Enhancing Autonomous Systems' Awareness: Conceptual Categorization of Anomalies by Temporal Change During Real-Time Operations

Rialda Spahic
Engineering Cybernetics
Norwegian University of Science and Technology
Trondheim, Norway
email: rialda.spahic@ntnu.no

Vidar Hepsø
Geoscience and Petroleum
Norwegian University of Science and Technology
Trondheim, Norway
email: vidar.hepso@ntnu.no

Mary Ann Lundteigen
Engineering Cybernetics
Norwegian University of Science and Technology
Trondheim, Norway
email: mary.a.lundteigen@ntnu.no

***Abstract*—The Unmanned Autonomous Systems (UAS) are anticipated to have a permanent role in offshore operations, enhancing personnel, environmental, and asset safety. These systems can alert onshore operators of hazardous occurrences in the environment, in the form of anomalies in data, during real-time inspections, enabling early prevention of hazardous events. Time series data, collected by sensors that detect environmental phenomena, enables the observation of anomalous data as dynamic instances of the dataset. Recent research characterizes anomalies in terms of their patterns of occurrence in data. However, there is insufficient research on anomalous temporal change patterns. In this paper, we examine anomalies in relation to one another and propose a conceptual categorization system for anomalies based on their temporal changes. We demonstrate the categorization through a case study of potentially hazardous occurrences observed by UAS during underwater pipeline inspection. Analyzing anomalies based on their behavior can provide further information about current environmental changes and enable the early discovery of unwanted events, simultaneously minimizing false alarms that overwhelm the systems with low-significance information in real-time.**

***Keywords*—anomalies, anomalous change detection, anomaly detection, time-series analysis, autonomous systems**

I. Introduction

Sensors integrated into Unmanned Autonomous Systems (UAS), such as underwater autonomous vehicles, are reshaping our perception of the world by detecting environmental phenomena and responding to them through inputs such as graphics, motion, pressure, and heat. Underwater UAS, particularly in the offshore industry, are intended to replace operators in remote and potentially dangerous locations by residing on the seabed, collecting the data, and continuously monitoring and inspecting assets and the environment. In crucial situations, real-time data collection and analysis of the environment or assets can provide critical information, signaling us of potentially harmful deviations within the data, known as anomalies. Failure to capture anomalies effectively can have a devastating effect on the environment and result in severe financial loss.

Despite their ample presence in research and industry, anomaly detection methods have not yet matured as they are frequently too specialized or complex to evaluate [1]. Detecting anomalies, particularly for time-series data, is a challenging task that needs real-time processing while learning from analyzed data and making predictions [2]. Most anomaly detection methods are based on statistical samples of some data regions collected over time [3]. When the input data for these data regions changes, it becomes challenging to select the most appropriate strategy for detecting anomalies [3]. More compellingly, it becomes challenging to detect anomalies and capture their changing nature in real-time. The anomalous change detection method searches for unusual discrepancies between measurements taken at the same site at various periods [4]. These discrepancies may be due to harmless changes in atmosphere or sensor equipment. However, they may also be pervasive and potentially indicative of something hazardous evolving at the monitored site, i.e., a deteriorating material of a pipeline surface at the offshore oil and gas platform. Unfortunately, anomaly detection methods can have two significant drawbacks: they can ignore anomalies for the sake of efficiency as tolerable collateral damage [5], or they can overload the system with low-significance data, referred to as false alarms or noise [6]. The ideal outcome of anomaly detection is to alert operators of anomalous occurrences as soon as they are detected while minimizing false alarms [2].

Historically, anomalies have been defined primarily by their pattern of occurrence in data. However, there is insufficient investigation and categorization of anomalies based on how they relate to one another, particularly by the patterns of their temporal change. The time-series data enables the collection and observation of anomalies as dynamic instances of data that alter, evolve, disappear, and reappear. Therefore, this paper's contributions is a conceptual categorization of anomalies according to patterns of their temporal change, through an overview of the identification of anomalies during time-series change detection. Analyzing anomalies based on their behavior can provide more information about current environmental changes and allow for the early detection of anomalous, potentially hazardous occurrences in real-time. Consequentially, analyzing anomalies by their behavior can assist in minimizing false alarms by allowing for the more certain elimination of noisy data.

This paper is structured as follows: Section II discusses related work exploring anomalies' characteristics and categorization, anomalous change detection methods, and real-time anomaly detection. In Section III, we describe the proposed anomaly categorization according to their temporal changes. Section IV summarizes the findings and concludes the paper. Finally, Section V discusses future research.

 ISBN: 978-1-61208-966-9

II. Related Work

A. Anomaly Characteristics and Categorization

Anomalies are instances in a dataset that are unusual in some way and deviate from the dataset's overall or predicted trend [7]. There have been numerous attempts in the literature to categorize anomalies based on their presence in data, the data structures in which they arise, or even application-specific high-level categorization.

1) Anomalies by Data Structure: In a recent review on the nature and categories of anomalies, Foorthius [1] presents an overview of anomaly categories from a data-centric perspective. Because most datasets follow a well-defined, organized format, the author [1] describes the anomalies by examining the data structures that include them: cross-sectional, time-series, time-oriented, sequence, graph, tree, spatial, and spatio-temporal data structures. The author [1] then divides anomalies into univariate, multivariate, and multivariate aggregate anomalies, each of which includes numerical, class, or categorical anomalies and mixed data anomalies.

2) Anomalies by Occurrence in Data: While categorizing anomalies according to the data structure in which they occur simplifies their detection, the literature most often refers to a more general approach to anomaly categorization [8]:

- Global anomaly - one or more independent data points that deviate from the rest of the data. Global anomalies are alternatively referred to as point, and content anomalies [9] [10].
- Collective anomalies - a group of data points that differ from the rest of the data. When observed individually, these points often do not constitute an anomaly. Collective anomalies are alternatively referred to as group or aggregate anomalies.
- Contextual anomalies - anomalies that deviate when an intentionally chosen context is considered, i.e., weather, season, or location. Contextual anomalies are alternatively referred to as conditional anomalies [11].

3) Anomalies by Data Source: According to Erhan et al., [12], sensor systems have become the primary source of data. Therefore, the authors [12] categorize anomalies according to their origins and potential causes (see Table I). Sensor data frequently deviate from predicted behavior. The authors [12] underline the importance of evaluating the performance of anomaly detection systems using physical world data, as opposed to virtual testing with simulators. Since anomalies occur suddenly and are frequently unusual in physical world data, artificially manufacturing them through simulations or data extrapolation can be challenging.

TABLE I
Anomaly Categorization by Origin, adapted from Erhan et al. [12]

Anomaly origin	**Potential cause**
Environment	Unusual events, disasters, weather changes, new objects or compounds
System	Hardware limitations, system malfunctions
Communication	Network loss or delay
Attacks	Malevolent attacks on the physical components, malevolent interference or attack in network
Spike	Short peak in measured values, distinct deviation from common measurements
Noise	Increase in the variance in successive data samples
Constant	A constant neutral value reported by sensor
Drift	Off-set in the measurements

4) Application-Defined and Specific Anomaly Types: Ragozin et al. [13] approached forecasting complex time-series within an automated industrial system by *basing anomalies on their distinct dynamic characteristics* to increase the efficiency of information security management within the observed system. The authors [13] developed a method based on structural analysis of multi-component time series and digital signal processing technology for decomposing complex multi-component time series into several essential components for further real-time monitoring of the industrial information system and detecting any component-specific behavior anomaly event or proximity to such event.

Lutz et al. [14] analyzed operational safety-critical anomalies. The authors [14] argue that despite the widely-established benefits of anomaly analysis for operational software, research on anomaly analysis for safety-critical systems has been sparse. Patterns of software anomaly data for operational, safety-critical systems, in particular, are poorly known [14]. The authors [14] describe the findings of two hundred abnormalities on seven spacecraft systems using classification methods. The results of their study demonstrated various classification patterns, including the causal significance of data access and delivery issues, hardware degradation, and unusual incidents. Anomalies frequently revealed hidden software needs critical for the system's robust, accurate operation [14].

B. Anomalous Change Detection

In a recent review of change detection, Liu et al. [15] classify change detection methods based on their application purpose, data availability, and automation degree. The authors [15] describe anomalous change detection, and time-series change detection as application-specific methods most frequently used in image analysis. By suppressing background and emphasizing alterations, anomalous change detection finds anomalous changes between images. Anomalous change detection is typically focused on detecting minor changes caused by the insertion, deletion, or movement of produced small items and on small stationary objects that exhibit spectrum shifts between images, as with camouflage concealment and deception [15]. The authors [15] argue that the critical point is to examine the image statistics, increase the likelihood of detecting changes

 ISBN: 978-1-61208-966-9

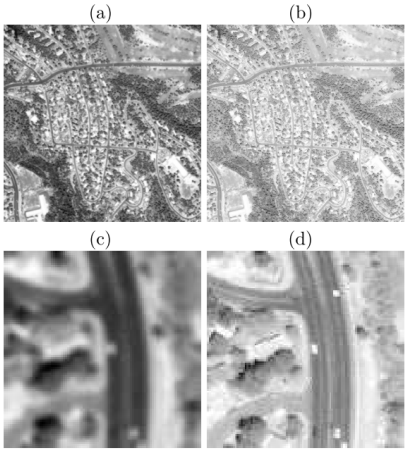

Fig. 1. (a,b) Predictable change in image contrast and brightnes; (c,d) Interesting change with (artificially) added vehicle, adapted from [4]

induced by human activity, and suppress background in image scene sequences.

Theiler et al. [4] employed anomaly detection to identify uncommon changes in images of the same scene captured at various periods and often under varying viewing conditions (see Figure 1). The detection of anomalous changes in imaging is of broad general interest and is particularly useful in remote sensing [4]. The authors [4] emphasize that anomalous change is distinct from and more unusual than changes across an entire scene. The authors [4] propose a framework based on a non-flat background distribution stated in terms of data distribution, with anomaly detection treated as a classification problem. The proposed framework identifies anomalous changes capturing meaningful differences between images while avoiding predictable noisy information caused by the camera's focus, contrast, or brightness.

C. Time-Series Anomaly Detection

Although many organizations collect time-series data, Feremans et al. [16] contend that automatically analyzing them and extracting valuable knowledge, such as a comprehensible model that flags critical anomalies, remains a complex problem, despite decades of effort. After examining various benchmark datasets for time series anomaly detection, the authors [16] discovered that these datasets frequently contain univariate time series with local or global extrema or point anomalies. By contrast, their research concentrated on collective and contextual anomalies, requiring data analysis from multiple sources to detect anomalies successfully. As a result, the authors [16] proposed a method for detecting anomalies in mixed-type time series. The method uses frequent pattern mining methods to create an embedding of mixed-type time series to train a prevalent anomaly detection method, isolation forest. Assuming that the anomalies are infrequent in the data, the isolation forest isolates them by continually splitting the data with low computational costs [17]. Experiments on multiple real-world univariate and multivariate time series and a synthetic mixed-type time series demonstrate that the proposed method outperforms established anomaly detection methods such as MatrixProfile, Pav, Mifpod, and Fpof [16].

Hannon et al. [18] used anomaly detection on streaming data to explain a power-grid system's real-time behavior and provide insight to system operators. The authors examined a real-time anomaly detection followed by a data-driven framework based on the statistical machine learning methods (decision trees and k-nearest neighbors) to enable the remote analysis of individual grid components for monitoring, detecting, and classifying anomalies that generate warnings of possible shortcomings in the system. They [18] concluded that classification of identified anomalies using well-defined probabilistic scores and classification of detected anomalies using interpretable decision trees demonstrates a high level of accuracy, as a result enabling operators to take corrective action to avert cascading blackouts and prevent system failures.

Previous research has established a variety of applications for anomaly detection and a need for a more profound comprehension of anomalies. In a discussion paper *Anomalousness: How to measure what you can't define*, Theiler [19] describes anomaly detection as target detection with unknown targets and with the objective to differentiate anomalies (unknown targets with stubbornly undefined attributes) from a background that is generally too cluttered to support an explicit model. Despite the challenges in defining and categorizing anomalies, the outcomes and discussions of previous studies demonstrate a promising direction in application-specific and dynamic-oriented anomaly categorization.

III. Categorization of Anomalies Based on Their Temporal Changes

After decades of research on anomaly detection, selecting anomalies to investigate and those to disregard as noise continues to be a complex problem, particularly with the pressure of a growing need for autonomous systems. Given the poor camera vision and ambiguous sensor inputs in the subsea environment [20], it is only natural to assume that strange phenomena, such as biological growth or misplaced objects, are frequently misinterpreted. This misinterpretation can further result in the misallocation of resources or the omission of signs indicating a more hazardous occurrence. Using inspiration from prior research on grouping time-series data [21] and integrating time-series and event logs into itemsets [16], we open opportunities to investigate prospects for isolating and analyzing changes in anomalies based on their geospatial context. By combining insights from time-series change detection on dynamic data points [21]–[23] with application-specific anomalies [14] [24], we observe that anomalies can display behavioral patterns such as frequent or reoccurring, disappearing and reappearing, and expanding.

a) Frequent or Recurring Anomalies: Feremans et al. [16] discuss frequent patterns in data, assuming that because

 ISBN: 978-1-61208-966-9

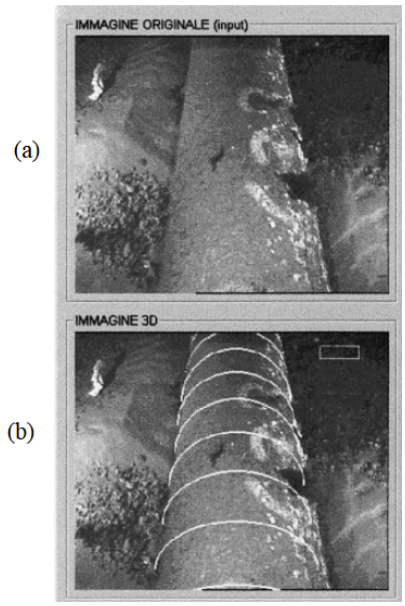

Fig. 2. (a) Visual inspection of underwater pipeline, images taken by autonomous underwater vehicle, adapted from [20]; (b) 3D scan over the underwater pipeline, adapted from [20]

anomalous activity infrequently occurs in time series, the frequent patterns represent frequently seen normal behavior. The main advantage of frequent pattern extraction is that the extracted patterns are easily interpretable and aid classifiers and anomaly detection methods in differentiating between normal and anomalous behavior in data. However, it might quickly become problematic if an anomalous event occurs repeatedly or in patterns. Anomalies that reoccur in patterns, hence generating a recurrent pattern in obtained data, present a concern because they can be difficult to spot or even mistaken as part of the normal dataset. Normal data can mask these anomalies, making it particularly difficult to detect when using unsupervised methods.

A practical example, seen on Figure 2, is the pipeline with unclear surface material, provided by images collected during a visual inspection of sea bottom infrastructure by an autonomous underwater vehicle. Visually inspecting structures can detect various phenomena, from object detection to material degradation such as corrosion monitoring [25]. However, a less intrusive process, such as biological growth, happens frequently and can readily obscure a more intrusive process, corrosion. Although additional measurements like ultrasonic testing and electromagnetic mapping are used to identify additional information about the corrosion process, the pace of corrosion (spread over time), the exact location, and even plausible causes [25], relying on unsupervised visual inspection of anomalies may not be sufficient.

b) Disappearing and Reappearing Anomalies: Although disappearing anomalies are not usually mentioned in industrial anomaly detection applications, they are a fairly common topic in stock market anomaly detection. During the analysis of the dynamic persistence of anomalies, Marquering et al. [26] highlighted the occurrences of disappearing and reappearing anomalies. Since most seasonal or predictable anomalies are well-known, they should not persist [26]. However, the authors [26] question the persistence of such anomalies as a source of contention. They highlight essential questions on disappearing and reappearing anomalies in data: *Are there still anomalies in recent data? Are they just existent during specific periods, or did they completely vanish? What is the immediate cause of the endurance of the anomaly?* The occurrence of disappearing and reappearing anomalies may be of interest in time-series change detection for various applications.

During a real-time inspection of an underwater pipeline, as depicted in Figure 3, recordings of fading unusual events may represent a low-importance environmental phenomenon that does not require comprehensive inspection, thus saving additional resource allocation. However, the persistence of such occurrences may represent something of more profound research interest [26].

c) Expanding Anomalies: As the environment evolves and changes over time, assuming that anomalous occurrences will exhibit similar changes is natural. Despite anomalies' dynamic and evolving nature being frequently discussed in sensor networks, it is not often discussed in other applications. What appears to be an innocuous anomaly may grow to affect various regions of the inspected structure. The purpose is to identify the onset of the anomaly as fast as feasible while maintaining a low false alarm rate [23]. This detection problem is formulated as a stochastic optimization problem utilizing a delay metric based on the anomaly's worst-case path [23]. In Figure 4, we illustrate a point anomaly (Figure 4 (a)) expanding into a collective anomaly (Figure 4 (b-j)). At an early stage (Figure 4 (a)), the detected point anomaly or a smaller collection of anomalies may not yet indicate a high-significance unusual occurrence. However, if unexplored, the anomalous collection may develop into a possibly hazardous state (Figure 4 (j)), leaving less time for a reactive response. Detecting anomalies early enables preventative measures. Expanding fractures of the pipeline surface material are a practical example of expanding anomalies during an underwater pipeline inspection.

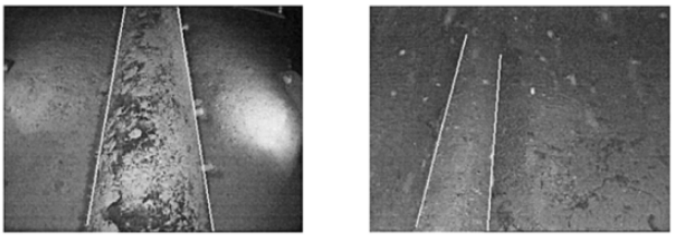

Fig. 3. (a) Visual inspection of underwater pipeline, images taken by autonomous underwater vehicle: Possible material degradation or biological growth?, adapted from [20]; (b) 3D scan over the underwater pipeline, adapted from [20]

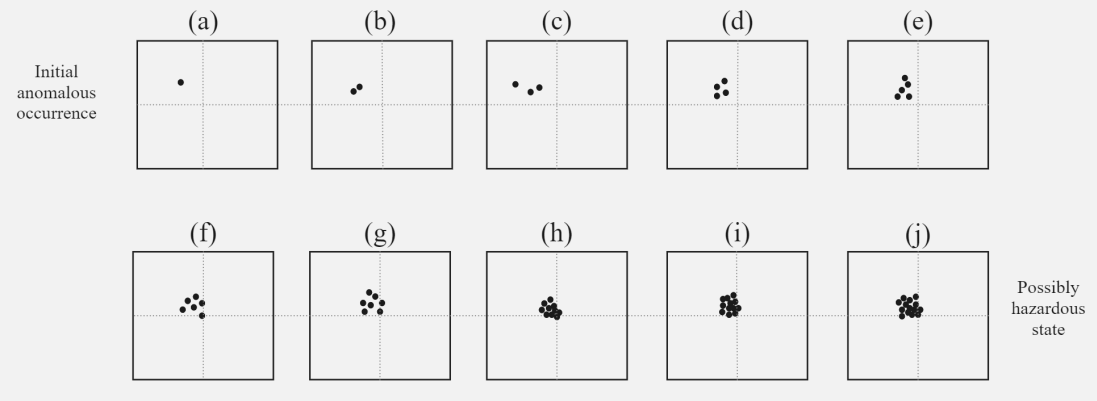

Fig. 4. Anomalies that expand over time

TABLE II
DESCRIBING ANOMALIES BY TEMPORAL CHANGE

Anomaly Type	**Frequent / Recurring**	**Disappearing and Reappearing**	**Expanding**
Point	Frequently occurring point anomaly.	Disappearing and reappearing point anomaly may be a sign of pervasive environmental phenomena.	Point anomaly may evolve into a collective anomaly of larger size and impact.
Collective	Frequently occurring collection of anomalies with similar properties (i.e., geospatial context).	Disappearing and reappearing collective anomaly may be a sign of pervasive environmental phenomena.	Collective anomalies may evolve into a more intrusive anomalous occurrence of larger size and impact.
Contextual	Anomalous depending on the context due to a potential risk of being misinterpreted as normal and left unexposed or a frequent anomaly collection obscuring more intrusive processes.	Context (i.e., geospatial, seasonal, weather) aids in determining the anomalousness of the disappearing/reappearing phenomena and finding the causes of their persistence.	Anomalous depending on the context.

The proposed conceptual categorization of anomalies according to their temporal changes does not impede their occurrence in data as point, collective, and contextual anomalies. Table II summarizes the two categories that are intended to complement one another, aiding in our comprehension of unusual events occurring during autonomous operations. Anomalies' behavior is highly dependent on context, not just on their occurrence as a single point or collection of anomalies. The criticality of frequently occurring point and collective anomalies varies by context, as they may be seen as normal and therefore obscure more intrusive processes. This increases the likelihood that the unexposed anomaly may develop into a potentially hazardous event that could have been discovered earlier. Similarly, the context (i.e., seasonal, weather) of disappearing and reappearing anomalies can aid in identifying the cause of their pervasiveness and provide additional reasoning for unanticipated environmental phenomena. Additionally, the point anomaly may expand creating a collective anomaly of more impactable volume and intrusiveness. Contextual information (e.g., changed material properties due to chemical or temperature variations) can assist in determining the criticality and anomality of observed unanticipated changes. Observing and categorizing anomalies according to their temporal changes adds context to our understanding of how anomalies relate to one another and evolve in a normal and predictable data environment. This knowledge enables the UAS to perceive environmental phenomena and anomalous events in their geospatial and temporal context, improving understanding of the significance and criticality of anomalous occurrences.

IV. CONCLUSION

The research on time-series anomaly detection has been application-oriented and vague. Despite decades of research and categorization approaches, persistent obstacles prevent anomaly detection from maturing and becoming a dependable component of autonomous systems. While an unsupervised and data-driven strategy is common in industry and research, it is insufficient to achieve reliable autonomy. Therefore, this paper proposes a fundamentally different perspective of anomalies via a conceptual categorization of anomalies according to their temporal changes. Frequent or recurrent, disappearing and reappearing, and expanding anomalies describe the behavior of anomalies and provide context for their dynamics observed through time-series data analysis. Observing anomalies as they evolve through time enables us to deduce the underlying causes of anomalous occurrences, focusing on more pertinent data from the vast collections of sensor measurements, thus allowing the UAS to react if and when the situation requires it during real-time operations.

 ISBN: 978-1-61208-966-9

V. Future Work

We regard our approach of categorizing anomalies according to their temporal change as a starting point for future research to construct a framework for detecting anomalous change in real-time by identifying practical time-series anomaly detection methods. Thus, future work involves simulating streaming data and analyzing images collected by the UAS during visual inspection of an underwater pipeline to validate the proposed temporal categorization of anomalies and identify potential shortcomings.

Acknowledgment

This research is a part of BRU21 – NTNU Research and Innovation Program on Digital and Automation Solutions for the Oil and Gas Industry (www.ntnu.edu/bru21) and supported by Equinor.

References

[1] R. Foorthuis, "On the nature and types of anomalies: a review of deviations in data," *Int. J. Data Sci. Anal.*, vol. 12, no. 4, pp. 297–331, 2021.

[2] A. Lavin and S. Ahmad, "Evaluating Real-time Anomaly Detection Algorithms - the Numenta Anomaly Benchmark," in *IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*. Miami, Florida, USA: Institute of Electrical and Electronics Engineers Inc., 2015, pp. 38–44.

[3] A. S. Alghawli, "Complex methods detect anomalies in real time based on time series analysis," *Alexandria Eng. J.*, vol. 61, no. 1, pp. 549–561, 2022.

[4] J. Theiler and S. Perkins, "Proposed framework for anomalous change detection," in *ICML Work. Mach. Learn. Algorithms Surveill. Event Detect.*, 2006, pp. 7–14.

[5] K. Makhlouf, S. Zhioua, and C. Palamidessi, "On the applicability of ML fairness notions," *arXiv*, pp. 1–32, 2020.

[6] R. Sekar et al., "Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. - CCS '02*. New York, NY, USA: Association for Computing Machinery, 2002, pp. 265–274.

[7] C. C. Aggarwal, "An Introduction to Outlier Analysis," in *Outlier Anal.* Springer, Cham, 2017, ch. 1, pp. 1–34.

[8] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection," *ACM Comput. Surv.*, vol. 14, no. 1, pp. 1–22, jul 2009.

[9] A. Fisch, I. Eckley, and P. Fearnhead, "Subset Multivariate Collective And Point Anomaly Detection," *J. Comput. Graph. Stat.*, pp. 1–51, 2019.

[10] M. A. Hayes and M. A. Capretz, "Contextual anomaly detection in big sensor data," in *Proc. - 2014 IEEE Int. Congr. Big Data, BigData Congr. 2014*. Institute of Electrical and Electronics Engineers Inc., sep 2014, pp. 64–71.

[11] S. Xiuyao, W. Mingxi, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 631–644, may 2007.

[12] L. Erhan et al., "Smart anomaly detection in sensor systems: A multi-perspective review," *Inf. Fusion*, vol. 67, no. September 2020, pp. 64–79, 2021.

[13] A. N. Ragozin, V. F. Telezhkin, and P. S. Podkorytov, "Forecasting complex multi-component time series within systems designed to detect anomalies in dataflows of industrial automated systems," *ACM Int. Conf. Proceeding Ser.*, pp. 1–5, 2019.

[14] R. R. Lutz and I. C. Mikulski, "Empirical analysis of safety-critical anomalies during operations," *IEEE Trans. Softw. Eng.*, vol. 30, no. 3, pp. 172–180, mar 2004.

[15] S. Liu, D. Marinelli, L. Bruzzone, and F. Bovolo, "A review of change detection in multitemporal hyperspectral images: Current techniques, applications, and challenges," *IEEE Geosci. Remote Sens. Mag.*, vol. 7, no. 2, pp. 140–158, 2019.

[16] L. Feremans et al., "Pattern-Based Anomaly Detection in Mixed-Type Time Series," *Mach. Learn. Knowl. Discov. Databases*, vol. 11906, pp. 240–256, 2020.

[17] F. T. Liu, K. M. Ting, and Z. H. Zhou, "Isolation forest," in *Proc. - IEEE Int. Conf. Data Mining, ICDM*. IEEE, 2008, pp. 413–422.

[18] C. Hannon, D. Deka, D. Jin, M. Vuffray, and A. Y. Lokhov, "Real-time Anomaly Detection and Classification in Streaming PMU Data," in *2021 IEEE Madrid PowerTech*. Madrid: IEEE, 2021, pp. 1–6.

[19] J. Theiler, "Anomalousness: how to measure what you can't define," *Fourier Transform Spectrosc. Hyperspectral Imaging Sound. Environ.*, p. JT1A.2, 2015.

[20] G. L. Foresti, "Visual inspection of sea bottom structures by an autonomous underwater vehicle," *IEEE Trans. Syst. Man, Cybern. Part B Cybern.*, vol. 31, no. 5, pp. 691–705, oct 2001.

[21] T. Rakthanmanon, E. J. Keogh, S. Lonardi, and S. Evans, "Time series epenthesis: Clustering time series streams requires ignoring some data," *Proc. - IEEE Int. Conf. Data Mining, ICDM*, pp. 547–556, 2011.

[22] S. Guggilam, V. Chandola, and A. Patra, "Tracking clusters and anomalies in evolving data streams," *Stat. Anal. Data Min. ASA Data Sci. J.*, vol. 15, no. 2, pp. 156–178, 2021.

[23] G. Rovatsos, V. V. Veeravalli, D. Towsley, and A. Swami, "Quickest Detection of Growing Dynamic Anomalies in Networks," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, vol. 2020-May, pp. 8926–8930, may 2020.

[24] T. Wang, C. Fang, D. Lin, and S. F. Wu, *Localizing temporal anomalies in large evolving graphs*. Society for Industrial and Applied Mathematics Publications, 2015.

[25] Y. T. Al-Janabi, "Monitoring of Downhole Corrosion: An Overview," *Soc. Pet. Eng. - SPE Saudi Arab. Sect. Tech. Symp. Exhib. 2013*, pp. 108–118, may 2013.

[26] W. Marquering, J. Nisser, and T. Valla, "Disappearing anomalies: A dynamic analysis of the persistence of anomalies," *Appl. Financ. Econ.*, vol. 16, no. 4, pp. 291–302, 2006.

 ISBN: 978-1-61208-966-9