INTI JOURNAL | Vol.2025, Issue 3, No.3
eISSN:2600-7320

A Review of Electromagnetic Safety Protection Technologies

Wen Zheng[1*], Leong Wai Yie[1]

[1]Faculty of Engineering and Quantity Surveying, INTI International University, 71800 Negeri Sembilan, Malaysia.

***Email:** i25031583@student.newinti.edu.my

Abstract

This paper provides a systematic review and comparative analysis of five pivotal electromagnetic-compatibility (EMC) and safety-protection technologies: the "OODA-loop"-based intelligent protection system, shielding techniques, energy-selective electromagnetic protection, cooperative electromagnetic-security suppression, and electromagnetic-noise jamming. By clarifying their technical principles, applicable scenarios, and current state-of-the-art, the study offers a reference for technology selection under diverse application requirements and for future research directions. A systematic review and analysis of the relevant technical literature and experimental reports was conducted, focusing on the working principles, typical applications, and measured performance of each technology. The results indicate that OODA-loop-based systems offer high automation and rapid response, making them well-suited for facility-wide protection of large-scale infrastructures; shielding techniques are the most mature and lowest-cost solution, hence the most widely deployed; energy-selective protection achieves nanosecond-level adaptive suppression, effectively countering high-power electromagnetic pulses entering through intended apertures, but at higher expense; cooperative suppression technology significantly improves jamming effectiveness and resource utilization through optimized algorithms; and electromagnetic-noise jamming, being mature and straightforward, is mainly employed for low-level information-leakage prevention. Each technology presents distinct advantages and limitations, necessitating judicious selection according to the specific operational scenario. This review compares their application contexts and highlights advantages/limitations.

Keywords

Electromagnetic Safety, Protection Technology, Process Innovation

Introduction

With the transformation from mechanization to informatization, intelligence, and networking, human society has evolved from the tangible physical world into an intangible physical realm characterized by electromagnetic fields and waves (Antić, 2024). The understanding of the

Submission: 7 July 2025; **Acceptance:** 29 August 2025; **Available online:** September 2025

electromagnetic domain has evolved from electromagnetic compatibility to electromagnetic security, which can be roughly divided into three stages. The first stage is the narrow understanding of electromagnetic compatibility, where the goal of achieving electromagnetic compatibility is mainly realized by controlling electromagnetic interference, with the core issue being the resolution of self-interference within the system. The second stage is the improvement of electromagnetic environmental adaptability, which, based on effectively controlling electromagnetic interference, further controls the effects of the electromagnetic environment. The core issue here is the system's adaptability to the electromagnetic environment under conditions of "self-interference, mutual interference, and hostile interference." The third stage focuses on electromagnetic security under strong electromagnetic attacks. Based on paying attention to electromagnetic compatibility and electromagnetic environmental adaptability, this stage aims to enhance the system's security capabilities under strong electromagnetic attacks, with the core issue being the electromagnetic vulnerability under electromagnetic attack conditions (Shafiq, 2024). The accuracy of OODA-loop-based protection systems in complex electromagnetic environments, their level of intelligence, and the cooperative mechanisms among multiple systems require further in-depth investigation. The development of lightweight, flexible, and high-performance shielding materials is a key research focus. The feasibility of energy-selective electromagnetic protection and its compatibility with traditional circuits need to be thoroughly studied. The transition of electromagnetic security cooperative suppression technology from theoretical simulation to practical deployment, as well as its capability to counter intelligent jamming strategies, needs to be enhanced. The effectiveness of electromagnetic noise jamming and its deep integration with other protection methods represent a future research direction. This paper reviews current electromagnetic safety protection technologies, analyzes their principles and applications, and compares their strengths and weaknesses.

Methodology

This section adopts a systematic, descriptive review to analyze the principles and applications of the five technologies, compare their effectiveness and limitations, and thereby fill the existing research gap in technical comparison and applicability assessment, providing a reference for the construction of integrated protection systems.

The Electromagnetic Security Protection System Based on the "OODA Loop"

The "OODA Loop" model, proposed by U.S. Air Force Colonel John Boyd, consists of four processes: Observe, Orient, Decide, and Action (Mao et al., 2020). The electromagnetic security protection system based on the "OODA Loop" includes electromagnetic environment monitoring and direction-finding devices, leakage shielding devices, and UAV countermeasures in its front end. The back end features application servers equipped with electromagnetic security protection software and database servers with electromagnetic spectrum databases, forming a monitoring system with one center and multiple perception nodes (Shafiq, 2024; Leong, 2002). This protection system divides the electromagnetic security protection process of the core area of the space launch site into four loops: spectrum perception, situation analysis, assessment and warning, and risk disposal. It operates in an autonomous, cyclic, and feedback-driven manner, enabling rapid response from signal detection to anomaly handling. The principle is shown in Figure 1.

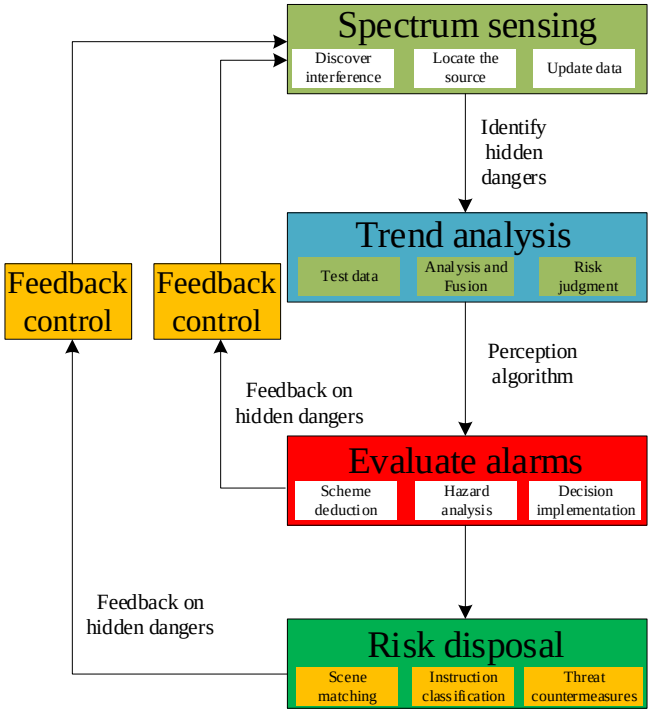

Figure 1. The Principle of the OODA Loop in Electromagnetic Safety Protection Systems

The spectral perception loop serves as the starting point of the “OODA Loop,” which involves the monitoring equipment in the core area to sense and collect electromagnetic signals from the surrounding environment. The situation analysis loop analyzes the electromagnetic data collected by the spectral perception loop. Meanwhile, it integrates data from the central station and perception nodes, and in combination with the electromagnetic wave propagation model in the core area, employs algorithms such as interpolation to depict the electromagnetic spectrum situation map (Leong, 2024). The assessment and warning loop receives feedback data from the situation analysis loop and evaluates the risk level based on the built-in risk assessment mechanism. The risk disposal loop is the precision energy release phase. According to the input from the assessment and warning loop, it coordinates the equipment within the system to perform localization, classification, and counteraction, forming a closed loop for anomaly disposal and feeding the results back to the spectral perception loop. The Hainan Commercial Space Launch Site in China has established a regional perception network and countermeasures based on the "OODA Loop". It can detect typical electromagnetic security risks such as electromagnetic noise, interference, radiation leakage, and UAV harassment at the launch site. It can identify electromagnetic interference events within 1 minute and locate the interference source within 30 minutes. This has solved the previous problem of low efficiency and automation in detecting interference sources, which required professional personnel to carry equipment for monitoring and was incapable of dealing with short-duration electromagnetic interference signals. This method has improved the efficiency of handling and enhanced electromagnetic security protection capabilities (Liu & Zhang, 2025).

Shielding Protection Technology

Shielding protection technology employs specific technical methods to confine the effects and impacts of electromagnetic radiation within a designated spatial area. It is currently the most widely used technique for electromagnetic radiation protection (Mostafavi, 2023). Wang Baoguo et al. employed a single-sided shielding protection method for electromagnetic interference and network information protection in building environments. A single-sided conductive glass curtain wall can provide partial electromagnetic shielding for information and radio-frequency devices within a room. This reduces the likelihood of electromagnetic signals within the area being intercepted externally and diminishes the interference of external electromagnetic signals on indoor information devices, thereby bringing electromagnetic security risks within a controllable range. Additionally, the conductive glass curtain wall also has the capability to acquire voice and image data through communication reconnaissance means. Experiments were conducted to evaluate the electromagnetic protection effectiveness of the conductive glass curtain wall. The radiation field distribution in both longitudinal and transverse directions for a rectangular shielded body in a deep-shadowing scenario, considering multiple edge diffractions, was calculated. The experimental results are consistent with the classical theory's predictions of longitudinal attenuation convergence and transverse shell-like distribution. Using radiation field distribution maps and indoor-outdoor radio wave propagation models, they analyzed the shielding effectiveness and safety impact distance of single-sided shielding in specific engineering contexts. Simulations showed that for a 10m×3m conductive glass curtain wall, shielding reduced the outdoor safety distance by over 10 times and increased the indoor safety distance by 1.30 - 1.56 times. These findings guide the quantitative design of single-sided shielding projects. The method, now successfully applied, is gaining industry favor for its cost-efficiency (Mostafavi et al., 2023).

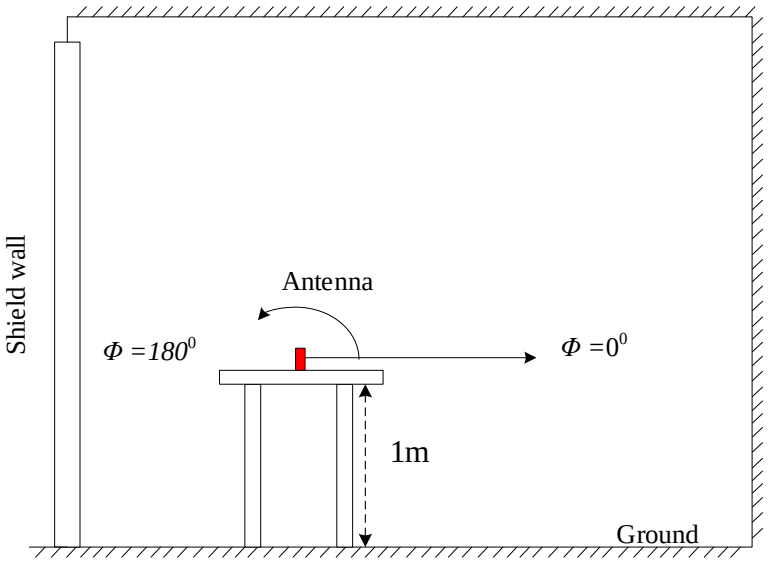

Figure 2. Layout of a Single-sided Shielding Protection Model Room

Energy-Selective Electromagnetic Protection Technology

Under intense electromagnetic pulses, the focus of electromagnetic protection lies in severing the coupling pathways between the intense electromagnetic pulses and sensitive equipment, thereby reducing the electromagnetic energy received by the sensitive devices (Leong, 2025). Electromagnetic protection can be categorized into front-door protection and back-door protection

based on the coupling pathways. Front-door protection primarily prevents high-power microwaves (HPM) from entering the system through the front-door paths, such as antennas and transmission lines. In contrast, back-door protection aims to prevent HPM from entering the system through back-door paths, including holes, gaps, and cable interfaces on the electronic equipment enclosures. Research on back-door protection is relatively comprehensive, and effective measures such as grounding and shielding can be employed to cut off the back-door coupling pathways. However, research on front-door protection is relatively limited (Liu, 2020). Under instantaneous intense electromagnetic pulses, traditional protection methods face limitations, and front-door protection encounters challenges such as in-band operation, high power, and rapid response. To address these issues, Liu Peiguo et al. proposed an energy-selective electromagnetic protection method, which is a novel adaptive intense electromagnetic protection technology. This method is realized through the principle of field-induced impedance transformation. Impedance-sensitive materials or artificial electromagnetic structures are employed to sense the intensity of electromagnetic wave energy in real time, thereby achieving self-adaptive impedance regulation. When the incident electromagnetic wave energy is below the safety threshold, the protection device maintains a high impedance, allowing the electromagnetic wave to transmit with low loss. Upon detecting an intense electromagnetic pulse, the nonlinear characteristics of the material or device trigger a sudden impedance drop. This impedance mismatch significantly attenuates the electromagnetic energy. This state transition occurs without external control and has a response time on the nanosecond scale. It overcomes the contradiction between power capacity and response speed of traditional protection devices. Moreover, it provides effective protection without affecting the normal operation of the equipment, thus solving the dilemma of "protection" and "compatibility" in front-door protection of electronic devices. This method offers a new approach for intense electromagnetic protection and is of great significance for enhancing the electromagnetic protection capabilities of electronic equipment (Liu & Hu, 2024).

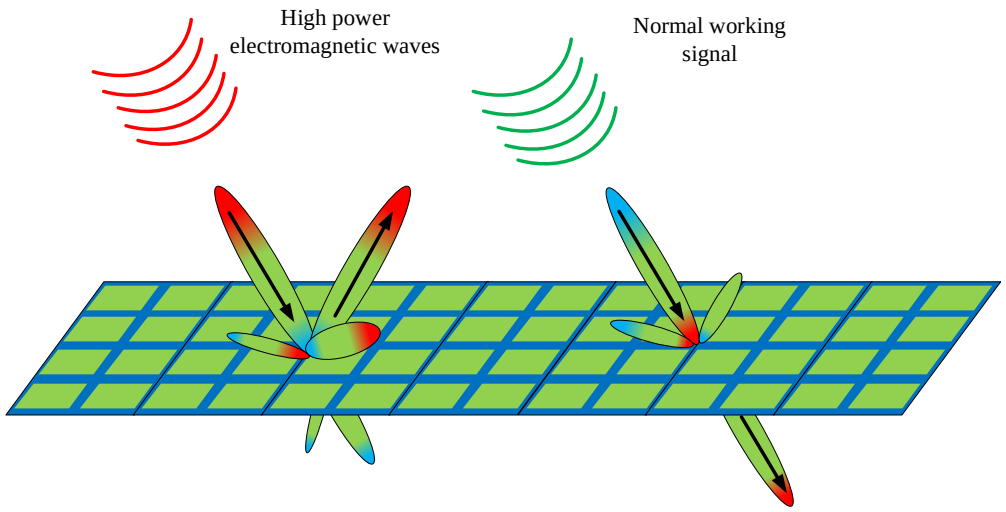

Figure 3. Schematic diagram of energy selection electromagnetic protection

Electromagnetic Security Cooperative Suppression Technology

The management and control of electromagnetic security is complex and diverse and is a key issue in communication interference and related fields (Kong et al., 2022). Shi Jia et al. have put forward the technology of electromagnetic security cooperative suppression. They first built a radio wave propagation model for complex urban environments, and through simulation analysis, they

revealed the characteristics of such environments. Then, to achieve effective electromagnetic suppression and avoid harmful interference, they designed a collaborative deployment strategy for electromagnetic suppression devices using potential game theory and proposed a power optimization method based on genetic algorithms. This enables collaborative multi-device operations and efficient delivery in complex electromagnetic environments, significantly enhancing the overall effectiveness of electromagnetic suppression systems. Simulation experiments show that the developed electromagnetic suppression device layout algorithm performs close to the theoretical optimum with lower computational complexity. Further analysis indicates that the new power optimization algorithm reduces transmission power by over 50% compared to traditional interference power allocation schemes, improving collaborative and precise control capabilities (Shi et al., 2024).

Electromagnetic Noise Interference Technology

Electromagnetic noise interference technology conceals useful information in electromagnetic leakage emissions by increasing the intensity and complexity of the electromagnetic leakage radiation noise. Even low-radiation emission products inevitably leak unconscious electromagnetic signals. To prevent adversaries from acquiring information, the interference device employs a wide frequency range and high amplitude to mask the information from two aspects simultaneously (Mao et al., 2020). For example, computer video information jammers are information security and confidentiality protection products developed to address the issue of electromagnetic leakage from computers. They provide multiple layers of protection for computer radiation information through spatial random number encryption technology, correlated interference, and noise confusion, thereby making it more difficult for adversaries to steal information. Spatial random number encryption technology: The electromagnetic radiation signals from classified computers are scrambled. Even if an adversary receives these signals, it is extremely difficult to decode the effective information they carry. Correlated interference technology refers to the ability of the interference device to generate signals that can track the computer's radiation information in real time and maintain a high degree of correlation with it. This technology effectively overcomes the weakness of using pure white noise as an interference signal, which is easily demodulated, thereby reducing the likelihood of being cracked. Electromagnetic interference technology is currently relatively mature, easy to use, and has strong resistance to decryption. However, its level of protection is somewhat limited and is mainly used to protect information with lower levels of confidentiality (Antić, 2024).

Results and Discussion

The “OODA Loop” Security Protection System is well-suited for scenarios such as space launch sites, military bases, and communication hubs. Shielding protection technology is well-suited for scenarios such as indoor protection, localized sensitive areas, and temporary protection. The energy-selective electromagnetic protection technology is well-suited for applications in electronic warfare and information countermeasures, aerospace and critical infrastructure, and industrial control systems. The Electromagnetic Security Collaborative Suppression Technology is well-suited for applications such as security assurance for major events, electromagnetic control in densely built-up areas, and protection of communication hubs. Electromagnetic noise interference technology is suitable for general office environments and temporary combat scenarios.

Table 1. Comparative Overview of Electromagnetic Safety Protection Technologies (Miao, 2019)（Lv et al., 2025）

Technical Name	Maturity	Advantages	Drawbacks	Cost / Adoption Rate	Potential research gaps
"OODA Loop" Security Protection System	relatively high	Multi-device collaboration, high degree of automation, active defense, and reduced human intervention.	Regular calibration of equipment is required to enhance system performance, which involves a significant amount of maintenance work.	High cost, low adoption rate	Accuracy in complex electromagnetic environments, level of intelligence, and inter-system cooperative mechanisms.
Shielding Protection Technology	high	It has a relatively high cost-effectiveness ratio, with significant directional shielding effectiveness and superior performance in high-frequency bands.	It requires high precision in deployment and has limited environmental adaptability.	Cost varies with material and scale; adoption rate is the highest.	Novel lightweight, flexible, and high-performance shielding materials
Energy-Selective Electromagnetic Protection Technology	relatively low	Strong adaptive response capabilities, high power tolerance, and suitable for protection against intense electromagnetic pulses.	In complex electromagnetic environments, it may lead to misjudgments, and the protection performance significantly degrades in high-frequency bands.	Relatively high cost and low adoption rate.	Feasibility for large-scale integrated deployment and compatibility with conventional circuitry
Electromagnetic Security Cooperative Suppression Technology	Moderate, leaning theoretical.	Efficient collaborative suppression and precise control to avoid collateral damage to whitelisted devices.	The computational complexity is high, and the rapid response capability to sudden electromagnetic interference needs to be improved.	High cost, low adoption	Technical feasibility and compatibility with conventional circuits
Electromagnetic Noise Interference Technology	high	Easy to deploy and quick to implement.	The protection level is limited. It relies on the intensity of the interference, and if the adversary employs advanced filtering techniques, the effectiveness of the interference can be weakened.	Low cost, high adoption.	Effectiveness and deep integration with other protection measures

Conclusion

This review comparatively analyzes the distinctive features and inherent limitations of existing electromagnetic-protection techniques. OODA-loop systems hinge on sensor accuracy and algorithmic reliability; shielding struggles against high-frequency threats and complex environments; energy-selective protection must yet guarantee stability under high-power stresses; cooperative suppression demands further optimization of real-time performance and resource allocation; noise jamming remains restricted to low-classification information protection. Grounded in literature analysis, the survey concludes that future work should pursue converged deployments of multiple technologies, develop intelligent self-adaptive protection algorithms, engineer novel high-performance materials, and establish unified test and evaluation standards, thereby advancing an integrated, intelligent electromagnetic-protection architecture.

Acknowledgements

We would like to thank the editorial team and anonymous reviewers for their time and thoughtful comments, which helped enhance the clarity and rigor of our work.

References

Antić, V., Protić, D., Stanković, M., Prodanović, R., Manić, M., Ostojić, G., Stankovski, S., & Kučević, D. (2024). Protecting data at risk of unintentional electromagnetic emanation: TEMPEST profiling. *Applied Sciences, 14*(11), 4830. https://doi.org/10.3390/app14114830

Choi, S., Kwon, O.-J., Oh, H., & Shin, D. (2020). Method for effectiveness assessment of electronic warfare systems in cyberspace. *Symmetry, 12*(12), 2107. https://doi.org/10.3390/sym12122107

Kong, D. Q., Yang, B. P., & Li, F. (2022). Research on prototype system for electromagnetic spectrum management and control based on GIS. In *Proceedings of the 8th Annual International Conference on Network and Information Systems for Computers* (ICNISC 2022), Hangzhou, China. IEEE. https://doi.org/10.1109/ICNISC57059.2022.00156

Leong, W. Y., & Homer, J. (2002). Hop selection in peer-to-peer WPAN networks. In *ICCS 2002: 8th International Conference on Communications Systems* (Vol. 2, pp. 870–872). IEEE. https://doi.org/10.1109/ICCS.2002.1183255

Leong, W. Y., Leong, Y. Z., & Leong, W. S. (2024). System-on-Chip (SoC) medicine. In *2024 IEEE International Workshop on Electromagnetics: Applications and Student Innovation Competition (iWEM)* (pp. 1–2). IEEE. https://doi.org/10.1109/iWEM59914.2024.10649387

Leong, W. Y. (2025). Digital twin models for real-time failure prediction in industrial machinery. *ASM Science Journal*, *20*(1). https://doi.org/10.32802/asmscj.2025.1923

Liu, P. G., & Hu, N. (2024). Theory and application of energy-selective electromagnetic protection method. *Chinese Journal of Radio Science, 39*(3), 385–394, 431. https://dx.doi.org/10.12265/j.cjors.2023181

Liu, P. G., Liu, H. Q., & Wang, K. (2020). Application of graphene in strong electromagnetic protection technology for ships. *Chinese Journal of Ship Research, 15*(4), 1–8. https://doi.org/10.19693/j.issn.1673-3185.01662

Liu, T., & Zhang, J. Y. (2025). Design of electromagnetic safety protection system for core area based on "OODA loop." *Radio Engineering, (02),* 393–397. http://dianda.cqvip.com/Qikan/Article/Detail?id=7200297418

Lv, J., Luo, C., Zhao, J., Han, H., Lu, H., & Zheng, B. (2025). Development of energy-selective surface for electromagnetic protection. *Micromachines, 16*(5), 555. https://doi.org/10.3390/mi16050555

Mao, J., Liu, J., Zhang, J., Wang, Y., & Li, H. (2020). A method for detecting image information leakage risk from electromagnetic emission of computer monitors. *Journal of Intelligent & Fuzzy Systems, 40*(2), 2981–2991. https://doi.org/10.3233/JIFS-189337

Miao, C. (2019). Research status and development trend of electromagnetic information security technology. *Secrecy Science and Technology, (2),* 5–11.

Mostafavi Yazdi, S. J., Lisitski, A., Pack, S., Hiziroglu, H. R., & Baqersad, J. (2023). Analysis of shielding effectiveness against electromagnetic interference (EMI) for metal-coated polymeric materials. *Polymers, 15*(8), 1911. https://doi.org/10.3390/polym15081911

Shafiq, Z., Li, T., Xia, J., Li, S., Yang, X., & Zhao, Y. (2024). Addressing EMI and EMF challenges in EV wireless charging with the alternating voltage phase coil. *Actuators*, *13*(9), 324. https://doi.org/10.3390/act13090324

Shi, J., Li, A. T., Li, Z., Xiao, S. G., & Wei, Q. (2024). Collaborative electromagnetic suppression methods for electromagnetic security control of major events. *Journal of Electronics and Information Technology*, *46*(5), 1908–1919. https://doi.org/10.11999/JEIT231318