Paul Skare for
Eric Andersen
Pacific Northwest
National Laboratory

Improving Situation Awareness/Assessment for Utility Operators and Cybersecurity Professionals

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

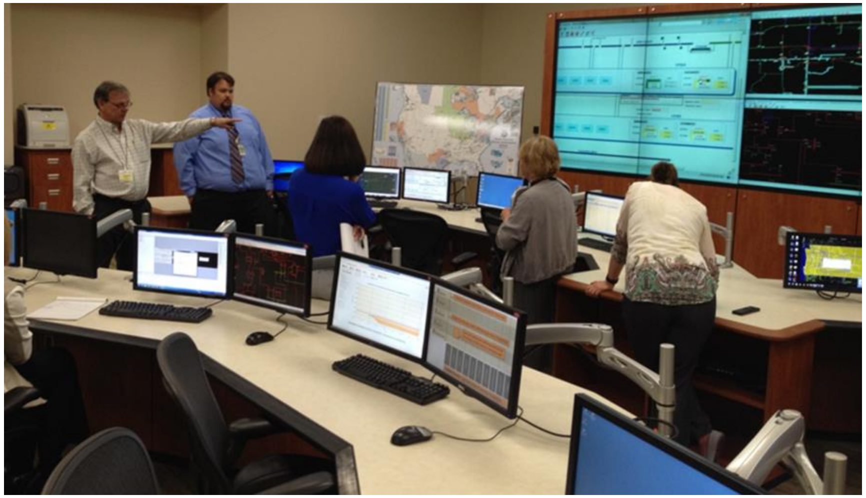
Summary: Project Title

Objective

- Develop visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situations, enabling them to maintain situation awareness during unfolding events.

Schedule

- 2015-2018
- Initiate utility observations – 8/30/2105
- Initial display concepts designed – 10/3/2016



Performer:	Pacific NW National Laboratory
Partners:	Idaho National Laboratory Western Area Power Administration General Electric (Alstom Grid)
Federal Cost:	$1.98M
Cost Share:	None
Total Value of Award:	$1.98M
Funds Expended to Date:	50%

Advancing the State of the Art (SOA)

- Cybersecurity visualizations for control rooms and network security operations centers are being developed to aid decision making with increasing volumes of operations data. Some work has been done in the past in this area, but the tools developed have seen little use in utility operations.
- Our approach is different because we are engaging the primary stakeholders, the control room operators and cybersecurity professionals, as part of our iterative based design process which includes human cognitive analysis.
- By engaging our primary stakeholders, we build credibility, and ensure that our design is robust, but more importantly, that it will work in their environment, and that it will meet their needs.
- Utilities will benefit from having a visualization tool/s to aid and speed decision making when faced with cybersecurity concerns.

Challenges to Success

Challenge 1- OT Cyber Data: who owns it, who cares?

- Working with our stakeholders to better understand what information is monitored, by whom, and who owns the actions – all within the utility.

Challenge 2 – Understand the communication pathways for cyber information

- Conducting analyses to determine how to facilitate communications between appropriate parties so a shared awareness of the situation is quickly reached.

Challenge 3 – Designing useful visualizations

- Using the iterative design process with our stakeholders to understand the context in which the information needs to be displayed so a rapid, optimal decision is made by the appropriate personnel.

Progress to Date

Major Accomplishments

- Assembled a project advisory group of utility cybersecurity experts.
- Observations/Interviews/Surveys have been conducted with success.
- WAPA allowed the research team to observe while participating in GridEx III.
- Cybersecurity workshop conducted at the Alstom Grid North American User’s Group conference with wide utility participation.
- First wireframe visualizations were designed.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

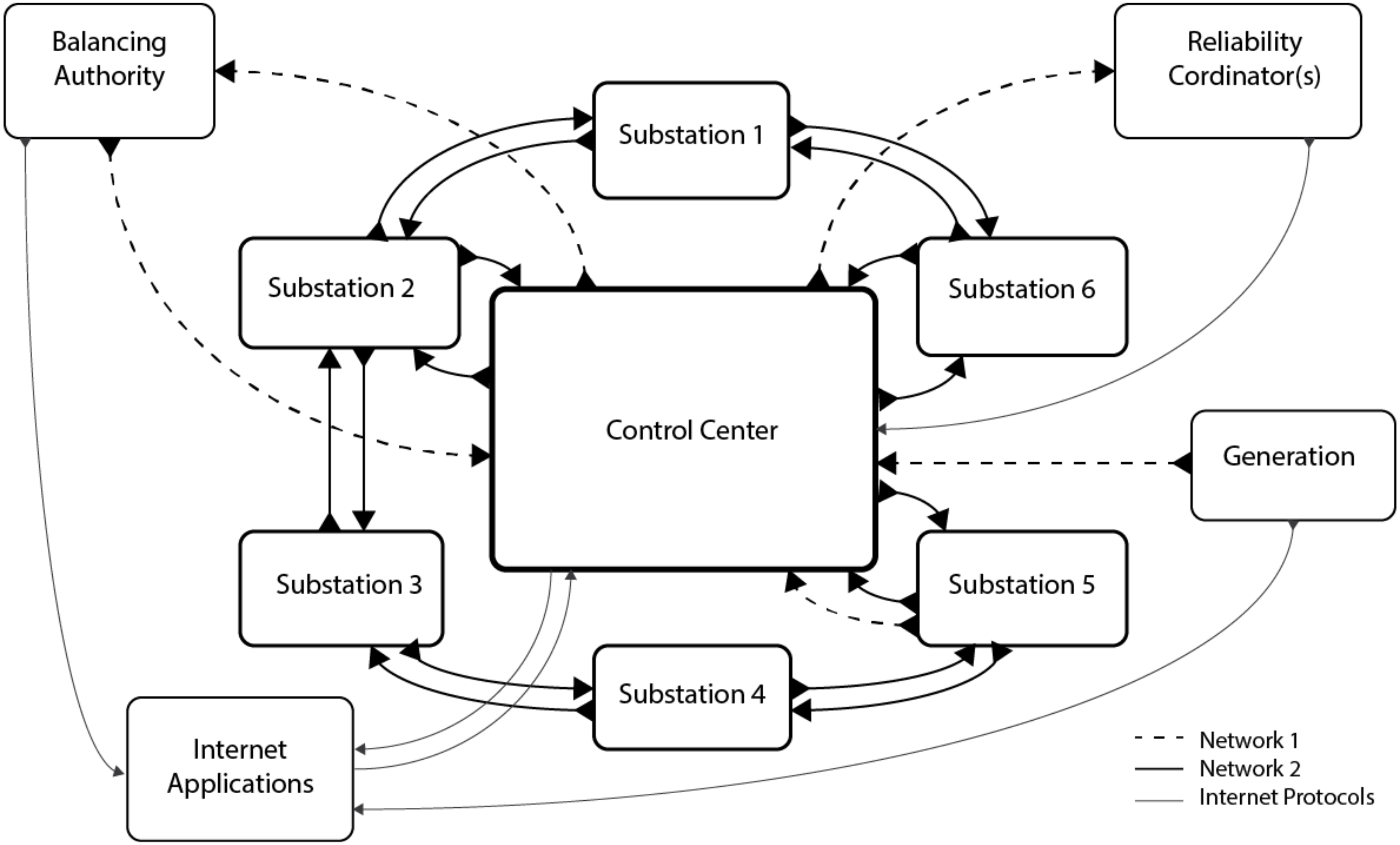
- This project will develop agnostic prototype visualizations that could be used by a wide variety of utility-based systems, including vendors for EMS, DMS, and NSOC applications.
- What are your plans to gain industry acceptance?
  - PNNL’s EIOC is being configured with a GE EMS to prototype the visualizations as a testbed with real utility operators and cybersecurity professionals providing real time feedback and input. Target date for starting these evaluations at PNNL is in FY18.

Next Steps for this Project

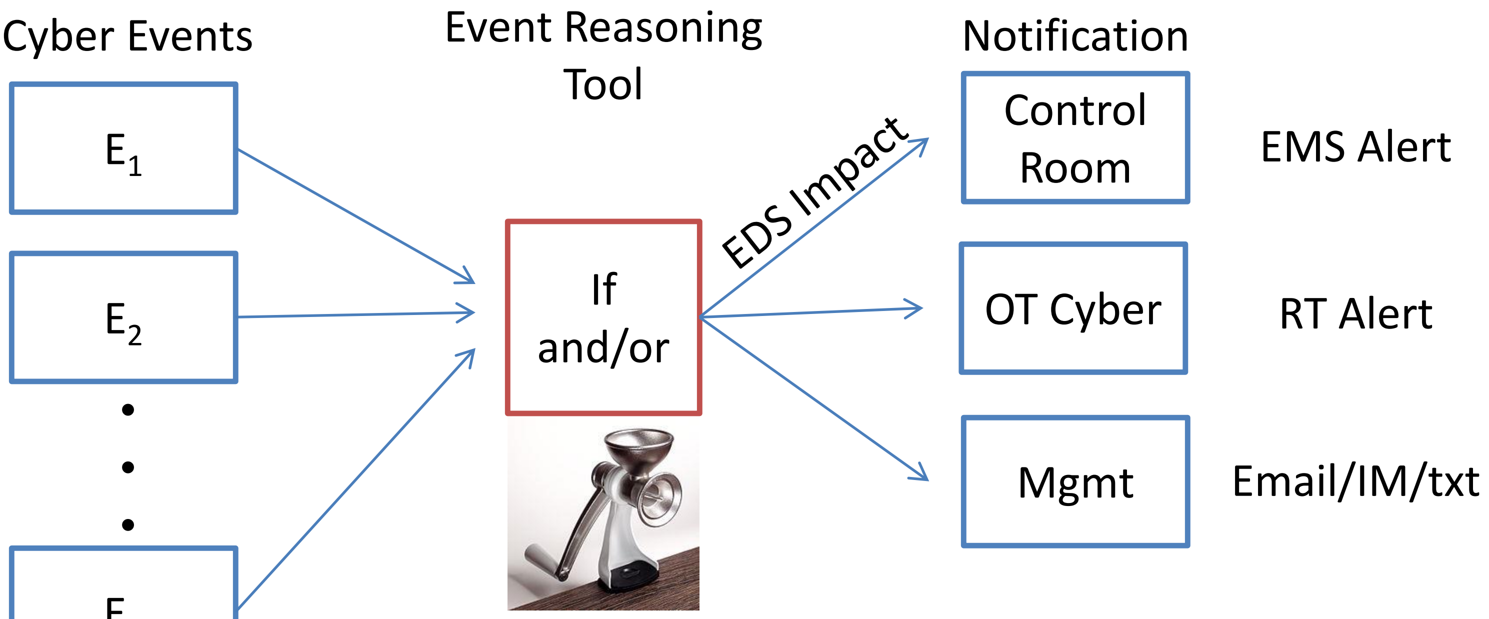
Approach for the next year or to the end of project

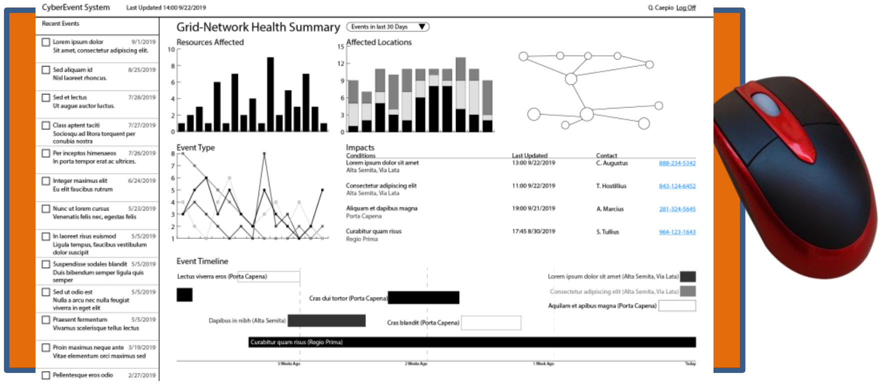
	Milestone	Due	Completed	Comments
	Task 1: Cognitive Analysis			
FY15	Initiate contextual observations and cognitive work analyses at participating utility (2/13/15)	8/30/15	8/30/15	Complete
FY16	Deliver whitepaper discussing results of cognitive analysis	5/12/2016	5/12/2016	Complete
	Task 1 Go/No Decision Point: Authorization to start Task 2	6/23/2016	6/23/2016	Complete
	Present paper at the 7th International Conference on Applied Human Factors and Ergonomics	7/31/2016	7/31/2016	Complete
	Task 2: Design Iteration and Prototyping			
FY17	Initial display concepts are designed	10/3/2016		Complete
	First-round of operator feedback on initial display concepts completed	12/19/2016		On Track
	Operator interviews providing feedback on next-level of design completed	4/14/2017		On Track
	Operator interviews providing feedback on next-level of prototypes completed	7/14/2017		On Track
	Operator interviews providing feedback on next-level of prototypes completed	9/11/2017		On Track
FY18	Whitepaper of results from iterative design and prototyping task completed	10/13/2017		On Track
	Submission of paper to appropriate conference venue	10/13/2017		On Track
	Task 2 Go/No Decision Point: Authorization to start Task 3	10/13/2017		On Track
	NOTE: Task 3 Milestones will be revisited as part of the Task 2 Go/No go Decision Point.			

Bulk Electric System Control Rooms



Decision Support: If-and/or/ then outputs




CyberEvent System Last Updated 14:00 9/22/2019 Q. Caepio Log Off

Recent Events

□ Lorem ipsum dolor 9/1/2019
Sit amet, consectetur adipiscing elit.

□ Sed aliquam id 8/25/2019
Nisl laoreet rhoncus.

□ Sed et lectus 7/28/2019
Ut augue auctor luctus.

□ Class aptent taciti 7/27/2019
Sociosqu ad litora torquent per conubia nostra

□ Per inceptos himenaeos 7/26/2019
In porta tempor erat ac ultrices.

□ Integer maximus elit 6/24/2019
Eu elit faucibus rutrum

□ Nunc ut lorem cursus 5/23/2019
Venenatis felis nec, egestas felis

□ In laoreet risus euismod 5/5/2019
Ligula tempus, faucibus vestibulum dolor suscipit

□ Suspendisse sodales blandit 5/5/2019
Duis bibendum semper ligula quis semper

□ Sed ut odio est 5/5/2019
Nulla a arcu nec nulla feugiat viverra in eget elit

□ Praesent fermentum 5/5/2019
Vivamus scelerisque tellus lectus

□ Proin maximus neque ante 3/19/2019
Vitae elementum orci maximus sed

□ Pellentesque eros odio 2/27/2019

Grid-Network Health Summary

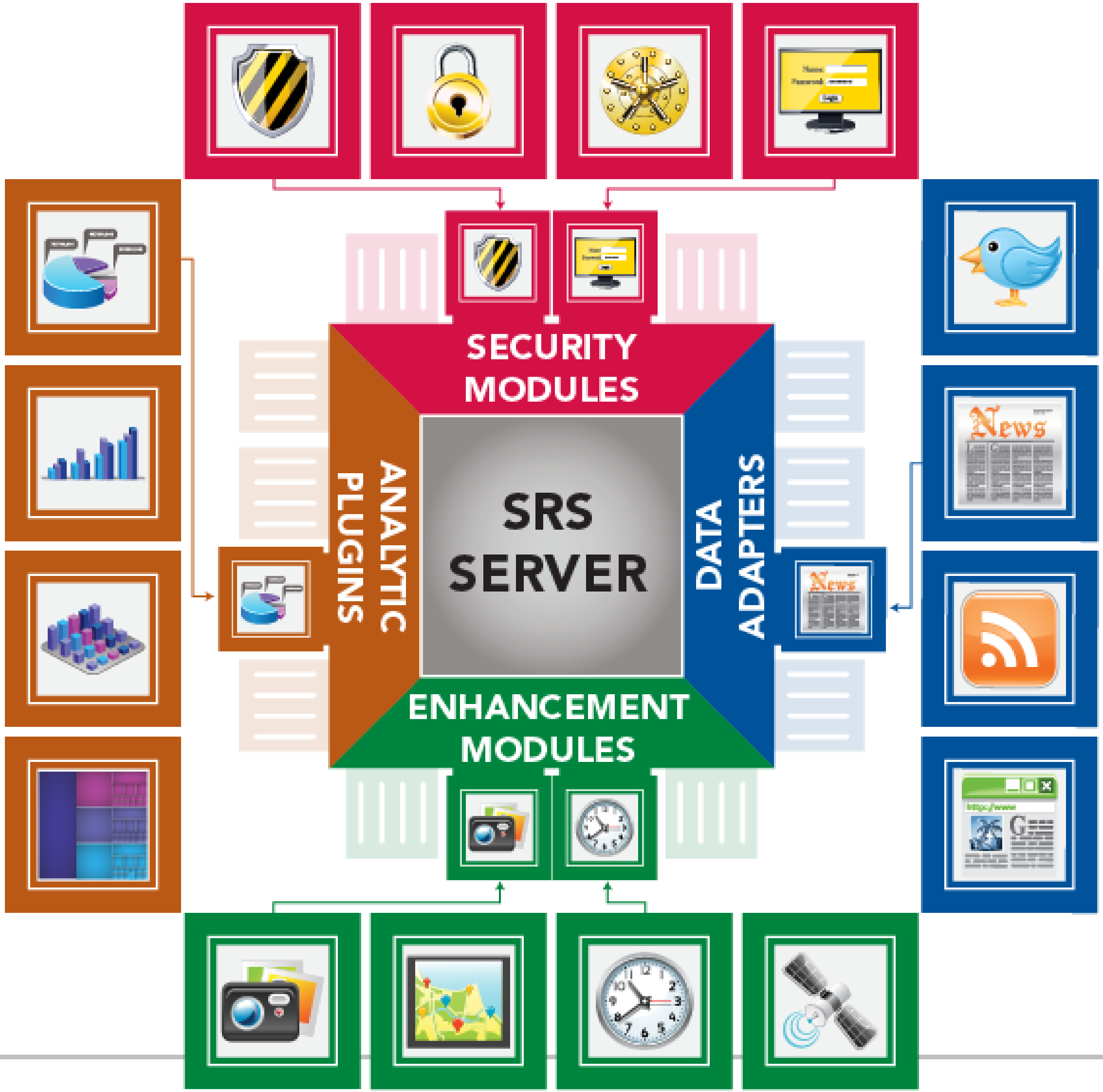
Events in last 30 Days ▼

Impacts

Conditions	Last Updated	Contact	
Lorem ipsum dolor sit amet Alta Semita, Via Lata	13:00 9/22/2019	C. Augustus	888-234-5342
Consectetur adipiscing elit Alta Semita, Via Lata	11:00 9/22/2019	T. Hostillius	843-124-6452
Aliquam et dapibus magna Porta Capena	19:00 9/21/2019	A. Marcius	281-324-5645
Curabitur quam risus Regio Prima	17:45 8/30/2019	S. Tullius	964-123-1643

Resources Affected
10
8
6
4
2
0
Affected Locations
15
12
9
6
3
0
Event Type
8
7
6
5
4
3
2
1
Event Timeline
Lectus viverra eros (Porta Capena)
Cras dui tortor (Porta Capena)
Dapibus in nibh (Alta Semita)
Cras blandit (Porta Capena)
Curabitur quam risus (Regio Prima)
Lorem ipsum dolor sit amet (Alta Semita, Via Lata)
Consectetur adipiscing elit (Alta Semita, Via Lata)
Aquilam et apibus magna (Porta Capena)
3 Weeks Ago
2 Weeks Ago
1 Week Ago
Today

Using SRS framework for the prototype development



Initial Outcomes: Operations Requirements

Dispatchers should not be solely responsible for monitoring for signs of cyber-attack.

Dispatchers need

- Actionable statements about the impacts of a cyber-attack.
- Reliable estimates of time-to-resolve cyber issues.
- This new information integrated with current displays.
- Well-defined procedures for dialogues with IT/SCADA engineers about cyber-security.
- Simple tools for communication with IT/SCADA engineers.

IT/SCADA need

- A more global view of situation awareness in the surrounding grid.
- A better understanding of equipment in substations.

Initial Cybersecurity/OT Requirements

System Administrators and Cyber Security Analysts need consistent tools to monitor separate logical/physical networks in consistent ways.

Cyber Security Analysts need

- consistent documentation of device names and ownership so that they can contact responsible parties quickly when alerts are sent.
- displays where they can correlate potentially related events.
- displays which support them following-up on investigations underway and assigned to others outside the cyber analytics team.

Operations staff need displays which let them make better use of historical data.

Where we go from here

Pulling this all together we feel that we have a set of good requirements for devising a security detection system based on the various sets of data inputs and developing good visualizations.

What we need is:

- To better understand what information is monitored and by whom?
- To facilitate the communication between the appropriate parties so a shared awareness of the situation is quickly reached
- To understand context in which the information needs to be displayed so a rapid, optimal decision is made by the appropriate personnel

Task 2: Iterative Prototyping Activities

- Develop a framework that is configurable to accept multiple alarm inputs or use an alarm processor.
- Begin implementation of decision support, guided action and response.
- Design initial visualizations - Iterate with control room operators and cybersecurity professionals on the usefulness of the designs.
- Continue to collect information from our partner utilities and other utilities.