***M.tech project presentation –Mid Semester***

# Detection and mitigation of cyber-attack in AC microgrid

Under the supervision of : **Dr Ranjana Sodhi**

**Presented by:**

**Mohd Anas Khan**

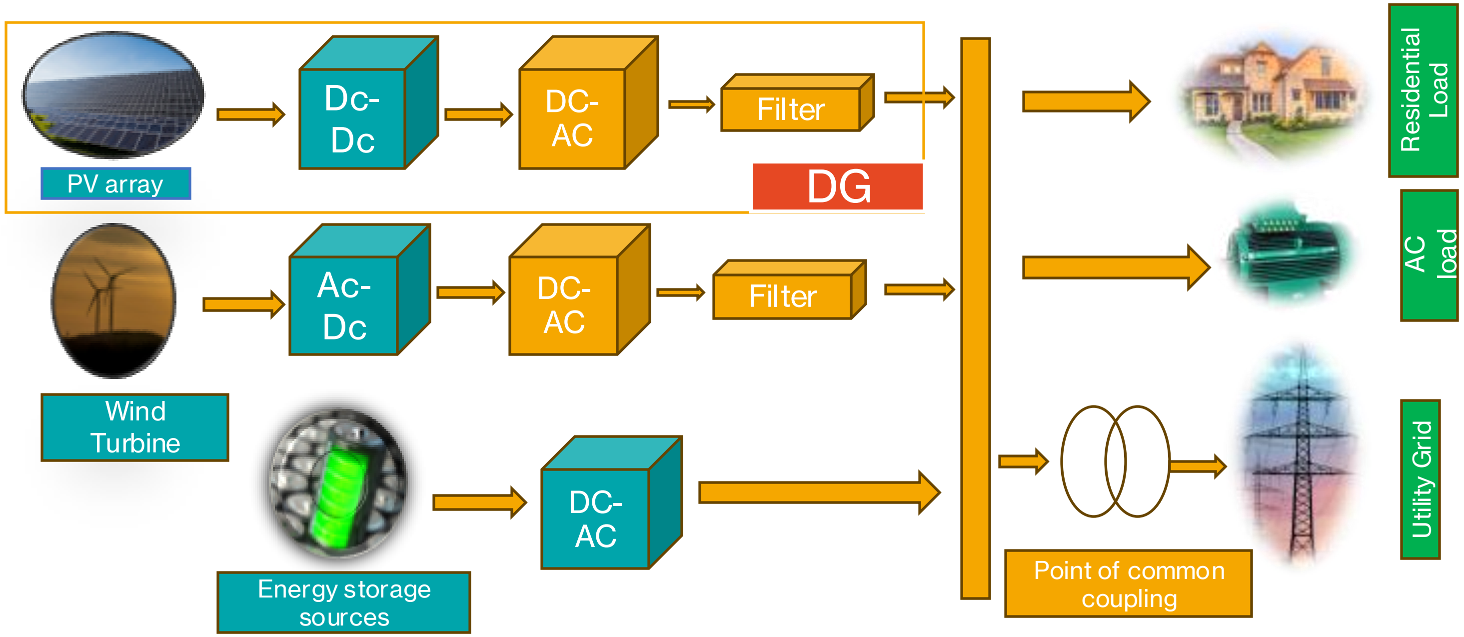
**2023eem1046**

# Outline

- Introduction to microgrid
- Literature review
- Research gap
- Motivation
- Work progress
- Results
- References

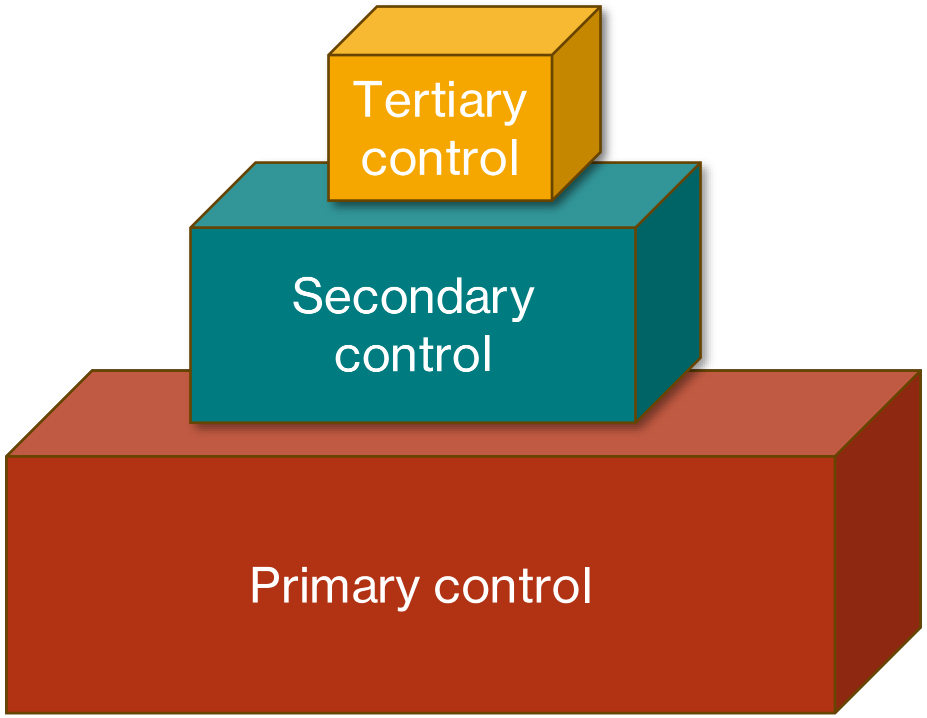
# Introduction to AC microgrid

- AC microgrid consists of distributed generation units, energy storage sources and load circuits.
- It can operate in islanded mode or in grid connected mode

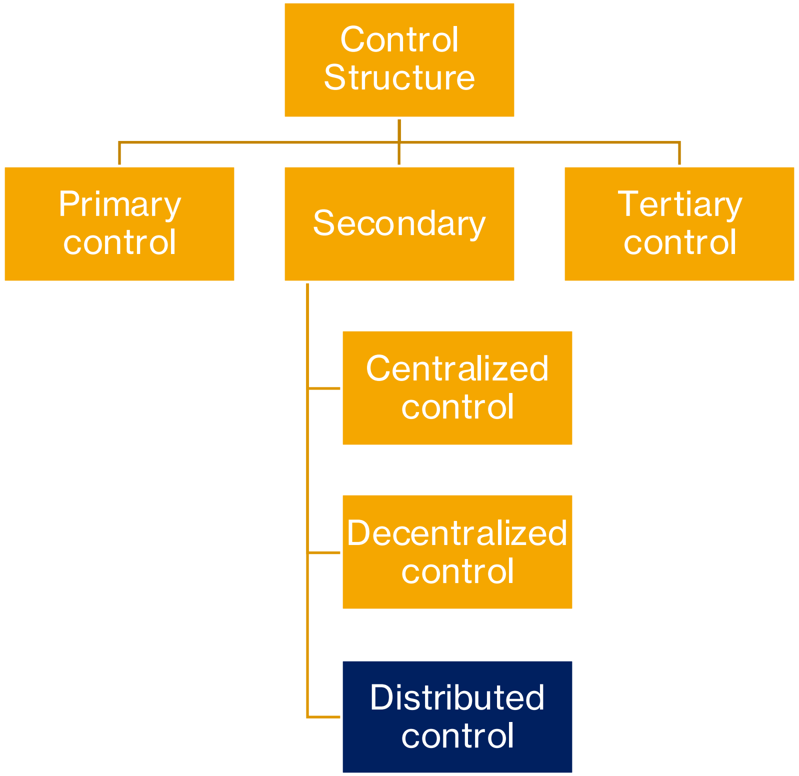



Structure of AC Microgrid

# Hierarchical control of AC microgrids

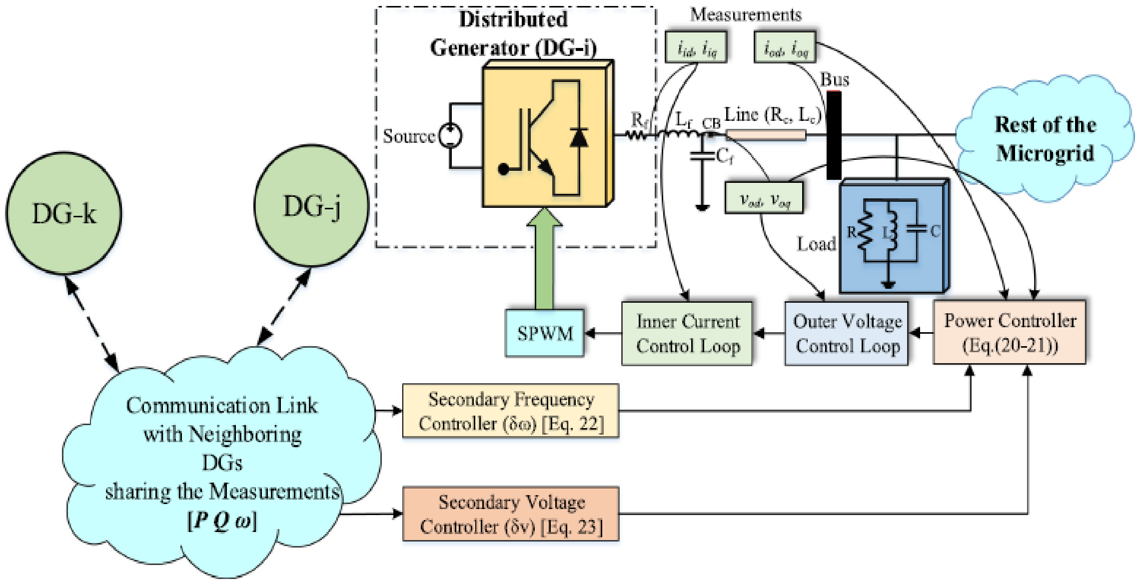


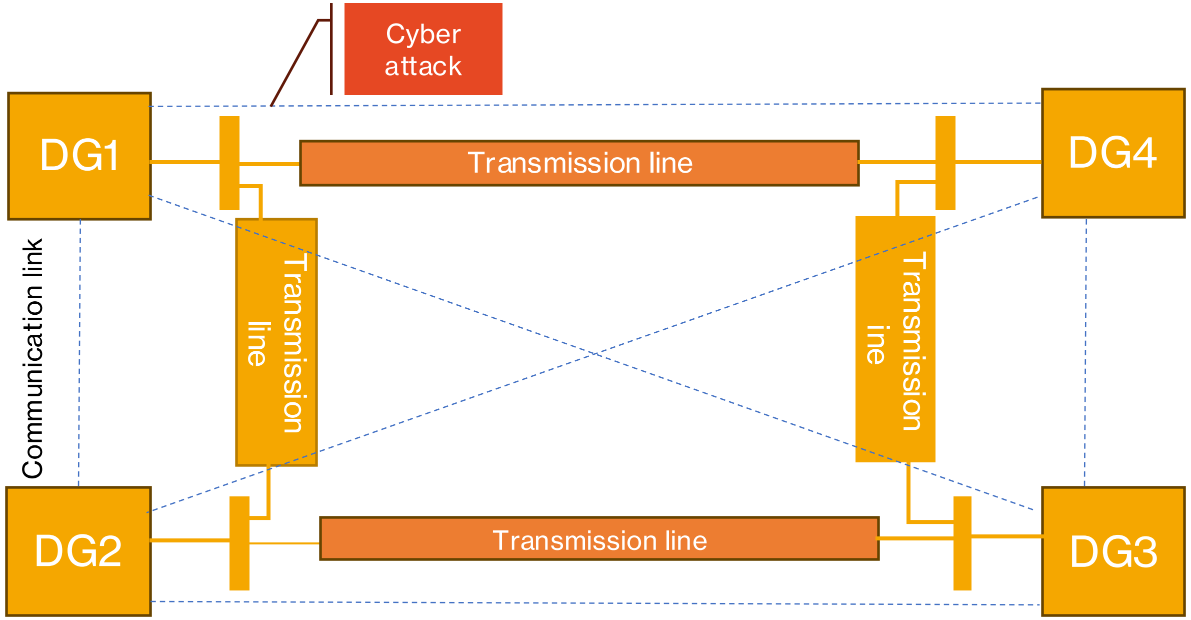

Hierarchical control



# Different types of control layer

- Primary control is used to stabilize the voltage and frequency and provide reference points for the voltage and current control loops of DERs .
- Secondary control is responsible for power quality enhancement, restoring frequency and voltage in the microgrid caused due to primary level droop control actions.
- Tertiary control is the slowest control level that considers the economic concerns in the optimal operation of microgrid and manage power flow between microgrid and utility grid.



# Literature Review

| Paper | Type of attack | Mitigation or detection | Simulation | Hardware | Distributed Control used |
|---|---|---|---|---|---|
| [1] | FDIA, controller hijacking attack, DOS attack | Only Vulnerability assesses | MATLAB | NO | Consensus based , average based, robust finite time |
| [2] | Balanced attack and unbalanced attack | asynchrony index-based detection metric, reconstructs a trustworthy frequency signal | Not mention (For fault cases, load variation also given) | No | Distributed Cooperative control |
| [3] | FDIA, DoS, Replay | For detection encoding and decoding using key is given, for mitigating Reconfiguration of network is given | MATLAB | Opal RT, Arduino, CAN bus protocol, Raspberry pi | Consensus distributed control |
| [4] | Only FDI | linear quadratic regulator (LQR) with unknown input observer for removing frequency deviation. | MATLAB Simulink | Opal RT | Something different because no inverter based DG is there |
| [5] | Trained for FDI, uncertainties related to solar radiance, wind irregularities, and noise did not consider faults | SVM classifier for detecting the attack And Reinforcement learning control is used. | MATLAB | No | Same setup as above paper |

# Literature Review

| Paper | Type of attack | Mitigation or detection | Simulation | Hardware | Distributed Control used |
|---|---|---|---|---|---|
| [6] | Strategic State-Dependent FDI Attack | Virtual layer base control is given | MATLAB Simulink | dSpace, Intelligent power module from semikron | consensus-based secondary control |
| [7] | Periodic FDI is given only, DoS attack is absent | Kulback-Liebler divergence factor method for detecting an attack.<br>And for mitigating the attack, concept of self and external belief of DER s is used | MATLAB (IEEE 34 bus test system with 6 DGs, an islanded MG with 20DER ) | Raspberry pi used for four DG and an OPAL RT used | consensus distributed secondary controller |
| [9] | Link, node, concurrent deception attack,<br>DoS attack is absent | Attack detection is simple and mitigation is removing that link | No | 14-bus/6-DG and 34-bus/8-DG isolated AC MG is in real time simulation environment in Opal RT. | PPD based consensus algorithm |
| [12] | Only FDI attacks | distributed adaptive frequency control algorithm | MATLAB | FPGA, Real time simulator | Distributed co-operative control is used |
| [13] | FDI attack is bounded and DoS attack has duration | | MATLAB | No | Distributed secondary control for DGs and ESSs so the control equations are little bit change. |

# Research gap

In most of the paper either they detect FDIA or Dos not both.

In some of the papers, machine learning based algorithm are used which are infeasible to implement on hardware.

Very few papers have implemented their strategy on hardware.

In some of the literature they mitigate attack by changing communication topology which is not a good way of mitigation as for this method required extra number of links.

# Motivation

Protecting the AC microgrid from cyber threat.

Develop a novel algorithm which is computationally less and feasible to implement on hardware also.

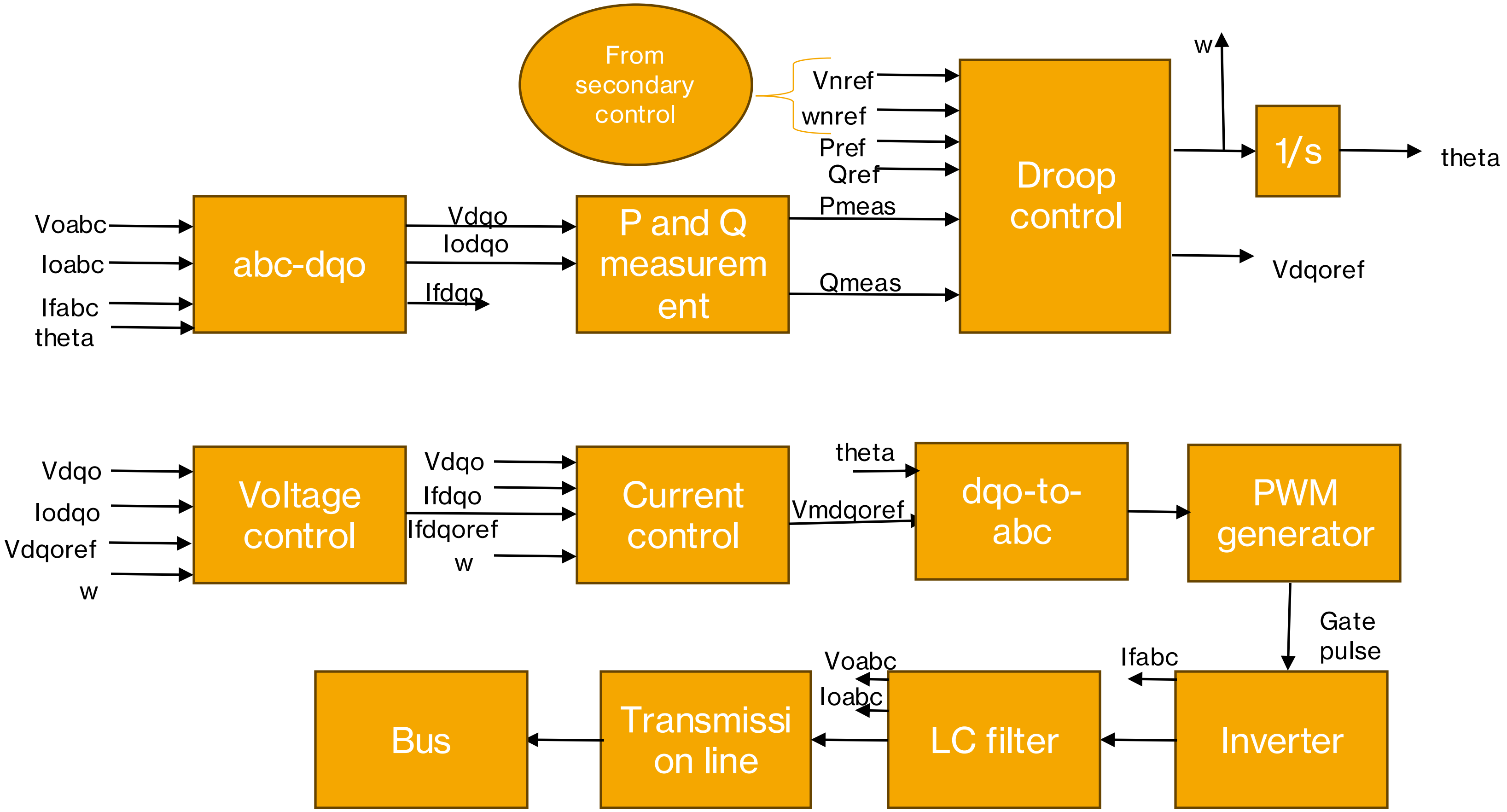
Detection of both Denial of service attack and false data injection attack by single algorithm.

Mitigation of these attacks to make AC microgrid resilient to these attack and able to supply critical loads.

Validation of proposed algorithm by implementing it on RTDS.

# Work progress

- Implementation of primary control of a DG.
- Four DGs of the same specifications are connected through transmission line



# Secondary control design

- $a_{ij}$ are the elements of adjacency matrix (A)
- $g_i$ is diagonal elements of pinning gain matrix (G).
- I have considered the DG1 as a master DG whose pinning gain is 1 all other DG have zero pinning gain.
- It provides reference value to the primary control.
- A = [0 1 1 0;1 0 0 1;1 0 0 0;0 1 0 0]

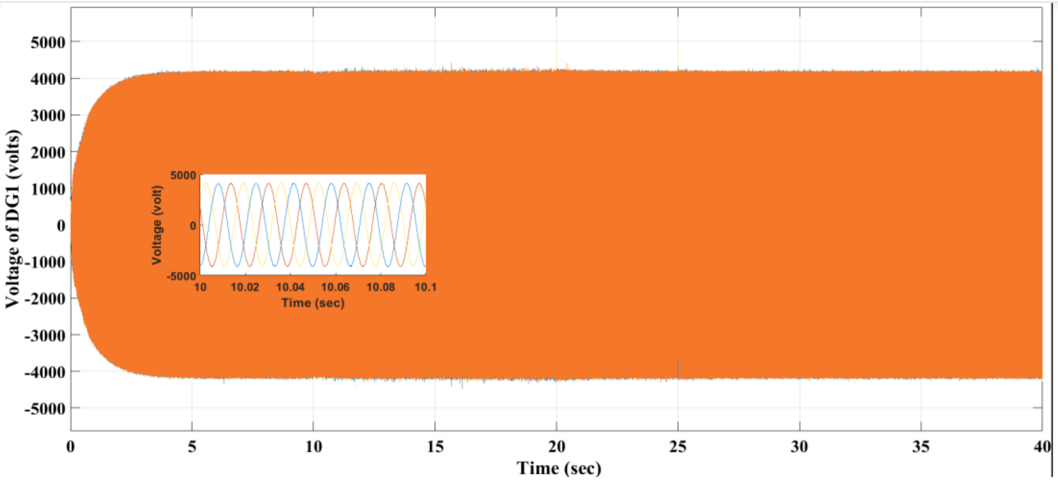
$$\omega_{niref} = -\int C_\omega * \delta\omega_i$$

$$V_{niref} = -\int C_v * \delta v_i$$

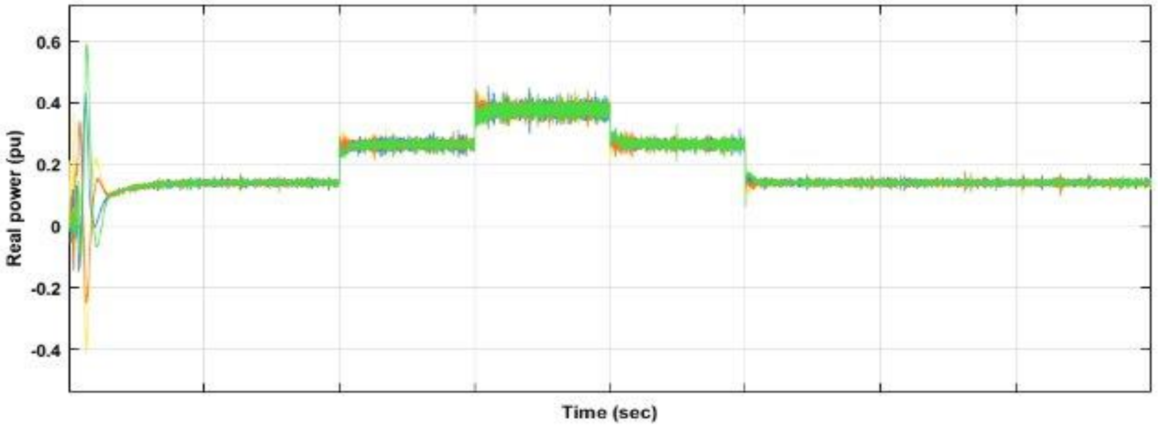
$$\delta\omega_i = \sum_{j\in N_i} a_{ij}(\omega_i - \omega_j) + g_i(\omega_i - \omega_{ref}) + \sum_{j\in N_i} a_{ij}(m_{pi}P_i - m_{pj}Pj)$$

$$\delta v_i = \sum_{j\in N_i} a_{ij}(V_{omag,i} - V_{omag,j}) + g_i(V_{omag,i} - V_{omag,j}) + \sum_{j\in N_i} a_{ij}(n_{qi}Q_i - n_{qj}Q_j)$$

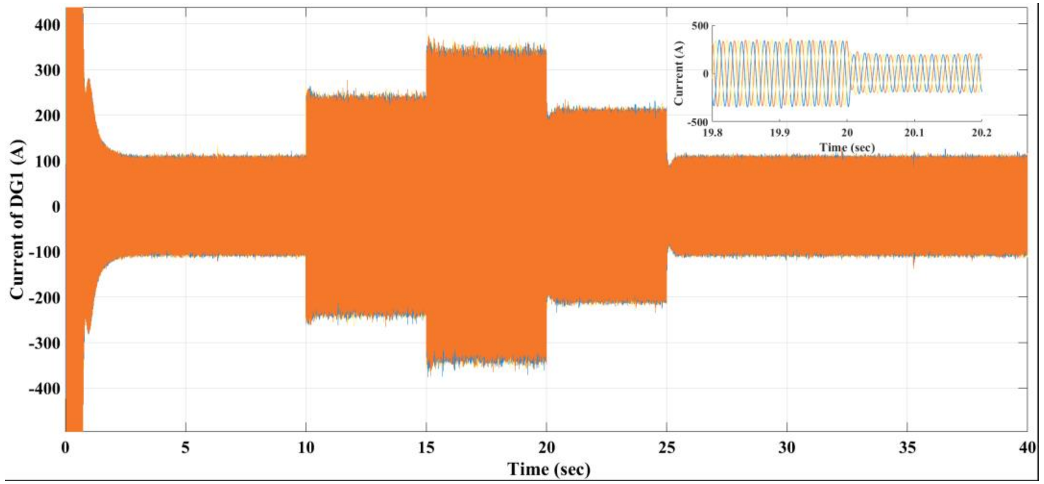
# Key Result



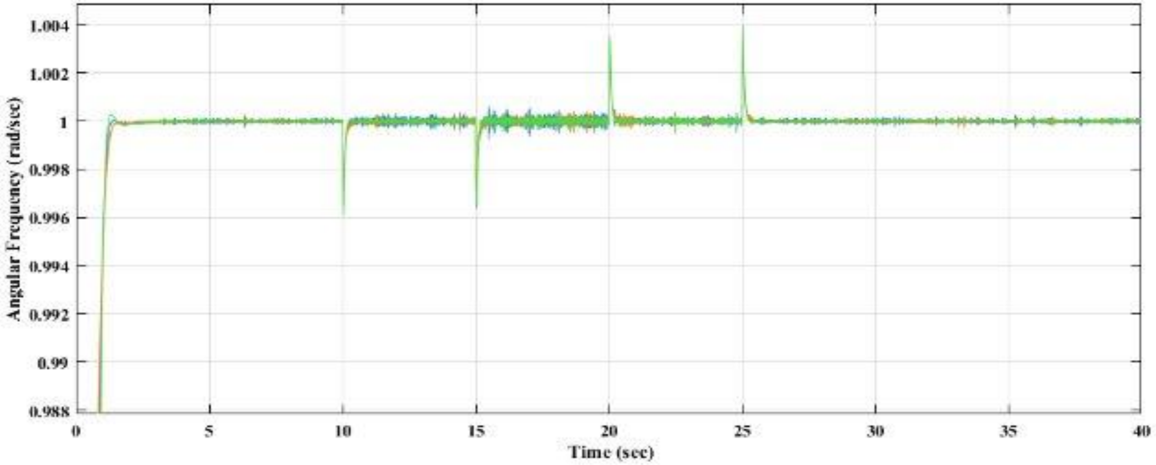
Voltage of DG1 (volts)
Time (sec)
Voltage (volt)
Time (sec)

Real power (pu)
Time (sec)

Current of DG1 (A)
Time (sec)
Current (A)
Time (sec)

Angular Frequency (rad/sec)
Time (sec)

# Timeline

## October

- Simulating the different types of attacks.
- Deployment of these DGs to IEEE 13 bus distribution system

## November

- Implementation of base paper for comparison.

# References


1. Z. Shahbazi, A. Ahmadi, A. Karimi and O. Shafiee, "Performance and Vulnerability of Distributed Secondary Control of AC Microgrids under Cyber-Attack," 2021 7th International Conference on Control, Instrumentation and Automation (ICCIA), Tabriz, Iran, 2021, pp. 1-6, doi: 10.1109/ICCIA52082.2021.9403548
2. S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," in IEEE Transactions on Power Electronics, vol. 36, no. 1, pp. 73-77, Jan. 2021, doi: 10.1109/TPEL.2020.3005208.
3. S. Rath, D. Pal, P. S. Sharma and B. K. Panigrahi, "A Cyber-Secure Distributed Control Architecture for Autonomous AC Microgrid," in IEEE Systems Journal, vol. 15, no. 3, pp. 3324-3335, Sept. 2021, doi: 10.1109/JSYST.2020.3020968.
4. M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban and A. Sargolzaei, "Resilient Frequency Control Design for Microgrids Under False Data Injection," in IEEE Transactions on Industrial Electronics, vol. 68, no. 3, pp. 2151-2162, March 2021, doi: 10.1109/TIE.2020.2975494.
5. Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control
6. M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo and F. Blaabjerg, "Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks," in IEEE Transactions on Industrial Electronics, vol. 71, no. 5, pp. 4719-4730, May 2024, doi: 10.1109/TIE.2023.3281698.
7. A. Mustafa, B. Poudel, A. Bidram and H. Modares, "Detection and Mitigation of Data Manipulation Attacks in AC Microgrids," in IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2588-2603, May 2020, doi: 10.1109/TSG.2019.2958014.
8. Residual-Based Detection of Attacks in Cyber-Physical Inverter-Based Microgrids
9. L.-Y. Lu, J.-H. Liu, S.-W. Lin and C.-C. Chu, "Concurrent Cyber Deception Attack Detection of Consensus Control in Isolated AC Microgrids," in IEEE Transactions on Industry Applications, vol. 59, no. 6, pp. 7584-7596, Nov.-Dec. 2023, doi: 10.1109/TIA.2023.3299256
10. S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese and A. Davoudi, "Synchrony in Networked Microgrids Under Attacks," in IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 6731-6741, Nov. 2018, doi: 10.1109/TSG.2017.2721382.
11. H. Yang, C. Deng, X. Xie and L. Ding, "Distributed Resilient Secondary Control for AC Microgrid Under FDI Attacks," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 7, pp. 2570-2574, July 2023, doi: 10.1109/TCSII.2023.3245282.
12. Distributed adaptive secondary control of AC microgrid under false data injection attack
13. A cyber-resilient control approach for islanded microgrids under hybrid attacks

# Thank You