Network Function Insertion for Reliable and Secure Control Messaging over Commodity Transport

Nicholas Bastin, Chris Bronk, Wm. Arthur Conklin, and Deniz Gurkan

MOTIVATION

- SDN is a promising new networking paradigm that can offer unprecedented flexibility, visibility, and QoS in a network. The challenge is in demonstrating the delivery of these promises in actual control system networks used in critical infrastructures associated with energy delivery systems.

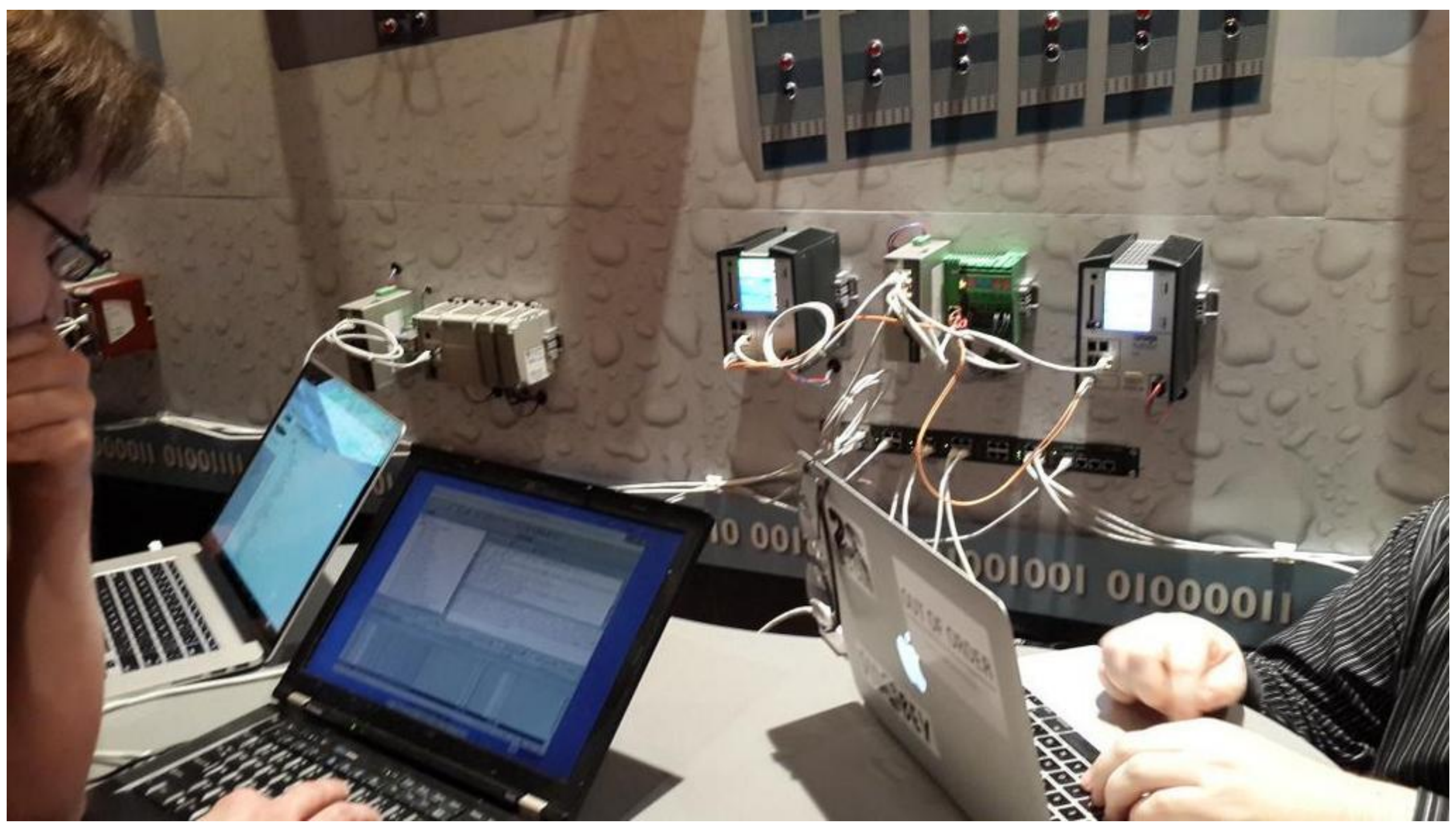
PROJECT GOALS

- Evaluate the application of software-defined networking (SDN) in control system networks.
  - What are opportunities for security function deployment via SDN in a control system network?
  - What are the operational limitations of using SDN in a control system network?
  - What are applicable metrics associated with SDN and control system networks?
- Design and develop a testbed that integrates simulations of both the cyber and physical infrastructure of control system networks.
  - Enclaved and non-enclaved designs.
  - Incorporation of VPN to third parties.
- Investigate the ability to engineer in resilience using SDN network function deployment.
  - Use testbed to explore the operational limitations and opportunities for resilience.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Can SDN be used to improve operational resilience of EDS through the control system network?
  - Model resilience system interactions with control system network.
- What applications are needed in SDN to deploy network functionality?
  - How can these applications impact system-level resilience?
  - Risk introduced by SDN vs. conventional networking.
- Can SDN enhance the ability to recover and maintain critical services?
  - Accidental failure scenarios.
  - Malicious attacks.
- Can SDN create a form of adversarial tolerance in a control system network?

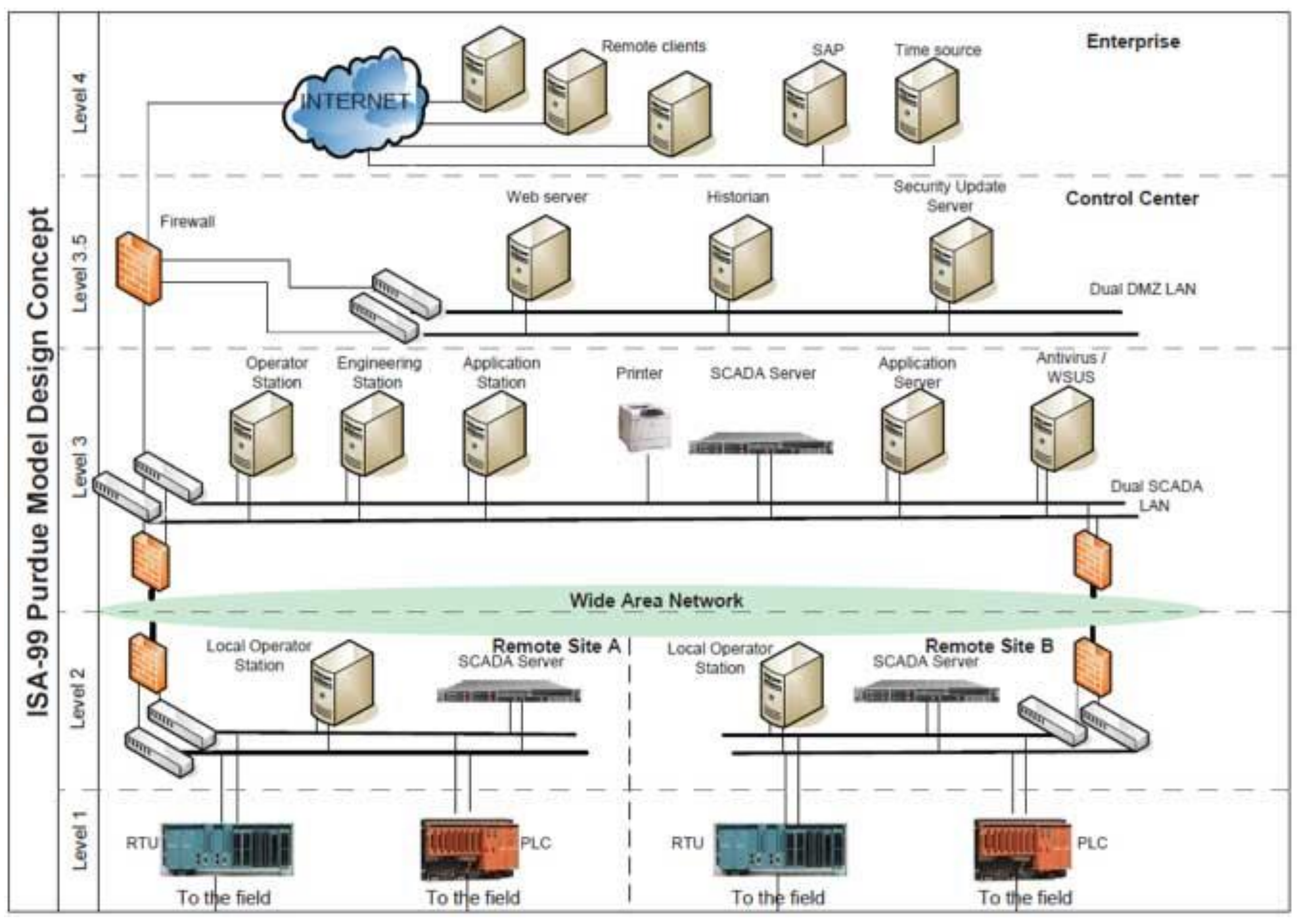
TESTBED ENVIRONMENT



- The building out of testbed experiments in the University of Houston lab offers students, academics, and industry opportunities to determine answers to real-world operational questions surrounding the configuration and use of control system network technology to improve security and resilience of the critical infrastructure elements employed in the field.
- The UH lab has an ongoing relationship with many energy firms and has served as a learning location in SCADA and Industrial Control Systems security efforts for several years. The expansion of this mission to examine resilience as driven by new technologies such as SDN builds upon that history.

RESEARCH PLAN

- Explore the operational use of SDN in levels 2 and 3 of ISA-99 Purdue model in an actual testbed.



- SDN is still 80% theory and 20% practice.
- Implement testbed using actual OpenFlow controllers.
- Testbed will enable directed studies using operational control systems to close the gap between theory and practice.
  - Applied research vs. theory.
  - Examine the opportunities and risks associated with operationalizing SDN in OT networks.
- Evaluate how SDN-managed network activities impact the operations of the control systems network.
  - Resilience.
  - Security.
  - Operational constraints and issues.
- Examine the operational characteristics of SDN technology in a live OT environment to develop an understanding of risk and resilience impacts.
- Open the testbed environment to student projects in classes to facilitate unguided discoveries.

BROADER IMPACT

- Resilience is an emergent property from system design, and SDN offers promising new opportunities in system designs.
- The control system networks used in energy delivery systems are different from standard IT system networks; understanding how SDN operates in this environment is crucial for future advancement of this technology and its promises.
- Understanding of the operational requirements to use SDN in OT networks is needed before adoption of new capabilities can be pursued.

INTERACTION WITH OTHER PROJECTS

- An equipment grant from the National Security Agency is supporting physical equipment in the building of testbeds using SDN.
- Internal funding sources have built Industrial Control System testbed apparatus.

FUTURE EFFORTS

- Use SDN and ICS testbed for research experiments to understand operational deployment issues:
  - Evaluate the deployment of network functions into ICS networks.
  - Evaluate operational options created through network function deployment to combat known attack tactics, techniques, and procedures (TTP).
  - Investigate the total system resiliency with and without SDN operations.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG
FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY