Edge-based Analytics for Detecting Anomalies in Manufacturing Equipment

Akio Nakabayashi *1

The Internet of Things (IoT) technology enables the use of various data from manufacturing equipment, which used not to be possible with existing manufacturing execution systems. AI technology can help experts to execute their tasks by analyzing such data and identifying points to be improved or detecting anomalies in equipment for improving availability. However, most of the information infrastructure is not designed for the IoT and AI, and thus large amounts of informative data are not fully used. Yokogawa has therefore developed edge-based solutions that use computers near manufacturing equipment, in order to solve customer needs. While making full use of existing manufacturing execution systems, these solutions enable the construction of an IoT/AI system that analyzes data acquired in the field and transmits the analysis results to upper-level systems. This paper describes the technical points of Yokogawa's edge computing system that can detect anomalies in manufacturing equipment.

INTRODUCTION

Recently, manufacturing companies are facing serious problems in production, such as growing pressure for improving quality and reducing cost, amid increasingly fierce global competition. Moreover, many expert engineers are retiring and there are concerns about maintaining the capabilities of the remaining field workers. To overcome this situation, the Internet of Things (IoT), as well as analysis technologies including AI, machine learning, and statistics, are expected to innovate manufacturing operations. IoT technology has enabled the integration and use of various data from manufacturing equipment, such as detailed process data, which was not possible with existing systems. Meanwhile, AI technology is increasingly being used to help experts identify points to be improved or detect anomalies in equipment. However, most of the information infrastructure is not designed for the IoT and AI, and so, for example, vast amounts of sensing data on the vibration of mechanical systems is not fully collected in many sites with existing infrastructure.

An approach to resolving this situation is edge computing, in which some analysis is performed at the edge (near the equipment) and the results are then forwarded to upper-level systems. Edge computing enables large amounts of data to be analyzed using data infrastructure with limited resources.

Spotting this trend early, Yokogawa Electric Corporation has developed an edge-based solution, with the primary target of supporting equipment management tasks that are needed by users(1). By leveraging these solutions, Yokogawa Solution Service Corporation released in June 2018 the DUCSOnEX software package for detecting anomalies in manufacturing equipment.

This paper describes the technical background and outline of Yokogawa's edge-based solution for detecting anomalies.

*1 Incubation Department, Innovation Center, Marketing Headquarters

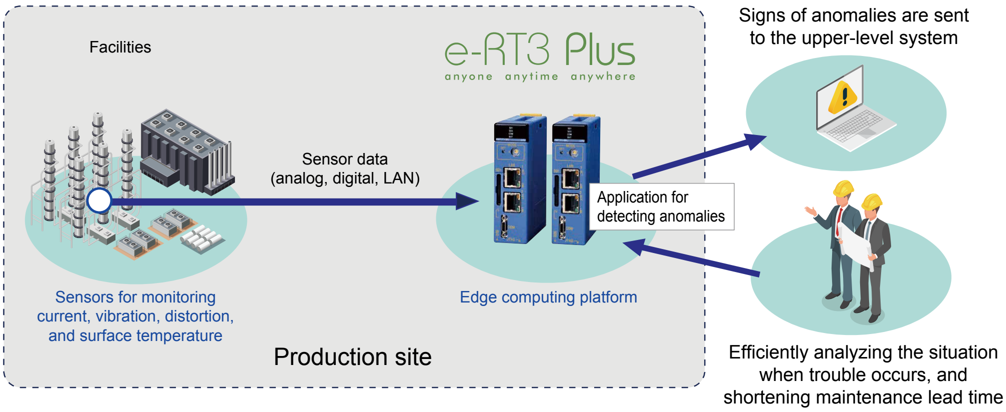

Figure 1 Conceptual diagram of batch analysis and online analysis

EDGE-BASED SOLUTION FOR DETECTING ANOMALIES

System Architecture

Figure 1 shows the architecture of the edge-based solution for detecting anomalies. The core of the system is the e-RT3 Plus edge computing platform and an application program for detecting anomalies installed on this platform. Various sensors can be connected to the e-RT3 Plus for monitoring manufacturing equipment. An edge analysis module in the anomaly-detecting application calculates various analytical values such as the degree of anomaly in sensor data. The degree of anomaly is an index for checking the normality of data, and is described in detail later. In general, the calculated analytical values are forwarded to upper-level systems using various communication protocols via the LAN interface of the e-RT3 Plus.

Configuration of Application for Detecting Anomalies

Many physical quantities, such as vibration and current, must be measured at high sampling rate to detect anomalies in manufacturing equipment. Recent progress in deep learning technology has enabled the direct analysis of raw data containing vast amounts of information. However, it is usually difficult to perform such analysis in edge devices because of limited computing resources, memory, and storage. Generally, for detecting anomalies, basic reference data (training data) are accumulated, then analyzed in batch processing mode for pattern learning. It is also difficult to accumulate training data in edge devices due to limited memory and storage. To overcome these challenges, Yokogawa took the following three approaches when developing its application for detecting anomalies: narrowing down the data to be analyzed, extracting features from sensor data, and online pattern learning without accumulating data. Figure 2 shows the logical configuration of this application.

The segment extraction block narrows down the data to be analyzed by clipping out segment data over a certain period of sampled sensor data. For example, data for a certain interval or period may be extracted as segment data in the case of continuously operating equipment. In the case of mechanical processing equipment, control signals can be used to extract segment data from batch processes.

The feature extraction block reduces the amount of data by transforming the entire segment data into several feature values (referred to as a feature vector), each of which represents the characteristics of the segment data. This transformation also facilitates the handling of problems such as variations in data length in the batch process and the phase difference arising from mismatched sampling start time.

Six types of feature extraction method are available on DUCSOnEX, embodying Yokogawa's expertise in offering

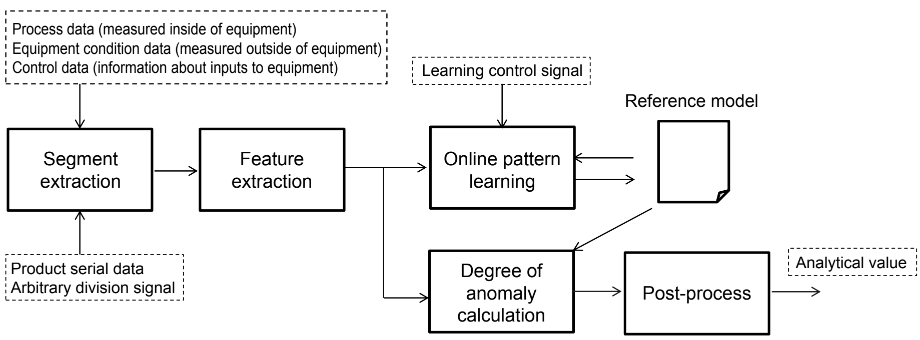

Figure 2 Configuration of anomaly-detecting application

analysis and consulting services to the manufacturing industry. These include feature extraction methods based on basic statistics and frequency analysis (FFT), which are combined to enable various types of equipment to be handled. Figure 3 shows an example of feature extraction based on basic statistics, in which a feature vector is composed of mean value, standard deviation, minimum value, and maximum value.

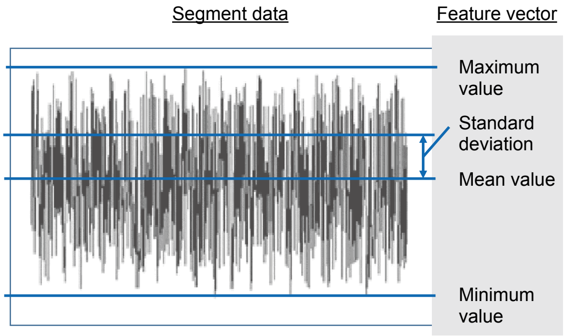

Figure 3 Example of feature extraction

When a feature vector is obtained, the online pattern learning block learns patterns calculated by the feature extraction block and generates models. Learning is performed only when the application user explicitly designates via learning signals. The details of learning are described later.

When the signal is not given, a newly input feature vector is not learned. Instead, the degree-of-anomaly calculation block quantifies the deviation of the feature vector from the model described above. This deviation is called degree of anomaly. A high degree of anomaly indicates that the feature vector, and thus the segment data, is different from the learned ones, and that the monitoring results of the equipment are changing.

Finally, the post-process block reduces the noise associated with sensing (including the variation due to external disturbances) by applying filters on the degree of anomaly and other analytical values.

We have developed a program that is optimized for the edge computing platform to perform the processes described above. These elements collaborate with each other to enable the application to detect anomalies.

ANOMALY DETECTION BASED ON ONLINE PATTERN LEARNING

The core analysis for anomaly detection is the learning of patterns of a data set that is considered to be normal. Batch-type pattern learning has been used in many industrial applications; its outline and anomaly detection based on it are described first, and then online (sequential processing) pattern learning, which is adopted in DUCSOnEX, is explained.

Batch-type Pattern Learning and Anomaly Detection

Figure 4 shows a learning data set example of two-dimensional feature vectors [x_1 x_2].

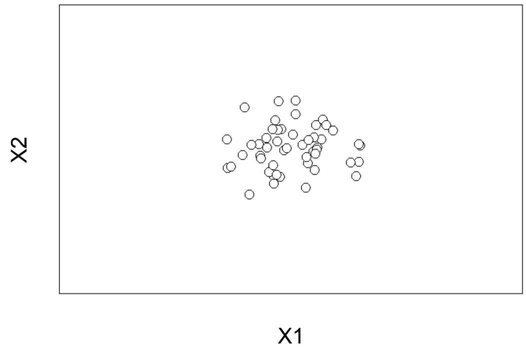

Figure 4 Example of data

Note that the feature vector is usually a set of several ten- to several thousand-dimensional data, depending on the equipment. From a statistical viewpoint, pattern learning means deducing from such data sets a function to estimate the occurrence probability of a data sample. That is, this function is a probabilistic model for the data.

For example, a simple probabilistic model can be constructed based on the assumptions of normality of feature vector occurrence and independence among the elements of feature vectors.

$$p(x_1, x_2) = N(x_1|\mu_1, s_1^2)N(x_2|\mu_2, s_2^2) \qquad (1)$$

where, N represents the probability density function of a normal distribution, and μ and s are the mean value and standard deviation parameters, respectively. Pattern learning based on this model is equivalent to estimating the mean value and standard deviation as the parameters of the normal distribution, which is given by Equation (2):

$$\mu_i = \frac{1}{T}\sum_t x_{t,i}\,,\; s_i^2 = \frac{\mathrm{T}}{\mathrm{T}-1}\left\{\frac{1}{\mathrm{T}}\sum_t x_{t,i}^2 - \mu_i^2\right\},\; \mathrm{i} = 1,2 \qquad (2)$$

where, t is a sample index and T is the number of samples of the feature vector. Note that all samples are referred to in the summation and that the parameters are estimated by batch processes on all samples.

This kind of probabilistic model estimates parameters for a given learning data set and shows a probability density for the feature vector. In other words, this model gives high values where data are expected to exist and low values otherwise.

Anomalies are detected by comparing this probability density with the ones under normal conditions. The degree of anomaly of data, as viewed from the model, is defined by the following equation:

$$\text{Degree of anomaly of data} \quad \propto -\ln p(x_1, x_2) \qquad (3)$$

Figure 5 shows a color map of the degree of anomaly for the model estimated based on the data of Figure 4.

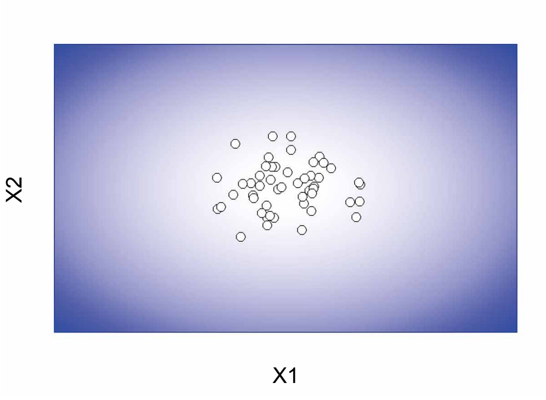

Figure 5 Example of the degree of anomaly calculated based on a stochastic model

In Figure 5, the part with higher values in Equation (3) appears darker, and the part with lower values is lighter. It is clear that the degree of anomaly becomes higher as it goes farther from the data.

Pattern learning and anomaly detection are carried out as described above when a learning set of feature vectors is given. As explained earlier, it is difficult to accumulate original data in edge computing systems. For this reason, Yokogawa adopted an online pattern learning algorithm, rather than batch-type pattern learning. This algorithm is described below.

Online Pattern Learning

The summation in Equation (2) is carried out over all samples to calculate the parameters of the normal distribution. Such calculated values required for estimating the stochastic model are called sufficient statistics.

Here, it is possible to calculate sufficient statistics for samples (1 to T) recursively by following Equation (4):

$$\begin{aligned} x_{sum,t} &= x_{sum,t-1} + x_t, \quad x_{sum,0} = 0 \\ x_{sum,t}^2 &= x_{sum,t-1}^2 + x_t^2, \quad x_{sum,0}^2 = 0 \end{aligned} \tag{4}$$

where, $x_{sum,t}$ and $x^2_{sum,t}$ are the sum and square sum of the feature vector at time t, respectively. The information required for calculating the sufficient statistics for the t-th sample is the sufficient statistics for the (t-1)-th sample and the value of the t-th sample. The sufficient statistics up to the T-th sample calculated by Equation (4) are identical with those calculated by Equation (2).

Therefore, there is no need to retain the entire data of feature vectors. With sufficient statistics, pattern learning can be performed when one sample is obtained. After updating the sufficient statistics, the feature vector used for pattern learning can be discarded. DUCSOnEX applies three types of online algorithms based on this scheme to pattern learning.

CONCLUSION

This paper outlined the core scheme of Yokogawa's edge-based anomaly detecting system.

Due to recent progress in IoT, the amount of data to be handled by manufacturing systems is increasing rapidly. Ideally, analyses would be performed using the entire data, but the investment in huge information infrastructure required to handle such vast amounts of data could not be justified because the return on investment is not clear at an early stage. The edge computing technology described in this paper enables quick and flexible introduction of IoT solutions with existing information infrastructure. Yokogawa will continue to research and develop edge-based analysis technology and expand its capabilities.

REFERENCES

(1) Tomohisa Shirai and Akio Nakabayashi, "Solution for Monitoring Signs of Anomalies in Facilities by Using Edge Computing," Keiso, Vol. 60, No. 3, 2017, pp. 14-17 (in Japanese)

* e-RT3 is a registered trademark of Yokogawa Electric Corporation.