FN-DFE: Fuzzy-Neural Data Fusion Engine for Enhanced Resilient State-Awareness of Hybrid Energy Systems

D. Wijayasekara, *Student Member, IEEE*, O. Linda, *Member*, *IEEE*, M. Manic, *Senior Member, IEEE*, C. Rieger, *Senior Member, IEEE*

***Abstract*— Resiliency and improved state-awareness of modern critical infrastructures, such as energy production and industrial systems, is becoming increasingly important. As control systems become increasingly complex, the number of inputs and outputs increase. Therefore, in order to maintain sufficient levels of state-awareness, a robust system state monitoring must be implemented that correctly identifies system behavior even when one or more sensors are faulty. Furthermore, as intelligent cyber adversaries become more capable, incorrect values may be fed to the operators. To address these needs, this paper proposes a Fuzzy-Neural Data Fusion Engine (FN-DFE) for resilient state-awareness of control systems. The designed FN-DFE is composed of a three-layered system consisting of: 1) traditional threshold based alarms, 2) anomalous behavior detector using self-organizing fuzzy logic system, and 3) artificial neural network based system modeling and prediction. The improved control system state-awareness is achieved via fusing input data from multiple sources and combining them into robust anomaly indicators. In addition, the neural network based signal predictions are used to augment the resiliency of the system and provide coherent state-awareness despite temporary unavailability of sensory data. The proposed system was integrated and tested with a model of the Idaho National Laboratory's (INL) hybrid energy system facility known as HYTEST. Experimental results demonstrate that the proposed FN-DFE provides timely plant performance monitoring and anomaly detection capabilities. It was shown that the system is capable of identifying intrusive behavior significantly earlier than conventional threshold based alarm systems.**

***Index Terms*— Artificial Neural Networks, Data Fusion, Fuzzy Logic Systems, Resilient Control Systems, State-Awareness**

I. Introduction

RESILIENCY and enhanced state-awareness are highly desirable properties of modern control systems. It is of paramount importance that critical infrastructures, such as energy production and industrial systems, are equipped with intelligent components for timely reporting and understanding of the status and behavioral trends of the control system. This goal can be achieved via complex system monitoring, real-time system behavior analysis and timely reporting of the system state to the responsible human operators [1]. Here, the enhanced state-awareness is understood as set of diverse performance criteria such as cyber or intelligent analysis that is used to maximize the adaptive capacity of the system to respond to threats.

As modern control systems become increasingly complex, operators rely on multiple heterogeneous sensors located at various different locations, to understand system behavior. If one or more sensors or communication pathways are disrupted critical system information maybe lost which leads to a lowered state-awareness. Therefore, in order to maintain complete state-awareness in such situations, various different component based methodologies are implemented such as redundancy. Similarly, as intelligent cyber adversaries become more and more capable and motivated, sensor "spoofing" maybe done to mask intrusion activities, where sensor values are manipulated before it is sent to the user. Such methodologies can be used to disrupt critical systems while keeping the system operators in the dark. This also leads to a reduced state-awareness of system operators.

However, in these types of scenarios, advanced data-fusion techniques can be used. Data fusion techniques combine information from multiple heterogeneous sources, and utilize the inherent interdependencies within the data as well as system knowledge to achieve better understanding and thus improved state-awareness, than those achieved by a single sensor alone [2]-[7].

To address these issues, this paper proposes a novel architecture of Fuzzy-Neural Data Fusion Engine (FN-DFE) for increased state-awareness of resilient control systems [7]. The main purpose of the FN-DFE is to provide real-time monitoring and analysis of complex critical control systems. The improved control system state-awareness is achieved via fusing input data from multiple sources and combining them into robust system modeling methodologies and anomaly indicators. These anomaly indicators are then delivered to the operator via a Human Machine Interface (HMI). The proposed robust state-awareness architecture is based on the previously proposed anomaly detection methodology for advanced

This work was supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

D. Wijayasekara, O. Linda and M. Manic are with the Computer Science Department, University of Idaho, Idaho Falls, ID 83402 USA (e-mail: olindaczech@gmail.com, dumidu.wijayasekara@gmail.com, misko@ieee.org).

C. Rieger is with the Idaho National Laboratory, Idaho Falls, ID 83402 USA (e-mail: craig.rieger@inl.gov)

control systems [7]. The proposed FN-DFE architecture uses Computational Intelligence (CI) algorithms such as Artificial Neural Networks (ANN) and Fuzzy Logic Systems (FLS) for system behavior modeling, prediction and anomaly detection [8]-[12].

The proposed FN-DFE architecture consists of a dedicated data fusion module for each individual unit of the control system. Each module implements a three-layered system behavior monitoring system consisting of: 1) traditional threshold based alarms, 2) anomalous behavior detector using Self- Organizing Fuzzy Logic System (SOFLS), and 3) Artificial Neural Network (ANN) based control system modeling and behavior prediction. Both the SOFLS and the ANN predictor are trained offline on a set of recorded normal behavior data. The SOFLS is used to learn fuzzy rules that describe this normal behavior data. During the testing phase, individual fuzzy rules calculate the degree of similarity of the observed behavior with the previously known normal behavior patterns. The feed-forward ANN is used to forecast the future measurements for each sensor based on the previously observed history. This ANN based signal forecasting layer is used to augment the resiliency of the system and to provide coherent state-awareness in case of temporally unavailable sensory data. Furthermore, the predicted measurements are then retrospectively matched to the true observation and the prediction error is fused into a robust anomaly indicator using a fuzzy logic controller.

The rest of the paper is organized as follows. Section II briefly describes related work. Section III provides high-level overview of the FN-DFE's three-layered architecture. Section IV descries the implemented threshold based alarm system. Section V discusses the SOFLS based anomaly detection. Section VI focuses on the behavior prediction using artificial neural networks including the fuzzy logic based alarm generation. Finally, Section VII presents experimental results and the paper is concluded in Section VIII.

II. Related Work

Early work related to CI-based nuclear power plant modeling shows the possibility of utilizing methodologies such as ANN to model plant behavior accurately [13], [14]. However, these works only focused on predicting very small number of dimensions and used low complexity models.

Fuzzy logic has been previously used for monitoring sensory data and alarm processing in nuclear power plants in [15]-[19]. ANNs have been applied to nuclear reactor monitoring in [15], [16]. In [22], the fusion of Support Vector Machines (SVM) and Adaptive Neuro-Fuzzy Inference System (ANFIS) was used for fault detection and diagnosis in industrial steam turbines.

Many other related CI-based approaches for plant monitoring can be found in literature. However, most of the approaches in literature focus on alarm generation and fault diagnosis.

ANNs have been widely used for alarm detection and fault identification in nuclear power plants [23]. The authors use ANN to identify and classify transient behavior in nuclear power plants using ANN in [24]. In [23] the authors used ANN to identify previously seen and unseen malfunctions in nuclear power plants. Hadad et al. used optimized ANN architectures for fault diagnosis and dynamic fault identification [25]. Similar online fault diagnosis method using ANN for nuclear power plants was proposed in [26]. Fuzzy logic based fault diagnosis methodologies have also been proposed in literature [27].

The cyber-security of critical infrastructure control systems was also analyzed using fuzzy logic and artificial neural networks in [28], [29]. However, cyber-security aspect is mostly focused on network traffic analysis and other such methods to identify intrusions. In [30] the authors proposed a intrusion detection system by means of system state monitoring. The system proposed in [30] utilizes previously described system states and identifies system deviations for intrusion detection.

An ANN based sensor validation architecture was proposed in [31] and was tested on EBR-II reactor simulation. In [32], a novel HyBUTLA algorithm for learning the behavior of hybrid (discrete and continuous) systems was used for identification of behavior models of industrial production processes. A pre-alarm system where alarms are generated to alert system operators of probable future changes in the system was proposed in [33].

Very little work has been focused on robust state-awareness schemes for operators of large scale systems using CI-based methodologies. Similarly, intrusion detection systems proposed are largely focused on network traffic monitoring or rely on identifying intruders by means of monitoring system behavior via sensors. Furthermore, majority of the previously published work was applied to small scale systems. In the presented work, the developed FN-DFE was integrated with a model of the INL's hybrid energy testing facility called HYTEST [34], [35].

III. Fuzzy-Neural Data Fusion Engine – FN-DFE Architecture

This section provides a high level overview of the proposed FN-DFE architecture. This architecture is depicted in Fig.1. The system consists of three main blocks: knowledge base, online processing and system state identification. The knowledge base block is constructed offline based on the acquired normal training data and is used as a normal behavior model for on-line anomaly detection. The online processing block analyzes the incoming stream of sensory measurements. The input measurements are passed through a sequential three-layered anomaly detection system. Finally, the full system behavior is identified and forwarded to the user interface.

The first layer of the anomaly detection systems consists of known thresholds on the normal operating conditions. When the incoming measurements reach outside the normal behavior interval, an alarm is immediately reported. The second layer consists of SOFLS, which is trained offline to model the previously observed normal behavioral patterns. The online processing engine interprets each fuzzy rule of the FLS as a similarity measure between the current plant behavior and the

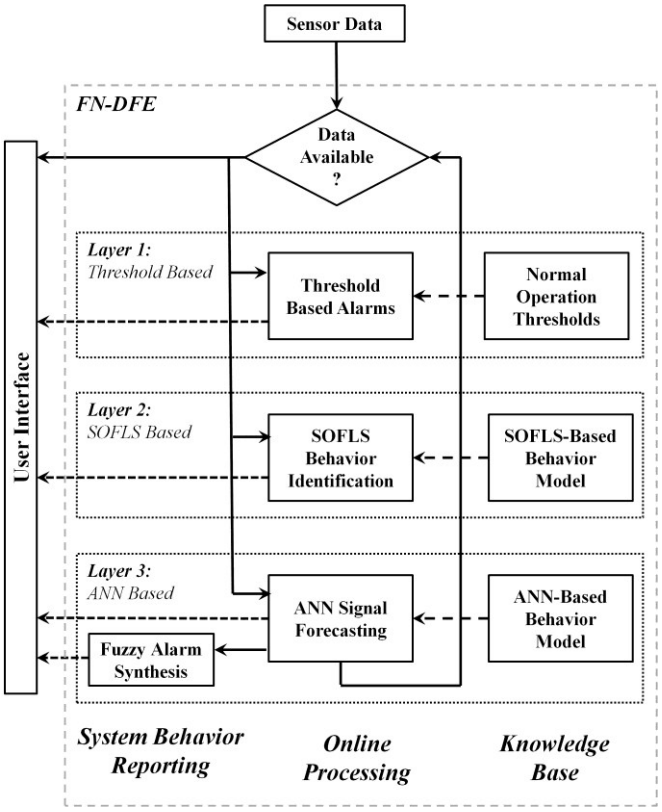


Fig. 1 Architecture of the proposed FN-DFE.

previously observed normal patterns. The third layer of the FN-DFE consists of ANN based behavior predictor, which processes the temporary previous history of plant's behavior and predicts the expected near future behavioral patterns. In case of temporary unavailability of sensory measurements, the ANN predicted future values are used instead of the missing values to maintain coherent state awareness of the system.

Thus for a given time-step, the available sensor data, or the predicted values are sent to each of the 3 layers simultaneously. If an alarm is produced at any of the 3 layers that alarm will be sent to the operator immediately, thus notifying the operator of abnormal system behavior.

Furthermore, the predicted patterns are then retrospectively compared to the real plant behavior. Significant deviations are reported in form of prediction error vectors. The prediction error vector is fused into a scalar robust anomaly indicator by a fuzzy logic controller.

IV. Layer 1: Threshold Based Alarms

The first layer of the presented FN-DFE architecture is the traditional threshold based alarm system (See Fig. 1). This layer implements simple threshold based system state validation methodology.

The knowledge base for this layer is known bounds of the system process, i.e. the minimum and maximum possible values for each sensor.

Once sensor data is retrieved, a simple comparison with the known interval for normal operation is made. If the current sensor measurement is outside the normal operation interval an alarm is generated and immediately sent to the human operator.

This method of alarm generation is extremely robust and has very low computational complexity, thus it is an ideal method for initial alarm generation. The traditional threshold based alarm generation method restricts the known system behavior into a multi-dimensional hypercube. However, potential unwanted system behavior can occur within this hypercube as well. Thus, layer 2 and layer 3 of the presented FN-DFE is implemented to identify these situations.

V. Layer 2: Anomaly Detection with Self-Organizing Fuzzy Logic System

This section describes the self-organizing construction of fuzzy logic system. Next, the second layer of the FN-DFE, which uses the SOFLS for anomaly detection, is discussed.

A. Self Organizing Fuzzy Logic System (SOFLS)

The proposed FN-DFE uses self-organizing algorithm for learning the structure and parameters of a fuzzy logic system. This method is inspired by the FLS structure learning algorithm previously used by Juang et al. [36], [37]. The advantages of this learning approach is that it automatically derives the structure of the FLS from the input data, it ensures continuous coverage of the input data points with fuzzy rules and it is suitable for large data sets, because the structure identification is performed during a single pass through the data.

Initially, there are no rules and no fuzzy sets in the FLS. A fuzzy rule can be understood as a cluster in the input space and the degree of firing of this rule for an input pattern can be seen as a degree of belonging of this pattern to the cluster [36]. For an m-dimensional input vector X_t the SOFLS learning method can be summarized as follows:

IF X_t is the first input **THEN DO**
  {Generate new fuzzy rule for X_t}
ELSE{
  FOR each pattern X_t **DO**{
    Find the rule R_I with the maximum degree of firing:

$$I = \arg \max_{1 \le i \le M(t)} \mu_{R_i}(X_t) \tag{1}$$

    IF $\mu_{R_I}(X_t) \le \phi$ **DO**{
      Generate new fuzzy rule for X_t
      $M(t+1) = M(t) + 1$
    }
  }
}

Here, $M(t)$ denotes the number of existing fuzzy rules at time t, $\phi \in [0,1]$ is a predefined threshold and the degree of firing of rule R_i can be calculated using the minimum t-norm operations applied to the rule antecedents as:

$$\mu_{R_i}(X_t) = \min\{\mu_{A_j^k}(x_t^i)\}, \quad j = 1 \ldots m \tag{2}$$

Here, A_j^k is the j^{th} antecedent fuzzy sets of the k^{th} fuzzy rule and x_t^i is the i^{th} component of the input vector X_t. New fuzzy rules are generated by projecting the input pattern X_t into the input domain and generating a Gaussian membership function in each dimension by setting its mean in the j^{th} dimension as $m_{M(t)}^j = x_t^j$ and its standard deviation to predefined spread parameter as $\sigma_{M(t)}^j = \beta$.

The threshold parameter ϕ controls the number of clusters. Smaller values of ϕ result in generating smaller number of clusters as more input patterns are assigned to already existing fuzzy rules with smaller membership. The spread parameter β determines the generalization capability of the model. Larger values result in Gaussian membership functions with greater spread covering larger areas around the input data.

B. System Modeling Using SOFLS

The traditionally used thresholds restrict the admissible system behavior into a multi-dimensional hypercube. As long as any anomalous plant behavior stays in this hypercube, the anomaly remains undetected. In order to alleviate this issue, the 2nd layer of the FN-DFE uses SOFLS for system modeling and behavior identification. The SOFLS is trained to detect deviations from a normal behavior model.

The input vector X_t for the SOFLS training is constructed from the current measurements W_t, the previous measurements W_{t-1} and the derivative of the sensory measurements $\Delta_t = W_t - W_{t-1}$:

$$X_t = \{W_t, W_{t-1}, \Delta_t\} \tag{3}$$

The trained SOFLS models the topology of the normal data within the threshold hypercube. During the on-line processing stage, each fuzzy rule describes the similarity of an input vector with a specific region of the threshold hypercube. The strength of firing $\mu_{R_i}(X_t)$ of rule R_i can be computed using the minimum operator as in (2). In this application of system modeling, the output of each fuzzy rule is a singleton fuzzy set expressing the belonging of input pattern X_t to the normal behavior class. Hence, the output of a particular fuzzy rule is its own firing strength $\mu_{R_i}(X_t)$. The output of all rules is aggregated using the maximum operator:

$$y(X_t) = \max_{i=1..M(t)} \mu_{R_i}(X_t) \tag{4}$$

In this manner, the SOFLS computes the similarity of the input vector with the approved normal behavior training data. This similarity measure can be used to signal any deviations from the normal behavior model.

Thus this type of system modeling is capable of identifying anomalous system behavior that might fall within the aforementioned hypercube of traditional threshold based system modeling.

VI. Layer 3: Behavior Prediction Using Artificial Neural Networks

This section first briefly describes the structure and learning of feed-forward artificial neural network. Next, the 3rd layer of the FN-DFE, which uses the ANN for behavior prediction, is discussed.

A. Feed-Forward Artificial Neural Networks

A feed-forward ANN is composed of multiple interconnected layers, each consisting of several neurons. The training of ANN proceeds in a supervised manner. The gradient descent approach is used to optimize system parameters with respect to the error between the computed and the desired output. Here, a specific combination of the Error Back-Propagation and the Levenberg-Marquardt - EBP-LM algorithm was used [38]-[40].

First, an input vector $X_t = \{x_t^1, \ldots, x_t^m\}$ is provided to the input layer of ANN. The net input value of neuron *i* in layer $k+1$ is calculated as the weighted sum of the input connections:

$$n^{k+1}(i) = \sum_{j=1}^{Sk} w^{k+1}(i,j)\, a^k(j) + b^{k+1}(i) \tag{5}$$

Here *Sk* denotes the number of neurons in layer k, $w^{k+1}(i,j)$ is the weight of the connection from neuron *j* in layer *k*, $b^{k+1}(i)$ is the bias of neuron *i* and $a^k(j)$ is the output from neuron *j* in layer *k*.

The output of neuron i in layer $k+1$ is:

$$a^{k+1}(i) = f^{k+1}(n^{k+1}(i)) \tag{6}$$

Here f^{k+1} is the activation function of neuron *i*. Typically, a sigmoidal activation function is used.

For an ANN with *L* layers, the task of the EBP-LM algorithm is to minimize the total error:

$$E = \sum_{p=1}^{P} \sum_{m=1}^{M} \left(d_{pm} - a_{pm}^L\right)^2 \tag{7}$$

Here *P* and *M* are the number of patterns and the number of outputs respectively, and d_{pm} denotes the desired output. The weight update rule for the EBP-LM algorithm is derived from the Newton's method using the Hessian and the gradient of system parameters. For the error function *E*, which is a sum of squares, the Hessian and gradient can be computed using the Jacobian of partial derivative of error with respect to the weights. Details of the algorithm can be found in [40].

B. Artificial Neural Network Based Signal Forecasting

The dynamics of the sensor measurements in a complex control system are determined by the basic underlying processes. For example, in a nuclear power plant these measurements are governed by complex physical and

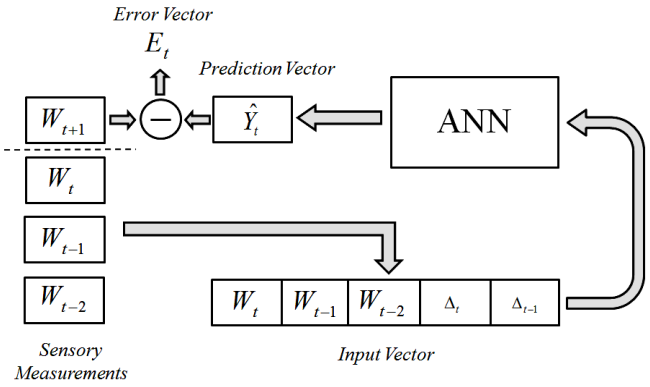


Fig. 2 ANN based signal forecasting component of DFE.

chemical processes. Because such complex physical process contain inherent sources of uncertainties such as unknown non-linear multi-dimensional dependencies and measurement noise, the dynamics are difficult to model using conventional mathematical modeling techniques. However, the temporal behavioral patterns of the system can be modeled using computational intelligence techniques such as the feed-forward ANN. In the 3rd layer of the proposed FN-DFE, the ANN based signal forecasting block, that was first presented in [7], is used to forecast the near future behavior of the plant based on the temporal historical data.

Fig. 2 depicts the implemented ANN based signal forecasting block. The input vector to the ANN is constructed from the previous three sensory measurements and the previous two measurements derivative vectors as follows:

$$X_t = \{W_t, W_{t-1}, W_{t-2}, \Delta_t, \Delta_{t-1}\} \tag{8}$$

While the derivative terms, Δ_t, Δ_{t-1} represent redundant information already in the input vector, the derivative terms were included as they reduce the total number of neurons as they represent a vital relationship between the other input vectors.

A unique ANN was trained offline for forecasting the values of each individual sensor. The future expected p values of the sensory readings are assigned as the desired output vector Y_t. Once the set of ANNs are trained, a prediction vector $\hat{Y}_t$ that predicts the future p values of all available sensors based on the history of the previous measurements is produced.

This prediction is then used as a model of the system behavior in the future p steps. In case of lost sensor values, this prediction can be used temporarily so that state-awareness of operators is not affected.

After obtaining the real p future measurements from the actual plant, the predicted values can be matched against the observations and an error vector E can be computed. For the i^{th} sensor the prediction error e_t^i for the expected signal forecasted at time t can be calculated as follows:

$$e_t^i = \frac{\sum_{j=1}^{k} | y_t^j - x_{t+j}^i |}{p} \tag{9}$$

Here, y_t^j is the j^{th} component of the prediction vector $\hat{Y}_t$, and x_{t+j}^i is the real measurement value for the i^{th} sensor at time $(t+j)$. Hence, the ANN based signal forecasting block generates a prediction error vector E_t. Each vector element is the average prediction error for a specific sensor.

This prediction error is an indication that the sensor values being reported are not the values that the system should have given normal operating conditions. Thus this type of behavior may indicate faulty sensors that are reporting incorrect values or a cyber attack where actual sensor values are substituted by incorrect values. In both cases the state-awareness of operators is severely hindered. Therefore, the proposed FN-DFE identifies this type of behavior and produces an alarm.

However, calculating this alarm vector does not necessarily contribute to the enhanced state-awareness of the operator [7]. In order to avoid the alarm flooding problem, this error vector is transformed into a robust scalar anomaly indicator by a fuzzy logic controller.

C. *Fuzzy Logic based Alarm Generation*

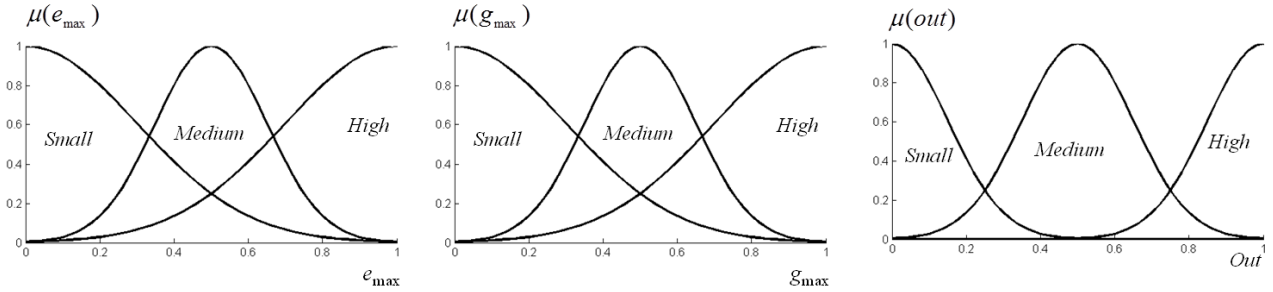
Generating a small set of robust and easy-to-understand alarms increases the state-awareness of operators considerably [7]. For a specific control system module, the ANN based signal forecasting block generates a prediction error vector. In the proposed FN-DFE, a Fuzzy Logic Controller (FLC) is implemented to fuse the prediction error vector into a robust scalar anomaly indicator.

The proposed FN-DFE uses the two-input FLC presented in [7]. The first input is the maximum error e_{max} from the calculated prediction based error vector. The second input is the absolute value of the current gradient of the sensory input with the highest prediction error g_{max}. After normalization, both inputs are fuzzified using 2 sigmoid fuzzy sets *Small*, *High* and one Gaussian fuzzy set *Medium* as depicted in Fig. 3(a) and Fig. 3(b). Similarly, the output of the anomaly indicator is also modeled using 2 sigmoid fuzzy one Gaussian fuzzy depicted in Fig. 3(c). These outputs express the anomaly level of the obtained sensory measurements.

Table I shows the rule base with 9 linguistic fuzzy rules. The respective output control surface is depicted in Fig. 4. The used fuzzy rules suppress the amplitude of the produced anomaly indicator when a significant system transient is observed. The rationale behind this design is that it is more likely to encounter a prediction error when the plant is in a dynamic transient behavior. However, prediction error generated during a steady system behavior is a strong indication of an anomaly.

VII. Experimental Results

This section presents experimental testing of the implemented FN-DFE integrated with the HYTEST plant monitoring. Four test scenarios have been considered: 1)



(a) (b) (c)

Fig. 3 Input fuzzy sets (a), (b) and output fuzzy sets (c) for the prediction error based anomaly indicator FLC.

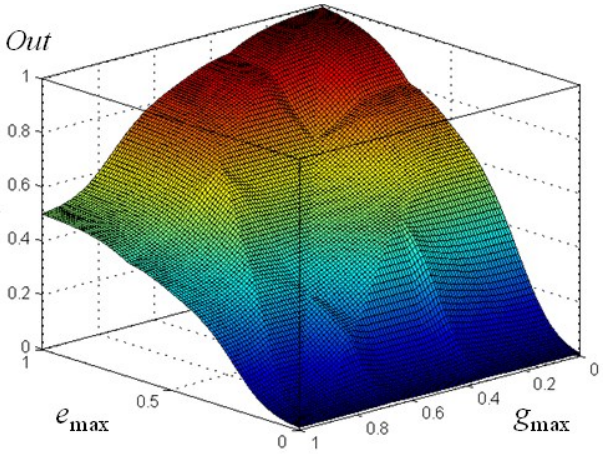


Fig.4 Fuzzy logic control surface of the anomaly indicator.

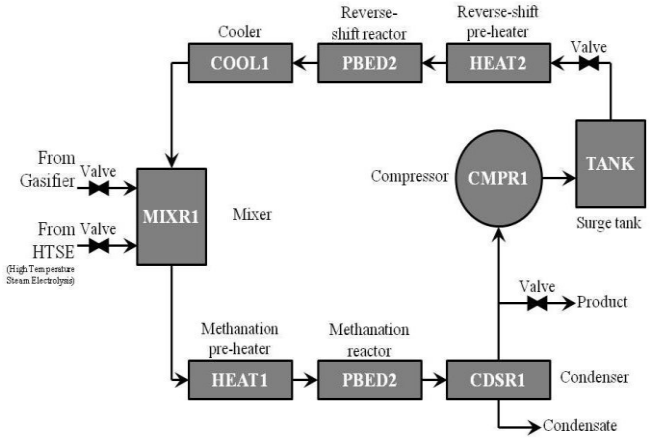


Fig.5 Basic block diagram of the INL HYTEST system

TABLE I
FUZZY RULE TABLE FOR ALARM SYNTHESIS

		e_{max}		
		Low	*Medium*	*High*
g_{max}	*Low*	**Low**	**High**	**High**
	Medium	**Low**	**Medium**	**High**
	High	**Low**	**Medium**	**Medium**

normal plant behavior, 2) control system behavior prediction when no sensor data is received, 3) intrusion with sensor data substitution, 4) plant behavior with faulty components.

A. HYTEST – Hybrid Energy System Facility Test Bed

This section describes the hybrid energy system testing facility known as HYTEST, which was used as the experimental test-bed for the developed FN-DFE. The actual test-bed depicted in Fig. 5 consists of Matlab Simulink model of the INL's HYTEST process. The HYTEST is a testing facility for hybrid energy systems composed of tightly-coupled chemical processes [34], [35]. The system is composed of interconnected units such as chemical reactors, heaters, condensers, storage tanks or compressors. Each HYTEST unit is equipped with a suite of sensors measuring its physical state (See Fig. 5).

The overall HYTEST system is composed of 16 units (some not pictured in Fig. 5) with 9 sensors in each unit (e.g. temperature, pressure or flow rate sensors). For each unit, a separate FN-DFE module was implemented. Altogether 144 ANNs were trained to forecast the future behavior of the plant. Due to the limited space, this section only demonstrates the experimental testing of the FN-DFE on a selected HYTEST component – a chemical reactor PBED2 (See Fig. 5).

The training data set composed of normal behavior transients, where the temperature set point on the PBED2 controller was adjusted by {-100K, -75K, -50K, -25K, 0K, 25K, 50K, 75K, 100K}. The SOFLS was trained with $\phi = 0.7$. This value was experimentally determined to provide a compromise between accuracy and the number of generated fuzzy rules. In total 94 fuzzy rules were created by the SOFLS learning method. Set of 9 ANNs were trained to predict the future $p = 4$ sensory readings. Each ANN had 45 inputs as in eq. (8), and contained 2 hidden layers with 20 and 10 neurons, respectively. This architecture of the ANN was selected by trial and error process as a compromise between the size of the model and the accuracy of the predictions.

B. Test Scenario 1: Normal Behavior

In the first test case, the FN-DFE system was used for system monitoring in a normal operating transient. The purpose of this test was to verify that 1) the FN-DFE correctly learns the normal behavior model, 2) no alarms are generated when the system is at normal operation, and 3) the set of ANNs is capable of correctly predicting the future sensory measurements.

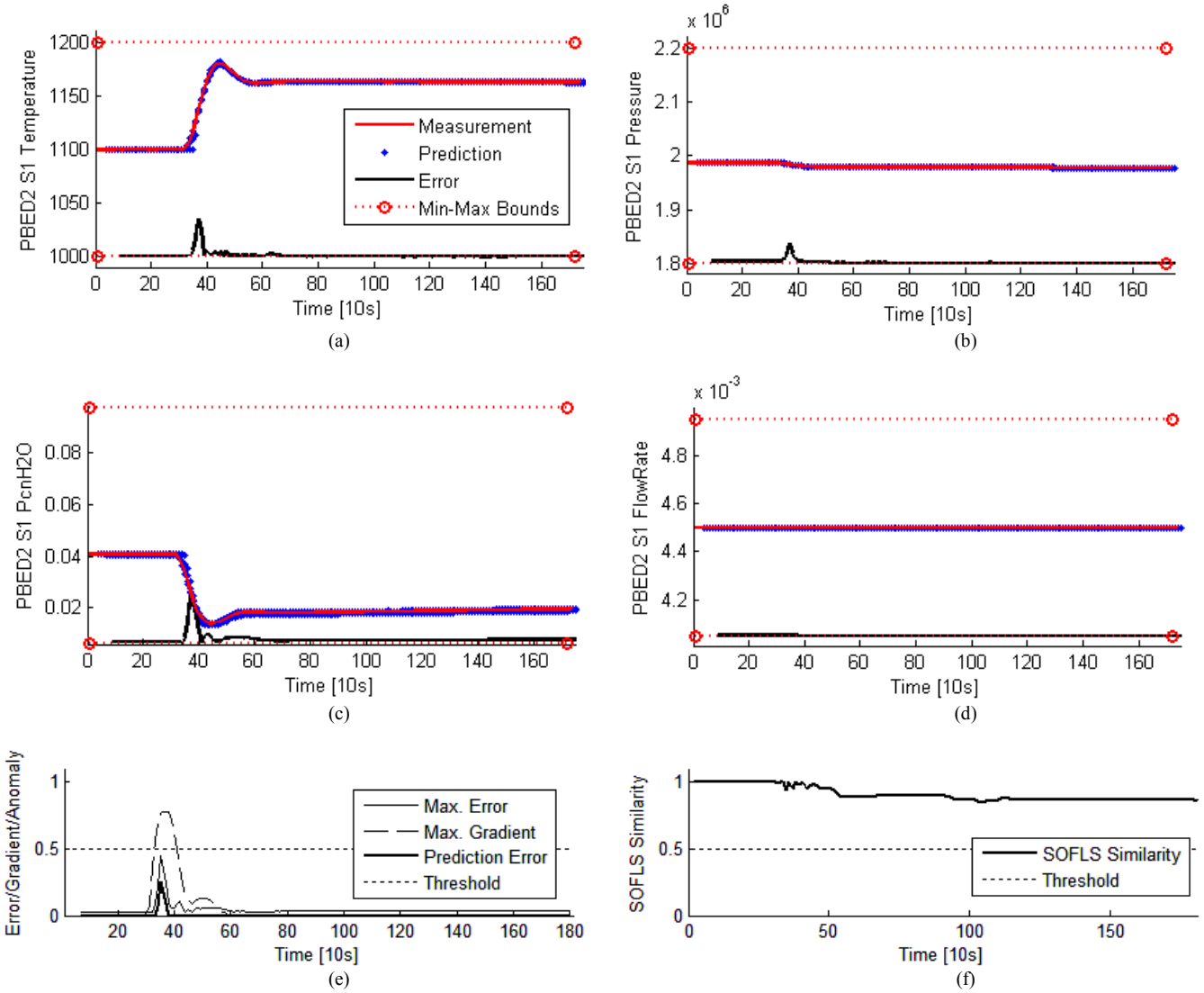


Fig. 6 ANN prediction of temperature (a), pressure (b), H2O concentration (c) and flow rate (d) sensors. ANN prediction error alarm (e) and SOFLS similarity based alarm (f).

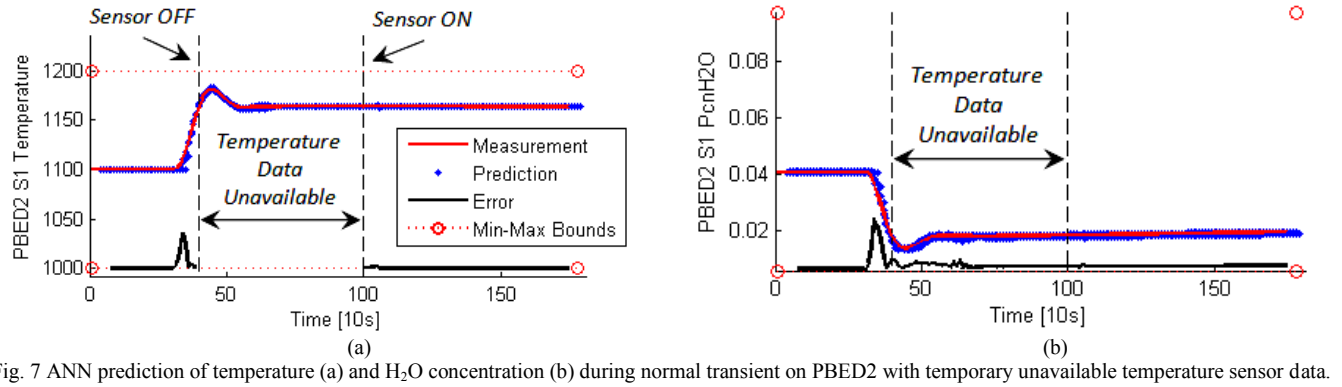


Fig. 7 ANN prediction of temperature (a) and H_2O concentration (b) during normal transient on PBED2 with temporary unavailable temperature sensor data.

For testing normal operating transient behavior, the PBED2 temperature set point was increased by 62.5K at time t=300s (See Fig. 6(a)). It should be noted that this temperature gradient was not part of the training data set and constitutes previously unseen testing data.

The comparison of the actual and the predicted sensory readings for four selected sensors can be seen in Fig. 6(a)-(d). It can be seen that the change in the set point resulted in an increase of temperature of the reactor (Fig. 6(a)). At the same time the concentration of H_2O in the gas significantly dropped (Fig. 6(c)) and the pressure also decreased slightly (Fig. 6(b)).

Fig. 6(e)-(f) then show the aggregated robust prediction error indicator and the SOFLS anomaly indicator. Fig. 6(e) depicts the prediction error generated from the fuzzy alarm generation, using the maximum error and maximum gradient. The generated prediction error is below the alarm threshold. Thus an alarm is not generated in this normal operation scenario. Similarly, Fig 6(f) shows that the SOFLS similarity

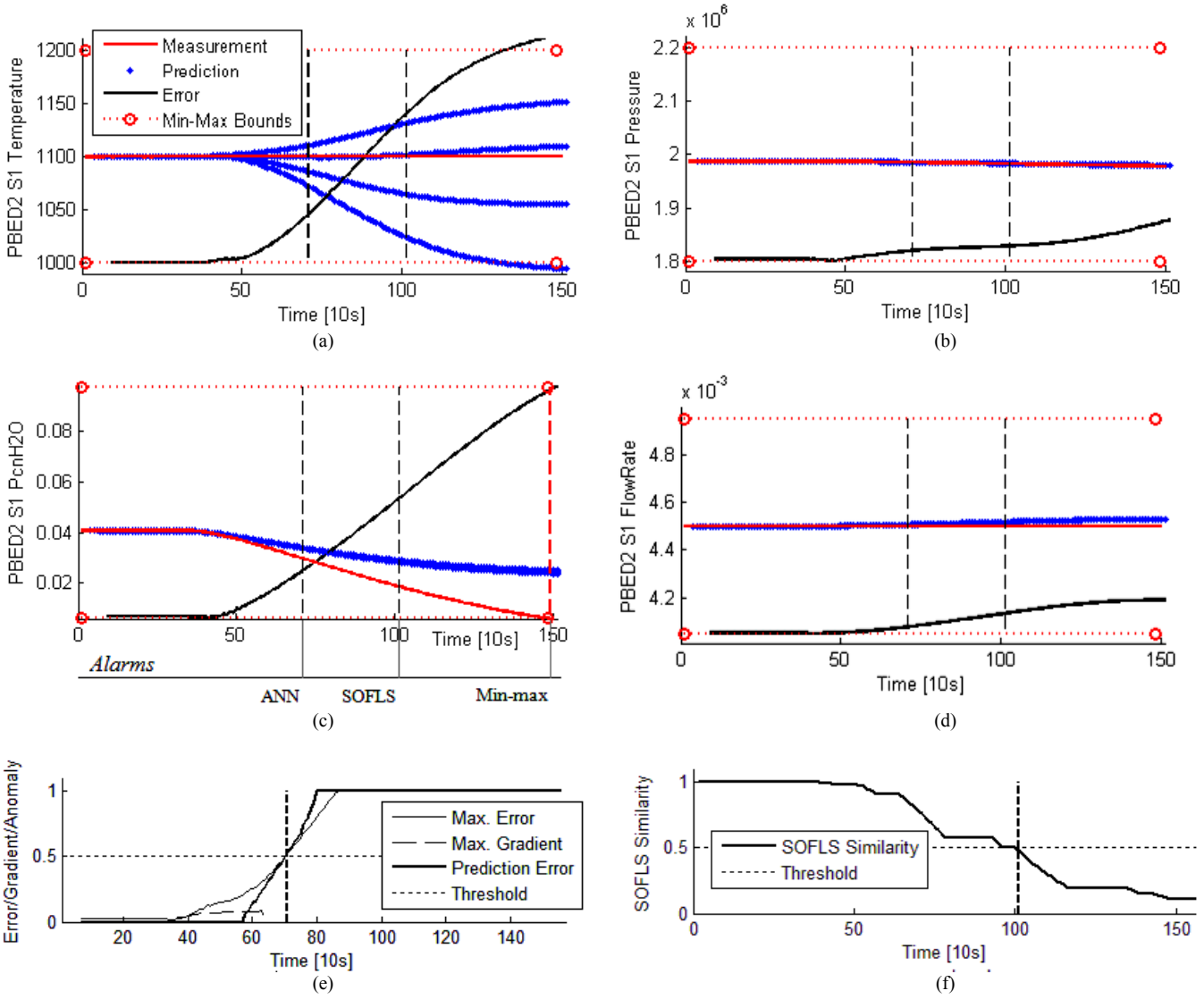


Fig. 8 ANN prediction of temperature (a), pressure (b), H2O concentration (c) and flow rate (d) sensors. ANN prediction error alarm (e) and SOFLS similarity based alarm (f).

indicator shows high similarity to observed values and does not go below the similarity threshold. Thus, the FN-DFE correctly accepted the transient normal operating procedure and no alarm was generated.

C. *Test Scenario 2: No Sensor Data Received*

Next, the performance of the presented FN-DFE when sensor readings are temporary unavailable was investigated. Typical real world scenario might be faulty sensor network communication failure. In this experiment the data from the temperature sensor was unavailable from time t=400s to time t=1000s.

Since the temperature reading is utilized by all ANN predictors for forecasting the signal from all sensors, such network failure would completely disable the FN-DFE. However, in case of unavailability of the sensory data, the FN-DFE automatically uses the previous ANN signal prediction in place of the real data, thus maintaining approximated but coherent state-awareness of the system.

This property is demonstrated in Fig. 7, which displays the signal predictions for the temperature and the H_2O concentration sensors. The dashed vertical lines mark where the temperature sensor data was unavailable. It can be observed, that both the approximated prediction of the temperature and the selected H_2O concentration sensor maintained coherent state indication for the time of temporary unavailability of the sensory readings.

Thus, the operators were able to identify system state even when the sensor data was temporarily unavailable, thereby maintaining the state-awareness of the system.

D. *Test Scenario 3: Sensor Data Substitution*

Next, the detection of a potential cyber-attack where attackers have taken control of one or more critical systems and sensor data is being substituted with incorrect values, as with the case of Stuxnet [41], was investigated.

In this scenario, an intruder gained network access to the control system of the reactor and starts linearly increasing the power to the chemical reactor heaters in an attempt to overheat

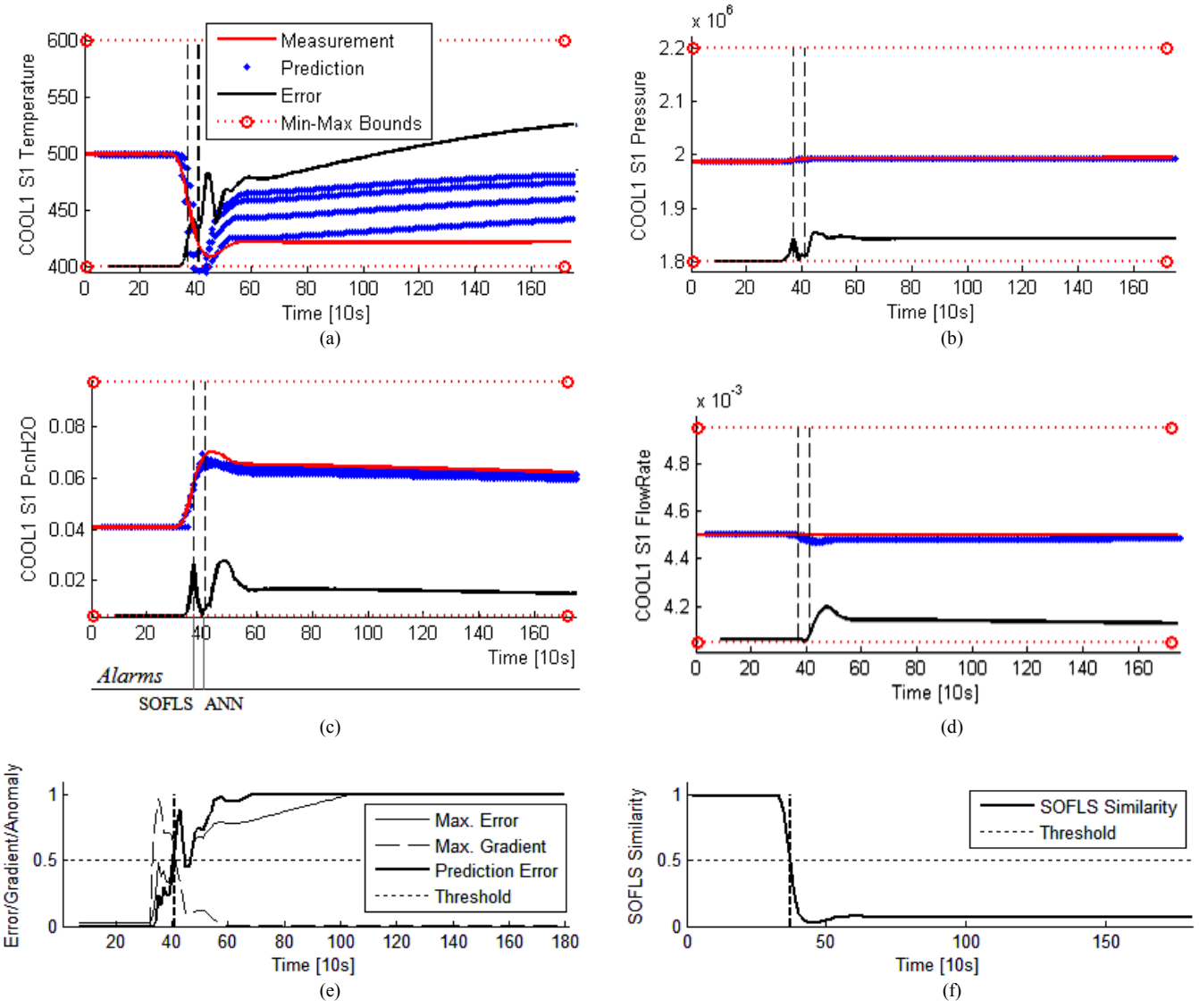


Fig. 9 ANN prediction of temperature (a), pressure (b), H2O concentration (c) and flow rate (d) sensors. ANN prediction error alarm (e) and SOFLS similarity based alarm (f).

the systems at time *t*=300s. Furthermore, to disguise the attack from the operator, the intruder manipulates the values of the temperature sensors and supplies a faulty constant temperature reading to the system.

The comparison of the value received from the sensor and the predicted sensory readings can be seen in Fig. 8(a)-(d). It can be observed in Fig. 8(a), the measurement, i.e. the value returned from the temperature sensor is constant at 1100K. However, the control changes performed by the intruder results in system state changes such that the predicted value of the temperature start diverging from the manipulated measured value. Fig. 8(a) shows each of the 4 ANN predictions diverging significantly from the spoofed value.

Fig. 8(e)-(f) then show the aggregated robust prediction error indicator and the SOFLS anomaly indicator. It can be seen that while the SOFLS still indicates high similarity of the manipulated incorrect sensor values with normal behavior until reporting a similarity alarm at time *t*=1010s, the significantly deviating ANN prediction cause a prediction alarm at time t=710s. For a comparison, the conventional threshold based alarm triggers at time *t*=1420s. The FN-DFE thus provides 710s earlier alarm indication than the traditional threshold based alarm.

The prediction error produced by the ANN is driven by the previously learnt model of the system dynamics. While the attacker was able to change the values returned by the temperature sensor to cover the heating of the reactor, this change of the plant state also affected other measured variables, such as the concentration of H_2O in Fig. 7(c). These additional variables caused the ANN predictor to forecast an expected sharp temperature gradient, which is manifested by the diverging temperature readings predictions in Fig. 7(a). Since these did not match the manipulated temperature values that were sent from the sensor, a prediction alarm was reported.

E. Test Scenario 4: Component Failure Detection

Finally, a scenario where a component has failed and the system is deviating from normal operating parameters, was investigated.

The FN-DFE was tested on a scenario of performing a normal operating procedure by decreasing the temperature set point by 50K at time *t*=300s. During this transient, the cooler component COOL1 neighboring the PBED2 component was malfunctioning with a cooling control signal "stuck" at a constant value irrespective of the dynamic transients.

The comparison of the actual and the predicted sensory readings for COOL1 can be seen in Fig. 9(a)-(d). Fig. 9(e)-(f) then show the aggregated robust prediction error indicator and the SOFLS anomaly indicator. It can be seen that the observed behavior is immediately marked at time *t*=370s as anomalous by the SOFLS. Shortly after at time *t*=410s follows the ANN prediction alarm due to high prediction errors of the ANN model. Note, that the conventional threshold based alarm did not trigger because the plant remained in the interval of normal behavior.

This early alarm reporting is triggered by the modified dynamics of the system due to the stuck controller component for COOL1 unit. This modification caused a significant divergence of the recorded plant's behavior and the previously learnt normal behavior model.

VIII. Conclusion

This paper presented the design of a Fuzzy-Neural Data Fusion Engine (FN-DFE) for enhanced state-awareness of resilient hybrid energy systems. The implemented FN-DFE consists of a three-layered system behavior monitoring system consisting of: 1) traditional threshold based alarms, 2) anomalous behavior detector using self organizing fuzzy logic system, and 3) Artificial Neural Network (ANN) based control system modeling and behavior prediction. The improved control system state-awareness is achieved via fusing input data from multiple sources and combining them into robust system modeling and anomaly indicators.

The proposed FN-DFE was integrated with a model of INL's HYTEST hybrid energy systems testing facility. It was shown that it can provide timely plant performance monitoring and anomaly detection capabilities. It was demonstrated that the neural network based signal predictions can be used to augment the resiliency of the system and provide coherent state-awareness despite temporary unavailability of sensory data. In addition, it was also shown that the system is capable of robust alarm reporting significantly earlier than conventional threshold based alarm systems.

Future work includes improving the ANN based behavior prediction model by utilizing data preprocessing steps such as outlier detection. Furthermore, the proposed system can be coupled with advanced Fault Detection and Isolation (FDI) methodologies to further enhance the state-awareness of system operators.

References

[1] C. G. Rieger, D. I. Gertman, M. A. McQueen, "Resilient Control Systems: Next Generation Design Research," in *Proc. IEEE HSI*, Catania, Italy, May 2009, pp. 632-636.

[2] D. L. Hall, J. Llinas, "An introduction to multisensor data fusion," in *Proc. IEEE*, vol. 85, no. 1, pp. 6–23, Jan. 1997.

[3] E. L. Waltz, D. M. Buede, Dennis "Data Fusion and Decision Support for Command and Control," *IEEE Trans. on Syst., Man, and Cybern.*, vol. 16, no. 6, pp. 865-879, Nov. 1986.

[4] V. V. S. Sarma, S. Raju, "Multisensor data fusion and decision support for airborne target identification," *IEEE Trans. on Syst., Man, and Cybern.*, vol. 21, no. 5, pp. 1224-1230, Sep/Oct 1991.

[5] S. L. Sun, "Multisensor optimal information fusion input white noise deconvolution estimators," *IEEE Trans. on Syst., Man, and Cybern. B, Cybern.*, vol. 34, no. 4, pp. 1886–1893, Aug. 2004.

[6] S-F. Su; K-Y. Chen, "Fuzzy hierarchical data fusion networks for terrain location identification problems," *IEEE Trans. on Syst., Man, and Cybern. B, Cybern.*, vol. 34, no. 1, pp. 731-739, Feb. 2004.

[7] O. Linda, M. Manic, T. R. McJunkin, "Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine," in *Proc. IEEE ISRCS*, Boise, ID, 2011.

[8] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, H. Rhy, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks," *IEEE Trans. on Ind. Informat.*, vol. 6, no. 4, pp. 744-757, Nov. 2010.

[9] D. Wang, "Robust Data-Driven Modeling Approach for Real-Time Final Product Quality Prediction in Batch Process Operation," *IEEE Trans. on Ind. Informat.*, vol. 7, no. 2, pp. 371-377, May 2011.

[10] D. De Silva, X. Yu, D. Alahakoon, G. Holmes, "A Data Mining Framework for Electricity Consumption Analysis From Meter Data," *IEEE Trans. on Ind. Informat.*, vol. 7, no. 3, pp. 399-407, Aug. 2011.

[11] K. Y. Chan, T. S. Dillon, C. K. Kwong, "Modeling of a Liquid Epoxy Molding Process Using a Particle Swarm Optimization-Based Fuzzy Regression Approach," *IEEE Trans. on Ind. Informat.*, vol. 7, no. 1, pp. 148-158, Feb. 2011.

[12] T.-H. Pan, B.-Q. Sheng, D. S.-H. Wong, S.-S. Jang, "A Virtual Metrology System for Predicting End-Of-Line Electrical Properties Using a MANCOVA Model With Tools Clustering," *IEEE Trans. on Ind. Informat.*, vol. 7, no. 2, pp. 187-195, May 2011.

[13] W. J. Kim, S. H. Chang; B. H. Lee, "Application of neural networks to signal prediction in nuclear power plant," *IEEE Trans. on Nucl. Sci.*, vol. 40, no. 5, pp. 1337-1341, Oct 1993.

[14] Z. Guo, R. E. Uhrig, "Nuclear power plant performance study by using neural networks," *IEEE Trans. on Nucl. Sci.*, vol. 39, no. 4, pp. 915-918, Aug 1992.

[15] S. S. Choi, K. S. Kang, H. G. Kim, S. H. Chang, "Development of an On-Line Fuzzy Expert System for Integrated Alarm Processing in Nuclear Power Plants," *IEEE Trans. on Nucl. Sci.*, vol. 42, issue: 4, pp. 1406-1418, Aug. 1995.

[16] J. Rabatel, S. Bringay, P. Poncelet, "Fuzzy Anomaly Detection in Monitoring Sensor Data," in *Proc. WCCI*, Barcelona, Spain, July 2010.

[17] K. Hadad, M. Pourahmadi, H. Majidi-Maraghi, "Fault diagnosis and classification based on wavelet transform and neural network," *Progress in Nuclear Energy*, vol. 53, no. 1, pp. 41-47, Jan. 2011.

[18] H. Shen, J. M. Doster, "Application of a neural network based feedwater controller to helical steam generators," *Nuclear Engineering and Design*, vol. 239, no. 6, pp. 1056-1065, June 2009.

[19] M. Fast, T. Palme. "Application of artificial neural networks to the condition monitoring and diagnosis of a combined heat and power plant," in *Energy*, vol. 35, no. 2, pp. 1114-1120, Feb. 2010.

[20] K. Nabeshima, T. Suzudo, T. Ohno, K. Kudo, "Nuclear reactor monitoring with the combination of neural network and expert system," *Mathematics and Computers in Simulation*, vol. 60, no. 3-5, pp. 233-244, Sep. 2002.

[21] R. Razavi-Far, H. Davilu, V. Palade, C. Lucas. "Model-based fault detection and isolation of a steam generator using neuro-fuzzy networks," *Neurocomputing*, vol. 72, no. 13-15, pp. 2939-2951, Aug. 2009.

[22] K. Salashoor, M Kordestani, M. S. Khoshro, "Fault detection and diagnosis of an industrial steam turbine using fusion of SVM (support vector machine) and ANFIS (adaptive neuro-fuzzy inference system) classifiers," *Energy*, vol. 35, no. 12, pp. 5472-5482, Dec. 2010.

[23] M. J. Embrechts, S. Benedek, "Hybrid identification of nuclear power plant transients with artificial neural networks," *IEEE Trans. on Ind. Electron.*, vol. 51, no. 3, pp. 686-693, Jun. 2004.

[24] M. G. Na, S. H. Shin, S. M. Lee, D. W. Jung, S. P. Kim, J. H. Jeong, B. C. Lee, "Prediction of major transient scenarios for severe accidents of nuclear power plants," *IEEE Trans. on Nucl. Sci.*, vol. 51, no. 2, pp. 313-321, Apr. 2004.

[25] K. Hadad, M. Mortazavi, M. Mastali, A. A. Safavi, "Enhanced Neural Network Based Fault Detection of a VVER Nuclear Power Plant With

the Aid of Principal Component Analysis," *IEEE Trans. on Nucl. Sci.*, vol. 55, no. 6, pp. 3611-3619, Dec. 2008.
[26] Y. Ren, L. Feng "An Online Fault Diagnosis Method for Nuclear Power Plant Based on Combined Artificial Neural Network," in *Proc. APPEEC,* Mar. 2010, pp. 1-4.
[27] J. G. M. S. Decanini, M. S. Tonelli-Neto, C. R. Minussi, "Robust fault diagnosis in power distribution systems based on fuzzy ARTMAP neural network-aided evidence theory," *Generation, Transmission & Distribution, IET*, vol. 6, no. 11, pp. 1112-1120, Nov. 2012.
[28] O. Linda, T. Vollmer, J. Wright, M. Manic, "Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor," in *Proc. IEEE ISRCS*, Paris, France, April, 2011.
[29] O. Linda, T. Vollmer, M. Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures," in *Proc. IEEE IJCNN*, Atlanta, Georgia, June 2009.
[30] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, A. Trombetta, "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," *IEEE Trans. on Ind. Informat.*, vol. 7, no. 2, pp. 179-186, May 2011.
[31] E. Eryurek, B. R. Upadhyaya, "Sensor validation for power plants using adaptive backpropagation neural network," *IEEE Trans. on Nucl. Sci.*, vol. 37, no. 2, pp. 1040-1047, Apr. 1990.
[32] A. Vodencarevic, H. K. Bunig, O. Niggemann, A. Maier, "Identifying Behavior Models for Process Plants, " in *Proc. IEEE ETFA*, Sep. 2011, pp. 1-8.
[33] S. L. Hwang, J. T. Lin, G. F. Liang, Y. J. Yau, T. C. Yenn, C. C. Hsu, "Application control chart concepts of designing a pre-alarm system in the nuclear power plant control room," *Nuclear Engineering and Design*, vol. 238, no. 12, Dec. 2008.
[34] C. Stoots, L. Shun, J. O'Brien, "Integrated Operation of the INL Hytest System and High-Temperature Steam Electrolysis for Synthetic Natural Gas Production," in *Proc. International Meeting of the Safety and Technology of Nuclear Hydrogen Production, Control and Management*, June 2010.
[35] L. Shun, R. Boardman, S. Cherry, C. Rieger, "HYTEST Phase I Facility Commissioning and Modeling," *INL External Technical Report*, INL-EXT-09-16961, Sep. 2009.
[36] Ch.-F. Juang, Y.-W. Tsao, "A Type-2 Self-Organizing Neural Fuzzy System and Its FPGA Implementation," *IEEE Trans. on Syst., Man, and Cybern. B, Cybern.*, vol. 38, no. 6, pp. 1537-1548, Dec. 2008.
[37] Ch.-F. Juang, Ch.-H. Hsu, "Reinforcement Ant Optimized Fuzzy Controller for Mobile-Robot Wall-Following Control," *IEEE Trans. on Ind. Electron.*, vol. 56, no. 10, pp. 3931-3940, Oct. 2009.
[38] P. J. Werbos, *The Roots of Backpropagation*, New York: Johns Wiley & Sons, 1994.
[39] D. Marquardt, "An algorithm for least squares estimation of non-linear parameters," *J. Soc. Ind. Appl. Math.*, pp.431-441, 1963.
[40] M. Hagan, M. Menhaj, "Training feedforward networks with the Marquardt algorithm," *IEEE Trans. on Neural Netw.*, vol. 5, no. 6, pp. 989-993, 1994.
[41] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013.

Ondrej Linda (S'09–M'13) received his B.Sc. in Electronic Engineering and Informatics from Czech Technical University in Prague in 2007, M.Sc. in Computer Graphics from Czech Technical University in Prague in 2010, M.Sc. in Computational Intelligence from the University of Idaho at Idaho Falls in 2009, and Ph.D. in Computational Intelligence from the University of Idaho at Idaho Falls in 2012. His research experience includes research assistant positions at Kansas State University and at the University of Idaho, and an internship with the Robotics Group at the Idaho National Laboratory. He is currently at Expedia Inc. Seattle, WA. His fields of interest include machine learning, pattern recognition, intelligent control systems, data mining and computer graphics.

Dumidu Wijayasekara (S'10) received his B.Sc. in Computer Science from University of Peradeniya in Sri Lanka in 2009 and his M.Sc. in Computational Intelligence from the University of Idaho at Idaho Falls, ID, USA in 2014. He is currently reading for a Doctoral degree at the University of Idaho in Idaho Falls. His research experience includes research assistant positions at the University of Peradeniya and the University of Idaho. His fields of interest include Fuzzy Systems, machine learning, pattern recognition, data mining, and advanced visualization systems.

Milos Manic (S'95–M'05–SM'06) received the Dipl.Ing. and M.S. degrees in electrical engineering and computer science from the University of Niš, Niš, Serbia in 1991 and 1997 respectively, and the Ph.D. degree in computer science from the University of Idaho in 2003.

Dr. Manic is an Associate Professor with Computer Science Department and is a Director of Modern Heuristics Research Group. He has over 20 years of academic and industrial experience and appointments with ECE Dept. and Neuroscience program at University of Idaho. His previous positions include faculty position at University of Nis, Serbia, Fellow of the Brain Korea 21 Program, Seoul 2008, and Director of the Computer Science Program at Idaho Falls. As principal investigator he lead number of research grants with the National Science Foundation, Idaho National Laboratory, EPSCoR, Dept. of Air Force, and Hewlett-Packard, in the area of data mining and computational intelligence applications in process control, network security and infrastructure protection.

Dr. Manic is an IEEE Industrial Electronics Society (IES) Officer and is a member of numerous standing and technical committees and boards of this Society such as IES Committees for Conferences and for Publications. Also involved in various capacities in Technical Committees on Education, Industrial Informatics, Factory Automation, Smart Grids, Standards, and Web and Information Committee (WIC), and is a co-founder and chair of Technical Committee on Resilience and Security in Industry.

Craig Rieger (SM'08), PhD, PE, is the lead for the Instrumentation, Control and Intelligent Systems distinctive signature area, a research and development program at the Idaho National Laboratory (INL) with specific focus on next generation resilient control systems. In addition, he has organized and chaired six Institute of Electrical and Electronics Engineers (IEEE) technically co-sponsored symposia in this new research area, and authored more than 30 peer-reviewed publications. He received B.S. and M.S. degrees in Chemical Engineering from Montana State University in 1983 and 1985,

respectively, and a PhD in Engineering and Applied Science from Idaho State University in 2008. Craig's PhD coursework and dissertation focused on measurements and control, with specific application to intelligent, supervisory ventilation controls for critical infrastructure. Craig is a senior member of IEEE, and has 20 years of software and hardware design experience for process control system upgrades and new installations. Craig has also been a supervisor and technical lead for control systems engineering groups having design, configuration management, and security responsibilities for several INL nuclear facilities and various control system architectures.