Synchrophasor Data Quality

Website: http://cred-c.org/researchactivity/synchdataq

Researchers (Illinois): Peter Sauer, Karl Reinhard, John Lee, Grace Rogers

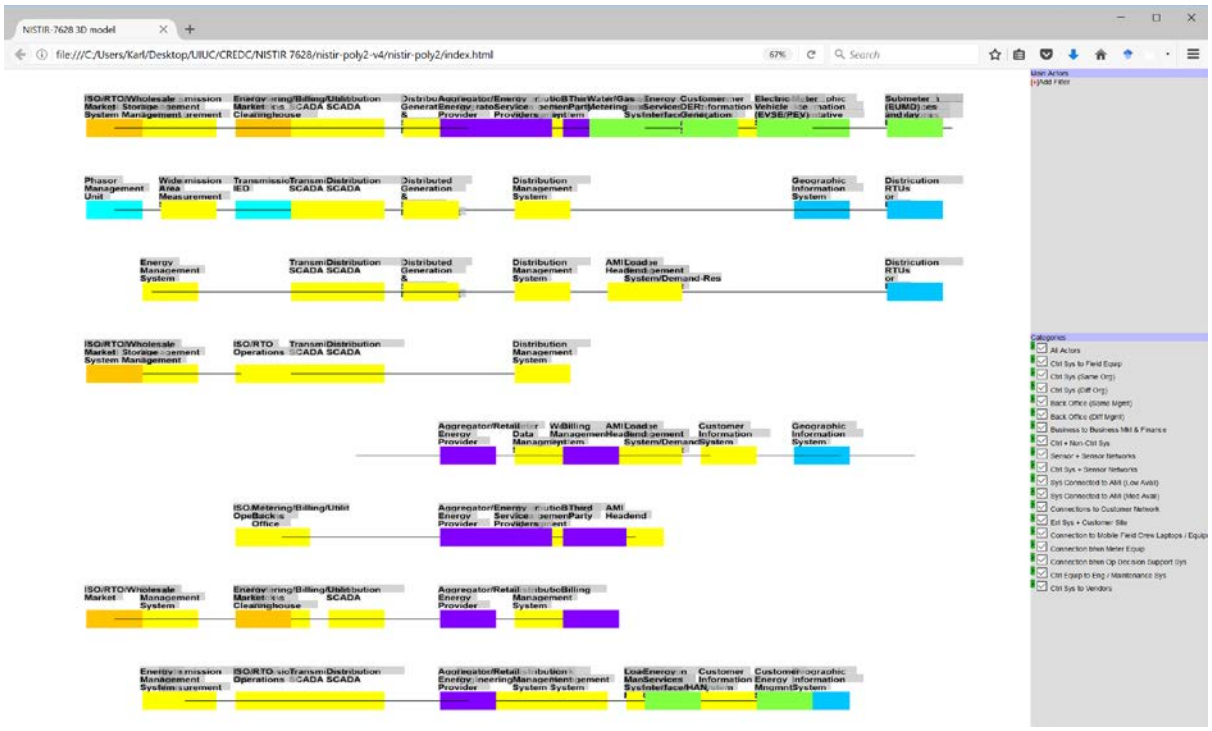
Industry Collaboration:

- Kaedago, Inc.
- EPRI
- PNNL
- American Transmission Company (ATC)

Description of research activity: Our research objective is to continue development of a flexible, adaptive 3D visualization tool that changes the paradigm for learning about and understanding cyber security structure and requirements outlined in NISTIR 7628 and NESCOR "Failure Scenarios".

This effort is an extension of research and tool development carried forward from the TCIPG project. The current tool version is web-implemented using HTLM-5. The tool provides a 3D representation of NISTIR requirements with the players in each logical interface category or architecturally significant use case depicted on a plane; the planes are vertically stacked. With the computer mouse and on-screen menus, the user narrows displayed NISTIR 7628 information to focus upon specific actors and their relationships. The user can

- Zoom, pan, and rotate the 3D representation for readability.
- Adjust the distance between layers for readability
- Select any combination of layers and actors to be displayed (filtering unneeded information).
- View hyperlinked descriptive data by selecting an actor with the cursor.
- Open multiple descriptive data windows
- Annotate actor descriptive data with relevant notes
- Add additional graphic objects and descriptive data to adapt the tool to organizationally specific cyber security visualization requirements.



3D Visualization of NISTIR 7628 cyber security logical interfaces and architecturally significant use cases depicted as model layers. Actor arrangement and coloring are consistent with NISTIR 7628; actors in multiple layers are aligned vertically.

The tool is being developed to allow automatic ingestion of complex tabular data (such as table data in NISTIR 7628) to accommodate updates as security requirements and concepts evolve with time. This includes anticipated future extension to integrate NESCOR "Failure Scenarios".

The need for a 3-D tool for visualizing complex relationships between many system players is not unique to NISTIR 7628. The tool is being developed with the intent to enable straight forward adaption to similar visualization needs, e.g. cyber requirements for the oil and natural gas energy delivery system.

We also envision and EDS organization adapting the tool's information content to meet their unique system architecture and needs.

The tool will accelerate assembling data and information to facilitate synthesizing the complex ideas and relationships necessary to improve cyber security. This innovative approach to visualizing NISTIR 7628 and NISTIR Special Publication (SP) 1108 (release 3) content will provide an adaptable tool that can be tailored to educate the entire EDS work force.

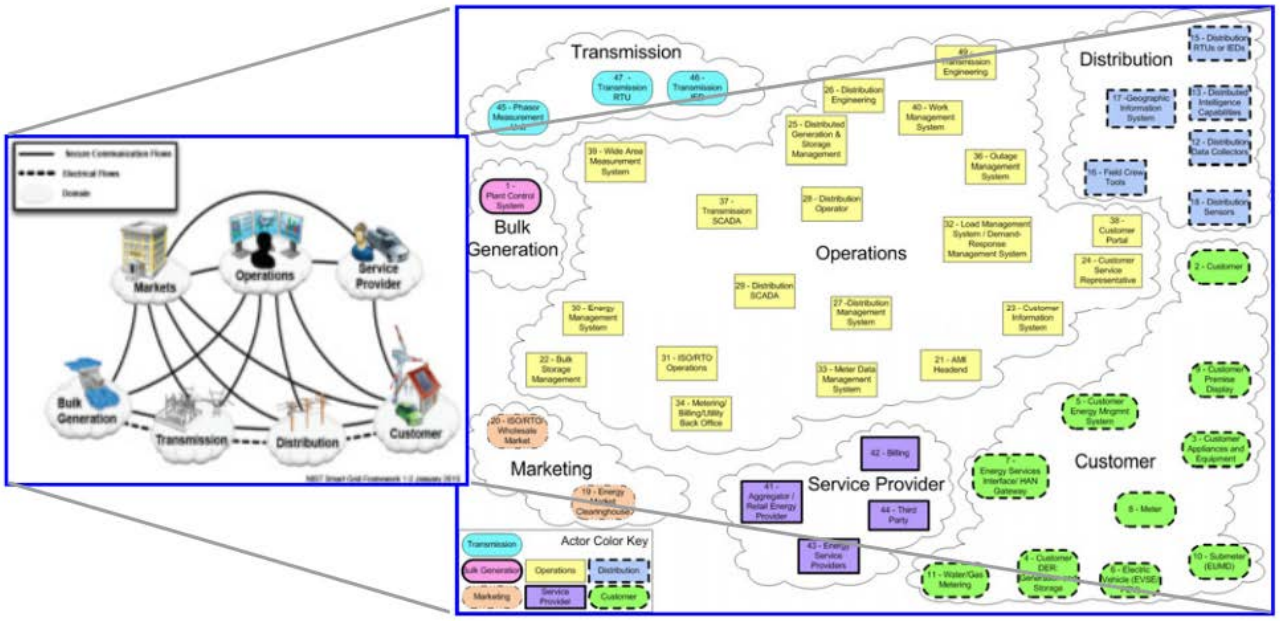
This activity is scheduled to complete by September 30, 2017.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This research activity is most closely aligned with the "Build a Culture of Security" goal. This activity seeks to deliver a tool that supports EDS workforce knowledge and understanding of system cyber security requirements. Improved workforce knowledge and understanding support improved performance within the other roadmap goals and outreach educating interested people outside the EDS sector.

Summary of EDS gap analysis: DOE's Roadmap to Achieve Energy Delivery Systems (2011) explicitly identifies knowledgeable people, who understand and appreciate energy delivery system (EDS) security requirements and risks as

vital to sustaining critical power system functions over the long term. An implicit barrier to educating the diverse EDS workforce is the extraordinary effort individual effort necessary to make sense of the power system cyber security framework detailed in NISTIR 7628, *Guidelines for Smart Cyber Security* and the derivative NESCOR report "Electric Sector Failure Scenarios and Impact Analyses."

Full EDS gap analysis: DOE's Roadmap to Achieve Energy Delivery Systems (2011) explicitly identifies knowledgeable people who understand and appreciate energy delivery system (EDS) security requirements and risks as vital to sustaining critical power system functions over the long term. An implicit barrier to educating the EDS workforce (with diverse needs) is the extraordinary effort individual effort necessary to make sense power system cyber security.



NISTIR 7628 mapping of seven Smart Grid domains to 46 actors; not depicted are the 130 functional interactions between the actors.

In August of 2010, the National Institute of Standards and Technology (NIST) Computer Security Division published NISTIR 7628, *Guidelines for Smart Cyber Security*, which expands upon the Smart Grid cyber security principles published in NIST's Special Publication (SP) 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards* (2010; updated release 3.0 Sep '14).

NISTIR 7628 conceptualizes the power grid as being composed of the seven domains, which are defined as a high-level grouping of organizations, buildings, individuals, systems, and devices with similar objectives or functions; the seven named domains are marketing, operations, service provider, bulk generation, transmission, distribution, and customer. NISTIR 7628 identifies 46 actors, which are defined as devices, systems, or programs that make decisions and exchange the information necessary for the Smart Grid to function. NISTIR 7628 further identifies 130 logical interface sets between actors that describe that describe interactions inherent to the operating Smart Grid.

NISTIR also identifies 10 architecturally significant use cases that involve different actor and logical interface sets: Advanced Metering Infrastructure (AMI), Demand Response, Customer Interfaces, Electricity Market, Distribution Automation, Plug-in Hybrid Electric Vehicles (PHEV), Distributed Resources, Transmission Resources, Regional Transmission Operations / Independent System Operators (RTO/ISO), Operations, and Asset Management.

In September 2013, the Electric Power Research Institute (EPRI) published the National Electric Sector Cybersecurity Organization Resource (NESCOR) report "Electric Sector Failure Scenarios and Impact Analyses" based upon the work of NESCOR Technical Working Group 1 (TWG1) (hereafter "Failure Scenarios"). This report supports NISTIR 7628 guidelines by detailing failure scenarios organized in six categories based upon NISTIR SP 1108 categories including (1) Advanced

Metering Infrastructure (AMI), (2) Distributed Energy Resources (DER), (3) WAMPAC (Wide Area Monitoring, Protection, and Control), (4) Electric Transportation (ET), (5) Demand Response (DR), (6) Distribution Grid Management (DGM), and a seventh cross-cutting category "Generic".

Making sense of complex Smart Grid security requirements is both daunting and time consuming – even for those having a professional interest. NISTIR 7628 details Smart Grid cyber security requirements in more than 30 figures depicting complex interactions and detailed tabular information spanning more than 100 pages. The entire NISTIR 7628 document spans more than 600 pages and is densely packed with technical information drawn from multiple disciplines, which to many readers is difficult to broadly conceptualize and apply. There is a need for a tool to facilitate visualization and organization of these complex requirements.

Bibliography:

Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," U.S. Department of Energy, 2011

Harvey, Matthew, Daniel Long, and Karl Reinhard. "Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security." *Power and Energy Conference at Illinois (PECI), 2014*. IEEE, 2014**.**

National Electric Sector Cybersecurity Organization Resource, "Electric sector failure scenarios and impact analyses," Electric Power Research Institute, Tech. Rep. 1.0, Sep. 2013.

Smart Grid Interoperability Panel Cyber Security Working Group. "NISTIR 7628-Guidelines for Smart Grid Cyber Security vol. 1-3.", 2010.

Smart Grid Interoperability Panel Cyber Security Working Group. "NISTIR 7628-Guidelines for Smart Grid Cyber Security introduction", 2010.