. Experimental results indicated that the fully shielded cable scheme provided the best protection, significantly suppressing the lightning energy absorption of the surge arresters. This provided important technical references and practical guidance for lightning protection of 10 kV overhead distribution line transformers [8]. Software and hardware decoupling involves abstracting hardware resources and encapsulating hardware functions and characteristics into interfaces that

can be invoked by software, enabling software development based on these interfaces. Kundu L et al. conducted a systematic analysis of the current status and future trends of hardware acceleration technology in response to the performance challenges faced by open wireless access networks. The study demonstrated that by utilizing dedicated hardware acceleration for physical layer processing and software and hardware decoupling methods, system energy efficiency and latency performance could be significantly improved. This approach exhibited a notable advantage over general-purpose processors in computationally intensive tasks within 5G networks [9].

YOLOv7 adopts a single-stage object detection approach, treating object detection as a regression problem. It performs a single inference on the input image to simultaneously predict the bounding box location and category information of the object. Samma H et al. achieved breakthrough progress in the early detection and diagnosis of lung cancer by combining the YOLOv7 object detection algorithm with transfer learning technology. According to the experimental findings, this technique greatly increased the precision and effectiveness of lung nodule detection. It provided an automated auxiliary tool for clinical lung cancer screening [10]. Jiang D et al. proposed a multi-scale automatic detection method for contact network support devices based on an improved YOLOv7 model. According to experimental data, the enhanced YOLOv7 model greatly enhanced detection performance, achieving a mAP of 81.3% on the test set [11]. Yang Y et al. proposed a technique based on simulated weather algorithms and an enhanced YOLOv7 model to overcome the difficulties of insulator defect identification under harsh weather conditions. Experimental results indicated that this method could effectively detect insulator defects under extreme weather conditions, providing a robust safeguard for the safe operation of PSs [12].

In summary, most existing studies have not fully achieved coordinated optimization of software and hardware. This has led to performance bottlenecks and safety hazards in the devices. When faced with complex faults, existing methods often exhibit slow identification speeds and insufficient accuracy. This fails to meet the smart grid's demand for rapid and precise fault handling. Therefore, this study focuses on a 10 kV-LPCD based on an independent chip. It employs a software and hardware decoupling method to construct an efficient and reliable protection and control system. By deeply exploring the hardware's performance potential and flexibly optimizing the software system, the study enhances the device's detection and protection capabilities in complex fault scenarios. This provides a solid foundation for the intelligent upgrading and safe, stable operation of PSs.

Table 1 Results of ablation experiment

Category	Parameter	Specification
Core	Configuration	16 Cores/32 Threads (Single-Die)
	Microarchitecture	LA664 (4th-Gen LoongArch ISA)
	Frequency	2.4–3.4 GHz (Dynamic Scaling)
Memory	Type	DDR4-3200
Input/Output	Channels	Quad-Channel
	PCIe Version	PCIe 4.0
	PCIe Lanes	$\times$64 Lanes
Interconnect	Technology	LoongLink 1.0
Security	Acceleration	GM/T SM4 (30 Gbps Bandwidth)
Power	TDP	135 W
Performance	SPEC CPU 2017 Gain	+60–95% vs. 3C5000

2 Methods and Materials

2.1 Construction of 10 kV-LPCD Based on Independent Chip

The deep application of industrial IoT in power grids has driven the deployment of massive sensing devices and edge nodes, enabling comprehensive monitoring of operational status and millisecond-level response times. In an environment where devices are interconnected and data is interoperable, the 10 kV line serves as a critical component of power transmission. The performance and reliability of its protection and control devices are decisive factors in maintaining the stable and safe operation of the PS. Traditional 10 kV-LPCDs primarily utilize foreign chips, which pose issues such as technological dependency and information security risks [13, 14]. The Loongson 3C6000/S processor, developed by Loongson Technology, is a domestically developed high-performance chip. This processor features a high-frequency main processor and exceptional floating-point computation capabilities. It addresses the shortcomings of traditional digital signal processing (DSP) systems, including insufficient computational power, poor scalability, high security risks, and reliance on imported chips [15]. In addition, the chip is equipped with large storage capacity and is compatible with multiple communication protocols, demonstrating excellent anti-interference performance. It is particularly suitable for critical applications such as power secondary equipment that require high security and reliability. Therefore, after comprehensively considering factors such as computing power, power consumption, and anti-interference capabilities, the Loongson 3C6000/S chip is selected to replace traditional DSPs. The relevant parameters of the Loongson 3C6000/S chip are shown in Table 1.

Table 1 shows that the Loongson 3C6000/S chip architecture fundamentally ensures the security of information technology systems and eliminates dependence on external authorization. Its built-in attack protection mechanisms effectively prevent security vulnerabilities such as "Spectre" and "Meltdown". It significantly enhances system security at the hardware level and reduces the risk of vulnerability attacks. Additionally, the chip integrates a secure and trustworthy module and a commercial encryption module, supporting national cryptographic algorithms. It enables hardware-level encryption and decryption functions, providing robust encryption protection for data transmission and storage. A 10 kV-LPCD is a protective device used in PSs with voltage levels of 10 kV or below. Its primary function is to protect power equipment and lines from faults caused by current imbalances. Three-stage current protection is the most commonly used phase-to-phase short-circuit protection scheme in power distribution lines at 10 kV and below. It consists of instantaneous current instantaneous protection, time-limited current instantaneous protection, and time-limited overcurrent protection [16, 17]. Instantaneous current instantaneous protection can quickly clear short-circuit faults near the line, as shown in Equation (1).

$$I_{op.I} = K_{rel} \times I_{k.max}^{(3)} \tag{1}$$

In Equation (1), $I_{op.I}$ represents the setting value of the first-stage action current. K_{rel} represents the reliability coefficient. $I_{k.max}^{(3)}$ represents the maximum three-phase short-circuit current at the end of the line. The time-limited instantaneous current protection can clear faults outside the first-stage protection range, as shown in Equation (2).

$$I_{op.II} = K_{rel} \times I_{op.I}^{next} \tag{2}$$

In Equation (2), $I_{op.II}$ represents the setting value of the second-stage operating current. $I_{op.I}^{next}$ represents the first-stage operating current value of the next-level circuit. The time-limited overcurrent protection serves as a backup protection, as shown in Equation (3).

$$I_{op.III} = \frac{K_{rel} \times K_{st}}{K_{re}} \times I_{L.max} \tag{3}$$

In Equation (3), $I_{op.III}$ is the setting value of the action current for Section III. $I_{L.max}$ is the maximum load current of the line. K_{st} is the self-starting coefficient. K_{re} represents the return coefficient. In the protective and control device under study and design, the Loongson multi-core architecture

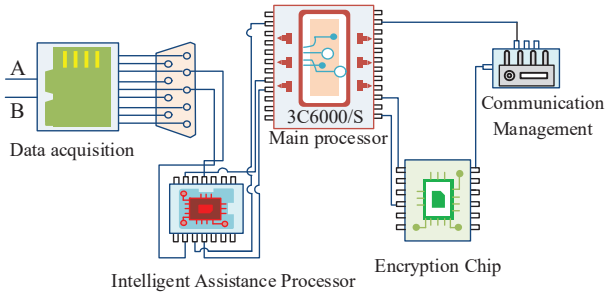

Figure 1 Hardware platform structure of 10 kV-LPCD.

can provide dedicated computing resources for each section of protection. It achieves a balance between selectivity and speed through the dual coordination of "current steps+time steps". The hardware platform structure of the 10 kV-LPCD is shown in Figure 1.

In Figure 1, the hardware platform of the 10 kV-LPCD designed for this study includes a main processor, data acquisition, security encryption, communication control, and intelligent management units. The main processor uses the Loongson 3C6000/S. Data acquisition utilizes the Xinshai Technology CSE7780. The encryption chip employs the Lingke Xian'an LKT4305GM. Communication control utilizes a fiber-optic gigabit network. The intelligent management assistant processor uses the Cambricon MLU220. Among them, the data acquisition module is connected through PCIe 4×64 bus. The security encryption module is mounted through SPI interface to realize SM2/SM3/SM4 algorithm acceleration. All modules are uniformly powered by dual redundant 12 V/5 V power supply. The software design of the 10 kV-LPCD based on an independent chip is shown in Figure 2.

In Figure 2, the software architecture of the measurement and control device constructed in this study is divided into three layers, covering the cross-platform interface layer, service layer, and application layer. Layered design means dividing modules into layers according to specific principles. Standardizing the interaction between modules within each layer and the communication method between layers can effectively reduce the complexity of interaction between modules.

2.2 Optimization of LPCDs Based on Software and Hardware Decoupling Methods

In industrial IoT, the high degree of integration between software and hardware in traditional embedded systems often leads to issues such as low

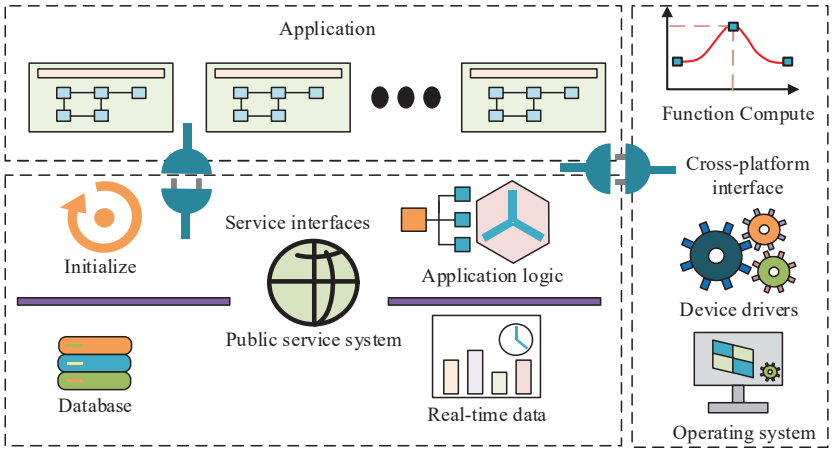

Figure 2 Software design of 10 kV-LPCD based on independent chip.

system development efficiency, difficulty in upgrading, and high platform migration costs. Among these, low hardware resource utilization makes it challenging to flexibly allocate and share resources. The mutual dependence between software and hardware complicates fault diagnosis and makes it difficult to quickly pinpoint issues. Software and hardware decoupling, by separating hardware and software, enables the deployment of more flexible security protection strategies. The hardware layer can focus on optimizing hardware resources such as security chips and encryption modules to improve data processing and encryption speeds. The software layer can dynamically update and upgrade security algorithms and protection mechanisms according to different security requirements without requiring significant hardware modifications. Therefore, this study focuses on optimizing the hardware architecture and software design of line protection and control devices (LPCDs) centered around an independent chip. In terms of hardware, functional units are modularly divided. In terms of software, a layered architecture is constructed to separate system software from application software. Middleware ensures cross-platform compatibility, enabling flexible allocation and expansion of software functions to adapt to the trend of grid intelligence. The operation mode of software and hardware decoupling is shown in Figure 3.

Figure 3 shows the process of creating and iterating a set of execution primitives based on the evaluation results of the design space. This continues until a set of execution primitives is obtained that meets application

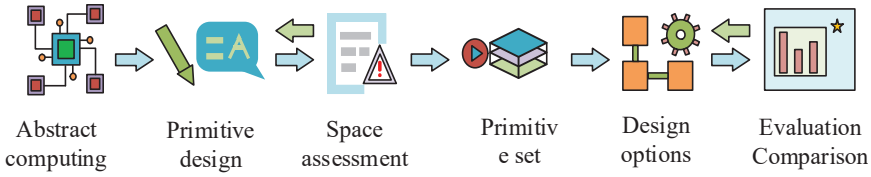

Figure 3 Software and hardware decoupling process.

requirements and conforms to neuromorphic completeness. Subsequently, multiple hardware design schemes are explored for this set of execution primitives. Iterative optimization is performed based on feedback from the hardware evaluation platform, and the optimal hardware design scheme is ultimately determined. For the core function of fault identification in line protection measurement and control devices, the key to enhancing performance lies in efficiently and accurately capturing abnormal patterns in electrical quantity data. The YOLOv7 algorithm, with its high precision, lightweight architecture, and flexible design, is particularly suitable for real-time fault pattern detection on embedded platforms. The hardware platform can efficiently execute model inference by deeply integrating YOLOv7 with a hardware-software decoupling architecture. The decoupling of the software layer enables flexible deployment, updates, and optimization of models. This dual approach collectively improves the recognition speed and accuracy of protection devices in complex fault scenarios. Therefore, this study deeply integrates the lightweight YOLOv7 with a software and hardware decoupling architecture to provide an integrated solution for line protection devices that offers high-precision detection and low-latency response. This can drive the evolution of power secondary equipment toward autonomous control and intelligent agility [18]. Figure 4 displays the YOLOv7 network structure.

In Figure 4, the backbone network of YOLOv7 consists of multiple convolutional layers and pooling layers. Each module can automatically extract rich feature information from the input image and capture the key features of various types of information [19]. Then, through the neck structure of the feature pyramid network (FPN)+path aggregation network (PAN), the feature maps extracted by the backbone network at different levels are fused. This enables the model to simultaneously focus on targets and details at different scales, better adapting to the software and hardware decoupling requirements of LPCDs. In this study, the Backbone adopts CBS (Conv+BN+SiLU) and ELAN module stack to extract the time-frequency domain features of the waveform. Neck adopts FPN+PAN structure to fuse multi-scale features.

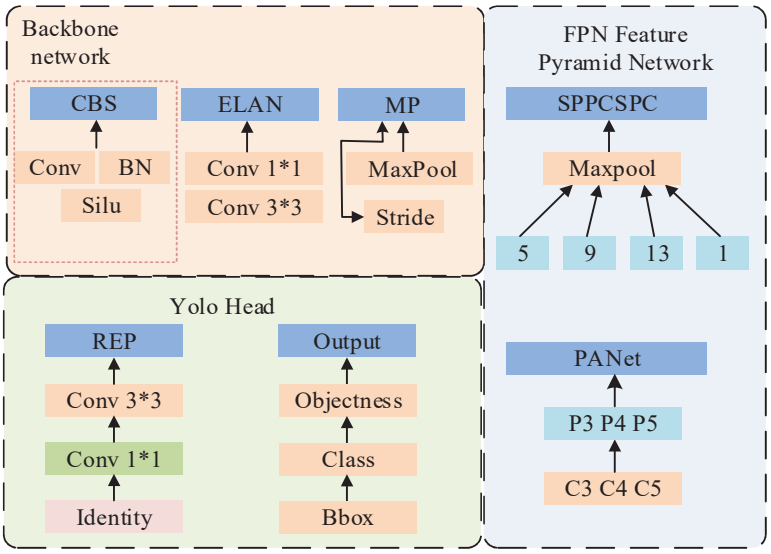

Figure 4 The network structure of YOLOv7.

Head corresponds to large, medium and small targets respectively, and outputs fault types and confidence levels. In the specific configuration parameters of the model, the input specifications are converted into 640×640 grayscale images through continuous wavelet transform of current/voltage waveforms. With a network zoom coefficient of 0.67 and a width factor of 0.50, the compressed model size is 12.5 MB. The anchor box configuration is optimized for fault characteristics using prior box sizes [(12,16), (19,36), (40,28)]. The loss function employs a loss weight of 0.6 and a classification weight of 0.3. By employing different scaling methods, the width and depth of the YOLOv7 model can be flexibly adjusted according to specific application needs, with different scaling coefficients set. The depth scaling is shown in Equation (4).

$$a = \begin{Bmatrix} \max(round(a^* depth), 1), & a > 1 \\ a, & other \end{Bmatrix} \tag{4}$$

In Equation (4), a represents the number of network blocks used for depth scaling. This process mainly involves adjusting the number of layers in the network, i.e., increasing or decreasing the number of convolutional layers, modules, etc. in the network. Width scaling is shown in Equation (5).

$$\mathrm{b} = \mathrm{make\_divisible}(\mathrm{b} * \mathrm{width}, 6) \tag{5}$$

In Equation (5), b represents the number of network channels, and width scaling is achieved by changing the number of channels in the convolutional layer of the network. To ensure the security and privacy of sensor devices, the study incorporates a security module into the protection and control device to encrypt the collected sensor data. The KT4305GM security chip adopted in the research follows the national secret standard and provides anti-physical tampering key storage function. The key destruction mechanism is automatically triggered when the shell is opened illegally. The study adopts a combination of symmetric and asymmetric encryption algorithms. This not only enhances the security of data encryption but also improves encryption efficiency [20]. Additionally, a public security service component for the protective measurement and control device is developed to implement data access control. Device data can only be accessed and used by authorized users thanks to user authentication and permission procedures. Furthermore, an access control list is established to manage user operation permissions in detail, effectively preventing data leakage and unauthorized operations. The encryption process of the security module is shown in Equation (6).

$$\begin{cases} C_1 = E_{K_s}(M) \\ C_2 = E_{K_{pu}}(K_s) \end{cases} \tag{6}$$

In Equation (6), C_1 represents the ciphertext obtained after symmetric encryption. C_2 is the ciphertext obtained by encrypting the symmetric encryption key using an asymmetric encryption method. The research adopts a three-tier system for the practical management of encryption modules. Specifically, the hardware layer generates and stores keys internally within the chip, ensuring that root keys are never disclosed externally. In the protocol layer, session keys are dynamically negotiated through the SM2-KEM mechanism. Meanwhile, the operation and maintenance layer implements certificate revocation via the power grid system. Symmetric encryption uses the SM4-CBC model with a 128-bit key. The initial vector is generated by the built-in hardware true random number generator of the LKT4305GM. Asymmetric encryption utilizes the SM2 elliptic curve algorithm, with a 256-bit private key encapsulating the session key. Integrity protection uses SM3 to generate 256-bit message digests for packet signature verification. The key management framework includes three components: key generation, key exchange, and certificate revocation. Specifically, the device's unique SM2 key pair is generated through the security chip in the factory. Key exchanges involve temporary SM4 session keys that are negotiated via the SM2 key encapsulation mechanism and rotate every five minutes or after

10,000 operations. Certificate revocation is managed by an OCSP client that periodically checks certificate status against the power grid PKI system. To achieve efficient resource utilization and intelligent management, reduce costs, and enhance efficiency and data processing capabilities, the study integrates edge computing and artificial intelligence (AI) technologies to optimize data processing workflows. Data preprocessing and feature extraction are performed at the edge, while deep analysis and model training are executed in the cloud. Through a feedback mechanism, the AI model at the edge is continuously optimized. The 10 kV-LPCD, which is designed through research, achieves software and hardware decoupling optimization. This is done through a standardized hardware platform, an open software ecosystem, and self-controlled security capabilities. These features improve operational efficiency and security. The device is based on the Loongson 3C6000/S chip.

3 Results

3.1 Performance Testing of 10 kV-LPCD Based on Independent Chip

To test the performance of the software and hardware decoupling of the LPCD designed in this study, the Ubuntu 20.04 operating system and PyTorch deep learning library are selected. Development is carried out on an advanced computing platform equipped with an NVIDIA RTX 3090 GPU and an Intel Core i9-12900K CPU. The test dataset uses the IEEE PS Fault Dataset (https://ieeexplore.ieee.org/Xplore/home.jsp) and the CIC-IDS Intrusion Detection Dataset (https://www.unb.ca/cic/datasets/ids-2017.html). The study compares the designed lightweight algorithm YOLOv7 with long short-term memory (LSTM) and artificial neural network (ANN). The training loss curve on the dataset is shown in Figure 5.

As shown in Figure 5(a), when trained on the IEEE dataset, the initial loss value of YOLOv7 is only 1.02. After 25 iterations, the loss value drops to near zero and remains relatively stable. The initial loss value for ANN is 1.21. By the 170th iteration, the loss value has decrease to near zero and remains relatively stable. The initial loss value for LSTM is 1.23. By the 220th iteration, the loss value has decrease to near zero and remains relatively stable. In Figure 5(b), when trained on the CIC-IDS dataset, the initial loss value of YOLOv7 is only 0.99. After 53 iterations, the loss value drops to near 0 and remains relatively stable. The initial loss value of ANN is 1.07. After 122 iterations, the loss value drops to near 0 and remains relatively stable.

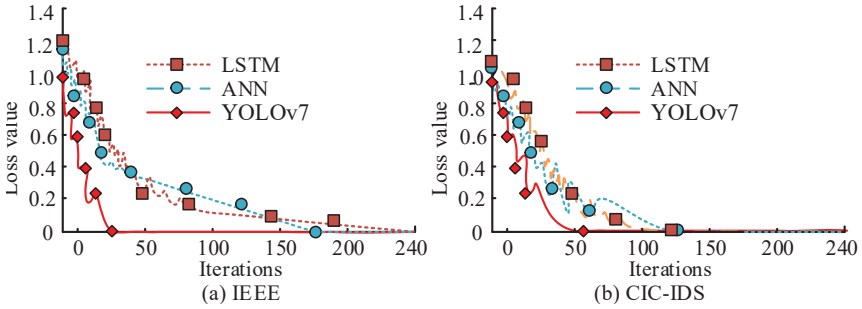

Figure 5 Method training loss testing.

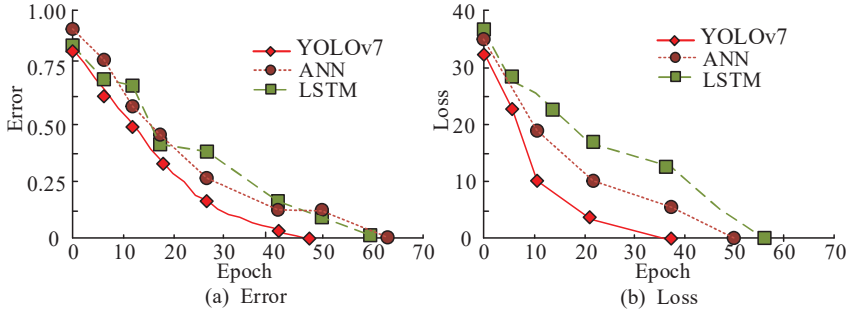

Figure 6 Convergence performance of different methods.

The initial loss value of LSTM is 1.23. When the number of iterations reaches 125, the loss value drops to near 0 and remains relatively stable. This suggests that the study method's YOLOv7 algorithm has a more stable training process and a faster training efficiency. Figure 6 illustrates how the study compares the convergence performance of various approaches.

In Figure 6, the overall convergence trends of different methods during training are consistent. In Figure 6(a), during the error convergence process, the error value of YOLOv7 decreases rapidly and approaches 0 by the 47th iteration. ANN also shows a gradual decrease in error convergence, approaching 0 by the 64th iteration. LSTM approaches 0 by the 61st iteration during error convergence. In Figure 6(b), during the loss convergence process, YOLOv7's error value at the start of iteration is 32, lower than that of ANN and LSTM. YOLOv7's loss value decreases rapidly in the early stages and then slows down gradually until training is complete. Compared to ANN and LSTM, YOLOv7 demonstrates significantly better convergence performance and higher training efficiency. To verify the performance of the encryption

Table 2 Encryption module performance test

Type of Attack	Test Method	Resist the Results
Replay attack	Inject historical encrypted packets 10,000 times	Time validation interception rate is 100%
Side channel attack	Monitor the power consumption of the chip for 48 hours	No valid key information is extracted
Firmware tampering	Embed malicious code into the application layer	SM3 signature check is blocked at startup

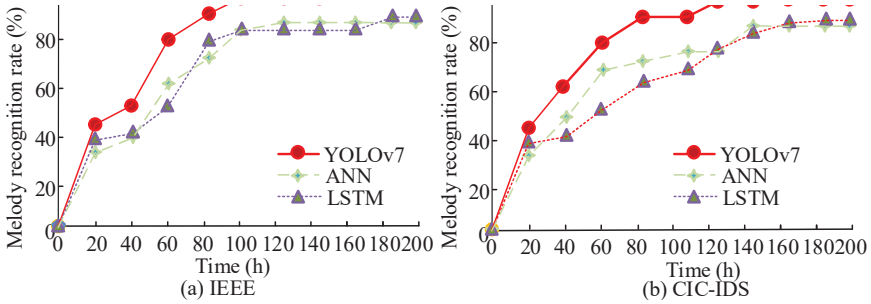

Figure 7 Accuracy of fault identification by different methods.

module, the research conducts physical attack tests and data tampering attack tests on the encryption module, as shown in Table 2.

As shown in Table 2, the device demonstrates robust resistance to replay attacks, side-channel attacks, and firmware tampering during security testing. Specifically, it achieved a 100% interception rate for time-verification against replay attacks. It successfully intercepted no valid key information during side-channel attacks and effectively blocked SM3 signature verification during startup firmware tampering attempts. These results confirm that the encryption module provides excellent cryptographic performance and meets the real-time protection requirements of 10 kV power line systems.

3.2 Practical Application of Independent Chip LPCDs

The study uses Simulink PS simulation software to establish a digital model of the distribution network. Power sources of different capacities are connected to the system, and different types of short-circuit faults are simulated to observe the operation of the measurement and control devices. The study compares the fault identification accuracy of different methods, as shown in Figure 7.

In Figure 7(a), the recognition accuracy of YOLOv7 gradually increases with the number of iterations. It reaches a maximum recognition accuracy of 98.87% after the 100th iteration and stabilizes. The recognition accuracy of ANN also shows a gradual upward trend with the number of iterations. It reaches a maximum recognition accuracy of 90.03% after the 180th iteration and stabilizes. LSTM achieves the highest recognition accuracy of 91.02% after 180 iterations. In Figure 7(b), the recognition accuracy of YOLOv7 gradually increases with the number of iterations, reaching a maximum of 98.46% at the 120th iteration and then stabilizing. The recognition accuracy of ANN also shows a gradual upward trend with the number of iterations, reaching a maximum of 84.32% at the 160th iteration and then stabilizing. LSTM achieves the highest recognition accuracy of 86.47% after 180 iterations. In summary, the method designed in this study performs best in practical applications and demonstrates high feasibility and effectiveness. The study analyzes the hardware resource consumption of different methods during computation, as shown in Figure 8.

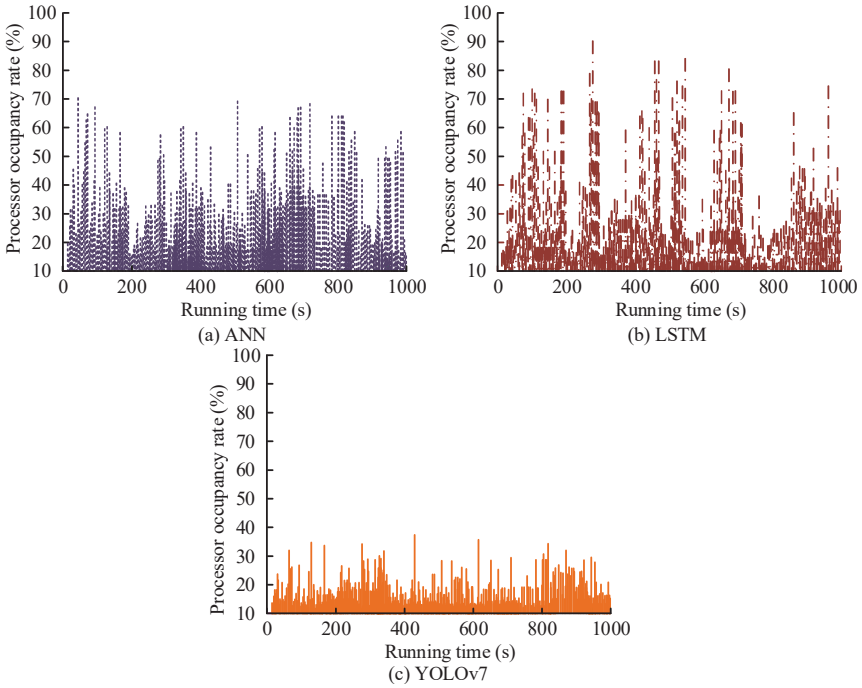

Figure 8 Hardware occupancy analysis during computation.

In Figure 8, different methods exhibit varying processor utilization rates during runtime. In Figure 8(a), the ANN achieves a maximum processor utilization rate of 71.2% over a runtime of 1000 seconds. During this period, processor utilization exceeds 50% for 5.1% of the runtime, and exceeds 30% for approximately 30% of the computations. In Figure 5(b), the LSTM achieves a maximum CPU utilization of 89% over a runtime of 1000 seconds. During this period, approximately 5% of computations reach CPU utilization of 70% or higher, and over 30% of computations reach CPU utilization of 40%. In Figure 5(c), YOLOv7 achieved a maximum CPU utilization of 39% over a runtime of 1000 seconds. During this period, the CPU utilization rate exceeds 25% for 5% of the time, and exceeds 20% for 10% of the time. This indicates that the computational load is lower when performing disturbance identification using the proposed method, resulting in reduced hardware overhead. The clustering performance of the voltage data collected by the measurement and control device is shown in Figure 9.

Figure 9(a), (b), and (c) shows the dimension reduction effect of ANN, LSTM, and YOLOv7. YOLOv7 has a good dimension reduction effect and

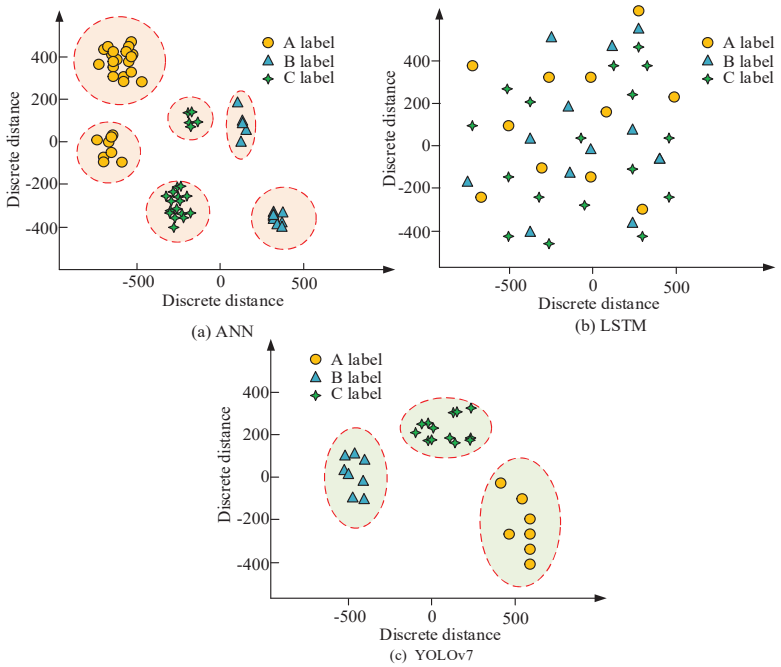

Figure 9 Clustering effect of voltage data recognition.

Table 3 Results of ablation experiment

Performance Metric	The Device Described Herein	Siemens 7SJ686 Device
Fault identification accuracy	98.2%	97.8%
Average response delay	12.3 ms	14.7 ms
GOOSE message encryption delay	1.8 ms	2.4 ms*
CPU peak occupancy	43%	41%

can retain the feature differences between phases. While the voltage data points of various phases are clearly separated, those of the same phase are obviously crowded. To evaluate the practicality of the device engineering, this study selects a 10 kV outgoing line station at an 110 kV substation in Guizhou Power Grid as the research base. The proposed design methodology is compared with existing Siemens 7SJ686 devices. The comparison device is installed in the protection compartment of a 10 kV feeder cabinet. It monitors the following parameters: phase currents (L1, L2, and L3), zero-sequence current, bus voltage, fault type, and simulated single-phase ground faults and phase-to-phase short circuits. Key test results are presented in Table 3.

As shown in Table 3, the proposed device demonstrates slight advantages over the 7SJ686 device in both fault diagnosis accuracy and average response time. With an accuracy rate of 98.2%, it outperforms the 7SJ686 device's rate of 97.8%. Additionally, the average response time is reduced to 12.3 ms, which is faster than the 7SJ686 device's time of 14.7 ms. In the latency performance evaluation of GOOSE message encryption, the proposed device shows a delay of 1.8 ms, lower than the 7SJ686 device's 2.4 ms. However, in terms of CPU peak utilization, the proposed device achieves 43% usage, slightly higher than the 7SJ686 device's 41%. A comprehensive analysis indicates that, while the proposed device has certain advantages in terms of fault diagnosis and response speed, it lags slightly behind the 7SJ686 device in CPU efficiency.

4 Conclusion

The accelerated advancement of intelligent PSs and the deep integration of the Industrial IoT technology directly affect the performance of 10 kV-LPCDs. These devices are key components of power transmission systems and directly affect the safe and stable operation of power networks. However, traditional devices mostly rely on foreign chips, which pose technical limitations and information security risks. Therefore, the study used the

Loongson 3C6000/S chip to build a platform that includes hardware units such as the main processor, data acquisition, and security encryption. It also designed a software architecture with cross-platform interface layers, service layers, and application layers. Through software and hardware decoupling optimization, it achieved hardware modularization and software dynamic upgrades. Experimental results indicated that YOLOv7 had an initial loss of 1.02 on the IEEE dataset, which decreased to near 0 after 25 iterations. On the CIC-IDS dataset, the initial loss was 0.99, which decreased to near 0 after 53 iterations. The error value approached 0 at the 47th iteration, and the loss value decreased rapidly at first and then slowly. In practical applications, the fault detection accuracy of YOLOv7 ranged between 98.46% and 98.87%. The processor utilization rate was as high as 39%, which was a relatively light computational load. In terms of voltage data identification clustering, YOLOv7 could effectively retain the differences between phase features, achieving clear data point separation and good dimension reduction effects. This study achieved hardware-software decoupling for a 10 kV line protection, measurement, and control device based on domestic chips. However, challenges remain, including increased GOOSE latency due to encryption during large-scale node concurrency, the 25%-30% higher cost of Loongson chips compared to commercial ARM chips, and insufficient interoperability with existing IEC 61850-90-5 systems, as well as inadequate adaptability to extreme environments. The three-year roadmap will be implemented in phases: From 2025-2026, conduct HIL validation using Real-Time Data Services (RTDS) across 50 nodes and scale to platforms like Phytium D2000 and Zhaoxin KX-7000. From 2026-2027, more than 20 field devices are planned to be deployed in secondary substations of Guizhou Power Grid. This integrates hybrid encryption of quantum-inspired Kyber and China's SM9 cryptographic standard to reduce key negotiation latency by 40%. Starting in 2028, it is planned to build a one-thousand node system using ASIC-accelerated YOLOv9 to achieve 50% inference acceleration with 5W power consumption. Ultimately, this will establish a replicable, self-reliant standardization solution for smart grid protection, enhance device performance in complex environments, explore potential applications of autonomous chips, and further advance the intelligent, secure development of PSs.

Funding

This research is supported by the technology project: Key Technologies and Flexible Equipment Research for Efficient Operation of Secondary

Equipment (Protection, Integrated Automation) Project 3: Development and Application of a New Generation of Domestic Safety Controllable Protection Measurement and Control Device 0665002023030103JB00001 from Guizhou Power Grid Co., Ltd.

References

[1] Li H, Hao T, Li Z, Zhao E, Wang C, Xu L. Research on a self-coordinated optimization method for distributed energy resources targeting risk mitigation. Distributed Generation and Alternative Energy Journal, 2024, 39(3): 659–690. DOI 10.13052/dgaej2156-3306.39312.

[2] Hiremath R, Moger T. Improving the DC-link voltage of DFIG driven wind system using modified sliding mode control. Distributed Generation and Alternative Energy Journal, 2023, 38(3): 715–742. DOI 10.13052/dgaej2156-3306.3831.

[3] Wang Z, Jiao Z, Liu L. Design and research of power information acquisition system for smart grid. Distributed Generation and Alternative Energy Journal, 2022, 37(2): 185–198. DOI 10.1109/ICISCE.2016.73.

[4] Xia X, Xiao Y, Liang W, Cui J. Detection methods in smart meters for electricity thefts: A survey. Proceedings of the IEEE, 2022, 110(2): 273–319. DOI 10.1109/JPROC.2021.3139754.

[5] Ullah M H, Eskandarpour R, Zheng H, et al. Quantum computing for smart grid applications. IET Generation, Transmission & Distribution, 2022, 16(21): 4239–4257. DOI 10.1049/gtd2.12602.

[6] Munkhbaatar B, Bayasgalan Z, Namsrai I, Ulzii N. Reliability Supporting of Relay Protection for 110 kV Transmission Line with High-load and Short-distance in a Ring Network. Embedded Selforganising Systems, 2023, 10(6): 4–11. DOI 10.14464/ess.v10i6.654.

[7] Yasui S, Kano T, Triruttanapiruk N, Tsuchida T. Lightning surge overvoltage protection for low-voltage equipment placed outdoors in TT system. IEEE Transactions on Electromagnetic Compatibility, 2023, 65(3): 831–838. DOI 10.1109/TEMC.2023.3251311.

[8] Cao J, Du Y, Ding Y, Qi R, Li B, Chen M, Li Z. Practical schemes on lightning energy suppression in arresters for transformers on 10 kV overhead distribution lines. IEEE Transactions on Power Delivery, 2022, 37(5): 4272–4281. DOI 10.1109/TPWRD.2022.3148280.

[9] Kundu L, Lin X, Agostini E, Ditya V, Martin T. Hardware acceleration for open radio access networks: A contemporary overview. IEEE

Communications Magazine, 2023, 62(9): 160–167. DOI 10.1109/MCOM.023.2300281.

[10] Samma H, Al-Azani S, Luqman H, Alfarraj M. Contrastive-based YOLOv7 for personal protective equipment detection. Neural Computing and Applications, 2024, 36(5): 2445–2457. DOI 10.1007/s00521-023-09212-6.

[11] Jiang D, Liu K, Jia L, Qin Y, Jiang Y, Wang Z. Automatic Detection Strategy of Multi-Scale Catenary Support Device Based on Improved YOLOv7. IFAC-PapersOnLine, 2023, 56(2): 7597–7602. DOI 10.1016/j.ifacol.2023.10.1741.

[12] Yang Y, Yang S, Li C, Wang Y, Pi X, Lu Y, Wu R. Insulator defect detection under extreme weather based on synthetic weather algorithm and improved YOLOv7. High Voltage, 2025, 10(1): 69–77. DOI 10.1049/hve2.12513.

[13] Jin-ze Han, Xi Gao, Rong-Pei Zhang, Xin Z. Hen, Peng-fei M A, Peng-yuan Jia. N G, Xiao-dong H U A. Development of Interphase Spacer based on Live Installation of 10 kV Line. Mechanical Research & Application, 2023, 36(4): 115–117. DOI 10.16576/j.ISSN.1007-4414.2023.04.033.

[14] Yang L, Chen Z, Hao Y, Lin X, Yu L, Li Y, ... et al. Experimental study on ice monitoring method for 10 kV transmission line with tangent tower in alpine landform. High Voltage, 2024, 9(1): 182–194. DOI 10.1049/hve2.12372.

[15] Zhong Y, Tang J, Li X, Liang X, Liu Z, Li Y, ... et al. A memristor-based analogue reservoir computing system for real-time and power-efficient signal processing. Nature Electronics, 2022, 5(10): 672–681. DOI 10.1038/s41928-022-00838-3.

[16] Zheng L, Han X, Xu C, Kandula R P, Graber L, Saeedifard M, Divan D. 7.2 kV three-port SiC single-stage current-source solid-state transformer with 90 kV lightning protection. IEEE Transactions on Power Electronics, 2022, 37(10): 12080–12094. DOI 10.1109/TPEL.2022.3172946.

[17] Zhao R, Su B, Yu Z, Wang K L, Lu J G. A hybrid protection scheme for active distribution networks based on fault components principle. Journal of Electrical Engineering & Technology, 2025, 20(1): 141–155. DOI 10.1007/s42835-024-02015-2.

[18] Nergiz M. Enhancing strawberry harvesting efficiency through Yolo-v7 object detection assessment. Turkish Journal of Science and Technology, 2023, 18(2): 519–533. DOI 10.17714/tjst.2023.18.2.13.

[19] He J, Wang Y, Wang Y, Li R, Zhang D, Zheng Z. A lightweight road crack detection algorithm based on improved YOLOv7 model. Signal, Image and Video Processing, 2024, 18(Suppl 1): 847–860. DOI 10.1007/s11760-024-03197-y.

[20] Zhang Z, Tang J, Ni H, Huang T. Image adaptive encryption algorithm using a novel 2D chaotic system. Nonlinear Dynamics, 2023, 111(11): 10629–10652. DOI 10.1007/s11071-023-08397-8.

Biographies

Jialin Bai (March 1994–), male, graduated from Shanghai Jiao Tong University with a master's degree in Power System and Automation. After graduation, I worked as a senior engineer at the Power Dispatch Control Center of Guizhou Power Grid Co., Ltd. My current research direction is engaged in the study of power systems.

Shengguo Han (December 1978–), male, graduated from North China Electric Power University with a master's degree in Power System Automation. After graduation, I worked as a senior engineer at Guizhou Power Grid Co., Ltd. Guiyang Power Supply Bureau. My current research direction is engaged in the study of power system relay protection and stable operation.

Jing Niu (October 1984–), female, graduated from Guizhou University with a master's degree in Electrical Engineering. After graduation, I worked as a senior engineer at the Power Dispatch Control Center of Guizhou Power Grid Co., Ltd. My current research direction is mainly engaged in the study of power system relay protection.

Weixiang Qiao (January 1993–), male, graduated from Guizhou University with a Bachelor's degree in Electrical Engineering and Automation. After graduation, I worked as an engineer at the Power Dispatch Control Center of Guizhou Power Grid Co., Ltd. My current research direction is in the field of relay protection.

Wuzhi Zhao (September 1974–), male, graduated from Wuhan University with a master's degree in Electrical Engineering and Automation. After graduation, I worked as a senior engineer at the Power Dispatch Control Center of Guizhou Power Grid Co., Ltd. My current research direction is engaged in the study of power systems.