

Research on Precision Detection and Intelligent Early Warning of Medical Devices: Current Status, Practical Challenges, and Development Pathways

Wang Jiaqi*, Ye Keing, Qiu Yingting, Zhu Qianying, Zeng Lincong, Chen Jiaqi, Li Tian

Zhuhai City Polytechnic, Zhuhai Guangdong, China, 519000

*corresponding author: 2529943837@qq.com.

Abstract: *With the increasing intelligence, connectivity, and complexity of medical devices, conventional periodic inspection and reactive maintenance methods can no longer fully meet the requirements of clinical safety and lifecycle risk management. Precision detection and intelligent early warning integrate multisource sensing, condition monitoring, fault diagnosis, artificial intelligence, and risk prediction to identify device abnormalities and potential safety hazards at an early stage. Using literature review, comparative analysis, and inductive synthesis, this paper examines the core concepts, technical logic, current applications, practical challenges, and development pathways of precision detection and intelligent early warning for medical devices. It reviews representative applications in manufacturing quality inspection, clinical operation monitoring, fault diagnosis, predictive maintenance, and post-market surveillance, and compares rule-based methods, machine learning, deep learning, data fusion, and digital-twin technologies. The analysis shows that intelligent technologies can improve fault-identification accuracy, detect complex degradation patterns, and support proactive risk intervention. However, their practical application remains constrained by insufficient high-quality fault data, inconsistent data standards, limited model generalizability and interpretability, false alarms, inadequate system interoperability, cybersecurity risks, and incomplete regulatory frameworks. Accordingly, this paper proposes establishing standardized medical device data systems, developing trustworthy and generalizable artificial intelligence models, constructing lifecycle-oriented monitoring mechanisms, optimizing risk-graded warning and human–AI collaboration, and improving technical standards and regulatory systems. These pathways may facilitate the transition of medical device safety management from periodic inspection and corrective maintenance toward continuous monitoring, predictive maintenance, and proactive risk governance.*

Keywords: Medical devices; precision detection; intelligent early warning; artificial intelligence; condition monitoring; risk assessment; medical device safety

1. Research Introduction

Advances in artificial intelligence, the Internet of Medical Things, multisource sensing, and digital twins have increased the connectivity, autonomy, and functional complexity of medical devices^{[1][2][3]}. Diagnostic imaging systems, life-support equipment, infusion systems, surgical robots, implantable devices, and wearable monitors now support a wide range of clinical activities. This growing technical complexity also creates safety risks associated with component degradation, calibration drift, sensor failure, software faults, communication interruptions, and abnormal operating states. Medical device management has traditionally relied on scheduled inspections, preventive maintenance, fixed alarm thresholds, and corrective action after failure^[4]. Although these measures remain necessary, they may fail to detect early

degradation or predict device-related risks under changing clinical conditions. Medical device safety management is therefore moving from periodic inspection and fault correction toward continuous monitoring, risk prediction, and early intervention.

Precision detection and intelligent early warning support this transition. In this review, precision detection refers to the accurate identification and quantitative assessment of device states, performance deviations, component faults, and potential safety hazards through multisource data collection and computational analysis. Intelligent early warning refers to estimating the probability, severity, and possible consequences of device failure and issuing graded alerts before an adverse event occurs. By combining condition monitoring, machine learning, deep learning, digital twins, and risk assessment, these systems can identify complex fault patterns, estimate degradation trends, and inform maintenance decisions^{[2][3][4][5]}. This approach also supports lifecycle-based device governance by linking premarket evaluation, clinical operation, maintenance, and post-market surveillance^[6].

Previous studies have examined fault detection, operating-state monitoring, predictive maintenance, and adverse-event analysis for medical devices. However, many studies address a single device category, one analytical method, or a specific lifecycle stage. Research that links precision detection, fault diagnosis, risk prediction, and early warning within a unified framework remains limited. Practical adoption is also restricted by scarce fault data, inconsistent data and evaluation standards, weak model transferability and interpretability, excessive false alarms, cybersecurity threats, and incomplete regulatory provisions.

This review uses literature analysis, comparative analysis, and inductive synthesis to examine the concepts, technical processes, current applications, practical constraints, and development paths associated with precision detection and intelligent early warning. The discussion proceeds from conceptual foundations and application status to method comparison, implementation barriers, and proposed responses. The review aims to provide an analytical basis for medical device condition monitoring, predictive maintenance, and lifecycle safety management.

2. Core Concepts, Technical Logic, and Research Status

2.1 Core Concepts and Characteristics

Medical device precision detection refers to the accurate identification, measurement, and evaluation of a device's operating condition, performance deviation, component fault, and potential safety risk. Its purpose is to determine whether a device functions within specified technical and clinical limits. Detection data may include electrical parameters, mechanical vibration, temperature, pressure, flow rate, acoustic signals, medical images, software logs, environmental conditions, and maintenance records. After data collection, signal processing, feature extraction, pattern recognition, and state assessment are used to identify abnormal changes. Unlike conventional inspection, which often depends on scheduled testing and fixed thresholds, precision detection can combine multiple data sources to detect small deviations and complex fault patterns.

Intelligent early warning refers to the use of monitoring data and computational models to estimate the probability, severity, and possible consequences of a future device failure. It extends device assessment from identifying current abnormalities to predicting risk before failure occurs. A typical early-warning process includes condition monitoring, anomaly detection, fault diagnosis, risk estimation, warning classification, and response recommendation. According to the predicted risk level, the system may recommend continued observation, calibration, preventive maintenance, component replacement, restricted operation, or device shutdown. Intelligent early warning therefore connects technical detection results with equipment-management and clinical-safety decisions^{[1][5]}.

Precision detection and intelligent early warning are related but perform different functions. Precision detection

answers whether a device is currently operating normally and identifies the location and degree of any deviation. Intelligent early warning assesses how the detected condition may develop and when intervention may be required. Detection supplies the data and evidence for prediction, while early warning converts analytical results into risk information and recommended actions. Their integration forms a continuous process involving data acquisition, state recognition, risk prediction, warning generation, and management response.

These systems have four main characteristics. First, accuracy requires reliable measurement, low rates of missed detection and false alarms, and consistent identification of weak or early fault signals. Second, real-time capability requires the timely collection and analysis of device data so that abnormal conditions can be recognized without delaying clinical work. Third, predictability enables the estimation of degradation trends, failure probability, and remaining useful life rather than limiting analysis to current faults. Fourth, lifecycle management extends monitoring from manufacturing and premarket testing to clinical operation, maintenance, post-market surveillance, and device retirement. Together, these characteristics support a shift from scheduled inspection and corrective maintenance to continuous assessment and risk-based intervention.

2.2 Technical Logic of Precision Detection and Intelligent Early Warning

Precision detection and intelligent early warning form a progressive process from data acquisition to safety intervention. Medical devices continuously generate operational parameters, sensor signals, software logs, alarm records, and maintenance information. After preprocessing and quality control, these data are used to identify performance deviations, abnormal states, and component degradation. Fault-diagnosis models then determine the possible type, location, and cause of an abnormality, while predictive models estimate its development trend, failure probability, and possible consequences.

Based on these results, the system assigns risk levels according to fault severity, clinical function, patient exposure, and intervention urgency^[6]. Each warning level corresponds to a defined response, such as continued observation, calibration, preventive maintenance, component replacement, or suspension of device use. Maintenance outcomes and operational feedback are returned to the detection system to adjust thresholds and evaluate model performance. This process connects condition monitoring, fault analysis, warning generation, and management decisions, thereby supporting continuous medical device safety control.

2.3 Current Research and Applications

Research on medical device detection and early warning has expanded across the United States, Europe, Japan, South Korea, and China. Studies in the United States place greater emphasis on lifecycle monitoring, adverse-event reporting, software performance, and data-based post-market surveillance. European research commonly connects device risk assessment with quality management, clinical evaluation, and regulatory compliance. Japan and South Korea have applied sensing, automated inspection, and predictive maintenance to precision manufacturing and hospital equipment management. Research in China has developed rapidly in equipment fault diagnosis, operating-state monitoring, intelligent maintenance, and medical device data platforms. However, differences in technical standards, data availability, and regulatory systems limit the direct transfer of methods across countries and institutions.

Current applications cover several stages of the medical device lifecycle. During manufacturing, machine vision, signal analysis, and automated testing are used to detect surface defects, assembly errors, dimensional deviations, and performance instability. During clinical operation, embedded sensors and software logs support continuous monitoring of electrical, mechanical, thermal, and communication states^{[1][2]}. Fault-diagnosis models identify abnormal components and probable failure causes, while predictive models estimate degradation trends and maintenance requirements^{[4][5]}.

Post-market surveillance further uses adverse-event reports, repair records, and operational data to identify recurring faults and emerging safety signals^{[6][7]}. Despite this progress, many applications remain limited to individual device types or controlled settings, and evidence from multicentre clinical deployment is still insufficient^{[7][8]}.

3. Multidimensional Comparative Analysis

To clarify the technical changes introduced by artificial intelligence and identify suitable methods for different medical device scenarios, this section compares traditional detection with AI-enabled detection and examines five major early-warning technologies. The comparison considers data sources, detection accuracy, real-time performance, predictive capacity, interpretability, technical limitations, and application scope.

3.1 Comparison between Traditional Teaching Teams and New AI Empowered Teaching Teams

Traditional detection mainly relies on scheduled inspection, preset thresholds, and expert-defined rules^[4]. It is suitable for known faults with clear technical limits but has limited capacity to identify weak, nonlinear, or combined fault patterns. AI-enabled detection analyses historical and real-time data to learn device-state changes and estimate future risks^{[2][5]}. The main differences are shown in Table 1.

Table 1. Comparison between traditional and AI-enabled medical device detection

Comparison dimension	Traditional detection	AI-enabled detection
Data sources	Uses individual measurements, inspection records, and predefined technical parameters	Combines sensor signals, software logs, images, environmental data, and maintenance records
Detection accuracy	Performs well when fault thresholds and mechanisms are clearly defined; may miss weak or complex abnormalities	Can identify nonlinear and multivariable patterns, but performance depends on data quality and model validation
Fault-prediction capability	Mainly detects existing faults and provides limited prediction of degradation	Estimates failure probability, degradation trends, and remaining useful life
Interpretability	Rules and thresholds are generally clear and easy to trace	Complex models may provide limited explanations for their outputs
Application scope	Commonly used for standardized testing and known fault types	Applicable to manufacturing inspection, clinical monitoring, predictive maintenance, and post-market surveillance

3.2 Comparison of Major Intelligent Early-Warning Technologies

Intelligent early-warning methods differ in their data requirements, analytical capacity, explainability, and deployment cost^{[5][7][9]}. No single method is suitable for all medical devices or risk scenarios. Selection should consider device complexity, fault characteristics, available data, computing resources, and safety requirements. The main differences are presented in Table 2.

Table 2. Comparison of major intelligent early-warning technologies

Technology	Basic principle	Main advantages	Main limitations	Suitable applications
Rule- and threshold-based methods	Compare measured values with preset limits or expert-defined rules	Simple, transparent, and easy to implement	Limited ability to detect unknown or combined faults; sensitive to threshold selection	Standardized testing and devices with clear safety limits
Conventional machine learning	Learn fault patterns from manually selected features	Effective with moderate datasets and lower computing requirements	Depends on feature engineering and labelled samples	Equipment classification, anomaly detection, and fault diagnosis
Deep learning	Automatically extracts features from signals, images, or time-series data	Detects nonlinear relationships and complex degradation patterns	Requires substantial data and computing resources; explanations may be limited	Imaging equipment, waveform monitoring, and predictive maintenance
Digital-twin-based methods	Link a virtual device model with real operating data	Supports simulation, condition estimation, and failure prediction	Requires accurate physical models and continuous data exchange	Complex equipment and lifecycle condition management
Multimodal and foundation-model-based methods	Combine signals, images, logs, text, and prior knowledge	Processes heterogeneous data and supports cross-task analysis	High computing cost, uncertain transferability, and limited validation in clinical settings	Integrated monitoring, maintenance support, and post-market surveillance

Rule-based methods remain suitable for clear and stable risk boundaries, whereas data-driven methods are better suited to faults involving multiple variables. Digital twins add physical constraints and simulation capacity, while multimodal models combine different forms of device information^{[3][11]}. In practice, hybrid systems may provide more

reliable warnings by combining explicit safety rules with learned patterns and engineering knowledge.

4. Practical Challenges and Their Causes

4.1 Insufficient and Fragmented Device Data

The development of precision detection and early-warning systems depends on sufficient, accurate, and representative device data. However, real fault samples are difficult to obtain because medical device failures occur infrequently, while deliberate failure testing may involve high costs and safety restrictions. Available datasets therefore contain large amounts of normal operating data but relatively few examples of degradation, malfunction, or adverse events. This class imbalance can cause models to favour normal conditions and miss rare but serious faults^{[7][8]}.

Device data are also distributed across manufacturers, healthcare institutions, maintenance providers, and regulatory systems. Differences in device models, sensor configurations, data formats, sampling frequencies, fault definitions, and annotation methods make data integration difficult. Maintenance records and adverse-event reports may contain incomplete descriptions or inconsistent terminology, which further reduces their analytical value. Data sharing is restricted by commercial confidentiality, patient privacy, cybersecurity requirements, and unclear ownership. As a result, many studies rely on small, single-device, or single-institution datasets, limiting model training, independent validation, and transfer across clinical settings.

4.2 Limited Model Reliability and Generalizability

AI models for medical device detection are often trained using data from a limited number of device models or healthcare institutions. Differences in hardware configuration, sensor accuracy, software version, operating environment, maintenance history, and clinical workflow can change data distributions. A model that performs well in its original setting may therefore produce lower accuracy when applied to another device type or institution. Limited external validation makes it difficult to determine whether reported results can be reproduced under routine clinical conditions.

Model interpretability presents an additional concern. Complex learning models may identify abnormal patterns without explaining the relevant variables, fault mechanisms, or reasons for a warning^[9]. This limits the ability of clinicians and biomedical engineers to verify predictions and select appropriate responses. Model performance may also decline over time as devices age, software is updated, and operating practices change^[8]. Without continuous monitoring, such model drift may remain undetected. In addition, many systems provide risk scores without estimating predictive uncertainty. This can result in excessive confidence, inappropriate maintenance decisions, or delayed intervention when the available data are incomplete or differ from the training data.

4.3 Weak Integration with Clinical and Maintenance Workflows

Many intelligent detection systems produce anomaly scores or fault classifications without linking them to specific clinical or maintenance actions. Poor compatibility with hospital information systems and equipment-management platforms further limits their use in routine practice.

High false-alarm rates may interrupt clinical work, increase staff workload, and cause alarm fatigue^[10]. This problem often arises when warning thresholds do not consider device type, clinical context, or risk severity. Moreover, limited participation by clinicians and biomedical engineers in model development and evaluation may result in warning rules that do not match actual workflows. Effective application requires clear links between model outputs, risk levels, responsible personnel, and response procedures.

4.4 Inadequate Standards and Regulatory Mechanisms

Unified standards for evaluating medical device detection and early-warning systems remain insufficient. Existing rhythms differ in data quality, performance metrics, test conditions, and risk thresholds, which makes results difficult to compare across devices and institutions. Validation requirements for adaptive AI models are also unclear because model performance may change after software updates or exposure to new data^[6]^[8].

Privacy and cybersecurity create additional concerns when systems collect, transmit, and store device or patient-related information. Responsibility may also be difficult to assign when an incorrect warning results from data errors, algorithm failure, device malfunction, or human response. Clear standards are therefore needed for model validation, data protection, software updates, system auditing, and responsibility allocation.

4.5 Insufficient Resource and Organizational Support

The deployment of precision detection and intelligent early-warning systems requires sensors, data platforms, computing equipment, software integration, system validation, and continuing maintenance. These requirements create considerable costs, particularly for smaller healthcare institutions with limited technical staff and ageing equipment. Differences among device brands and hospital systems further increase the cost of interface development and data integration.

Implementation also depends on personnel who understand medical devices, clinical practice, biomedical engineering, data analysis, and regulatory requirements. Such professionals remain limited, and existing teams often work within separate departments. Coordination among hospitals, manufacturers, maintenance providers, research institutions, and regulators is also insufficient. Unclear responsibilities and restricted data exchange delay Rutgers slow system development, validation, and adoption. Long-term operation therefore requires stable funding, interdisciplinary teams, defined responsibilities, and formal cooperation mechanisms.

5. Development Pathways

5.1 Establish Standardized Medical Device Data Systems

A standardized data system should define common requirements for data acquisition, storage, annotation, exchange, and quality control. Unified fault-classification standards should specify fault types, severity levels, device states, operating conditions, and maintenance outcomes^[6]. Consistent terminology and data formats would improve the comparability of research results and support model transfer across devices and institutions.

Multicentre and multi-device databases should include normal operation, performance degradation, component failure, maintenance, and adverse-event data. Data should represent different manufacturers, device models, clinical settings, and stages of service life. Hospitals, manufacturers, testing institutions, and research organizations should establish clear procedures for data access and use. Privacy-protection measures should include data minimization, de-identification, access control, encrypted transmission, and audit records. Federated analysis may also support collaborative model development when direct data exchange is restricted. These measures can improve data availability while protecting patient information and commercial interests.

5.2 Develop Trustworthy and Generalizable AI Models

AI models should maintain stable performance across device types, manufacturers, institutions, and operating environments. Transfer learning and domain adaptation can reduce the effect of differences in sensor configuration, data distribution, and clinical workflow. Training/truncate should include data from varied devices and settings, while external validation should assess performance beyond the original development dataset.

Model outputs should include understandable evidence, such as relevant signals, detected abnormalities, and factors affecting risk estimates. Uncertainty estimation should indicate when a prediction lacks sufficient confidence and requires manual review^{[7][9]}. Continuous monitoring is also needed to identify performance decline caused by device ageing, software updates, or changes in clinical use. Model updates should follow documented procedures for data review, testing, approval, and version control. These measures can improve reliability while maintaining traceability and human supervision.

5.3 Integrate Detection with Device Lifecycle Management

Precision detection should cover the full medical device lifecycle rather than operate as an isolated maintenance function^{[4][6]}. Manufacturing inspection data can provide baseline information on component quality and initial performance. Clinical monitoring can then record operating conditions, workload, alarms, and performance changes, while maintenance records document faults, repairs, calibration, and component replacement. Post-market surveillance can combine these data to identify recurring defects and wider safety signals.

Each device should have a longitudinal health record containing its manufacturing information, installation status, operating history, inspection results, maintenance activities, and risk assessments. Continuous records can support degradation analysis and help determine appropriate maintenance intervals. Predictive maintenance should use actual device condition and estimated failure risk instead of relying only on fixed schedules. This approach supports earlier intervention, reduces unnecessary servicing, and improves the allocation of maintenance resources.

5.4 Improve Risk-Graded Warning and Human–AI Collaboration

Early-warning systems should classify risks according to failure probability, fault severity, clinical function, patient exposure, and urgency of response. Hierarchical thresholds can distinguish minor deviations from conditions requiring immediate action. Thresholds should be adjusted for different device categories and clinical settings because the same technical abnormality may produce different consequences.

Each warning level should correspond to a defined response procedure, responsible person, and completion time. Possible actions include continued observation, repeated testing, calibration, maintenance, component replacement, restricted operation, or device suspension. Warning messages should explain the detected abnormality, supporting evidence, estimated risk, and recommended action. Clinicians and biomedical engineers should review high-risk decisions, particularly when device shutdown or treatment interruption may affect patients^{[2][7]}. Human oversight also allows users to correct unsuitable recommendations and provide feedback for later system evaluation.

5.5 Strengthen Standards, Regulation, and Collaborative Support

Unified evaluation systems should specify requirements for data quality, detection accuracy, false-alarm rates, response time, model transferability, uncertainty reporting, and clinical applicability. Testing should include internal validation, external validation, simulated fault conditions, and assessment under actual operating conditions. Evaluation results and model versions should be documented to support review and accountability.

Regulatory provisions should address adaptive algorithms, software updates, data governance, cybersecurity, and post-deployment monitoring. Security controls should cover device access, data transmission, identity management, vulnerability reporting, and recovery procedures. Responsibilities among developers, manufacturers, healthcare institutions, and users should also be defined. Hospitals can provide clinical and operational data, manufacturers can supply device knowledge, universities can develop and evaluate methods, and regulators can establish assessment requirements. Regular cooperation among these groups can support data sharing, independent testing, professional training, and the controlled use of early-warning systems.

6. Conclusion and Prospect

6.1 Research Conclusion

Precision detection and intelligent early warning are changing medical device management from periodic inspection and fault correction toward continuous monitoring, predictive assessment, and early intervention. Current applications include manufacturing quality inspection, clinical condition monitoring, fault diagnosis, predictive maintenance, and post-market surveillance. Machine learning, deep learning, multisource data fusion, and digital twins have improved the detection of abnormal states and the prediction of degradation trends. However, practical implementation remains restricted by scarce fault data, inconsistent data formats, class imbalance, limited model transferability and interpretability, false alarms, weak system integration, and incomplete regulatory provisions. To address these problems, this review proposes five development paths: establishing standardized data systems, developing reliable and transferable models, connecting detection with lifecycle management, improving risk-graded warnings and human–AI cooperation, and strengthening evaluation standards, regulation, cybersecurity, and organizational support. These measures can support safer device operation and more efficient maintenance decisions.

6.2 Future Prospects

Future research is expected to advance in five directions. First, multimodal intelligent detection will combine sensor signals, images, software logs, maintenance records, and clinical information to provide a more complete assessment of device condition. Second, digital twins will link physical devices with virtual models to simulate degradation, estimate remaining useful life, and evaluate maintenance options. Third, foundation models may support cross-device learning, fault-text analysis, maintenance assistance, and knowledge transfer when labelled data are limited^[11]. Fourth, explainable and trustworthy artificial intelligence will receive greater attention. Future systems will need to report prediction evidence, model uncertainty, performance changes, and conditions under which human review is required. Fifth, medical device risk management will move toward a closed process that connects monitoring, diagnosis, prediction, warning, intervention, and feedback. Progress in these areas will depend on coordinated work in data governance, engineering validation, clinical assessment, human factors, cybersecurity, and regulatory supervision.

References:

- [1] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.
- [2] E. J. Topol, "High-performance medicine: The convergence of human and artificial intelligence," *Nature Medicine*, vol. 25, pp. 44–56, 2019, doi: 10.1038/s41591-018-0300-7.
- [3] J. Corral-Acero et al., "The 'digital twin' to enable the vision of precision cardiology," *European Heart Journal*, vol. 41, no. 48, pp. 4556–4564, 2020, doi: 10.1093/eurheartj/ehaa159.
- [4] M. Sezdi, "Two different maintenance strategies in the hospital environment: Preventive maintenance for older technology devices and predictive maintenance for newer high-tech devices," *Journal of Healthcare Engineering*, vol. 2016, Art. no. 7267983, 2016, doi: 10.1155/2016/7267983.

- [5] Y. Lei, N. Li, L. Guo, N. Li, T. Yan, and J. Lin, "Machinery health prognostics: A systematic review from data acquisition to remaining useful life prediction," *Mechanical Systems and Signal Processing*, vol. 104, pp. 799–834, 2018, doi: 10.1016/j.ymssp.2017.11.016.
- [6] International Organization for Standardization, *ISO 14971:2019—Medical Devices: Application of Risk Management to Medical Devices*. Geneva, Switzerland: ISO, 2019. Available: <https://www.iso.org/standard/72704.html>.
- [7] C. J. Kelly, A. Karthikesalingam, M. Suleyman, G. Corrado, and D. King, "Key challenges for delivering clinical impact with artificial intelligence," *BMC Medicine*, vol. 17, Art. no. 195, 2019, doi: 10.1186/s12916-019-1426-2.
- [8] S. G. Finlayson et al., "The clinician and dataset shift in artificial intelligence," *New England Journal of Medicine*, vol. 385, no. 3, pp. 283–286, 2021, doi: 10.1056/NEJMc2104626.
- [9] M. Ghassemi, L. Oakden-Rayner, and A. L. Beam, "The false hope of current approaches to explainable artificial intelligence in health care," *The Lancet Digital Health*, vol. 3, no. 11, pp. e745–e750, 2021, doi: 10.1016/S2589-7500(21)00208-9.
- [10] M. Cvach, "Monitor alarm fatigue: An integrative review," *Biomedical Instrumentation & Technology*, vol. 46, no. 4, pp. 268–277, 2012, doi: 10.2345/0899-8205-46.4.268.
- [11] M. Moor et al., "Foundation models for generalist medical artificial intelligence," *Nature*, vol. 616, pp. 259–265, 2023, doi: 10.1038/s41586-023-05881-4.