



U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

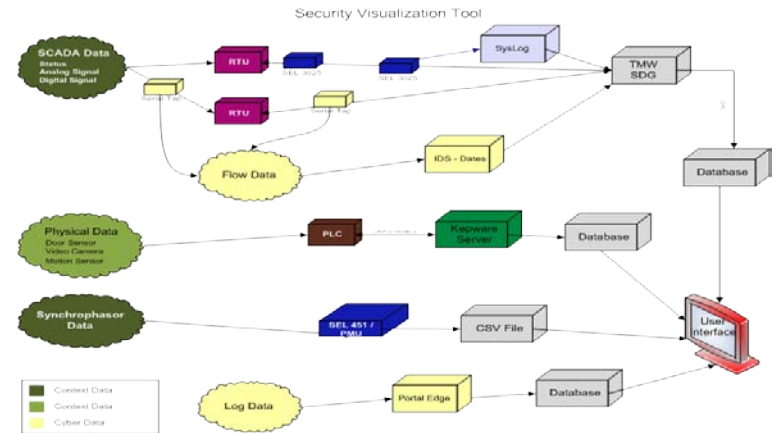
Philip A Craig Jr

Pacific Northwest National Laboratory

Real-Time Security State Visualization

Real-Time Security State Visualization

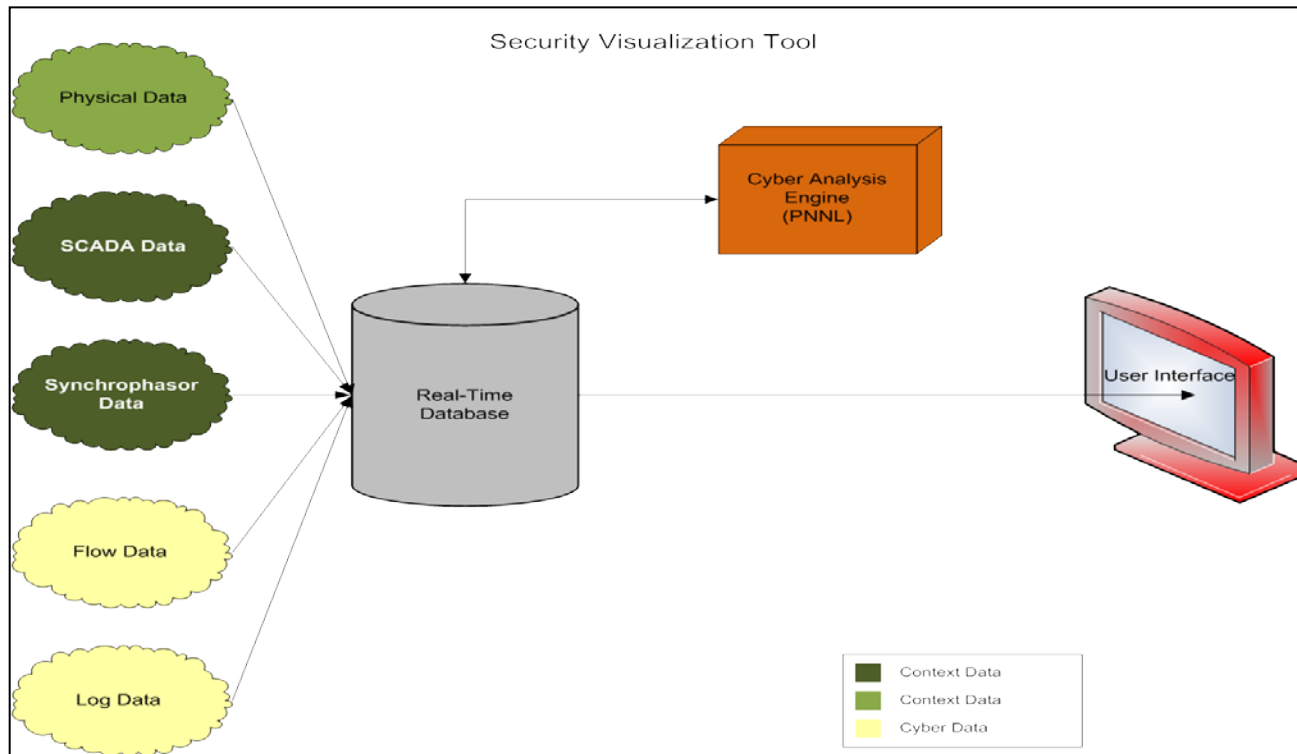
- **Outcomes:** Near real-time situational awareness utilizing a diverse set of data feeds with a flexible visualization implementation.
- **Roadmap Challenge:** Fusing perimeter security, network traffic analysis, signature-based intrusion detection systems, routable and serial traffic analysis.
- **Major Successes:** Produced an integrated view of real-time network and physical security events at a power substation



- **Schedule:** Deliver 1st POC, 2nd POC Fall 2010
- **Level of Effort:** \$325K
- **Funds Remaining:** \$75K
- **Performers:** PNNL
- **Partners:** ANL, STI, OSIsoft

Real-Time Security State Visualization

High Level Illustration of Functions/Components



Technical Approach and Feasibility

- **Approach**
 - Define data feeds and data types (both network & physical)
 - Define data collection and aggregation methods
 - Define the events of interest
 - Correlation tool evaluation & implementation
 - Visualization tool evaluation & implementation
- **Metrics for Success**
 - Security events are recognized, and the appropriate response is taken
 - Tool is relevant and useful to grid operators

Technical Approach and Feasibility

- **Challenges to Success**

- Access to data (serial, synchrophasor, etc.)
 - Created a serial tap device to access the vast amount of serial data
- Different operators want different visualizations
 - Design & implement an XML-based architecture

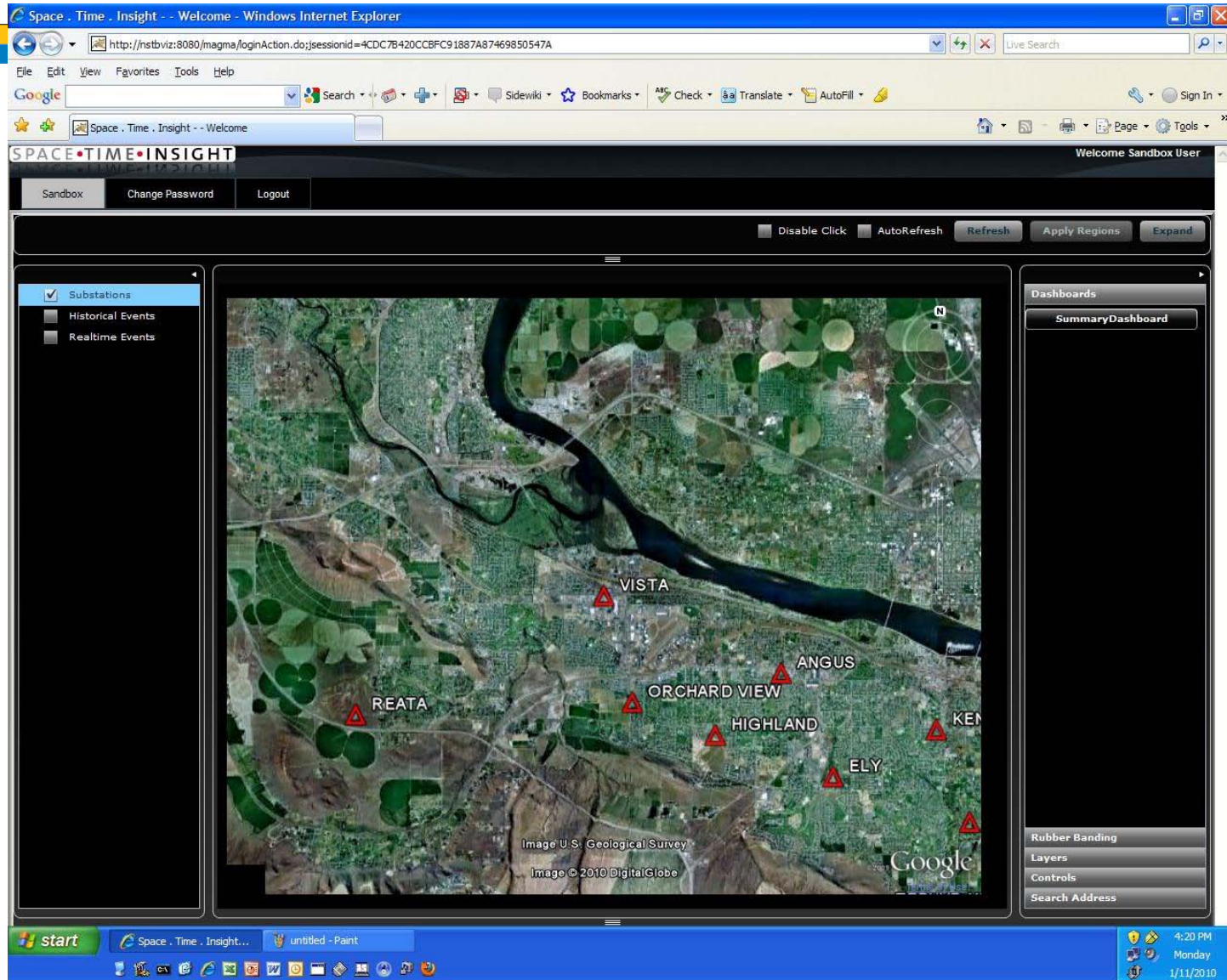
- **Technical Achievements to Date**

- Delivered a visualization product that is substation focused
- Data feeds all come into the visualization tool directly
- Heterogeneous data types include: Physical security, cyber security, routable and serial flow data

Collaboration/Technology Transfer

- **Plans to gain industry input**
 - Created industry advisory board comprised of electrical, oil & gas
 - Solicited input from board during design phase, demoed proof of concept
 - Input from demo driving next version of the product
- **Plans to transfer technology/knowledge to end user**
 - Interest in serial tap commercialization from industry
 - Commercialization Plan / Business case created
 - PNNL investing IR&D money into the serial tap
 - Documentation of data types and implementation underway
- **Value proposition**
 - Leverages existing network and power systems data already being generated
 - Give operators a powerful tool to recognize and response to cyber events without information overload via an intuitive user interface

Using Google Earth as the visualization tool



Port scan at substation event

The screenshot displays the Space-Time Insight web application interface. The main content area shows an aerial satellite view of a substation with a pop-up window for a port scan event. The event details are as follows:

- Name:** PortScan
- Time:** Tue Jan 12 10:12:10 PST 2010
- Sid:** 2
- Cid:** 6835
- Signature:** 1
- Risk Type:** High
- Troubleshooting Steps:** [Launch](#)

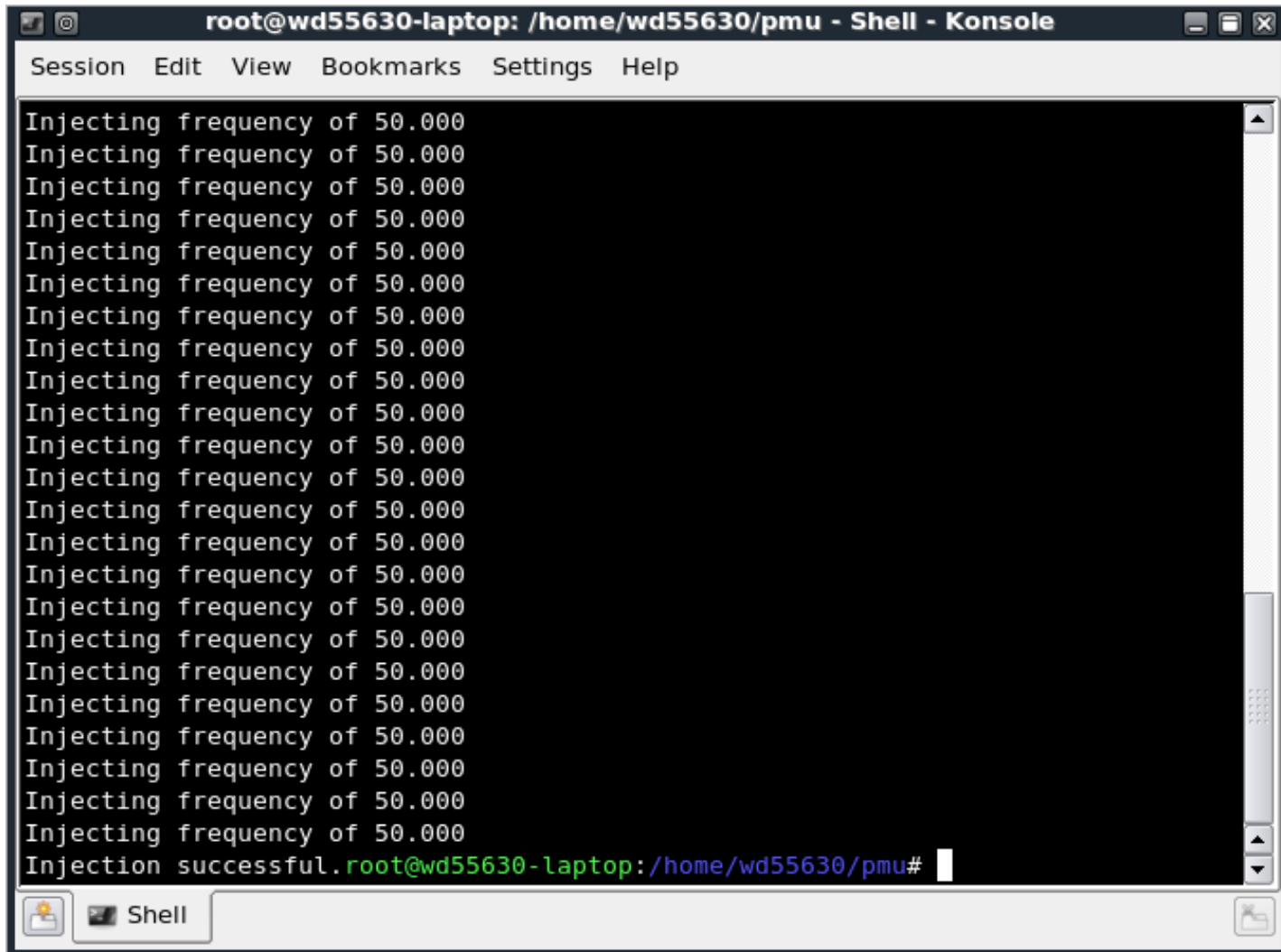
Below the main view, there are two panels:

- Info Frame: Portscan Event Troubleshooting Steps**
 1. Contact security personnel or law enforcement.
 2. Monitor other cyber systems for signs of compromise.
 3. Do not trust any data from this substation. Verify with other sources before acting upon an event data from this station until security personnel or law enforcement clear station.
 4. Identify any available containment mechanisms.
 5. Utilize physical security sensors to monitor adversary.
 6. Schedule maintenance crew/incidence response team to visit station, check for compromise, and cyber trust is restored.
- Realtime Events: PortScan Events**

sid	cid	signature	timestamp
2	6833	1	Tue Jan 12 10:12:10
2	6834	1	Tue Jan 12 10:12:10
2	6835	1	Tue Jan 12 10:12:10
2	6830	1	Tue Jan 12 10:12:00
2	6831	1	Tue Jan 12 10:12:00
2	6832	1	Tue Jan 12 10:12:00
2	6828	2	Tue Jan 12 10:11:18
2	6829	2	Tue Jan 12 10:11:18

The interface also includes a navigation menu on the left with options for Substations, Historical Events, and Realtime Events. On the right, there are buttons for various event types: OPC Events, PortScan Events, SerialTap Events, SSCPLog Events, Rubber Banding, Layers, Controls, and Search Address. The bottom of the screen shows the Windows taskbar with the Start button, several open applications, and the system tray displaying the time as 10:06 AM on Tuesday, 1/12/2010.

Synchrophasor Attack



A terminal window titled "root@wd55630-laptop: /home/wd55630/pmu - Shell - Konsole" displays a series of 20 lines of text: "Injecting frequency of 50.000". The 21st line shows "Injection successful." followed by the prompt "root@wd55630-laptop:/home/wd55630/pmu#". The terminal has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The window title bar includes standard Linux window controls (minimize, maximize, close) and a search icon.

```
root@wd55630-laptop: /home/wd55630/pmu - Shell - Konsole
Session Edit View Bookmarks Settings Help
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injecting frequency of 50.000
Injection successful.root@wd55630-laptop:/home/wd55630/pmu#
```

Synchrophasor attack event

The screenshot displays the Space-Time Insight web application interface within a Windows Internet Explorer browser. The browser's address bar shows the URL: `http://nstbviz:8080/magma/loginAction.do?jsessionid=4CDC7B420CCBFC91887A87469850547A`. The application header includes the logo "SPACE•TIME•INSIGHT" and a "Welcome Sandbox User" message. Navigation tabs for "Sandbox", "Change Password", and "Logout" are visible. A control bar at the top right contains buttons for "Disable Click", "AutoRefresh", "Refresh", "Apply Regions", and "Expand".

The main content area features a central map view with a Google Maps overlay. A pop-up window displays event details for a synchrophasor attack:

Mon Jan 11 16:40:36 PST 2010	
Name	EIOC_451_Frequency
Time	Mon Jan 11 16:40:36 PST 2010
Value	50.0
Frequency	Launch
Risk Type	Medium
Troubleshooting Steps	Launch

On the left side, a sidebar menu is active, showing "Substations", "Historical Events", and "Realtime Events" (which is selected). On the right side, a "Dashboards" panel lists event types: "OPC Events", "PortScan Events", "SerialTap Events", and "SSCLog Events". Below this, there are sections for "Rubber Banding", "Layers", "Controls", and "Search Address".

At the bottom, an "Info Frame" titled "Phasor Event Troubleshooting Steps" provides a list of actions:

1. Contact security personnel or law enforcement.
2. Monitor other cyber systems for signs of compromise.
3. Do not trust any data from this substation. Verify with other sources before acting upon an event data from this station until security personnel or law enforcement clear station.
4. Identify impact of modified/injected synchrophasor data.
5. Notify operations staff.
6. Utilize physical security sensors to monitor adversary.
7. Monitor synchrophasor data for end to cyber event.
8. Schedule maintenance crew/incidence response team to visit station and check for compromise.

The Windows taskbar at the bottom shows the Start button, the application title "Space . Time . Insight...", and the system tray with the time "4:41 PM" and date "Monday 1/11/2010".

Serial Tap Event

Space . Time . Insight - Welcome - Windows Internet Explorer

http://nstbviz:8080/magma/loginAction.do?sessionId=4CDC7B420CCBFC91887A87469850547A

File Edit View Favorites Tools Help

Google Search


Space . Time . Insight - Welcome

SPACE • TIME • INSIGHT Welcome Sandbox User

Sandbox Change Password Logout

Disable Click AutoRefresh Refresh Apply Regions Expand

Substations
Historical Events
Realtime Events



Tue Jan 12 11:24:40 PST 2010

Name SerialTap
Time Tue Jan 12 11:24:40 PST 2010
Sid 1000001
Cid 6820
Signature 1
Risk Type Extreme
Troubleshooting Steps [Launch](#)

Dashboards

OPC Events
PortScan Events
SerialTap Events
SSCPLog Events

Rubber Banding
Layers
Controls
Search Address

: Info Frame

SerialTap Event Troubleshooting Steps

1. Contact security personnel or law enforcement.
2. Monitor other systems for signs of compromise.
3. Do not trust any data from this substation. Verify with other sources before acting upon an event data from this station until security personnel or law enforcement clear station.
4. Identify impact of modified/injected commands.
5. Notify operations staff.
6. Utilize physical security sensors to monitor adversary.
7. Monitor security logs for end to cyber event.
8. Schedule maintenance crew/incidence response team to visit station and check for compromise.

Realtime Events: SerialTap Events

sid	cid	signature	timestamp
1000001	6820	1	Tue Jan 12 11:24:40 P
1000001	6819	1	Tue Jan 12 11:22:41 P
1000001	6818	1	Mon Jan 11 15:05:33 P
1000001	6817	1	Mon Jan 11 14:52:03 F
1000001	6816	1	Mon Jan 11 14:51:45 F

Done

start Space . Time . Insight... nstbviz - Remote Des... C:\Documents and Se... Substation view Seria...

Local intranet 100%

11:27 AM
Tuesday
1/12/2010

Next Steps

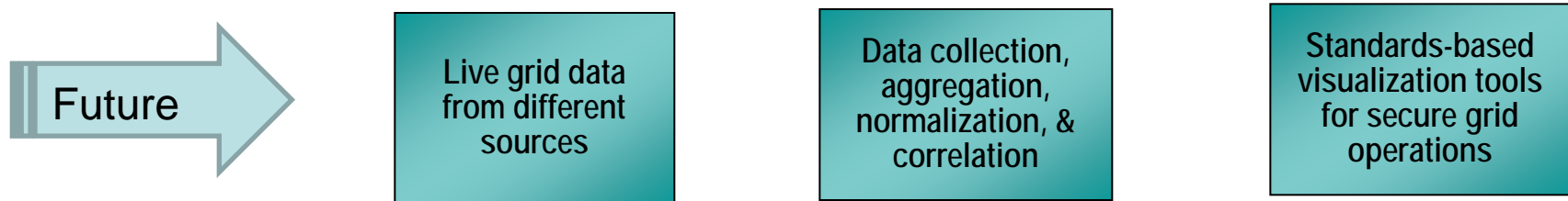
- **Approach For the Next Year**
 - Utilize real time database
 - Separate cyber analytics function from display tool
 - Define approach to link analysis engine with multiple display tools via XML
 - Correlate events across data types and substations
- **Leverage National Visualization & Analytics Center**
- **Describe potential follow-on work, if any**
 - Next generation visualization tools
 - Multiple substations
 - More sophisticated analytics
 - Cost: \$400K-\$700K depending on scope



Take the Operations Control Center to the Next Level



Begin to leverage recognized world class National Visualization & Analysis Center (NVAC) capabilities



Goal: Increase the situational awareness of grid security in order to allow operators to easily respond to network events in real time, while minimizing information overload.

Next Generation Collaborative Visualization Ideas



These displays, technology, and expertise exist at PNNL and can be leveraged to increase the security of the nation's power grid

Real-Time Security State Visualization

