VAE-based anomaly detection for embedded computer electronic components

Shuda Gao
Xi’an Microelectronic Technology Institute, Xi’an, China

Zhong Ma
Xi’an Microelectronic Technology Institute, Xi’an, China

Zhanzhuang He
Xi’an Microelectronic Technology Institute, Xi’an, China

Yuanhong Mao
Xi’an Microelectronic Technology Institute, Xi’an, China

ABSTRACT

The current maintenance of aerospace equipment generally uses regular maintenance, scheduled maintenance, seasonal maintenance, after-the-fact maintenance, and replacement maintenance. These methods are ill-timed, time-consuming, and wasteful of materials. Monitoring the reliability and healthy operating status of each embedded computer electronic component is essential, and maintenance staff will benefit greatly from a data-driven approach to anomaly detection. It can be altered from "repair afterward" to "repair as necessary" and from " repair regularly" to "repair at any time" to solve the practical problems arising from maintenance. The Variational Autoencoder (VAE), which is based on the component storage aging acceleration data, is used in this paper to model the component’s normal operating status and perform anomaly detection. The precision and recall of this anomaly detection method are 0.950 and 0.977. This method evaluates the operating status and reliability of each component, improves the reliability and service life of the computer, and establishes the technological framework for the next generation of computer Prognostics and Health Management (PHM) systems.

CCS CONCEPTS

• **Computer systems organization**; • **Embedded systems;**; • **Computing methodologies**; • **Artificial Intelligence.**;

KEYWORDS

Embedded computer, Anomaly detection, Variational Autoencoder

ACM Reference Format:
Shuda Gao, Zhong Ma, Zhanzhuang He, and Yuanhong Mao. 2022. VAE-based anomaly detection for embedded computer electronic components. In *2022 6th International Conference on Computer Science and Artificial Intelligence (CSAI) (CSAI 2022), December 09–11, 2022, Beijing, China.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3577530.3577536

1 INTRODUCTION

With the development of science and technology and the continuous updating of electronic technology, electronic product design is becoming more precise, the structure is becoming more complex, and the probability of reliability risks and faults is also increasing. This strongly requires reliability, repairability, and maintainability for electronic systems.

At present, the cost of electronic components has accounted for more than 30% of the total cost of large computer systems, electronic system faults accounted for more than 40% of the total system faults, the electronic system use and security costs have accounted for more than 70% of the total cost. Electronic equipment repairs and maintenance costs are much higher than the cost of procurement. To address the practical issues resulting from maintenance, the maintenance and guarantee mode of the equipment must be altered from "repair afterward" to "repair as necessary" and from " repair regularly" to "repair at any time" to solve the practical problems arising from maintenance.

If maintenance staff can keep track of each electronic component’s reliable operation and healthy operating status. If the electronic component that frequently produces anomalies and deteriorates reliability can be quickly replaced and maintained, the reliability will improve. Accidents can be efficiently avoided, and maintenance costs can be decreased.

Conventional methods rely on sensors to gather data from the component and use straightforward thresholds to assess the component’s health status. It cannot represent the component health status accurately.

Embedded computer anomaly detection involves many fields, the component-level parameter detection has a high degree of reliability because it can most directly reflect the computer operating status. Moreover, the component can be fixed as necessary throughout the maintenance phase to lower maintenance costs, depending on the reliability of the number of anomalies.

Embedded computer anomaly detection is a long-term process, and such anomalies are usually presented as sudden changes in parameters. The embedded computer design tolerance margin is quite wide. The abrupt change of parameters cannot impact the operating status, so the real machine anomaly data is difficult to obtain. In engineering, this process can often be accelerated by the acceleration method. The acceleration method is performed by increasing a certain kind of stress and thus reducing the service life. The components that show more anomalies during the acceleration method are less reliable and more easily degradable [1], which affects the computer operating status.

Due to the stable operation of the electronics, the parameters do not change much and the fluctuations are small. Data fluctuations are more obvious when there is an anomaly. Feature extraction on the raw data is necessary to make better use of the data.

CSAI 2022, December 09–11, 2022, Beijing, China

ACM ISBN 978-1-4503-9777-3/22/12…$15.00
https://doi.org/10.1145/3577530.3577536

Embedded computers in actual operation cannot manually label the monitoring data effectively, which creates difficulties in modeling the normal operation of the components. Using traditional unsupervised algorithms for modeling, the anomalies generated in actual operation can bring serious bias to the normal operation status modeling. Therefore, it is necessary to rule out the possible anomalous status, and the pseudo label is quite helpful in this situation.

Because each electronic component has different degradation trends and physical degradation models, and the current number of detector pieces is small, it cannot reflect the whole board operating status well. Using the Variational Autoencoder, the raw data of various components are independently modeled for the normal operating status.

This paper proposes a new data-driven embedded computer component anomaly detection approach. It uses difference as the extracted feature with the raw data. It uses Spectral Residual to generate the pseudo label to exclude the effect of the anomalous portion on the model. It uses VAE to model the normal status and anomaly detection is performed based on reconstruction error. Compared to the conventional method, it can more accurately reflect the component's operating status and health status. Additionally, it satisfies the need for real-time.

2 RELATED WORK

The data-driven anomaly detection approach is based on the rapid development of sensor technology, deep learning, and database technology. Historical operational data of the operating process is stored, which reflects the dynamic characteristics of the actual system. When accurate object models are not unavailable, the data-driven anomaly detection approach becomes an ideal approach to utilize these data resources for process monitoring and anomaly detection.

The research in data-driven embedded computer anomaly detection technology is still in the exploratory stage, it is now classified primarily into two categories: operating status detection method and normal operating status-based modeling and detection.

Based on the operating status detection method is to collect computer operation status information. And the computer running status is classified as normal running status and anomaly status. Maxion [2] used anomaly detection as an early means of fault detection. He used sensors as anomaly detectors for anomaly analysis and detection. Zhang [3] studied real-time checkpoint-based fault detection and recovery. Peti [4] introduced ONAs into electronic components and as a diagnostic measure operating on distributed states to detect relevant component faults. Zandrahimi [5] used the probability of data events to evaluate the behavior of electronic systems and perform anomaly detection, reducing the detection overhead. Mojarad [6][7][8] introduced and compared the above three methods for real-time anomaly detection: Markov-based, Stide (Sequence Time-Delay Embedding), and clustering-based methods.

However, because there is a lack of anomaly data in the computer's actual operation, it is not possible to accurately describe the anomaly status, and directly classify it is easy to generate a large number of false alarms. Modeling and detecting based on the normal operating status by extracting normal operation state features and modeling those features. The operation states that do not conform to the model features are regarded as an anomaly. Wang [9] proposed a PHM high-performance computing platform based on FPGA and DSP as the core. And used the time domain feature extraction approach and BP neural network to perform anomaly diagnosis on the platform. Sandborn [10] proposed a cumulative damage model for anomaly prediction, anomaly symptom detection, and early warning. Lall [11] proposed to combine sensor parameters with the damage mathematical model for detecting damage in aerospace electronics.

With the development of machine learning and neural networks, new techniques will be gradually applied in anomaly detection. Kingma [12] proposed Variational Autoencoder (hereinafter referred to as VAE), and several people later used VAE for anomaly detection. Xu [13] uses unsupervised VAE for anomaly detection on KPI data. Chen [14] adds a self-adversarial training mechanism to VAE to improve the model effect. Kawachi [15] proposes a supervised VAE anomaly detection algorithm, which effectively avoids the influence of the anomalous part of the data on the model. Linp [16] additionally introduces an LSTM module to analyze the long-term correlation of time series, which can detect anomalies across more time scales of anomalies.

3 METHOD

3.1 VAE-based anomaly detection architecture

Data collection for embedded computer electronics component parameters employing detecting devices with sensors. First, normalize the feature data and raw data. The pseudo label is done using Spectral Residual to mark the anomalous regions. The processed data are modeled by Variational Autoencoder (VAE), and the anomalies are determined by the sum of the reconstruction errors output from different models.

Each component's test results are counted, and the number of anomalies that were generated is noted. The reliability index is reduced for the devices with more repeated anomalies. The threshold value is determined by the combination of actual operating conditions and engineers' experience.

3.2 Data preprocessing

Preprocess the data first. The features of the original data are extracted as feature data, and both of them are then normalized.

Spectral Residual [17] can be processed effectively for data from a single electronic component to mark suspected anomaly regions as the pseudo label. Applying Spectral Residual to time series for anomaly labeling can effectively reduce the manual labeling cost and can meet the real-time standard.

The SR variation process is as follows:

$$A(f) = Amplitude(F(x)) \tag{1}$$

$$P(f) = Phrase(F(x)) \tag{2}$$

$$L(f) = log(A(f)) \tag{3}$$

$$AL(f) = hq(f) \cdot L(f) \tag{4}$$

$$R(f) = L(f) - AL(f) \tag{5}$$

$$S(x) = \left\| F^{-1} \quad (exp(R(f) + iP(f))) \right\| \tag{6}$$

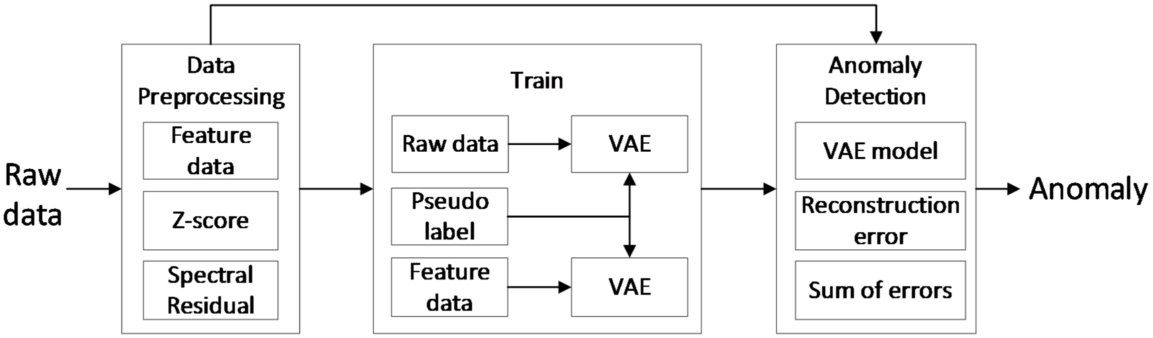

Figure 1: Overall Structure

x is the input sequence sliding window data. $F(x)$ is the data by Fourier transform, then calculate the amplitude spectrum $A(f)$, calculate the phase spectrum $P(f)$, then do Log to get $L(f)$, $AL(f)$ is the average of $L(f)$, $R(f)$ is the result obtained by Spectral Residual, $S(x)$ is the significant region obtained after Inverse Fourier transform. $S(x)$ is called the saliency map of x. It is possible to mark suspected anomalies as the pseudo label by setting the percentile η. It will identify the most significant anomalies. The anomaly score $O(x_i)$ is defined as:

$$O\left(x_i\right)=\begin{cases}1,\ if\frac{S(x_i)-\overline{S(x_i)}}{\overline{S(x_i)}}\geq\eta\\ 0, \qquad\qquad Otherwise\end{cases}\tag{7}$$

With the pseudo label, the influence of anomalies can be excluded in building a normal operation model and improving the accuracy.

3.3 Train

Variational Autoencoder (VAE) [12] is a deep generative model. It combines the ideas of deep learning and Bayesian probabilistic inference to be able to model the normal operating state of electronic components. VAE assumes that the data are generated by some random process with unobservable continuous random hidden variables. Its training objective is to take a given training set $X=\{x_1,x_2,\ldots.,x_n\}$ and create a random variable $x\sim p(x)$, $p(x)$ is the true distribution of the data.

VAE consists of an encoder (with parameter ϕ), a decoder (with parameter θ), and a hidden layer. The encoder transforms the input data x into a probability distribution of the latent variable $p_q(z|x)$. Then the latent variable z is randomly sampled and reconstructed by the decoder to obtain the reconstructed data $\hat{x}$. Because $p_q(z|x)$ is difficult to calculate, VAE uses a variational inference technique to construct a new function $q_\phi(z|x)$ to approximate the distribution, assuming that $q_\phi(z|x)$ obeys a Gaussian distribution. The likelihood function of the model is:

$$p\left(x\right)\ =\ \int\ p_\theta(x|z)p_\theta\left(z\right)dz\tag{8}$$

Where, $p_\theta(x|z)$ is the generating model, which can be described as a multivariate Gaussian distribution, and $p_\theta(z)$ is the prior, which is usually set simply as a standard Gaussian distribution.

Its logarithmic format is as follows:

$$lnp\left(x\right)=ln\int p_\theta\left(x|z\right)p_\theta\left(z\right)\frac{q_\phi\left(z|x\right)}{q_\phi\left(z|x\right)}dz\tag{9}$$

However, because the generative model's parameters θ and the hidden variables are unknown, here the integration of the hidden variables and the posterior probabilities is difficult to process. Therefore, VAE introduces an additional Variational Distribution as an inferential model to approximate the intractable true posterior based on the idea of variational inference. Similar to the generative model, the inferential model can be described as a multivariate Gaussian distribution.

For the above equation to find the expectation, according to Jensen's inequality, the above equation can be rewritten as:

$$lnp\left(x\right)=lnE_{q_\phi(z|x)}\frac{p_\theta\left(x|z\right)p_\theta\left(z\right)}{q_\phi\left(z|x\right)}\geq E_{q_\phi(z|x)}ln\left(\frac{p_\theta\left(x|z\right)p_\theta\left(z\right)}{q_\phi\left(z|x\right)}\right)\tag{10}$$

$$=E_{q_\phi(z|x)}\left(-ln\frac{q_\phi\left(z|x\right)}{p_\theta\left(z\right)}\right)+E_{q_\phi(z|x)}\left(lnp_\theta\left(x|z\right)\right)\tag{11}$$

$$=E_{\phi(z|x)}\left[lnp_\theta\left(x|z\right)\right]-D_{KL}\left[q_\phi\left(z|x\right)\|p_\theta\left(z\right)\right]\tag{12}$$

$= E_{\phi(z|x)}[lnp_\theta(x|z)] - D_{KL}[q_\phi(z|x)\|p_\theta(z)]$ is the evidence lower bound (ELBO) of the log-likelihood function $lnp(x)$. If the $lnp(x)$ is to be maximized, the evidence lower bound must be maximized. Therefore, the optimization objective of the VAE is to maximize the evidence lower bound function, defined as $L(\theta,\ \phi)$:

$$L\left(\theta,\phi\right)=E_{q_\phi(z|x)}\left[lnp_\theta\left(x|z\right)\right]-D_{KL}\left[q_\phi\left(z|x\|p_\theta\left(z\right)\right)\right]\tag{13}$$

The first term to the right of the equal sign is the expectation of $lnp_\theta(z|x)$ when given $p_\theta(x|z)$. It is used to ensure the matching degree between the reconstructed data and the actual data. The second term is a Kullback-Leibler (KL) scattering term that can be viewed as a regularization that guides the approximate posterior distribution to be as close as possible to the prior distribution.

Using data with the pseudo label allows for better modeling of the normal operating status. The original variational autoencoder is an unsupervised model that cannot use label information. Self-Adversarial Variational Autoencoder [18], which solves this problem by adding restrictions, eliminates the contribution of anomalous data to the model training.

The optimization objective is updated as:

$$\begin{aligned}L\left(\theta,\phi\right)\quad=\quad & E_{q_\phi(z|x)}\left[\sum_{w=1}^{W}\left(1-O\left(x_i\right)lnp_\theta\left(x|z\right)\right)\right]\\ & -D_{KL}\left[q_\phi\left(z|x\right)\|p_\theta\left(z\right)\right]\end{aligned}\tag{14}$$

Table 1: Statistical information of experimental data

optocoupler	type 1	type 2	type 3	type 4	type 5	type 6
Number	1#∼9#	10#∼18#	19#∼27#	28#∼36#	37#∼45#	46#∼54#
Number of anomalies	62	48	58	58	56	50

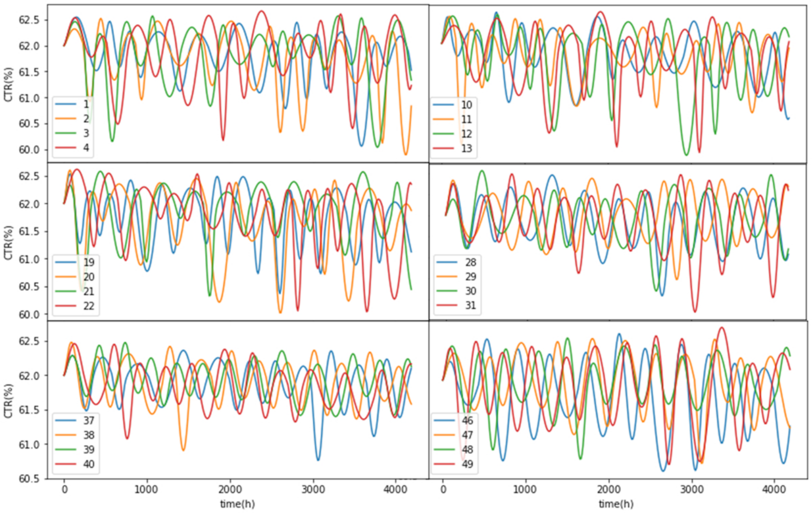

Figure 2: Partial data

Self-Adversarial Variational Autoencoder, which also introduces the adversarial training idea of GAN. An additional encoder E that functions as a discriminator to verify the authenticity of the reconstructed data is added on the basis of the VAE.

In the actual training. The normalized component detection data with the pseudo label is sliced through a sliding window, then passed into the VAE for training to get the reconstruction error.

3.4 Anomaly detection

Usually, the model sets a threshold value d. When the reconstruction error score f is larger than the threshold value d, the current time t is determined as an anomaly. However, to avoid the selection of thresholds, the model does not use a predetermined threshold for anomaly determination. This model enumerates all possible thresholds using the various thresholds of the decision function that calculates precision and recall. And the best F1 score is used to indicate the best detection result possible with a given best threshold.

4 EXPERIMENTAL ANALYSIS

4.1 Data Collection

The test data were from the optocoupler data on the embedded computer of the thermal stress accelerated aging test. The optocoupler test parameter is the normal current transfer ratio (CTR) with a normal operating range of 50% to 200%. There are nine motherboards in total, each with six different types of optocouplers on the motherboard with the same function.

The actual anomaly data is less and cannot be modeled effectively in the actual test. After analyzing the anomaly data patterns, similar anomalies are injected into the remaining data. The statistical data for different types of optocouplers are shown in Table 1.

Some of the data are shown in Figure 2.

4.2 Experimental Setting

The experiments were conducted using Ubuntu 18.04, and Python 3.83, and the model was implemented using PyTorch. the Spectral Residual algorithm uses the upper 2.5% of the data as the pseudo label for suspected anomalies. the VAE is parameterized with a sliding window size of 300, a Batch Size is 256, the learning rate of encoder is 2×10^{-4}, the learning rate of decoder is 5×10^{-4}, and training epochs is 100. In training, the data is divided into the first 50% as a training set and the second 50% as a test set.

4.3 Evaluation Protocol

The model is evaluated using Precision, Recall, and F1. The ability of the anomaly detector is commonly evaluated using three intuitive values of Precision, Recall, and F1, calculated as follows:

$$Precision = \frac{TP}{TP + FP} \tag{15}$$

$$Recall = \frac{TP}{TP + FN} \tag{16}$$

Table 2: Experimental results

	Precision	Recall	F1
Only SR	0.421484	0.634937	0.502558
No label	0.884259	0.677961	0.763001
Raw data	0.930353	0.927764	0.925267
All data	0.949551	0.976708	0.961638

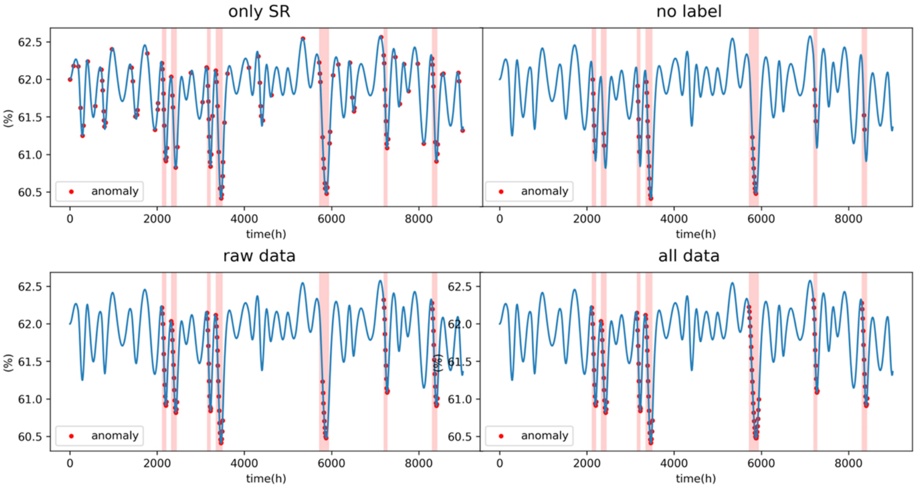

Figure 3: Visualization comparison

$$F1 = 2 \times \frac{precision \times recall}{precision + recall} \tag{17}$$

TP (True Positive) indicates the number of anomalies correctly detected by the anomaly detection model, FP (False Positive) indicates the number of normal data judged as anomalies by the detection model, FN (False Negative) indicates the number of anomalies judged as normal by the detection model, and TN (True Negative) indicates the number of normal data correctly detected by the anomaly detection model.

4.4 Results

The model was trained using the above dataset and the model anomaly detector was evaluated to validate the model's effectiveness. The model was divided into a Spectral Residual with a change threshold, a VAE model with unlabeled raw data input, a VAE model with the pseudo label raw data input, and a VAE model with different data and raw data with labeled input for comparison.

The experimental results are shown in Table 2.

Visualization comparison is shown in Figure 3.

The red background area is the actual anomaly region, and the red dots are the anomaly regions detected by the model.

When only SR, a large number of FP appears in the actual detection, resulting in a decrease in Precision. This is because the Spectral Residual algorithm labels all the dramatically changing regions of the data, and as an anomaly detector, it can effectively find anomalies. The number of true anomalies is lower than the number of labeled pseudo-anomalies, leading to more false positives.

Without the pseudo label, when using VAE as an unsupervised learning algorithm, multiple FNs occur, resulting in a decrease in Recall. This is because the portion of the raw data with anomalies significantly affects the VAE's modeling of normal operating status and will treat anomalies as normal. Insignificant anomalies will be ignored or the complete anomaly region won't be detected when it is used as an anomaly detector.

The raw data with pseudo-labeling input VAE model detects all anomalies but fails to detect the complete anomaly for the fifth one. The method proposed in this paper can detect all the anomalous regions, compared with just the raw data, using the difference data can detect the data change trend more effectively and detect the complete region of anomalies.

The precision, recall, and F1 value of the anomaly detection method presented in this paper are all 0.950. Perform at the highest level. Spectral Residual generated pseudo label, improved supervised VAE, and data difference have good results, and also show that the overall is better than using a particular model alone. By using the VAE model, the device's typical operation is established, and detection accuracy is improved. Using the pseudo label, which excludes the influence of anomaly regions on the modeling, improves the accuracy of the model. Using different data captures the variation trend more accurately and identifies a more complete anomaly region.

5 CONCLUSION

Anomaly detection is a part of computer Prognostics and Health Management, and this paper proposes a new data-driven embedded computer component anomaly detection method. This anomaly detection method achieves a precision of 0.950, a recall of 0.977, and an F1 value of 0.962. It can analyze the reliability and operation status of each component by extracting and modeling the key component parameters of the embedded computer. To achieve the Prognostics and Health Management of the embedded computer, to meet the needs of repair as necessary, and to improve the reliability and expected life of the embedded computer. In the subsequent analysis, it is found that there are interrelated characteristics between multiple components of the computer, and the interaction of each component, with the environment, can also lead to an anomaly, which affects the reliability and service life of each component and the computer. Therefore, to further investigate the correlation between the anomaly of each component and the impact on the reliability of the computer, it is necessary to collect the data of various vulnerable computer components and analyze and quantify their correlation.

REFERENCES

[1] CHAI Bo. 2018."Full life cycle reliability design assurance technology for military embedded computer" Beijing: China Aerospace publishing house.

[2] Maxion, R.A., and K.M.C. Tan. 2002. "Anomaly Detection in Embedded Systems." IEEE Transactions on Computers 51 (2): 108–20. https://doi.org/10.1109/12.980003.

[3] Zhang, Ying, and Krishnendu Chakrabarty. 2003. "Fault Recovery Based on Checkpointing for Hard Real-Time Embedded Systems." In Proceedings 18th IEEE Symposium on Defect and Fault Tolerance in VLSI Systems, 320–27. https://doi.org/10.1109/DFTVS.2003.1250127.

[4] Peti, P., R. Obermaisser, and H. Kopetz. 2005. "Out-of-Norm Assertions [Diagnostic Mechanism]." In 11th IEEE Real Time and Embedded Technology and Applications Symposium, 280–91. https://doi.org/10.1109/RTAS.2005.38.

[5] Zandrahimi, Mahroo, Alireza Zarei, and Hamid R. Zarandi. 2010. "A Probabilistic Method to Detect Anomalies in Embedded Systems." In 2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems, 152–59. https://doi.org/10.1109/DFT.2010.25.

[6] Mojarad, Roghayeh, Hossain Kordestani, and Hamid R. Zarandi. 2016. "A Cluster-Based Method to Detect and Correct Anomalies in Sensor Data of Embedded Systems." In 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), 240–47. https://doi.org/10.1109/PDP.2016.104.

[7] Mojarad, Roghayeh, and Hamid R. Zarandi. 2015. "Two Effective Anomaly Correction Methods in Embedded Systems." In 2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST), 1–6. https://doi.org/10.1109/RTEST.2015.7369849.

[8] Mojarad, Roghayeh, and Hamid R. Zarandi. 2017. "Comparison and Analysis of Three Anomaly Correction Methods in Embedded Systems." Scientia Iranica 24 (6): 3087–3100. https://doi.org/10.24200/sci.2017.4579.

[9] Wang, Yun, Bo Jing, Yifeng Huang, Xiaoxuan Jiao, Shenglong Wang, and Qinglin Liu. 2019. "Research of Equipment Fault Diagnosis Based on PHM High Performance Computing Platform." In 2019 Prognostics and System Health Management Conference (PHM-Qingdao), 1–6. https://doi.org/10.1109/PHM-Qingdao46334.2019.8942892.

[10] Sandborn, P. 2005. "A Decision Support Model for Determining the Applicability of Prognostic Health Management (PHM) Approaches to Electronic Systems." In Annual Reliability and Maintainability Symposium, 2005. Proceedings., 422–27. https://doi.org/10.1109/RAMS.2005.1408399.

[11] Lall, Pradeep, Madhura Hande, Chandan Bhat, and Jay Lee. 2011. "Prognostics Health Monitoring (PHM) for Prior Damage Assessment in Electronics Equipment Under Thermo-Mechanical Loads." IEEE Transactions on Components, Packaging and Manufacturing Technology 1 (11): 1774–89. https://doi.org/10.1109/TCPMT.2011.2160542.

[12] Kingma, Diederik P., and Max Welling. 2014. "Auto-Encoding Variational Bayes." arXiv. https://doi.org/10.48550/arXiv.1312.6114.

[13] Xu, Haowen, Wenxiao Chen, Nengwen Zhao, Zeyan Li, Jiahao Bu, Zhihan Li, Ying Liu, *et al.* 2018. "Unsupervised Anomaly Detection via Variational Auto-Encoder for Seasonal KPIs in Web Applications." In Proceedings of the 2018 World Wide Web Conference, 187–96. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee. https://doi.org/10.1145/3178876.3185996.

[14] Chen, Wenxiao, Haowen Xu, Zeyan Li, Dan Pei, Jie Chen, Honglin Qiao, Yang Feng, and Zhaogang Wang. 2019. "Unsupervised Anomaly Detection for Intricate KPIs via Adversarial Training of VAE." In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 1891–99. https://doi.org/10.1109/INFOCOM.2019.8737430.

[15] Kawachi, Yuta, Yuma Koizumi, and Noboru Harada. 2018. "Complementary Set Variational Autoencoder for Supervised Anomaly Detection." In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2366–70. https://doi.org/10.1109/ICASSP.2018.8462181.

[16] Lin, Shuyu, Ronald Clark, Robert Birke, Sandro Schönborn, Niki Trigoni, and Stephen Roberts. 2020. "Anomaly Detection for Time Series Using VAE-LSTM Hybrid Model." In ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 4322–26. https://doi.org/10.1109/ICASSP40776.2020.9053558.

[17] Akbari, Mohammad, and Jie Liang. 2018. "Semi-Recurrent CNN-Based VAE-GAN for Sequential Data Generation," June. https://doi.org/10.48550/arXiv.1806.00509.

[18] Liu, Yunxiao, Youfang Lin, QinFeng Xiao, Ganghui Hu, and Jing Wang. 2021. "Self-Adversarial Variational Autoencoder with Spectral Residual for Time Series Anomaly Detection." Neurocomputing 458 (October): 349–63. https://doi.org/10.1016/j.neucom.2021.06.030.

[19] Cheng-gang Wang, Xiao-dong Zhou, and Xue-wei Wang. 2010. "Testability Analysis for Complex Circuit Board Based on Fault Simulation and Rough Set." Microelectronics & Compute 27 (1): 131–34.

[20] YIN Zong-run, LI Jun-shan, SU Dong. 2014. "A Novelty Method for Bayesian Reliability Assessment of Electronic Equipment". Microelectronics & Computer, 2014, 31(6): 107-110.