

Research on the Standardization Process Tracking of Cyber Security for Mobile Embodied Intelligent Agents and Landing Requirements

Xia Liu, Wen Shao and Chang Meng *

CATARC Intelligent Technology (Tianjin)Co., Ltd., Tianjin, 300300, China

* Corresponding author: Chang Meng

Abstract

Mobile embodied intelligent agents, as a product of the deep integration of embodied intelligence and mobile platforms, are moving from laboratories to open scenarios such as logistics, inspection, and household services. However, their attributes of "mobility + openness + wireless + physical execution" simultaneously amplify cyber security risks. Taking "robots—cyber security—standards" as the thread, this paper systematically tracks the cyber security standardization process of mobile embodied intelligent agents at home and abroad: it sorts out international governance frameworks including ISO/IEC, IEEE and the European Union, analyzes the standard formulation and revision progress in China centered on the Technical Committee for Standardization of Humanoid Robots and Embodied Intelligence of the Ministry of Industry and Information Technology and the National Cybersecurity Standardization Technical Committee, and summarizes the adaptability of existing standards in light of the "Standard System for Humanoid Robots and Embodied Intelligence (2026 Edition)", the embodied intelligence benchmark testing industry standard, and a batch of national standards under development. The study shows that existing standards still have obvious gaps in the aspects of perception data security, open wireless communication protection, algorithm and model trustworthiness, and loss of control in human-robot collaboration. Accordingly, countermeasures and suggestions for accelerating the alignment between landing requirements and standard coordination are proposed from the three levels of technology, management and industrial ecosystem.

Keywords

Mobile Embodied Intelligent Agent; Embodied Intelligence; Cyber Security; Standardization; Landing Requirements.

1. Introduction

Embodied intelligence, as a new paradigm of the deep integration of artificial intelligence and physical entities, is regarded as a key support for the transition from Industry 4.0 to Industry 5.0. In March 2025, embodied intelligence was written into the Report on the Work of the Government for the first time and was included in the key directions of future industries for the "15th Five-Year Plan"[20]. According to institutional estimates, the global embodied intelligence market size was about RMB 90 billion in 2025 and is expected to reach RMB 150–200 billion in 2026, while that of China was about RMB 60 billion in 2025[15]. Morgan Stanley forecasts that shipments of humanoid robots in China will reach 50,000 units in 2026 and 446,000 units by 2030, corresponding to a compound annual growth rate of about 106%[14]. 2026 is regarded by the industry as the "year of mass production" for humanoid robots, and the Ministry of Industry and Information Technology and the State-owned Assets Supervision and Administration Commission of the State Council have jointly launched a special action for real-

scenario training of humanoid robots and embodied intelligence, aiming to build the capability of delivering landing at the ten-thousand-unit scale by the end of 2026.

Mobile embodied intelligent agents are representative carriers of this wave. They combine autonomous mobile platforms (AGV/AMR, wheeled or legged chassis) with embodied cognition, multimodal perception, autonomous decision-making and physical execution, and are widely deployed in open scenarios such as warehousing logistics, park inspection, building delivery and household services. Unlike fixed-station industrial robots, they operate for a long time in uncontrolled, open and dynamic environments, generally rely on wireless networks and cloud-edge collaboration, have greatly expanded attack surfaces, and the consequences of cyber security incidents are amplified from "data loss" to "physical injury". Meanwhile, as the "infrastructure" for industrial landing, the mismatch between the standardization process and the needs is becoming increasingly prominent. Oriented to the approved project "Standardization Process Tracking and Landing Requirements of Mobile Embodied Intelligent Agents", this paper focuses on the cross-field of "robots—cyber security—standards", tracks the standardization process, analyzes gaps and proposes landing requirements.

2. Mobile Embodied Intelligent Agents and Their Cyber Security Connotations

2.1. Concept Definition

A mobile embodied intelligent agent can be defined as an intelligent system that uses an autonomous mobile chassis as its physical carrier, embeds artificial intelligence (large models, reinforcement learning, multimodal perception, etc.) into the robot entity, enables it to possess the full-stack closed-loop capability of "perception—cognition—decision—execution", and is able to interact with scenarios in real time in mobile open environments. Its essential difference from traditional mobile robots lies in the added intelligent core of "embodied cognition + autonomous control + safe execution": it no longer relies on preset programs and fixed trajectories, but achieves autonomous planning and adaptive interaction through environmental perception. With reference to the analysis in the "Technical Research Report on Cybersecurity Standardization — Research on the Standardization of Industrial Embodied Intelligence Security" of the National Cybersecurity Standardization Technical Committee[1], mobile embodied intelligent agents also possess characteristics such as multimodal active perception, autonomous behavior learning, knowledge reasoning and embodied navigation. Moreover, due to the "mobile" attribute, they impose higher requirements on environment modeling, path planning, human-robot distance control and wireless communication reliability.

2.2. Cyber Security Risks Faced by Mobile Embodied Intelligent Agents

Table 1. Cyber security risk classification of mobile embodied intelligent agents

Layer	Main Risk	Typical Manifestation / Consequence
Perception layer	Perception data injection and deception	Camera, LiDAR and IMU data are forged, misleading mapping and obstacle avoidance; GPS spoofing causes path deviation
Communication layer	Wireless link hijacking and man-in-the-middle attacks	WiFi/Bluetooth/BLE is taken over, control commands are tampered with or replayed, and telemetry data is stolen
Algorithm layer	Model backdoor, adversarial examples and prompt injection	The large-model agent is induced by constructed voice or text input to execute arbitrary code, and decisions are unexplainable
Execution layer	Control command hijacking causing physical injury	The robot is remotely taken over to punch or ram, causing personal injury or equipment damage

With reference to the security analysis framework of industrial embodied intelligence[1], the security of mobile embodied intelligent agents can be divided into four mutually coupled dimensions: physical security, cyber security, control security and cognitive security, among

which cyber security is the link connecting perception, control and cognition. This paper summarizes the main risks at four levels — the perception layer, communication layer, algorithm layer and execution layer — as shown in Table 1.

Real cases have repeatedly corroborated the above risks. In September 2025, security research institutions disclosed that Unitree's Go2/B2 quadruped robots and G1/H1 humanoid robots had a high-risk Bluetooth BLE vulnerability codenamed UniPwn (corresponding to CVE-2025-35027, CVE-2025-60250 and CVE-2025-60251), through which attackers could achieve root-level command execution via the BLE interface, forcing Unitree to issue urgent fixes[16][18]. At the GEEKCON security hacking competition in October 2025, white-hat hackers "infected" another unconnected Unitree G1 robot through an already-connected one, causing it to punch a dummy directly; researchers also found that arbitrary code execution permission on the target robot could be obtained through a specific voice input "open sesame"[17]. In addition, CVE-2025-41110 shows that the Ghost Robotics Vision 60 quadruped robot lacks default authentication in the ROS 2 environment, allowing attackers to connect via WiFi and fully control the robot through SSH; the SlowROS slow denial-of-service attack against the ROS architecture has also been proven able to paralyze the robot system[16].

2.3. Special Nature of Cyber Security in Mobile Embodied Intelligent Agents

Compared with fixed industrial robots and ordinary IoT devices, the cyber security of mobile embodied intelligent agents presents three special characteristics. First, the environment is open and the attack surface is uncontrollable; nodes can dynamically join during operation, and spoofing and injection attacks are difficult to defend against through closed boundaries. Second, they depend on wireless communication; safety-related communication must guarantee integrity, confidentiality and availability over open channels, and the communication complexity is far higher than that of wired systems[19]. Third, the physical consequences are direct; cyber security incidents can be directly transformed into physical injuries such as arm swings and chassis collisions, involving personal safety. Therefore, the cyber security of mobile embodied intelligent agents cannot simply follow the "boundary defense" approach of traditional information systems, but must establish a differentiated protection framework covering the whole chain of perception, communication, algorithm and execution at the standard level.

3. Tracking the Standardization Process of Cyber Security for Mobile Embodied Intelligent Agents

3.1. International Standardization Process

At the international level, a coordinated pattern of multiple standard families of "safety + trustworthiness + cyber security" has been formed. ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) has published 258 standards, providing the foundation for data and privacy protection[12]; ISO/IEC 27400:2022 and 27402:2023 respectively provide guidelines on IoT security and privacy and device baseline requirements, and can serve as the general baseline for mobile embodied intelligent agents as networked devices[10][11]. With regard to the robot body itself, ISO 13482 specifies safety requirements for service robots, and its clause 6.15 specifically addresses cyber security and data privacy[7]; ISO 22166-1:2021 sets module-level cyber security clauses in the general requirements for the modularity of service robots[9]. ISO 10218-1:2025, published in 2025, adds clause 5.3.6, which introduces "transmission categories" (TC1 closed type, TC2 semi-open type and TC3 fully open type) by drawing on railway communication standards, implements differentiated threat protection for different transmission categories, and makes clear that mobile devices such as humanoid robots need to adopt the highest level of protection for most threats because of wireless

communication[8][19]. At the governance level, ISO/IEC 38507:2022 clarifies the governance framework for industrial robots, ISO/IEC TR 24028:2020 provides guidelines for trustworthy AI, and IEEE P7007 and IEEE 2841-2022 focus on the safety operation digital passport and adversarial robustness testing respectively[1]. The European Union "Artificial Intelligence Act" (effective in 2024) imposes compliance requirements on high-risk AI systems by means of risk classification; the United States implements "standard guidance + industry self-discipline" based on the NIST AI RMF 1.0[1].

3.2. Domestic Standardization Process

The domestic process presents a multi-layered parallel trend of "top-level design—industry standards—association standards—national standards under development". On December 27, 2025, the Technical Committee for Standardization of Humanoid Robots and Embodied Intelligence of the Ministry of Industry and Information Technology was formally established, undertaking the formulation and revision of industry standards in such fields as fundamental commonalities, key technologies, components, complete machines and systems, applications, and safety[2]. On February 28, 2026, the "Standard System for Humanoid Robots and Embodied Intelligence (2026 Edition)" was compiled and released by the Committee with the participation of more than 120 units. As China's first top-level design of standards covering the whole industry chain and full life cycle of humanoid robots and embodied intelligence, it sets up sections including fundamental commonalities, brain-like intelligence and computing power, limbs and components, complete machines and systems, applications, and safety and ethics[3]. In March 2026, the Ministry of Industry and Information Technology approved and released YD/T 6770-2026 "Artificial Intelligence — Key Basic Technologies — Benchmark Test Methods for Embodied Intelligence", becoming the first industry standard in the field of embodied intelligence[4]. On May 22, 2026, the association standard "Management Specification for the Full Life Cycle of Humanoid Robots" was released, proposing a 29-character identity code ("one machine, one code"). By the time of release, about 28,000 robots had obtained the "identity card", laying the foundation for the traceability and security management of mobile embodied intelligent agents[5].

On the cyber security dimension, the National Cybersecurity Standardization Technical Committee (TC260) continues to make arrangements. On the one hand, China has published 1 mandatory national standard, 12 recommended national standards and 1 technical document on AI security, among which GB 45438-2025 is a mandatory standard, GB/T 45654-2025 puts forward basic security requirements for generative artificial intelligence services, GB/T 42888-2023 regulates the security assessment of machine learning algorithms, and GB/T 41871-2022 clarifies the data processing security requirements for automobiles[1]. On the other hand, the "AI Security Standard System (V1.0)" (draft for comments) explicitly sets up two development directions, "agent security" and "embodied intelligence security", under the key technology category[1]; the "Technical Research Report on Cybersecurity Standardization — Research on the Standardization of Industrial Embodied Intelligence Security" released in March 2026 systematically sorted out domestic and foreign policies and standards and put forward construction suggestions, providing a direct basis for the development of national standards for the cyber security of mobile embodied intelligent agents[1].

In terms of special standards for embodied intelligence and mobile robots, a batch of national standards and guidance technical documents are being intensively landed or developed: GB/Z 220-2026 "Artificial Intelligence — Technical Requirements for Embodied Intelligence Data Generation Platforms" was published in August 2026; "Artificial Intelligence — General Requirements for the Trustworthiness of Embodied Intelligence", "Artificial Intelligence — Technical Requirements for Embodied Intelligence Large Model Systems", "Artificial Intelligence — Specifications for Embodied Intelligence Data Quality" and "Guidelines for the

Construction of Embodied Intelligence Data Training Grounds" are under development; GB/T 48317.3/4/5-2026 "Technical Requirements for Humanoid Robots" (motion control, operation, etc.) have been published and will be implemented in 2027; and the national standard plan "Artificial Intelligence — Intelligence Grading of Embodied Intelligence" has entered the approval stage[6]. For mobile scenarios, GB/T 45750-2025 "Warehouse Logistics Equipment — Automated Guided Vehicle — Safety Specification", GB/T 47494/47495-2026 "Logistics Robots — Electrical Safety Requirements and Test Methods", GB/T 10827.4-2023 "Industrial Trucks — Safety Requirements and Verification — Part 4: Driverless Industrial Trucks and Their Systems", GB/T 30029-2023 "Automated Guided Vehicles — General Design Rules" and GB/T 47864-2026 "Requirements for Underlying Data Interfaces of Industrial Mobile Robot Dispatching Systems" provide support for the functional, electrical and interface safety of mobile robot bodies and dispatching[6].

3.3. Key Milestones of the Standardization Process

As shown in Table 2, the cyber security standardization of mobile embodied intelligent agents has moved from "scattered following" to "systematic construction", and the process has accelerated notably since late 2025.

Table 2. Key milestones of the cyber security standardization process for mobile embodied intelligent agents

Time	Event	Type / Significance
2022-2023	GB/T 41871-2022 data security, GB/T 42888-2023 algorithm security assessment; ISO/IEC 27402:2023, GB/T 10827.4-2023	Foundations for data and algorithm security, device baseline, and mobile vehicle safety
2025-05	GB/T 45750-2025 "Warehouse Logistics Equipment — Automated Guided Vehicle — Safety Specification" released	National standard on mobile logistics robot safety
2025-09	Unitree UniPwn vulnerability disclosed; CVE-2025-41110 and others published	Industrial security incidents pushing standardization
2025-12-27	Technical Committee for Standardization of Humanoid Robots and Embodied Intelligence of MIIT established	Top-level standards organization
2026-02-28	"Standard System for Humanoid Robots and Embodied Intelligence (2026 Edition)" released	First top-level design of standards
2026-03	YD/T 6770-2026 embodied intelligence benchmark test method released	First industry standard in the field of embodied intelligence
2026-03	TC260 releases technical research report on the standardization of industrial embodied intelligence security	Special research on cyber security
2026-05-22	"Management Specification for the Full Life Cycle of Humanoid Robots" released (about 28,000 units certified)	Identity coding and full life cycle traceability
2026-08	GB/Z 220-2026 technical requirements for embodied intelligence data generation platforms released	Support for data security

4. Current Standard System and Gap Analysis

4.1. Inventory of Relevant Standards

Combining international and domestic contexts, the standards directly or indirectly related to the cyber security of mobile embodied intelligent agents can be divided into four categories: fundamentals and governance, cyber security and data, robot safety, and special standards for embodied intelligence, as shown in Tables 3 and 4.

4.2. Layered Applicability Analysis

From the perspective of applicability, the cyber security assurance provided by existing standards for mobile embodied intelligent agents presents the feature of "three layers with weakness at both ends": the foundation layer (general cyber security, data security, and AI algorithm security) is relatively mature and can be reused directly or after tailoring;

Table 3. Major relevant international standards

Category	Standard	Description
Cyber security and data	ISO/IEC 27400:2022, 27402:2023, 27701:2025	IoT security and privacy guidelines, device baseline, privacy information management
Robot safety	ISO 13482, ISO 10218-1/2:2025, ISO 22166-1:2021	Service/industrial robot safety, graded protection by communication transmission category
Industrial safety networks	IEC 62443, IEC 61508, ISO 13849, IEC 61784-3	Industrial control network security, functional safety, machinery safety, safe data communication
AI trustworthiness and governance	ISO/IEC 38507:2022, TR 24028:2020, IEEE P7007, NIST AI RMF	Governance framework, trustworthy AI, ethics and adversarial robustness
Regional regulation	EU Artificial Intelligence Act, US National AI Initiative	Risk-graded regulation, standard guidance

Table 4. Major relevant domestic standards and their formulation/revision status

Category	Standard / Document	Status
Top-level system	"Standard System for Humanoid Robots and Embodied Intelligence (2026 Edition)"	Published
Embodied intelligence industry standard	YD/T 6770-2026 benchmark test methods for embodied intelligence	Published
Embodied intelligence national standards	GB/Z 220-2026 data generation platform; GB/T 48317.3/4/5-2026 technical requirements for humanoid robots	Published / to be implemented
Embodied intelligence under development	General requirements for trustworthiness, technical requirements for large model systems, data quality specification, data training ground construction guidelines, intelligence grading	Under development / approval
Mobile robots	GB/T 45750-2025, GB/T 47494/47495-2026, GB/T 10827.4-2023, GB/T 30029-2023, GB/T 47864-2026	Published
AI security (including cyber security)	GB 45438-2025, GB/T 45654-2025, GB/T 42888-2023, GB/T 41871-2022	Published
Top-level system	"Standard System for Humanoid Robots and Embodied Intelligence (2026 Edition)"	Published

The body layer (service/industrial/mobile robot safety) mainly addresses physical and functional safety, and the cyber security clauses are mostly principled requirements[7][8]; the special layer (embodied intelligence), although accelerating, focuses mainly on "capability-type" standards such as perception, training and benchmarking, while highly specific clauses for the cyber security of mobile embodied intelligent agents remain blank. At the same time, the international graded protection approach for mobile scenarios (such as the transmission categories of ISO 10218-1:2025) is insufficiently connected with domestic standards, and the mapping relationship across standard families has not yet been established[8][19].

4.3. Standard Gaps

Based on a comprehensive judgment, there are five main gaps. First, the specificity gap: there is no national standard or industry standard specifically targeting "the cyber security of mobile embodied intelligent agents", and the embodied intelligence security standard system is still in the stage of soliciting comments[1]. Second, the communication security gap: there is no unified regulation on the protection requirements, threat grading and test methods for safety-related communication over open wireless channels (WiFi/BLE/5G). Third, the data security gap: the rules for desensitization, cross-border transmission and evidence preservation of the multimodal (vision, force, point cloud) data collected by mobile embodied intelligent agents at edge nodes are unclear[1]. Fourth, the algorithm trustworthiness gap: there is a lack of executable assessment specifications for prompt injection, adversarial examples, backdoor detection and explainability of large-model agents[1]. Fifth, the testing and enforcement gap: there is a lack of unified cyber security test benchmarks, evaluation indicators and mandatory certification, and most standards are recommended or association standards with limited binding force.

5. Landing Requirement Analysis

5.1. Technical Landing Requirements

At the technical level, "security by design" needs to be embedded in the full life cycle of mobile embodied intelligent agents: at the requirement stage, clarify identity authentication, encrypted communication, least privilege and a secure boot baseline; at the design stage, draw on the transmission category approach of ISO 10218-1:2025 to implement graded threat protection for open wireless channels (such as timestamp plus timeout, long sequence numbers, and end-to-end encryption)[8][19]; at the development stage, strengthen the security alignment and prompt injection protection of large-model agents and establish adversarial example and backdoor detection processes; at the verification stage, build scenario-based test benchmarks covering perception injection, communication hijacking, algorithm deception and execution loss of control, and incorporate real mobile/open environment evaluation.

5.2. Management and Compliance Landing Requirements

At the management level, a full-life-cycle cyber security management system that gives equal weight to functional safety needs to be established: connect graded protection compliance, data classification and grading, and personal information protection with the "one machine, one code" full-life-cycle management of mobile embodied intelligent agents[5]; implement security assessment and mandatory certification for high-risk scenarios such as passenger delivery, park inspection and household services; and, through explicit requirements in standards, promote enterprises to establish vulnerability reporting, emergency response and firmware upgrade mechanisms to shorten the window from vulnerability disclosure to remediation.

5.3. Industrial Ecosystem and Governance Landing Requirements

At the industrial and governance level, standards should serve as the bond to promote coordination: promote the Technical Committee for Standardization of Humanoid Robots and Embodied Intelligence of the Ministry of Industry and Information Technology, the National Cybersecurity Standardization Technical Committee and relevant industry standardization committees to launch projects collaboratively in the directions of "embodied intelligence security" and "agent security", so as to avoid duplication and blank spots[1][2]; accelerate the development of special standards for the cyber security of mobile embodied intelligent agents by referring to the international ISO/IEC graded protection approach; build an integrated public service platform for standard verification, testing and certification, and personnel training; and participate in international governance through standard mutual recognition to export the Chinese solution.

5.4. Mapping of Standard Gaps to Landing Requirements

Table 5. Mapping of standard gaps to landing requirements

Standard Gap	Landing Requirement	Recommended Priority
Specificity gap	Develop special standards for the cyber security of mobile embodied intelligent agents	Launch projects under the embodied intelligence security direction of the AI Security Standard System
Communication security gap	Graded protection and testing for open wireless channels	Draw on the transmission categories of ISO 10218-1:2025 to form domestic test methods
Data security gap	Rules for desensitization, cross-border transmission and evidence preservation of multimodal data	Formulate special national standards/guidelines on data security
Algorithm trustworthiness gap	Assessment specifications for prompt injection, adversarial examples and backdoors	Improve algorithm security assessment standards and extend them to large-model agents
Testing and enforcement gap	Unified test benchmarks, evaluation indicators and mandatory certification	Implement mandatory certification for high-risk scenarios and promote national/compulsory standard projects

Table 5 establishes the correspondence between the above gaps and landing requirements, providing a checklist-based basis for subsequent standard development and industrial promotion.

6. Recommendations

Based on the above analysis, four recommendations are put forward. (1) Accelerate the development of special standards for the cyber security of mobile embodied intelligent agents, and materialize the development directions of "agent security" and "embodied intelligence security" into concrete standard projects as soon as possible, giving priority to filling the gaps in open wireless communication, multimodal data and large-model agents. (2) Establish an integrated "functional safety + cyber security" standard framework, promote the mapping and connection with international standards such as ISO 10218 and IEC 62443, and form a mutually recognizable graded protection system. (3) Build a full-life-cycle security management and certification mechanism, connect "one machine, one code", vulnerability emergency response and mandatory certification, and first carry out pilot applications in high-risk scenarios such as passenger transport and parks. (4) Strengthen test and evaluation and public service supply, rely on cyber security test benchmarks and testing and certification platforms to reduce compliance costs for small and medium-sized enterprises, and simultaneously carry out personnel training and mutual recognition of international standards.

7. Conclusion

Mobile embodied intelligent agents are at the critical stage of transitioning from "technical verification" to "large-scale commercial application", and their mobility, openness, wireless dependence and physical execution attributes make cyber security a prerequisite for landing rather than an optional configuration. This paper systematically tracked the cyber security standardization process of mobile embodied intelligent agents at home and abroad: at the international level, a pattern of multiple standard families of "cyber security + robot safety + AI trustworthiness" has been formed; at the domestic level, centered on the Technical Committee for Standardization of Humanoid Robots and Embodied Intelligence of the Ministry of Industry and Information Technology and the National Cybersecurity Standardization Technical Committee, intensive arrangements have been made at the multiple levels of top-level systems, industry standards, association standards and national standards under development. However, existing standards still have five gaps in specificity, communication security, data security, algorithm trustworthiness and testing enforcement. In view of these gaps, the alignment of landing requirements should be promoted from the three levels of technology, management and industrial ecosystem, and efforts should be made to accelerate the development of special standards, the construction of an integrated framework, full-life-cycle management and the supply of test and evaluation, so as to support the safe, trustworthy and large-scale landing of mobile embodied intelligent agents by the power of standards. Subsequent research will carry out standard applicability evaluation and gap priority ranking in combination with specific scenarios.

References

- [1] National Cybersecurity Standardization Technical Committee. (2026). Technical research report on cybersecurity standardization — Research on the standardization of industrial embodied intelligence security (v1.0-202603). National Cybersecurity Standardization Technical Committee of China.
- [2] (n.d.). [Webpage content]. Retrieved October 19, 2026, from https://www.gov.cn/lianbo/202512/content_7052939.htm.

- [3] (n.d.). [Webpage content]. Retrieved October 19, 2026, from https://m.gmw.cn/2026-02/28/content_1304359382.htm.
- [4] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://miittc1.caict.ac.cn/newsDetail/?id=80&type=undefined>.
- [5] (n.d.). [Webpage content]. Retrieved October 19, 2026, from https://tech.gmw.cn/2026-05/27/content_38792078.htm.
- [6] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://std.samr.gov.cn/>.
- [7] International Organization for Standardization. (2014). Robotics — Safety requirements for service robots (ISO 13482:2014).
- [8] International Organization for Standardization. (2025). Robotics — Safety requirements — Part 1: Industrial robots (ISO 10218-1:2025).
- [9] International Organization for Standardization. (2021). Robotics — Modularity for service robots — Part 1: General requirements (ISO 22166-1:2021).
- [10] International Organization for Standardization / International Electrotechnical Commission. (2022). Cybersecurity — IoT security and privacy — Guidelines (ISO/IEC 27400:2022).
- [11] International Organization for Standardization / International Electrotechnical Commission. (2023). Cybersecurity — IoT security and privacy — Device baseline requirements (ISO/IEC 27402:2023).
- [12] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://www.iso.org/foresight/cyber-physical-systems.html>.
- [13] International Electrotechnical Commission. (2024). Industrial communication networks — Network and system security (IEC 62443).
- [14] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://finance.sina.com.cn/stock/relnews/cn/2026-06-23/doc-iniemfsn1884853.shtml>.
- [15] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://m.askci.com/news/chanye/20260805/143320278591159933441412.shtml>.
- [16] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <https://nvd.nist.gov/vuln/detail/cve-2025-41110>.
- [17] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <http://www.news.cn/digital/20251027/45af13caf8784e1a839b0c262a29784d/c.html>.
- [18] (n.d.). [Webpage content]. Retrieved October 19, 2026, from https://m.thepaper.cn/newsDetail_forward_33064137.
- [19] (n.d.). [Webpage content]. Retrieved October 19, 2026, from https://m.eeworld.com.cn/news_mp/ADI/a433172.aspx.
- [20] (n.d.). [Webpage content]. Retrieved October 19, 2026, from <http://www.jjckb.cn/20260531/70724c8a56c7440aaba95ecf81b5dfc4/c.html>.