DOI: 10.35598/mcfpga.2026.029

Reliability And Security Of EDGE Inference In Mobile Robot Control Systems: Model Degradation, Fallback Modes, And Real-Time Validation

Vladyslav Yevsieiev
ORCID 0000-0002-2590-7085
Department of Computer Integrated Technologies, Automation, Robotics and Safety Engineering
Kharkiv National University of Radio Electronics
Kharkiv,Ukraine
vladyslav.yevsieiev@nure.ua

Nikolaj Starodubcev
ORCID 0000-0001-7856-5771
Department of Computer Integrated Technologies, Automation, Robotics and Safety Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
nikolaj.starodubcev@nure.ua

Abstract — **The paper investigates the problem of ensuring the reliability and safety of EDGE inference in mobile robot control systems for Industry 5.0 applications in the context of neural model degradation, anomalous data, and limited computing resources. An analysis of modern mechanisms for validating inference results, detecting anomalies, and implementing fallback control modes was conducted, and their comparison was performed based on the criteria of reliability, safety, and suitability for use on EDGE platforms. The results obtained showed that the most effective approach is to combine mechanisms for controlling the reliability of inference, detecting anomalies, and multi-level safe control modes, which allows increasing the resilience of the robotic system to failures, prediction errors, and unknown situations. The proposed solutions can be used in the development of new-generation intelligent mobile robots for cyber-physical production systems of Industry 5.0.**

Keywords — Industry 5.0, EDGE inference, mobile robot, inference validation, anomaly detection, fallback control modes, reliability of robotic systems, safety of autonomous systems

I. Introduction

In modern autonomous control systems for mobile robots, the use of artificial intelligence algorithms and neural networks that run directly on EDGE platforms to ensure real-time operation is becoming increasingly widespread [1]. Along with the increase in the complexity of models, problems arise with the degradation of inference accuracy under the influence of environmental changes, limited computing resources, overloading of hardware modules, and the appearance of data different from those on which the neural network was trained [2]. In such conditions, mechanisms for validating inference results, timely detection of anomalies, and transition to safe fallback control modes that allow maintaining the operability of the robotic system even in the presence of prediction errors or partial failure of individual components become of particular importance [3]. Therefore, research into methods for ensuring the reliability and safety of EDGE inference is a relevant direction in the development of intelligent mobile robots for Industry 5.0, where the continuity of operation, the safety of interaction with a person and the guaranteed adoption of correct decisions in real time are of critical importance.

Let us analyze the latest publications within the framework of this study.

In the article, Nikolaos Filinis, Dimitrios Spatharakis and co-authors investigated the use of EDGE AI technologies for robotic applications within the computing continuum and analyzed the architectures of distributed data processing between robots, EDGE nodes and cloud services. The proposed approach allows to increase the efficiency of artificial intelligence algorithms, reduce data transmission delays and improve the autonomy of robotic systems by distributing computing tasks between different levels of infrastructure [4]. The use of this approach to ensure the reliability and safety of EDGE inference of mobile robots is limited due to the focus of the research mainly on the architecture of the computational continuum and resource allocation without a detailed consideration of the mechanisms of inference validation, model degradation, and the implementation of safe fallback control modes.

In their study, Hong-Wei Zhang, Yi-Min Qin, and co-authors reviewed ground-based mobile robots for high-throughput plant phenotyping based on a closed-loop "perception–decision–action" and analyzed modern sensor, navigation, and control technologies. The studied approach allows for increased accuracy of agricultural object monitoring, robot navigation efficiency, and the quality of automated decision-making in complex field conditions [5]. The presented solutions are focused mainly on applied aspects of agricultural robotics and do not consider the issues of assessing the reliability of inference results, detecting anomalies, controlling the degradation of neural models, and transitioning to safe modes of operation of the robotic system.

In their work, Arjun Ashok, Ritam Maiti, and Thomas Z. H. Ernest investigated an Edge-Intelligence mechanism with inference-oriented offloading of computations for delay-sensitive Internet of Things agents and proposed a method for optimal distribution of computational tasks between local and remote resources. The proposed approach allows to reduce inference execution delays, increase the efficiency of computing resources use, and improve the quality of service in IoT networks [6]. The practical application of this solution for mobile robot safety tasks is limited, since the main focus is on optimizing performance and computation delays without taking into account mechanisms for checking the reliability of inference results and fault-tolerant control. In their work, Farimah Pasandideh, Mohammad Azarafza, and Axel Rettberg investigated the impact of hardware failures on the performance of object detection systems on edge platforms by modeling various fault injection scenarios and analyzing the use of hardware resources during inference execution. The proposed approach allows to assess the stability of computer vision models to hardware failures, to identify critical components of the computing architecture and to predict the deterioration of the quality of object recognition [7]. Despite the direct connection with the issue of edge inference reliability, the study focuses mainly on the analysis of hardware errors and does not cover complex mechanisms for detecting anomalies, validating inference results and implementing multi-level fallback control modes for mobile robots. In the article, Hyun-Ho Choi and Kwangho Lee proposed a method for joint optimization of confidence thresholds for inference results and the distribution of computing resources in cooperative Mobile Edge Computing systems. The developed approach allows to simultaneously take into account the quality of neural network prediction and the availability of computing resources, which contributes to increasing the efficiency of inference and rational use of edge infrastructure [8]. The presented solution is promising for tasks of assessing the reliability of inference, but does not consider the issues of model degradation during operation, multi-level anomaly detection and automatic transition to safe control modes of mobile robots in critical situations.

The analysis of modern scientific publications indicates a significant interest of researchers in the issues of EDGE AI, distributed inference, mobile robotics and increasing the efficiency of the use of computing resources. [9-13] At the same time, most of the existing works focus on issues of productivity, optimization of calculations, navigation or resistance to certain types of hardware failures and do not consider the comprehensive provision of reliability and safety of EDGE inference in conditions of model degradation, the appearance of anomalous data and partial failures of components. This confirms the need and relevance of research aimed at developing integrated mechanisms for validating inference results, detecting anomalies and implementing multi-level fallback control modes for Industry 5.0 mobile robots. [14-17]

II. ANALYSIS OF THE VALIDATION MECHANISM OF EDGE INFERENCE RESULTS AND SAFE FALLBACK CONTROL MODES

We will analyze the validation mechanisms of EDGE inference results and safe fallback control modes from the point of view of comparing their advantages and disadvantages [18-20].

Confidence Monitoring – the mechanism is based on the analysis of the level of confidence of the neural network in the formed forecast and allows you to quickly detect potentially unreliable inference results. The main advantage of the approach is the simplicity of implementation and low computational costs, but it does not guarantee the detection of all errors, since the neural network can form an incorrect solution with a high level of confidence.

Output distribution entropy monitoring – this mechanism assesses the degree of uncertainty of the forecast by analyzing the entropy of the output probability distribution of the neural network. The advantage of the method is the ability to detect ambiguous situations during classification and detection of objects, but its effectiveness is significantly reduced for regression problems and complex multilevel models.

Bayesian Neural Networks – the approach uses a Bayesian representation of neural network parameters to obtain not only a forecast, but also an assessment of its reliability. The main advantage is the ability to quantify the uncertainty of inference results, but the implementation requires significant computing resources and is often difficult to use on EDGE platforms.

Monte Carlo Dropout – the mechanism performs multiple runs of the neural network with random disconnection of individual neurons to assess the stability of the forecast. The method allows you to obtain an approximate estimate of uncertainty without changing the model architecture, but increases the inference time and the load on the computing system.

Out-of-Distribution Detection (OOD) – the principle of operation is to detect input data that significantly differ from the training sample of the neural network. The advantage of the approach is to increase the safety of the mobile robot in unknown environments, while the disadvantage is the need for additional training and the complexity of setting the detection criteria.

Autoencoder-Based Anomaly Detection – the mechanism uses an autoencoder to reconstruct input data and identify anomalies based on the reconstruction error. The advantage is the effective detection of non-standard situations and corrupted sensor data, but its implementation requires separate model training and additional computing resources.

Statistical Residual Monitoring – this approach is based on comparing the predicted and actual values of system parameters with subsequent analysis of the residual error. The method is characterized by ease of implementation and suitability for low-power edge platforms, but is sensitive to noise and requires careful adjustment of threshold values.

Watchdog Monitoring – the mechanism monitors the performance of software and hardware modules by checking the execution time of processes and the regularity of their functioning. Its advantage is the effective detection of hangs and hardware failures, but it does not allow assessing the correctness of the results of the neural network.

Hardware Redundancy – the approach involves duplicating critical hardware components or computing modules to ensure system redundancy. The main advantage is high fault tolerance and operational safety, while the main disadvantage is an increase in the cost, energy consumption and complexity of the system.

Model Ensemble – the mechanism uses several independent neural networks to form a joint decision based on voting or averaging the results. The advantage is increased accuracy and reduced risk of errors of individual models, but the implementation requires significant computing resources and can be problematic for edge platforms.

Safe Rule-Based Supervisor – this approach involves checking the results of neural network inference using a set of predefined security rules and logical constraints. Its advantage is high explainability and the ability to guarantee safe system behavior, while the disadvantage is limited adaptability to new situations and the need to manually form a rule base.

Digital Twin Validation - the mechanism is based on comparing the solutions obtained by the neural network with the results of modeling the digital twin of the mobile robot and the environment. The advantage is the ability to predict potential errors even before executing control commands, however, the creation and maintenance of a digital twin require significant computing resources and high implementation complexity.

Safe Stop - fallback mode provides for an immediate safe stop of the mobile robot when a critical inference error or system failure is detected. The advantage is the maximum level of safety, but the execution of the current task is completely stopped.

Emergency Brake – the mechanism provides emergency braking in the event of a collision or loss of control over the robot's movement. The main advantage is the rapid prevention of emergency situations, while the disadvantage may be false alarms when the danger is incorrectly determined.

Rule-Based Navigation – in this mode, control is transferred to classical navigation algorithms that operate independently of the neural network. The advantage is the predictability of the robot's behavior and high reliability of operation, but the navigation efficiency may be lower compared to intelligent algorithms.

Fallback PID Controller – the mechanism involves disabling neural network algorithms and switching to a classical PID control circuit. Its advantage is stable operation and low requirements for computing resources, while the disadvantage is the loss of adaptability to complex dynamic environmental conditions.

Sensor Priority Switching – the principle of operation is to switch the system to backup sensors in the event of failure or degradation of the main data sources. The advantage is increased system fault tolerance, but the implementation requires the installation of additional sensors and complicates the robot architecture.

Human-in-the-Loop Control - the mechanism provides for the transfer of control to the operator in cases where the system cannot guarantee the correctness of the decision made. The advantage is maximum reliability of decision-making in critical situations, while the disadvantage is the dependence on the availability of the operator and the stability of the communication channel. [21-24]

For a better understanding, we present the existing mechanisms in the form of a comparative graph with a conditional expert assessment of the suitability of the mechanisms for the reliability and safety of EDGE inference in robotic systems in Figure 1.

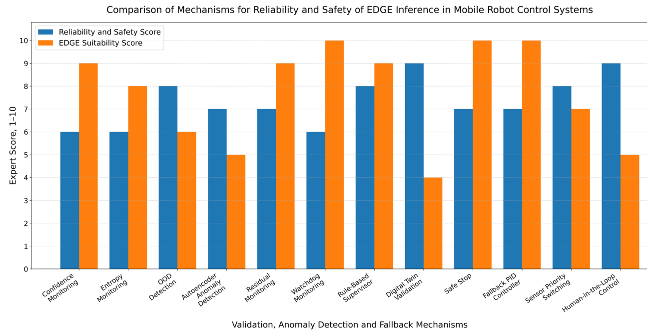

Figure 1 - Comparison of Mechanisms for Reliability and Safety of EDGE Inference in Mobile Robot Control Systems

The numerical analysis of the results presented in the graph "Comparison of Mechanisms for Reliability and Safety of EDGE Inference in Mobile Robot Control Systems" (Fig. 1) showed that the highest values of the reliability and safety indicator are the Digital Twin Validation and Human-in-the-Loop Control mechanisms, which received a score of 9 out of 10 possible, which indicates their high ability to detect inference errors and ensure the safe functioning of the mobile robot. At the same time, the highest scores for usability on EDGE platforms were received by Watchdog Monitoring, Safe Stop and Fallback PID Controller, which reached the maximum value of 10 points due to low requirements for computing resources and the ability to work in real time. The greatest imbalance between reliability and usability on EDGE platforms is observed for Digital Twin Validation and Human-in-the-Loop Control, where a high level of security is accompanied by relatively low implementation efficiency on limited hardware resources. Among the anomaly detection mechanisms, OOD Detection, Rule-Based Supervisor and Sensor Priority Switching were the most balanced, for which the reliability ratings are within 8 points, and the suitability ratings for use on EDGE platforms are from 6 to 9 points. [25,26]

Qualitative analysis of the results shows that (Fig. 1) the mechanisms for controlling model confidence and monitoring entropy are simple to implement on edge platforms, but do not provide a sufficient level of security guarantees when working in conditions of uncertainty. The Bayesian Neural Networks, Monte Carlo Dropout and Digital Twin Validation methods demonstrate high potential for assessing the reliability of inference results, but their use is limited by significant computational costs and increased requirements for hardware resources. The most practical for Industry 5.0 mobile robots are combined solutions that combine anomaly detection mechanisms, verification of inference results and automatic transition to safe control modes. Rule-Based Supervisor, OOD Detection, and Sensor Priority Switching attract particular attention, as they provide an acceptable balance between the level of security, implementation complexity, and the ability to work on modern EDGE platforms.

Conclusion

The results obtained confirm that the use of only one mechanism does not allow to simultaneously ensure the maximum level of reliability, safety and efficiency of work on edge platforms. For mobile robot control systems, the most appropriate is a comprehensive approach that combines mechanisms for controlling the reliability of inference, anomaly detection and multi-level fallback control modes. Such an architecture allows to increase the resistance of the robotic system to the degradation of neural models, failures of individual components and the emergence of unknown situations, ensuring the safe functioning of mobile robots in Industry 5.0 environments.

REFERENCES

[1] Saha, S., & Xu, L. (2025). Vision transformers on the edge: A comprehensive survey of model compression and acceleration strategies. Neurocomputing, 643, 130417. https://doi.org/10.1016/j.neucom.2025.130417

[2] Ngo, D., Park, H. C., & Kang, B. (2025). Edge intelligence: A review of deep neural network inference in resource-limited environments. Electronics, 14(12), 2495. https://doi.org/10.3390/electronics14122495

[3] Hybrid Approaches to Building Intelligent Robotic Systems on FPGAs and MCUs for Industry 5.0 Tasks / V. Yevsieiev, S. Maksymova, N. Demska, N. Starodubcev // Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA-2025) : VII International Scientific and Practical Conference, June 27-28, 2025. – Kharkiv : NURE – P.30-35.

[4] Filinis, N., Spatharakis, D., Dimolitsas, I., Kapoor, G., Fu, L., Toffetti, G., ... & Papavassiliou, S. (2026). Edge ai-driven robotic applications in the computing continuum. IEEE Internet of Things Magazine. https://doi.org/10.1109/MIOT.2026.3655981

[5] Zhang, H. W., Qin, Y. M., Wu, A. Q., Xi, X., Hu, P., & Wang, R. F. (2026). Ground Mobile Robots for High-Throughput Plant Phenotyping: A Review from the Closed-Loop Perspective of Perception, Decision, and Action. Plants, 15(8), 1218. https://doi.org/10.3390/plants15081218

[6] Ashok, A., Maiti, R., Ernest, T. Z. H., & Madhukumar, A. S. (2026). Edge-Intelligence With Inference-Aware Offloading for Latency-Sensitive Agents in IoT Networks. IEEE Communications Letters, 30, 837-841. https://doi.org/10.1109/LCOMM.2026.3651860

[7] Pasandideh, F., Azarafza, M., & Rettberg, A. (2026). Hardware Utilization and Inference Performance of Edge Object Detection Under Fault Injection. arXiv preprint arXiv:2604.09631. https://doi.org/10.48550/arXiv.2604.09631

[8] Choi, H. H., & Lee, K. (2026). Joint Optimization of Confidence Thresholds and Resource Allocation for Cooperative Inference in Mobile Edge Computing Systems. IEEE Transactions on Vehicular Technology. https://doi.org/10.1109/TVT.2025.3650751

[9] Kadve, G., Chowdhury, A., Singh, V. K., & Pal, A. (2025). Engineering a multi model fallback system for edge devices. Results in Engineering, 26, 105165. https://doi.org/10.1016/j.rineng.2025.105165

[10] Wang, L., Li, L., Xu, L., Peng, X., & Fei, A. (2024). Failure-resilient distributed inference with model compression over heterogeneous edge devices. arXiv preprint arXiv:2406.14185. https://doi.org/10.48550/arXiv.2406.14185

[11] Vermesan, O., Pagani, A., Bahr, R., Coppola, M. A., & Urlini, G. (2026). Edge AI Systems Verification and Validation. In Charting the Intelligence Frontiers–Edge AI Systems Nexus (pp. 1-52). River Publishers.

[12] Rodríguez-Arozamena, M., Matute, J., Araluce, J., Rastelli, J. P., & Zubizarreta, A. (2025). Fault Tolerance and Fallback Strategies in Connected and Automated Vehicles: A Review. IEEE Open Journal of Intelligent Transportation Systems. https://doi.org/10.1109/OJITS.2025.3583787

[13] Yevsieiev, V., & Holod, I. (2026). HARDWARE-SOFTWARE MODULE FOR INTELLIGENT MICROCLIMATE CONTROL IN INDUSTRIAL FACILITIES. Scientific Papers of Donetsk National Technical University. Series: "Computer Engineering and Automation", 4(6(38), 7–17. https://doi.org/10.32782/2786-9024/v4i6(38).359113

[14] Development of a program for modeling and simulating a collaborative robot workspace / Igor Nevliudov, Vladyslav Yevsieiev, Svitlana Maksymova, Olena Chala, Dmytro Gurin // Computer Systems of Design. Theory and Practice. — Lviv : Lviv Politechnic Publishing House, 2024. — Vol 6. — No 3. — P. 31–40.

[15] Yevsieiev, V., Gurin, D., Kulish, S., & Voloshyn, Y. (2025). Development of a partially supervised Markov decision-making model for a 3-link collaborative robot-manipulator. Radioelectronic and Computer Systems, 2025(4), 83-94. doi:https://doi.org/10.32620/reks.2025.4.06

[16] Yevsieiev V., Holod I. Development of a Self-Learning and Adaptation Algorithm for Microclimate Control System Using Sensor Networks // In Proceedings of the 7th International Scientific and Practical Conference «Innovative Development in the Global Science», May 26-28, 2026. Boston: Independently Published, 2026. P.152-157. https://doi.org/10.51582/interconf.2026.296

[17] Yevsieiev V., Holod I. Prospects for the Implementation of Cyber-Physical System for Monitoring and Control of Microclimate in the Context of Industry 4.0 // The Proceedings of the 16th International Scientific and Practical Conference "Challenges in Science of Nowadays", April 26-28. 2026. Washington, USA. P. 254-260. https://doi.org/10.51582/interconf.2026.292

[18] Yevsieiev V. Digital Twins of Collaborative Robotic Systems for Decision Support in Emergency Situations / V. Yevsieiev, S. Svetlana // Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations (ICSTRO-2026) : Proceedings of I-st All-Ukrainian Conference, February 12-23, 2026. – Kharkiv, 2026. - P. 153-156

[19] Abu-Jassar, A., Attar, H., Hafez, M., Hamdan, M., Yevsieiev, V., & Lyashenko, V. (2025, December). Adaptive System for Constructing a Mobile Robot Trajectory Using Neural Network and Stochastic Optimizer. In 2025 26th International Arab Conference on Information Technology (ACIT) (pp. 422-428). IEEE. https://doi.org/10.1109/ACIT68900.2025.11510567

[20] Nevliudov I., Yevsieiev V., Horovyi K. Model of the Technological Process of Wedge Bonding Based on FEK Delvotec 6400 in the Production of Hybrid Electronic Modules // In Proceedings of the XII International Scientific and Theoretical Conference, June 12, 2026. Chicago, USA: International Center of Scientific Research. P. 170-173. https://doi.org/10.36074/scientia-12.06.2026

[21] Nevliudov I., Yevsieiev V., Horovyi K. Analysis of the Technological Process of Wedge Bonding Using FEK Delvotec 6400 in Microelectronics // Current scientific goals, approaches and challenges: Collection of Scientific Papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, June 5, 2026. Dresden, Federal Republic of Germany: International Center of Scientific Research. P. 117-119. https://doi.org/10.36074/scientia-05.06.2026

[22] Nevliudov I., Yevsieiev V., Horovyi K. Analysis of the FEK Delvotec 6400 Wedge Bonding System // Débats scientifiques et orientations prospectives du développement scientifique: c avec des matériaux de la X conférence scientifique et pratique internationale, Paris, 5 juin 2026. P. 89-92. https://doi.org/10.36074/logos-05.06.2026

[23] Ngo, D., Park, H. C., & Kang, B. (2025). Edge intelligence: A review of deep neural network inference in resource-limited environments. Electronics, 14(12), 2495. https://doi.org/10.3390/electronics14122495

[24] Zhang, F., Zhang, C., Guan, J., Zhou, Q., Chen, K., Zhang, X., ... & Du, X. (2025). Breaking the edge: Enabling efficient neural network inference on integrated edge devices. IEEE Transactions on Cloud Computing. https://doi.org/10.1109/TCC.2025.3559346

[25] Xiang, M., Fernando, R., & Wang, B. (2025). On-device Qwen2. 5: Efficient LLM inference with model compression and hardware acceleration. arXiv preprint arXiv:2504.17376. https://doi.org/10.48550/arXiv.2504.17376

[26] Zhang, K., Fan, Z., Liu, Y., Wang, L., Liu, Y., Wu, H., ... & Li, W. (2026). HALO: A heterogeneous accelerator for low-latency and energy-efficient edge LLM inference. Future Generation Computer Systems, 185, 108646. https://doi.org/10.1016/j.future.2026.108646