TEXAS A&M UNIVERSITY
Engineering

Real-time Power System Simulation with Hardware Devices through DNP3 in Cyber-Physical Testbed

Hao Huang (Presenter), C. Matthew Davis, and Katherine R. Davis
Texas A&M University
hao_huang@tamu.edu

Outline

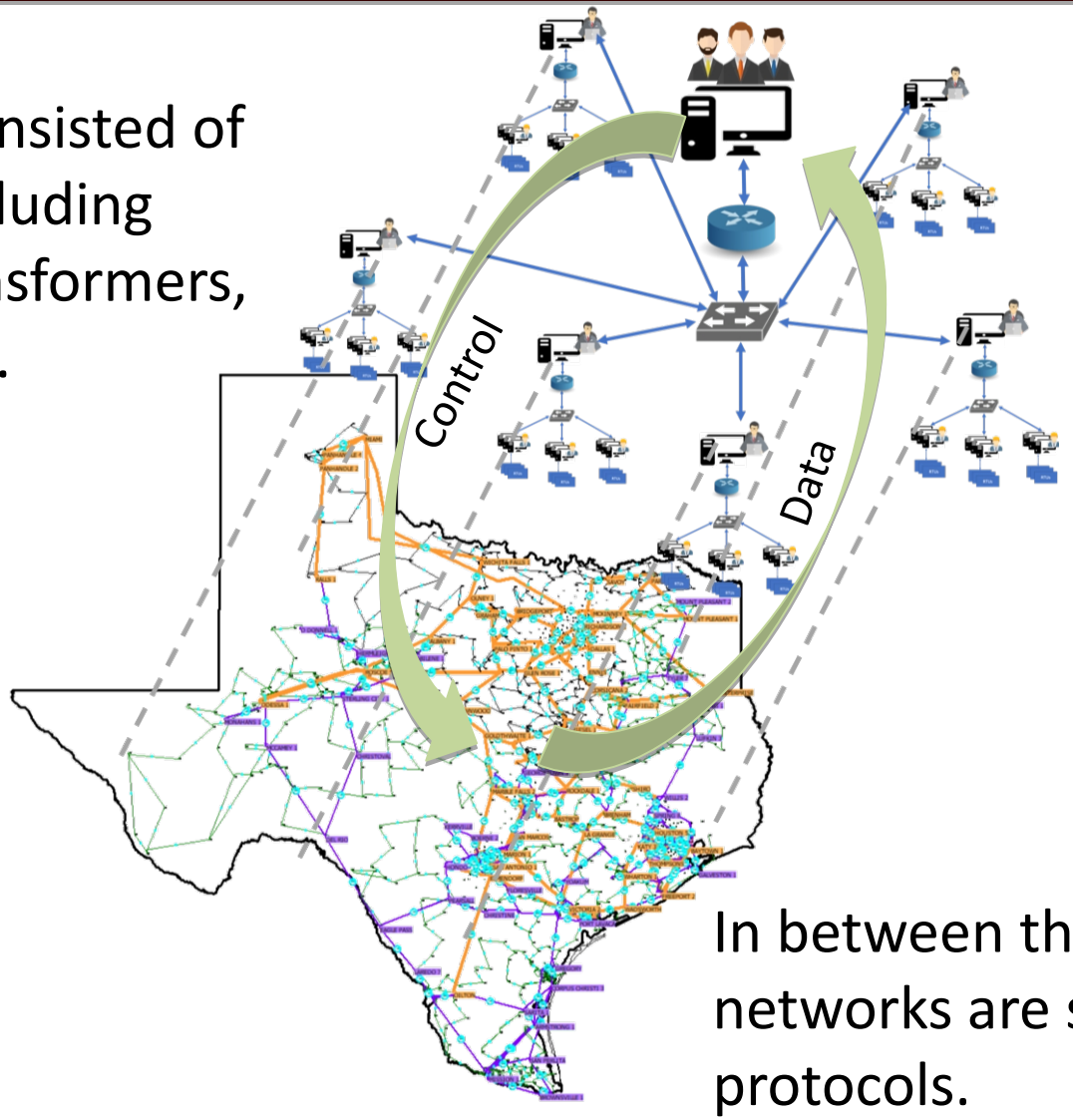
TEXAS A&M UNIVERSITY
Engineering

- Background of Cyber-Physical Power Systems
- Brief of DNP3 Protocol
- Hardware-in-the-loop Testbed using DNP3
- Configuration and Validation
- Exemplar of Data Acquisition and Control
- Conclusion and Future Work

Background of Cyber-Physical Power Systems

TEXAS A&M UNIVERSITY Engineering

Physical Network is consisted of power equipment, including generators, loads, transformers, transmission lines, etc.



Cyber Network is consisted of communication devices and management software, including routers, switches, EMS, etc.

In between the cyber and physical networks are sensors, IEDs, and ICS protocols.

Brief of DNP3 Protocol

TEXAS A&M UNIVERSITY
Engineering

Distributed Network Protocol 3 (DNP3) is commonly used in ICS for data acquisition and control, which is a protocol for transmission of data from point A to point B using serial and IP communications.

It provides the rules for remotely located computers and master station computers to communicate data and control commands.

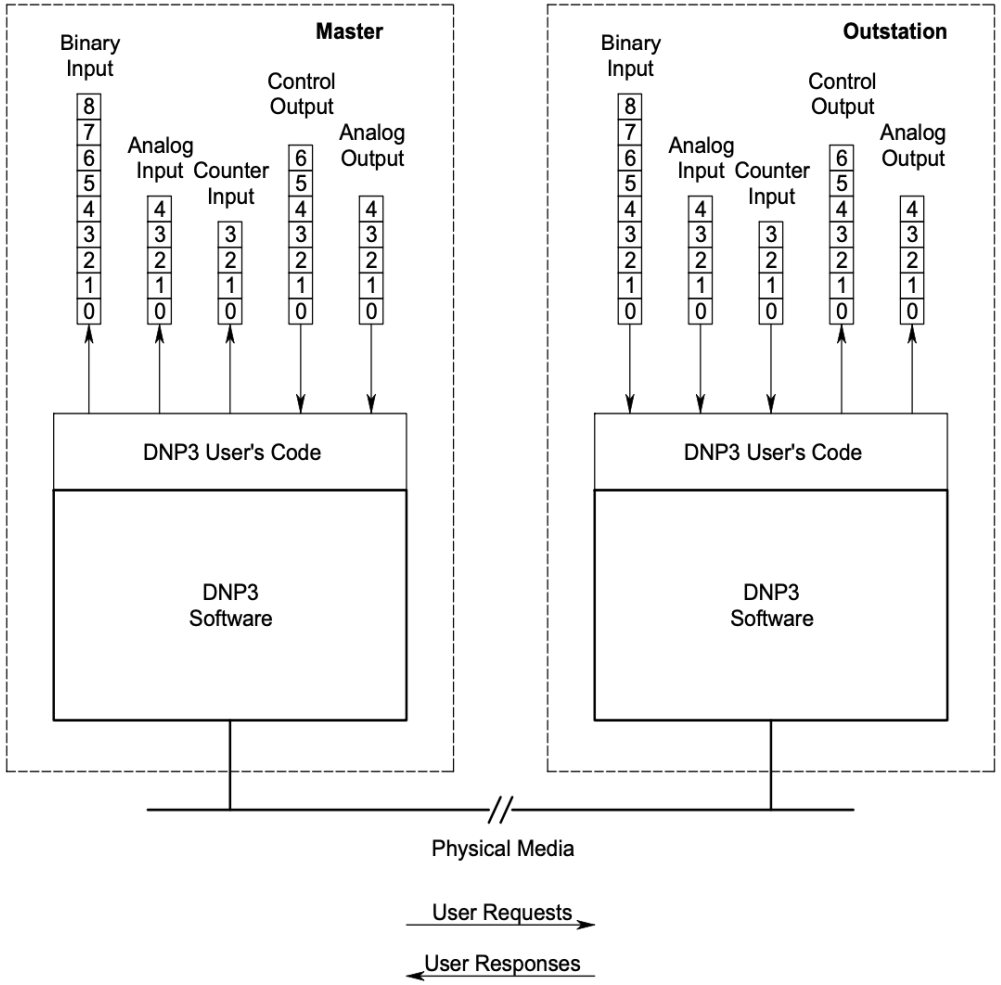


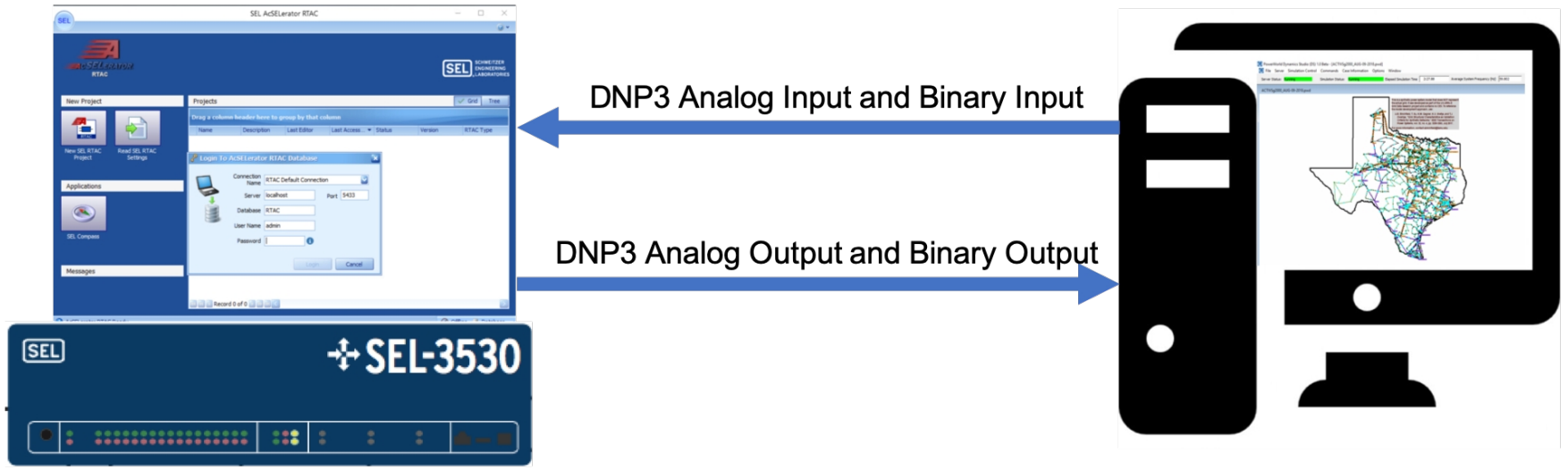
Figure source: A DNP3 Protocol Primer https://www.dnp.org/About/Overview-of-DNP3-Protocol

Hardware-in-the-loop Testbed using DNP3

TEXAS A&M UNIVERSITY Engineering

SEL Real-time Automation Controller (RTAC)

PowerWorld DynamicStudio (PWDS)



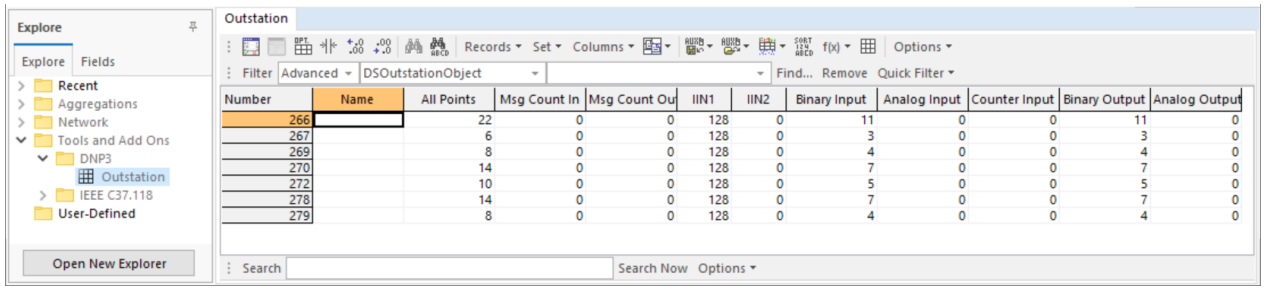
DNP3 Master/Client

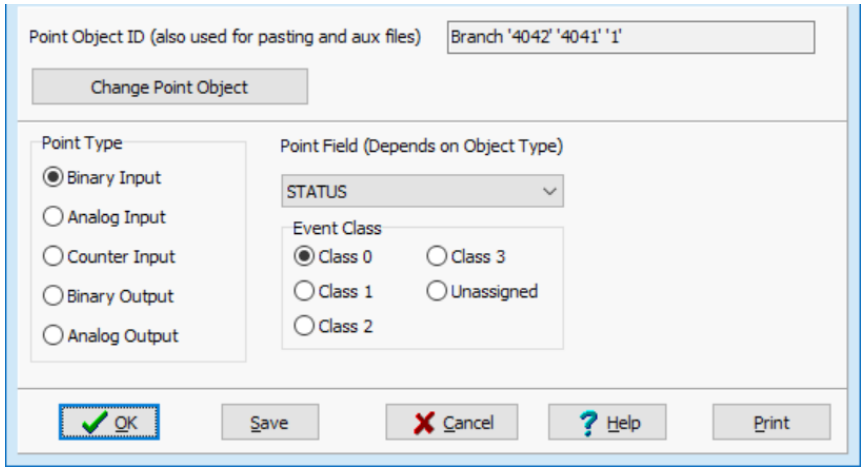
DNP3 Outstation/Server

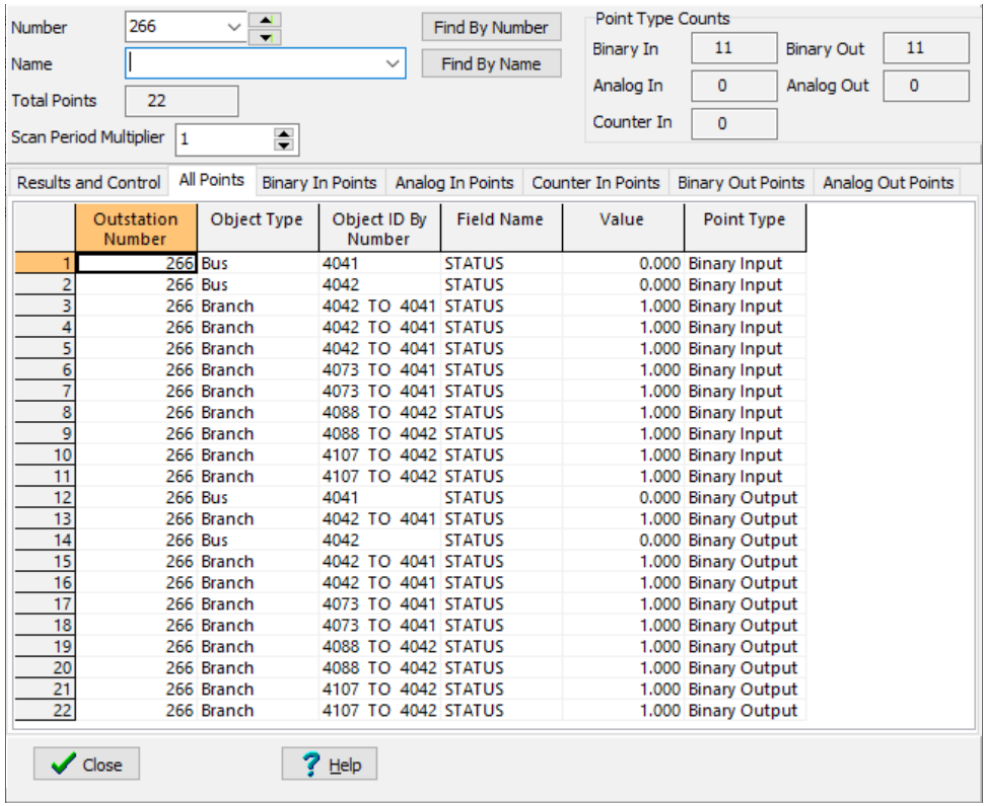
Configuration and Validation

TEXAS A&M UNIVERSITY Engineering

Physical Information



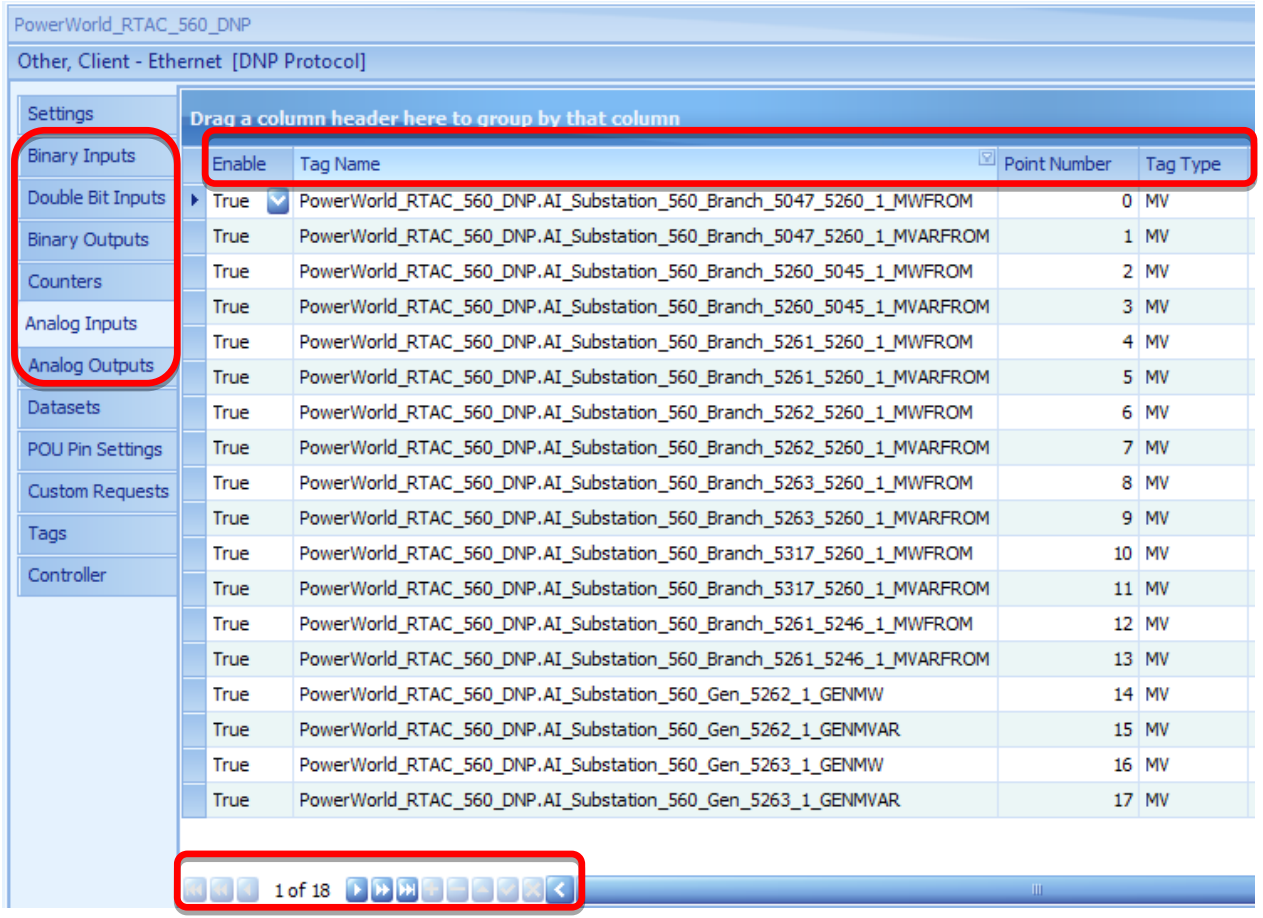




Configuration and Validation

TEXAS A&M UNIVERSITY Engineering

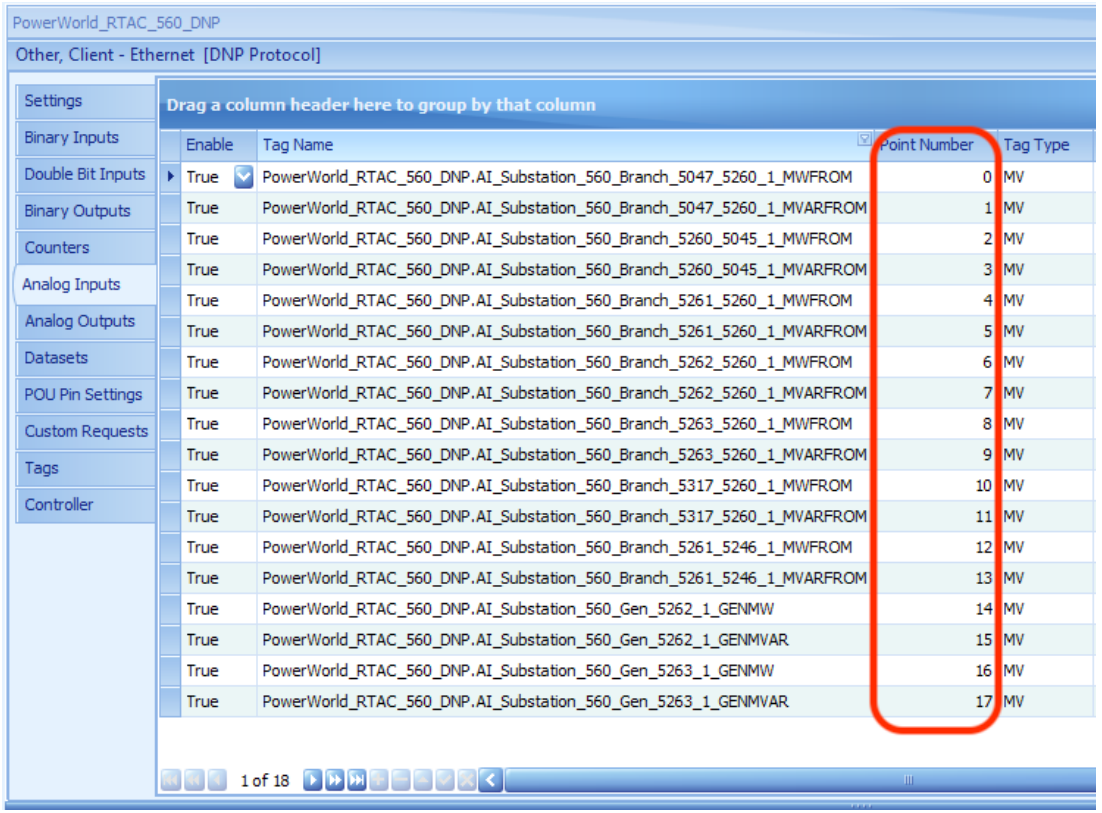
Physical Information

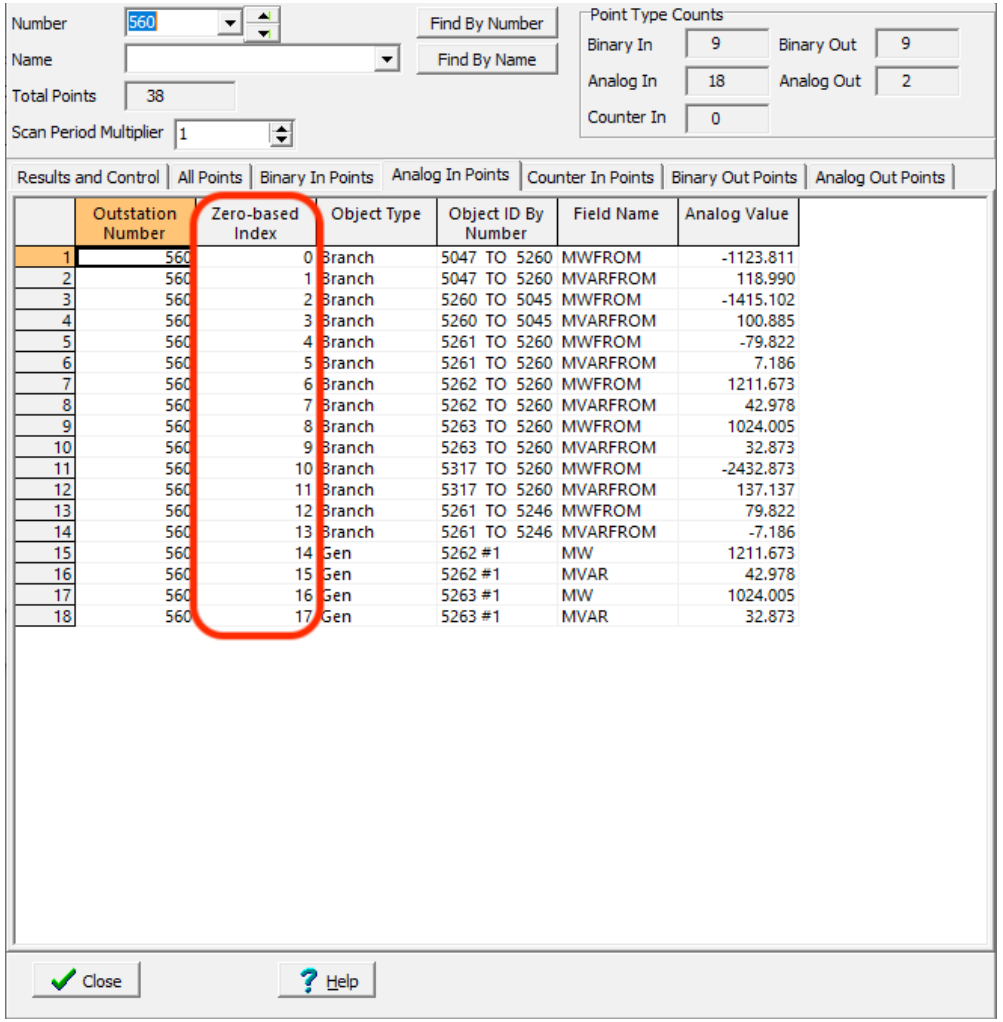


Configuration and Validation

TEXAS A&M UNIVERSITY Engineering

Physical Information

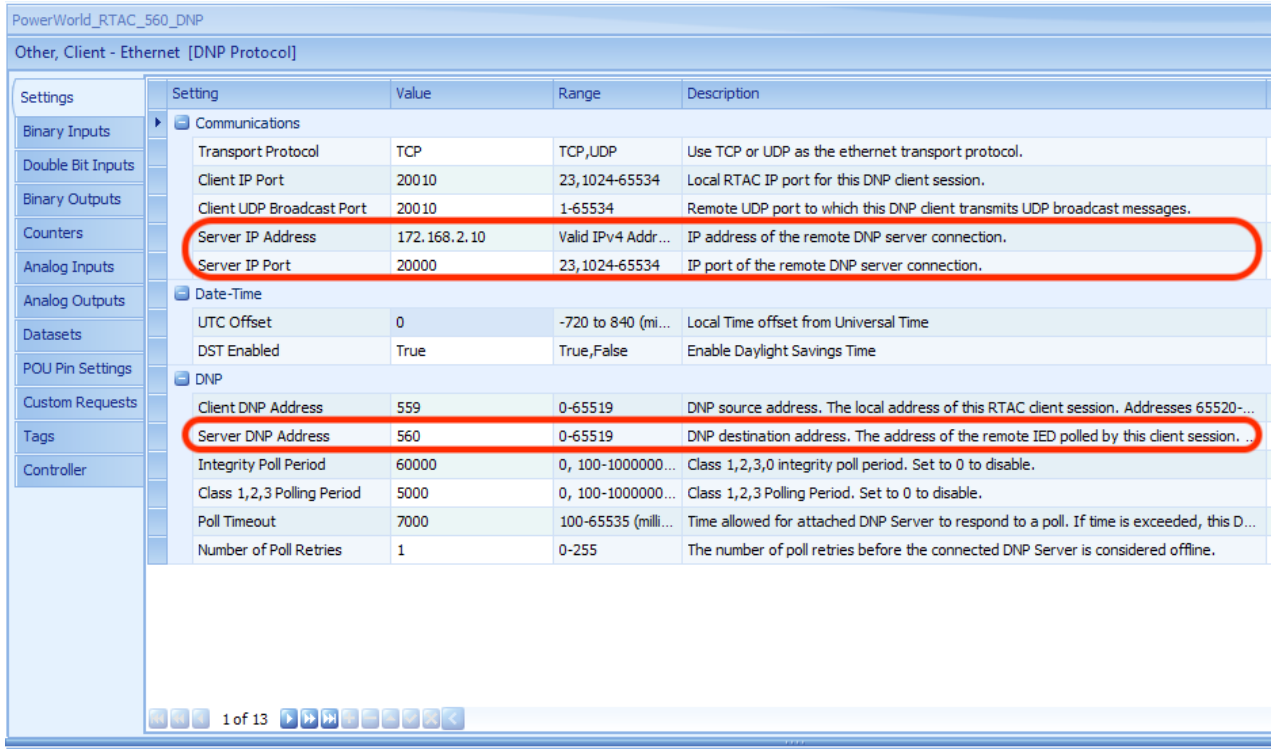




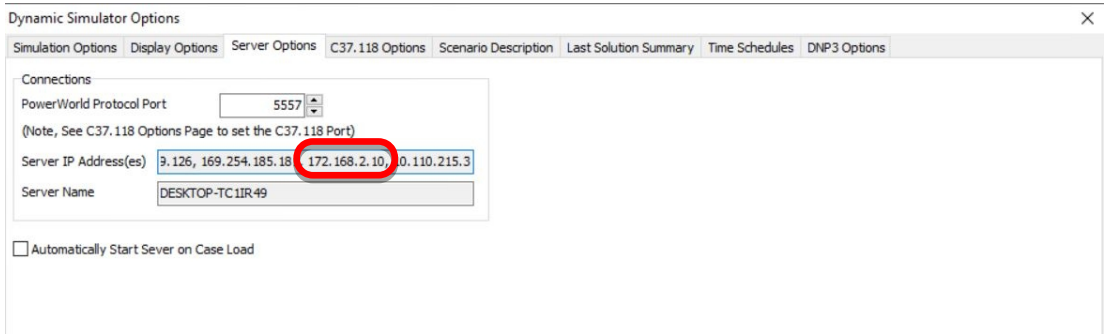
Configuration and Validation

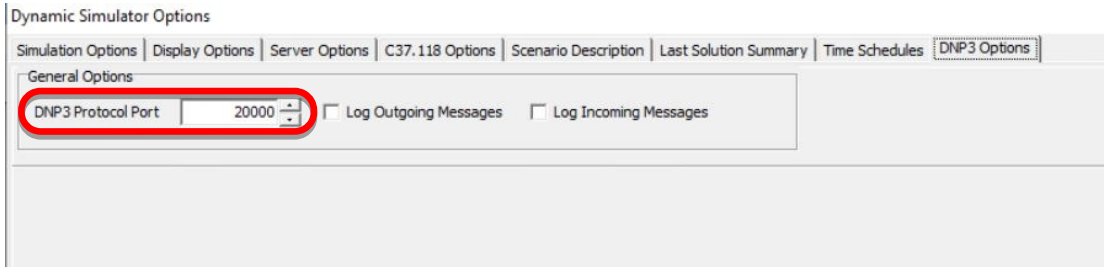
TEXAS A&M UNIVERSITY Engineering

Cyber Information



IP:172.168.2.2

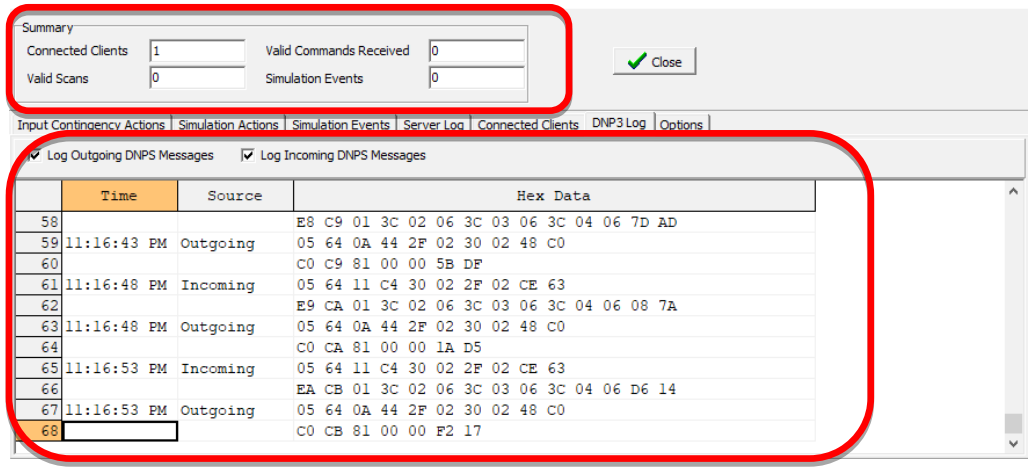


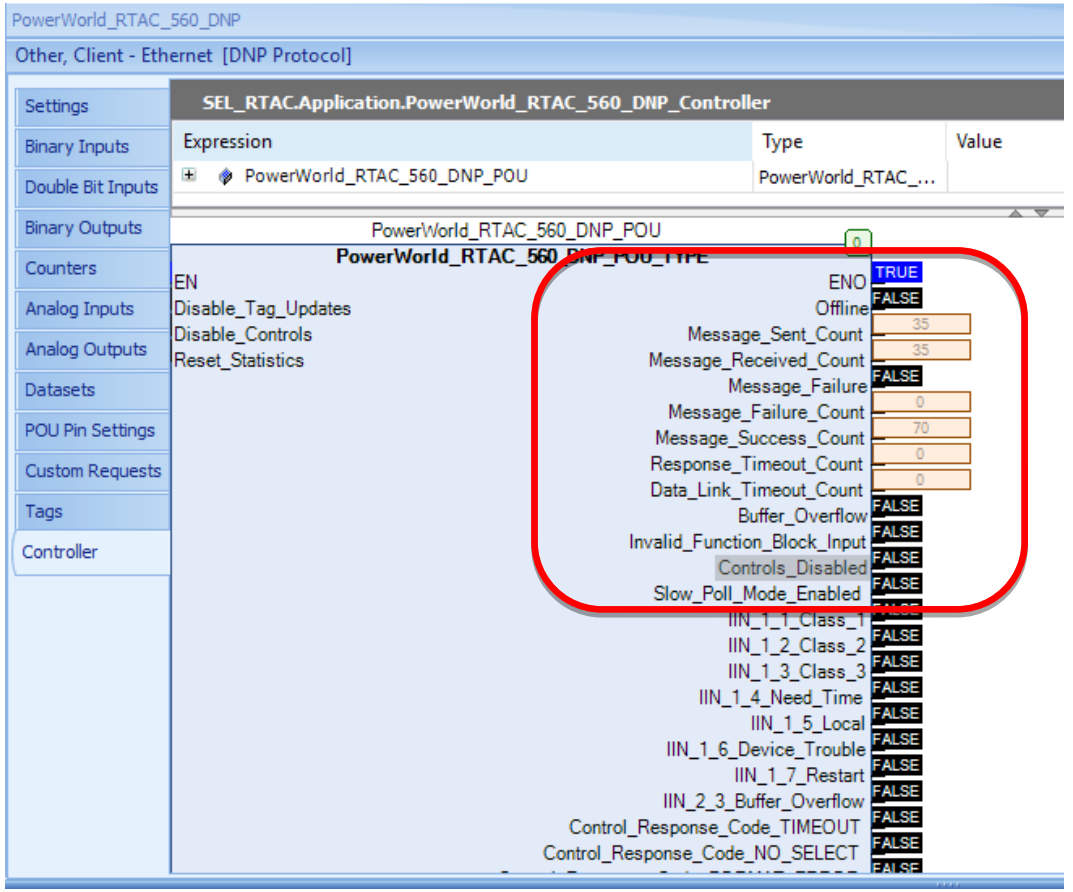


Configuration and Validation

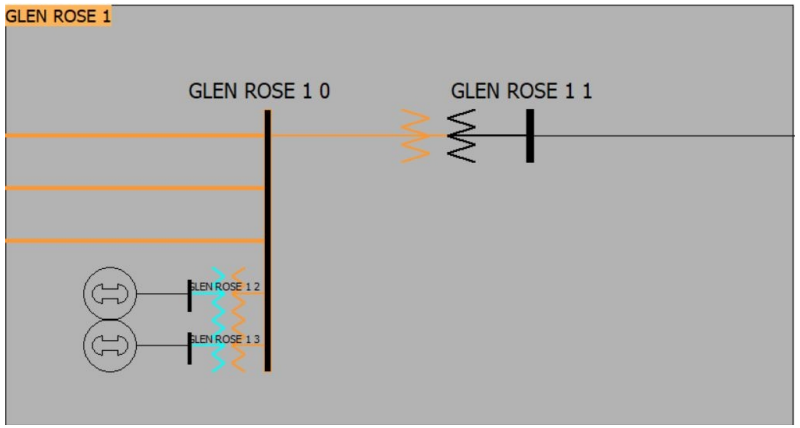
TEXAS A&M UNIVERSITY Engineering

Validation

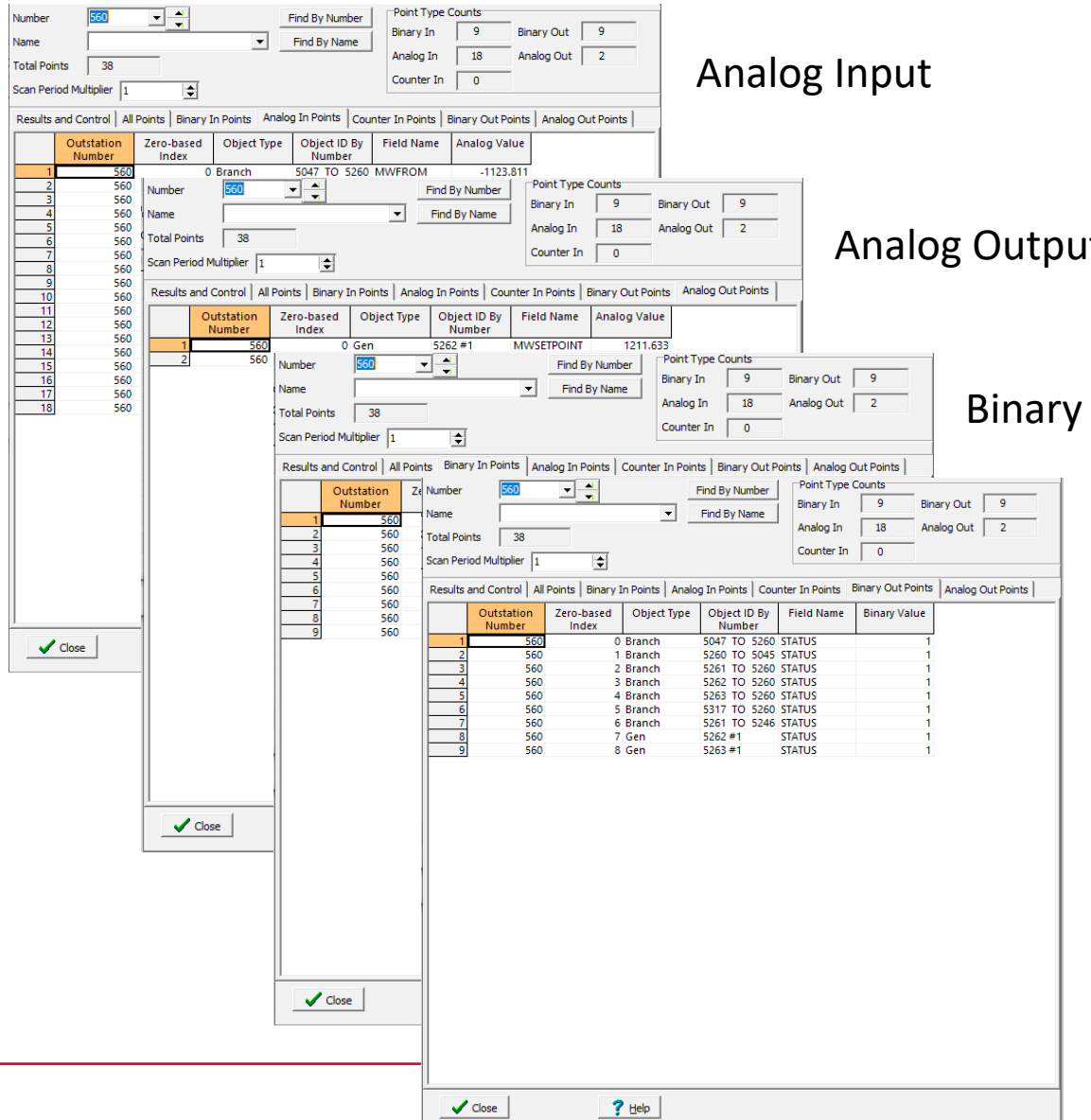




Exemplar

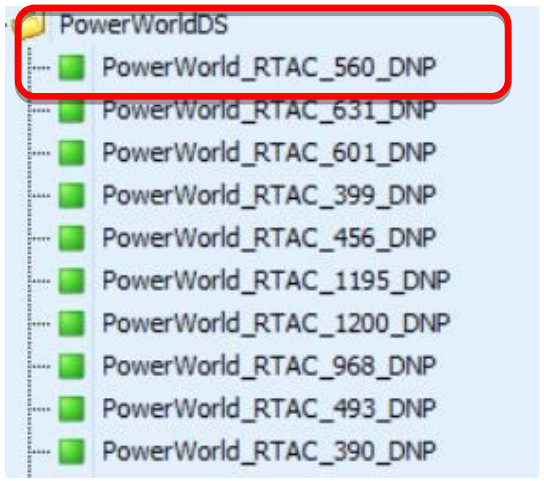


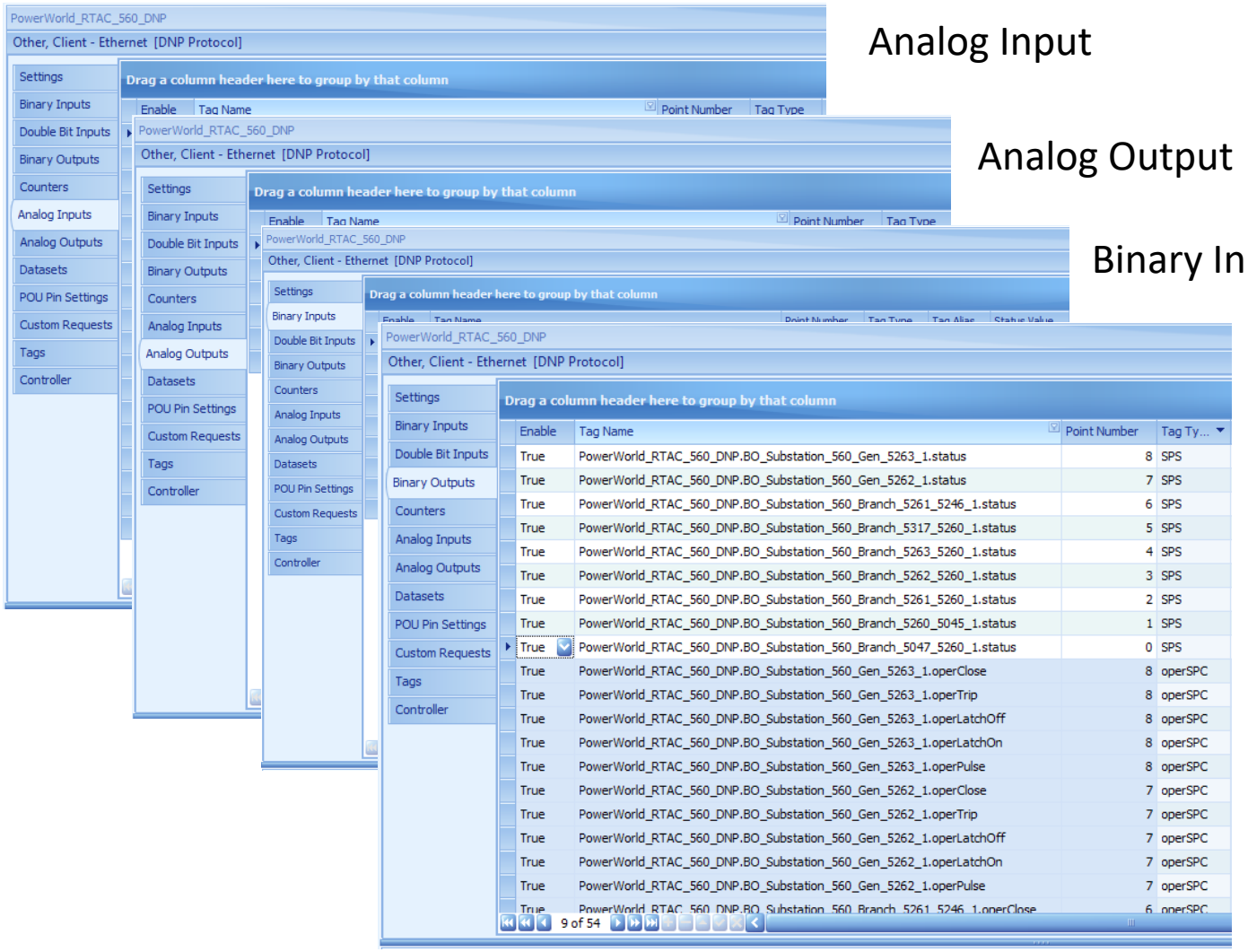
Substation 560 GLEN ROSE 1



Exemplar

TEXAS A&M UNIVERSITY
Engineering





Analog Input

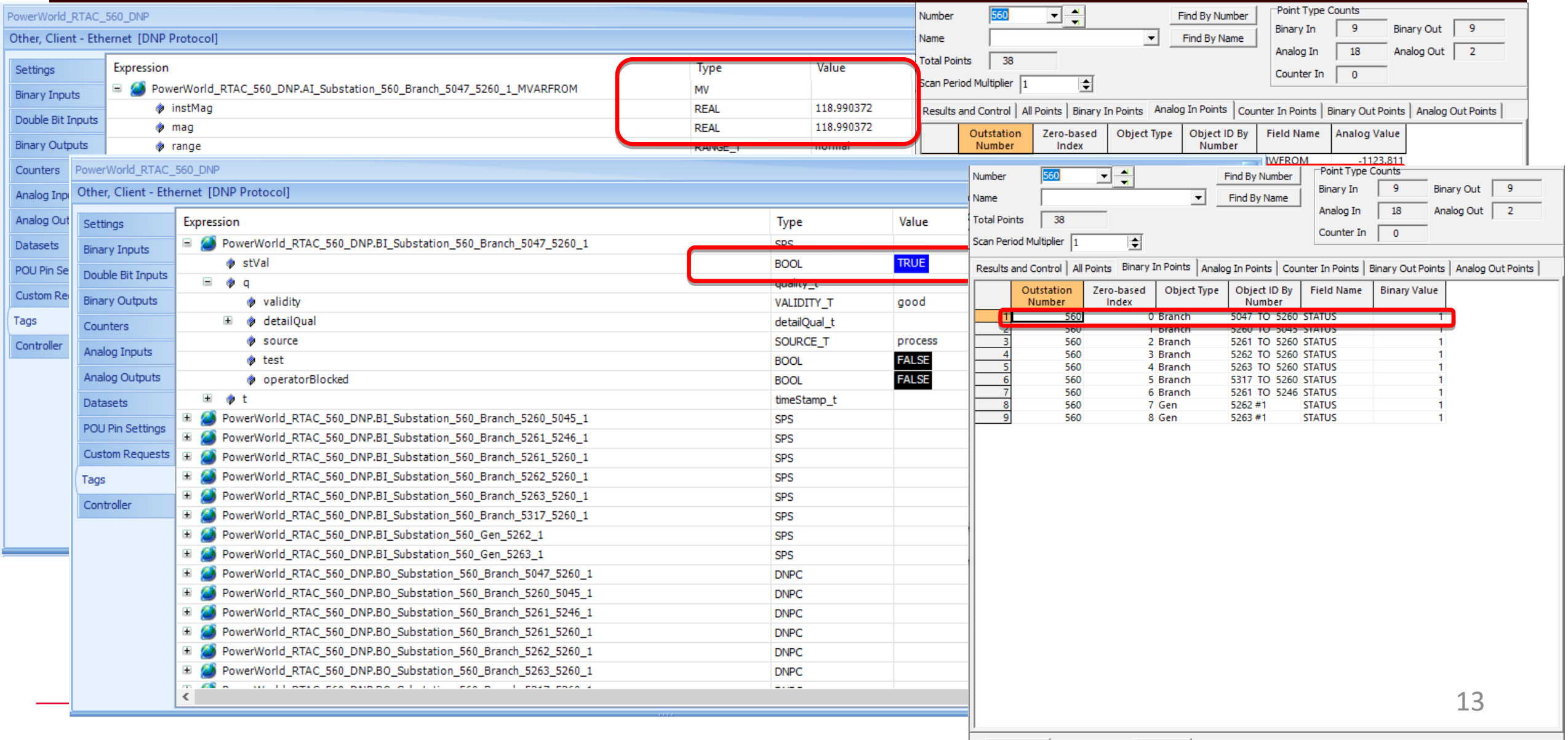
Analog Output

Binary Input

Binary Output

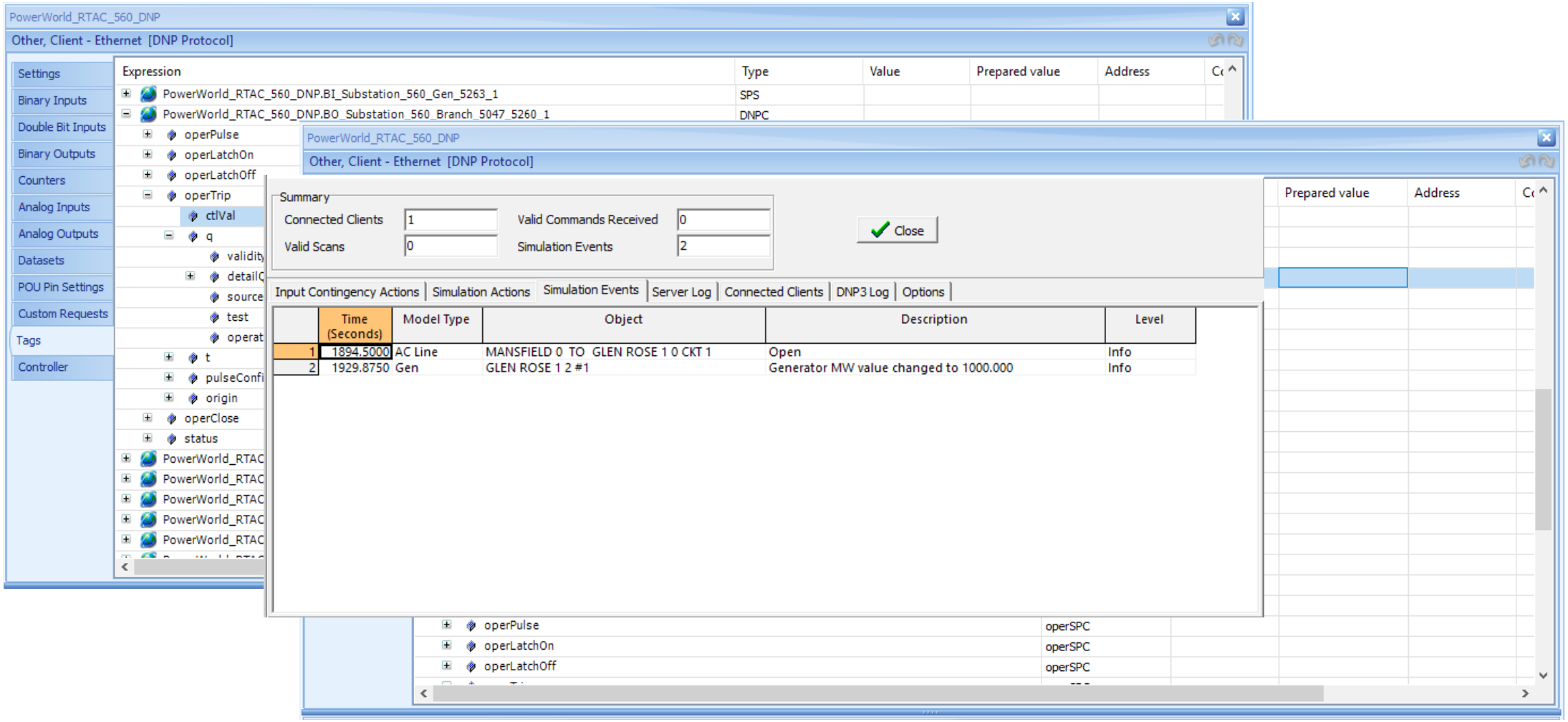
Data Collection

TEXAS A&M UNIVERSITY
Engineering



Control Implementation

TEXAS A&M UNIVERSITY
Engineering



Conclusion and Future Work

TEXAS A&M UNIVERSITY Engineering

This paper presents a cyber-physical testbed implementation of new DNP3 communication functionality of PWDS with SEL RTAC, mimicking the interactive control and response between real-time power system simulation and hardware devices in real world.

For future work, we can incorporate real or emulated communication network between PWDS and industrial hardware and software. Cyber intrusions can then be performed in the communication network, and the power system impacts can be observed in PWDS with real-time simulation; hardware devices can also detect such events with pre-defined alerts and control logic.

Acknowledgement

The work described in this paper was supported by funds from the US Department of Energy under award DE-OE0000895 and the National Science Foundation under Grant 1916142.

TEXAS A&M UNIVERSITY
Engineering

Thank you