UCONN

RISK ASSESSMENTS OF CYBERATTACKS TO DIFFERENT CONTROL ARCHITECTURES OF MICROGRIDS USING REAL-TIME TESTBEDS

HA THI NGUYEN

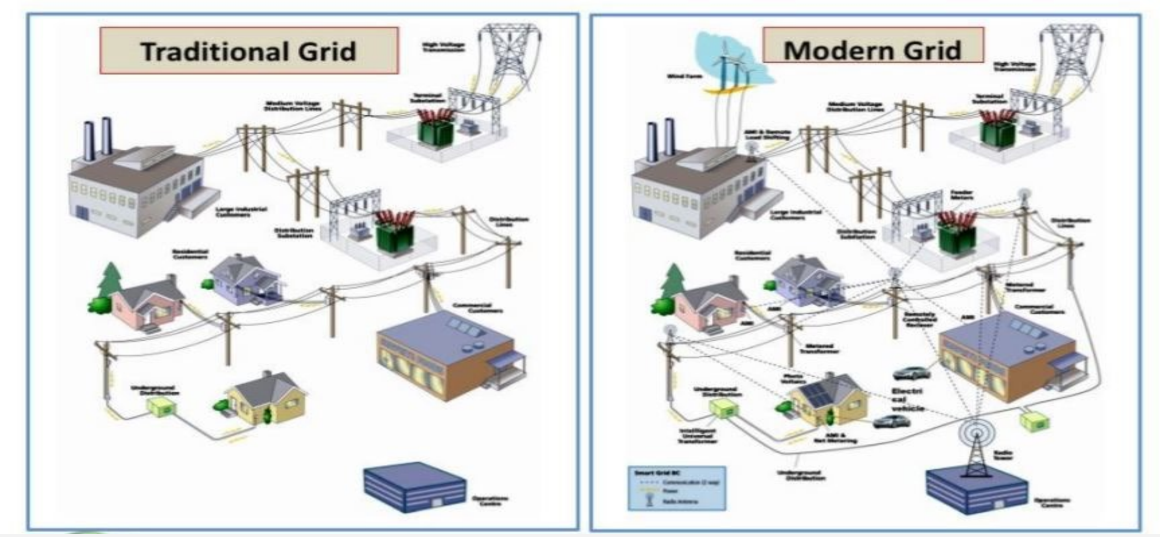
EVERSOURCE ENERGY CENTER, UNIVERSITY OF CONNECTICUT, CT, USA

AGENDA:

- ❑ Research overview
- ❑ Control Architectures & Methodology
- ❑ Testcase & Results
- ❑ Conclusions

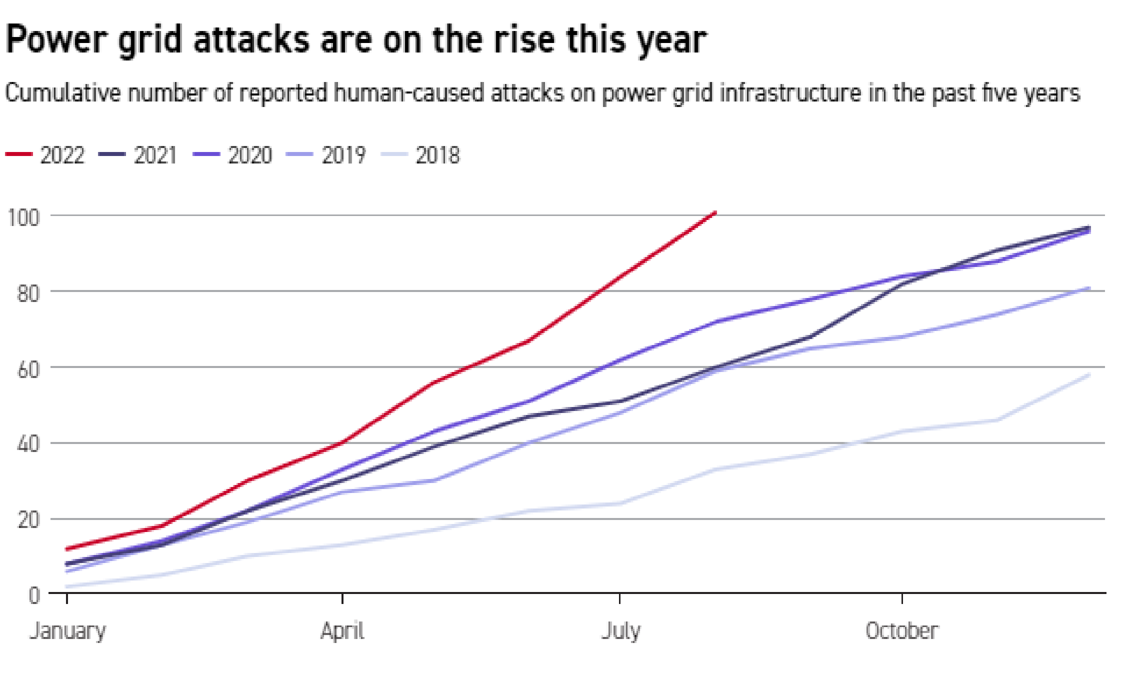
RESEARCH OVERVIEW

- ❑ Rapid integration of multi-vendor smart devices
- ❑ Transitioning to cyber physical systems (CPS)
- ❑ Vulnerabilities associated with the ICS (Industrial Control Systems)



Motivation:

- ❑ According to IBM study, 95% of cyberattacks have a human error component [1]
- ❑ Constant increase in cyberattacks on power grid in USA.
- ❑ Understanding the impacts of cyberattacks on CPS testbed would help with weaknesses in smart grids.



Cumulative human-caused attacks on US power grid [2]

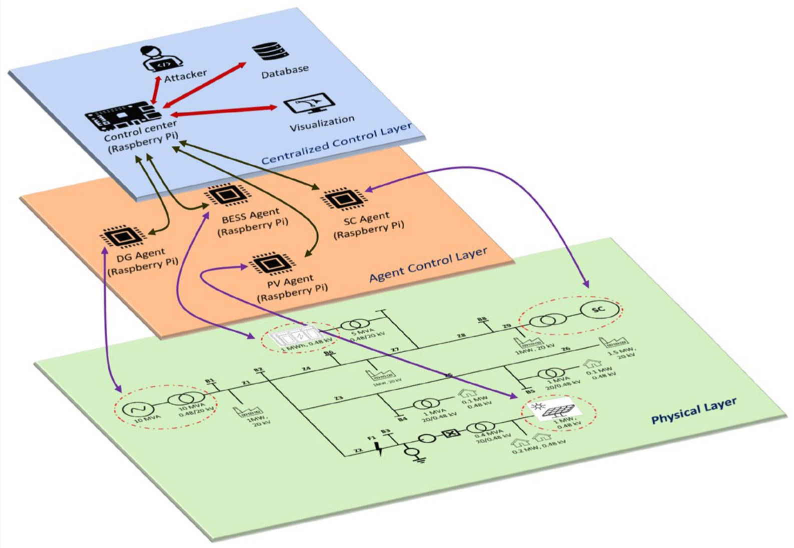
Contributions:

- ❑ Implementing CPS testbed with RTDS and Single board computer devices.
- ❑ Physical attack model implementation on CPS testbed.
- ❑ Exploring the impacts of DoS attacks on two different control architectures.
- ❑ Understanding the impacts with HiL testbed.

[1] Y. Soupionis and T. Benoist, "Cyber-physical testbed — the impact of cyber attacks and the human factor," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 326–331
[2] https://www.politico.com/news/2022/12/26/physical-attacks-electrical-grid-peak-00075216

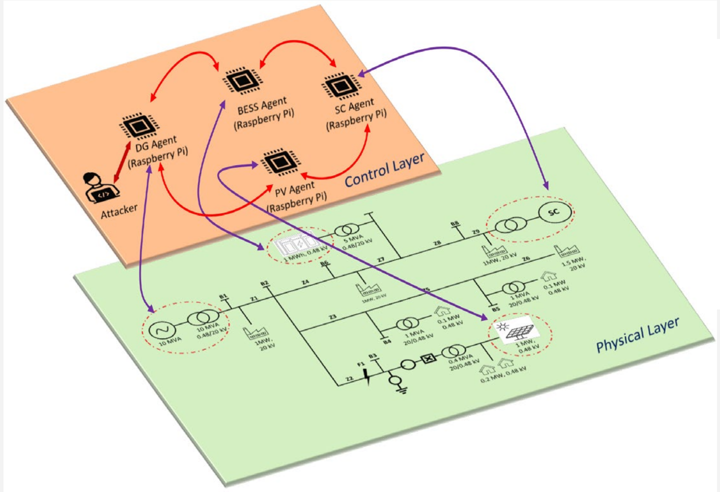
MULTI-AGENT SYSTEM CONTROL ARCHITECTURES:

Centralized secondary control architecture



- ❑ Traditional control architecture, with unidirectional messaging.
- ❑ Single point failure at the control center.
- ❑ Slow reaction to power system dynamics.

Distributed secondary control architecture



- ❑ Novel architecture with bi-directional informational exchange.
- ❑ This control architecture eliminates the single point failure as the secondary control action is distributed among agents.
- ❑ Faster reaction to power system dynamics.

Secondary control:

$$\nabla f_i = k_{pf}(f_i - f_{avg}) + k_{if}\int (f_i - f_{avg})dt$$

$$\nabla V_i = k_{pv}(V_i - V_{avg}) + k_{iv}\int (V_i - V_{avg})dt$$

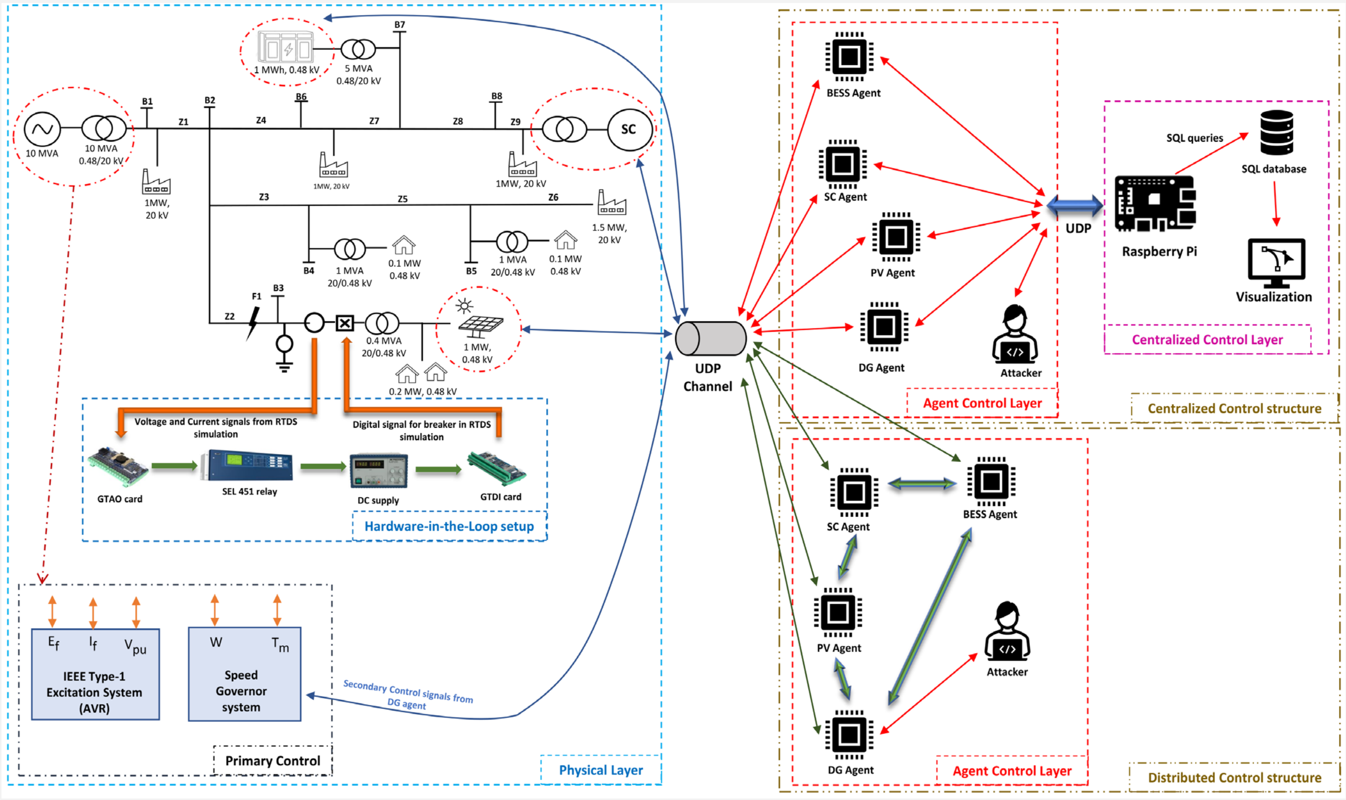
Average frequency $(f_{avg}) = \frac{\sum_{i=1}^{N} f_i}{N}$

Average Voltage $(V_{avg}) = \frac{\sum_{i=1}^{N} V_i}{N}$

$\nabla f_i, \nabla V_i$: Secondary control frequency & Voltage input for the i^{th} agent

N: Number of agents in Centralized control and Neighboring agents in Distributed control

CYBER-PHYSICAL TESTBED OVERVIEW:



Physical Layer :

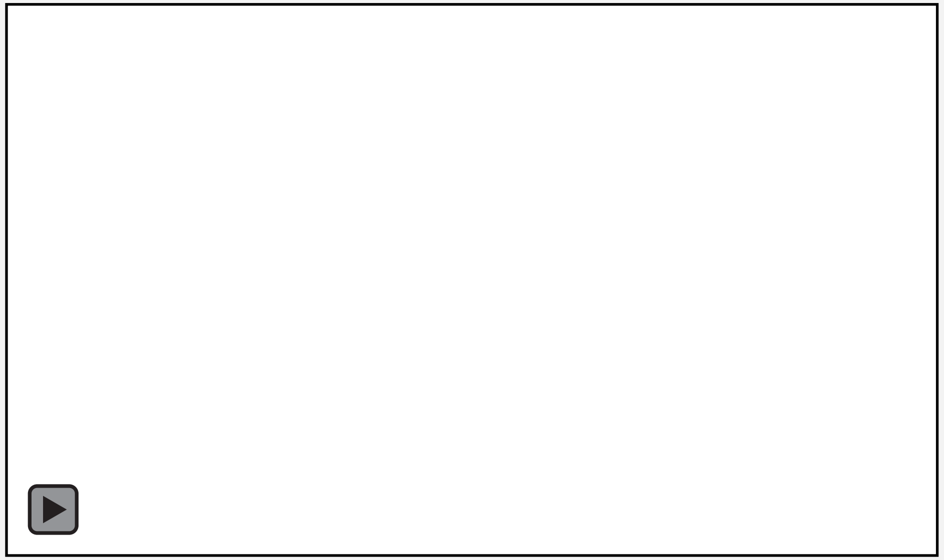
- Microgrid simulated in RTDS emulates physical layer.
- 1MW of PV and BESS with 10 MVA DG, forms microgrid.
- Hardware-in-the-loop setup with SEL relay to test the impacts of cyberattacks.
- The relay connected will act as a voltage relay with recommended settings under IEEE 1547

Cyber Layer :

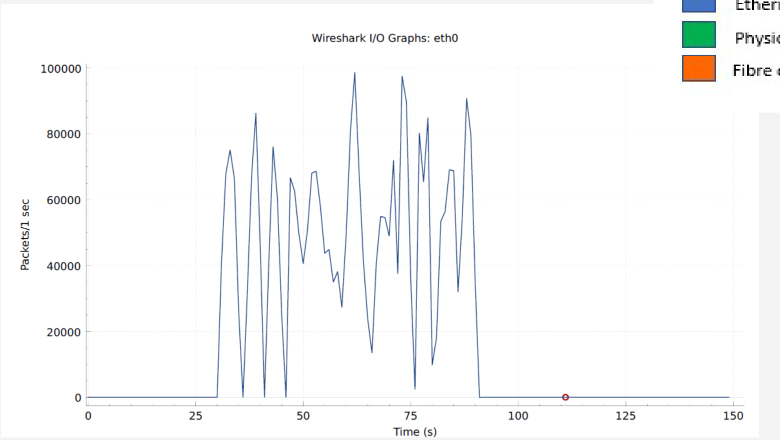
- SBC (Single Board Computer) devices works as agents in both control methodologies.
- UDP communication protocol is used for the communication.
- Physical attacker agent helps to simulate the network congestion during cyberattacks

DoS attacker agent and HIL implementation

- The DDoS attack map from [1] for the 2016 attack on the USA, shows the severity of cyberattacks.
- DoS is one of the simplest attacks to implement. A successful deployment of an attack could cripple the communication infrastructure.
- The DoS attack in the CPS testbed is implemented using ‘SYN flood’ method.

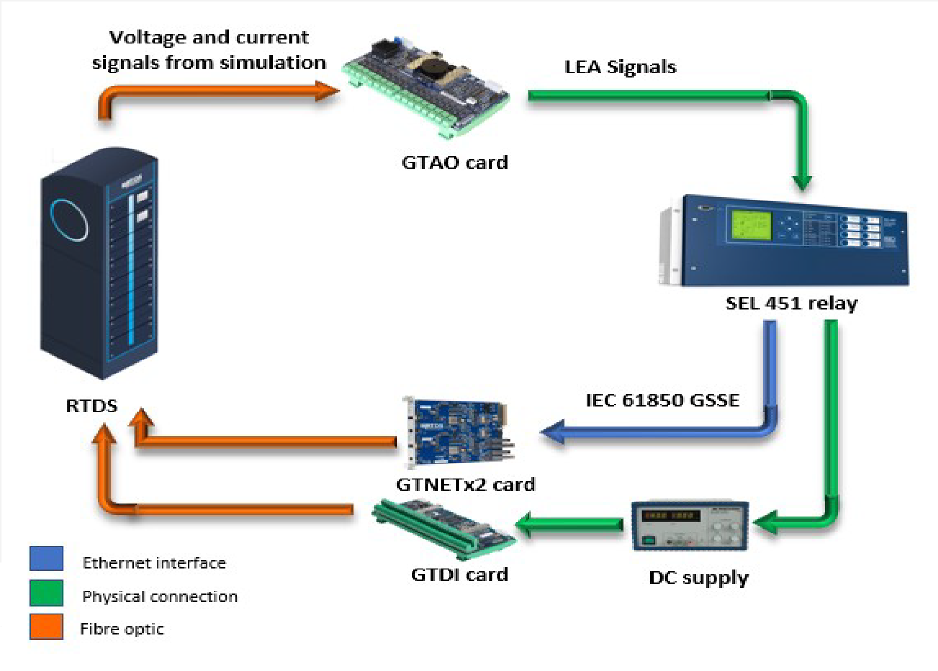


DDoS attack map for the 10/21/2016 attack [1]



Network traffic during DoS attack

HIL Implementation:



- Using LEA HiL for relay

Raspberry Pi 4B (DoS agent) [2]

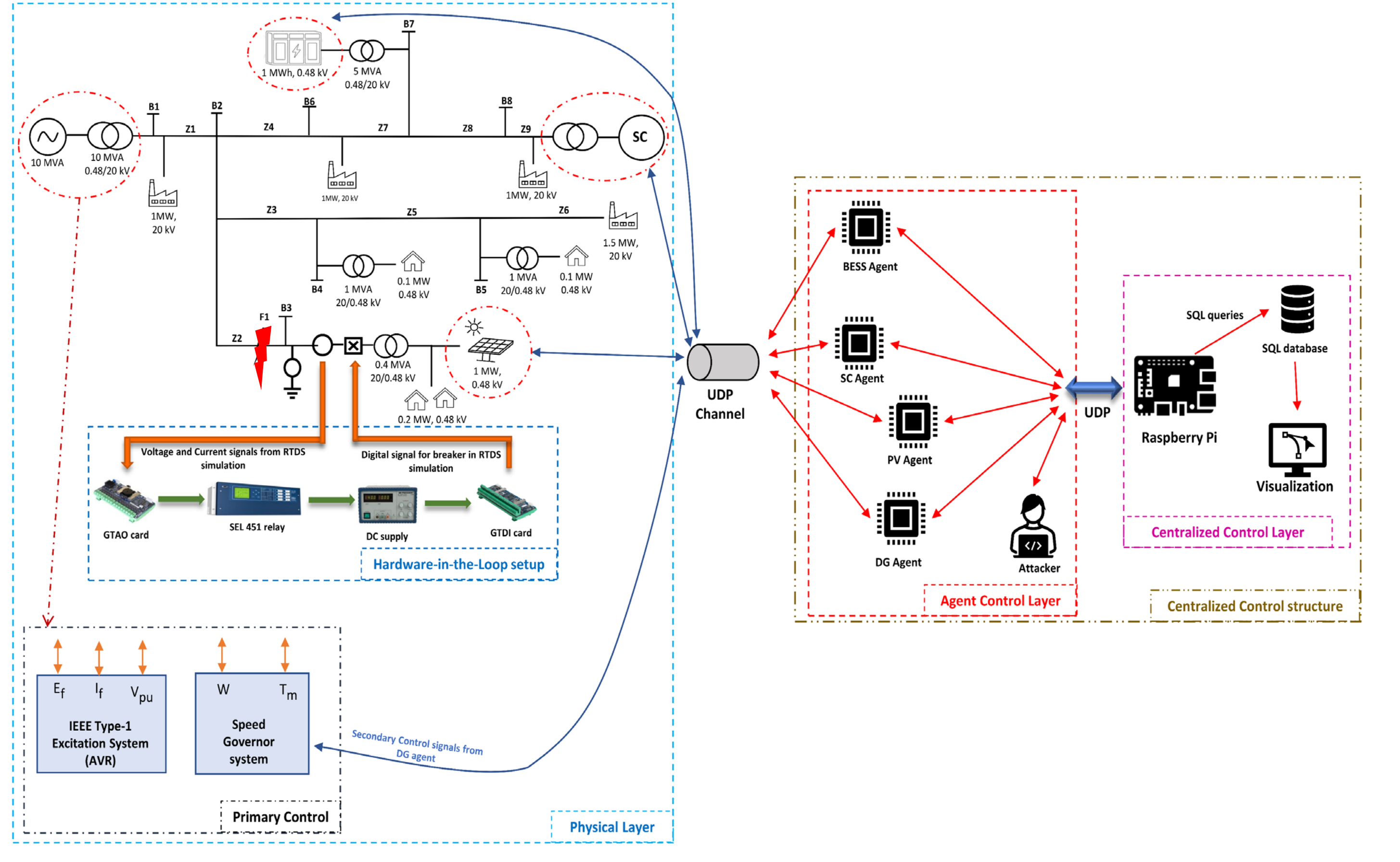
[1] https://horizon.netscout.com
[2] https://en.wikipedia.org/wiki/Raspberry_Pi

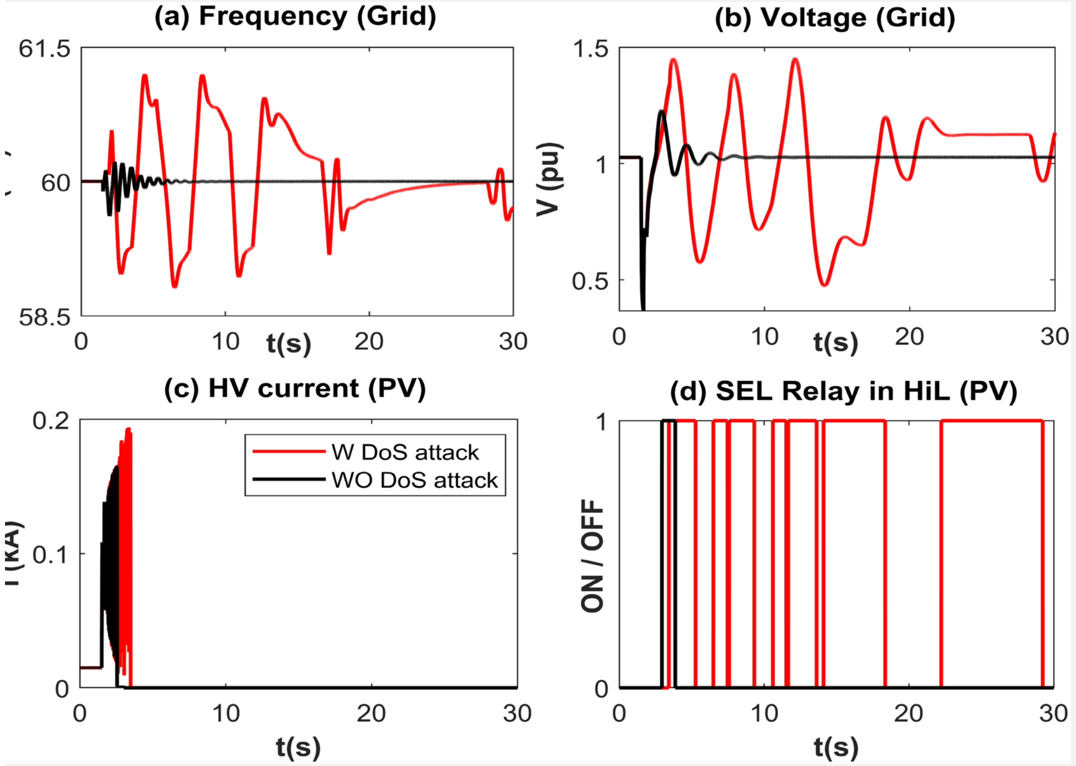
Testcase & Results:

DoS attack in Centralized control:

- The DoS attacks are simulated during the 3-Ph fault on the bus 'B3' for 10 cycles.

- The '**black**' curves in the plots show fault response under normal condition.
- The '**red**' curves shows the response during DoS attack on centralized control.
- The HiL test results shows the multiple operation of relay during DoS attack.





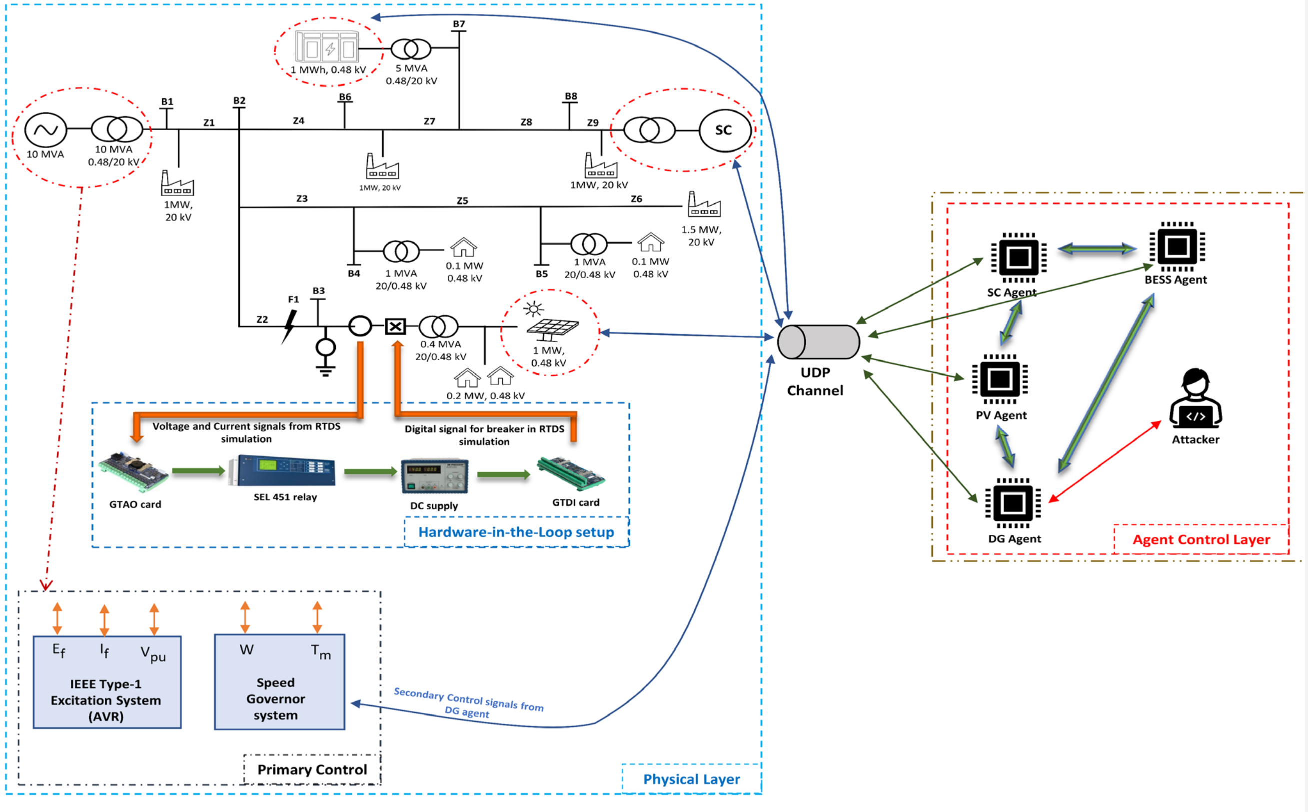
DoS attack on PV agent in the centralized control architecture

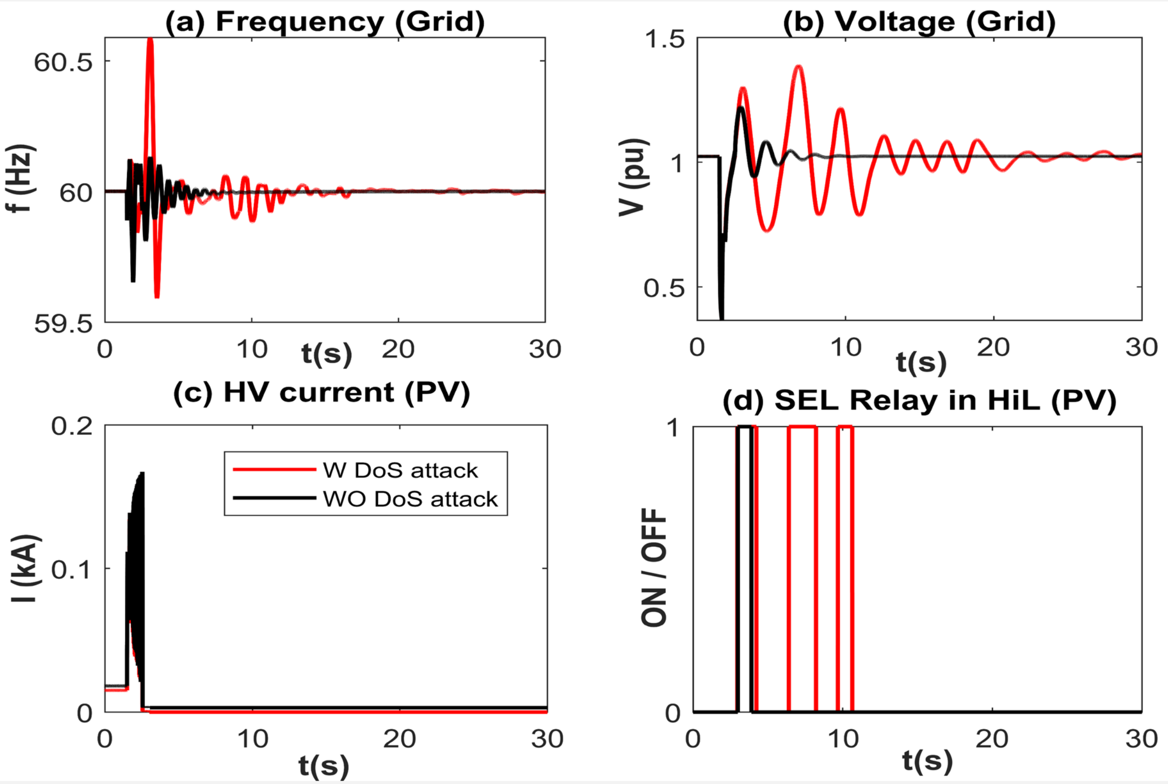
Testcase & Results:

DOS attack in Distributed control:

- ❑ In this control, DoS agent targets DG agent

- ❑ The **'black'** curves in the figures shows the fault response in distributed control
- ❑ The **'red'** curves shows the fault response during the DoS attack.
- ❑ Compared to centralized control, distributed control has no single point weakness, this salient feature of distributed control makes it **more resilient** to DoS attacks.





CONCLUSIONS:

- Two independent secondary control architectures are implemented in the Cyber-physical testbed.
- HiL testbed in the physical layer helps to study the physical impacts of the DoS attacks in both control architectures
- DoS attack is simulated using ‘SYN flood’ method with a physical agent (Raspberry Pi 4B).
- Distributed control architure offers **more resilient** solution for DoS attacks.
- Different types of cyberattacks on both control architectures should be further researched and validated

THANK YOU

Q & A