

Opportunities and challenges of security and safety in AI-empowered ecological construction

Jiangxing Wu^{1,2,3,4,*} 

¹ National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, 450002, China

² Purple Mountain Laboratories, Nanjing, 211111, China

³ Songshan laboratory, Zhengzhou, 450000, China

⁴ Fudan University, Shanghai, 200433, China

Received: 26 January 2026 / Revised: 26 January 2026 / Accepted: 28 January 2026 / Published online: 30 January 2026

Citation Wu JX. Opportunities and challenges of security and safety in AI-empowered ecological construction. Security and Safety 2026; 5: E2026005. <https://doi.org/10.1051/sands/2026005>

As the year turns and a new chapter unfolds, on behalf of the editorial board of Security and Safety (S&S), I extend my sincere gratitude and New Year's greetings to the editorial board members, peer reviewers, authors, and readers who have supported the journal's development.

Since its launch in 2022, S&S has coincided with a pivotal era when the global digital ecosystem's underlying paradigm is accelerating its shift toward cyber resilience. Cybersecurity and functional safety are increasingly intertwined, while cutting-edge technologies and applications (including artificial intelligence (AI), cloud computing, and the metaverse) evolve at a rapid pace. As the digital and physical worlds converge ever deeper, security boundaries continue to expand, and risk landscapes undergo constant transformation. Against this backdrop, as an international academic journal focusing on the interdisciplinary intersection of cybersecurity and functional safety, S&S adheres to the ethos of "cross-fertilization and innovative integrity". It serves as an academic exchange platform for safety science and technology, fostering in-depth synergy between cybersecurity and functional safety to address the unprecedented security challenges posed by complex systems. From its humble beginnings to steady growth, the journal has evolved into a prominent platform for sharing academic insights and innovative achievements in this interdisciplinary field with the global community.

Reflecting on this journey, we have collectively witnessed every milestone of the journal's progress. We have centered on hot topics in security and safety, publishing eight topical issues covering interdisciplinary security domains such as "Metaverse", "Unmanned Systems", "Physical Layer Systems", "Space-Air-Ground Integrated Networks", "Artificial Intelligence", "Cloud Computing", "Network Simulation and Evaluation", and "Next Generation Industrial Systems", alongside numerous high-caliber articles on open themes. Currently, we are organizing several cutting-edge interdisciplinary special topics, including "Intelligent Connected Vehicles", "Medical and Healthcare", "Embodied Intelligence", "Smart Grid", and "Decision-Making and Control of Multi-Agent Systems", which showcase top-tier research outcomes in the field. S&S has also been indexed by multiple international databases. These accomplishments would not have been possible without the dedication and hard work of every editorial board member.

Standing at this new juncture, we are deeply encouraged by our achievements yet soberly aware of the road ahead: Today, AI is penetrating all sectors of society with a revolutionary momentum characterized by "generalization, inclusiveness, and ecologicalization". It has not only reshaped the landscape of technology and industry but also presented the cybersecurity and data security field with the epochal

* Corresponding author (email: ndscwjx@126.com)

proposition: “New challenges in AI-driven ecological construction, and new opportunities for security and trustworthiness”. More critically, we must remain vigilant that the large-scale proliferation of AI, if decoupled from the bottom-line constraint of security and trustworthiness, risks “feeding a tiger only to be devoured by it”. Such risks span the entire AI lifecycle from data leakage, model poisoning, and adversarial attacks to the lack of traceability for large model-generated content and safety hazards in the autonomous decision-making of embodied intelligence’s physical forms. These threats can cascade through ecological chains, undermining the stability and balance of the digital ecosystem.

As an academic platform dedicated to the frontiers of security and safety theories and technologies in cyberspace, S&S must proactively adapt to the times. It will take “security and trustworthiness” as its core mission to steer industry ecosystem development, leveraging AI to drive the journal’s high-quality growth while resolutely upholding its academic responsibility to mitigate the risks of technological abuse. S&S will continue to pursue its mandate of “guarding security bottom lines and pioneering technological frontiers”, striving to become a cradle of safety science thought, a showcase for interdisciplinary innovations, and a repository of wisdom for global security governance. Let us navigate risks with scientific rigor and embrace challenges with innovative courage, collectively writing a new chapter in the advancement of safety science! The journal’s key priorities moving forward are as follows:

First, guide the direction with “academic acumen”. Rooted in its interdisciplinary focus, the journal will delve into emerging security issues stemming from AI’s large-scale penetration. It will prioritize research on endogenous security design and lifecycle quality assurance for AI products, including data security validation throughout the AI lifecycle, traceability and ethical compliance of large model-generated content, AI-driven risk mitigation for embodied intelligent systems, and the development of cross-scenario security standards. We will curate thematic issues, proactively inviting and featuring high-impact original research that pushes the boundaries of the field.

Second, uphold quality with “academic credibility”. For submitted manuscripts, we will rigorously assess three core criteria: “Is the problem practically meaningful? Is the methodology innovative and robust? Are the conclusions technically and engineeringly valuable?” We will firmly reject “bandwagon research”, “low-level repetition”, “nomenclatural gimmicks”, and “conceptual hype”, while giving precedence to innovative work that effectively addresses inherent individual or systemic security challenges in AI. Every published paper must withstand the scrutiny of both academic peers and real-world application. We will implement a dual-track screening mechanism of “AI-aided+manual review”, using AI tools to enhance the efficiency of similarity checks and domain relevance assessments, while strengthening manual oversight to mitigate academic integrity risks and foster a high-quality academic ecosystem for AI security research.

Third, expand research horizons with “academic openness”. We encourage submissions of security and safety research across interdisciplinary domains such as smart agriculture, smart healthcare, public opinion governance, embodied intelligence, and smart grids. We particularly welcome interdisciplinary innovations in areas including endogenous security architecture design for AI products, security quality testing technologies, and trustworthy evaluation systems, positioning S&S as a frontier for interdisciplinary innovation between cybersecurity and functional safety. AI’s large-scale penetration is breaking down traditional industry and technological silos, spawning new research agendas and opening innovative pathways for security and trustworthiness in cross-cutting fields.

AI is not only an epoch-making technological tool, but also a key catalyst for human societal progress. While we harness AI to streamline journal operations and empower security research, we must remain vigilant against ethical risks and ecological imbalances stemming from its misuse. The journal’s editorial board will continue to deepen its understanding of the dialectical relationship between “AI+ecology” and “security and trustworthiness”. With a forward-looking academic vision, rigorous quality standards, and an open collaborative stance, we will shape S&S into a thought leader and technological trailblazer in security and safety. Guided by the perseverance of “forging a sword for a decade”, we will elevate the journal into an internationally influential academic benchmark, contributing wisdom and strength to cyberspace security and the healthy, sustainable development of the AI era.

We warmly invite experts and scholars worldwide to submit your work, exchange ideas, and share insights, collectively advancing the field of security and safety. Thank you for your attention and support!