Format for uploading details of completed projects

1. Project details

a. *Title*: **Study on Detection of False Data Injection (FDI) Attacks in Smart Grid Cyber-Physical Systems: A Machine Learning Approach**

b. *Institute*: IIT Ropar, Rupnagar, Punjab

2. Aim / Objectives:

- To study the in-depth understanding of False Data Injection (FDI) attacks in smart-grids, helpful in identifying potential deceptive behaviours from the perspective of attackers.
- To study how machine learning can aid in FDI attack detection in smart cyber-physical grids.
- To study how to maximize the performance and efficiency of the machine learning attack detection algorithms. Further, to develop a generalized, novel attack-detection algorithm that is robust and scalable across varying attack sparsity and data imbalance.
- To develop a simulation platform for various attack simulations and detection, performance evaluation, and validation.

3. Executive Summary (*One page*):

The work focuses on addressing the challenges of detecting false data injection attacks in the Automatic Generation Control (AGC) system by building a secure and robust framework using Multi-Layer Perceptron (MLP)- based Artificial Neural Networks (ANNs). Further, the attack is eliminated by implementing an H-infinity filter-based protection mechanism, which is validated in real time.

The executive summary of the work carried out in this project is as follows:

- Developed and implemented an ANN-based detection mechanism to detect FDI attacks such as step, ramp, pulse, sine, and state-dependent attacks. The data for training of ANN detectors is generated using the simulated model. The model is developed in DIgSILENT Power Factory. Different scenarios for several types of FDI attacks are created to improve the detection mechanism's accuracy. To increase the ANN's efficiency and reduce its false alarm rate, training features such as Mean, Standard Deviation, and Principal Component Analysis (PCA) are extracted from the

measured signals, including the Tie-line power deviations and Frequency deviation for each area.

- Further, developed a novel attack elimination mechanism by proposing a modified H-infinity filter algorithm.

- The proposed methodology has been validated in external hardware and by keeping the power systems in RTDS. The hardware setup consists of an RTDS simulator from RTDS Technologies that emulates a real-world power system, and a Raspberry Pi board on which the estimator is implemented. During sensor measurement data transfer, packet drops may occur, so the data must be retransmitted to maintain data integrity. The two-area system is designed in RSCAD, a front-end software for the RTDS hardware, and the model is transferred to RTDS for real-time simulation. These measurements collected from PMUs were sent from the RTDS over the Ethernet LAN using TCP/IP. The RTDS is equipped with a GTNETx2 card for data communication with other peripherals via socket protocols. The Raspberry Pi board runs continuously and listens for data transmitted from the GTNETx2 card over TCP/IP. The attack is modeled and implemented in RSCAD. A low-cost estimator proposed here is tested to detect these attacks and return this data, so proper compensating measures can be taken before deciding on ACE signals. This test environment is then validated for the attack scenarios. The performance of the proposed estimator is validated across different attack signals, including step, ramp, pulse, sine, and state-dependent attacks. The attack has altered the area frequency deviation of area 1 and the tie-line power deviation data before sending them to the estimator. The deployed ANN detector successfully detected the attacks. The attacked state estimation estimated attack signal has been communicated back to the two-area system running on RTDS to compensate for the FDI attacks using the compensating method. The hardware-in-loop (HIL) simulation results are almost identical to the simulation results.

4. Scope for further work:

The work has the scope of further research as follows:

a) A feedforward network with multi-layer perception is used to train the network. However, the network architecture of feedback loops and self-feedback loops can be explored to improve results. Furthermore, self-tuning can be explored to provide adaptiveness to changes in power system operating conditions.
b) In power system state estimation, an H-infinity filter is used, which requires the state-space system model information. Further, the study can explore model-free estimation algorithms that work across any system condition.
c) The study is only validated in laboratory conditions using RTDS; however, the study is also validated in real-life system conditions by implementing particle power systems.

5. Benefits visualized:

The proposed work does not require any specific hardware to implement. It can be easily implemented using the PGCIL's existing communication infrastructure in India.

The developed estimator code needs to be deployed in the microcontroller board, and the output can be directed toward the existing AGC infrastructure in the power grid for full implementation. However, the training of ANNs and filtering and control algorithms require retuning under new system conditions. It can easily be done by following the mathematical derivations in this work, which are available in our publications.

The work has produced the following publications for the benefit of the research community at large:

1. S Beura, B P Padhy, "A Novel Reduced-Order H_∞ Filter for Simultaneous Detection and Mitigation of FDI-Attacks in AGC Systems" in IEEE Transaction on Instrumentation and Measurement, Nov. 2022
2. S Beura, B P Padhy, "Effect of Cyberattack on Event Detection Algorithm in Distribution System using Synchrophasor Measurements" in NPSC conference, 2022, IIT Delhi, India.
3. S Beura, B P Padhy, "False Data Injection Detection using H Infinity Filter in an Automatic Generation Controlled Two Area Power System" ISGT 2023, Abu Dhabi (accepted)

The work has demonstrated the full capability of the detection and FDI attack-avoidance mechanism against various types of attacks, including step, ramp, pulse, sine, and state-dependent attacks. Also, it successfully detected and eliminated multiple attacks. This research is highly important for the Indian power sector in the current scenario. The research proposes a methodology to quickly detect FDI attacks and estimate the attack signal, thereby helping determine the attacker's behavior and intentions in causing power system disturbances. Further, it eliminates the attack by utilizing the estimated attack signal. The input signal to the overall detector and estimator is the PMU-measured output signal, and the ANN-based detector does continuous monitoring. A lot of communication is required in the Indian power grid, and the proposed setup can be easily integrated into SCADA and Wide-Area Measurement Systems (WAMS) architectures. The proposed methodology is highly sensitive and could detect and eliminate minute additions of false data in the communication signal.