U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management

Texas A&M Engineering Experiment Station (TEES)

Katherine Davis

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- To enhance the resilience of our critical energy infrastructure through the design of a next-generation cyber-physical energy management system that can prevent and detect malicious events through fusion of cyber and physical data and facilitate online control actions that couple cyber and physical spaces.

Schedule

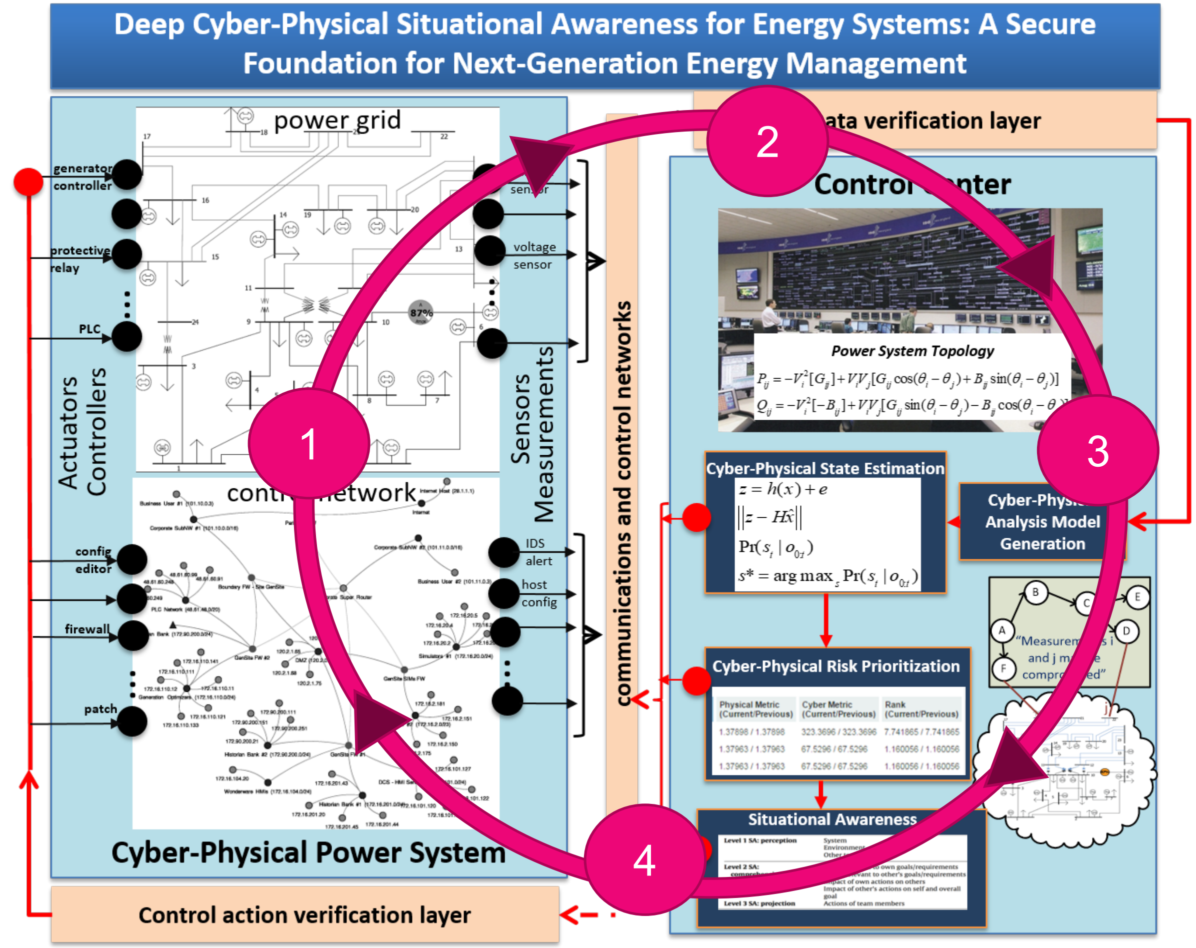
- **Start and end:** 10/01/18 to 12/31/21
  7/19: Kickoff Webex with DOE
- **Past and upcoming key dates:**
  11/19: Industry workshop & demo
  10/19: Publications & recorded demo
  2/20: Industry workshop & demo
  5/20: Approval for Phase 2
  11/20: Response publications & demo
  3/21: Vistra demonstration plan

Total Value of Award:	**$2,745,830**
Funds Expended to Date:	**33%**
Performer:	**Texas A&M Engineering Experiment Station (TEES)**
Partners:	**Rutgers, PNNL, Sandia, UIUC, & Vistra is demo partner**

Advancing the State of the Art (SOA)

CYPRES approach: Closing the loop with a unified model

1. **Model**
   - Represent, manage, and visualize the cyber physical model
2. **Monitor and Verify**
   - Fuse streaming inputs to the model
   - Estimate cyber-physical state
3. **Analysis**
   - Early attack detection
   - Cyber-physical risk analysis
   - Cyber-physical detection and situational awareness use cases
4. **Verify and Control**
   - Recommend cyber-physical actions
   - Mitigations, countermeasures



Cyber-Physical Resilient Energy Systems (CYPRES) https://cypres.engr.tamu.edu/

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Advancing the State of the Art (SOA)

- **State of the art:** Utility solutions siloed based on specific activities such as patching, detection, planning, operations, and protection.
- Difficult to broadly infer adversary actions targeting physical devices.
- **CYPRES research benefits:**
  1. Redesign of energy management systems to be intrinsically cyber-physical with analyses that enable the system to prevent, detect, and respond to events through fusion of cyber and physical data.
  2. Facilitating online and potentially automated control actions that couple cyber and physical control spaces.
  3. Facilitating how to integrate with existing tools to obtain broad sector adoption of such technology.

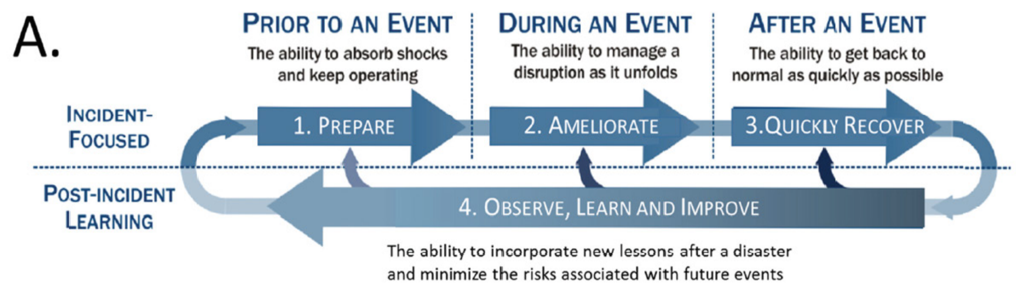
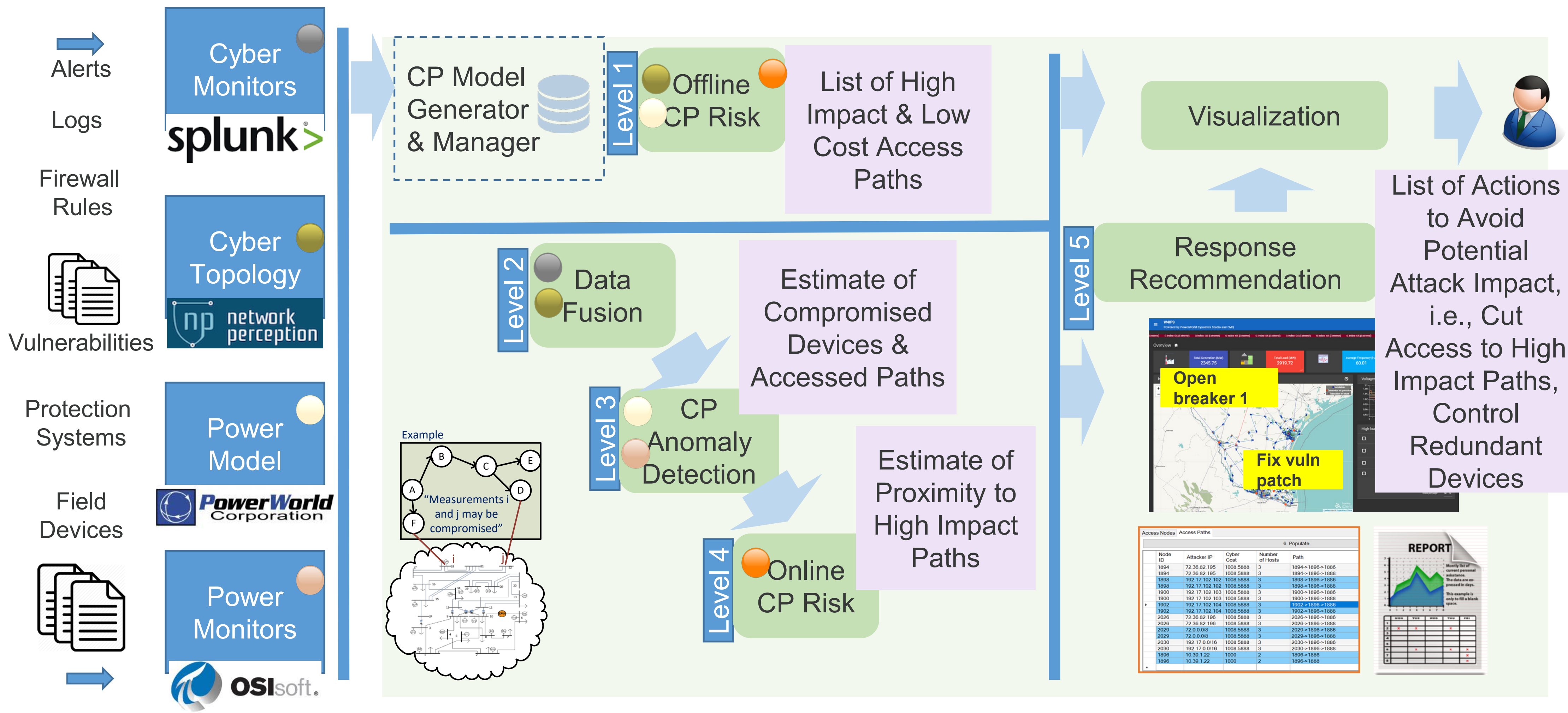


Fig. 1.2 (A), p. 36

The National Academies "Enhancing the Resilience of the Nation's Electricity System," July 2017.

CYPRES Modeling & Workflow



CYPRES Team & Industry

Kate Davis
Paula DeWitte
Tom Overbye
Ana Goulart
Hao Huang
Abhijeet Sahu
Amara Umunnakwe
Zeyu Mao

Patrick Wlazlo
Tasha Gaudet

Ben Stirling

Jim O'Rourke

Oladiran Obadina
Christine Hasha
Stefani Hobratsch

Robin Berthier

Walter Yamben

Edmond Rogers

Saman Zonouz

Shamina Hossain-McKenzie
Eric Vugrin

Contact: Kate Davis
katedavis@tamu.edu

James O'Brien
Mark Rice

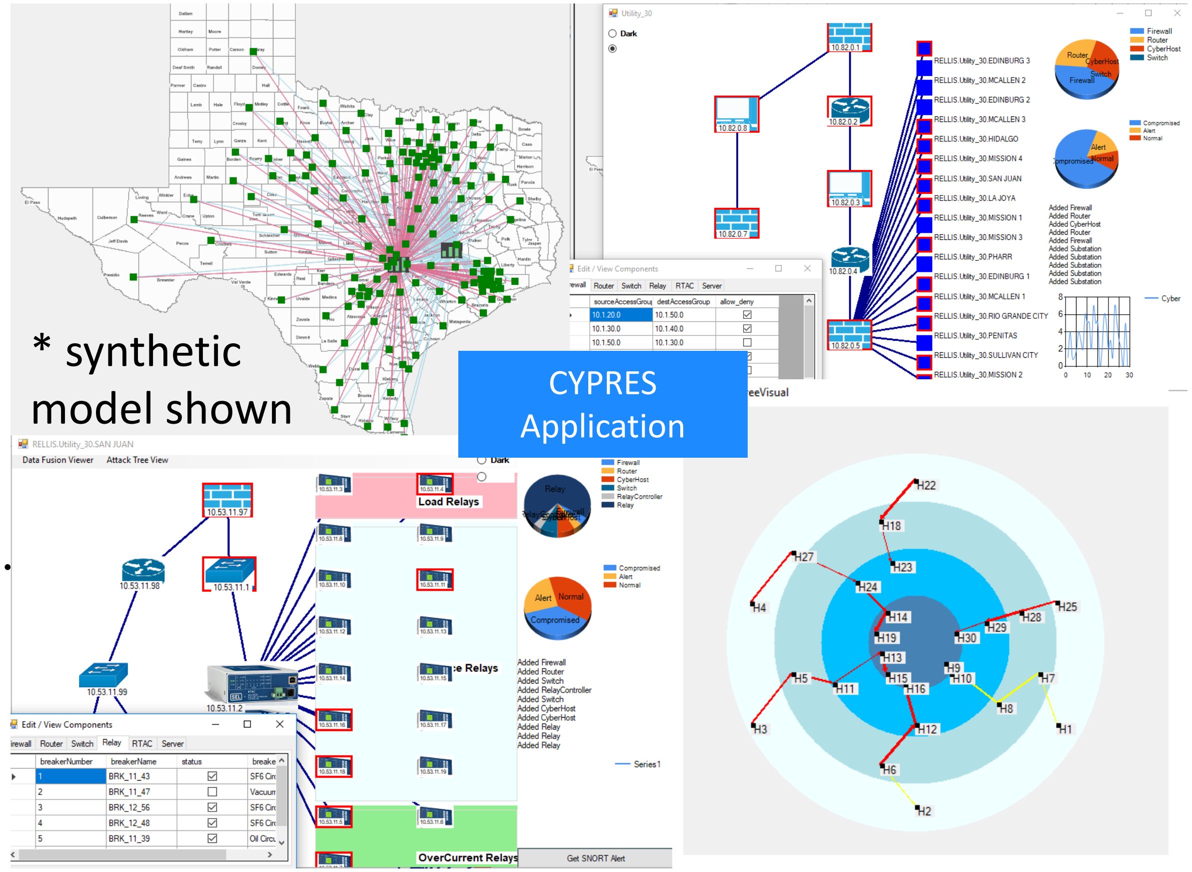
Cyber-Physical Resilient Energy Systems (CYPRES) https://cypres.engr.tamu.edu/

Progress to Date

Major Accomplishments

Model Development:

- Created cyber-physical 1250-substation power system case as our exemplar test system.
- Implemented exemplar system in RESLab that interfaces with CYPRES and is used for testing and evaluation.
- Developed and synthesized realistic use cases and scenarios in RESLab for CYPRES closing the loop from monitoring to analysis to control.



Technology Development & Validation

- Implemented major updates in our Resilient Energy Systems Lab (RESLab) testbed to enable the CYPRES technology to be developed, demonstrated, and evaluated.
- CYPRES was created to act as a next generation cyber-physical EMS/SCADA.

Progress to Date, continued

Major Accomplishments, continued

Technology Development & Validation

- CYPRES analyzes the system under intrusions that target multiple critical elements, using RESLab testbed with actual hardware, real-time power simulation, and network emulation.
- Algorithms being developed for cyber-physical data fusion, inferencing, and response.

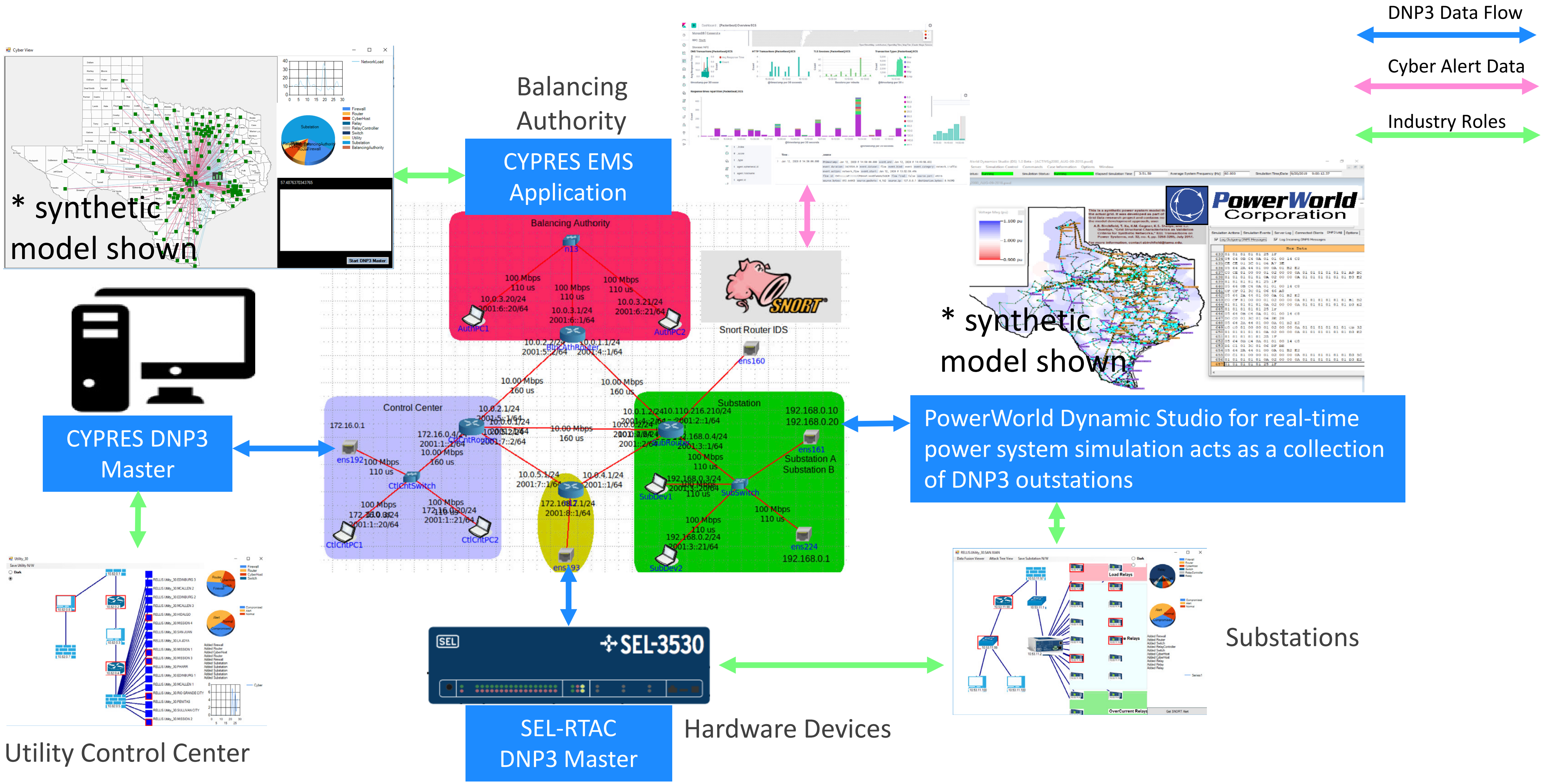
Texas A&M Testbed

- CYPRES reconfigures the network to mitigate cyber and physical contingencies discovered using graph theory combined with sensitivity analysis.
- Implemented and tested response of reconfigurable network solution with rerouting and firewall policy changes based on inferences from sensor data fusion.
- Incorporated firewall rules developed by our team with industry input that follow NERC standards and SCADA data pipeline into exemplar system model and RESLab.
- Updating synthetic cyber-physical grid models as we are validating them in RELab.

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Progress to Date, continued

CYPRES in RESLab Testbed: Status



Video, tutorials, & cases on our website:
https://cypres.engr.tamu.edu/

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- Targeted end users are asset owners and regional reliability organizations with a focus on transmission and generation.
- Security-oriented cyber-physical energy management application.
- Goal is to be easily deployable in utilities as a plugin, achieved by testing as a proof-of-concept in emulated utility in RESLab.
- Achieved by providing safe proving ground in RESLab with sharable test cases and engaging industry throughout project.
  - Collaborations including with Vistra, ERCOT CIPWG, Network Perception, OSIsoft, SEL, TDi.
  - Received utility data and developing demonstration plan.
  - Past and upcoming workshops and live/recorded demos to increase engagement with us.
  - Upcoming demos in October and November and creation of demo videos to share and post on website.

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Challenges to Success

Challenge 1: Scaling realistic cyber-physical grid emulation.

- Recognized inherent coupling of testbed, model, and analytics and created milestones that reflect and support agile development.
- Producing publications, algorithms, and software prototypes in agile manner.
- Research programmer support to help with daily testbed and code maintenance.
- Leveraging the expertise and prior experience of the team in the mathematical modeling of these systems combined with the team's real-world large-scale system expertise enable the development of new solutions to overcome these challenges.

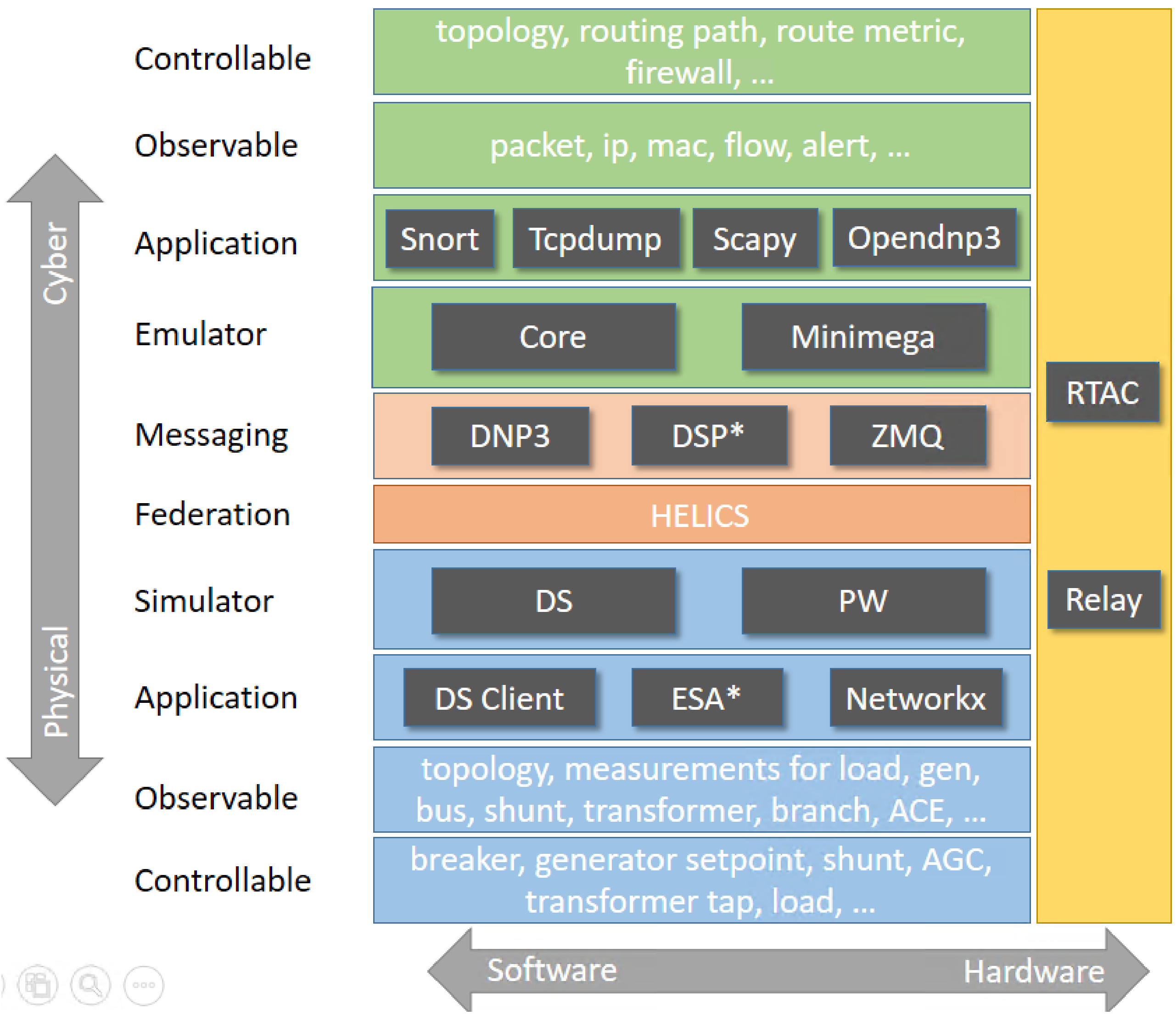
Challenge 2: Process delays particularly due to COVID-19.

- Frequent check-ins and reminders to university administration support staff.
- Working remotely with close team communication and regular check-in times.
- Success with accessing and working on RESLab testbed remotely.

Next Steps for this Project

Approach for the next year

- Testbed evaluation with large scale systems: scalability of emulations of raw traffic collection of ICS protocols for inference by emulating data I/O interface in substations in nodes of cyber emulator CORE making use of PowerWorld DS and HELICS.
- Demonstrate and validate with Vistra Energy.
- System integration with CYPRES modules, third party security solutions, and other applications.
- Evaluate and disseminate findings.



U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Project Publications to Date

[1] B. L. Thayer, Z. Mao, Y. Liu, K. Davis, T. Overbye "Easy SimAuto (ESA): A Python Package that Simplifies Interacting with PowerWorld Simulator," Journal of Open Source Software, 5(50), 2289, https://doi.org/10.21105/joss.02289

[2] A. Sahu, Z. Mao, K. Davis, and A. Goulart, "Data Processing and Model Selection for Machine Learning-based Network Intrusion Detection," IEEE workshop on Communication, Quality and Reliability (IEEE CQR 2020), May 2020.

[3] N. Gaudet, A. Sahu, A. Goulart, E. Rogers, and K. Davis, "Firewall Configuration and Path Analysis for Smart Grid Networks," IEEE workshop on Communication, Quality and Reliability (IEEE CQR 2020), May 2020.

[4] Z. Mao, H. Huang, K. Davis, "W4IPS: A Web-based Interactive Power System Simulation Environment For Power System Security Analysis," Hawaii International Conference on Science and Systems (HICSS), Jan. 2020.

[5] H. Huang, M. Kazerooni, S. Hossain-McKenzie, S. Etigowni, K. Davis, S. Zonouz, "Fast Generation Redispatch Techniques for Automated Remedial Action Schemes," IEEE 20th International Conference on Intelligent Systems Applications to Power Systems (ISAP), Dec. 2019.

[6] A. Sahu, H. Huang, K. Davis, S. Zonouz, "A Framework for Cyber-Physical Model Creation and Evaluation," IEEE 20th International Conference on Intelligent Systems Applications to Power Systems (ISAP), Dec. 2019.

[7] P. Wlazlo, K. Price, C. Verloz, A. Sahu, H. Huang, A. Goulart, K. Davis, S. Zonouz, "A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid," Principles, Systems and Applications of IP Telecommunications (IPTComm), Oct. 2019.

[8] A. Sahu, H. Huang, K. Davis, S. Zonouz, "SCORE: A Security-Oriented Cyber-Physical Optimal Response Engine," IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oct. 2019.