
Your world in real time.
RTDS
Technologies
RTDS.COM

Cyber-Physical simulation capabilities of the RTDS

RTDS Technologies

RTDS.COM

AGENDA

- Why cyber-physical simulations are important?
- Why use the RTDS simulator for the testing?
- What are the limitations?
- How to conduct the Co-simulatons?
- Summary

Why Cyber-physical Simulations are Important?

- Power systems rely on communication between the Intelligent Electronic devices (IED) and Control center
- Devastating cyber-attacks on power systems
- Security by obscurity is not working anymore
- Can test the response of controls and automated cyber resilience platforms to malicious data Fine tune the controls
- Conduct anomaly detection training and testing

Why use the RTDS simulator for the testing?

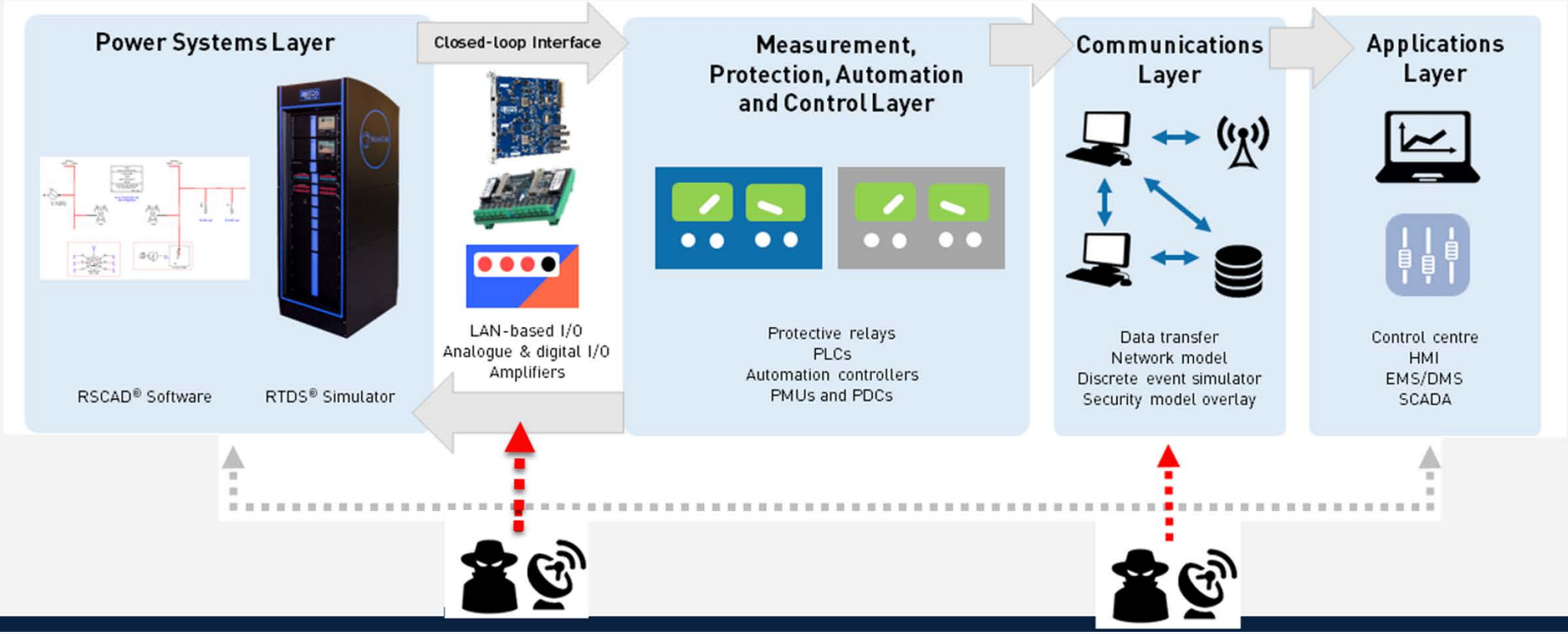
- RTDS Simulator is capable of Simulating a Power system in very high detail in real time
- It can run Hardware in the loop simulations
- It has network interfaces which supports a variety of ICS protocols
- Possible to do what if analysis without risk and with reproducibility

What are the limitations?

- Stages in a Cyber-attack

- Methods introduced only focus on the Actions on the Objective stage
- Work only on unencrypted data

How the RTDS Simulator fit in the Cyber-physical scenario

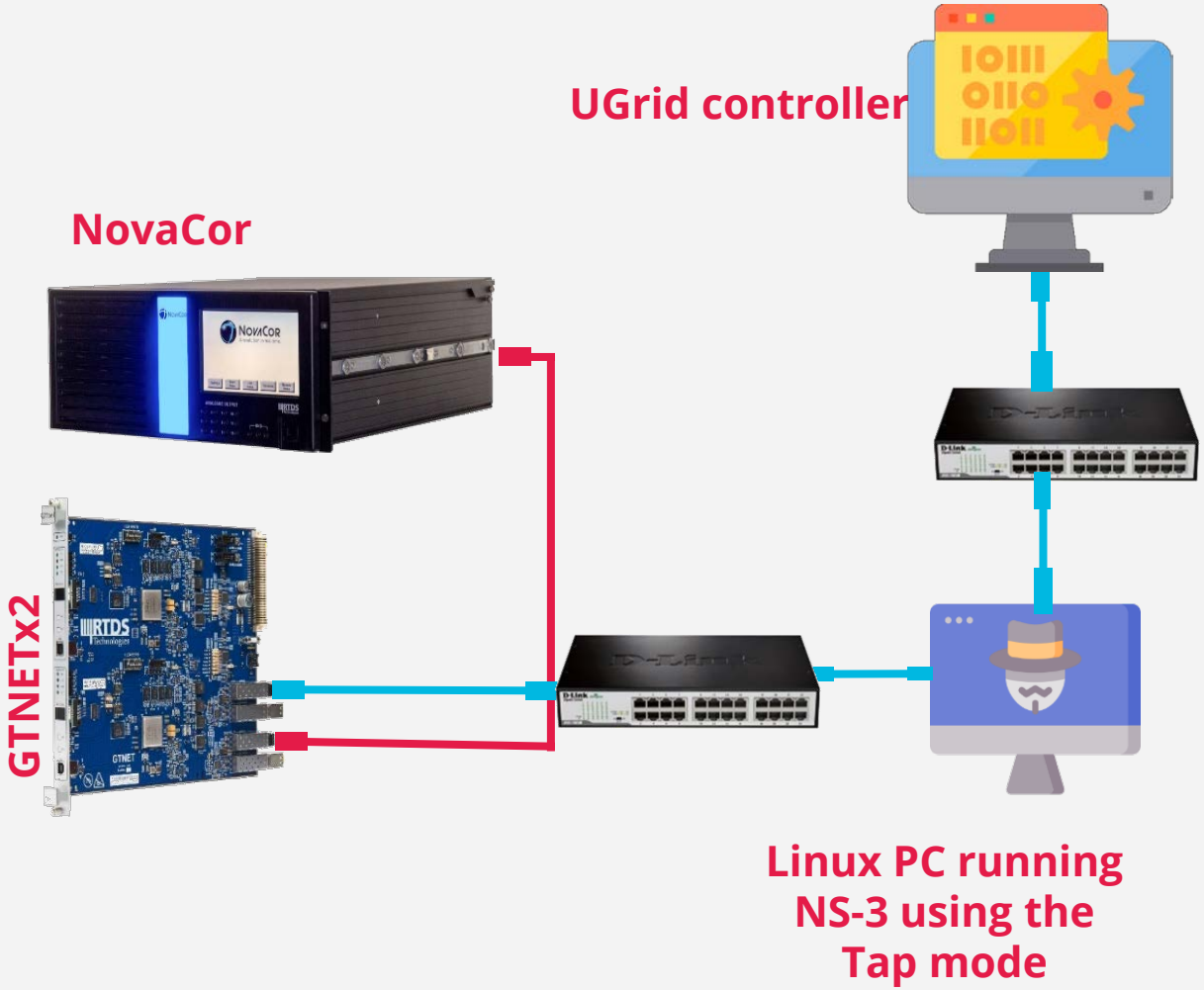


How to conduct the Co-simulations?

- RTDS Simulator can be interfaced with:
  - NS-3 network simulator
  - DeterLab Network emulation platform
  - The SNORT based packet modifier

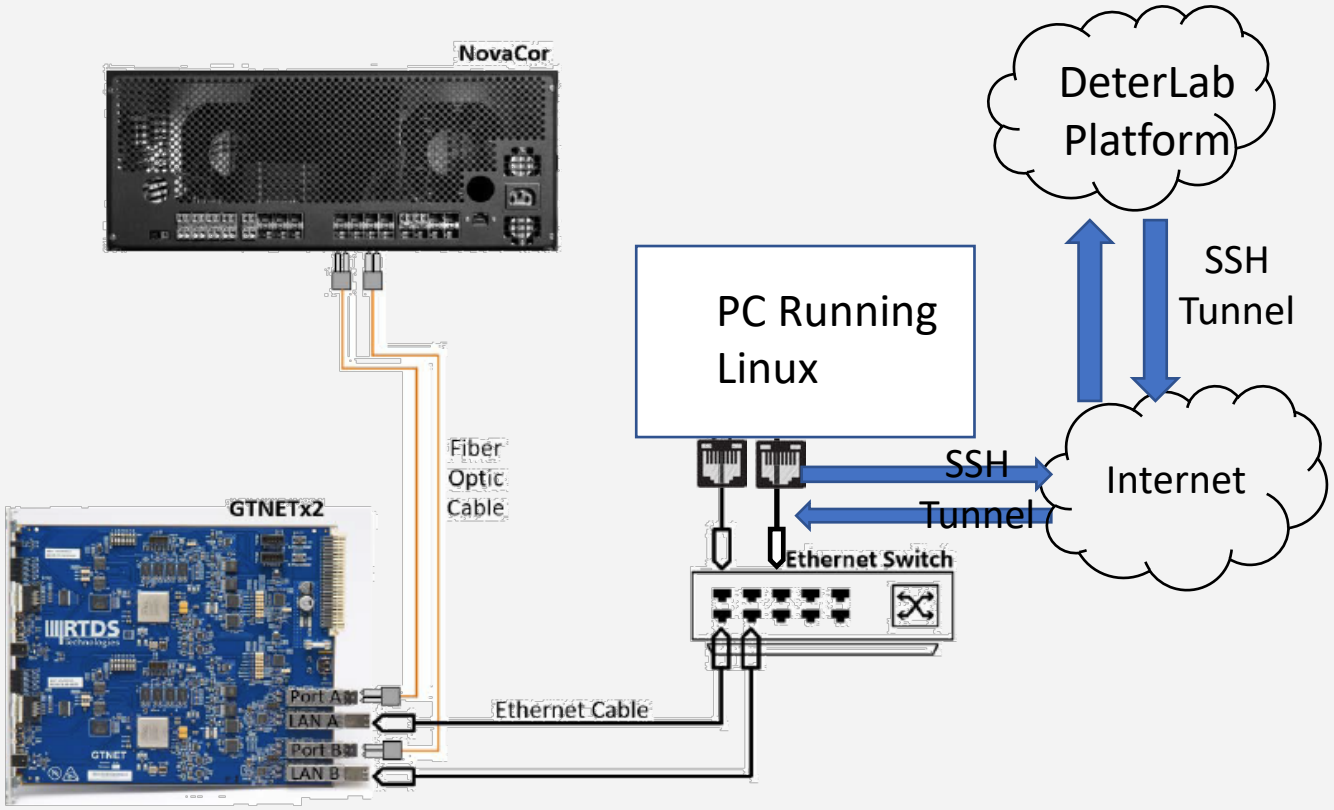
Using the NS-3 simulator with RTDS

- Advantages:
  - Can model an entire communications network
- Limitations:
  - Still can only modify data on general TCP/UDP socket communication and DNP3
  - We are develop functions to support other ICS protocols
  - The amount of traffic it can handle is limited



Using the DeterLab Network emulator with RTDS

- Advantages:
  - Can model an entire communications network using actual computers
- Limitations:
  - There is a node limit
  - Cannot use Ethernet multicast protocols
  - Need to develop functions to support ICS protocols



Using the SNORT based packet modifier with RTDS to modify packets/Frames

- Snort has APIs to modify/process the Ethernet Layer packets and the Transport layer packets
- We use preprocessors to modify the Ethernet Multicast Packets (SV and GOOSE)
- We use Dynamic preprocessors to modify the Transport layer packets (DNP3, MODBUS,PMU,MMS,IEC104)

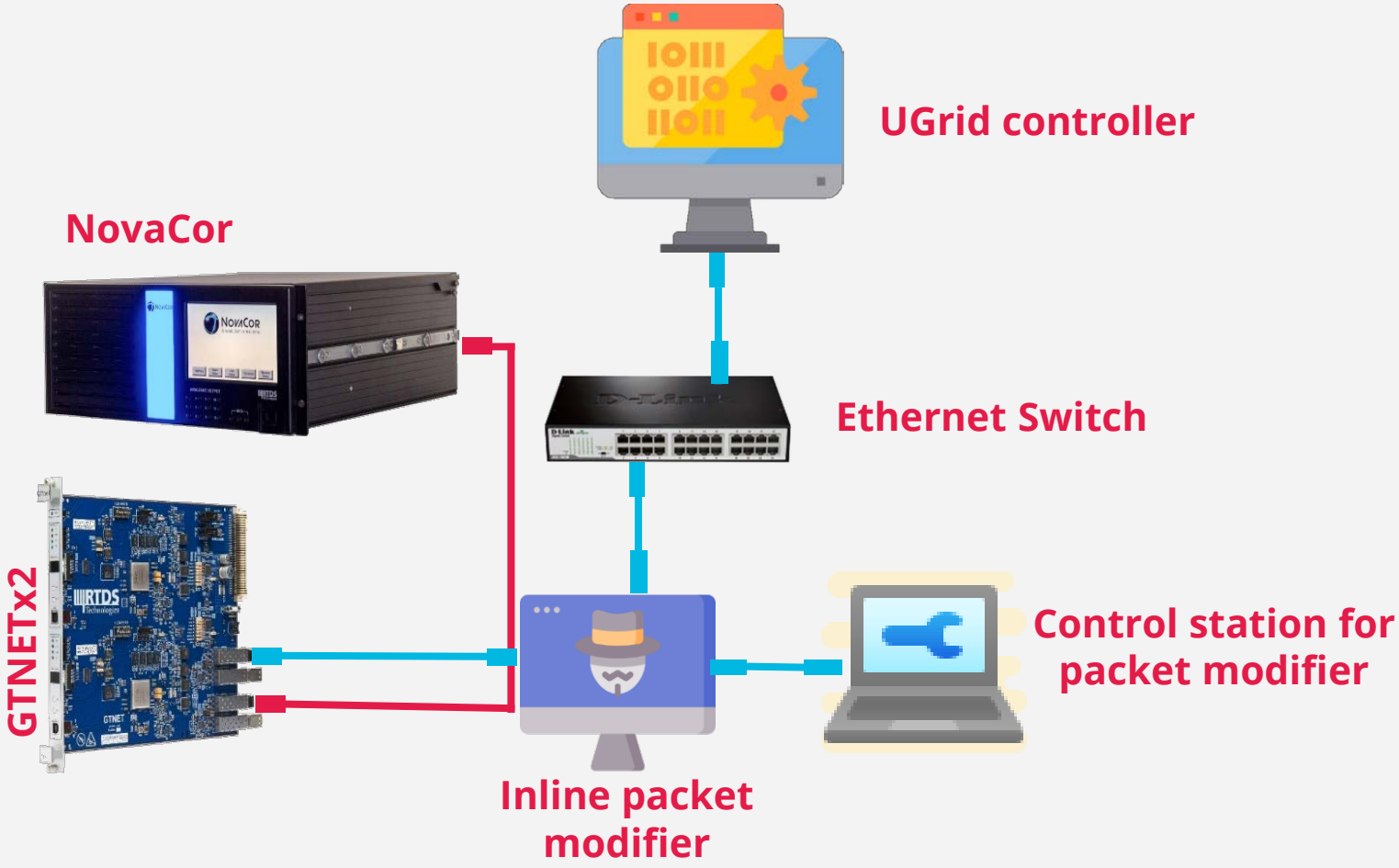
Introducing network impairment to packets

- We use the Linux traffic control module to:
  - Introduce Delay and Jitter to packets
  - Randomly drop a percentage of packets
  - Randomly duplicate a percentage of packets
  - Reorder packets
  - Randomly corrupt (modify a single bit in a random location) a percentage of packets

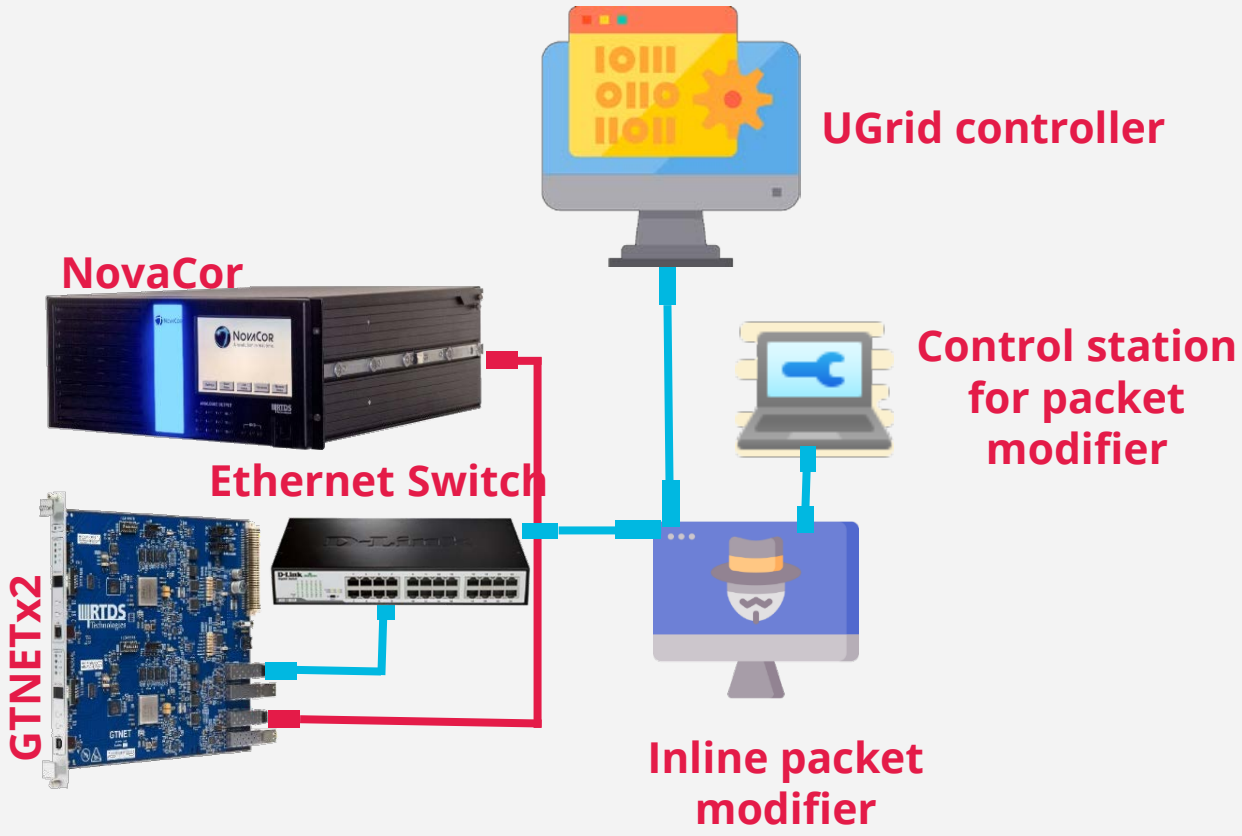
Placing the Inline packet modifier in the network

- The Transport layer protocols can be intercepted at either the Server or the Client
- The Ethernet Layer Multicast Protocol frames:
  - Can only be intercepted at the publisher (If you want to delay them or drop them)
  - Should use a fabricated Ethernet frame if you want to modify the data read by the subscriber after the frame enters the network

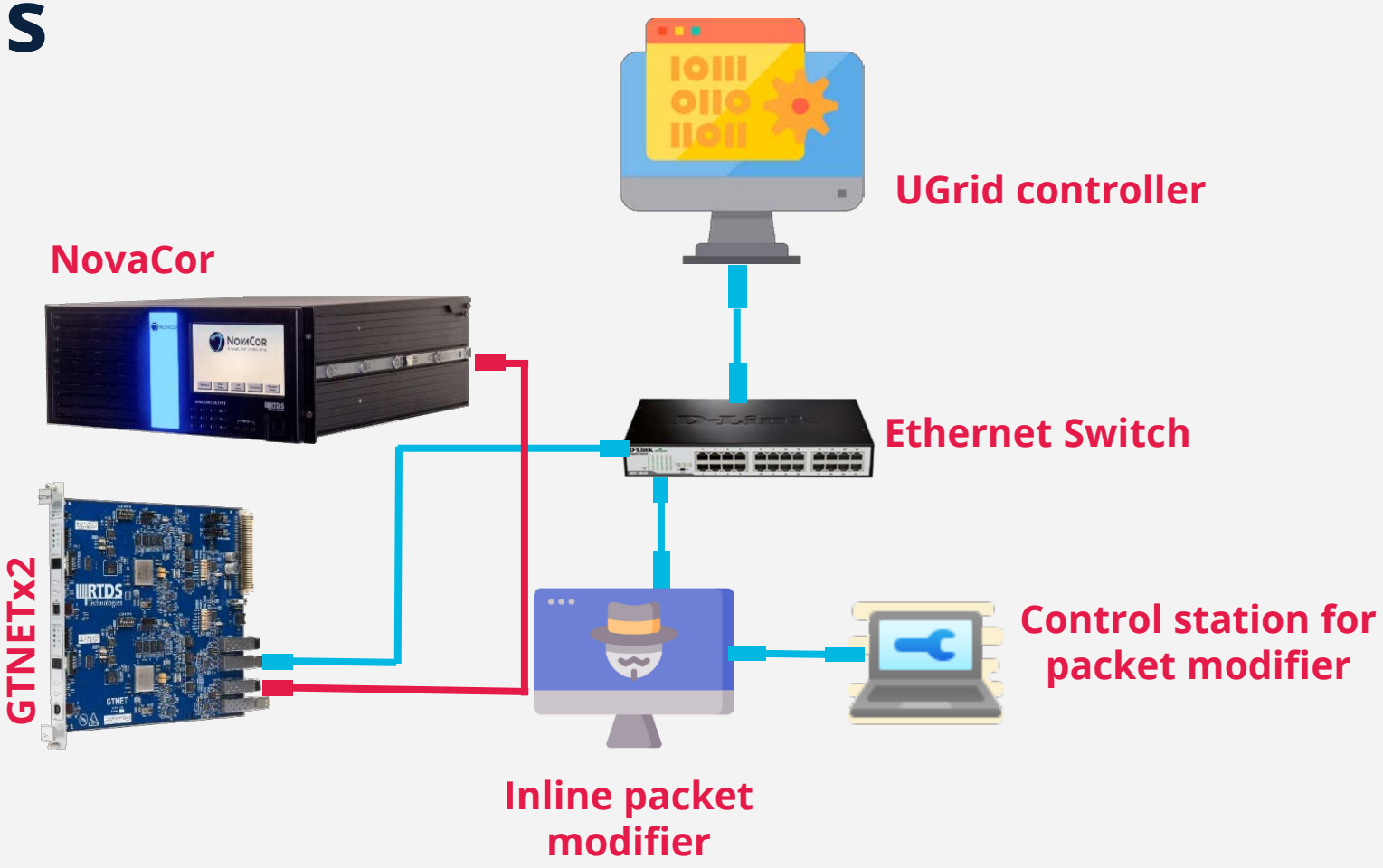
Placement in the server side



Placement in the Client side

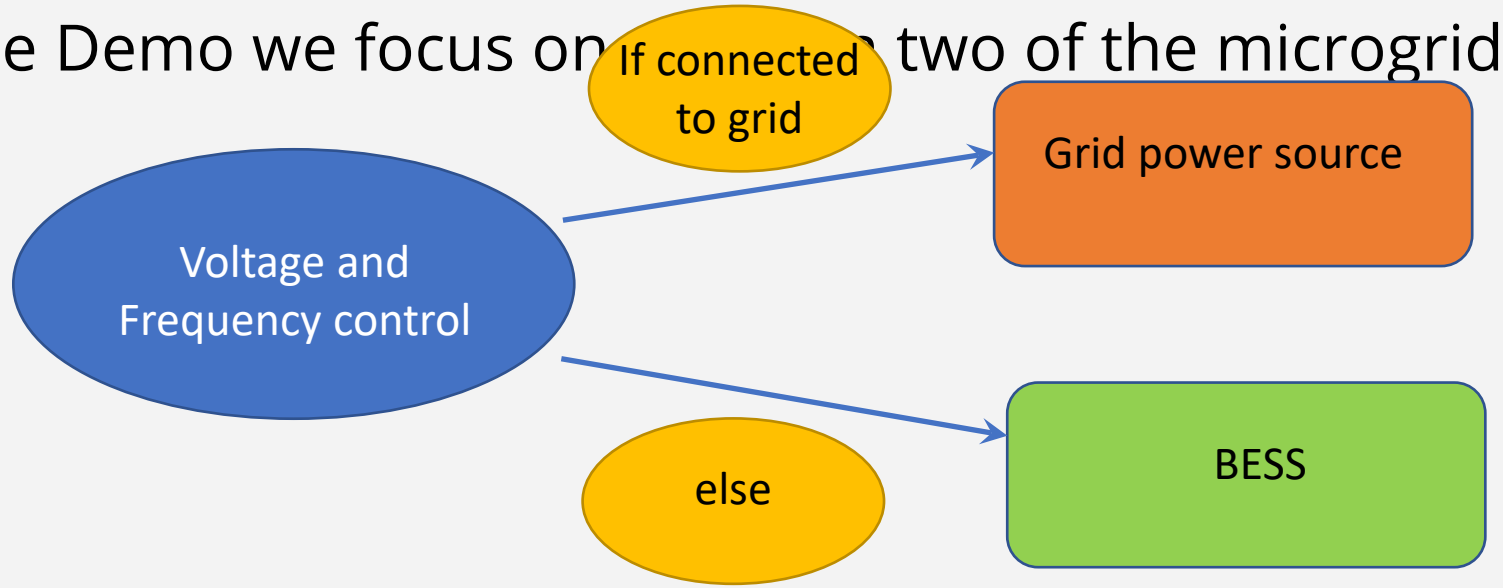


Placement for Multicast protocols

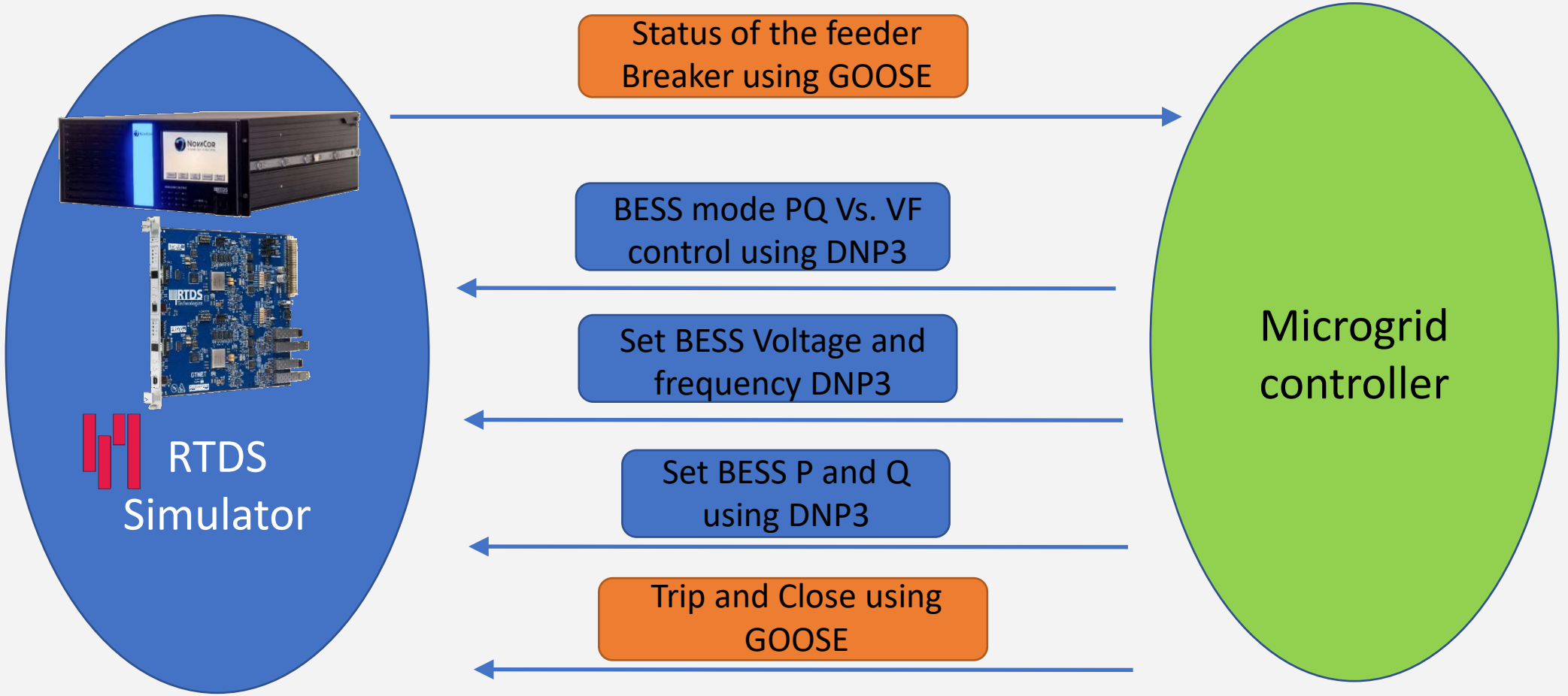


Example Microgrid Case with MITM Attack on DNP3 and GOOSE

- The Banshee Microgrid is modelled in the RTDS simulator
- We use a Microgrid controller to automate the controls of this microgrid
- In the Demo we focus on [illegible] two of the microgrid



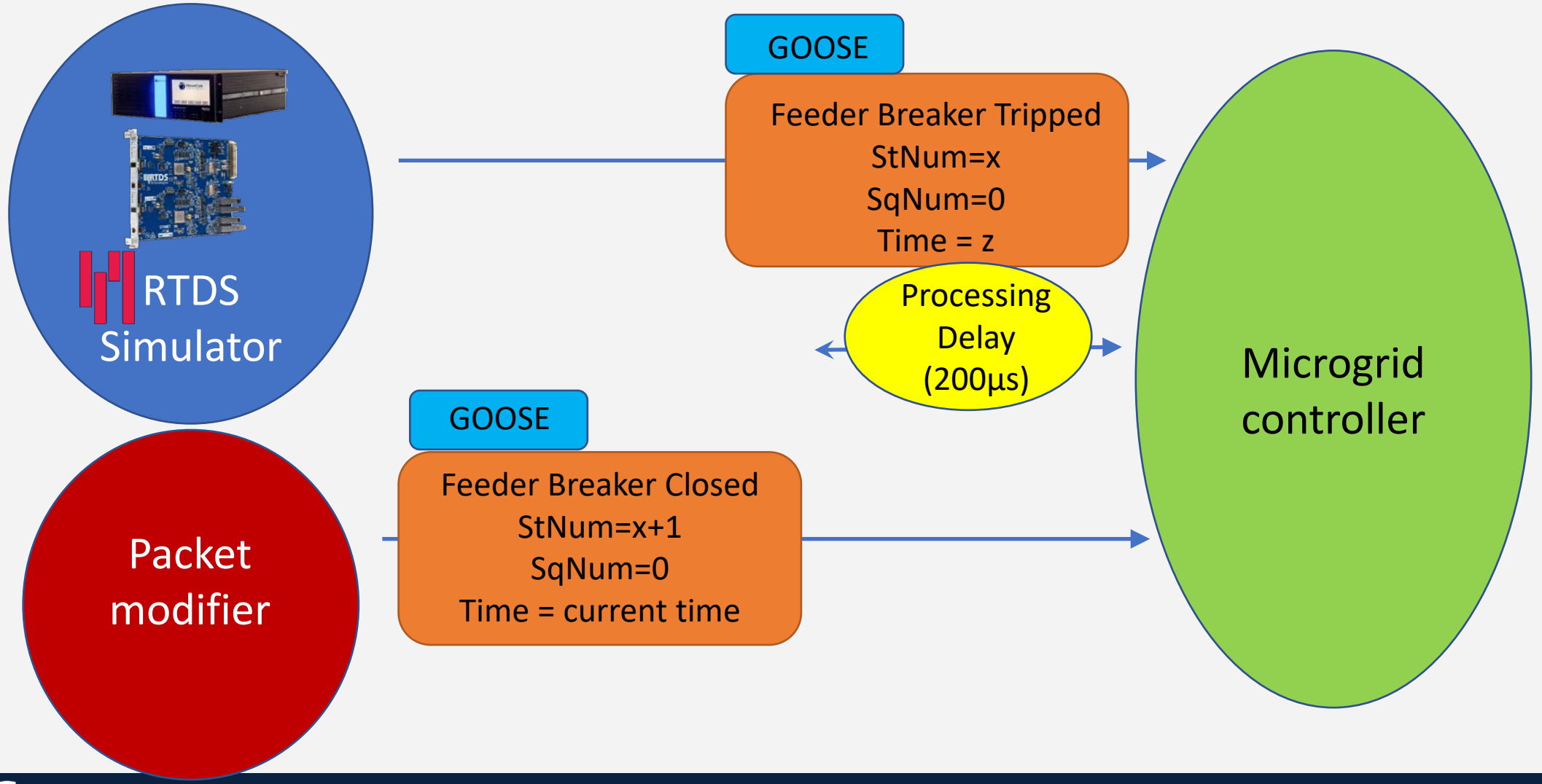
Control message flow



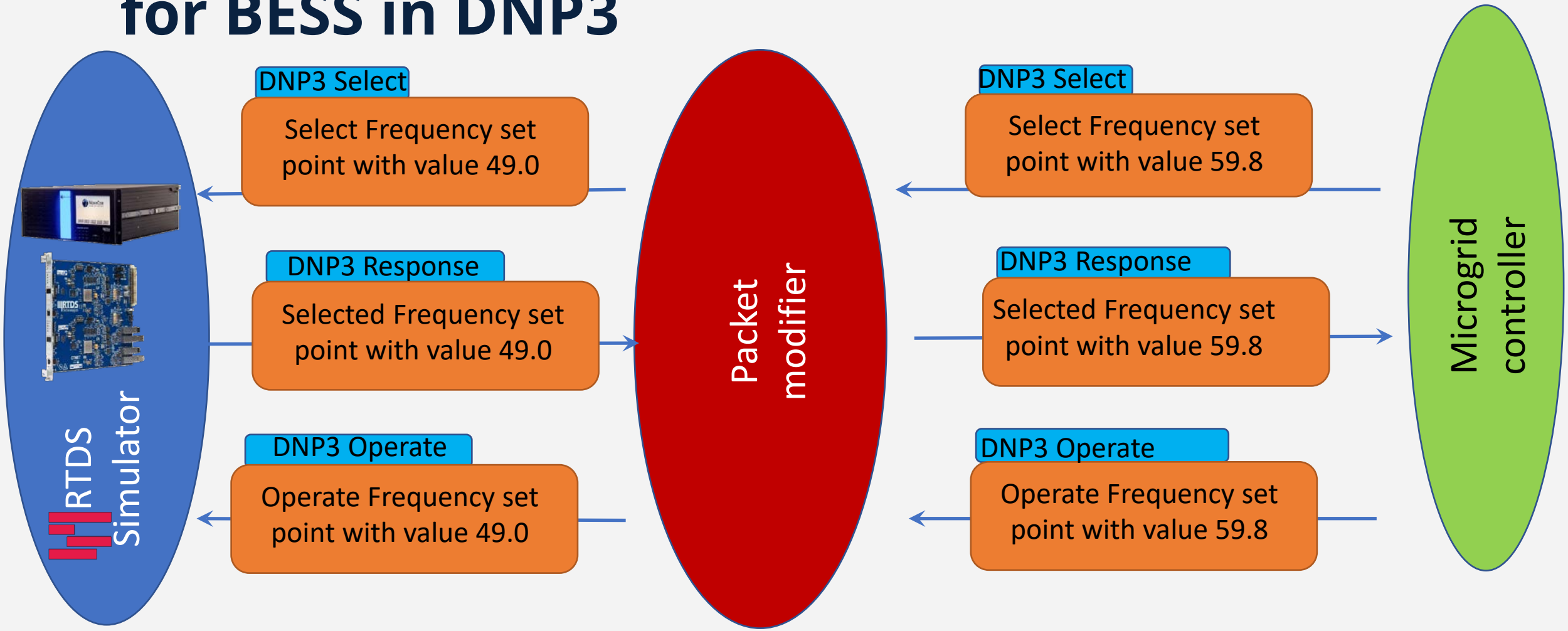
MITM attacks possible

- Sending GOOSE messages to overwrite the Feeder breaker status at the controller
- Modifying the Set voltage and frequency for the BESS during transit
- Modifying the set P and Q values for the BESS

Overwriting the feeder breaker status



Modifying Frequency set points for BESS in DNP3



Demo of normal operation

Simulation video with DNP3 set point modification

Simulation video with GOOSE feeder status modification

Summarize

- What makes Cyber-physical simulations important
- Reasons to use RTDS simulator for the testing
- The limitations
- Conducting Co-simulations

THANK YOU!
QUESTIONS?

RTDS Technologies

RTDS.COM