David M. Nicol

Information Trust Institute, University of Illinois

Cyber Resilient Energy Delivery Consortium (CREDC)

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

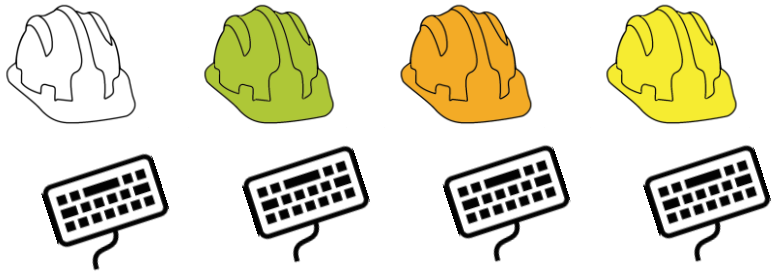
Summary: CREDC

Objective

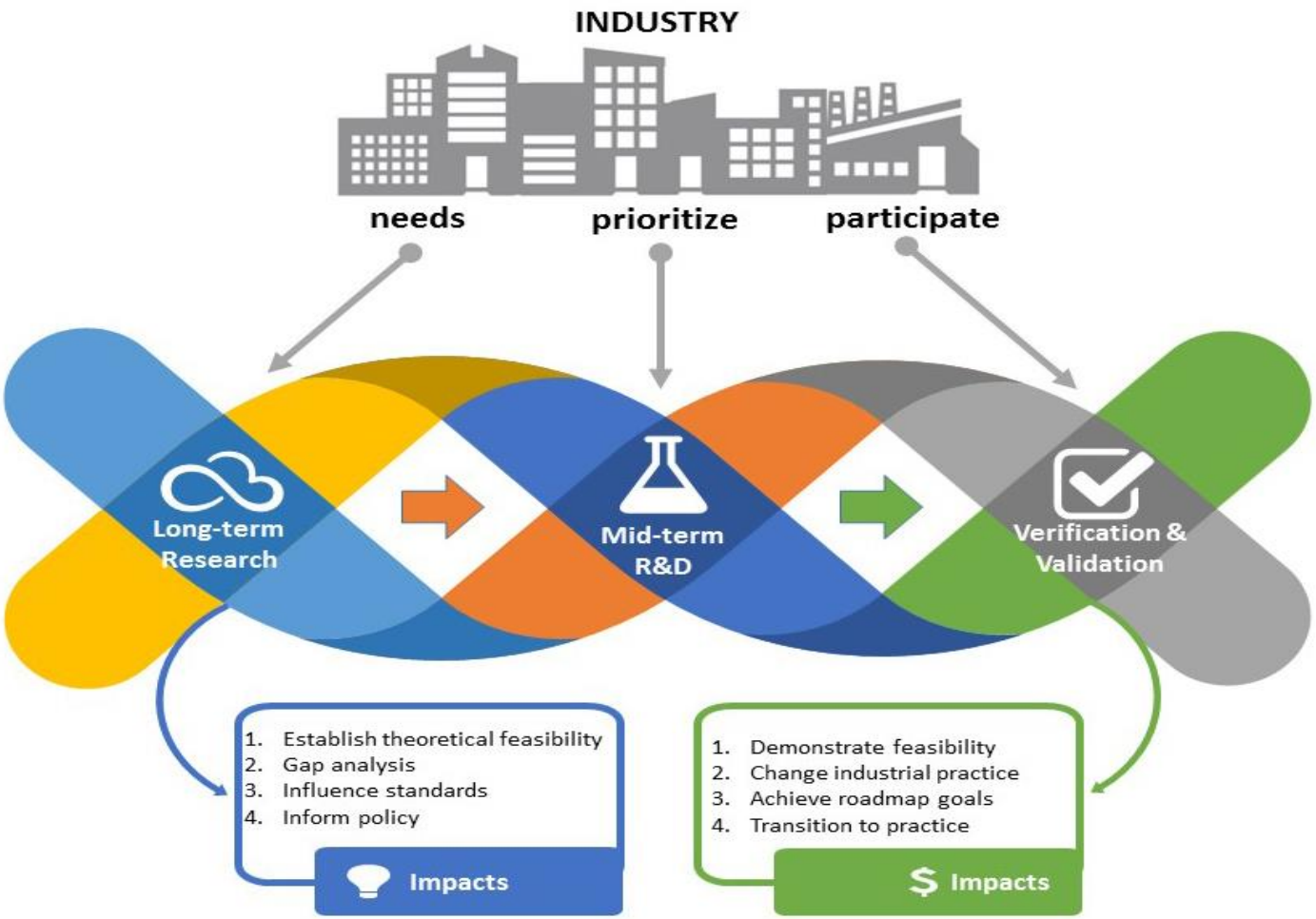
- Identify and perform cutting edge research and development whose results are actually used to increase cyber-resiliency of energy delivery systems.

Supporting Objectives

- Identify impediments and find highest impact *adoptable* solutions
- Develop, validate, verify high impact solutions, with industry
- Make solutions available
- Develop model of operation that is ultimately self-supporting



Approach


INDUSTRY
needs
prioritize
participate
Long-term Research
Mid-term R&D
Verification & Validation
1. Establish theoretical feasibility
2. Gap analysis
3. Influence standards
4. Inform policy
Impacts
1. Demonstrate feasibility
2. Change industrial practice
3. Achieve roadmap goals
4. Transition to practice
Impacts

Approach (2)

Over 30 Research activities ongoing

- Faculty lead + 1 to 3 students
- Industry involvement strongly encouraged
- Annual activity review against milestones, go/no go

Activities are long-term or mid-term

- Long-term: Addresses long-term issues that impact Energy Delivery Systems cyber security. Typically, research at TRL 2-4. Selected solutions may “graduate” to mid-term R&D.
- Mid-Term: Addresses problems with applied research, development, and testing that leads to technology transition, with one or more industry partners. TRL 4-6.

Cross-cutting efforts in V&V, industry engagement, and education/outreach related to new tools and technologies

CREDC Industrial Advisory Board

- **Mark Browning**, Exelon Utilities
- **Dennis Gammel**, Schweitzer Engineering Laboratories
- **Richard Jackson**, formerly with Chevron Corporation
- **Himanshu Khurana**, Honeywell Building Solutions
- **Blake Larsen**, Western Refining
- **Scott Mix**, North American Electric Reliability Corporation (NERC)
- **Paul Myrda**, Electric Power Research Institute (EPRI)
- **David Norton**, Federal Energy Regulatory Commission (FERC)
- **Kymie Tan**, Jet Propulsion Laboratory, Cyber Defense Engineering and Science Directorate
- **Zach Tudor**, Idaho National Laboratory

Summary: CREDC

Schedule

- Project Start: 10/1/2015
  Project End: 9/30/2020
- Year 1 Deliverables
  - Project Management Plan
  - IP Management Plan
  - Portfolio of selected research activities
  - Inter-Sector Mapping and Gap Analysis
  - Industry Workshop
  - Annual Reports
- Briefings/Presentations at industry and academic forums

Performer:	**University of Illinois at Urbana-Champaign**
Partners:	**9 academic; 2 national labs see list on next slide**
Federal Cost:	**$ 22,476,290**
Cost Share:	**$ 5,622,968**
Total Value of Award:	**$ 28,099,258**
Funds Expended as of 9/30/2016*:	**11.2%**

*Sub-invoices have 2-3 month delay in posting expenses. Contract with one academic partner not yet fully executed.

- What capability will result from this effort that will be transitioned to the energy sector?
  - Innovative methods and technology that enable EDS to continue critical operations
  - Education and workforce development that promotes an adoption of advanced cyber-technology for improved EDS resilience.

Summary: CREDC

CREDC Research Team

Advancing the State of the Art (SOA)

Current SOA:

- Vast improvement in EDS/ICS security over the last decade, but
- New challenges from expanding attack surfaces, cloud, IOT, DG, PHEV, and more.
- Evolving adversary, including nation-state (Ukraine)
- Increasing requirements for standardization, with a lack of supporting tools
- Increasing integration of renewable energy
- Increasingly stringent requirements for real-time operation over wide geographic areas

Advancing the State of the Art (SOA)

- **The diversity of research at various levels of maturity, the emphasis on industry involvement, and performing V&V in realistic environments support feasibility of our approach**
- **Overarching technical theme: Leverage system physics to reinforce cybersecurity**
  - Use cyber-physical models to enforce consistency of system state, physical measurements, and protocol traffic
  - Look-ahead impact assessment of control commands
- **End users benefit from technically sound, realistically validated solutions**
- **Cybersecurity of energy delivery systems is advanced by**
  - Efforts on multiple fronts, combining mid-term R&D with an “over the horizon” view to emerging threats,
  - Engagement with industry to prioritize research, validate research products

Challenges to Success

Challenge 1: Self-sustainability

- Stakeholder involvement in the form of paid subscription
  - Working on models that focus on value-add that leverages University basis
- Seek funding for synergistic R&D-V&V-Tech Transfer

Challenge 2*:* Sector acceptance of solutions

- Industry involvement at all stages
- Long term to mid-term to V&V pipeline
- IAB assures relevance of research

Progress to Date

Major Accomplishments

- Technical excellence: over 30 published papers, including some that won awards
- Kick-off Meeting, PMP, IP Plan
- Stakeholder engagement
  - Recruited Industry Advisory Board
  - CREDC Industry Workshop and Annual Review/Board Meeting – March 28-29, 2016
  - Engagement with companies such as NYPA, Reliability First, Riverside Public Utilities, Ameren, and others
  - To date, six paid memberships from leading EDS stakeholder organizations
- R&D Selection
  - First annual activity review process nearing completion

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Target audience: CREDC engages EDS asset owners as well as system and technology providers
- We have enjoyed success in getting access to vendor systems and stakeholder test environments
- We plan to gain industry acceptance by
  - Engagement of industry stakeholders at sector events, such as the recent InfraGard event promoting cybersecurity in the oil and gas (O&G) sector.
  - Recruitment of Industrial Advisory Board.
  - Ongoing engagement with leading utilities and equipment providers, many of whom donate equipment for CREDC testbeds and provide access to their own test environments.

Next Steps for this Project

Approach for the next year

- **Emphasize technical research excellence**
- **Complete activity review process**
- **Continued focus on EDS sector outreach**
  - 2017 Industry Workshop and Annual Review
  - Present CREDC at EDS and particularly O&G industry events
- **Increase industry involvement across the research portfolio**
- **Increase roster of paid industry memberships**
- **Workforce development: 2017 Summer Training Program**

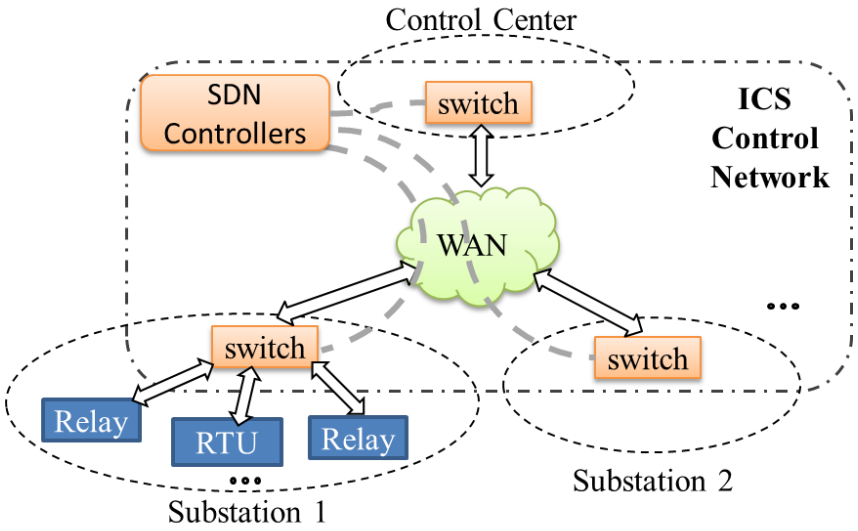
Technology Highlights

SDN in EDS

Software Defined Networking (SDN) is an example of a disruptive technology with benefits and risks for EDS.

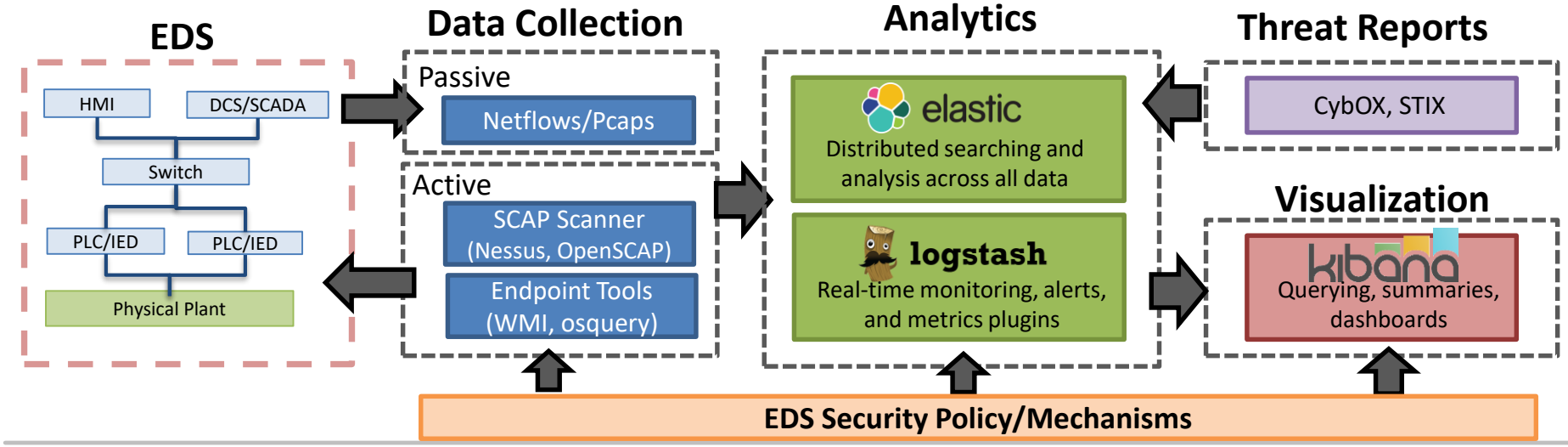
SDN as an *agile defense*:

- Use SDN to dynamically alter connectivity
- Use SDN controller to issue decoy measurements on behalf of "off-line" devices, disrupting adversary's ability to design effective attack strategy
- No modifications of the grid physical infrastructure, e.g., EMS in control centers
- No modifications of backbone wide area networks



Continuous Monitoring in EDS

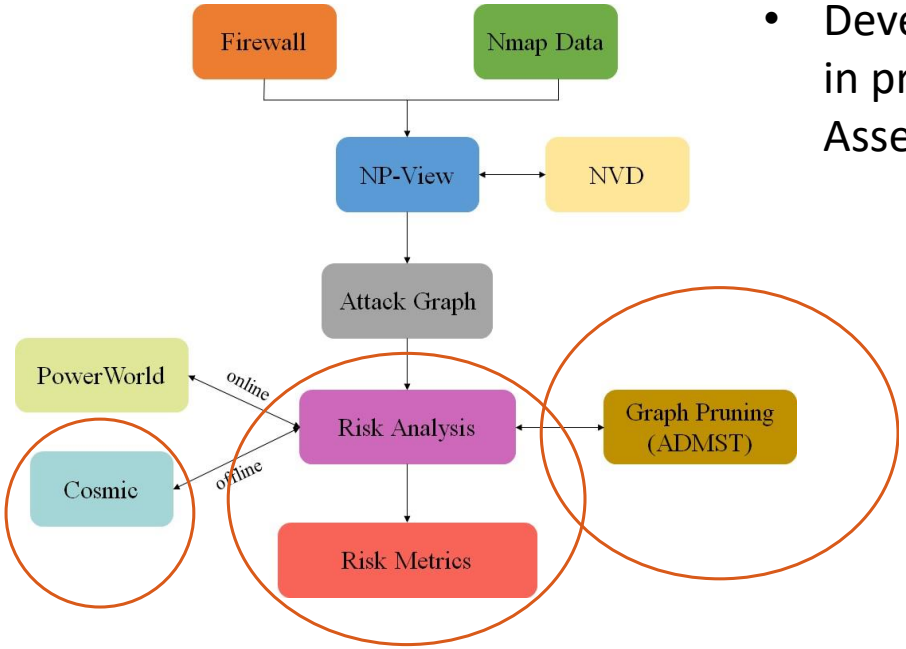
- Address roadmap requirement for “tools for real-time security state monitoring”
- Identify monitoring techniques that do not adversely impact EDS
- Identify analytics to process the collected data, and support the evaluation of EDS security policies and mechanisms
- Develop scalable attack detection techniques
- Implement the proposed techniques on a distributed software platform to automate the collection and analysis



Cyber-physical Modeling and Analysis for Cyber-induced Cascading Failure Risk Assessment

Research Goal

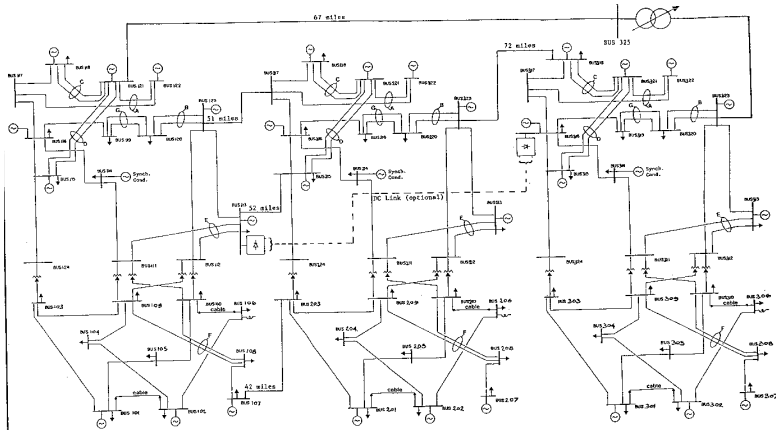
Modeling and analysis methodology for cyber-physical dependencies in order to assess the risk of *cyber-attack* induced *cascading failures*.



Solution Approach and Research Results

Accurate cyber-physical models to enable mapping of cyber-assets involved in cascading scenarios. Cyber-physical metrics that help in comparing the risk exposure. Analysis algorithms to compute pathways to reach target cyber-assets.

- Developed cyber-physical model for IEEE RTS-96 test system.
- Developed preliminary cyber-physical metrics for use in previously developed Cyber-Physical Security Assessment (CyPSA) framework.



Cyber-Physical Intrusion Detection Incorporating µPMU Measurements

Anna Scaglione, Mahdi Jamai, Reinhard Gentz — *Arizona State University (CREDC)*

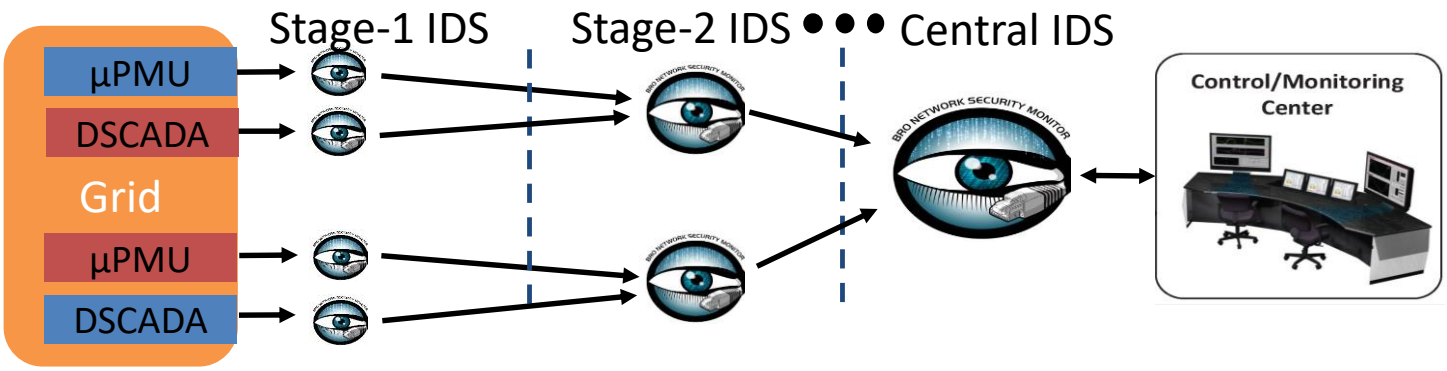
Collaborators:

Sean Peisert, Emma Stewart, Chuck McParland — *Lawrence Berkeley National Lab*

Alex McEachern — *Power Standards Lab*

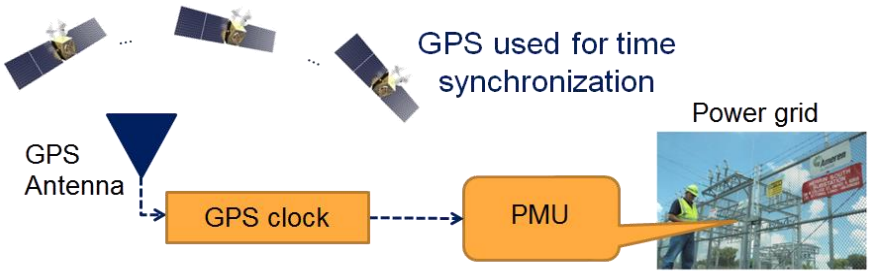
Objective: Developing hierarchical µPMU-based intrusion detection system (IDS) under BRO security framework that binds:

- **Passive DSCADA system state observations,**
- **Results leveraged from µPMU data analysis tools, and**
- **Knowledge about the circuit configuration and grid protection and operation.**
- **Packet flow inconsistent with µPMU data analysis may indicate ongoing attack.**
- **Engagement with Riverside Public Utility**

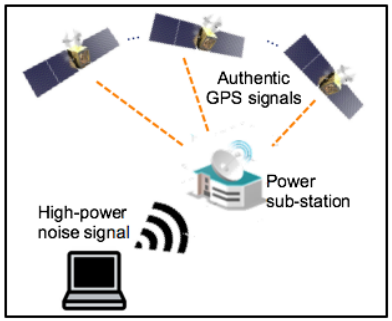


Robust GPS Timing for Wide Area Grid Monitoring

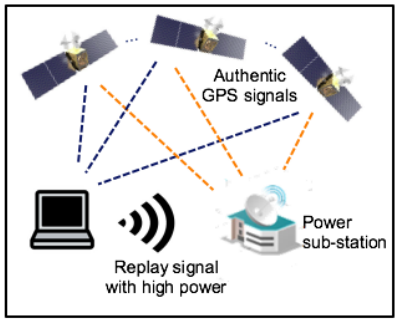
MOTIVATION



- Wide-area measurements depend on GPS clocks.
- GPS signals are vulnerable, because GPS signals are unencrypted and weak.



Jamming: Makes timing unavailable for PMUs



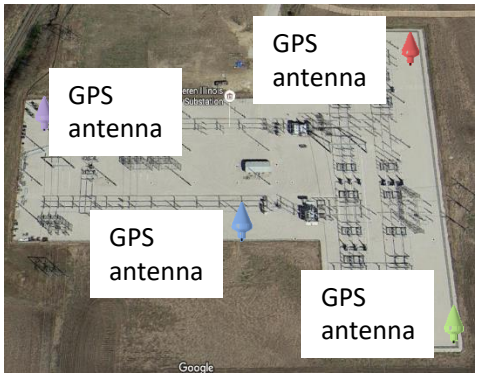
Meaconing: Mislead PMU with wrong time

OBJECTIVE

- Investigate robust GPS timing algorithms to harden PMUs against jamming and spoofing
- Develop a hardware-based testbed to demonstrate PMU vulnerabilities and mitigation measures.
- Verify and Validate (V&V) our robust GPS algorithms

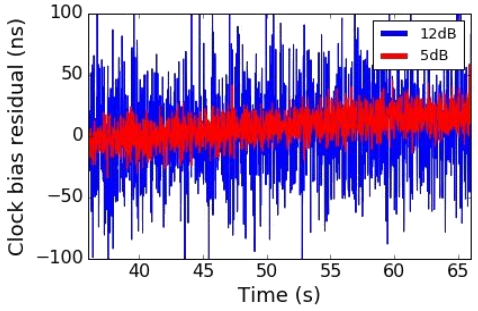
OUR APPROACH

- Multiple receiver
  - Geographical diversity
- Position-aided
  - Static receiver location
- Advanced algorithm
  - Direct Time Estimation
- Triggered by the same external clock

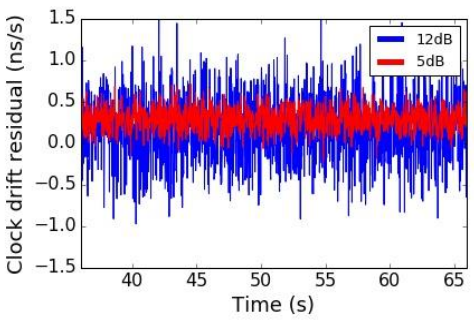


PRELIMINARY RESULTS

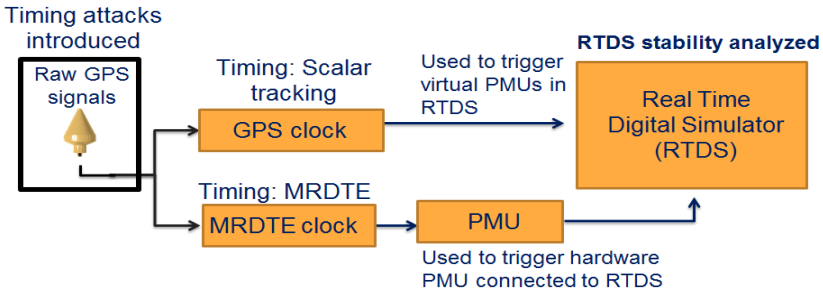
Clock Bias



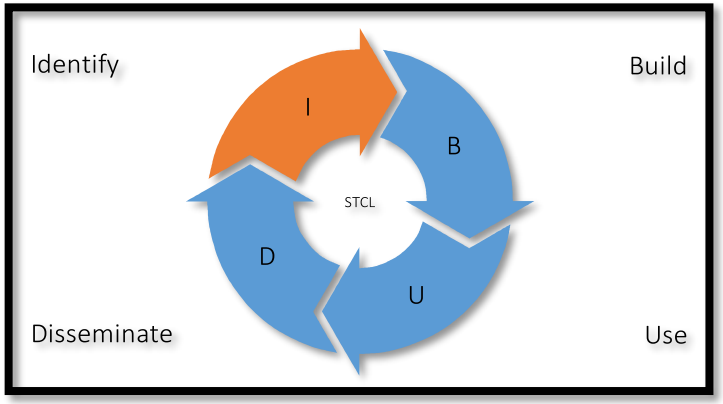
Clock drift

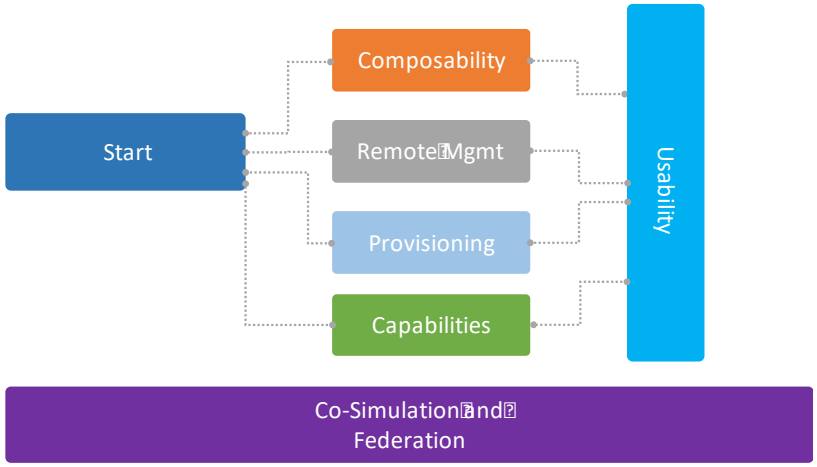


V&V PLAN



Verification and Validation





- In progress activities
  - Remote Management
    - New remote capabilities and management
  - Provisioning
    - New provisioning system being deployed
- Undercurrents
  - Composability
    - Layouts, Configurations, and Tools all being implemented to be modular
  - Capabilities
    - Bringing in massive new capabilities for the electric grid, and will be phasing in other energy delivery components as needed
  - Usability
    - New provisioning and toolsets will drastically improve usability
  - Co-Simulation
    - Progress being made on the science behind this and the use-case motivations

Research → Verify → Refine → Validate & Transition

Upcoming Events

Seminar Series

Upcoming Seminars

- Feb. 3, 2017: Bill Lawrence, E-ISAC
- Mar. 3, 2017: Blake Larsen, Western Refining
- April 7, 2017: Michael M. Johnson, U.S. Department of Energy

Past Seminars

- Dec. 2, 2016: Jonathon Monken, PJM Interconnection
- Nov. 7, 2016: Nancy Leveson, MIT
- June 24, 2016: Carol Hawk & DOE National Labs
- Feb. 12, 2016: David M. Nicol, CREDC

Industry Workshop

When and Where?

- First annual: March 28-29, 2016 in Champaign, Illinois
- **Next:** March 27-29, 2017 in Tempe, Arizona

Workshop Format

- Invited speakers on topics important to EDS stakeholders
  - 2016 event featured an invited talk on the Ukraine incident
- Featured research
  - Lightning talks
  - Poster session
- Breakout panel discussions
  - 2016: Identification of critical sector needs in several topic areas
  - Breakout discussion summary available at http://cred-c.org/iw2016/archives/

Summer Training

When and Where?

- June 11-17, St. Charles, Illinois (Chicago area)
- Held every two years

Program Format

- An intensive, engaging, and value-packed week of topics and workforce development activities focused on cybersecurity and resiliency of energy delivery systems for the electric power and oil & gas industries
- Mix of presentations with intensive hands-on exercises

Summary

CREDC is advancing Roadmap objectives

- **Technical excellence**
  - Balanced research portfolio
  - Research pipeline leading to sector impact and deployed solutions
- **Sector engagement**
  - Recruited IAB
  - CREDC hosts an annual industry workshop
  - Active outreach at EDS sector events
- **Workforce development**
  - Summer 2017 training
  - Educational outreach