12th IFAC International Symposium on
Advanced Control of Chemical Processes
July 14-17, 2024. Toronto, Canada

Fault Data Injection Detection on a Digital-Twin: Fresnel Solar Concentrator

William D. Chicaiza * **Diogo O. Machado** **
Adolfo J. Sánchez *** **Juan M. Escaño** *
Julio E. Normey-Rico ****

* *Departamento de Ingeniería de Sistemas y Automática, Universidad de Sevilla, Camino de los Descubrimientos s/n., 41092 Sevilla, Spain (wchicaiza@us.es, jescano@us.es)*
** *Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - IFRS - Campus Rio Grande, RS, Brasil. (diogo.machado@riogrande.ifrs.edu.br)*
*** *Department of Mechanical, Biomedical, Munster Technological University, Cork, Bishopstown, Ireland. (adolfo.sanchezdelpozofernandez@mtu.ie)*
**** *Universidade Federal de Santa Catarina - UFSC. Departamento de Automação e Sistemas. Florianópolis, SC, Brasil. (julio.normey@ufsc.br)*

Abstract:
This work focuses on developing a neurofuzzy detector capable of identifying a cyber attack of false data injection into the outlet temperature sensor of a Fresnel-type solar field which has a PI+FF controller to control the refered temperature. A digital twin of the Fresnel plant and its controller are used for simulation purposes. The digital twin is situated in the domain of behavior and rules, as it contains a set of models, including a partial differential equation (PDE) model and a neurofuzzy model. Results from simulation are shown using three different scenarios: (1) without fault, (2) a ramp and threhold with negative injection and (3) the last scenario with positive injection. The presented fault data injection detector has solid performance with more than 97% detection accuracy and precision.

Keywords: Solar energy, Fresnel solar collector, ANFIS, high pressure generator, absorption cooler.

1. INTRODUCTION

The increasing digital connection of industrial automated systems raises the threat of cyber attacks that may harm people, pollute the environment, damage industrial plants, and destabilize production. Cyber-security is a central concern accordingly to the last IEEE Control Systems Society roadmap 2030. The roadmap points to three societal drivers of technology in the following years: mitigation and adaptation to climate change, smart infrastructure systems, and resilience of societal-scale systems — furthermore, Artificial Intelligence (AI) and Big Data are technological trends. Therefore, there are opportunities to develop safety-critical systems, resilient cyber-physical-human systems, renewable energy processes as synergic solutions to generate affordable and clean energy (Alleyne et al., 2023).

In this context, digital twins are one of the technologies that can be employed to mitigate cyber-attacks in industry. A digital twin is a highly detailed digital replica of a physical system or entity, with which it is bidirectionally synchronized, allowing multi-scale tests and experiments to be conducted virtually, thus avoiding the expense of conducting them physically. Examples of DT for power systems, where abrupt failures could arise from random disturbances unknown to the virtual entity, such as human interference, are shown in Chicaiza et al. (2024). Another example of the use of this technology in a solar plant is presented in (Rodríguez et al., 2023), which focuses on deciding when to update the twin when the input data of the physical entity are altered or corrupted.

This work contributes to developing a fault data injection detector based on an AI technique while applying the conceptual proof in a Fresnel Solar Collector (FSC) Digital Twin (DT). Fault Data Injection (FDI) is a cyber attack that injects corrupted data to manipulate a system's behavior. FDI refers to bad-intentioned sensors, supervision systems, controllers, or other information source data manipulation. The effects of FDI range from poor operation and decision making to compromising systems and personnel integrity, as indicated in (Liang et al., 2017).

FDI detection and isolation refers to malicious data injection identification and countermeasure techniques to secure information reliability and quality for further trustful operation and decision-making, mitigating injection and corrupted data presence (Mo and Sinopoli, 2010). Several works have contributed to the field of FDI de-

tection, from computer systems (Hsueh et al., 1997) to applications on cyber-physical control systems (Sargolzaei et al., 2020). One approach to improve the effectiveness of FDI detection is through the development of unsupervised AI-based unsupervised models, such as artificial neural networks (ANNs) and neurofuzzy systems. These models employ dimensionality reduction techniques, such as Principal Component Analysis (PCA) and clustering. For example, in (Mohammadpourfard et al., 2017), DBSCAN was applied to each dimension of the reduced space to select appropriate partitions, followed by the application of Fuzzy C-Means to distinguish between fake and actual data. Similarly, (Aboelwafa et al., 2020) employed autoencoders, a technique for dimensionality reduction and input reconstruction, to correct false data in a multi-sensor industrial environment by extracting sensory features and their relationships. Furthermore, (Chicaiza et al., 2022) presents a combination of PCA and neurofuzzy systems to detect data injection in a wind turbine.

In this paper, the authors contribute to developing a neuro-fuzzy detector capable of identifying data injection in the flow sensor/transmitter of an FSC plant. The FSC plant related to this work is installed at the Engineer's School at Seville University, Spain (Machado et al., 2023). This work uses the FSC DT because it is a high-fidelity model framework to simulate the FSC process and the cyber attack to validate the proposed FDI detector. Digital Twins are replicas of the physical entities that make up the systems. Therefore, the FSC DT enables fast analysis in different scenarios with high accuracy and without needing the physical system, avoiding experimental costs and enabling fast what-if analysis.

The research hypothesis of this work is that Adaptive Neuro-Fuzzy Inference System (ANFIS) is suitable for FDI detection. ANFIS are gray box representations of a given system; therefore, they have the advantage of rules addition after training compared to ANN, the last are black box representations of a given system. This paper is the first to consider a solar FSC DT for training the ANFIS detector and its conceptual proof. In addition, the simulations consider a massive actual data quantity of 25 days of operational data. The process controller and process DT outputs are fed into the FDI detection input. The objective is to simulate three cases of operation, two with artificially injected fault data and one without data injection, and evaluate the detector performance. Each case simulates the Fresnel DT with positive, no-fault, and negative outlet temperature faults.

2. CONTROLLER DESIGN

The FSC energy balance considering the absorber's metal tube walls as the control volume is given by Eq. 1:

$$\rho_m c_m A_m \frac{\partial T_m}{\partial t}(t,x) = \dot{Q}_{sun}(t) - \dot{Q}_a(t,x) - \dot{Q}_f(t,x), \quad (1)$$

where subindex m refers to metal walls,ρ is specific mass, c is heat capacity, A is the tranversal area, T is temperature, t is time, x is space in x axis and $\dot{Q}$ is heat rate. Note that $\dot{Q}_{sun}$ refers to the solar heat rate input of the FSC, and $\dot{Q}_a$ is the ambient loss heat rate, while $\dot{Q}_f$ is the heat rate that is transferred from the metal walls to the fluid inside the absorber tube.

The energy balance considering the absorber's fluid inside the tube as the control volume is given by Eq. 2

$$\rho_f c_f A_f \frac{\partial T_f}{\partial t}(t,x) + \rho_f c_f q(t) \frac{\partial T_f}{\partial x}(t,x) = \dot{Q}_f(t,x). \quad (2)$$

where subindex f refers to the fluid and q is the flow. It should be noted that the inlet temperature is $T_{in} = T_f(t,0)$ and the outlet temperature is $T_{out} = T_f(t,\infty)$

Figure 1 depicts the feedback process controller. The outlet temperature T_{out} is the controlled variable, the flow $q(t)$ is the manipulated variable, and the inlet temperature T_{in}, the solar irradiance I, related to $\dot{Q}_{sun}$, and the ambient temperature T_{amb}, related to $\dot{Q}_a$, are the prominent disturbances variables. In some cases, it is possible to manipulate the mirror focus to add more control capabilities once it is possible to directly vary the solar heat rate $\dot{Q}_{sun}$.

This work implemented a proportional integral outlet temperature feedback controller, as indicated in Machado et al. (2022), and a feedforward controller to enhance the disturbances rejection performance as indicated in Sánchez et al. (2019).

3. NEUROFUZZY DETECTOR

The detector structure integrates multiple fuzzy inference systems (FIS) and the projection of data on the principal component obtained from a PCA of a data set, as shown in Figure 2. The detector shall be able to identify the injection of false data into the plant's FSC flow sensor.

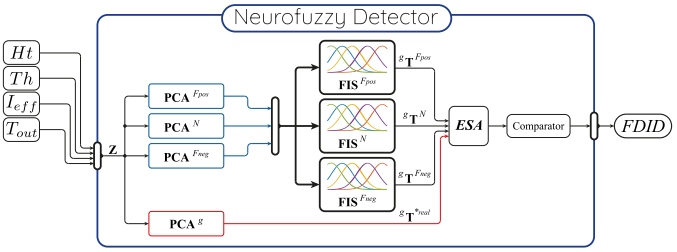


Fig. 2. Structure of the Neurofuzzy Detector

PCA is a statistical method that handles multiple variables. It efficiently projects data points from an n-dimensional space to a reduced dimension space, facilitating the identification of latent or unobserved parameters in the data set. The use of PCA transforms correlated variables into new uncorrelated variables, helping to improve convergence in the ANFIS training (Chicaiza et al., 2022).

The first step is to perform a correlation analysis of the system data according to the research conducted by (Chicaiza et al., 2022; Machado et al., 2023). As a result, the correlation coefficient matrix is calculated for the SFC data set, denoted ${}^{SFC}\mathbf{R} \in \Re^{7\times7}$, involving 7 variables ($M = 7$). PCA identifies how the plant variables correlate with (T_{out}), the primary variable of interest. Then, the correlation is represented by the Pearson correlation coefficient, denoted ρ, which can range from -1 to 1.

Figure 2 presents the neurofuzzy detector inputs variables. Where, $Ht = f(T_{out}, q)$ represents the coefficient of heat transfer fluid calculated at the outlet of the collector, q is

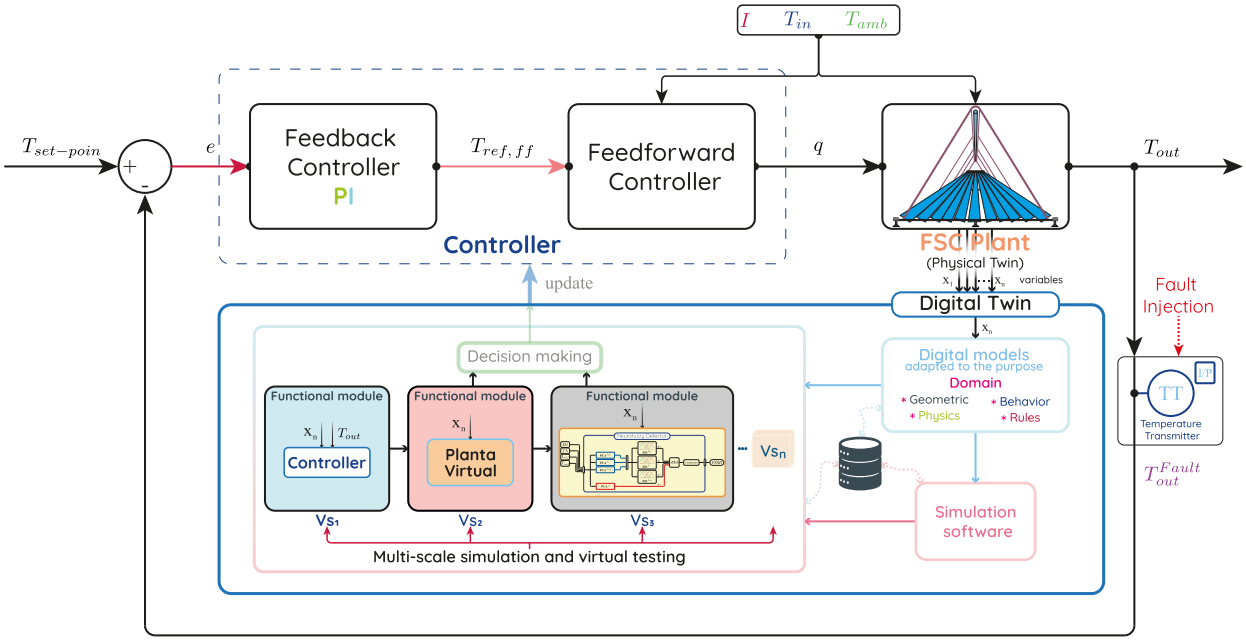


Fig. 1. Control schematic

the flow rate of the heat transfer fluid, $Th = f(T_{out}, T_{in})$ represents a thermal jump, which is the difference between the outlet temperature (T_{out}) and the inlet temperature (T_{in}), and I_{eff} is the effective irradiance. Additionally, PCA is applied to each data set, resulting in three principal component matrices (PCA^s), one per group, and a general (PCA^g) of all sets, as shown in Eq. (3).

3.1 Preparation of operational data

Data that present a significant correlation with the variable on which false data injection will be detected, in this case (T_{out}), are combined with variables derived from other quantities (H_t, Th), as well as with meteorological variables (T_{amb}, I) that exert substantial influence on the behavior of the system. The proposed detector uses these variables. The data collected for this purpose results from a hybrid data generation process with the SFC digital twin. In this process, the measured meteorological variables of plant operation, collected over 25 days, along with the presented controller outputs, are used to evaluate their behavior on the digital twin.

The controller and digital twin outputs generate three datasets together with meteorological measurements to assess the detector's performance. Case 1 involves positive data injection at the output temperature, case 2 has no fault injection, and case 3 involves negative injection at the SFC output temperature.

Next, an initial data processing task normalizes the variables to mitigate the inherent differences in their nature and scale, as well as the noise and discrepancies that typically impact the training procedure, as mentioned in (Chicaiza et al., 2022; Machado et al., 2023). Subsequently, normal operation (N), positive fault injection (F_{pos}) and negative fault injection (F_{neg}) on the outlet temperature of the heat transfer fluid make up three data groups, along with a general group (g) that aggregates data from both normal and faulty operations.

3.2 Data projection on the principal component

As outlined in Chicaiza et al. (2022), an offline PCA implementation is performed for each dataset, resulting in a covariance matrix $\mathbf{PCA}^s$ commonly referred to as the 'Loading Matrix'. This matrix encompasses the eigenvectors $\mathbf{v_r}$ and eigenvalues λ_r, indicating the orientation of the updated principal components space. Its purpose is to reduce the dimensionality of the variable space by projecting the original data, as described in Eq.(3)

$$^{N}\mathbf{T}^s = \mathbf{Z}^N \times \mathbf{PCA}^s \tag{3a}$$
$$^{Fpos}\mathbf{T}^s = \mathbf{Z}^{Fpos} \times \mathbf{PCA}^s \tag{3b}$$
$$^{Fneg}\mathbf{T}^s = \mathbf{Z}^{Fneg} \times \mathbf{PCA}^s \tag{3c}$$
$$^{g}\mathbf{T}^s = \mathbf{Z}^s \times \mathbf{PCA}^g \tag{3d}$$

where, $\mathbf{Z}^s$ is a matrix that contains normalized data for each group $s \rightarrow \{N, Fpos, Fneg\}$ and $\mathbf{T}^s$ is the matrix of scores for each s, which contains a new projected component in its corresponding Principal Component.

In general, the normalized data matrix $\mathbf{Z}^s$ is projected onto the first principal component, before calculating the explained variability ($0 - 100\%$) of the set of variables for each principal component, as noted in (Chicaiza et al., 2022). This new projected data set does not show correlation between variables. These projections are used in the ANFIS learning process. The training data set (80%) and the validation data set (20%) are created from these projected data. Furthermore, the sets of training (70%) and checking (30%) sets are formed from the learning data as follows:

$$^{N}\mathbf{Trn} = \left[{}^{N}\mathbf{T}^{N} \;\; {}^{N}\mathbf{T}^{Fpos} \;\; {}^{N}\mathbf{T}^{Fneg} \;\; {}^{g}\mathbf{T}^{N}\right] \tag{4a}$$

$$^{Fpos}\mathbf{Trn} = \left[{}^{Fpos}\mathbf{T}^{N} \;\; {}^{Fpos}\mathbf{T}^{Fpos} \;\; {}^{Fpos}\mathbf{T}^{Fneg} \;\; {}^{g}\mathbf{T}^{Fpos}\right] \tag{4b}$$

$$^{Fneg}\mathbf{Trn} = \left[{}^{Fneg}\mathbf{T}^{N} \;\; {}^{Fneg}\mathbf{T}^{Fpos} \;\; {}^{Fneg}\mathbf{T}^{Fneg} \;\; {}^{g}\mathbf{T}^{Fneg}\right] \tag{4c}$$

As can be seen, the projection of each group onto the others forms the training set, where the first three vectors serve as input for adjusting the parameters of each ANFIS to match the output, which is the last vector in each set. Similarly, the same procedure is followed to obtain the validation and testing sets.

3.3 Learning process of the detector

The configuration of the neurofuzzy detector comprises three FISs in parallel, derived from the training stages of three ANFIS networks. Each ANFIS network, as described in Jang (1993), utilizes training and checking sets to capture the fault behavior during the learning process. The ANFIS assesses the normalized root mean square error of both the training and checking sets. This evaluation prevents the model from overfitting solely to the training set, ensuring that the resulting FIS produces appropriate outputs for values not encountered during the learning phase. This approach aims to facilitate general learning across both datasets, as elaborated in (Chicaiza et al., 2022).

The training process for each ANFIS begins with the application of a clustering method, precisely the subtractive grouping technique (Machado et al., 2023). This method estimates the quantity and initial centers of the Gaussian membership functions used in the fuzzy rules. Subsequently, the elements of each ANFIS layer undergo a hybrid training approach, combining gradient descent with least squares estimation. This hybrid method is employed to obtain the elements defining the membership function of each fuzzy set (Gaussian standard deviation and mean). The deviation and mean are referred to as the antecedent parameters through gradient descent. The consequent parameters, in turn, determine the coefficients of every first-order polynomial function (g_{ij}) for each epoch or sweep using least squares.

After completing the ANFIS learning process, FIS^{N}, FIS^{Fpos} and FIS^{Fneg} have been obtained, both of which model the behavior of the faults in T_{out}. Each FIS contains two Gaussian membership functions for input and two Takagi–Sugeno type rules, outlined as follows:

$$\begin{aligned}&\texttt{IF } x_1 \texttt{ is } F_{1j} \texttt{ and } x_2 \texttt{ is } F_{2j} \texttt{ and } x_i \texttt{ is } F_{ij}\ ,\\ &\texttt{THEN}: f_j(x) = g_{0j} + g_{1j}x_1 + \cdots + g_{ij}x_i.\end{aligned}$$

The identification of fault injection data in T_{out} relies on the output of each FIS^{s}, obtained by projecting the input data set of the detector, $D^{in} = [Ht; Th; I_{eff}; T_{out}]$, onto the first principal component of the general group ($^{g}\mathbf{T}^{s}$). Subsequently, the detection considers both the exhaustive search algorithm and the comparator blocks, as shown in Figure 2, which comprises an exhaustive search and a rule, respectively. The Exhaustive Search involves a cost function that determines which FIS^{s} achieves the actual projection $^{g}\mathbf{T}^{*real}$ of a new incoming data set through direct evaluation, selecting the FIS that minimizes the cost function. The $\mathbf{FIS}^{s}$ that represents the minimum $J^{s} \rightarrow \left\{J^{N} \in 1, J^{Fpos} \in 2, J^{Fneg} \in 3\right\}$ identifies the group to which the updated data set (D^{in}) is associated.

$$J^{s} = \left\| {}^{g}\mathbf{T}^{*real} \; - \; {}^{g}\mathbf{T}^{s} \right\|_{2}^{2}. \tag{5}$$

Finally, the rule determines whether or not there is any data injection in T_{out}, as follows:

$\texttt{IF } J^{s} = 1 \texttt{ THEN } FDIdetection = 0 \texttt{ ELSE } FDIdetection = 1$

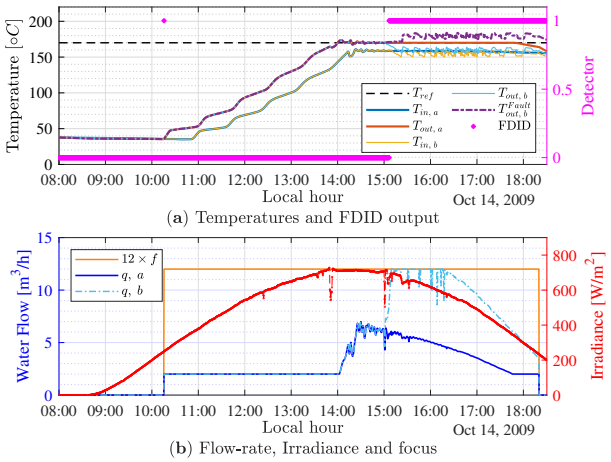
where $FDIdetection = 0$ indicates the normal state of the sensor and $FDIdetection = 1$ indicates the presence of data injection on the sensor in question.

4. RESULTS

The evaluation procedure involves the validation of the neurofuzzy detector using the validation data set. In this case, the control mentioned in Section 2 is implemented, together with the FSC Digital Twin, and incorporates the proposed neurofuzzy detector, as shown in Figure 1. The simulation with the control system employs actual meteorological variables of the plant operation. Three days of the total data comprising the validation set are used and organized in cases for clarity. During the second day (Case 2), no data injection is performed on T_{out}. On the first (Case 1) and third (Case 3) days, false data, both positive and negative, are injected until they reach a maximum or minimum value. In both cases, the ramp is $\pm 0.00277°C/20s$, which increases or decreases T_{out} progressively until it reaches a threshold of $\pm 20°C$. For all the cases mentioned above, false data injection occurs at 15:00 pm. In this way, the detector undergoes an evaluation without and with injection of fault data in two different ways.

If the new input D^{in} is free of the injected data, the output of FIS^{N} approximates the actual projection ($^{g}\mathbf{T}^{*real}$). On the other hand, if D^{in} includes the injection of false data in T_{out}, the output of (FIS^{Fpos}, FIS^{Fneg}) matches more closely the actual projection ($^{g}\mathbf{T}^{*real}$), depending on whether such injection occurs positively or negatively. The proposed Exhaustive Search block and comparator determine whether there is a false data injection in T_{out}. Subsequently, the rule within the comparator block identifies data injection and assigns the appropriate value to $FDIdetection$.

Figure 3.a depicts the behavior of the SFC when false positive data injection (Case 1) occurs on the sensor-transmitter. Note the difference between the orange line, for the outlet temperature without fault injection ($T_{out,\,a}$), and the dashed purple line ($T^{Fault}_{out,\,b}$), for outlet temperature with positive false data injection ($T^{Fault}_{out,}$) at 15:00. In Case 1 the detector successfully responds in the presence of false data injection, as can be seen by the FDI detection variable depicted as pink dots. Figure 3.a also illustrates the impact of false data injection in the operation and control of the process. The variables indicated by subindex a represent the FSC without fault data injection or normal operation, and the variables indicated by subindex b depict the FSC with faulty operation. Due to the positive injection of

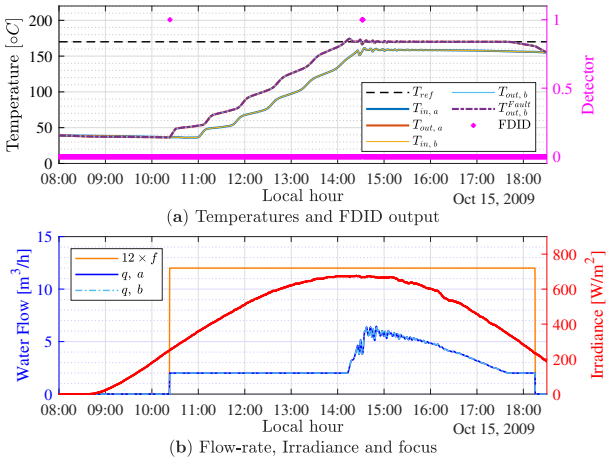


(a) Temperatures and FDID output

(b) Flow-rate, Irradiance and focus

Fig. 3. Case 1: Testing the NF detector with positive data injection. (a) Behavior of the outlet temperature and detector evaluation. (b) Fresnel's controller performance evaluation.

the corrupted outlet temperature, $(T_{out,\,b}^{Fault})$ deviates from the reference, and the controller attempts to deliver the maximum flow rate to stay at the set point. Figure 3.b contrasts the flow behavior considering normal flow $q,\ a$ and corrupted flow $q,\ b$. Consequently, flow affects the inlet temperature $T_{in,\,b}$ once the FSC collector process is a hydraulic loop, adding instability to the whole process.



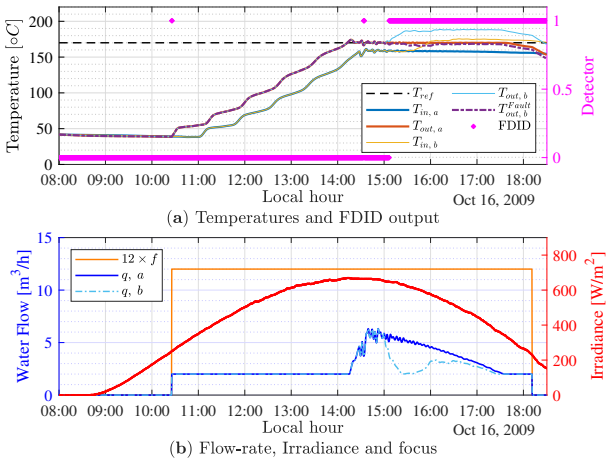
(a) Temperatures and FDID output

(b) Flow-rate, Irradiance and focus

Fig. 4. Case 2: Testing the NF detector with no fault injection data. (a) Behavior of the outlet temperature and detector evaluation. (b) Fresnel's controller performance evaluation.

Similarly, Figure 4 shows the results, as explained in detail in the previous paragraph. In Case 2, there is no false data injection, so $(T_{in,\,b},\ T_{out,\,b},\ q,\ b)$ are equal to $(T_{in,\,a},\ T_{out,\,a},\ q,\ a)$. The same is true for $(T_{out,\,b}^{Fault})$, which has the same behavior as (T_{out}). Note that the FDI detector indicates the absence of false data injection.

The results with false negative data injection (Case 3) are shown in Figure 5. The description of each of the legends is the same as shown in Case 1. Case 3, like the previous cases, shows the behavior that the plant would have in the absence of false data injection $(T_{in,\,a},\ T_{out,\,a},\ q,\ a)$. In addition, it shows how it would behave if false negative data injection were to occur. In this case, $(T_{out,\,b}^{Fault})$ follows



(a) Temperatures and FDID output

(b) Flow-rate, Irradiance and focus

Fig. 5. Case 3: Testing the NF detector with negative data injection. (a) Behavior of the outlet temperature and detector evaluation. (b) Fresnel's controller performance evaluation.

the reference, since the controller sees this fault as a disturbance. However, the actual behavior $(T_{in,\,b}, T_{out,\,b}, q, b)$ shows that $(T_{in,\,b})$ will exceed (T_{out}^{Fault}) at approximately 16:00 and that the $(T_{out,\,b})$ is actually above the given reference for the controlled variable. Additionally, the FDI detection remains at 1 when such false data injection occurs.

Table 1 presents the confusion matrix to evaluate the proposed detector. This matrix shows the dispersion of the predicted data groups concerning actual data groups.

Table 1. Confusion matrix T_{out}.

		Estimated classes		
		$\mathbf{F_{pos}}$	$\mathbf{N}$	$\mathbf{F_{neg}}$
Actual	$\mathbf{F_{pos}}$	611	20	0
	$\mathbf{N}$	0	631	0
	$\mathbf{F_{neg}}$	0	20	611

Precision	100 %	94.04 %	100 %
Recall	96.83 %	100 %	96.83 %
Accuracy	97.89 %		

The confusion matrix presents a relevant performance of the fault data injection concerning the T_{out} variable. The detector successfully correctly classifies most of the occurrences. Positive and negative false data injection are highlights of the detector, reaching 100% precision in both categories.

Table 1 indicates that the detector also presents a high recall of 96.83% in detecting false negative and false positive data injection. However, the detector also triggers normal false detections for case 1 and case 3. In general, the detector has good performance, especially in classifying the $\mathbf{F_{pos}}$, $\mathbf{N}$ and $\mathbf{F_{neg}}$ classes. Precision and recall are high in all classes, and the general accuracy reached is 97.89%.

Table 2 provides the results of the neurofuzzy detector for the output temperature for the three cases. The neurofuzzy detector operates throughout each case. Overall, the detector demonstrates a robust ability to predict regular and failure instances, with a close match between predic-

Table 2. NF detector results for all cases

Group	Outlet Temperature			
	Predicted	Actual	False Normal	False Fault
Case 1: 14th October				
Normal	1279	1260	0	1
Fault	612	631	20	0
Total samples	1891	1891	20	1
Case 2: 15th October				
Normal	1886	1891	0	5
Fault	5	5	0	0
Total samples	1891	1891	0	5
Case 3: 16th October				
Normal	1275	1260	0	5
Fault	616	631	20	0
Total samples	1891	1891	20	5

tions and actual values. However, in case 1, false positives and negatives were observed for 1.11% of the total data. Case 3 presents false positives and negatives for 1.32% of the total data. In addition, Table 2 shows that case 2 practically does not present anomaly detection (0. 26%), a positive result for the detector's ability to discern typical situations correctly.

5. CONCLUSION

In conclusion, this study proposes a novel approach to detect false data injection through a structure composed of FISs resulting from a learning process of a set of ANFIS systems. The main objective of this research was to prove that an ANFIS is suitable for fault data injection. In addition, this work shows how a false data injection into the controlled variable causes the control itself to change, which generates a wrong operation of the FSC, which could lead to its total shutdown or damage. The simulation results on the DT of the FSC illustrate the effectiveness of the suggested approach to address the false data injection detection problem. The results show that the neurofuzzy detector provides a reliable and robust solution to the FDI detection problem in the output temperature sensor-transmitter. Overall, the study highlights the potential of the detector in combination with ANFIS and PCA as a promising approach for fault data injection cyber attacks. In future work, the failure in the other variables will be inspected, considering even simultaneous failures where the presented approach will be validated. Besides, it will developed an FDI-tolerant control system powered by the ANFIS detector introduced in this work.

ACKNOWLEDGEMENTS

The authors thank the European Commission for funding this work under the DENiM project. This project received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 958339. Also, this work has been financed in part by the Grant PID2019-104149RB-I00 funded by MCIN/AEI/10.13039/ 501100011033 and by CNPq projects 403949/2021-1 and 406477/2022-1.

REFERENCES

Aboelwafa, M.M.N., Seddik, K.G., Eldefrawy, M.H., Gadallah, Y., and Gidlund, M. (2020). A machine-learning-based technique for false data injection attacks detection in industrial iot. *IEEE Internet of Things Journal*, 7(9), 8462–8471. doi:10.1109/JIOT.2020.2991693.

Alleyne, A., Allgöwer, F., Ames, A., and et. al (2023). *Control for Societal-scale Challenges: Road Map 2030*. IEEE Control Systems Society.

Chicaiza, W.D., Dorado, F., Rodríguez, F., Gómez, J., and Escaño, J. (2022). Detección de ataques de inyección de datos falsos en turbinas eólicas mediante sistemas neuroborrosos. In *XVII Simposio CEA de ControlInteligente*, 66–77. Universidad de León. doi:https://doi.org/10.18002/simceaci.

Chicaiza, W.D., Gómez, J., Sánchez, A.J., and Escaño, J.M. (2024). El gemelo digital y su aplicación en la automática. *Revista Iberoamericana de Automática e Informática industrial*, 21(2), 91–115. doi:10.4995/riai.2024.20175.

Hsueh, M.C., Tsai, T., and Iyer, R. (1997). Fault injection techniques and tools. *Computer*, 30(4), 75–82. doi:10.1109/2.585157.

Jang, J.S.R. (1993). Anfis: adaptive-network-based fuzzy inference system. *IEEE Transactions on Systems, Man, and Cybernetics*, 23(3), 665–685. doi:10.1109/21.256541.

Liang, G., Zhao, J., Luo, F., Weller, S.R., and Dong, Z.Y. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, 8(4), 1630–1638. doi:10.1109/TSG.2015.2495133.

Machado, D., Chicaiza, W., Escaño, J., Gallego, A., de Andrade, G., Normey-Rico, J., Bordons, C., and Camacho, E. (2023). Digital twin of a fresnel solar collector for solar cooling. *Applied Energy*, 339, 120944. doi:https://doi.org/10.1016/j.apenergy.2023.120944.

Machado, D., Sánchez, A., Gallego, A., and et. al (2022). Split-range control for improved operation of solar absorption cooling plants. *Renewable Energy*, 192, 361–372. doi:https://doi.org/10.1016/j.renene.2022.04.064.

Mo, Y. and Sinopoli, B. (2010). False data injection attacks in control systems. *Preprints of the 1st Workshop on Secure Control Systems*.

Mohammadpourfard, M., Sami, A., and Seifi, A.R. (2017). A statistical unsupervised method against false data injection attacks: A visualization-based approach. *Expert Systems with Applications*, 84, 242–261. doi:https://doi.org/10.1016/j.eswa.2017.05.013.

Rodríguez, F., Chicaiza, W.D., Sánchez, A., and Escaño, J.M. (2023). Updating digital twins: Methodology for data accuracy quality control using machine learning techniques. *Computers in Industry*, 151, 103958. doi:https://doi.org/10.1016/j.compind.2023.103958.

Sargolzaei, A., Yazdani, K., Abbaspour, A., and et. al (2020). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics*, 16(6), 4281–4292. doi:10.1109/TII.2019.2952067.

Sánchez, A., Gallego, A., Escaño, J., and Camacho, E. (2019). Adaptive incremental state space mpc for collector defocusing of a parabolic trough plant. *Solar Energy*, 184, 105–114. doi:https://doi.org/10.1016/j.solener.2019.03.094.