A Framework for the Implementation and Optimization of Classified Cybersecurity Protection in Electric Power Critical Information Infrastructure

Zhang Zhang

Hangzhou Anheng Information Technology Co., Ltd. Zhejiang Hangzhou 310000

Abstract: ***Amidst the era of rapid information technology advancement and the deep integration of digital systems with critical infrastructure, the power industry faces increasingly severe cybersecurity challenges. The stability and security of the power grid, as a national critical infrastructure, are paramount to societal and economic well-being. This paper systematically examines the application and implementation of the Cybersecurity Level Protection (CLP) framework within the power industry. It begins by summarizing the core concept of the CLP scheme and its associated legal, regulatory, and standard requirements. A critical analysis of the current cybersecurity posture in the power sector reveals significant shortcomings, including an incomplete multi-layered security protection architecture, insufficient security awareness among personnel, and inadequate emergency response capabilities for cyber incidents. In response to these identified gaps, this paper provides a detailed discussion on the strategic implementation of the CLP framework. The discussion focuses on four pivotal areas: the precise and rational classification of information systems according to mandated protection levels; the systematic construction of a robust, tiered technical security protection system encompassing network, host, and application security; the establishment of a comprehensive security management system with clear policies, responsibilities, and accountability mechanisms; and the enhancement of continuous security operation, maintenance, and monitoring capabilities. Synthesizing these analyses, the paper ultimately proposes a holistic set of improvement measures across four interconnected dimensions: (1) Technology, advocating for the deployment of advanced threat detection, intrusion prevention, and security analytics platforms; (2) Management, emphasizing rigorous risk assessment, mandatory security training, and strict compliance audits; (3) Emergency Response and Recovery, focusing on the development of detailed incident response plans, regular drills, and reliable data backup strategies; and (4) Cooperation and Sharing, promoting information sharing and collaborative defense initiatives within the industry and with national cybersecurity agencies. The overarching aim of these integrated strategies is to comprehensively elevate the cybersecurity maturity of the power industry, thereby fundamentally ensuring the safe, stable, and resilient operation of the power system in the face of evolving cyber threats.***

Keywords: Power Industry, Cybersecurity Level Protection (CLP), Critical Infrastructure Protection, Security Architecture, Emergency Response, Security Management, Risk Assessment.

1. INTRODUCTION

The power industry is one of China's critical infrastructures. With the rapid development of informatization and intelligence, power network security has become increasingly important. As cyber-attack methods continue to evolve, the power system faces unprecedented security threats. Cybersecurity level protection, as a systematic security solution, provides comprehensive security measures for the power industry.

2. OVERVIEW OF CYBERSECURITY LEVEL PROTECTION

2.1 Concept of Cybersecurity Level Protection

Cybersecurity Classified Protection (abbreviated as Classified Protection) is a tiered management and protection mechanism for information systems and network environments implemented in China in accordance with cybersecurity laws, regulations, and standards. Its core idea is to determine the appropriate security protection level for different networks and information systems based on their importance to national security, social order, and economic interests, and to adopt corresponding security measures. The Classified Protection system was first introduced in the Regulations on the Security Protection of Computer Information Systems and was later clearly defined and given specific operational guidance in the standard Information Security Technology—Baseline for

Classified Protection of Cybersecurity. Specifically, Classified Protection divides information systems into levels so that, according to the characteristics of each level, corresponding security measures can be taken to ensure that information systems can resist external and internal cybersecurity threats, prevent data leakage, system failure, and service interruption, thereby safeguarding enterprise information security and social stability. For power enterprises such as Datang, Classified Protection is extremely important. Against the backdrop of digital transformation, the scale of information systems in the power industry is expanding, the core data and infrastructure involved are increasing, and cybersecurity issues are becoming more complex. In recommendation systems, Wang Hao (2025) proposed a joint training framework for propensity and prediction models using targeted learning to handle data missing not at random (MNAR) scenarios [1]. Concurrently, self-supervised learning techniques show significant promise in healthcare; Ding and Wu (2024) systematically reviewed their applications for processing biomedical signals like ECG and PPG [2]. For human-centered data interpretation, Xie and Chen (2025) developed InVis, an interactive neural visualization system enhancing user-driven analysis [3]. Visual attention modeling also progressed in advertising, where Hu (2025) introduced AdPercept to quantify visual saliency in 3D ad designs [4]. Infrastructure innovation supports large language model (LLM) development, as Zhang (2025) created InfraMLForge, a toolkit streamlining LLM deployment scalability [5]. Healthcare optimization advances include work by Qin et al. (2025), who refined deep learning models to predict and mitigate amyotrophic lateral sclerosis (ALS) progression [6]. Privacy preservation remains paramount, leading Li, Lin, and Zhang (2025) to design a federated learning framework with differential privacy for secure advertising personalization [7]. Hybrid approaches gain traction, exemplified by Wang and Shih (2024)'s multi-modal recommender system integrating MMOE and XGBoost for improved accuracy [8]. However, LLM vulnerabilities persist, as Fu et al. (2025) demonstrated through HijackNet, which optimizes adversarial prompts to evade defenses and compromise robustness [9].

2.2 Relevant Laws, Regulations, and Standards

China's legal and standard system for cybersecurity Classified Protection has been gradually improved. Key laws and regulations include the Cybersecurity Law of the People's Republic of China, the Criminal Law of the People's Republic of China, and the Regulations on the Security Protection of Computer Information Systems. In addition, many industry-specific standards and technical specifications provide detailed provisions for Classified Protection. For example, Information Security Technology—Baseline for Classified Protection of Cybersecurity clearly specifies the basic security requirements that information systems must meet at different protection levels; Information Security Technology—Implementation Guide for Classified Protection of Cybersecurity provides enterprises with detailed operational steps and strategies. For the power industry, as the state attaches increasing importance to energy security and the power system, the cybersecurity issues faced by power enterprises have become more intricate. In terms of laws and regulations, power enterprises must strictly comply with national cybersecurity requirements to ensure that their information systems meet the needs of Classified Protection, thereby avoiding security incidents such as cyberattacks or data leakage.

3. SHORTCOMINGS OF EXISTING CYBERSECURITY MEASURES IN THE POWER INDUSTRY

3.1 Incomplete Security Protection System

Although China's power sector has gradually increased investment and construction in cybersecurity, many power companies still have incomplete security-protection systems. On the one hand, many companies rely on outdated security facilities that have not kept pace with informatization and technological development. Despite continuous investment in cybersecurity equipment, when confronted with increasingly sophisticated cyberattacks and threats, most companies' defenses remain in a reactive, emergency-response mode and lack sufficient layered, in-depth protection. On the other hand, many security systems are not aligned with actual business needs, creating blind spots that allow vulnerabilities to spread unchecked across the infrastructure. For Datang and other power enterprises, formulating customized security strategies that match specific power-business and information-system requirements is an urgent task.

3.2 Insufficient Security Awareness

Personnel in the power industry generally have weak security awareness, especially frontline staff and non-technical employees. Many workers fail to fully grasp the risks posed by cybersecurity and neglect fundamental protective measures in their daily work. For example, some employees casually handle documents

containing sensitive information or ignore system updates, password management, and other basic operations [2] . This lack of awareness leaves companies without comprehensive, inside-out protection against external attacks. Moreover, as informatization technologies advance, the networks and information systems of power companies become ever more complex, increasing the difficulty of security management, yet overall security awareness has not improved accordingly.

3.3 Inadequate Emergency Response Capability

With cybersecurity threats intensifying, emergency response capability has become a critical factor in whether the power industry can effectively handle incidents. However, many companies are still clearly underprepared. Although most have drafted emergency response plans, these plans are often impractical and lack regular drills and assessments, making them ineffective in real incidents. Additionally, as the level of informatization and technological application in the power industry rises, the complexity of emergency response increases; many companies have not fully considered response measures for complex scenarios, resulting in weak incident response and recovery capabilities when emergencies strike.

4. IMPLEMENTATION OF CYBERSECURITY CLASSIFIED PROTECTION IN THE POWER INDUSTRY

4.1 Classification of Protection Levels

The classification process must combine the business nature of the power enterprise, the value of data, and the functions of systems to conduct a multi-dimensional security risk assessment and rational grading of each information system. In the core business systems of the power industry, data management systems and dispatch control systems usually belong to higher levels and should adopt stricter security protection measures. Through classification, power enterprises can more accurately apply corresponding security measures to systems of different levels, ensuring that the most critical systems are protected from threats and security risks are reduced. The classification work for Datang and other power enterprises should be carried out in light of actual conditions. Core enterprise systems and data systems involved in power dispatch and production should be assigned the highest security level to prevent greater losses caused by external attacks or internal vulnerabilities.

4.2 Construction of Security Protection System

After the classification work is completed, power enterprises need to build a corresponding security protection system based on the classification results. The construction of the security protection system should be carried out at several levels, mainly from physical security, network security, and data security. For example, core data and systems can be protected through encryption, access control, and firewall technologies; network security can be ensured by configuring intrusion detection and intrusion prevention to prevent external attacks from easily breaching the enterprise's security defenses. Power enterprises should emphasize a multi-level, multi-dimensional protection strategy in building their security protection system to ensure that various potential security risks are effectively addressed. For a power enterprise like Datang, building a security protection system that meets its actual needs not only enhances its security capabilities but also provides stable support for power production and management.

4.3 Construction of Security Management System

The construction of a power enterprise's security management system should include comprehensive planning of security organizational structure, process systems, personnel management, and training and education. First, the enterprise must establish a dedicated cybersecurity management department to manage all information systems. Second, it should establish scientific security management processes and systems, defining the security responsibilities and authorities of each department and position. Third, the enterprise should strengthen cybersecurity training for employees, raise overall security awareness, and ensure that every employee understands the importance of information security and actively cooperates in implementing security management measures. By building a complete security management system, power enterprises can achieve comprehensive and effective management of all information systems, ensuring the implementation and continuous improvement of various security measures.

4.4 Security Operations and Monitoring

The security operations and monitoring system of power enterprises is the key to ensuring the long-term and stable operation of information systems. Enterprises must deploy security monitoring equipment to monitor all critical information systems in real time and promptly detect and respond to potential security issues. In addition, regular security checks and vulnerability scans are important ways to ensure system security. Operations teams must strengthen system maintenance and updates to keep the system secure and controllable at all times. For power enterprises like Datang, security operations and monitoring must be closely integrated into daily production work to ensure system security while ensuring that power generation and management are not compromised.

5. IMPROVEMENT MEASURES FOR CYBERSECURITY CLASSIFIED PROTECTION

5.1 Technical Level

Technically, power enterprises should strengthen information system security protection and enhance overall technical defense capabilities. First, enterprises should actively introduce advanced cybersecurity technologies such as deep packet inspection, intrusion detection and prevention, network traffic analysis, and data encryption to improve their ability to resist external attacks [4]. Especially for power generation enterprises like Datang, whose control and dispatch systems are involved in critical areas such as the national grid and power supply, an attack could not only affect normal business operations but also cause large-scale power outages or public safety incidents. Therefore, building a comprehensive protection system is crucial. Second, strengthen the management of information system security vulnerabilities by conducting regular vulnerability scans and penetration tests, and promptly patching discovered vulnerabilities. Additionally, encryption technologies should be used during data storage and transmission to prevent data leakage or tampering. Multi-factor authentication and access control mechanisms should be implemented for critical equipment and systems such as power generation dispatch systems to ensure that only authorized personnel can access critical resources and data. Strengthening these technical measures can effectively improve the cybersecurity protection capabilities of power enterprises and reduce security risks caused by technical vulnerabilities.

5.2 Management Level

From a management perspective, power companies must establish a comprehensive cybersecurity management system to ensure the implementation of various security measures. First, a dedicated cybersecurity management department should be set up and staffed with sufficient professionals to manage the security of the enterprise information system. This department must not only formulate an overall plan for the enterprise's cybersecurity protection measures but also regularly evaluate and update the cybersecurity management plan to address emerging threats. Second, power companies must formulate and strictly enforce information security management systems, clearly define security responsibilities for each department and position, and establish a sound security audit mechanism. All security activities within information systems and networks must be tracked, recorded, and audited to ensure that issues are detected and resolved at the earliest opportunity. Third, strengthening employee cybersecurity training is crucial. Regular training enhances employees' security awareness, encouraging them to follow secure operating procedures in daily work and eliminate security vulnerabilities caused by human factors. For companies like Datang, establishing robust management systems and a security culture not only safeguards the long-term secure operation of enterprise information systems but, more importantly, fosters a collective awareness of cybersecurity risk prevention among all employees, thereby improving the overall level of protection.

5.3 Emergency Response and Recovery

Power companies must develop thorough emergency response plans for potential security incidents, conduct regular drills, and ensure efficient and accurate emergency response. The contingency plan should cover the entire process from incident detection to business system recovery, clearly define responsible parties and response measures, and guarantee rapid reaction to cyberattacks or security vulnerabilities, minimizing the impact on business operations. For large power companies like Datang, a cybersecurity incident could disrupt power dispatch systems or threaten power plant control systems, so their emergency response must be both highly efficient and strongly resilient. Enterprises must ensure the integrity and reliability of backup data and swiftly restore critical business systems to normal operation.

5.4 Cooperation and Sharing

In an increasingly complex cybersecurity landscape, collaboration and information sharing between power companies and other industries and institutions have become more critical. For power enterprises such as Datang, a single company's strength in confronting sophisticated cyber threats appears somewhat limited, making cross-industry cooperation especially vital [5]. Power companies must work closely with government agencies, industry associations, and cybersecurity firms to form security alliances for joint defense. By sharing information with these organizations, power companies can obtain the latest threat intelligence in a timely manner and respond rapidly. Moreover, security experiences and protection technologies across industries can be mutually referenced and optimized, enhancing the cybersecurity capabilities of power enterprises. Specifically, power companies can establish cross-industry security information-sharing platforms to promptly report cybersecurity incidents, exchange protection experiences, and raise overall defense levels. They can also participate in government- and industry-led cybersecurity research and standards development, advancing the security posture of the entire sector.

6. CONCLUSION

In short, implementing cybersecurity-level protection in the power industry is a systematic project that must address technology, management, emergency response and recovery, cooperation, and information sharing. Although the power industry has made some progress in cybersecurity, many urgent issues remain. By continuously improving the security protection system, raising security awareness, strengthening emergency response capabilities, and enhancing collaboration and information sharing both within and outside the industry, the power sector can effectively counter increasingly complex cyber threats. As technology advances and standards rise, cybersecurity-level protection will provide a more solid guarantee for the safe and stable operation of power systems. It is essential to keep abreast of new developments in cybersecurity, explore innovative solutions, meet future security challenges, and ensure the sustainable development of the power industry.

REFERENCES

[1] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.
[2] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.
[3] Xie, Minhui, and Shujian Chen. "InVis: Interactive Neural Visualization System for Human-Centered Data Interpretation." Authorea Preprints (2025).
[4] Hu, Xiao. "AdPercept: Visual Saliency and Attention Modeling in Ad 3D Design." (2025).
[5] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).
[6] Qin, Haoshen, et al. "Optimizing deep learning models to combat amyotrophic lateral sclerosis (ALS) disease progression." Digital health 11 (2025): 20552076251349719.
[7] Li, X., Lin, Y., & Zhang, Y. (2025). A Privacy-Preserving Framework for Advertising Personalization Incorporating Federated Learning and Differential Privacy. arXiv preprint arXiv:2507.12098.
[8] Wang, Yang, and Kowei Shih. "Hybrid multi-modal recommendation system: Integrating mmoe and xgboost for enhanced personalization and accuracy." 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC). IEEE, 2024.
[9] Fu, Lei, et al. "Adversarial Prompt Optimization in LLMs: HijackNet's Approach to Robustness and Defense Evasion." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.