TEXAS A&M UNIVERSITY

# A Real-Time Cyber-Physical System Testbed for Studying the Impact of Cyberattacks on a Synthetic Power Distribution System


- Dr. Karen Butler-Purry
- Texas A&M University – ECE Dept.



ATC RTDS APPLICATIONS & TECHNOLOGY CONFERENCE

APPLICATIONS & TECHNOLOGY CONFERENCE 2025
CHICAGO, ILLINOIS, U.S.A.

RTDS Technologies
AMETEK

# Collaborators

Dr. Ana Goulart, Professor, Department of Engineering Technology and Industrial Distribution

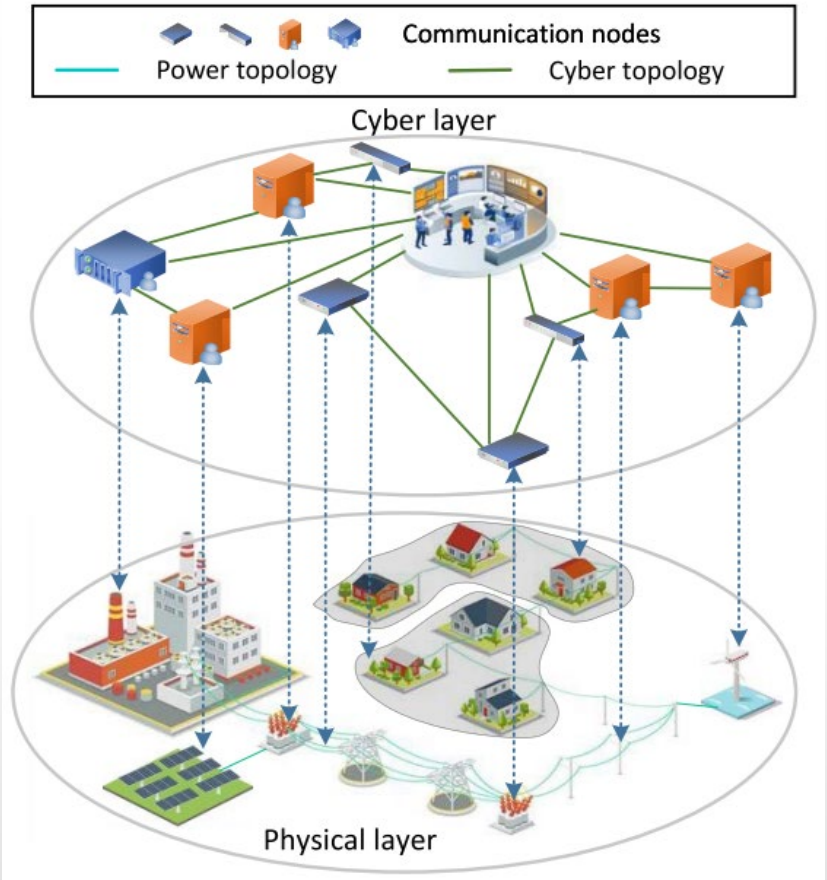
Students:

- Kumpanat Thongmai
- Vinicius Mazzilli Bobato
- Adel Heidari Akhijahani
- Edwin Tenkorang
- Vince Bartolo

# Introduction

# Smart distribution grid

- Power grid modernization has accelerated over the past decade through widespread deployment of advanced communication and automation technologies.
- Cyber-Physical Power Systems (CPPS) integrate the physical power grid with cyber layers—communication networks and computational platforms—to form a cohesive smart-grid architecture.
- In addition to reliability, resilience has become an important operational goal for power grids.
- Reliability is the ability of a power system to consistently deliver power to homes, buildings, and devices—even in the face of instability, uncontrolled events, cascading failures, or unanticipated loss of system components.
- Resilience is the ability of the grid to withstand and rapidly recover from power outages and continue operating with electricity.

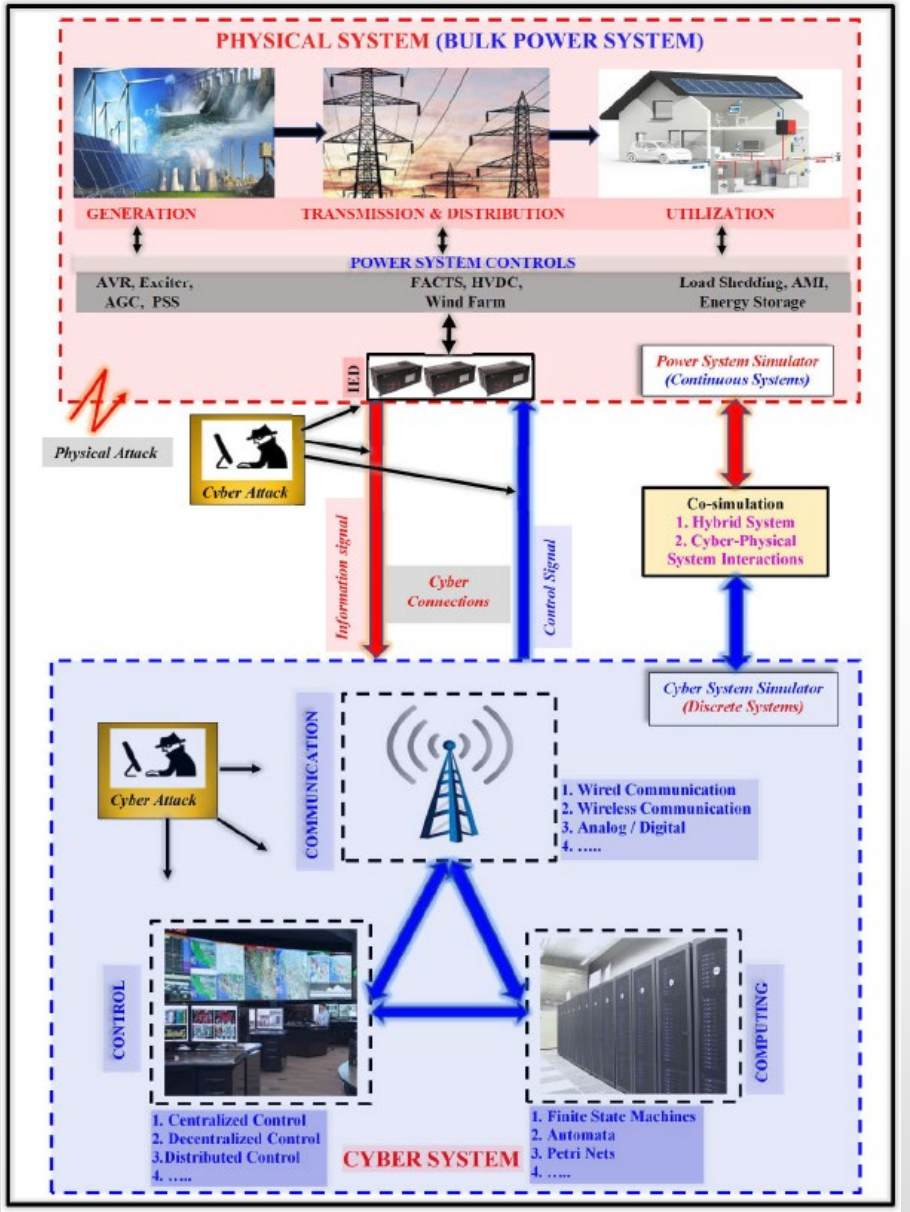



One to one CPPS mapping [1]

[1] M. Abdelmalak, V. Venkataramanan and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," in IEEE Access, vol. 10, pp. 99875-99896, 2022
[2] https://www.energy.gov/eere/energy-reliability-and-resilience

# Cyber-Physical Power Systems (CPPS)

- Two-way, cyber-secure communication enables real-time data exchange for enhanced monitoring, protection, and control of distribution components.
- CPPS deliver key smart-grid benefits: higher reliability, greater resilience to disturbances, strengthened security against faults, and improved sustainability through optimized resource usage.
- Exposed cyber layers introduce new vulnerabilities, making distribution systems susceptible to cyber and cyber-physical attacks.
- Ensuring continuous, efficient power delivery requires accurate and detailed modeling of both physical and cyber domains and their interdependencies.




Structure of the cyber-physical power system (CPPS) [1]


[1] M. Abdelmalak, V. Venkataramanan and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," in IEEE Access, vol. 10, pp. 99875-99896, 2022.

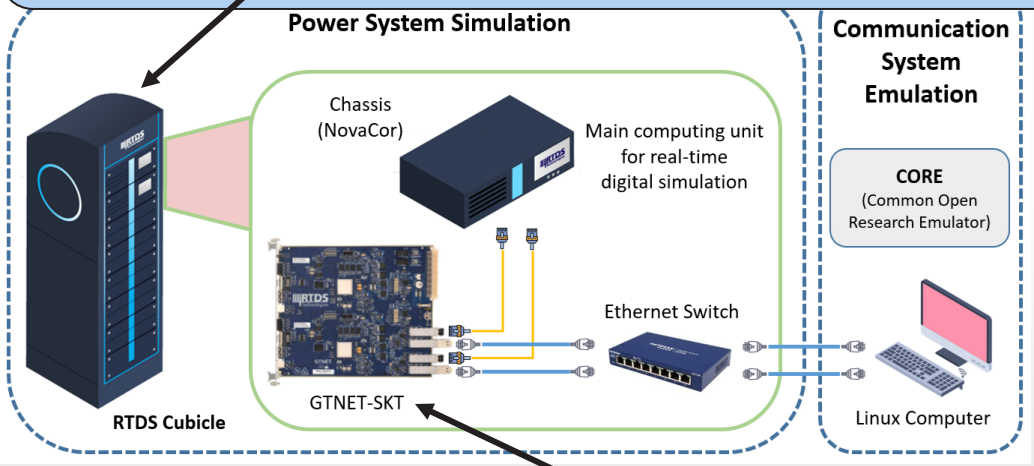
[2] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," in *IEEE Access*, vol. 8, pp. 151019-151064, 2020.

# CPPS Simulation Testbed Motivation

- Smart grids' tight coupling of information and communication technology (ICT) and power systems creates interdependencies that isolated simulators cannot capture.
- Realistic evaluation of cyber-physical security is essential for ensuring grid resilience and reliability under both cyber and physical disturbances.
- Cyber attacks (e.g., DoS) and physical faults propagate effects across both layers, necessitating a unified test environment.
- Traditional tools simulate only networks (e.g., NS2, OMNET) or power systems (e.g., RTDS, PSS/E) separately, missing cross-domain impacts.
- A CPPS testbed with real-time simulation capabilities enables hardware-in-the-loop testing and accurate modeling of bidirectional cyber-physical interactions
- It enables the study of system vulnerabilities and the operational impacts of cyberattacks on power system performance
- It also supports the development of effective detection, mitigation, and protection strategies against cyber-physical threats.

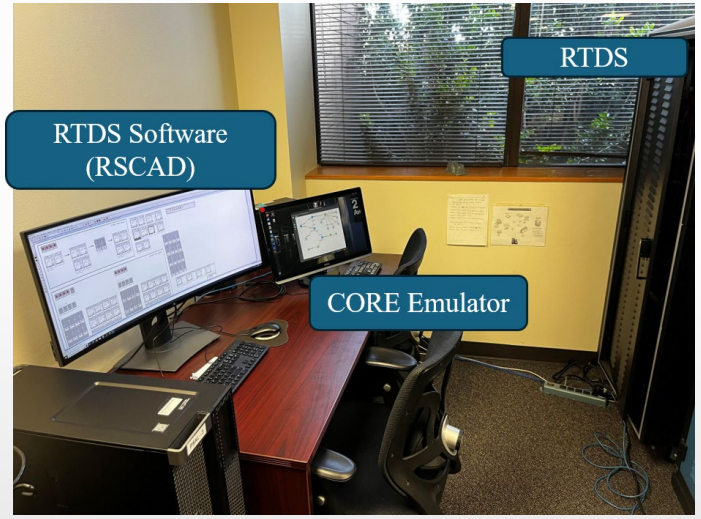
# Overview of our CPPS testbed

RTDS is a Real-Time Digital Simulator that can simulate real-time electromagnetic transient with a timestep as small as of 50 μs.




K. Thongmai, V. Bobato, K. Butler-Purry, and A. Goulart, "Cyber Security Use Case on a Smart Power Distribution System – Physical Subsystem," *2025 IEEE PES Grid Edge Technologies Conference & Expo,* Jan. 2025.

GTNETx2 network interface card can be used with various protocols. This research utilizes the socket protocol and TCP sockets.




V. Bobato, K. Thongmai, A. Goulart, and K. Butler-Purry, "Cyber Security of a Smart Power Distribution System – Cyber Subsystem Use Case," *2025 IEEE PES Grid Edge Technologies Conference & Expo,* Jan. 2025.

# Physical power grid subsystem

- The power grid forms the foundational layer upon which the CPPS is built.
- This physical layer defines the power system’s model, configuration, electrical characteristics, and network topology.
- It includes devices such as measurement units, and protection and control devices that are directly connected to grid components.
- Each component in this layer has distinct electrical properties and operational functions critical to system performance.

M. Abdelmalak, V. Venkataramanan and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," in IEEE Access, vol. 10, pp. 99875-99896, 2022

# RTDS and RSCAD

- The RTDS (Real-Time Digital Simulator) platform is used to model and analyze the behavior of power systems under various operating conditions.
- In CPPS studies, RTDS can interact with external communication and control systems through GTNET cards, which provide real-time data exchange between the physical power system model and cyber components.
- This capability allows researchers to evaluate how cyber events—such as communication delays or attacks—affect the power system's physical behavior.

# Cyber Subsystem

- The cyber layer in CPPS includes communication, computation, and control components that interface with the physical power grid.
- It facilitates wide-area measurements, system protection, and automated control to enhance grid operations.
- Secure two-way communication in the cyber layer enables real-time monitoring, protection, and control of physical power system assets.
- Despite its benefits, the cyber layer introduces vulnerabilities to cyberattacks that can impact the stability and reliability of the power system.

M. Abdelmalak, V. Venkataramanan and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," in IEEE Access, vol. 10, pp. 99875-99896, 2022

# Common Open Research Emulator (CORE)

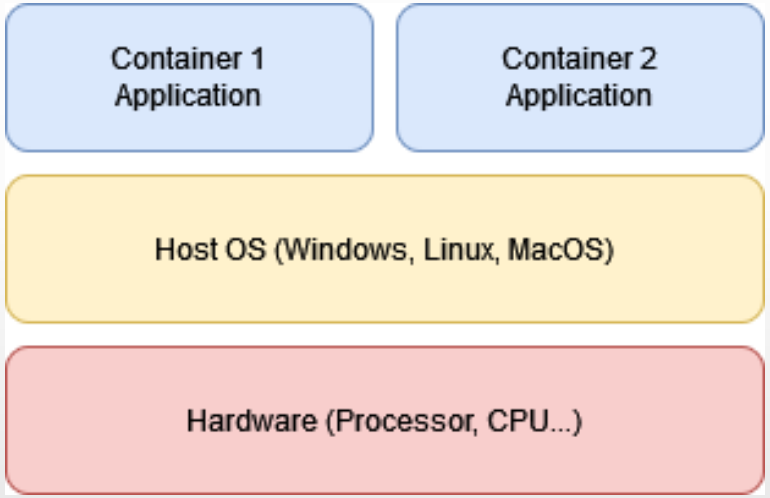
- CORE is the tool used to emulate the cyber layer. As an emulator, CORE builds a representation of a real computer network that runs in real time instead of simulation, where abstract models are used.
- CORE uses **container** technology for the nodes placed within the network, which provides independence and separation between node applications.
- Containers are able to run applications installed in the main operating system (OS).
- Routers use real routing protocols to forward packets to the right destination

J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, “CORE: A real-time network emulator,” in MILCOM 2008 - 2008 IEEE Military Communications Conference, pp. 1–7, 2008

# CORE

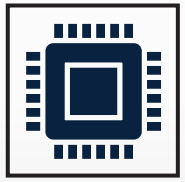
Container:

- Lightweight virtual machines using a fraction of the resources provided by the hardware to run independently from other containers.
  - “Tiny computers inside your computer”
- Each CORE node works independently from each other and assumes their own IP address.




J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, “CORE: A real-time network emulator,” in MILCOM 2008 - 2008 IEEE Military Communications Conference, pp. 1–7, 2008

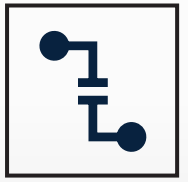
# Communication Network Modeling



GTNET-SKT module used to configure the RTDS to transfer IEEE 754 floating-point data through **TCP sockets**.

The network portion of each Use Case is modeled in Common Open Research Emulator (**CORE**) software.

CORE allows the user to model a network in a Linux environment with computer, router and switch nodes.



Each node in CORE is a **container**.

Communication from the RTDS to CORE is enabled through the use of a **TAP Interface**.

# CORE

TCP Sockets:

- Communication channel using TCP/IP model to transfer data between two applications.
- RTDS nodes are configured as TCP servers and assume IP addresses within the lab's subnet 10.125.184.0/23.
- All data is transferred using IEEE 754 float-point standard.
- CORE nodes are configured as TCP clients and have IP addresses within an arbitrary subnet.

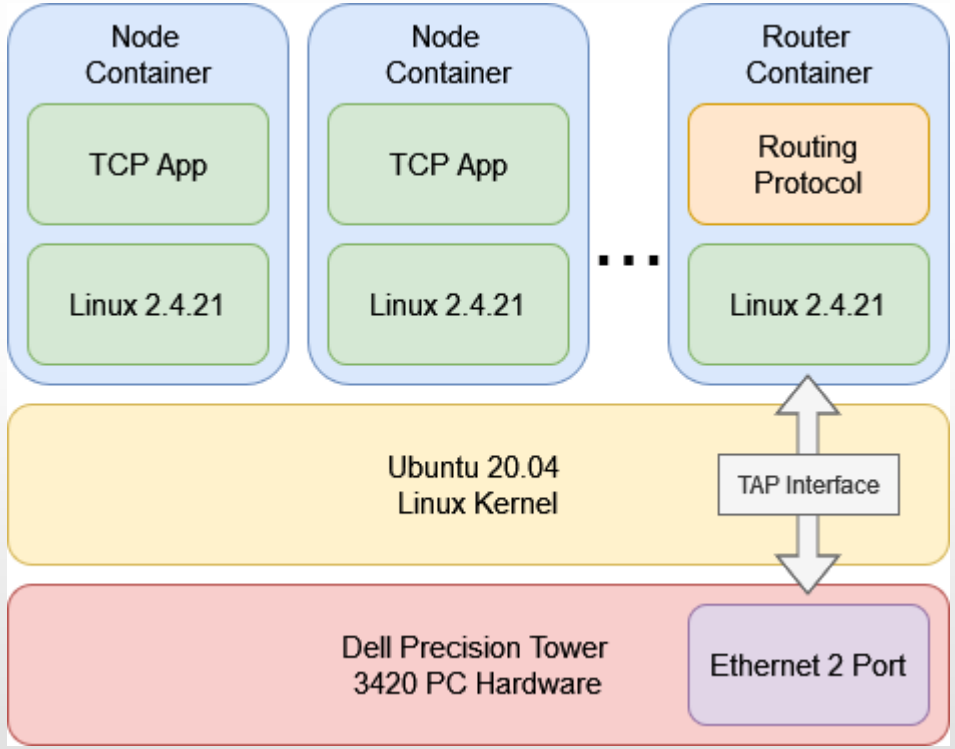
"IEEE Standard for Floating-Point Arithmetic," in IEEE Std 754-2019 (Revision of IEEE 754-2008) , vol., no., pp.1-84, 22 July 2019, doi: 10.1109/IEEESTD.2019.8766229.

# CORE

## TAP Interface

- TAP interface is represented by the RJ45 icon in CORE.
- Bridges the communication from the lab's network to CORE's network through a physical Ethernet 2 port of the Linux machine.
- If connected straight to a router, that router interface must assume an IP address in the 10.125.184.0/23 range and must be used as the RTDS default gateway.
- The routing table of the router connected to the TAP must display a rule for the lab's network.

```
root@R4:/tmp/pycore.1/R4.conf# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.125.184.0    0.0.0.0         255.255.254.0   U     0      0        0 eth0
172.24.9.0      172.24.9.53     255.255.255.240 UG    3      0        0 eth2
172.24.9.16     0.0.0.0         255.255.255.240 U     0      0        0 eth1
172.24.9.32     172.24.9.53     255.255.255.248 UG    2      0        0 eth2
172.24.9.40     172.24.9.53     255.255.255.252 UG    3      0        0 eth2
172.24.9.44     172.24.9.53     255.255.255.252 UG    2      0        0 eth2
172.24.9.48     172.24.9.53     255.255.255.252 UG    2      0        0 eth2
172.24.9.52     0.0.0.0         255.255.255.252 U     0      0        0 eth2
```



# Cyber Attack Descriptions

- A Reconnaissance attack is an initial and necessary step in the attempt to find vulnerabilities in a communication network [3]. The primary goal of the reconnaissance attack is to gather information rather than exploiting or causing harm. It identifies vulnerabilities, weaknesses, and points of entry in the targeted network or machine. The attackers may use various applications that employ different techniques such as port scanning, network enumeration, and packet sniffing.
- A Man-in-the-Middle (MITM) attack involves an adversary intercepting, modifying, or fabricating communication between two trusted entities without their knowledge [1]. In power systems, such attacks can manipulate sensor data or control commands, potentially leading to unsafe system states.
- A Denial-of-Service (DoS) attack aims to overwhelm a system's resources—such as network bandwidth, processor time, or memory—thereby delaying or entirely blocking legitimate communication [2]. In power systems, this could prevent critical data like voltage measurements or control commands from reaching their destinations in time.

[1] Conti, M., Dragoni, N., & Lesyk, V. "A Survey of Man In The Middle Attacks." IEEE Communications Surveys & Tutorials, 18(3), 2027-2051, 2016.
[2] L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, "Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid," 2018 IEEE/PES Transmission and Distribution Conference and Exposition (TD), Apr 2018.
[3] Odun-Ayo, I., et. al, "Evaluating Common Reconnaissance Tools and Techniques for Information Gathering," Journal of Computer Science, 18(2), 103-115, 2022. https://doi.org/10.3844/jcssp.2022.103.115

# Validation of CPPS Testbe

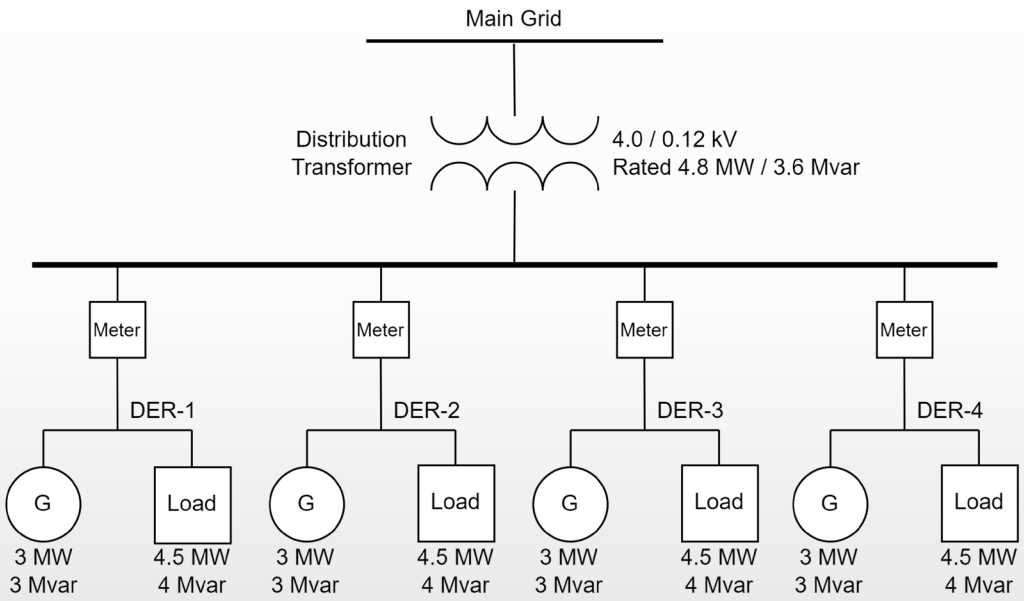
- To validate the CPPS testbed, the example case “Using GTNET and NS-3 for Cyber-Physical Simulation”, from the RTDS library was implemented to validate our CPPS testbed.
- The study aims to mitigate the overload of a distribution transformer by using the flexibility provided by DERs and load shedding.
- CORE software was used to simulate the cyber system instead of NS-3.

| NS-3 | CORE |
|---|---|
| A discrete event network simulator that allows users to model and analyze the performance of network protocols and architectures in a virtual environment. | A real-time network emulator that enables the creation and testing of network topologies using virtual nodes that behave like real system. |
| Focuses on simulating network behavior at a detailed level, including packet transmission delays, routing protocols, wireless interference, and queueing strategies, but does not run actual operating systems or applications. | Allows users to run real operating systems (e.g., Linux) and real network software on its virtual nodes, which makes it suitable for testing live protocols, deploying real-time cyber-defense mechanisms, and running real applications over virtualized networks |
| Simulation scenarios are written in C++ or Python and executed in a virtual time domain, meaning it does not operate in real time. | supports real-time operation, making it ideal for applications such as hardware-in-the-loop (HIL) testing, live demonstrations, or integration with other systems like RTDS |
| Useful when the goal is to test how protocols would behave under theoretical load, latency, and interference scenarios, making it a strong tool for protocol developers and academic simulations. | Excels when a user needs a functioning cyber layer, such as routing behavior, packet analysis, or attacker modeling, integrated with external systems like SCADA, IEDs, or other physical devices |

[1] C. Devanarayana, “Using GTNET and NS-3 for Cyber-Physical Simulation,” Oct. 2019. [Online]. Available: https://www.linkedin.com/pulse/using-rtds-ns-3-cyber-physicalsimulation-chamara-devanarayana/

# Validation of CPPS Testbed

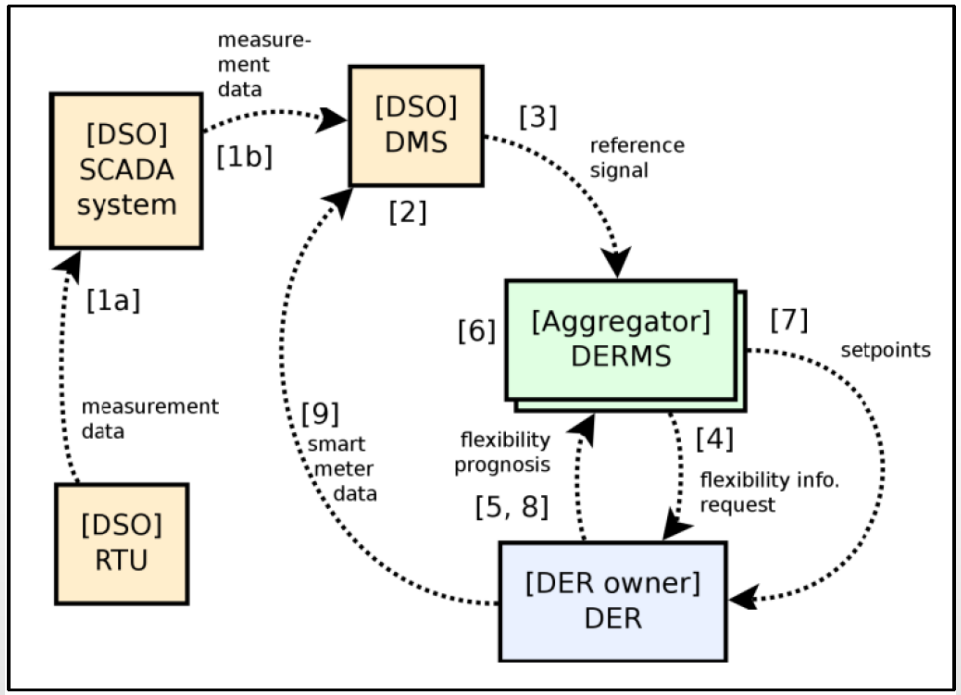
- Power System
  - Four DERs, each DER includes a dynamic source and a dynamic load.
  - Grid represented by a 4 kV source stepped down to 120 V using a distribution transformer.
  - Distribution transformer load is maintained at 6 MVA, monitored in real time using P & Q meters in RSCAD.
- Measurement data is collected by RTUs and sent to the Distribution Management System (DMS) for state estimation and overload detection.
- The DMS issues reference signals to aggregators, who query DERs for flexibility and optimize their portfolios to meet service needs efficiently.
- Aggregators send control set-points to DERs, receive updated flexibility forecasts, and smart meters report measurements back to the Distribution System Operator (DSO).




[1] C. Devanarayana, “Using GTNET and NS-3 for Cyber-Physical Simulation,” Oct. 2019. [Online]. Available: https://www.linkedin.com/pulse/using-rtds-ns-3-cyber-physicalsimulation-chamara-devanarayana/

# Validation of CPPS Testbed

- The SCADA collects real-time data from field devices and sends it to the DMS, which estimates power flows and identifies overloads.
- If a limit is exceeded, the DMS generates a reference signal and sends it to aggregators based on their capacity share.
- Aggregators then request flexibility information from their DERs, who respond with their capability to adjust output.
- The aggregator sends set-points to DERs and collects updated flexibility data. Smart meters finally report actual performance to the DSO for system monitoring.



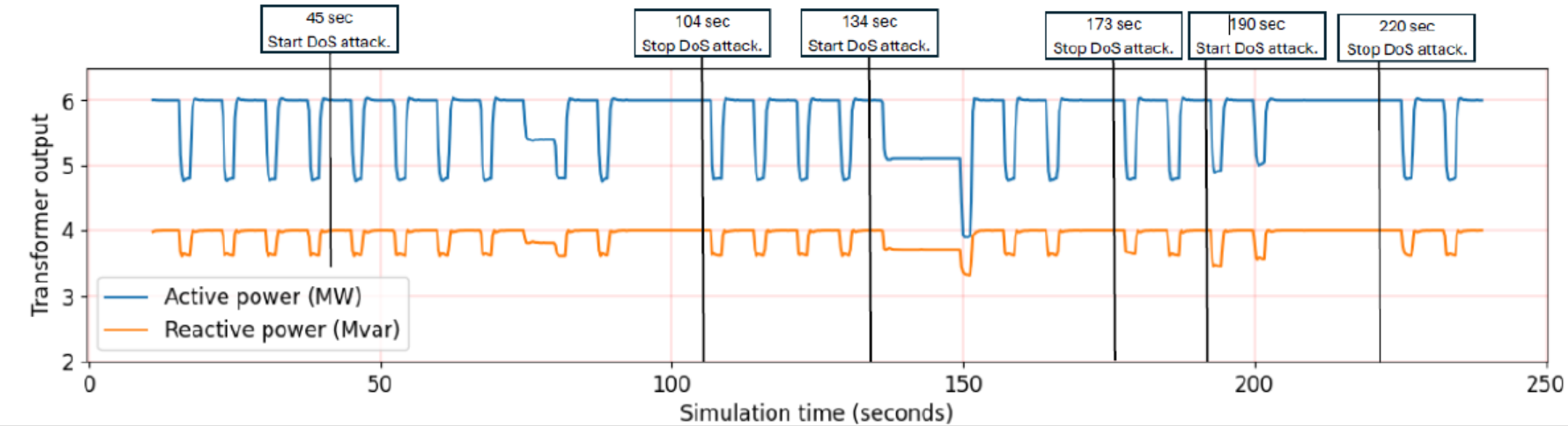

Data flow diagram [1]

[1] M. Korman, M. Ekstedt, O. Gehrke, and A. Kosek, “Deliverable 1.1 Smart grid scenario: Project: Cyber-phySicAl security for Low-VoltAGE grids (SALVAGE),” DTU - Technical University of Denmark, Apr. 2015.

# Validation of CPPS Testbed

DoS attack results:

- A DoS attack was activated at the simulation times of 45-104, 134-173, and 190-220 seconds.
- The Aggregator could not receive new data from DERs during the attacks.
- Since the Aggregator could not operate its task, the transformer output is overloaded at 6 MW and 4 MVAr for longer than normal.

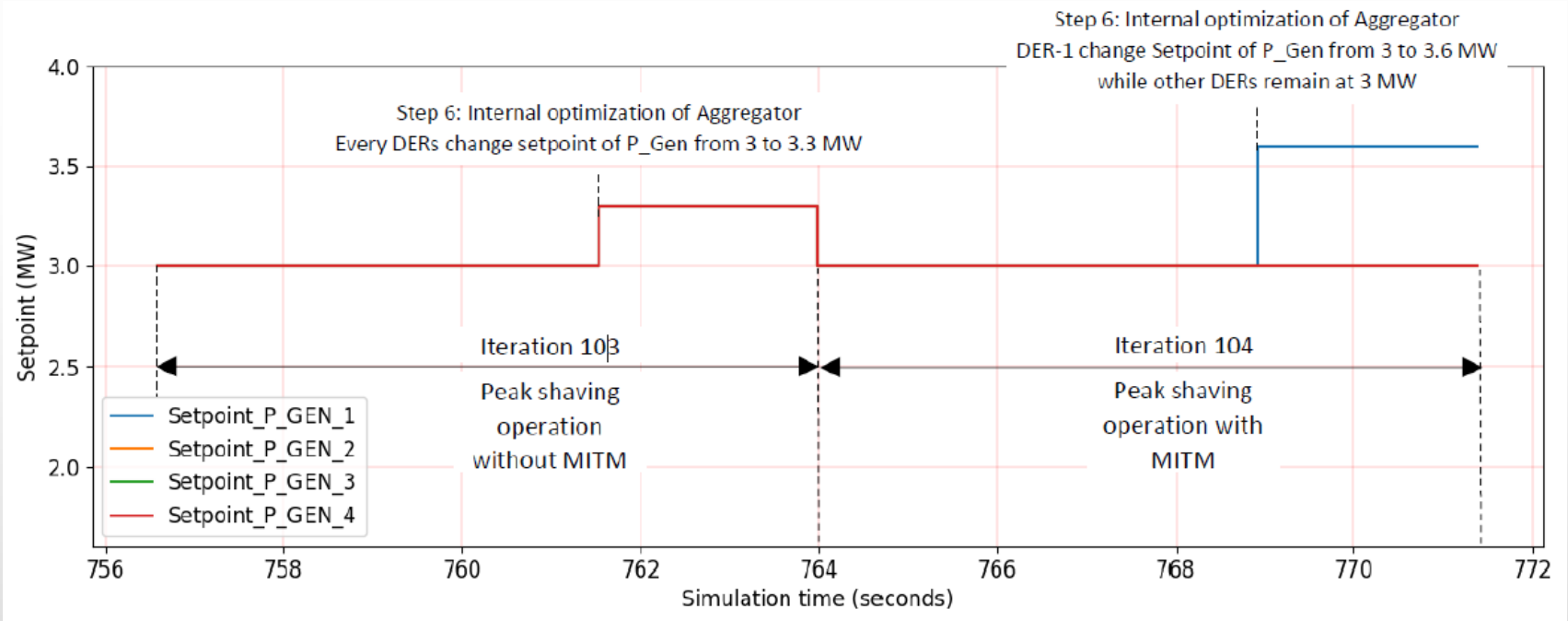


# Validation of CPPS Testbed

MITM attack results:

- Iteration 103 is a peak-shaving operation without MITM attack. The active power generation setpoint values from the Aggregator were changed from 3 to 3.3 MW for all DERs.
- On the other hand, iteration 104 was a peak-shaving operation with MITM attack. The active power generation setpoint value of only DER-1 was changed from 3 to 3.6 MW, while other DERs remained at 3 MW because the attacker changed the flexibility data of DER-2,3,4 to 0

Active power generation setpoint for 4 DERs

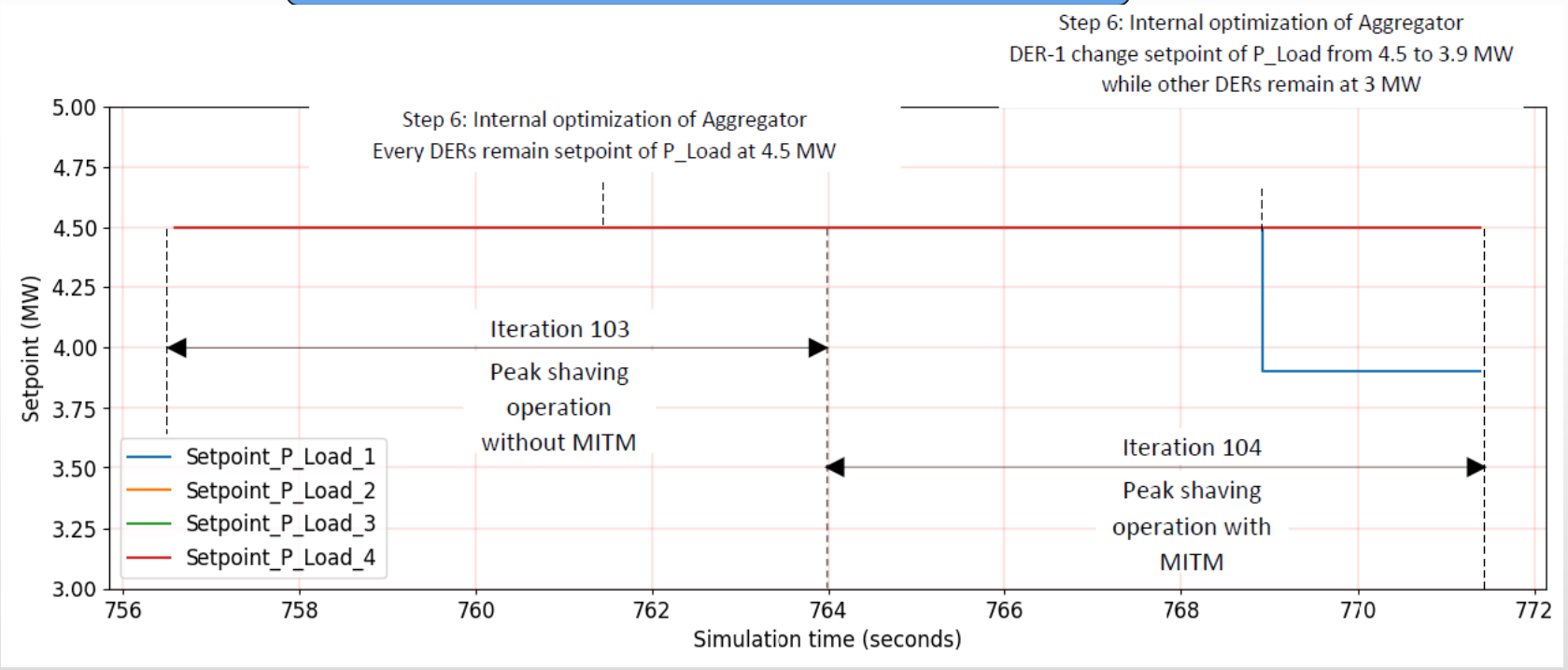


# Validation of CPPS Testbed

MITM attack results:

- Iteration 103 is a peak-shaving operation without MITM attack and the active power load setpoint values from Aggregator were set as 4.5 MW for all DERs.
- On the other hand, iteration 104 was a peak-shaving operation with MITM attack and the active power load setpoint value of only DER-1 was changed from 4.5 to 3.9 MW. The other DERs remained at 4.5 MW because the attacker changed the flexibility data of DER-2,3,4 to 0.

Active power load setpoint for 4 DERs

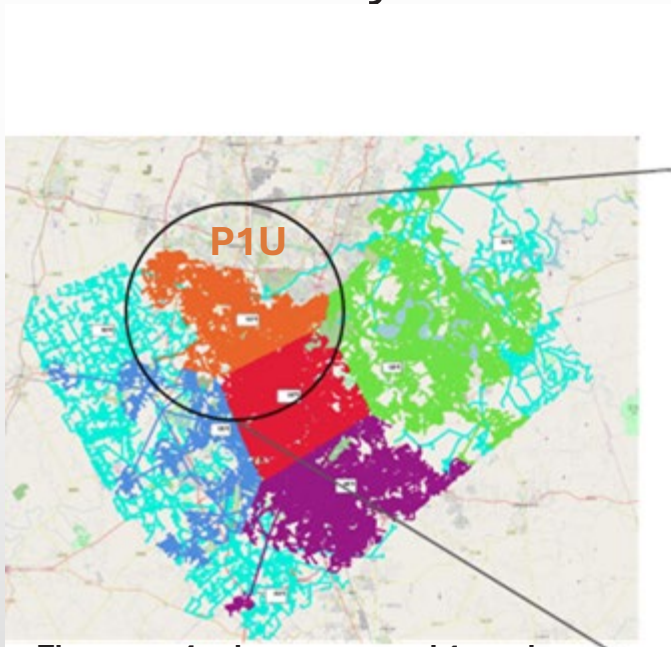


# Use Case – AMI Operation

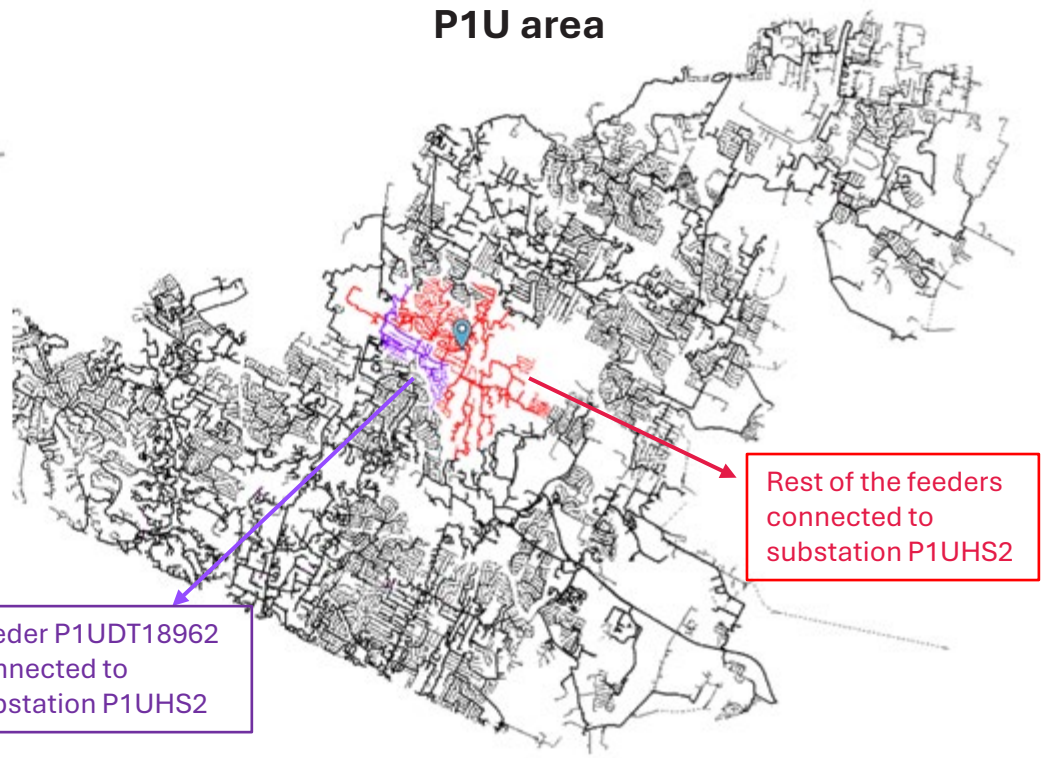
# Physical Subsystem Model

# Test Feeder and its components

- For this Use Case, we are studying a segment of the distribution feeder sourced from the SMART-DS synthetic dataset.



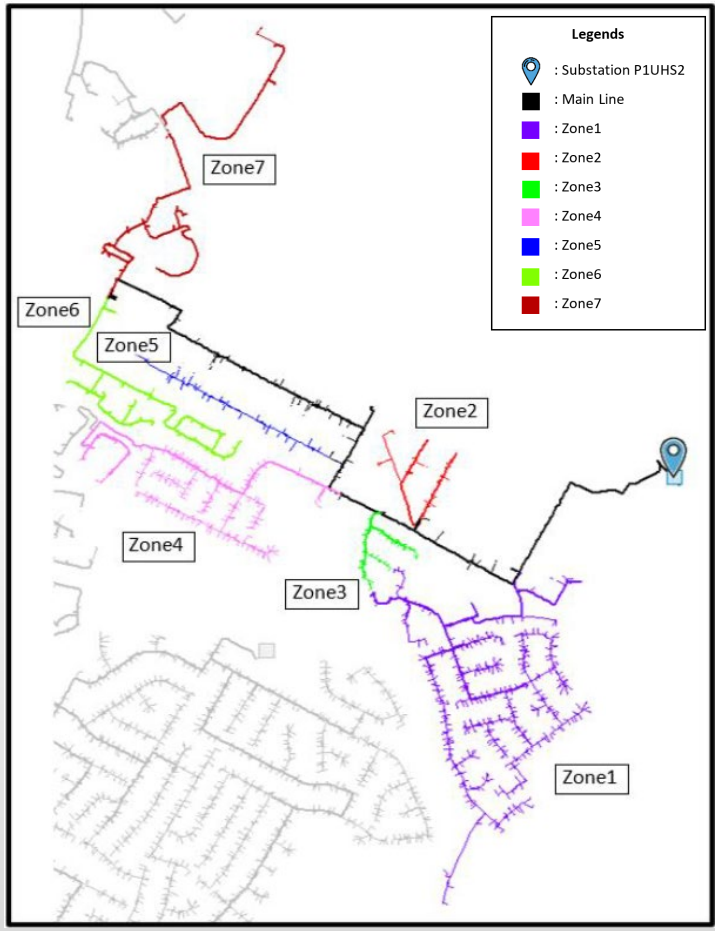

There are 4 urban areas and 1 rural area in Austin case. The P1U area (shaded in orange) is the area of interest.




*SMART-DS: Synthetic Models for Advanced, Realistic Testing: Distribution Systems and Scenarios*, National Renewable Energy Laboratory (NREL). [Online]. Available: https://www.nrel.gov/grid/smart-ds.html

# Test Feeder and its components

- Feeder P1UDT18962: This urban feeder, located in Austin, was divided into seven distinct zones—each corresponding to a lateral branch off the primary feeder.
- The feeder operates at a primary voltage of 12.47 kV and includes 0.48 kV buses. The low-voltage sections operate at 240 V (hot-to-hot) and 120 V (hot-to-neutral) using center-tap transformers.
- We are studying the extreme solar (85% of the loads have PV), high battery (35% of the loads have BESS), extreme EV (75% of loads have EV), and extreme AMI (all loads have smart meters). Loads are defined as individual buildings with associated demand profiles.



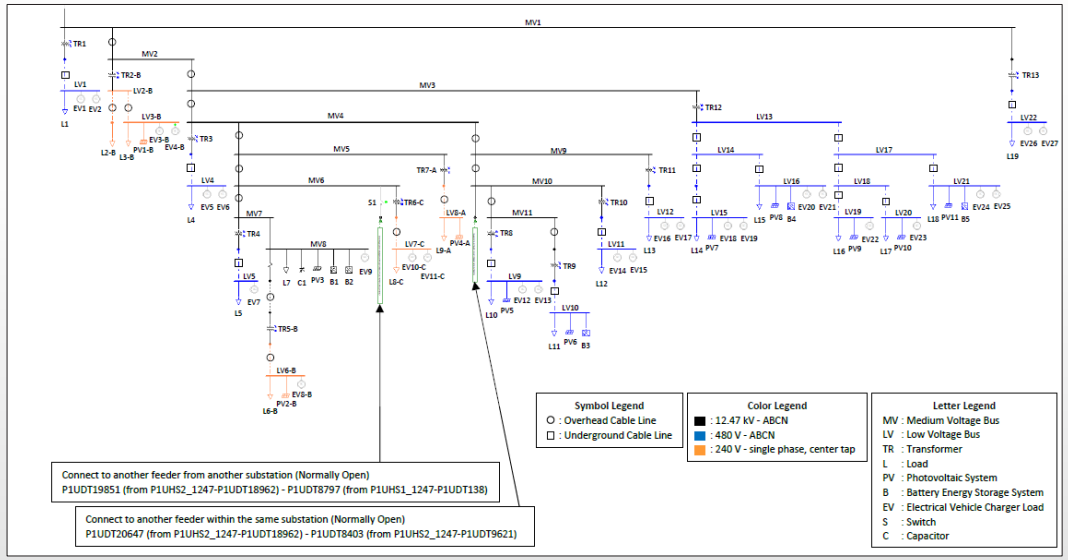
# Test feeder and its components

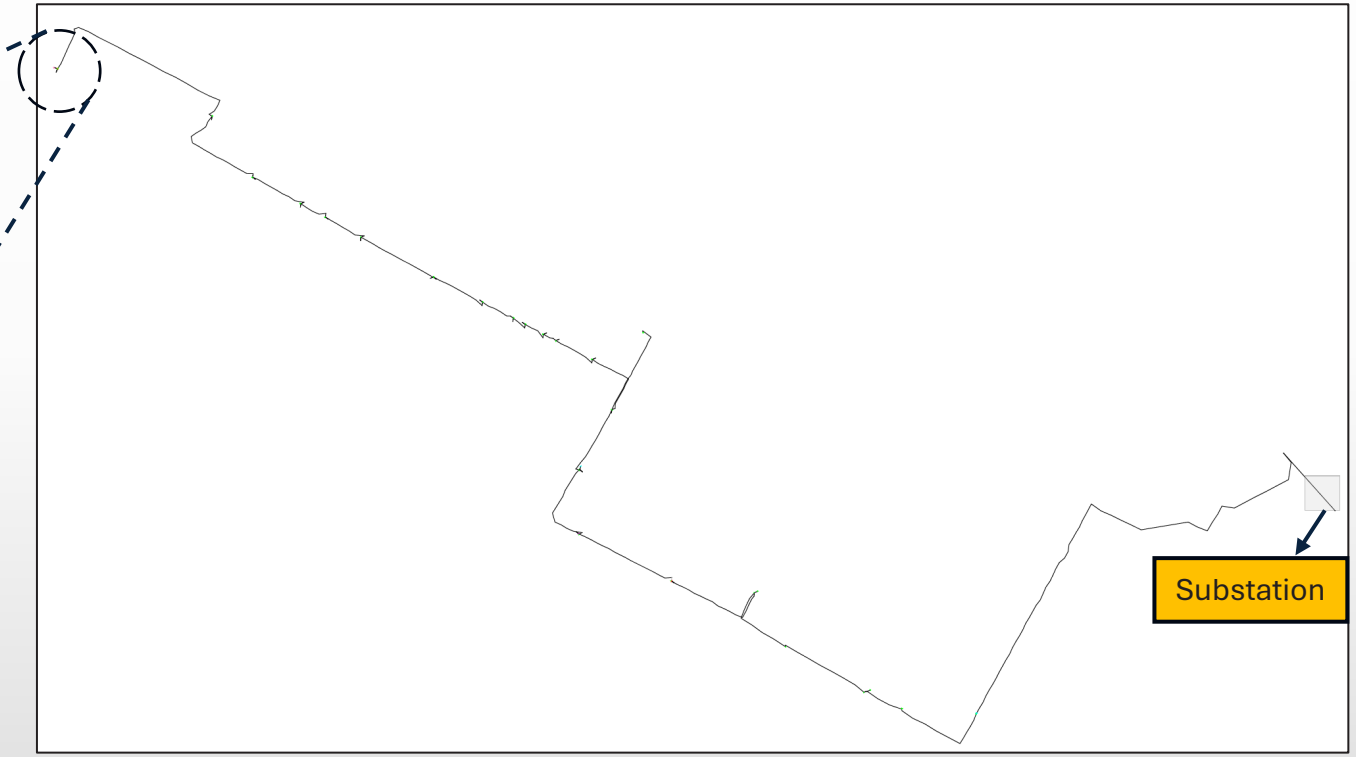
- Due to the computational limitations of our RTDS NovaCor system, which has only four processing cores, we only modelled Zone 7 of the feeder in detail.
- For the remaining six zones, the cumulative load demand and PV generation for each zone was aggregated into a single equivalent load and PV unit to reduce the model complexity.
- Similarly, the transformers along the main feeder line were not modeled individually; instead, they were represented as a lumped load and PV block.
- The goal was to maintain electrical equivalence and capture realistic interactions within Zone 7 while efficiently representing the rest of the feeder network.

| Equipment | Number of components in the feeder | Number of components in the studied zone |
|---|---|---|
| Transformer | 287 | 13 |
| Customer | 685 | 19 |
| PV (extreme PV scenario) | 582 | 11 |
| BESS (high Battery scenario) | 273 | 5 |
| EV (extreme EV scenario) | 792 | 27 |
| AMI (extreme AMI scenario) | 685 | 19 |

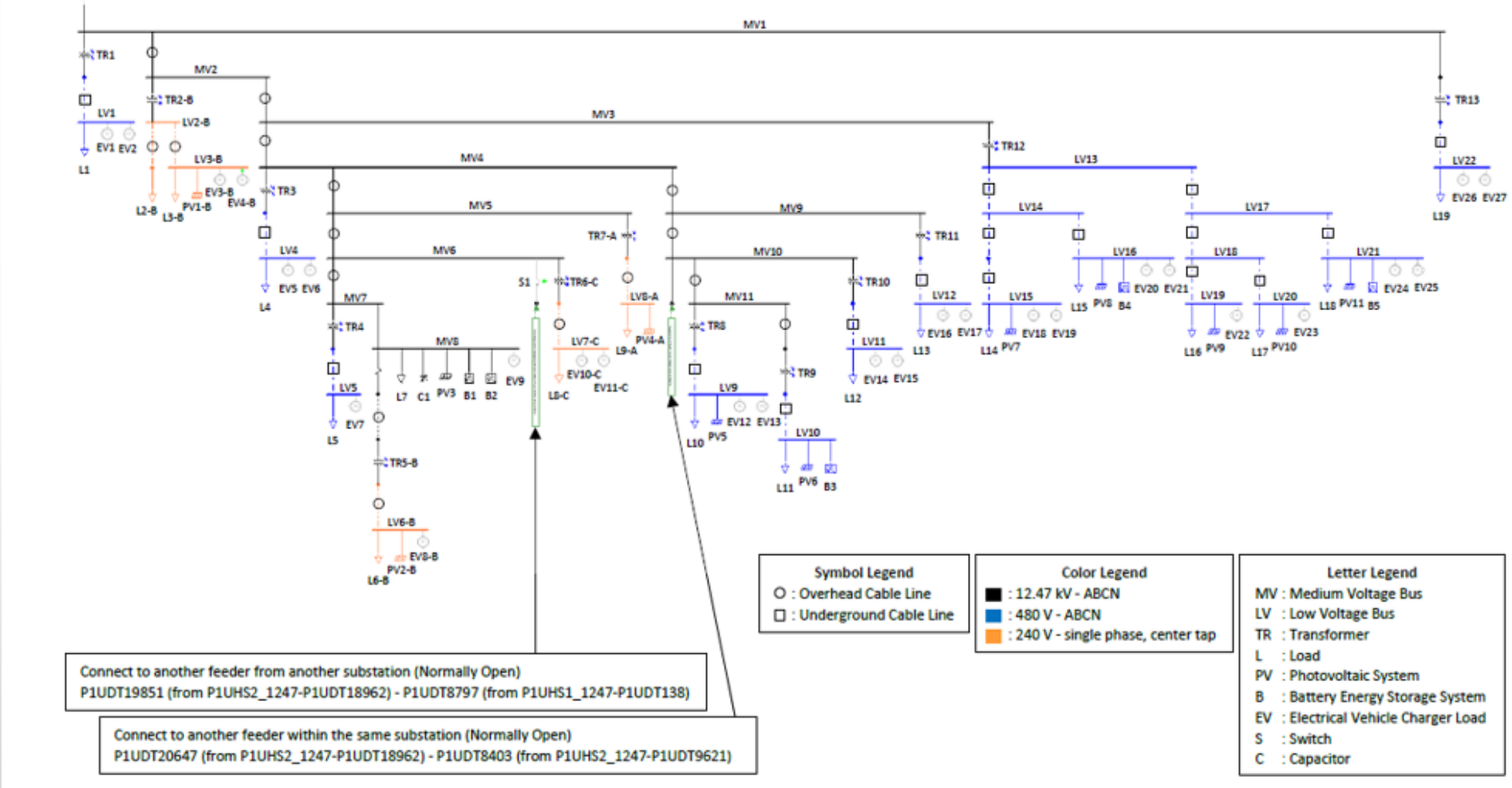
# Reduced Feeder Diagram

Zone 7



# Zone 7 Detailed Diagram

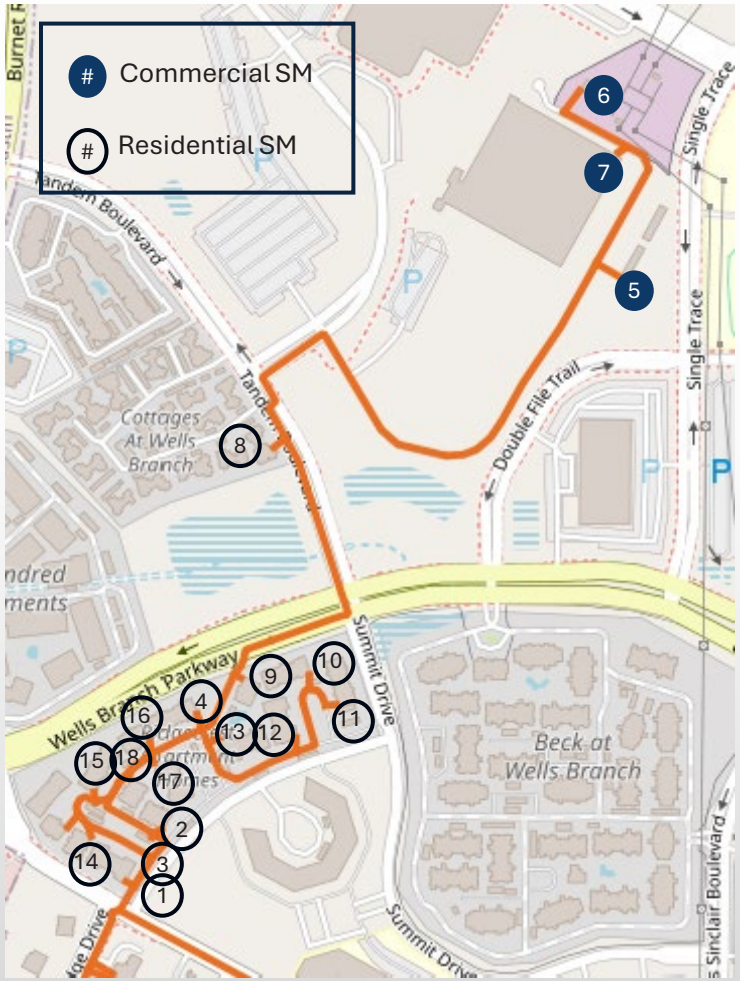


# Test Feeder and its components

- Equipment List of Feeder P1UDT18962 - Zone 7

| | | | | | | | | | | First EV | | Second EV | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Transformer No.** | **Tranformer Rated (kVA)** | **Load No.** | **Customer Type** | **Load Voltage** | **Load kW** | **PV No.** | **PV kW.** | **BESS No.** | **BESS kW.** | **EV Level** | **EV kW.** | **EV Level** | **EV kW.** |
| TR1 | 75 | L1 | Residential | 0.48 kV (3 phase) | 61.52 | | | | | Level2 | 3.3 | Level2 | 3.3 |
| TR2-B | 50 | L2-B | Residential | 0.24 kV (Phase B) | 46.8 | | | | | | | | |
| | | L3-B | Residential | 0.24 kV (Phase B) | 3.3 | PV1-B | 5.01 | | | Level1 | 1.5 | Level1 | 1.5 |
| TR3 | 75 | L4 | Residential | 0.48 kV (3 phase) | 49.56 | | | | | Level2 | 9.6 | Level2 | 9.6 |
| TR4 | 75 | L5 | Commercial | 0.48 kV (3 phase) | 27.38 | | | | | Level3 | 50 | | |
| TR5-B | 25 | L6-B | Commercial | 0.24 kV (Phase B) | 6.07 | PV2-B | 3.02 | | | Level2 | 16.8 | | |
| No Transformer Connected | | L7 | Commercial | 12.47 kV (3 phase) | 1622.58 | PV3 | 298.43 | B1 & B2 | 8 & 8 | Level3 | 300 | | |
| TR6-C | 50 | L8-C | Residential | 0.24 kV (Phase C) | 35.91 | | | | | Level2 | 3.3 | Level2 | 3.3 |
| TR7-A | 50 | L9-A | Residential | 0.24 kV (Phase A) | 36.72 | PV4-A | 7.96 | | | | | | |
| TR8 | 75 | L10 | Residential | 0.48 kV (3 phase) | 46.75 | PV5 | 7.96 | | | Level2 | 9.6 | Level2 | 9.6 |
| TR9 | 75 | L11 | Residential | 0.48 kV (3 phase) | 46.75 | PV6 | 7.96 | B3 | 8 | | | | |
| TR10 | 100 | L12 | Residential | 0.48 kV (3 phase) | 50.85 | | | | | Level2 | 16.8 | Level2 | 16.8 |
| TR11 | 75 | L13 | Residential | 0.48 kV (3 phase) | 61.52 | | | | | Level2 | 3.3 | Level2 | 3.3 |
| TR12 | 300 | L14 | Residential | 0.48 kV (3 phase) | 52.18 | PV7 | 7.96 | | | Level2 | 3.3 | Level2 | 3.3 |
| | | L15 | Residential | 0.48 kV (3 phase) | 28.87 | PV8 | 7.96 | B4 | 8 | Level2 | 3.3 | Level2 | 3.3 |
| | | L16 | Residential | 0.48 kV (3 phase) | 115.59 | PV9 | 7.96 | | | Level2 | 3.3 | | |
| | | L17 | Residential | 0.48 kV (3 phase) | 20.58 | PV10 | 7.96 | | | Level2 | 3.3 | | |
| | | L18 | Residential | 0.48 kV (3 phase) | 50.01 | PV11 | 7.96 | B5 | 8 | Level2 | 3.3 | Level2 | 3.3 |
| TR13 | 75 | L19 | Residential | 0.48 kV (3 phase) | 16.13 | | | | | Level2 | 16.8 | Level2 | 16.8 |

# Zone 7 GIS view with smart meters location

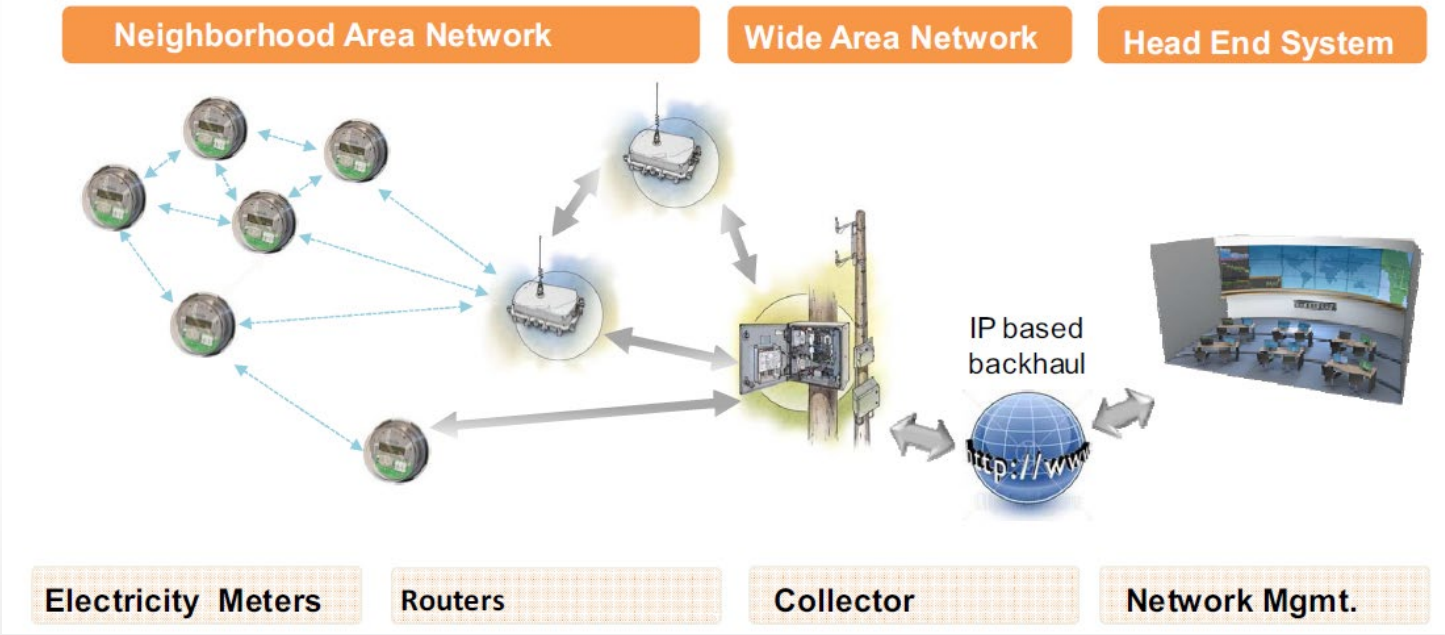


# Cyber Subsystem Model

# Communication Network Modeling

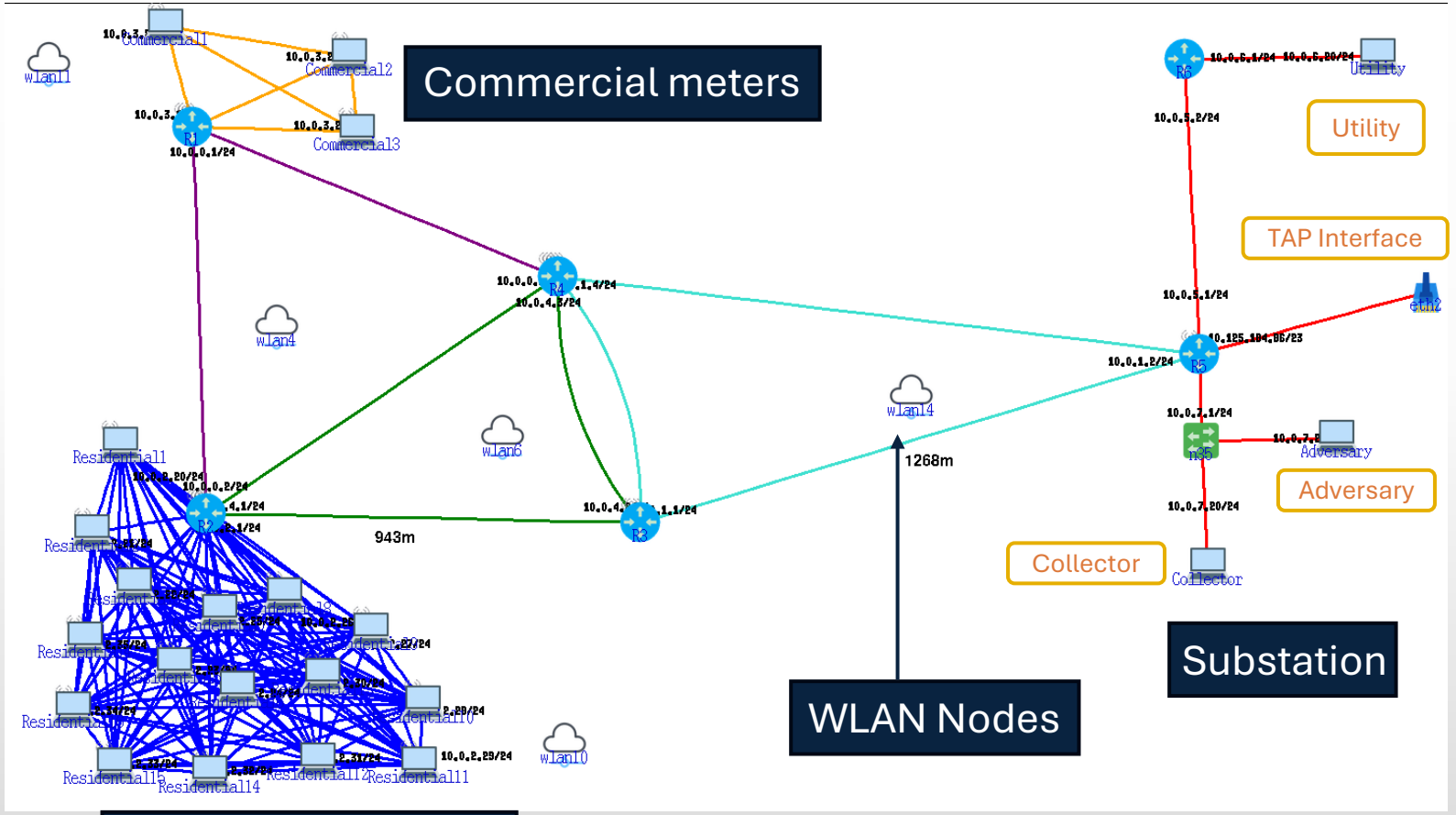
- AMI Communication Network Modeling
  - NAN - RF wireless mesh network between smart meters and data collectors.
  - An intermediate layer of network nodes or Routers interconnects with the meter mesh and routes traffic to a Collector gateway, which connects to the upper WAN layer.
  - WAN – Fiber optic connection between data collectors and the head-end system.
- RF Mesh communication uses frequency hopping equipment in the 900MHz ISM (Industrial, Scientific, and Medical) band, and involves the meters, routers, and collectors. This is the Neighborhood Area Network (NAN).
- Real distances between smart meters, a collector, and the substation were implemented in the communication network in CORE. Also, their bandwidth was adjusted (9.6kbps or 19.2kbps) to create a realistic and dynamic testbed containing real and accurate delays and signal loss.

B. Lichtensteiger, B. Bjelajac, C. Müller, and C. Wietfeld, "RF Mesh Systems for Smart Metering: System Architecture and Performance," *2010 First IEEE International Conference on Smart Grid Communications,* Nov. 2010.



# Communication Network Modeling

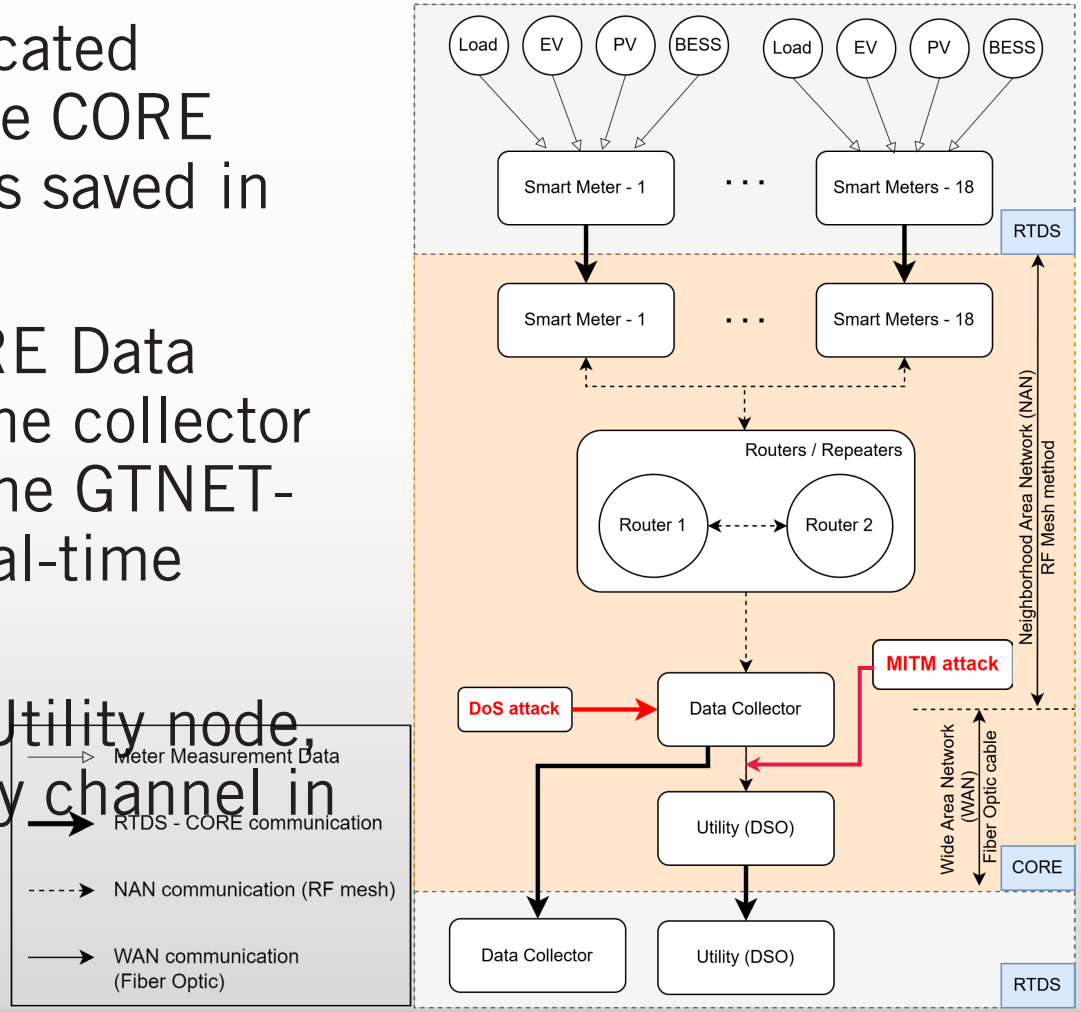
- All nodes within 10.0.0.0/20.
- TAP interface connects to R5.
- Each node connects to their counterpart node through the GTNET TCP servers.
- Communication within CORE through TCP client/server applications.
- The distances were determined based on the feeder GIS information



# CPPS Model – AMI Operation Use Case

# Overall Diagram of the AMI Use Case

- Smart meters transmit their data over dedicated channels in GTNET cards to their respective CORE nodes. A copy of each smart meter's data is saved in RSCAD for real-time recording
- Each CORE node sends its data to the CORE Data Collector node via the RF mesh network. The collector node sends the received collector data to the GTNET-SKT collector channel in the RSCAD for real-time recording.
- The collector sends the data to the CORE Utility node, and a copy is sent to the GTNET-SKT utility channel in RSCAD for real-time recording.



# GTNET Cards Configuration for the Use Case

- Two GTNET-SKT cards were used to facilitate data transfer between the physical and cyber layers of the testbed.
- The Data Collector and Utility channels were configured for receiving, while the remaining channels were configured for sending and receiving data.

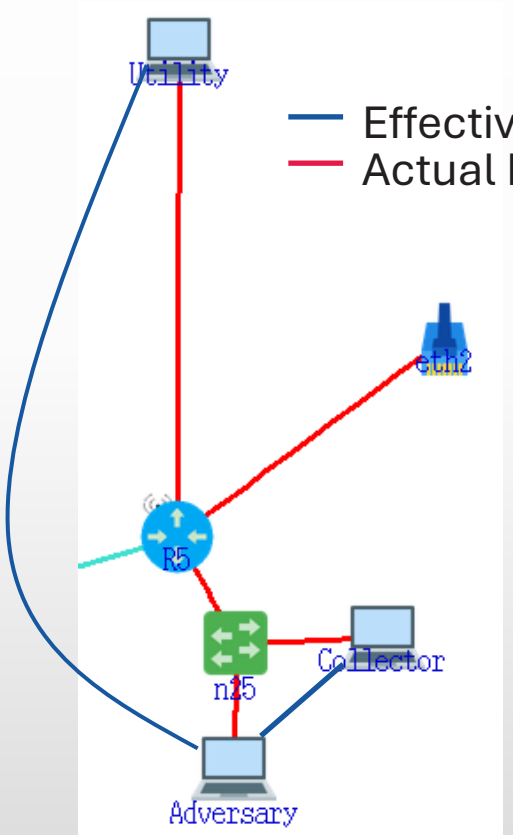
| | | | |
|---|---|---|---|
| GTNETx2 Port 7 | 1 | Data Collector | 10.125.184.71 |
| | 2 | UTILITY | 10.125.184.72 |
| | 3 | Smart Meter 1 | 10.125.184.73 |
| | 4 | Smart Meter 2 | 10.125.184.74 |
| | 5 | Smart Meter 3 | 10.125.184.75 |
| | 6 | Smart Meter 4 | 10.125.184.76 |
| | 7 | Smart Meter 5 (Commercial 1) | 10.125.184.77 |
| | 8 | Smart Meter 6 (Commercial 2) | 10.125.184.78 |
| | 9 | Smart Meter 7 (Commercial 3) | 10.125.184.79 |
| | 10 | Smart Meter 8 | 10.125.184.80 |

| | | | |
|---|---|---|---|
| GTNETx2 Port 8 | 1 | Smart Meter 9 | 10.125.184.81 |
| | 2 | Smart Meter 10 | 10.125.184.82 |
| | 3 | Smart Meter 11 | 10.125.184.83 |
| | 4 | Smart Meter 12 | 10.125.184.84 |
| | 5 | Smart Meter 13 | 10.125.184.85 |
| | 6 | Smart Meter 14 | 10.125.184.62 |
| | 7 | Smart Meter 15 | 10.125.184.63 |
| | 8 | Smart Meter 16 | 10.125.184.64 |
| | 9 | Smart Meter 17 | 10.125.184.65 |
| | 10 | Smart Meter 18 | 10.125.184.66 |

# Use Case: AMI Operation – MITM Attack

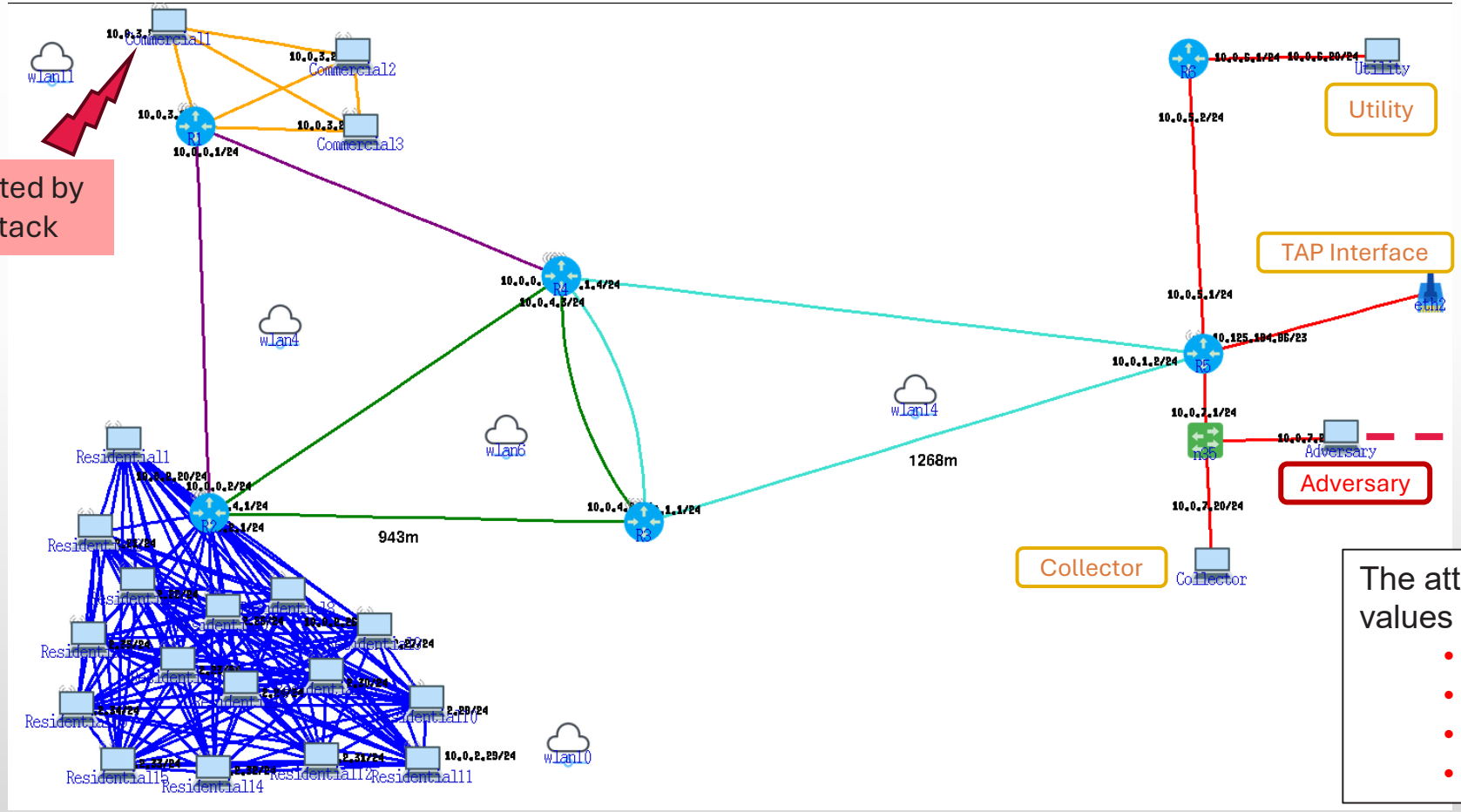
MITM Attack

- ARP spoofing techniques were used to model the attack by placing the adversary between the collector and the utility.
- The goal of the attack was to impact the integrity of the communication between the collector and the utility.
- NFQueue was used to access packets received.
- Data changed for the financial benefit of customer COMM 1. Lower load consumed and higher load generated.



# Use Case: AMI Operation – MITM Attack

SM #5 targeted by the MITM attack




The attacker changed the reported values of SM #5 to:

- Load: 5 kW, 5 kVAr
- PV generation: 200 kW
- BESS output: 25 kW
- EV load: 1 kW

# Use Case: AMI Operation – Denial of Service (DoS) Attack

- A SYN flood generated by Hping3 was used for the Denial-of-Service (DoS) attack.
- The target was the collector node in the CORE network.
- The attacker floods the collector with SYN packets, overwhelming its resources.
- As a result, the collector could not receive new data from the smart meters.
- Consequently, old data was forwarded to the utility node.

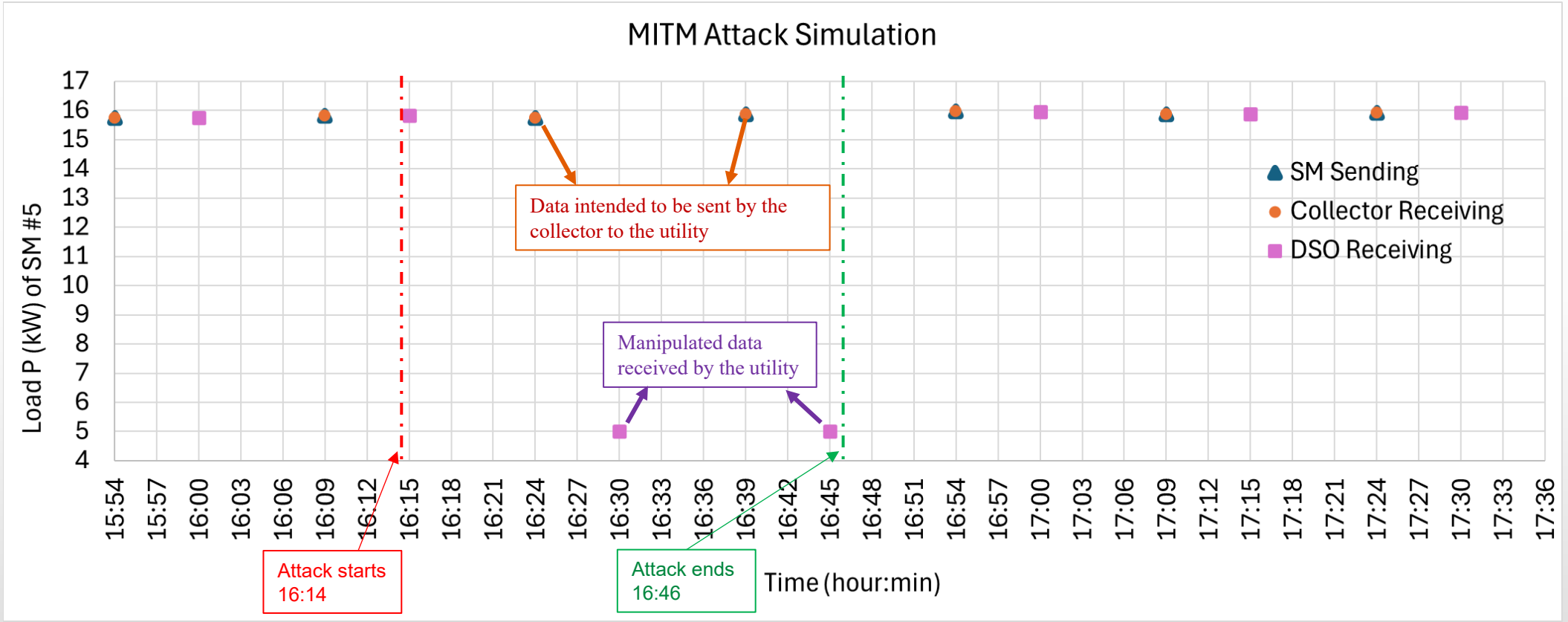
Hping3 -S -p 7001 –d 90 --flood --rand_source 10.0.5.20

# Studies and Results

# Use Case: AMI Operation -- Simulation Setup

- During the simulation, the smart meters sent the data every 15 minutes to the collector.
- The simulation was started at 15:54 and ended at 20:00.
- Smart meters sent the data to the collector at 15:54 and every 15 min after that.
- The collector sent the data to the utility at 16:00 and every 15 min after that.
- The MITM attack was started at 16:14 and ended at 16:45.
- The DoS attack was started at 17:52 and ended at 18:52.

# Case Study 1 -- MITM Attack Results




This figure illustrates the scenario for SM #5, where the data is affected. Data transmission for all other SMs proceeds normally.

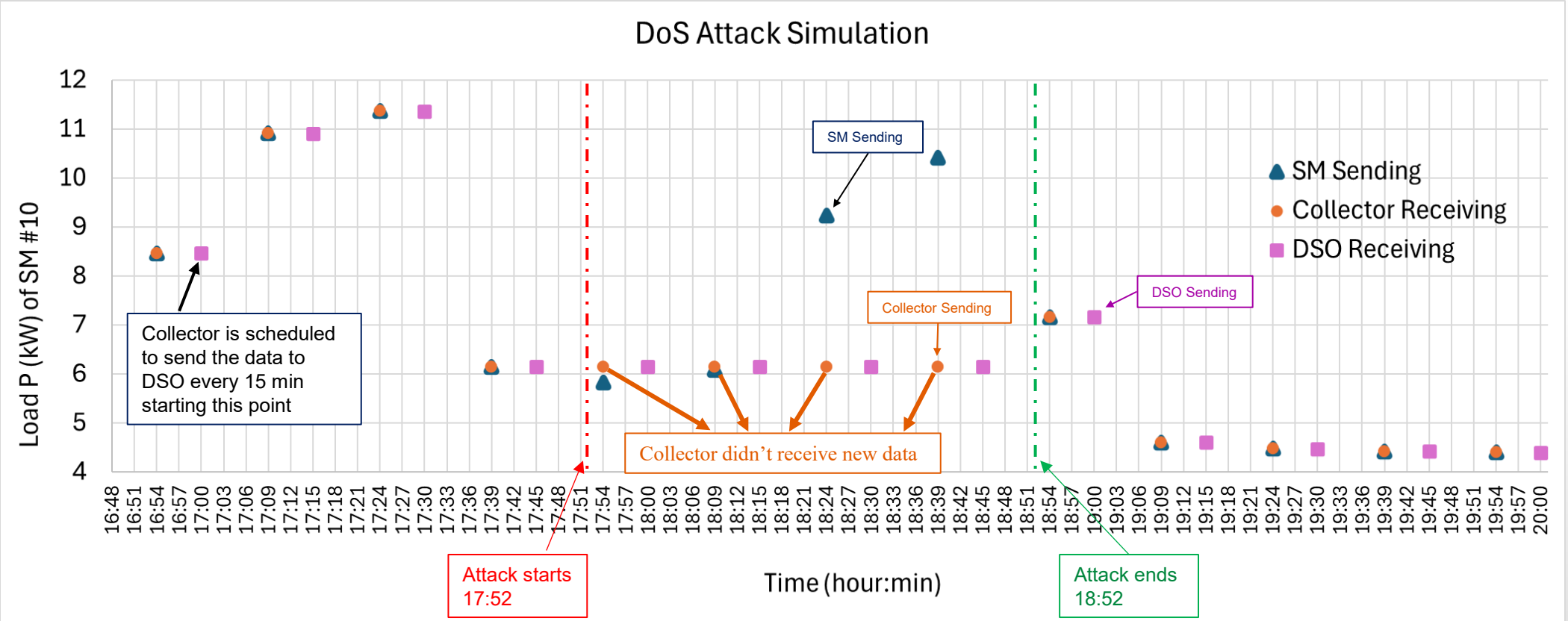
# Case Study 1 -- MITM Attack Results

| Send/Receive | Meter ID | Hour | Minute | Load P (MW) | Load Q (MW) | PV P (MW) | PV Q (MVar) | BESS P (MW) | BESS Q (MVar) | EV1 P (MW) | EV1 Q (Mvar) | EV2 P (MW) | EV2 Q (Mvar) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Collector_Receiving | 5 | 15 | 54 | 0.01575 | 0.002805 | 0 | 0 | 0 | 0 | 0.0001 | 0.0001 | 0 | 0 |
| Utility_Receiving | 5 | 16 | 0 | 0.01575 | 0.002805 | 0 | 0 | 0 | 0 | 0.0001 | 0.0001 | 0 | 0 |
| Collector_Receiving | 5 | 16 | 9 | 0.015823 | 0.002796 | 0 | 0 | 0 | 0 | 0.000101 | 0.0001 | 0 | 0 |
| Utility_Receiving | 5 | 16 | 15 | 0.015823 | 0.002796 | 0 | 0 | 0 | 0 | 0.000101 | 0.0001 | 0 | 0 |
| Collector_Receiving | 5 | 16 | 24 | 0.015741 | 0.002805 | 0 | 0 | 0 | 0 | 0.0001 | 0.0001 | 0 | 0 |
| Utility_Receiving | 5 | 16 | 30 | 0.005 | 0.005 | 0.2 | 0 | 0.025 | 0 | 0.001 | 0.001 | 0.001 | 0.001 |
| Collector_Receiving | 5 | 16 | 39 | 0.015882 | 0.002814 | 0 | 0 | 0 | 0 | 0.032681 | 0.0001 | 0 | 0 |
| Utility_Receiving | 5 | 16 | 45 | 0.005 | 0.005 | 0.2 | 0 | 0.025 | 0 | 0.001 | 0.001 | 0.001 | 0.001 |
| Collector_Receiving | 5 | 16 | 54 | 0.015962 | 0.002822 | 0 | 0 | 0 | 0 | 0.000101 | 0.0001 | 0 | 0 |
| Utility_Receiving | 5 | 17 | 0 | 0.015962 | 0.002822 | 0 | 0 | 0 | 0 | 0.000101 | 0.0001 | 0 | 0 |

During MITM attack, the collector receives these datasets and sends them to the utility.

The utility receives the manipulated data by the attacker.

# Case Study 1 -- DoS Attack Results




This figure illustrates the data flow for SM #10, which follows the same pattern as for all other SMs.

# Future Work

- Study vulnerabilities and operational impacts of cyberattacks on the synthetic feeder during the simulation of various automation applications
- Develop detection, mitigation, and protection strategies against cyber-physical threats.