OpenAIR @RGU
ROBERT GORDON UNIVERSITY ABERDEEN

This publication is made freely available under GREEN open access.

AUTHOR(S): MAJDANI, F., PETROVSKI, A. and DOOLAN, D.

TITLE: Designing a context-aware cyber physical system for smart conditional monitoring of platform equipment.

YEAR: 2016

Publisher citation: MAJDANI, F., PETROVSKI, A. and DOOLAN, D. 2016. Designing a context-aware cyber physical system for smart conditional monitoring of platform equipment. In Jayne, C. and Iliadis, L. (eds.) Communications in computer and information science, 629. Engineering applications of neural networks: proceedings of the 17th International conference on engineering applications of neural networks (EANN 2016), 2 - 5 September 2016, Aberdeen, UK. Cham: Springer [online], pages 198-210. Available from: https://doi.org/10.1007/978-3-319-44188-7_15

OpenAIR citation: MAJDANI, F., PETROVSKI, A. and DOOLAN, D. 2016. Designing a context-aware cyber physical system for smart conditional monitoring of platform equipment. In Jayne, C. and Iliadis, L. (eds.) Communications in computer and information science, 629. Engineering applications of neural networks: proceedings of the 17th International conference on engineering applications of neural networks (EANN 2016), 2 - 5 September 2016, Aberdeen, UK. Cham: Springer, pages 198-210. Held on OpenAIR [online]. Available from: https://openair.rgu.ac.uk

Publisher copyright statement:

This is the AUTHOR ACCEPTED version of proceedings originally published by SPRINGER and presented at the 17th International conference on engineering applications of neural networks (EANN 2016), 2 - 5 September 2016, Aberdeen UK. (ISBN 9783319441870; eISBN 9783319441887; ISSN 1865-0929).

The final publication is available at https://doi.org/10.1007/978-3-319-44188-7_15

OpenAIR takedown statement:

Section 6 of the "Repository policy for OpenAIR @ RGU" (available from http://www.rgu.ac.uk/staff-and-current-students/library/library-policies/repository-policies) provides guidance on the criteria under which RGU will consider withdrawing material from OpenAIR. If you believe that this item is subject to any of these criteria, or for any other reason should not be held on OpenAIR, then please contact openair-help@rgu.ac.uk with the details of the item and the nature of your complaint.

This publication is distributed under a CC BY-NC 4.0 license.

https://creativecommons.org/licenses/by-nc/4.0

OpenAIR at RGU

Digitally signed by OpenAIR at RGU DN: cn=OpenAIR at RGU, o=Robert Gordon University, ou=Library, email=publications@rgu.ac.uk, c=GB Date: 2017.06.06 09:44:59 +01'00'

Designing a Context-Aware Cyber Physical System for Smart Conditional Monitoring of Platform Equipment

Farzan Majdani[1], Andrei Petrovski[2] and Daniel Doolan[3]

[1] Robert Gordon University, School of Computing Science and Digital Media, Aberdeen, UK,
f.majdani-shabestari@rgu.ac.uk
[2] Robert Gordon University, School of Computing Science and Digital Media, Aberdeen, UK,
a.petrovski@rgu.ac.uk
[3] Robert Gordon University, School of Computing Science and Digital Media, Aberdeen, UK,
d.c.doolan@rgu.ac.uk

Abstract. An adaptive multi-tiered framework, which can be utilised for designing a context-aware cyber physical system is proposed and applied within the context of assuring offshore asset integrity. Adaptability is achieved through the combined use of machine learning and computational intelligence techniques. The proposed framework has the generality to be applied across a wide range of problem domains requiring processing, analysis and interpretation of data obtained from heterogeneous resources.

Keywords: Context Awareness, Cyber Physical System, Asset integrity

1 INTRODUCTION

There exists a growing demand for intelligent and autonomous control in engineering applications. This is especially true when some constraints are present that cannot be satisfied by human intervention with regard to decision making speed in life threatening situations (e.g. automatic collision systems, exploring hazardous environments, processing large volumes of data). Because machines are capable of processing large amounts of heterogeneous data much faster and are not subject to the same level of fatigue as humans, the use of computer-assisted control in many practical situations is preferable. Cyber physical systems are the integration of information processing, computation, sensing and networking that allows physical entities to operate various processes in dynamic environments [5]. Many of these intelligent cyber physical systems involve human intervention at some point, either during the development process by embedding expert knowledge into the systems, or during operation by requiring humans to monitor, evaluate, and confirm/reject the systems inferences. The latter type of intervention is often associated with another salient feature of cyber physical systems dealing with the big data phenomenon. Big data has become a common research focus in the last decade due to the increasing volume, velocity, variety and veracity of data enabled by technological advancements and by a reduction in data acquisition costs. The integration of multiple data sources into a unified system leads to data heterogeneity, often resulting into difficulty, or even infeasibility, of human processing, especially in real-time environments. For example, in real-time automated process control, information about a possible failure is more useful before the failure takes place so that prevention and damage control can be carried out in order to either completely avoid the failure, or at least alleviate its consequences. Computational Intelligence (CI) techniques have been successfully applied to problems involving big data in various application domains [4]. These techniques however require training data to provide reliable and reasonably accurate specification of the context in which a cyber physical system operates. The context enables the system to highlight potential anomalies in the data so that intelligent and autonomous control of the underlying process can be carried out. Anomalies are defined as incidences or occurrences, under a given circumstances or a set of assumptions, that are different from the expectance (for instance when Generator rotor speed of the gas turbine goes below 3000 rpm). By their nature, these incidences are rare and often not known in advance. This makes it difficult for the Computational Intelligence techniques to form an appropriate training dataset. Moreover, dynamic problem environments can further aggravate the lack of training data by occurrence of intermittent anomalies. Computational Intelligence techniques that are used to tackle dynamic problems should therefore be able to adapt to environmental/contextual changes. A multi-tiered framework for cyber physical systems with heterogeneous input sources is proposed in the paper that can deal with unseen anomalies in a real-time dynamic problem environment. The goal is to develop a framework that is as generic, adaptive and autonomous as possible. In order to achieve this goal both machine learning and computational intelligence techniques are applied within the framework, together with the online learning capability that allows for adaptive problem solving.

2 CYBER PHYSICAL SYSTEMS (CPS)

Rapid advances in miniaturisation, speed, power and mobility have led to the pervasive use of networking and information technologies across all economic sectors. These technologies are increasingly combined with elements of the physical worlds (e.g. machines, devices) to create smart or intelligent systems that offer increased effectiveness, productivity, safety and speed [5]. Cyber physical systems (CPS) are a new type of system that integrates computation with physical processes. They are similar to embedded systems but focus more on controlling the physical entities rather than processes embedded computers monitor and control, usually with feedback loops, where physical processes affect computations and vice versa. Components of cyber physical system (e.g., controllers, sensors and actuators) transmit the information to cyber space through sensing a real world environment; also they reflect policy of cyber space back to the real world [7]. Rather than dealing with standalone devices, cyber physical systems are designed as a network of interacting elements with physical inputs and outputs, similar to the concepts found in robotics and sensor networks. The main challenge in developing a CPS is to create an interactive interface between the physical and cyber worlds the role of this interface is to acquire the context information from the physical world and to implement context-aware computing in the cyber world [6].Figure 1 illustrates a conceptual framework for building context-aware cyber physical systems [9]. Each layer is dedicated to a certain context processing task, ranging from low-level context acquisition up to high level context application using either existing or acquired knowledge. Cyber physical systems may

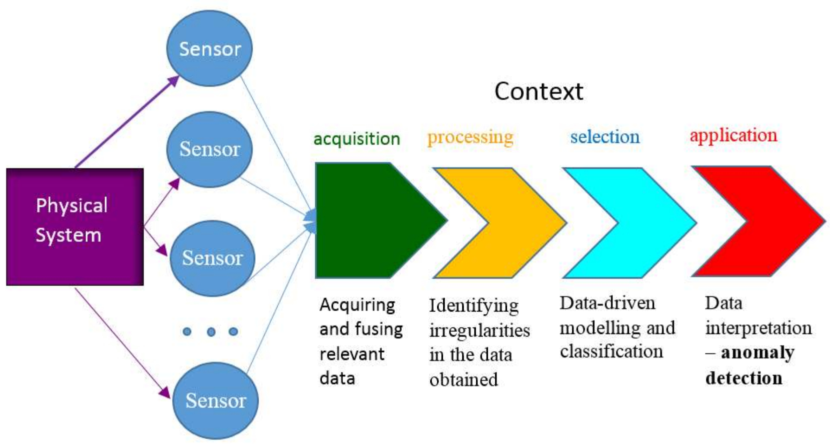

Fig. 1. Framework for designing context-aware CPS

consist of many interconnected parts that must instantaneously exchange, parse and act upon heterogeneous data in a coordinated way. This creates two major challenges when designing cyber physical systems: the amount of data available from various data sources that should be processed at any given time and the choice of process controls in response to the information obtained. An optimal balance needs to be attained between data availability and its quality in order to effectively control the underlying physical processes. Figure 2 illustrates a systematic approach to handling the challenges related to context processing, which has been successfully applied by the authors to various real world applications [8, 9]. As can be seen from Figure 2, the suggested approach segregates processing of the input stream into three distinct phases. The Processing minimises the volume of data and the data processing cost by analysing only inputs from easy to process data sources using context identification techniques for finding anomalies

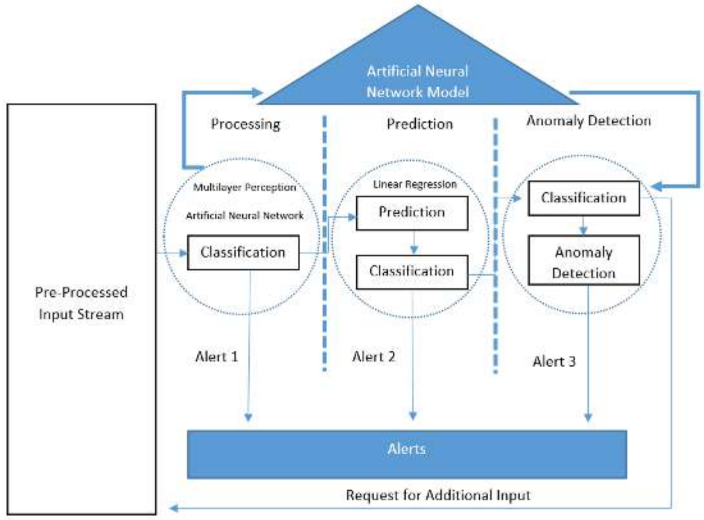

Fig. 2. Systematic approach to context processing

in the acquired data. If any anomalies are detected at this stage, Alert 1 gets activated. This phase of the process is used to analyse real-time data and is a safe guard process on scenarios where the frameworks prediction fail to predict occurrence of unexpected changes in the environment. In the Prediction Phase, future values of each of the gas turbine's sensors get predicted, using a linear regression model. Moreover a new column is added which gets populated with the "predicted status" value for each data instance. In this phase if any of the future predicted value of the sensors goes beyond the set threshold, Alert 2 gets activated. The final step of the process Anomaly Detection, classifies the overall predicted future values to identify anomalies being present in the underlying process on the operation of the cyber physical system. If any anomalies are detected at this stage Alert 3 is triggered. Such an approach allows for the acquisition of data and/or activation of the necessary physical entities on an ad-hoc basis, depending on the outcome at each phase. Moreover, the accuracy attained at the specified phases can be enhanced by incorporating additional data sensors or additional environmental factors. Computational intelligence techniques and expert systems have been successfully applied to tackling many anomaly detection problems, where anomalies are known a priori. More interesting, however, is to detect previously unseen anomalies. Statistical analysis and clustering are examples of techniques that are commonly used when the characteristics of anomalies are unknown [1]. Figure 3 illustrates a more detailed process for the systematic approach where machine learning and computational intelligence techniques are combined to tackle the unknown anomalies and learn from the experience when similar anomalies occur again. In Figure 3, "b" represents a belief function of the

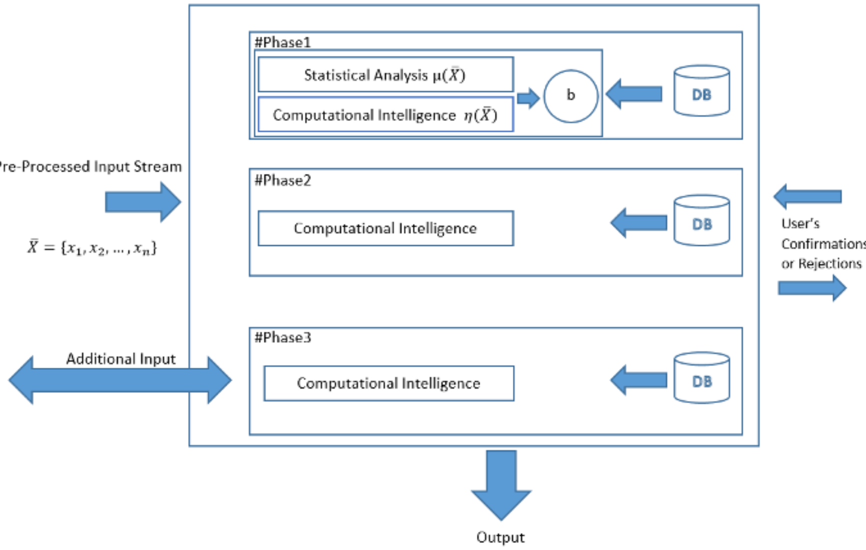

Fig. 3. Context Processing in a CPS

output from both the statistical analysis and computational intelligence nodes, such that

$$f(t) = \sum_{i=1}^{n} w_i \mu_i(\overline{X}) + \sum_{j=1}^{m} w_j \eta_j(\overline{X}) \tag{1}$$

The weights (w_i and w_j) of this belief function are adaptively adjusted depending on how much knowledge related to the problem context has been obtained. The contribution of the CI nodes increases with collection of more normal and abnormal data points that can be used for training. This allows the system to run autonomously if required, and any potential anomalies are flagged for closer inspection at the second (i.e. classification) phase. With the use of parallelisation and/or distributed systems, multiple machine learning and CI techniques and various belief functions can be evaluated simultaneously with their parameters being adaptively chosen. Anomaly identification using a combination of such techniques, as described in Figure 3, has been successfully applied to a traffic surveillance application [9], a smart home environment and automotive process control [8].

3 EXPERIMENTAL RESULTS

3.1 DATA DESCRIPTION

It is a common practice that most of the sensory data on a platform are stored in a historian system such as the PI system. PI is a form of historian system which act as a repository to store sensor information gathered from one or multiple installation. For this study we used historical sensor data of a gas turbine from an offshore installation in the North Sea. This data in real-time is transmitted offshore via satellite Internet. In this experiment about three months worth of

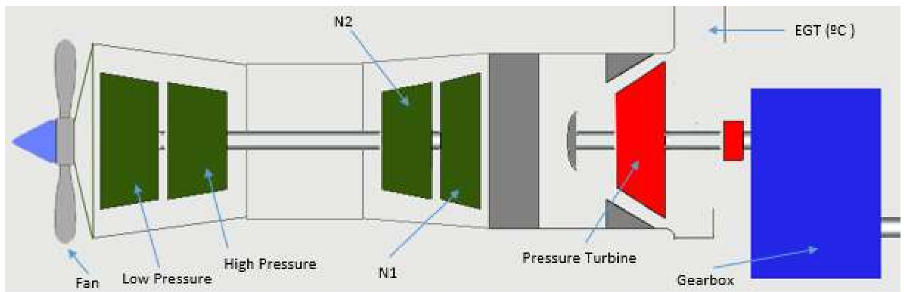

Fig. 4. Gas Turbine Process Design

data from a PI historian representing a total of 25 sensors from different parts of a gas turbine was used (see Figure 4).Within this period system experienced 8 failures which are highlighted in Figure 5) which are indicated by blue arrows. The sample data for the three months period includes around 217000 instances. Sensor used from the turbine are listed in Table 1. In addition to all the sensors we also had a turbine status which has each of the instances of the dataset labeled as either False, True or I/O timed out. False indicates the turbine failure state, True indicates the engine is running and I/O Timed out indicates when the engine is getting restarted or communication between the Pi historian and offshore is temporarily lost. The importance of having the I/O Timeout state is to prevent the system from sending an alarm when the system is actually in a state of reboot but not a failure.

3.2 PROCESSING

The processing Phase of the proposed context-aware CPS implements computational intelligence to classify the input stream. To implement this Phase the Multilayer Perceptron is used, which is a feedforward Artificial Neural Network (ANN). Funahashi[2], Hoenike and Stunchcombe [3] and Qiu et al [11] have all shown that only one hidden layer can effectively generate highly accurate results by also improving the processing time. Therefore an ANN Multilayer Perceptron with Backpropagation of error has been used to train the machine with 1, 2, 3 and 4 hidden layers 10 fold cross validation. The experiment had been continued up until 4 layer which eventually generated an excellent result. Table 3 lists the result gathered from the experiments with 1 to 4 hidden layers. Although by using only one hidden layer we have managed to classify 92.77 percent of the

Sensor Description	Unit	Count
Power Turbine Rotor Speed	rpm	2
Gas Generator Rotor Speed	rpm	2
Power Turbine Exhaust Temperature	F	6
None Drive End Direction	mm/SEC	1
Drive End Vibration X Direct	um P-P	1
Turbine Inlet Pressure	psia	1
Compressor Inlet Total Pressure	psia	1
Ambient Temperature	F	1
Axial Compressor Inlet Temperature	F	2
Mineral Oil Tank Temperature	F	1
Synthetic Oil Tank Temperature	F	1
OB Bearing Temperature	C	1
IB Bearing Temperature	C	1
IB Thrust Bearing Temperature	C	1
OB Thrust Bearing Temperature	C	1
Generator Active Power	Mwatt	1
Grid Voltage	V	1

Table 1. Gas Turbine Sensors

instances correctly, however by increasing the layers to 4 we have managed to classify 100 percent of the instances. Figure 6 illustrated the artificial neural network design. The input layer corresponds to the 25 input sensors of the gas turbine. The middle layers are used to form the relations between the neurons, their number being determined at runtime. The output neurons are the three classifications which indicates the status of the turbine.

3.3 PREDICTION

The second phase of the proposed model is Prediction Phase, which is to predict the future values for the next 24 hours of all 25 sensors. Times series was used to lag the data for 24 hours followed with linear regression to predict the next 24. During this phase by looking at the historical data we have already set threshold for each of the sensors. Therefore if any of the predicted values for each of the sensors falls below or beyond the allowed threshold then Alarm 2 gets activated. Figure 7 illustrates the predicted results for all the 25 sensors.

3.4 ANOMALY DETECTION

Since combination of all the sensors together reflect the status of the turbine, after predicting future value of all the sensors then all get merged into a single test dataset. The Artificial Neural Network model which has been trained as part of the Processing phase is used again, but this time to label the status of

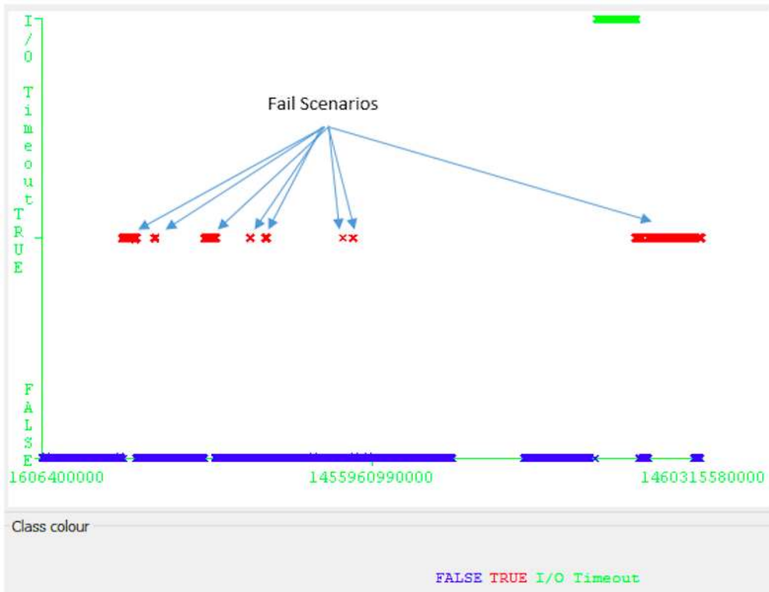

Fig. 5. Turbine's Fail Scenarios

Layers Count	One	Two	Three	Four
Correctly Classified (%)	92.77	92.77	94.95	100
Incorrectly Classified (%)	7.23	7.23	5.05	0
Kappa statistic	0.60	0.60	0.74	1
Mean absolute error	0.09	0.09	0.062	0
Root mean squared error	0.21	0.21	0.17	0
Relative absolute error (%)	57.32	57.79	39.10	0.34
Root relative squared error (%)	74.89	74.97	62.71	0.77
Coverage of cases (0.95 level) (%)	100	100	100	100
Mean rel. region size (0.95 level)	4.65	64.65	55.25	33.33

Table 2. ANN Multilayer Perceptron Optimisation

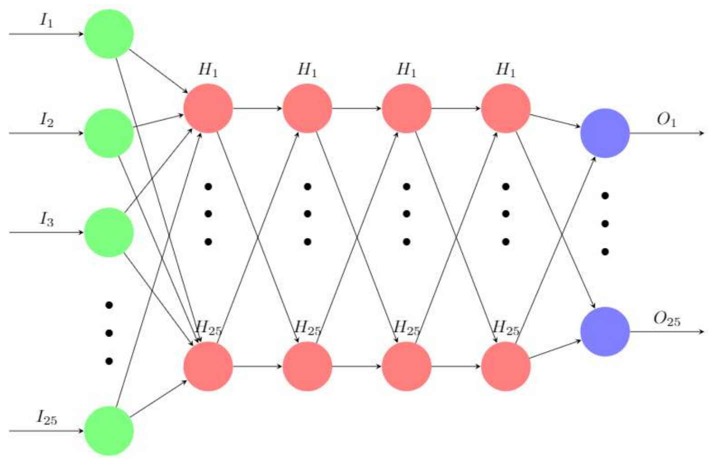

Fig. 6. ANN Multilayer Perceptron Proposed Model

the turbine for each of the instances. After predicting the status of the turbine for all instances of the dataset, the developed framework iterate through all labels and if any of the instances are labeled as failed Alarm 3 gets fired. System then picks the time stamp of the predicted time and deduct it from the current time to provide the estimated hours left until the system failure. In final step of the Anomaly Detection phase the total remainder hours gets included into an automatically generated email and sent out to the preset list of email addresses as well as playing an audio alarm on the PC.

3.5 OVERALL AUTOMATED PROCESS

Initially Weka was used to run each of the phases separately. However in the final stage of the process we have actually formed the proposed framework using Knime. Knime is an open source data analytics, reporting and integration platform. Although there are other alternatives such as Weka's KnowledgeFlow and Microsoft Azure's Machine Learning. Knime was chosen since it has the capability of importing most of Weka's features through the addition of a plugin. Also being able to run java snippets and write the developed model into disk to free up space on memory it is a preferred option in comparison to Azure's Machine Learning. The dataset was divided into two sets of training and test data as illustrated in Figure 8. Two months of data was used for training which included 8 cases of turbine failure with the remainder set aside for testing. The training dataset has been used to form an Artificial Neural Network Multilayer Perceptron (MLP) using Backpropagation of error. MLP is multilayer perceptron consists of multiple layers of artificial neurons which interact using weighted connections [10]. After training the model it was tested against the developed ANN MLP to classify the status of the engine. This implementation covered the

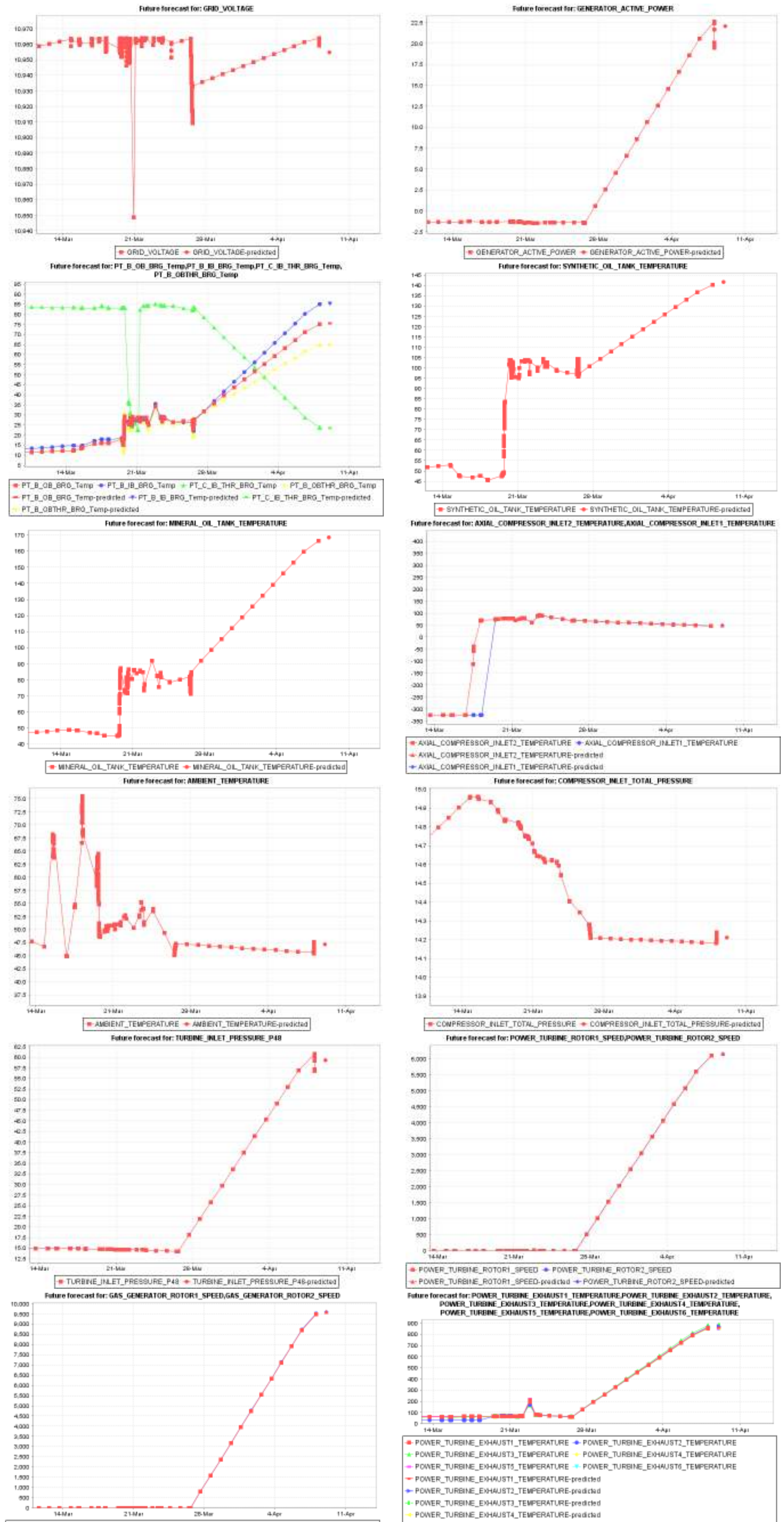

Fig. 7. Predicted Sensor values

Processing phase of the proposed Cyber Physical System. This was followed by introducing times series lag and linear regression model to predict the next 24 hours on the test dataset. By looking at the 8 failure situations thresholds were identified for each of the input sensors. Therefore if during the prediction stage any of the sensor's value go below or above the set threshold the second Alarm goes off. However this alarm is an amber rated alarm because that doesn't mean necessarily the turbine will fail. With all 24 hours of predicted data for all the sensors gathered, in the final stage of the process all the predicted data is put together as a test dataset and is tested against the model developed in Processing Phase. If the status of the engine gets classified as False then the third and last alarm gets fired.

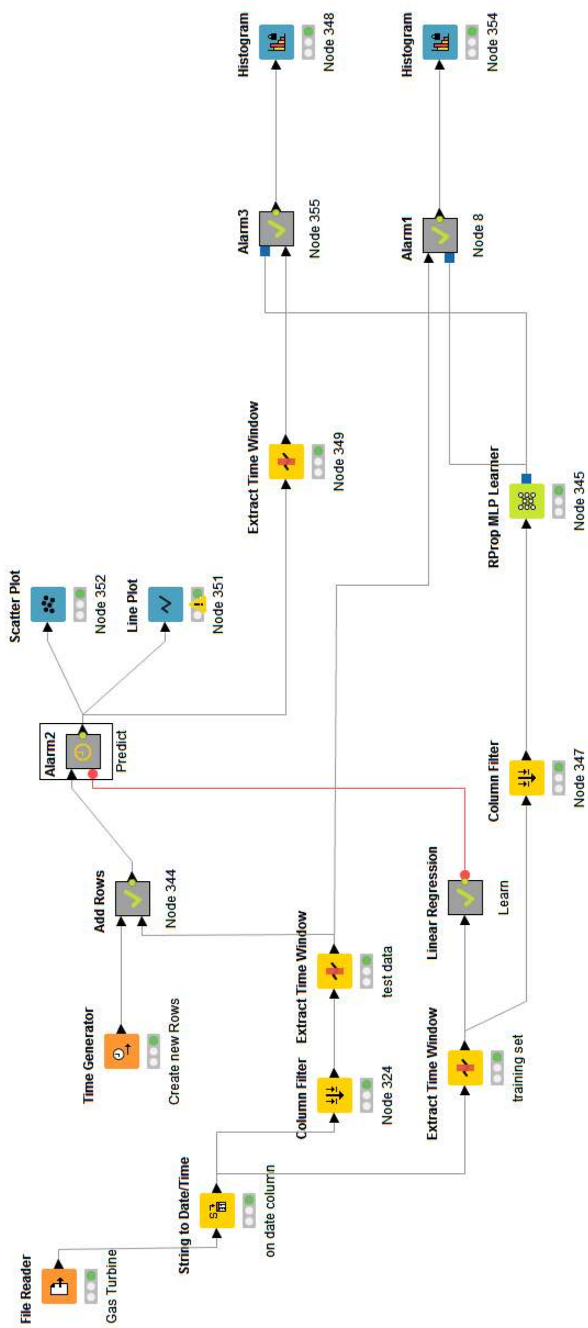

Fig. 8. Overal Automated Framework of the Process

3.6 EVALUATION

To test the accuracy and performance of the proposed model, 5 days worth of data was removed from the dataset and the developed model used to predict each of eliminated days hourly. To achieve this, performance of the turbine for the next 1, 3, 6, 9, 12, 14, 16, 18 and 24 hours for each days has been predicted. Then the average performance for all these 5 days has been calculated. The

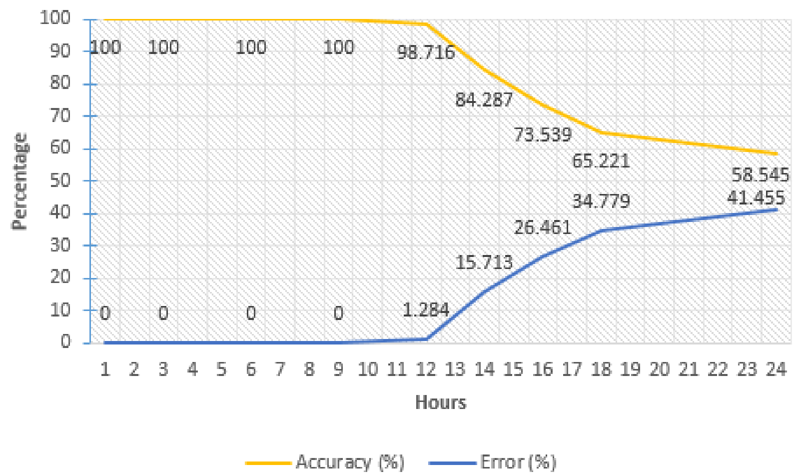

Fig. 9. Hourly performance evaluation

Hours	Accuracy (%)	Error (%)
	100	0
3	100	0
6	100	0
9	100	0
12	98.716	1.284
14	84.287	15.713
16	73.539	26.461
18	65.221	34.779
24	58.545	41.455

Table 3. Comparison of real-time Status vs. Predicted Status

average performance shows up until 12 hours system could predict the status of the turbine with nearly 99 percent accuracy which is a reasonably high performance. Even for the 16 hour period, prediction was around 73 percent which is still considered to be high performance. However after 18 hours the prediction performance shows sudden declines and when it gets to prediction of the next 24 hours the result is really poor by being around 58 percent. Table 3 lists the average value of the result for each prediction.

4 CONCLUSION

An implementation of a Context-Aware Cyber Physical System using Multilayer Perceptron Artificial Neural Network, to predict the status of a gas turbine on an offshore installation has been successfully developed. In this experiment a three phased model has been proposed. In the processing phase, historical data of 25 sensors was collected from different areas of turbine to train an Artificial Neural Network model as the basis of the prediction model. In the second phase future value of each sensor has been predicted for a certain period of time using linear regression. The final phase makes use of the model developed in phase one to label the predicted data to detect anomalies prior to their occurrence. The model developed proved to be capable of highly accurate predictions of gas turbine status up to 16 hours in advance with the accuracy of about 73 percent. Further research will focus on extending the prediction time frame by assuring high accuracy in anomaly identification through exploring various combinations of computational intelligence techniques with conventional classification approaches

References

1. Chandola, V., Banerjee, A., and Kumar, V. 2009. Anomaly detection: A survey. ACM Computing Surveys. 41,3 (September 2009), 1-72.
2. FUNAHASHI, K., 1989. On the approximate realization of continuous mappings by neural networks. Neural Networks, 2(3), pp. 183-192
3. HORNIK, K., STINCHCOMBE, M. and WHITE, H., 1989. Multilayer feedforward networks are universal approximators. Neural Networks, 2(5), pp. 359-366
4. Khan, Z., Shawkat Ali, A. B. M., and Riaz, Z., Eds. 2014. Computational Intelligence for Decision Support in Cyber-Physical Systems. Springer, 2014.
5. Lee, E. A. 2008. Cyber physical systems: design challenges. University of California, Berkeley Technical Report No. UCB/EECS-2008-8, January 2008.
6. Lun, Y., and Cheng, L. 2011. The research on the model of the context-aware for reliable sensing and explanation in cyber-physical system. In Procedia Engineering. 15 (2011), 1753-1757.
7. Park, K. J., Zheng, R., and Liu, X. 2012. Cyber-physical systems: Milestones and research challenges. Computer Communications. 36,1 (December 2012), 1-7.
8. Petrovski, S., Bouchet, F., and Petrovski, A. 2013. Data-driven Modelling of Electromagnetic Interferences in Motor Vehicles Using Intelligent System Approaches. In Proc. IEEE Symposium on Innovations in Intelligent Systems and Applications (INISTA). 2013, 1-7.

9. Rattadilok, P., Petrovski, A., and Petrovski, S. 2013. Anomaly monitoring framework based on intelligent data analysis. Intelligent Data Engineering and Automated Learning (IDEAL 2013), Lecture Notes in Computer Science. 8206 (2013) 134-141.
10. PAL, S.K. and MITRA, S., 1992. Multilayer perceptron, fuzzy sets, and classification. Neural Networks, IEEE Transactions on, 3(5), pp. 683-697
11. QIU, M., SONG, Y. and AKAGI, F., 2016. Application of artificial neural network for the prediction of stock market returns: The case of the Japanese stock market. Chaos, Solitons Fractals, 85, pp. 1-7