Panel Session on

Design and Simulation Tools for Secure Power Networks as Resilient CPS Infrastructures

- Prof. Osama A. Mohammed, Energy Systems Research Lab., ECE Department, FIU, Miami, FL
- Professor Lamine Milli, Virginia Tech
- Dr. Sandeep Shukla, Virginia Tech
- Professor Ganish Kumar Venayagamoorthy, Clemson, University
- Professor Marija Ilic, Carnegie Mellon University

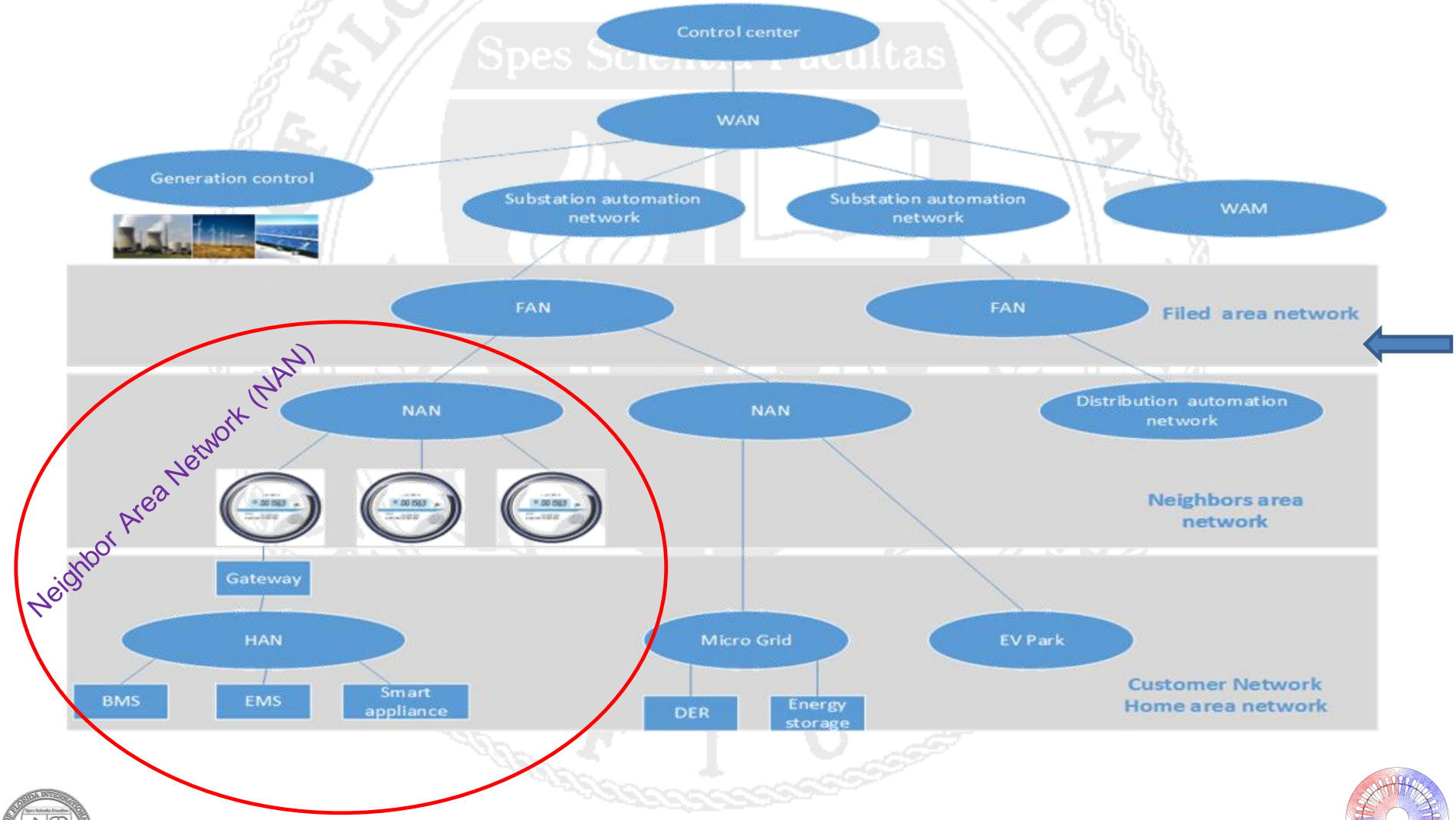
Challenges of integrating distributed resources

- Management of increased level of distributed and renewable energy sources
- Integrating a wide variety of systems governed by different regulations and owned by different entities.
- Variable nature of renewable energy sources which will increase the level of uncertainty in terms of generation resource availability
- real time energy forecasting and energy management system for generation and demand balancing.
- New distributed architectures with many microgrids.

We also have communication and control challenges:

- Interoperability between different protocols and applications.
- Communication network and bandwidth required to collect measurement and control remote sites.
- Data availability.

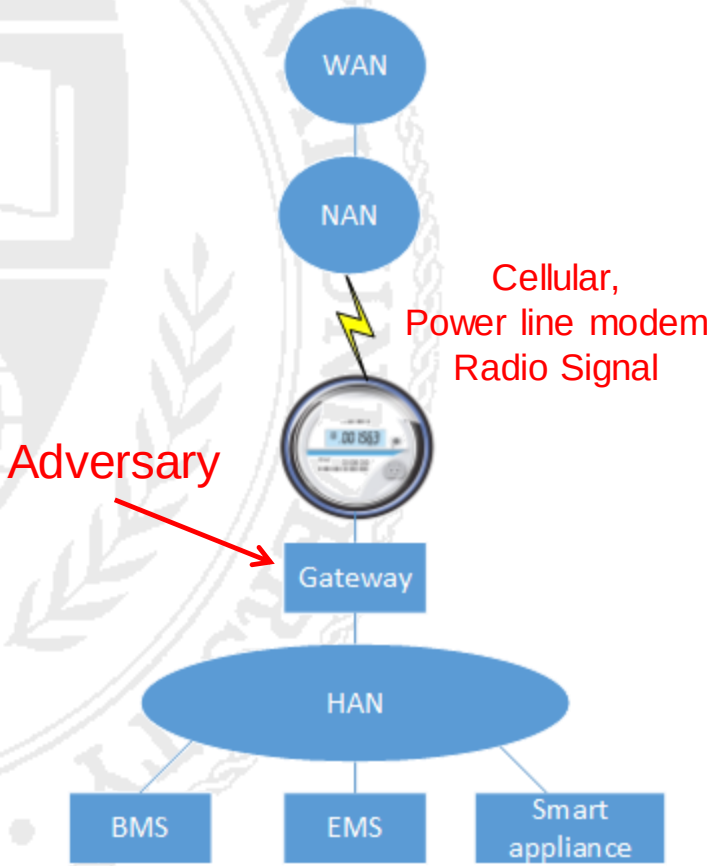
Smart Grid Cyber Infrastructure



Smart meter security threats

SMART Meter vulnerability:

- The AMI network is open to external unsecured environments such as cellular channels, power line carriers and radio signals.
- The AMI can provide a communication path to customer systems such as building management systems (BMS) through the customer gateway.
- If the adversary succeeds in penetrating into the AMI network and pretending to be a valid smart meter management system, he can easily send a disconnection signal to millions of customers.

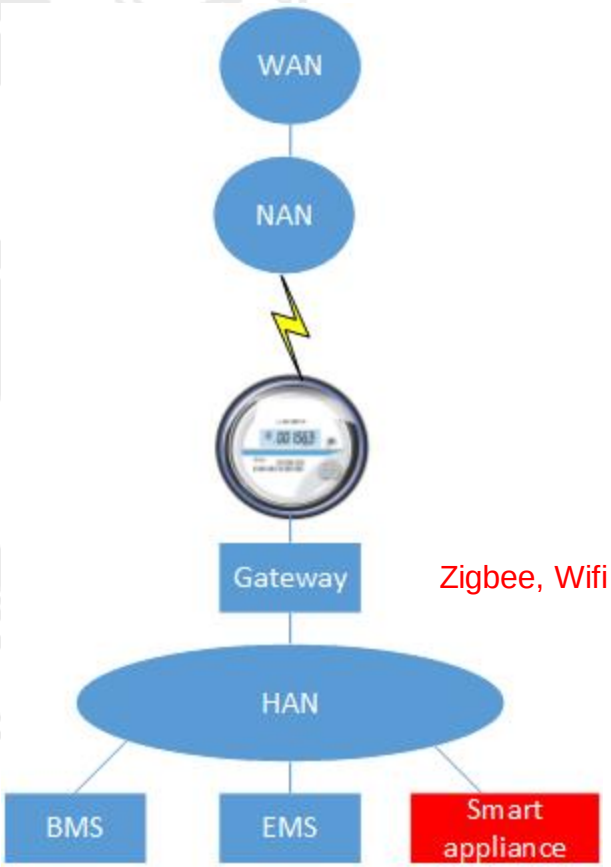


AMI: Advanced Meter Infrastructure

Smart meter security threats

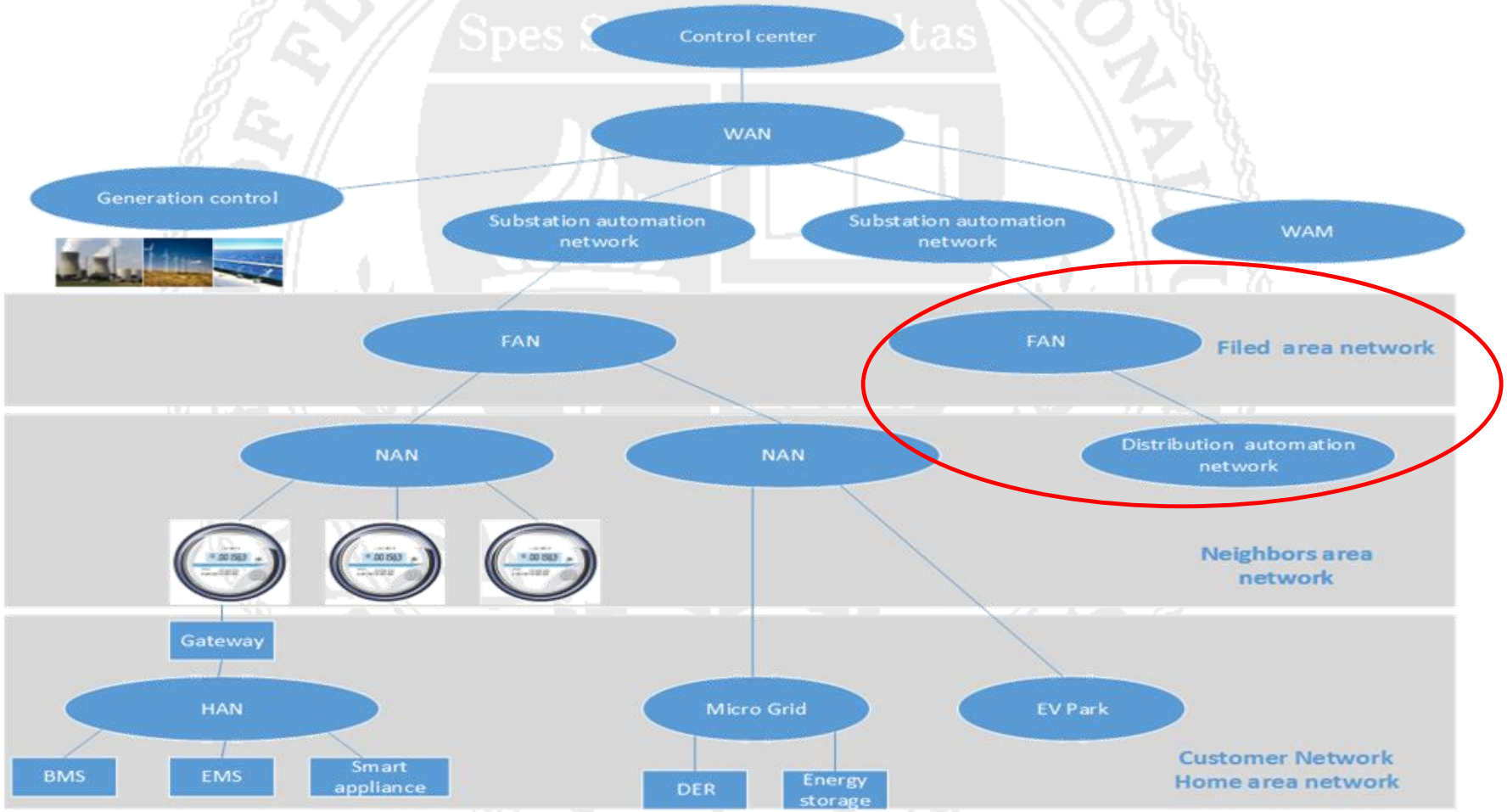
- In **January 16, 2014** Proofpoint, Inc. uncovered Cyber attack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks.
- The network topology should prevent interaction between customers in the NAN.
- Price signal should be authenticated
- Smart meters use X.509 certificate.
- Most of the smart meters doesn't update the certificate for life time.

Example: an attack on a customer appliance



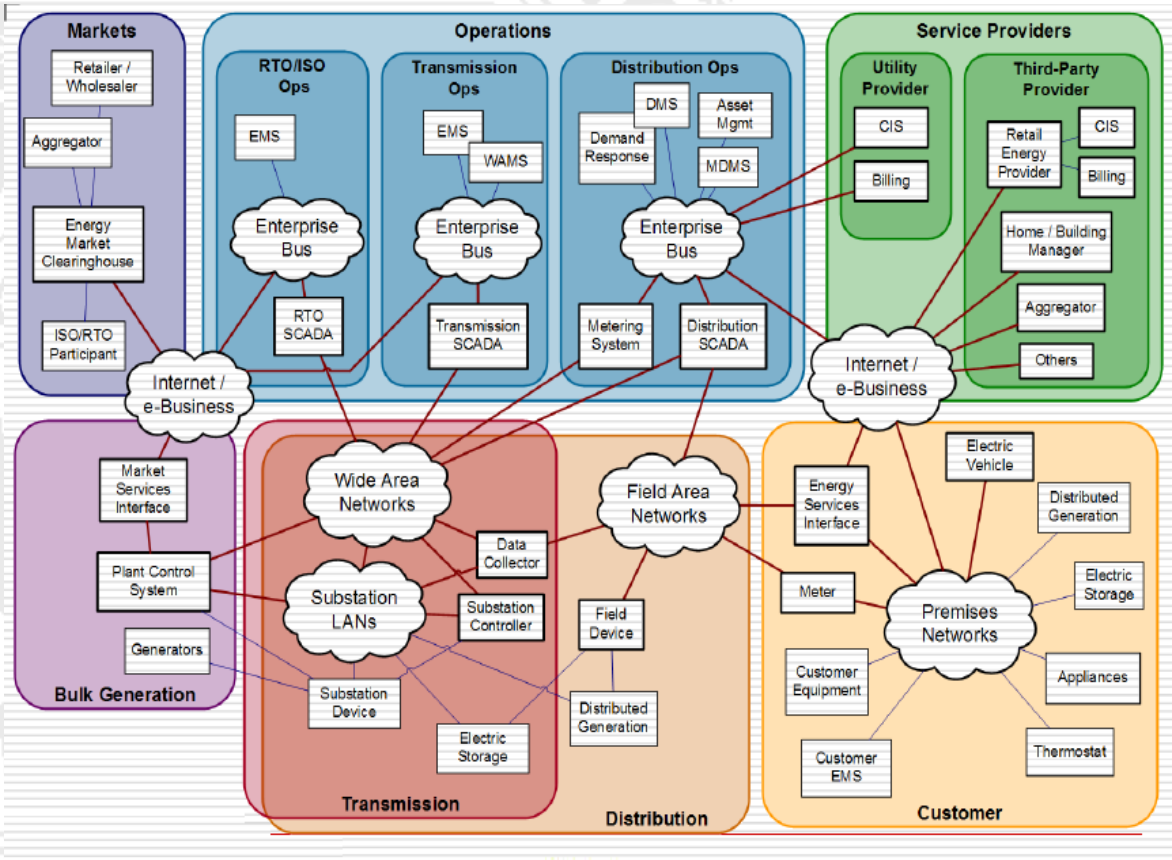
X.509 Certificate is an Authentication Protocol

Smart Grid Cyber Infrastructure



Field Area Network (FAN)

- FAN shared multi service IP network cover Distribution automation, Integrated Distributed resources, Demand Response and field devices
- Based on Broad Band wireless resources. FAN routers has WIFI interface for field technician.
- Data integrity and confidentiality should be ensured for smart meter data and field devices.
- If adversary succeed to compromise FAN router he could be easily send wrong signal to switches or field devices

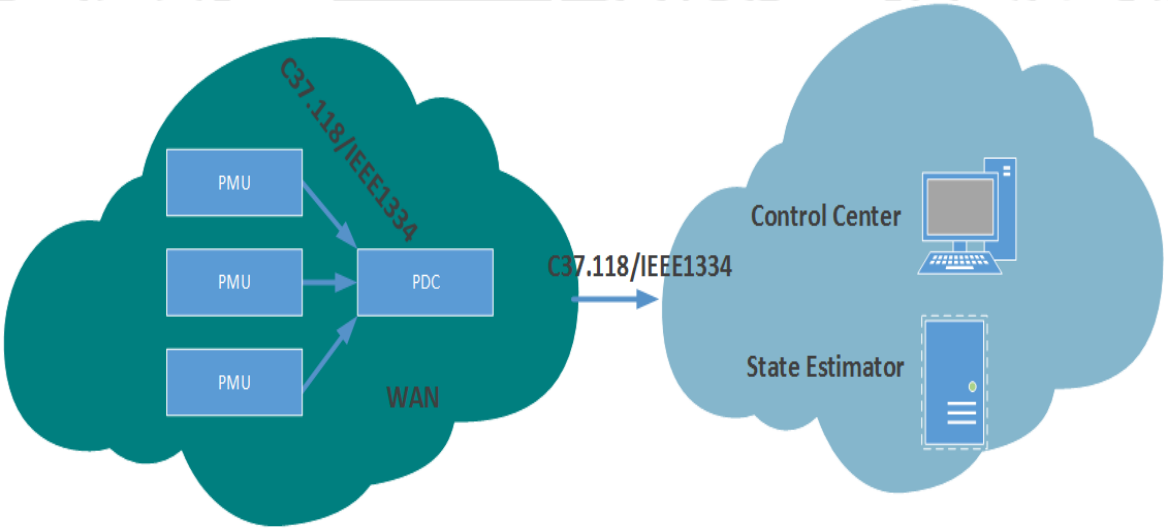


NIST reference Model

Wide area Monitoring security Threats

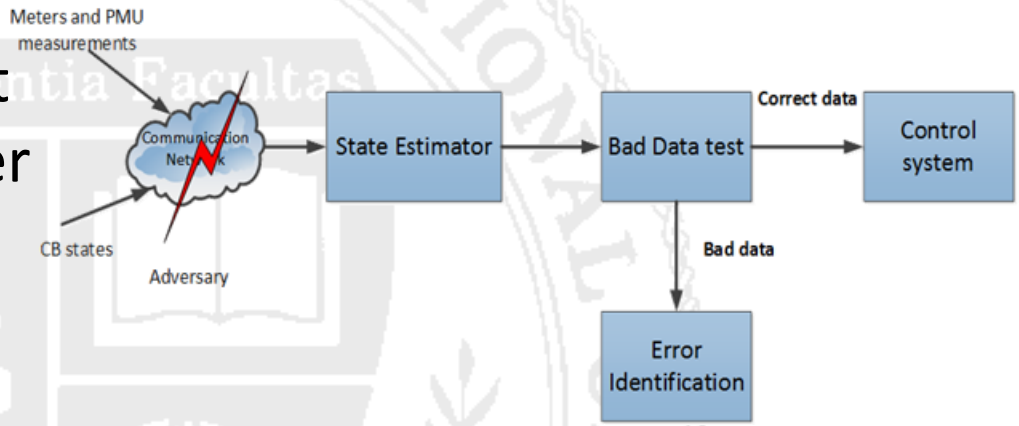
Security challenges:

- Most of the protocols were developed for efficient data transmission in isolated control network without considering security required for wide spread and open system.
- Phasor Measurement units PMU depend on external clock source which can be spoofed or jammed.
- PMU protocols (C37.118 and IEEE 1334) doesn't support authentication or data integrity check



Wide area monitoring security threats

- Lack of authentication and data integrity make different attack possible against power system measured data and control signals.
- Cyber attack against measured data can be used to perform different types of attack against the power system control and operation such as state attack and topology attack

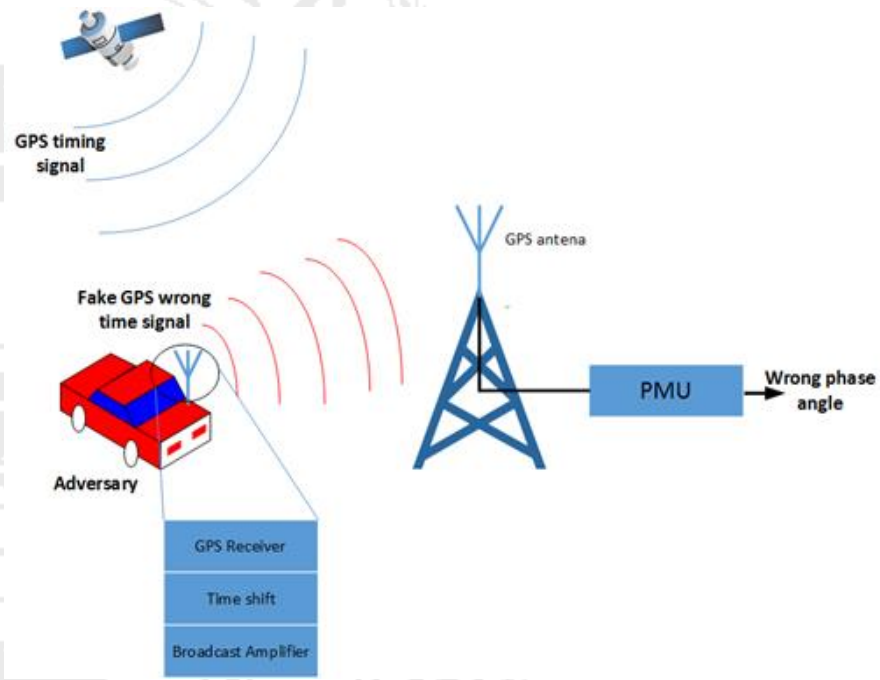


To design security aware WAM different factors should be considered in the security system design such as

- system topology,
- sensor locations
- communication protocol

PMU attack using GPS spoofing

- An adversary can spoof a weak GPS signal by broadcasting a signal with incorrect time data from any location close to the GPS antenna.
- PMUs on Critical buses could be protected by using phased array antenna.
- The number of and location of PMUs and meters should be also selected to avoid undetectable state estimation attacks such as state and framing attack.

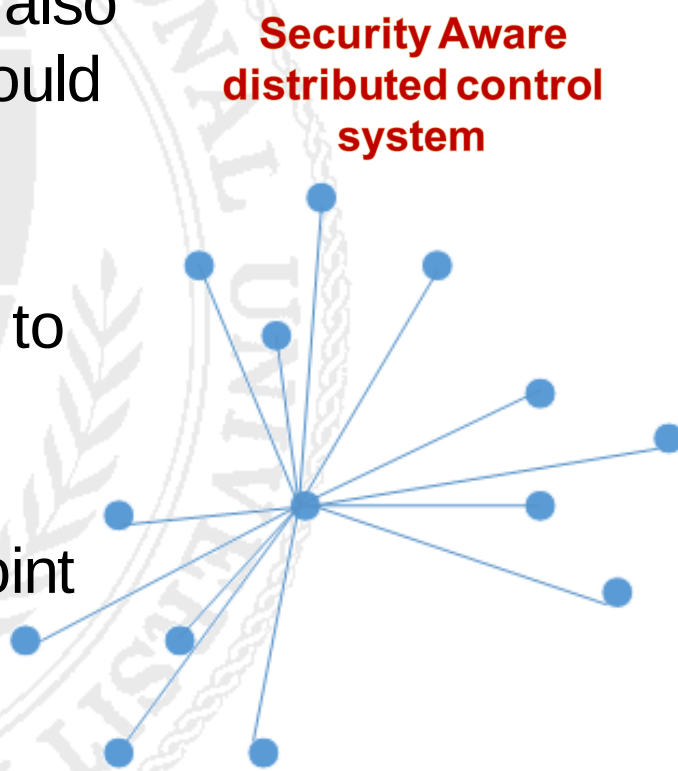


Spoofing GPS signal with wrong time in the future can cause permanent damage to some PMUs.

Wide area Monitoring security Threats

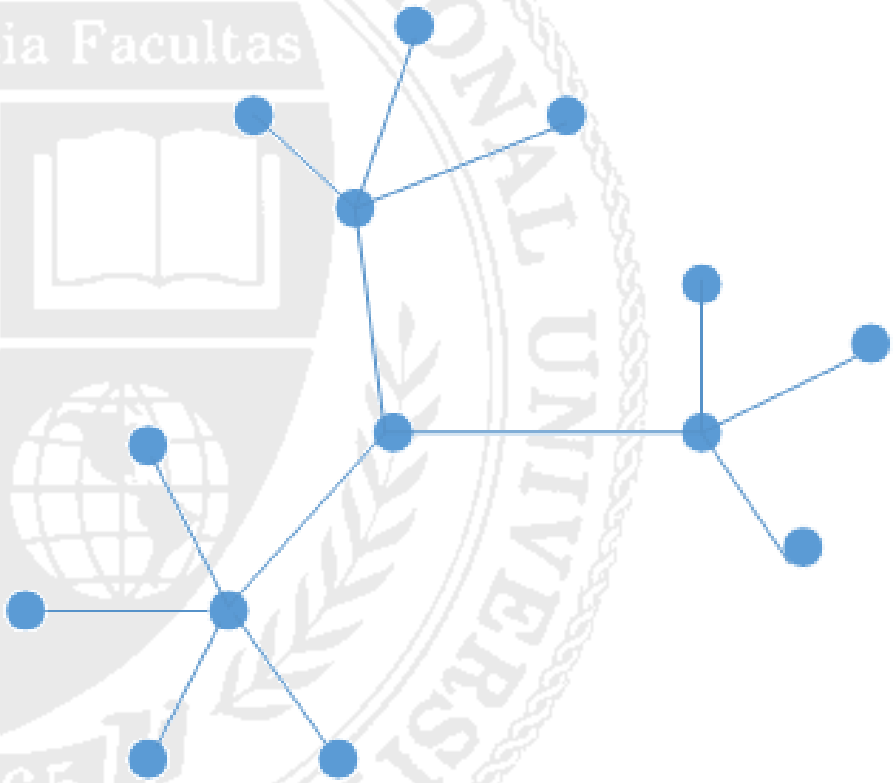
Co-design of Security Aware Power System Distribution Network as Resilient Cyber Physical System

- Cyber Physical security should not only be considered in the cyber component but also the power system network topology should be designed to be resilient in cases of attack.
- The control system should be designed to withstand cyber attack and cyber component failures.
- Centralized control suffer from single point of failure problems.
- Successful attack against centralized control system could lead to serious damage and loss of service



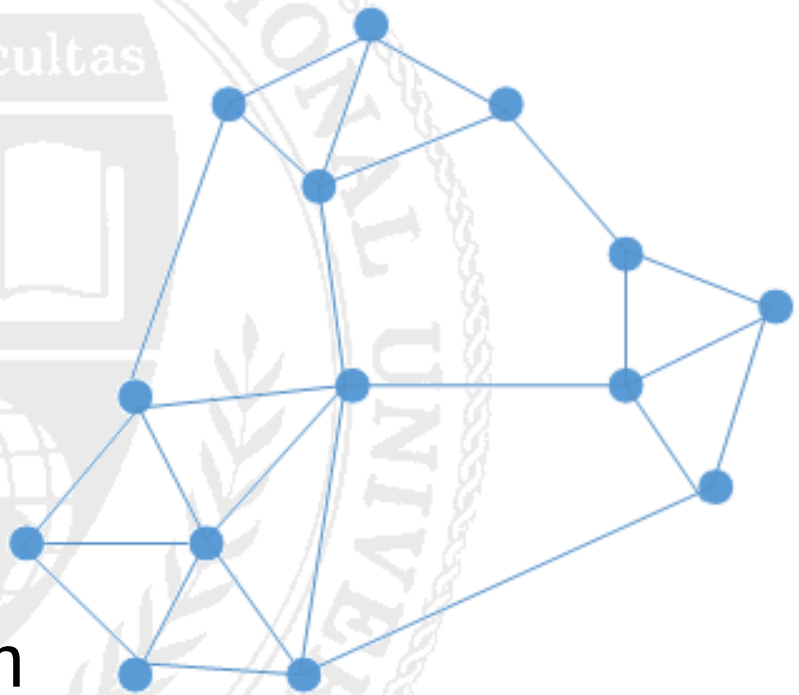
Security Aware Distributed control system

- Decentralized control reduce the risk of single point of failures and loss of service.
- Risk of attacking area and loss of service still high



Security aware distributed control system

- Distributed control minimize the risk of cyber attack.
- Each node exchange information and cooperate with neighbor node to improve the system stability.
- Attack detection can be improved by data mining from different sources



Completely distributed multi-agent control

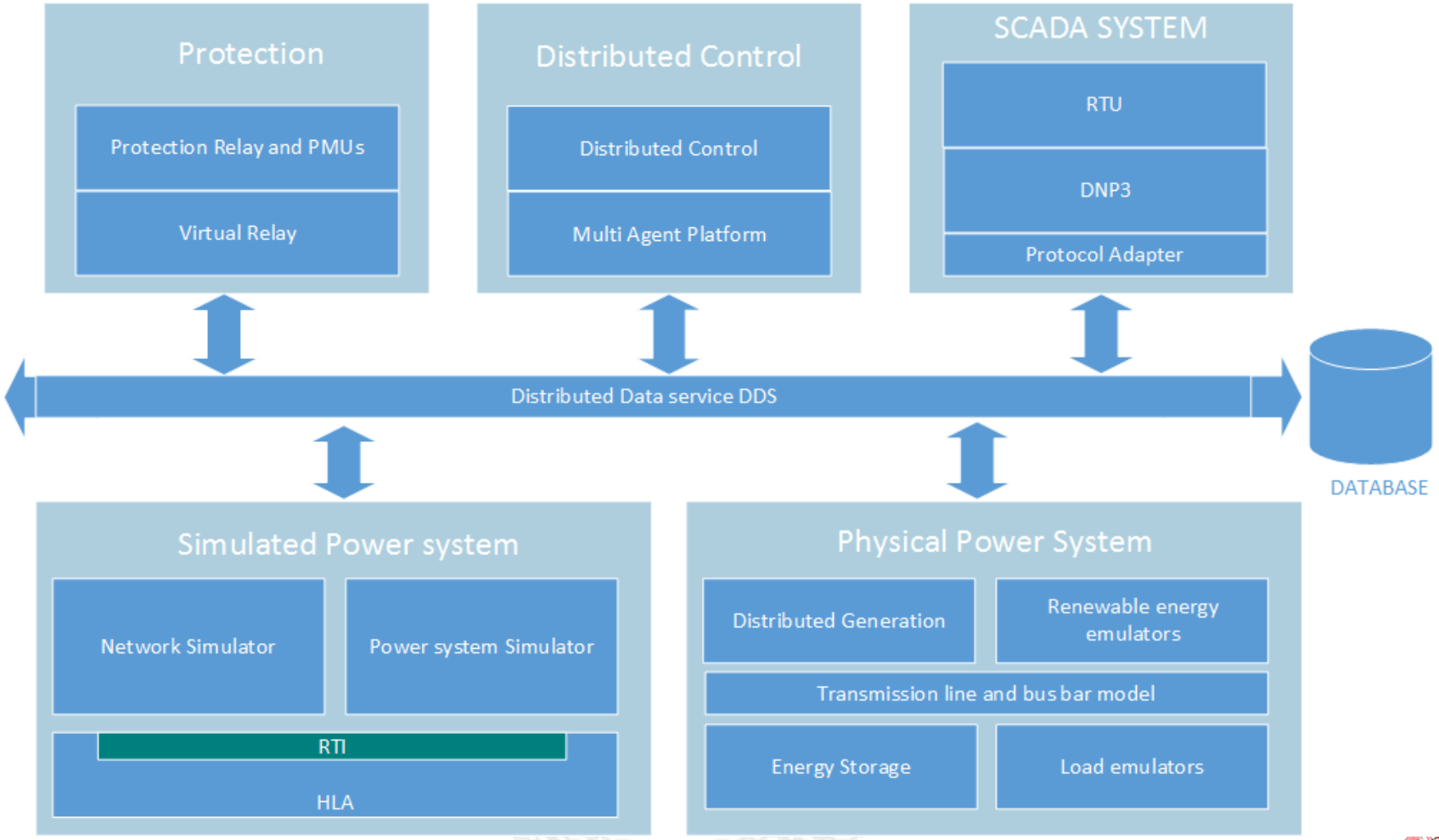
Co-design of Security Aware Power System (Summary)

- The types and levels of data protection used to encrypt or authenticate signals should be coordinated with signal sensitivity and impact on the system stability.
- The attack detection should rely on physical system characteristics beside the cyber security rules
- The cyber attack countermeasure should consider the dynamic and the special nature of power system.

Example
FIU Smart Grid Test bed Application on security aware design and validation

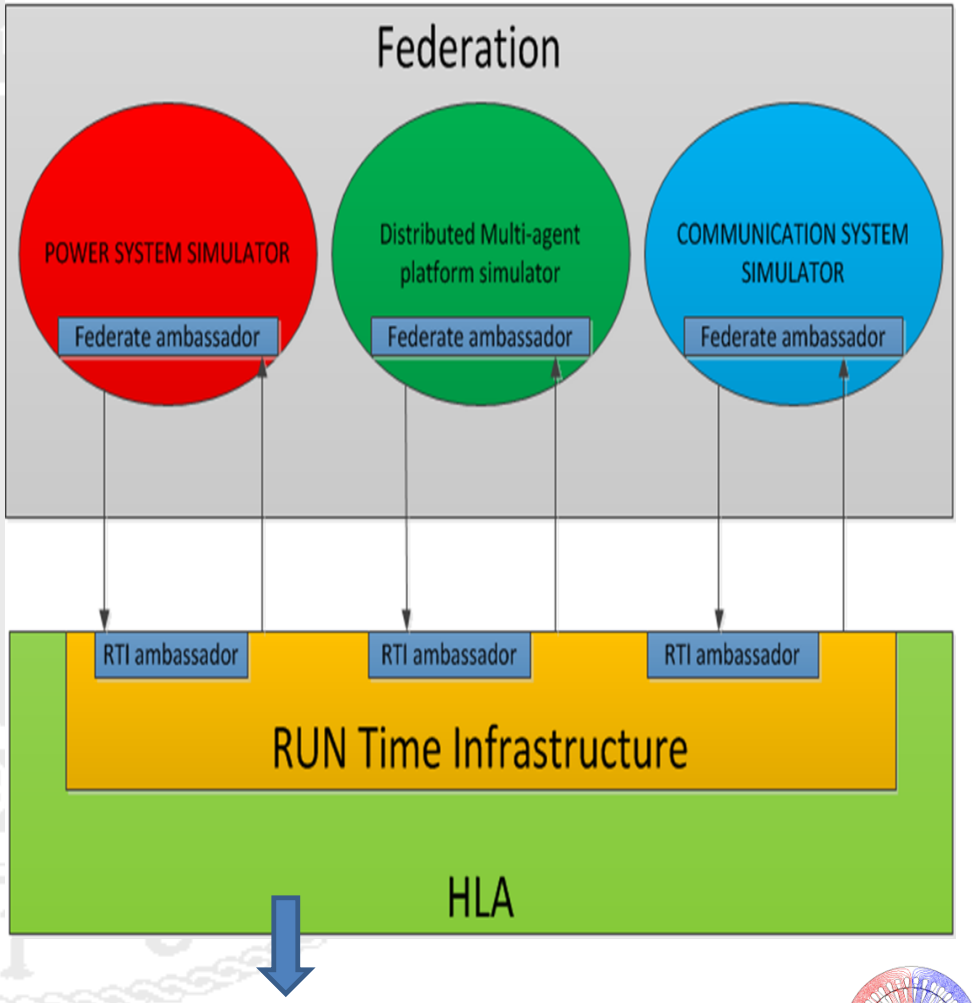
- Complex cyber physical infrastructure environment is required for identifying possible vulnerabilities and testing solutions
- The infrastructure should provide modular and flexible structure to implement different physical topologies and operational scenarios
- The test environment should seamlessly integrate with different protocols and support interoperability (standard???).

Smart Grid Test bed Infrastructure for security Aware design and validation



Modeling of overall grid as complex cyber physical system for security aware designs

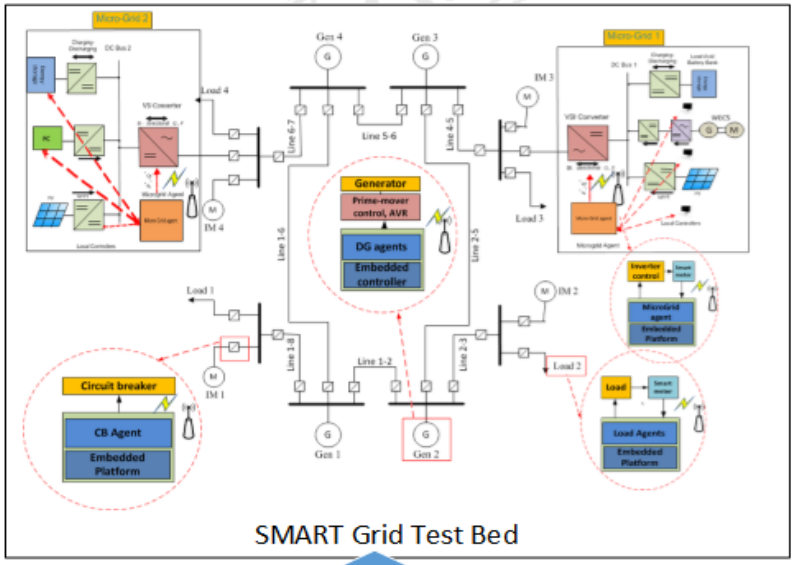
- A multi-scale and multi-resolution co-simulation technique is needed to model the integrated cyber physical system in response to various cyber and physical events.
- The co-simulation system seamlessly integrate various communication and power system components.
- The High Level Architecture (HLA) provide the standard for federated architecture that incorporate different simulation models and simulation packages

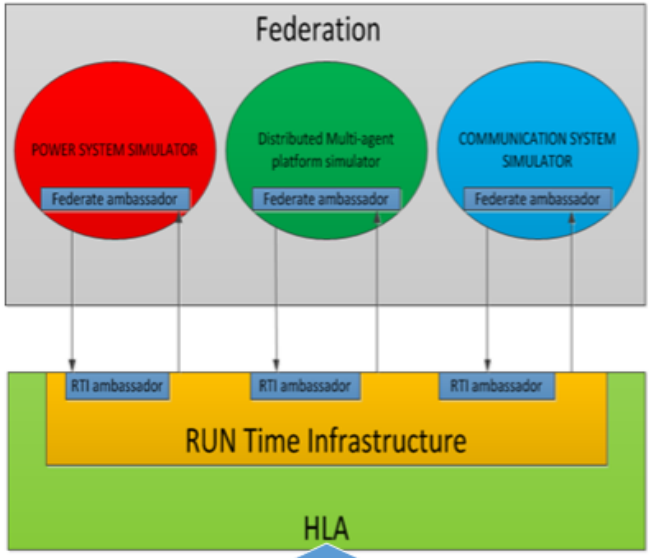


IEEE HLA Standard

To Physical System

HIL Simulation Environment





DDS Backbone

DDS: Data Distribution Service
Developed by OMG Group

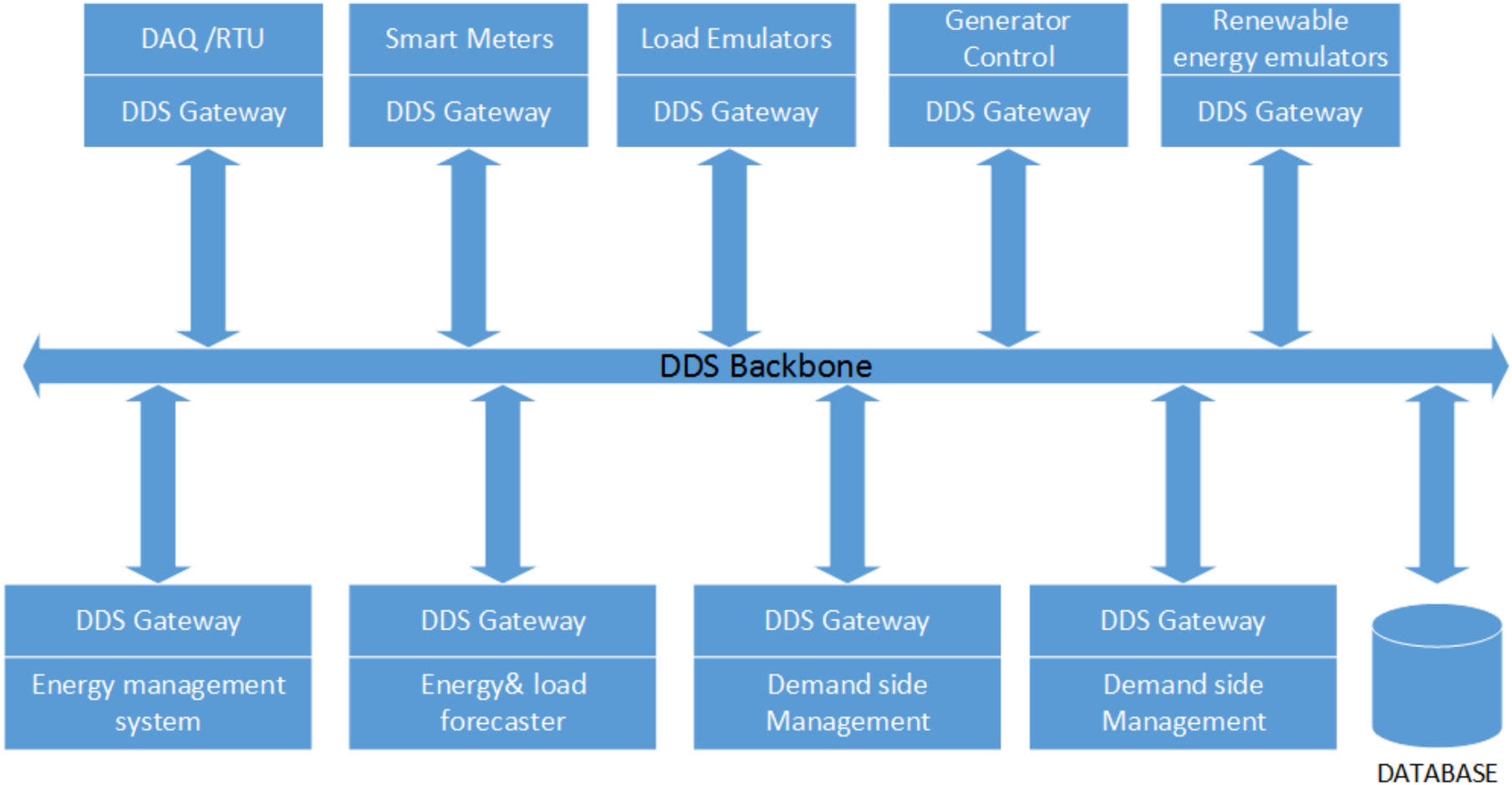
User Terminal

DATABASE

Implementation of Data Distribution Service (DDS) infrastructure on the Smart Grid Test-bed

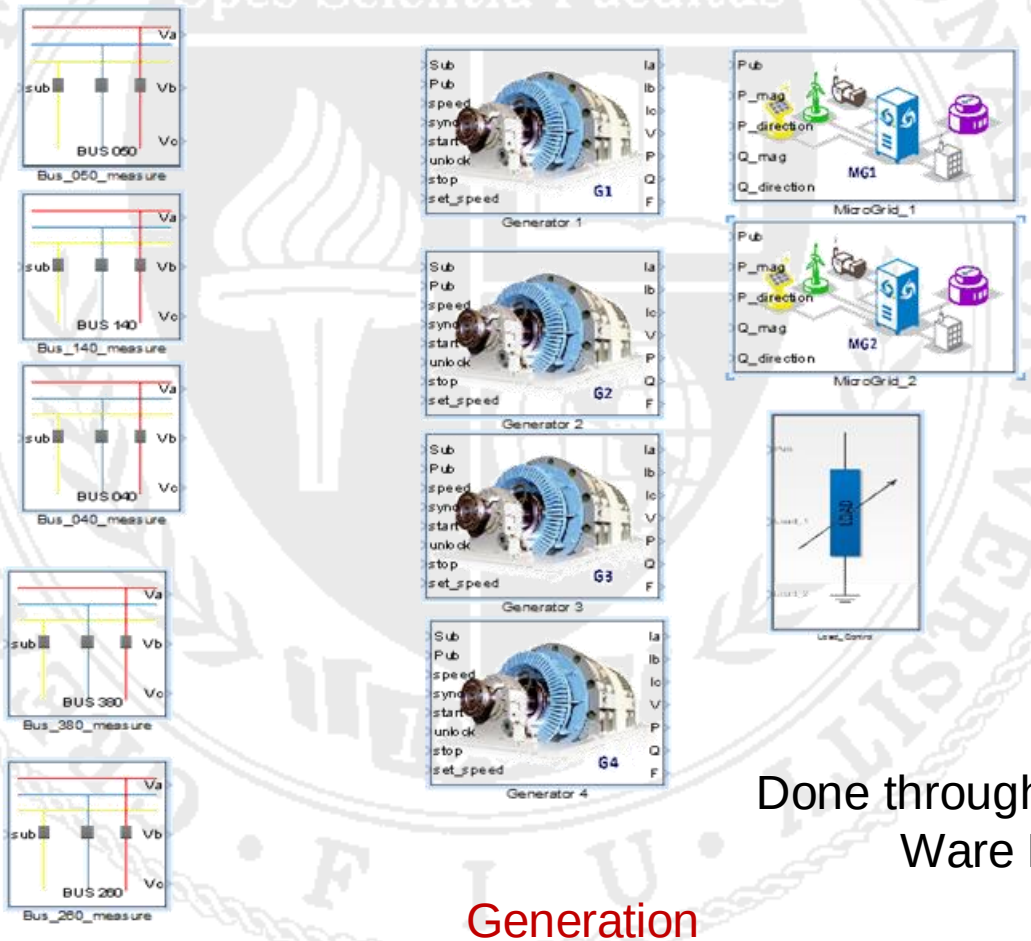
- Decentralized Data distribution standard by Object Management Group (OMG).
- Utilize real time publisher subscriber protocol (RTPS)
- No message broker or server which avoid single point of service.
- Reach set of quality of services profiles QoS
- Optimized for real time mission critical application.

Data distribution service (DDS) infrastructure for Smart Grid test bed



Smart Grid HIL interface using DDS

(Can be used by others who want to use our system to run experiments and verify control techniques)



T & D

PMU's

Wind & PV Emulator

Microgrids

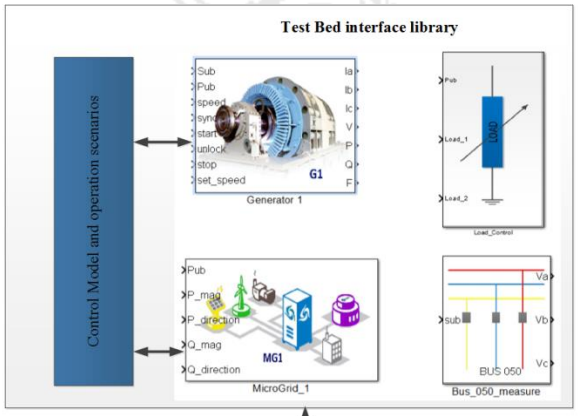
Loads

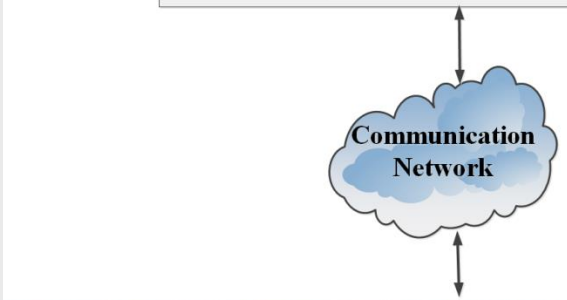
Generation

Done through DDS Middle Ware Library

Test Bed Interface Library

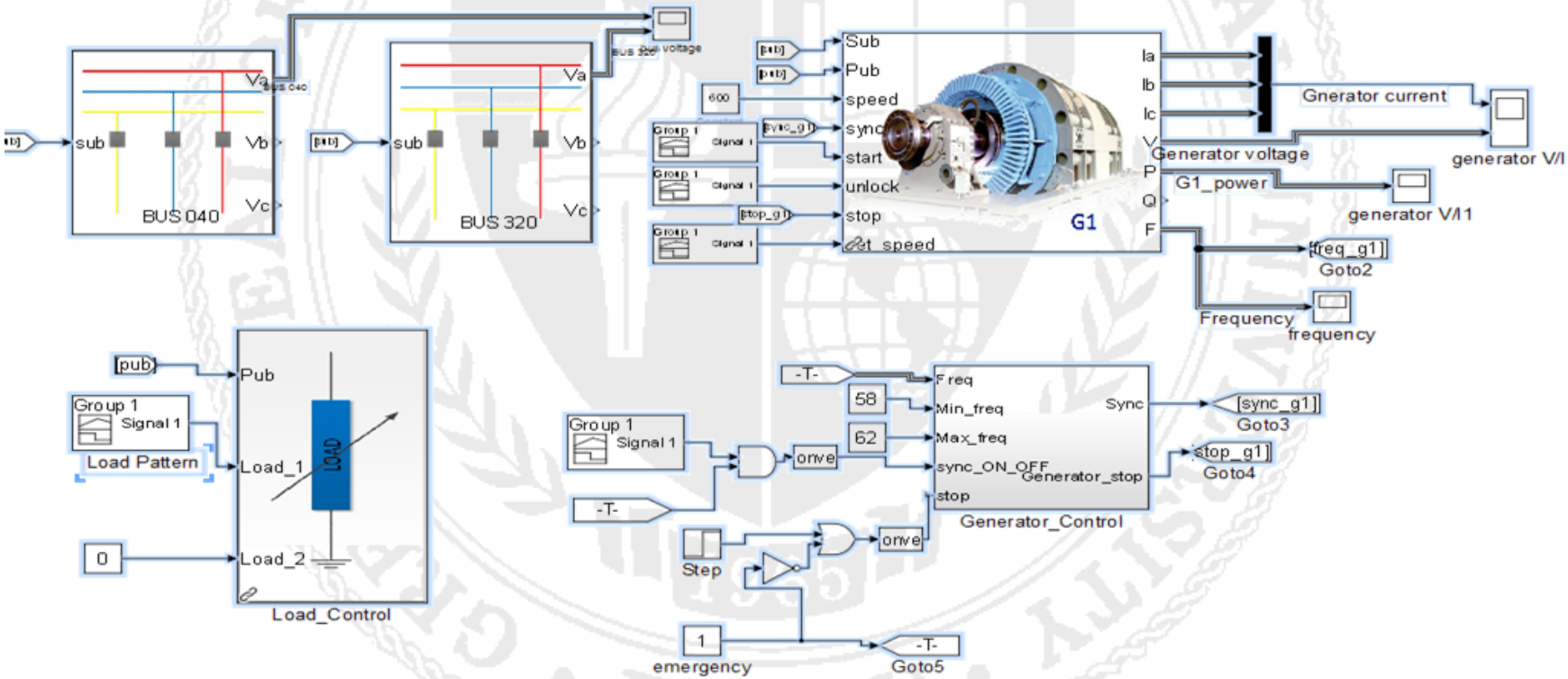
- Standard interface Library provide control function and data collection capability from local and remote network
- Real time publisher subscriber protocol (RTPS) insure interoperability
- Provide Flexible environment for Distributed control test and validation
- Currently available interface for generators, Micro Grids, CB, measurement nodes, PMU, Load emulators and renewable energy emulators



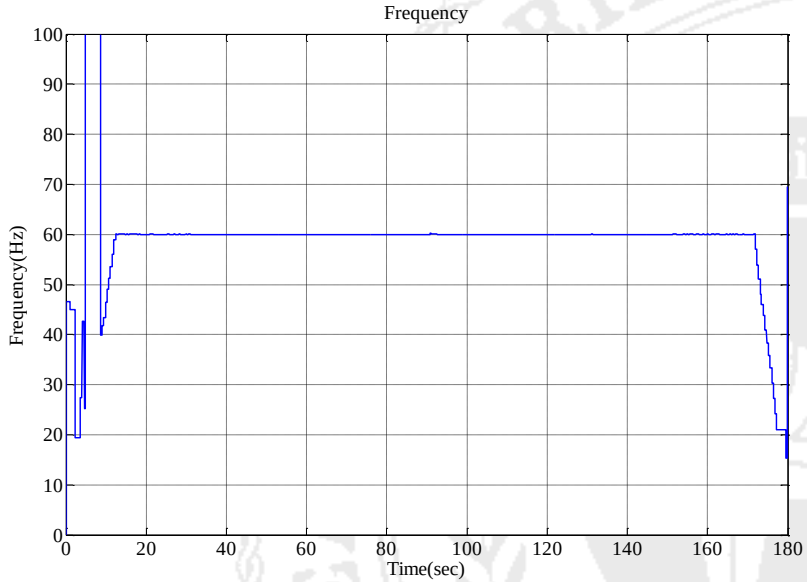


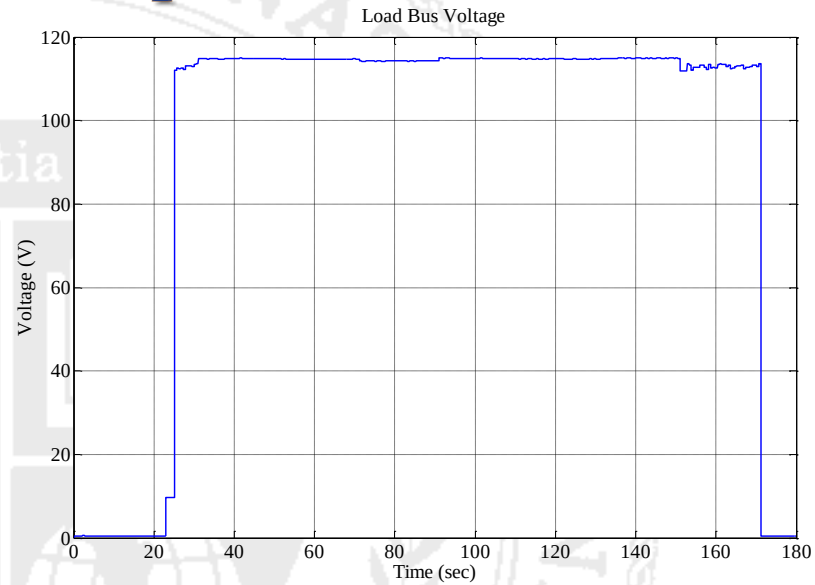
HIL Model

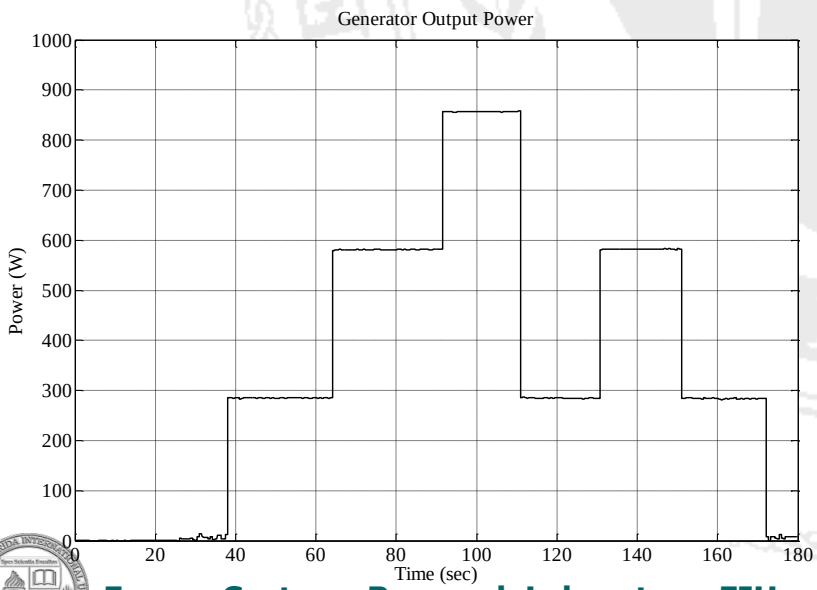
An Example for Emulating one Generator and the control of a load pattern

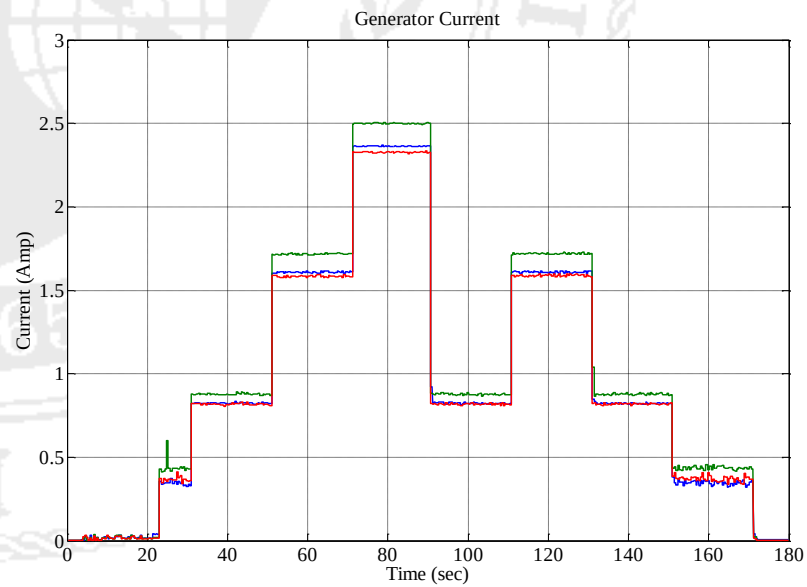


HIL Example


Frequency
Frequency(Hz)
Time(sec)
0
10
20
30
40
50
60
70
80
90
100
0
20
40
60
80
100
120
140
160
180


Load Bus Voltage
Voltage (V)
Time (sec)
0
20
40
60
80
100
120
0
20
40
60
80
100
120
140
160
180


Generator Output Power
Power (W)
Time (sec)
0
100
200
300
400
500
600
700
800
900
1000
0
20
40
60
80
100
120
140
160
180

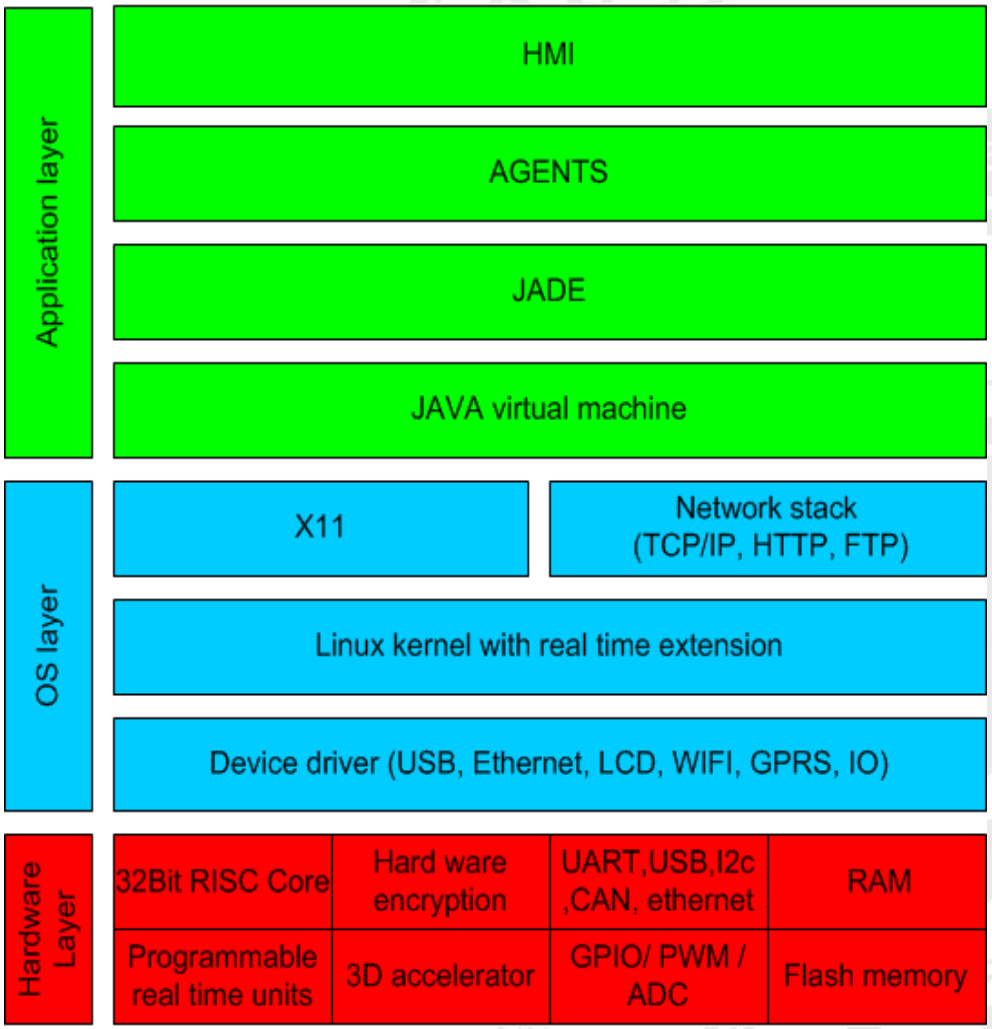

Generator Current
Current (Amp)
Time (sec)
0
0.5
1
1.5
2
2.5
3
0
20
40
60
80
100
120
140
160
180

Smart meter

- Smart meter Based on ARM processor
- Integrated power line carrier Modem (PLCM)
- Customized firmware (different protocol, encryption and authentication mechanism can be implemented)
- Support zigbee for HAN , serial, and power line communication

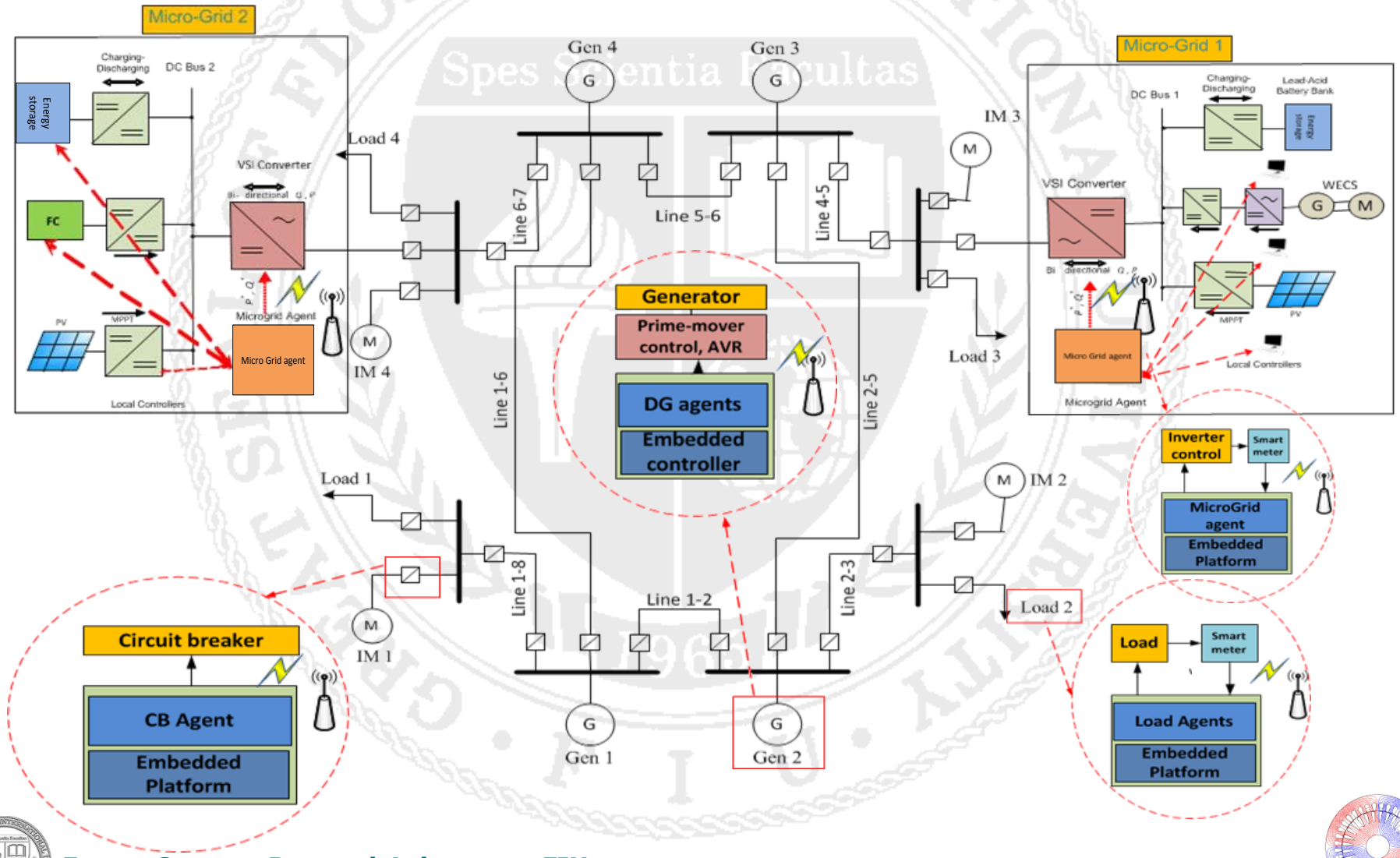
Smart Meter

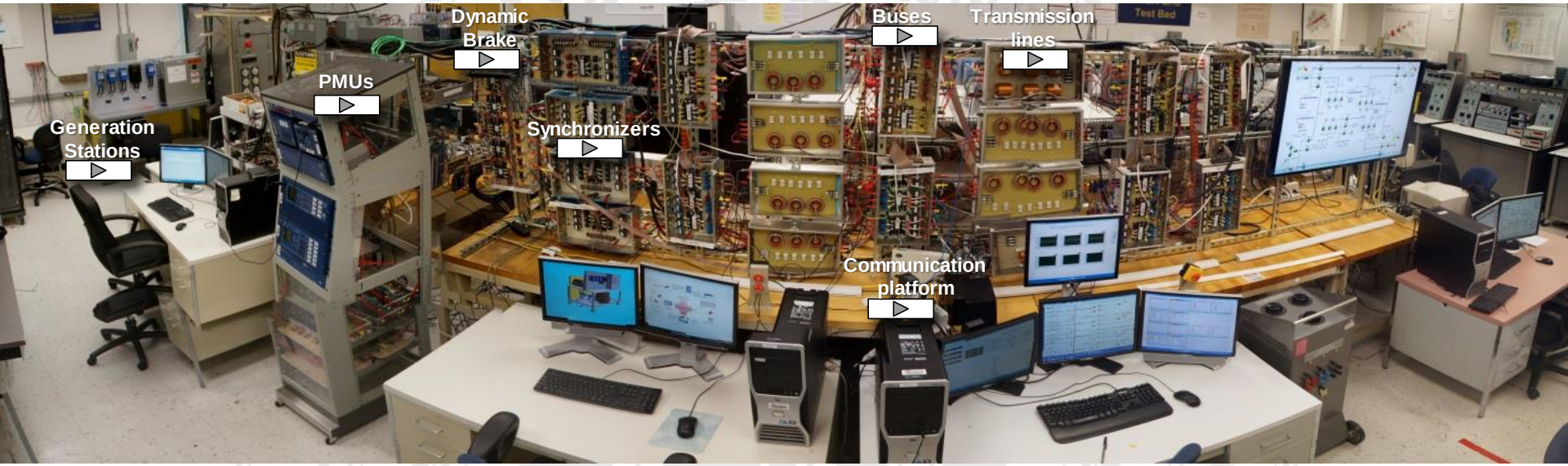
Embedded Platform for Multi Agent Control

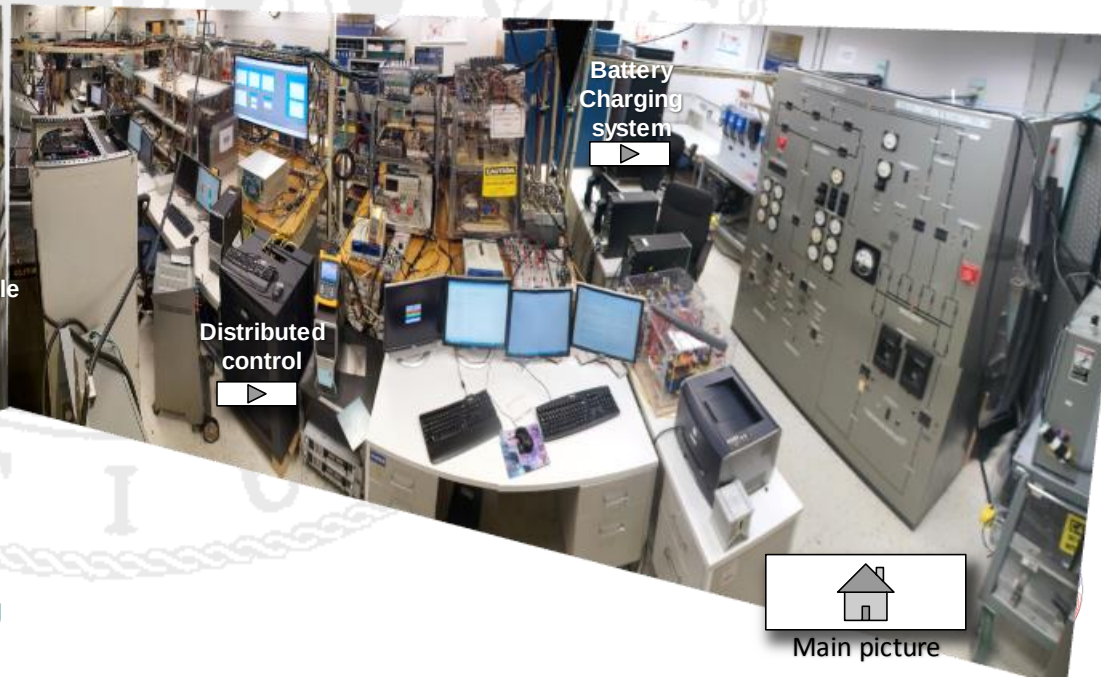


Used anywhere agent actions are required

Smart Grid Test Bed physical layer







Energy Systems Research Laboratory, FIU

Main picture