

AI-Based Anomaly Detection for Industrial Cybersecurity Applications

Andrej Šimunek

Associate Professor, Slovak University of Agriculture in Nitra, Slovakia

Abstract

The rapid digitalization of industrial environments has increased the dependence of manufacturing, energy, transportation, water, and process-control infrastructures on interconnected cyber-physical systems. While connectivity improves automation, operational visibility, and production efficiency, it also introduces security vulnerabilities that can be exploited through malware, unauthorized access, protocol manipulation, insider activity, and sophisticated network attacks. Conventional signature-based security mechanisms may be insufficient for identifying previously unseen or behaviorally complex threats. Artificial intelligence (AI)-based anomaly detection provides an alternative approach by learning patterns of normal system behavior and identifying deviations that may indicate malicious or abnormal activity. This paper examines the application of AI-based anomaly detection techniques to industrial cybersecurity environments. The study focuses on machine learning, deep learning, behavioral analytics, feature engineering, and intelligent classification approaches for detecting anomalous network and system activities. A structured analytical methodology is used to evaluate these technologies according to detection capability, adaptability, computational requirements, interpretability, and operational suitability.

The analysis demonstrates that AI-based approaches can enhance the detection of unknown attacks, abnormal industrial communication, unusual device behavior, and deviations from established operational patterns. However, their effectiveness depends strongly on the quality of training data, feature representation, model selection, and continuous adaptation to changing industrial conditions. The study further identifies challenges associated with false positives, concept drift, adversarial manipulation, limited labeled datasets, legacy equipment, and real-time processing requirements. An integrated cybersecurity architecture combining AI-based anomaly detection with network segmentation, industrial firewalls, identity management, and security monitoring can provide stronger protection than isolated AI systems. Future research should investigate explainable AI, federated learning, digital twins, adaptive learning, and autonomous cyber defense mechanisms for industrial environments. The paper concludes that AI-based anomaly detection can become an important component of modern industrial cybersecurity when implemented within a multilayered, risk-aware, and operationally compatible security framework.

Keywords: Artificial Intelligence, Anomaly Detection, Industrial Cybersecurity, Machine Learning, Deep Learning, Industrial Control Systems, Cyber-Physical Systems, Behavioral Analytics.

1. Introduction

Industrial environments are increasingly dependent on interconnected digital technologies that support automated production, process monitoring, energy management, transportation, and critical infrastructure operations. Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers, industrial sensors, and connected devices continuously exchange operational information. This digital transformation has improved productivity and decision-making but has simultaneously expanded the attack surface of industrial networks. Cybersecurity has consequently become an essential component of maintaining reliable and secure industrial operations.

Traditional industrial cybersecurity mechanisms have largely relied on predefined rules, signatures, access restrictions, and known attack patterns. These mechanisms remain valuable for identifying established threats but may have limitations when attackers employ novel techniques, modified malware, stealthy behavior, or legitimate credentials. Anomaly detection addresses this challenge by identifying deviations from expected system behavior. Instead of relying exclusively on known attack signatures, anomaly detection can examine network traffic, device behavior, command sequences, and operational measurements to identify unusual patterns.

Artificial intelligence provides advanced capabilities for developing anomaly detection models. Machine learning algorithms can identify relationships within large datasets and classify activities according to learned characteristics. Unsupervised and semi-supervised methods are particularly relevant to industrial environments because obtaining extensive labeled attack data can be difficult. Deep learning techniques can additionally identify complex patterns across high-dimensional and sequential datasets, supporting the detection of subtle deviations that may not be easily identified using conventional rules.

Industrial environments, however, present specific challenges for AI-based security. Normal operational behavior can change because of maintenance activities, production schedules, equipment replacement, seasonal conditions, or process modifications. A model trained under one operational condition may generate false alarms when system behavior changes. AI models must therefore distinguish between legitimate operational variation and malicious anomalies while maintaining sufficiently low latency for security monitoring.

Another important concern is the operational consequence of incorrect detection. In conventional enterprise environments, an incorrect security alert may primarily affect administrative processes. In industrial systems, unnecessary intervention can potentially disrupt production or affect physical processes. Therefore, anomaly detection technologies must provide reliable results and should ideally operate alongside human expertise and other cybersecurity controls.

This paper examines AI-based anomaly detection for industrial cybersecurity applications and analyzes how intelligent models can strengthen threat identification and security monitoring. It considers major AI approaches, their operational roles, implementation requirements, limitations, and future development opportunities.

2. Objectives

2.1 To Examine AI-Based Techniques for Industrial Anomaly Detection

The first objective is to examine artificial intelligence techniques used to detect abnormal behavior in industrial cybersecurity environments. The study considers machine learning, deep learning, clustering,

classification, behavioral analytics, and sequential modeling approaches. Particular attention is given to how these techniques process industrial network traffic, device activity, system events, and operational data to identify deviations from established behavioral patterns.

2.2 To Evaluate the Effectiveness and Challenges of AI-Based Detection

The second objective is to evaluate the potential effectiveness of AI-based anomaly detection while considering the practical challenges associated with industrial deployment. Detection accuracy, adaptability, false-positive management, computational requirements, interpretability, and real-time performance are examined. The objective also considers how AI detection can be integrated with existing cybersecurity mechanisms to improve industrial resilience and security response.

3. Review of Literature

3.1 Anomaly Detection in Industrial Cybersecurity

Anomaly detection has traditionally been used to identify behavior that differs from an established baseline. In industrial cybersecurity, the baseline may include normal network communication, device interactions, process measurements, command sequences, and system events. Deviations from these patterns may indicate cyberattacks, equipment problems, configuration errors, or unexpected operational conditions. This makes anomaly detection valuable for security monitoring in environments where attack signatures may not be available.

Industrial anomaly detection must account for the relatively stable and structured nature of many industrial processes. Devices often communicate according to predictable patterns, which can provide useful behavioral characteristics for machine learning models. However, operational changes may produce legitimate deviations. Consequently, effective detection models need to distinguish security-relevant anomalies from normal variations in industrial operations.

3.2 Machine Learning for Anomaly Identification

Machine learning provides several approaches for industrial anomaly detection. Supervised classification models can learn distinctions between normal and malicious activities when labeled datasets are available. Decision trees, support vector machines, random forests, and other classifiers have been applied to cybersecurity datasets. Their performance depends heavily on the representativeness and quality of training data.

Unsupervised learning provides another important approach because industrial attack datasets often contain limited labeled examples. Clustering and dimensionality-reduction techniques can identify groups of similar behavior and highlight observations that differ significantly from dominant patterns. Such approaches may be particularly useful for discovering previously unknown anomalies, although interpretation of detected deviations remains a challenge.

3.3 Deep Learning and Sequential Modeling

Deep learning techniques can analyze complex relationships across large industrial datasets. Neural networks can learn hierarchical representations of network traffic and system behavior, while recurrent architectures can model sequential dependencies in time-series data. Autoencoders can learn representations of normal behavior and identify anomalous observations through reconstruction errors.

Sequential modeling is particularly relevant to industrial environments because processes evolve over time. A command or network event may appear normal when considered independently but become suspicious when analyzed in relation to preceding events. Deep learning models capable of capturing temporal relationships can therefore provide additional detection capabilities. However, their computational complexity and limited interpretability can affect deployment in resource-constrained industrial environments.

3.4 Behavioral Analytics and Intelligent Security Monitoring

Behavioral analytics focuses on understanding how users, devices, applications, and industrial components normally behave. AI can establish behavioral profiles and identify deviations associated with suspicious activity. For example, an engineering workstation communicating with an unusual control device or generating unexpected command patterns may trigger an anomaly alert.

Integration with centralized security monitoring can improve the value of AI-based detection. AI models can generate alerts that are correlated with authentication events, firewall records, endpoint activities, and operational data. This allows security teams to investigate anomalies within a broader context. Such integration can reduce dependence on isolated detection mechanisms and support more comprehensive industrial threat analysis.

4. Methodology

4.1 Research Design

This study applies a structured qualitative and analytical research design to examine AI-based anomaly detection within industrial cybersecurity applications. The methodology focuses on established research concerning machine learning, deep learning, industrial network security, anomaly detection, and cyber-physical system protection. The technologies are categorized according to their learning mechanisms, detection objectives, data requirements, and operational characteristics. This approach supports systematic comparison of AI-based techniques without assuming that one algorithm is universally optimal for all industrial environments.

The research design also considers the distinctive characteristics of operational technology environments. Industrial systems often contain legacy equipment, deterministic communication patterns, and strict availability requirements. Therefore, AI detection technologies are evaluated not only on their theoretical detection capabilities but also on their potential compatibility with real-time industrial operations. Particular attention is given to false-positive management, adaptability, computational requirements, interpretability, and integration with existing security controls.

4.2 AI-Based Detection Framework

The proposed analytical framework organizes AI-based anomaly detection into four stages: data acquisition, feature processing, intelligent modeling, and security decision-making. Industrial network packets, system logs, device activities, process measurements, and authentication events may provide input data.

Feature engineering or representation learning is then used to identify relevant characteristics. AI models analyze these characteristics and generate anomaly scores or classifications that can support security decisions.

The principal framework components include:

- **Data acquisition:** Collection of network, device, process, and security-event information.
- **Preprocessing:** Cleaning, normalization, transformation, and noise reduction.
- **Feature engineering:** Selection or extraction of security-relevant characteristics.
- **Model development:** Training supervised, unsupervised, or deep learning models.
- **Anomaly scoring:** Estimation of deviation from learned behavioral patterns.
- **Alert generation:** Identification and prioritization of suspicious activities.
- **Response integration:** Connection with monitoring and incident-response systems.

4.3 Analytical Evaluation

The study evaluates AI-based anomaly detection approaches according to detection capability, adaptability, computational demand, interpretability, data requirements, and operational suitability. These dimensions provide a structured basis for understanding the strengths and weaknesses of different approaches. Rather than presenting experimental accuracy values without a common dataset and testing environment, the study uses comparative conceptual analysis to identify characteristics relevant to industrial deployment.

The analysis further examines how AI-based detection can operate as part of a defense-in-depth cybersecurity architecture. AI models are considered complementary to firewalls, segmentation, access control, endpoint security, and centralized monitoring. This perspective recognizes that an anomaly detector may identify suspicious behavior without independently preventing an attack. Combining intelligent detection with preventive and responsive controls can therefore create a more comprehensive industrial security framework.

5. Analysis

5.1 Comparative Evaluation of AI-Based Anomaly Detection Techniques

Different AI techniques offer distinct advantages for industrial cybersecurity. Their suitability depends on data availability, computational capacity, model complexity, and the nature of industrial behavior being analyzed.

Table 1: Comparative Evaluation of AI Techniques for Industrial Anomaly Detection

AI Technique	Primary Detection Approach	Major Strength	Major Limitation	Industrial Suitability
Decision Trees	Supervised classification	Interpretability	Requires labeled data	High
Random Forest	Ensemble classification	Robust classification	Higher computational demand	High
Support Vector Machine	Boundary-based classification	Effective in high-dimensional data	Sensitive to parameter selection	Medium–High

AI Technique	Primary Detection Approach	Major Strength	Major Limitation	Industrial Suitability
K-Means Clustering	Unsupervised grouping	Does not require attack labels	Cluster interpretation can be difficult	Medium
Autoencoders	Reconstruction-based detection	Effective for complex patterns	Limited interpretability	High
Recurrent Neural Networks	Sequential analysis	Captures temporal behavior	Computational complexity	Medium–High
Convolutional Neural Networks	Pattern recognition	Strong feature extraction	Requires substantial training data	Medium–High
Hybrid AI Models	Combined learning strategies	Flexible detection capability	Greater complexity	High

Interpretation: The comparison indicates that no single AI technique provides universal advantages across all industrial environments. Decision trees and random forests provide comparatively interpretable classification, while clustering approaches can support detection when labeled attack data are limited. Autoencoders and deep learning models can identify complex patterns and temporal behavior but generally require greater computational resources and careful model development. Hybrid approaches provide broader capabilities but increase architectural complexity. Consequently, algorithm selection should be based on operational requirements, available data, system resources, and cybersecurity objectives.

5.2 AI-Based Detection within Industrial Security Architectures

AI anomaly detection is most effective when integrated with existing industrial security controls. The technology can provide an intelligent detection layer that complements preventive and access-control mechanisms. Network segmentation can reduce exposure, while AI monitoring identifies suspicious behavior occurring within authorized communication pathways.

Table 2: Role of AI-Based Anomaly Detection in a Layered Industrial Cybersecurity Architecture

Security Layer	Supporting Technology	AI Contribution	Expected Security Benefit
Network Protection	Firewalls and Segmentation	Identifies unusual traffic patterns	Reduced attack exposure
Access Security	MFA and RBAC	Detects abnormal user behavior	Improved access monitoring

Security Layer	Supporting Technology	AI Contribution	Expected Security Benefit
Endpoint Security	Host Protection	Identifies unusual device activity	Earlier compromise detection
Process Monitoring	Sensors and Control Data	Detects abnormal process patterns	Improved operational awareness
Central Monitoring	SIEM Platforms	Correlates AI-generated alerts	Better incident investigation
Threat Response	Response Systems	Prioritizes anomalous events	Faster containment
Continuous Learning	Adaptive Models	Updates behavioral baselines	Improved long-term detection

Interpretation: The results demonstrate that AI-based anomaly detection provides the greatest value when distributed across multiple layers of an industrial security architecture. AI can examine network, user, endpoint, and process behavior while centralized monitoring combines these signals into a broader security perspective.

The technology can improve early identification and prioritization of suspicious events, but it should remain integrated with preventive and response mechanisms. Continuous learning can additionally help detection models adapt to changing operational conditions, provided that model updates are carefully controlled.

6. Discussion

6.1 Detection of Unknown and Behavioral Threats

AI-based anomaly detection offers an important advantage in identifying activities that may not correspond to known attack signatures. By learning behavioral patterns, AI systems can identify deviations associated with previously unseen attacks, compromised accounts, unusual network communication, or abnormal device behavior. This capability is particularly valuable in industrial environments where attackers may modify their techniques to avoid traditional signature-based security controls.

However, anomaly detection is inherently sensitive to changes in normal behavior. Maintenance activities, production changes, equipment replacement, and software updates can generate patterns that differ from the training baseline. Therefore, an anomaly should not automatically be interpreted as a confirmed cyberattack. AI-generated alerts require contextual validation and, where appropriate, human investigation before significant operational actions are taken.

6.2 False Positives and Model Reliability

False positives represent one of the major challenges affecting AI-based industrial anomaly detection. Excessive alerts can overwhelm security personnel and reduce confidence in the detection system. In operational environments, unnecessary intervention can also create risks to production continuity. Model

performance should therefore be evaluated using multiple measures rather than relying exclusively on overall classification accuracy.

Reliability also depends on the quality of training data. Industrial datasets may be imbalanced, incomplete, proprietary, or difficult to obtain because real cyber incidents are relatively infrequent. Models trained on limited datasets may fail to generalize to different industrial environments. Combining diverse datasets, controlled simulations, expert knowledge, and continuous validation can improve the reliability of AI-based detection systems.

6.3 Integration with Human Expertise

AI should be considered a decision-support capability rather than a complete replacement for cybersecurity professionals and industrial engineers. Human experts understand operational context and can determine whether unusual behavior is caused by a cyberattack, maintenance activity, equipment malfunction, or legitimate process change. This contextual knowledge is particularly important when security actions could influence physical operations.

Human-AI collaboration can therefore improve the effectiveness of industrial anomaly detection. AI can continuously process large quantities of data and prioritize suspicious events, while experts can investigate alerts and determine appropriate responses. Explainable AI can further strengthen this relationship by providing understandable reasons for anomaly classifications and supporting more informed security decisions.

7. Challenges

One of the principal challenges in AI-based industrial anomaly detection is the availability of high-quality cybersecurity datasets. Industrial organizations may have limited labeled attack records because security incidents are relatively infrequent, sensitive, or difficult to share. Synthetic datasets can support model development but may not fully represent the complexity of real industrial environments. Differences between training and operational environments can consequently reduce model generalization.

Another challenge involves concept drift and changing operational behavior. Industrial systems evolve because of production changes, maintenance, equipment upgrades, software modifications, and changes in network architecture. A static AI model may gradually become less accurate as the underlying behavioral patterns change. Continuous adaptation is therefore necessary, but uncontrolled retraining may introduce new errors or allow manipulated data to influence the model.

Adversarial attacks present an additional concern. Attackers may deliberately modify network traffic or system behavior to evade anomaly detection models. AI systems themselves can become targets through data poisoning, evasion attacks, or manipulation of model inputs. Industrial organizations must therefore secure not only the systems being monitored but also the AI models, training pipelines, data sources, and model-update mechanisms.

8. Future Research

8.1 Explainable and Trustworthy AI

Future research should focus on developing explainable AI models that can provide understandable reasons for anomaly classifications. Industrial cybersecurity personnel need to determine why an alert was generated before deciding whether operational intervention is necessary. Explainability can improve

trust, support investigation, and reduce unnecessary responses. Research should evaluate explanation quality, computational overhead, and consistency across different industrial datasets and AI architectures.

8.2 Federated and Privacy-Preserving Learning

Federated learning represents a promising direction for collaborative industrial cybersecurity research. Organizations could potentially train models across distributed environments without directly sharing sensitive operational datasets. Future research should investigate federated anomaly detection for heterogeneous industrial networks while addressing communication costs, model synchronization, privacy risks, and poisoning attacks. Such approaches may support broader cybersecurity intelligence without requiring organizations to expose proprietary operational information.

8.3 Digital Twins and Adaptive Cyber Defense

Digital twins can provide controlled environments for developing and testing AI-based anomaly detection models. Future research should investigate the use of digital twins to simulate normal operations, cyberattacks, equipment changes, and evolving network conditions. Adaptive AI systems could then learn from simulated and operational environments while reducing the risks associated with direct experimentation on production systems. Integration with automated response technologies could ultimately support more adaptive and resilient industrial cyber defense.

9. Limitations

This study provides a structured conceptual analysis rather than an experimental evaluation of AI models using a standardized industrial dataset. Consequently, the comparative assessments should not be interpreted as direct performance rankings. Actual detection effectiveness can vary according to industrial architecture, data quality, attack characteristics, model configuration, computational resources, and operational conditions.

The study also does not evaluate specific commercial anomaly detection platforms or conduct long-term deployment experiments. AI model behavior may change significantly when exposed to concept drift, adversarial manipulation, or previously unseen industrial processes. Future empirical research using real-world industrial testbeds and longitudinal datasets would provide stronger evidence regarding model reliability, scalability, computational efficiency, and practical deployment requirements.

10. Conclusion

AI-based anomaly detection represents an important technological approach for strengthening cybersecurity in increasingly connected industrial environments. Unlike conventional security mechanisms that primarily depend on predefined signatures and rules, AI techniques can learn behavioral patterns and identify deviations that may indicate unknown or sophisticated threats.

Machine learning, deep learning, clustering, autoencoders, and behavioral analytics provide different capabilities for examining industrial network traffic, device behavior, system events, and operational processes. Their appropriate application can improve threat visibility and support earlier identification of suspicious activity.

The analysis demonstrates that AI detection should not operate as an isolated cybersecurity mechanism. Industrial environments require multilayered protection combining network segmentation, firewalls, authentication, endpoint security, security monitoring, and incident response. AI can strengthen this architecture by providing intelligent analysis across different data sources and prioritizing potentially significant anomalies. However, false positives, limited training data, concept drift, adversarial manipulation, and operational constraints remain important challenges. Careful validation and human oversight are therefore necessary.

Future industrial cybersecurity architectures are likely to increasingly combine AI-based detection with explainable models, federated learning, digital twins, and adaptive defense mechanisms. These developments can improve the scalability and responsiveness of industrial security while supporting privacy and operational reliability. Nevertheless, advanced AI must be implemented with careful attention to safety, interpretability, model security, and industrial context. A balanced combination of intelligent analytics, established cybersecurity controls, and human expertise can provide a stronger foundation for resilient and trustworthy industrial cybersecurity.

References

1. Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, 60, 377–405. <https://doi.org/10.1007/s10844-022-00753-1>
2. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection*, 38, Article 100516. <https://doi.org/10.1016/j.ijcip.2022.100516>
3. Hou, Y., et al. (2022). Anomaly detection approach in industrial control systems based on measurement data. *Information*, 13(10), Article 450. <https://doi.org/10.3390/info13100450>
4. Kim, B., Alawami, M. A., Kim, E., Oh, S., Park, J., & Kim, H. (2023). A comparative study of time series anomaly detection models for industrial control systems. *Sensors*, 23(3), Article 1310. <https://doi.org/10.3390/s23031310>
5. Choi, W.-H., & Kim, J. (2024). Unsupervised learning approach for anomaly detection in industrial control systems. *Applied System Innovation*, 7(2), Article 18. <https://doi.org/10.3390/asi7020018>
6. Pinto, A., Herrera, L.-C., Donoso, Y., et al. (2024). Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection. *International Journal of Computational Intelligence Systems*, 17, Article 236. <https://doi.org/10.1007/s44196-024-00644-z>
7. Ni, C., & Li, S. C. (2024). Machine learning enabled Industrial IoT security: Challenges, trends and solutions. *Journal of Industrial Information Integration*, 38, Article 100549. <https://doi.org/10.1016/j.jii.2023.100549>
8. Ali, A. H., Charfeddine, M., Ammar, B. B. H., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. *Frontiers in Computer Science*, 6. <https://doi.org/10.3389/fcomp.2024.1387354>
9. Explainable anomaly detection for industrial control system cybersecurity. (2022). *IFAC-PapersOnLine*, 55(10), 1183–1188. <https://doi.org/10.1016/j.ifacol.2022.09.550>

10. A study on performance metrics for anomaly detection based on industrial control system operation data. (2022). *Electronics*, 11(8), Article 1213. <https://doi.org/10.3390/electronics11081213>
11. Raman, M. R. G., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: Challenges and lessons from experimental evaluation. *Cybersecurity*, 4, Article 27. <https://doi.org/10.1186/s42400-021-00095-5>
12. McCarthy, J., Powell, M., Tang, C., Stouffer, K., Zimmerman, T., Barker, W., Ogunyale, T., & Wynne, D. (2020). Securing manufacturing industrial control systems: Behavioral anomaly detection (NIST Interagency/Internal Report 8219). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8219>
13. Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach. (2021). *Computers in Industry*, 132, Article 103509. <https://doi.org/10.1016/j.compind.2021.103509>
14. Anomaly detection in industrial control systems using logical analysis of data. (2020). *Computers & Security*, 96, Article 101935. <https://doi.org/10.1016/j.cose.2020.101935>
15. Intrusion and anomaly detection for the next-generation of industrial automation and control systems. (2021). *Future Generation Computer Systems*, 119, 50–67. <https://doi.org/10.1016/j.future.2021.01.033>
16. Anomaly detection for industrial control systems using process mining. (2018). *Computers & Security*, 78, 103–125. <https://doi.org/10.1016/j.cose.2018.06.002>
17. A three-tiered intrusion detection system for industrial control systems. (2021). *Journal of Cybersecurity*, 7(1), Article tyab006. <https://doi.org/10.1093/cybsec/tyab006>
18. Wang, C., Wang, B., Liu, H., Qu, H., & Chen, H. (2020). Anomaly detection for industrial control system based on autoencoder neural network. *Wireless Communications and Mobile Computing*, 2020, Article 8897926. <https://doi.org/10.1155/2020/8897926>
19. FALCON: Framework for anomaly detection in industrial control systems. (2020). *Electronics*, 9(8), Article 1192. <https://doi.org/10.3390/electronics9081192>
20. Wang, W., Wang, C., Guo, Y., Yuan, M., Luo, X., & Gao, Y. (2021). Industrial control malicious traffic anomaly detection system based on deep autoencoder. *Frontiers in Energy Research*, 8, Article 555145. <https://doi.org/10.3389/fenrg.2020.555145>