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

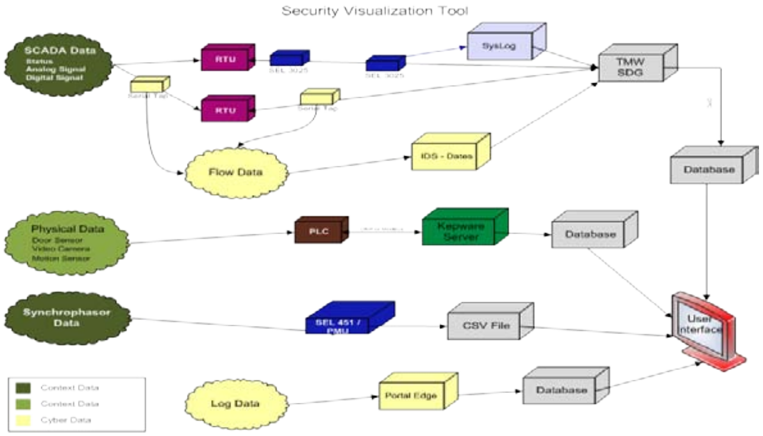
Philip A Craig Jr

Pacific Northwest National Laboratory

Real-Time Security State Visualization

Real-Time Security State Visualization

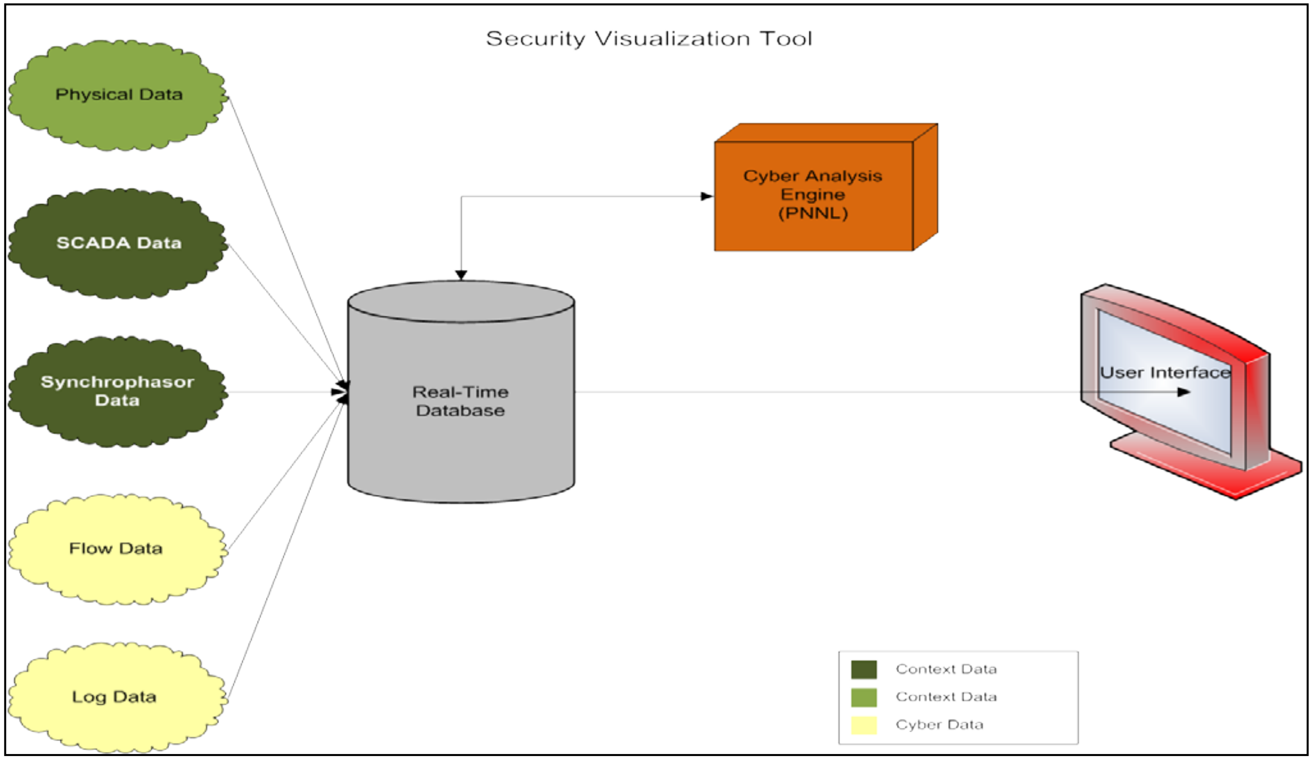
- **Outcomes:** Near real-time situational awareness utilizing a diverse set of data feeds with a flexible visualization implementation.
- **Roadmap Challenge:** Fusing perimeter security, network traffic analysis, signature-based intrusion detection systems, routable and serial traffic analysis.
- **Major 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

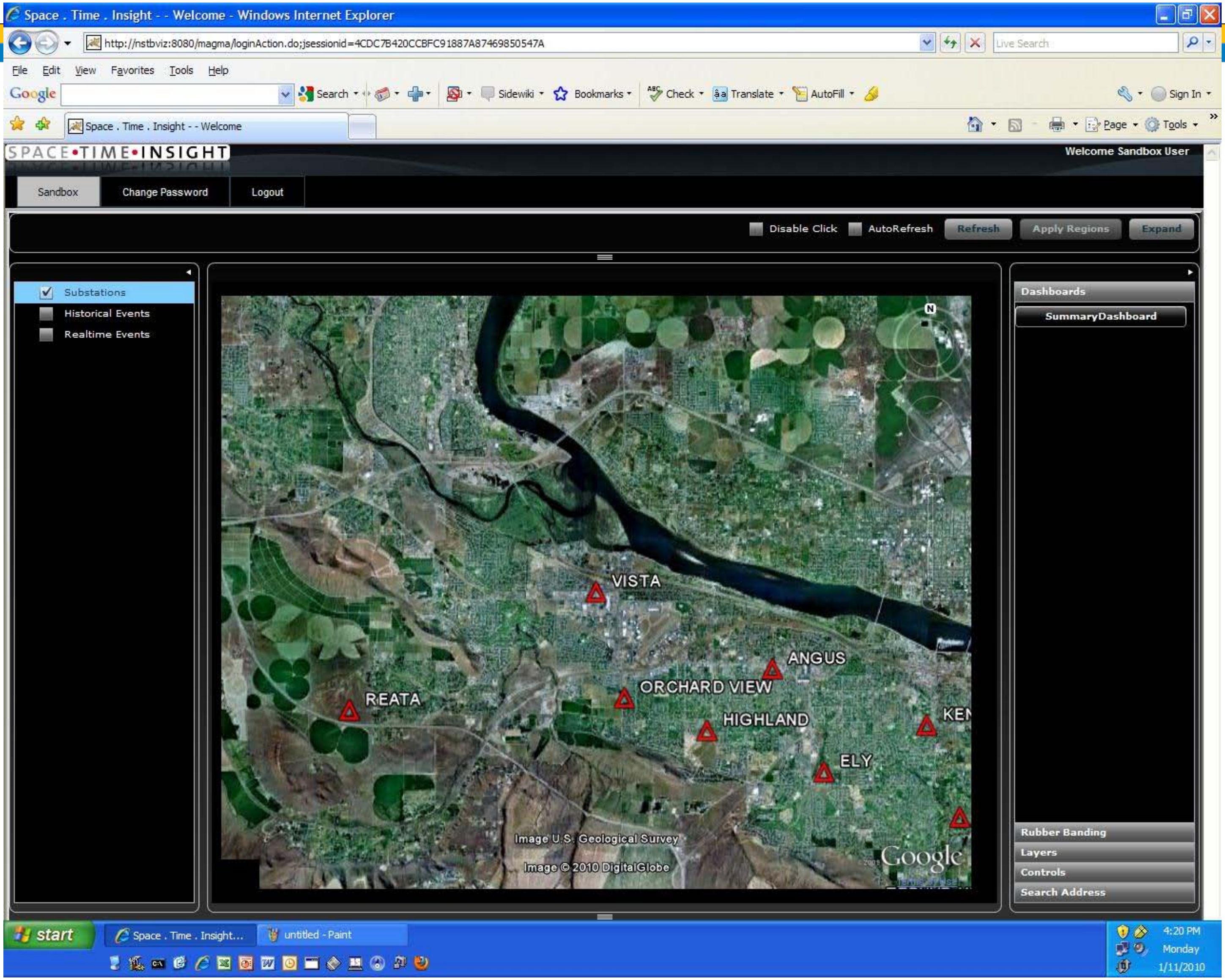
Technical Approach and Feasibility

- **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

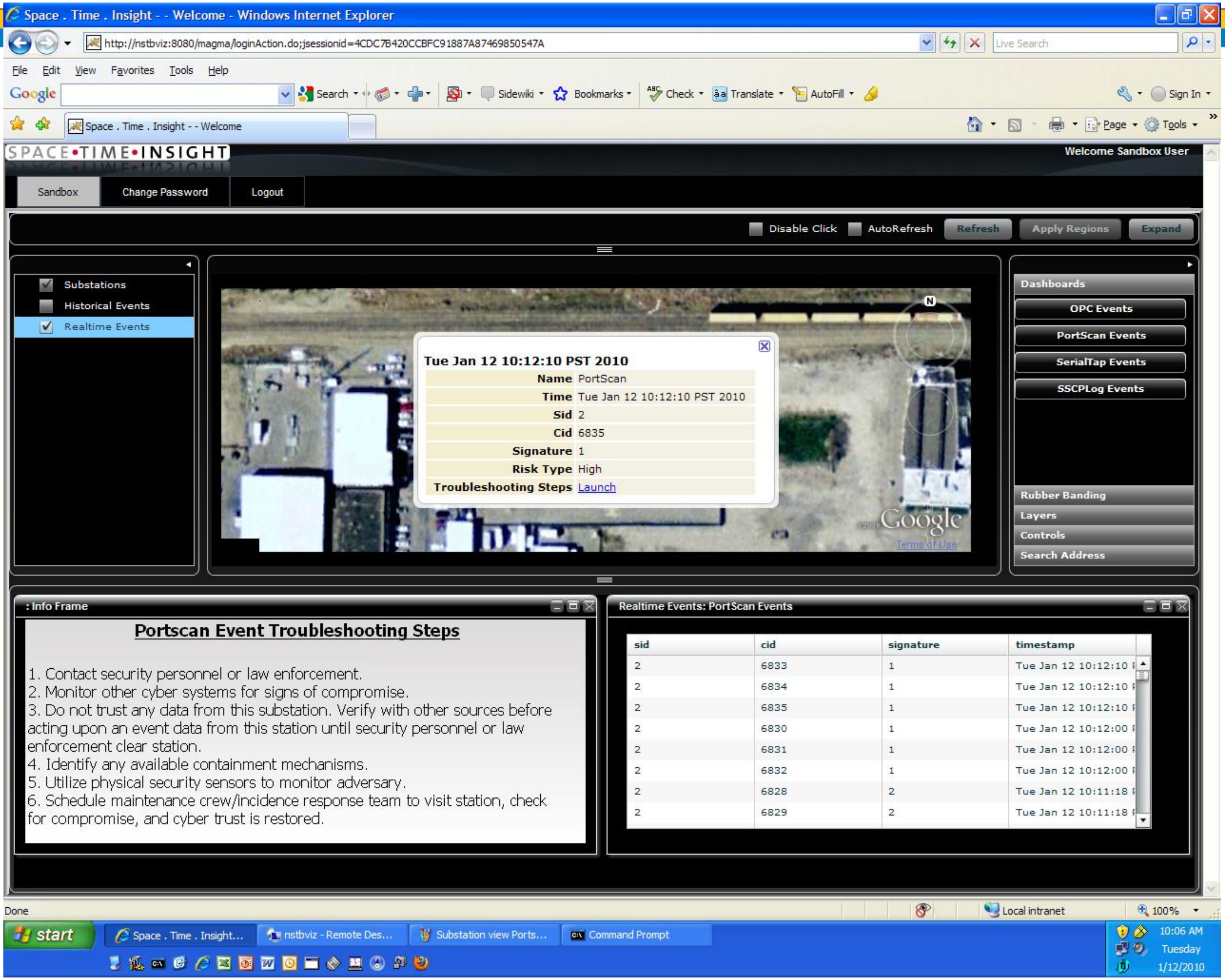
Collaboration/Technology Transfer

- **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



Tue Jan 12 10:12:10 PST 2010

Name	PortScan
Time	Tue Jan 12 10:12:10 PST 2010
Sid	2
Cid	6835
Signature	1
Risk Type	High
Troubleshooting Steps	Launch

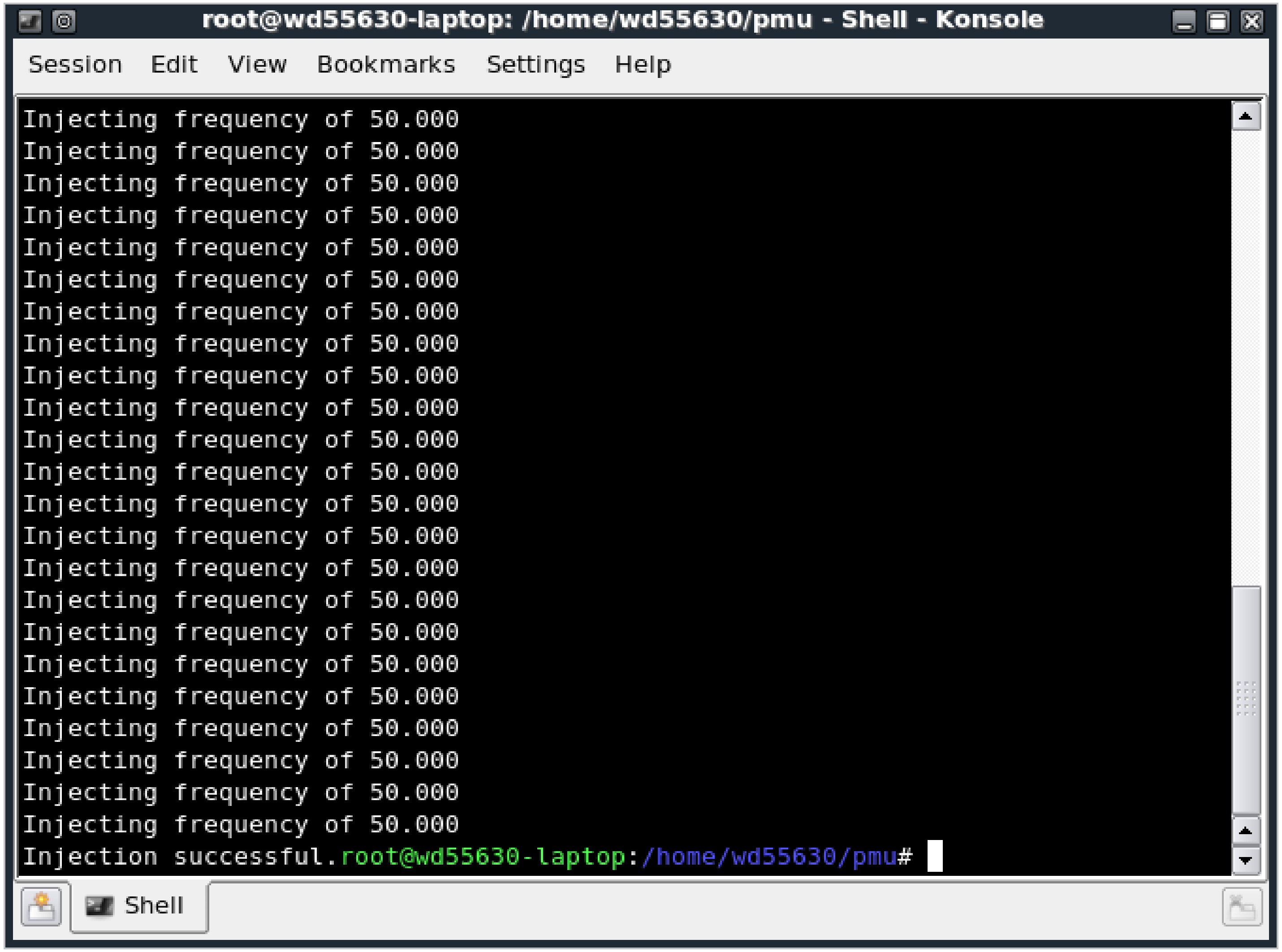
Portscan Event Troubleshooting Steps

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

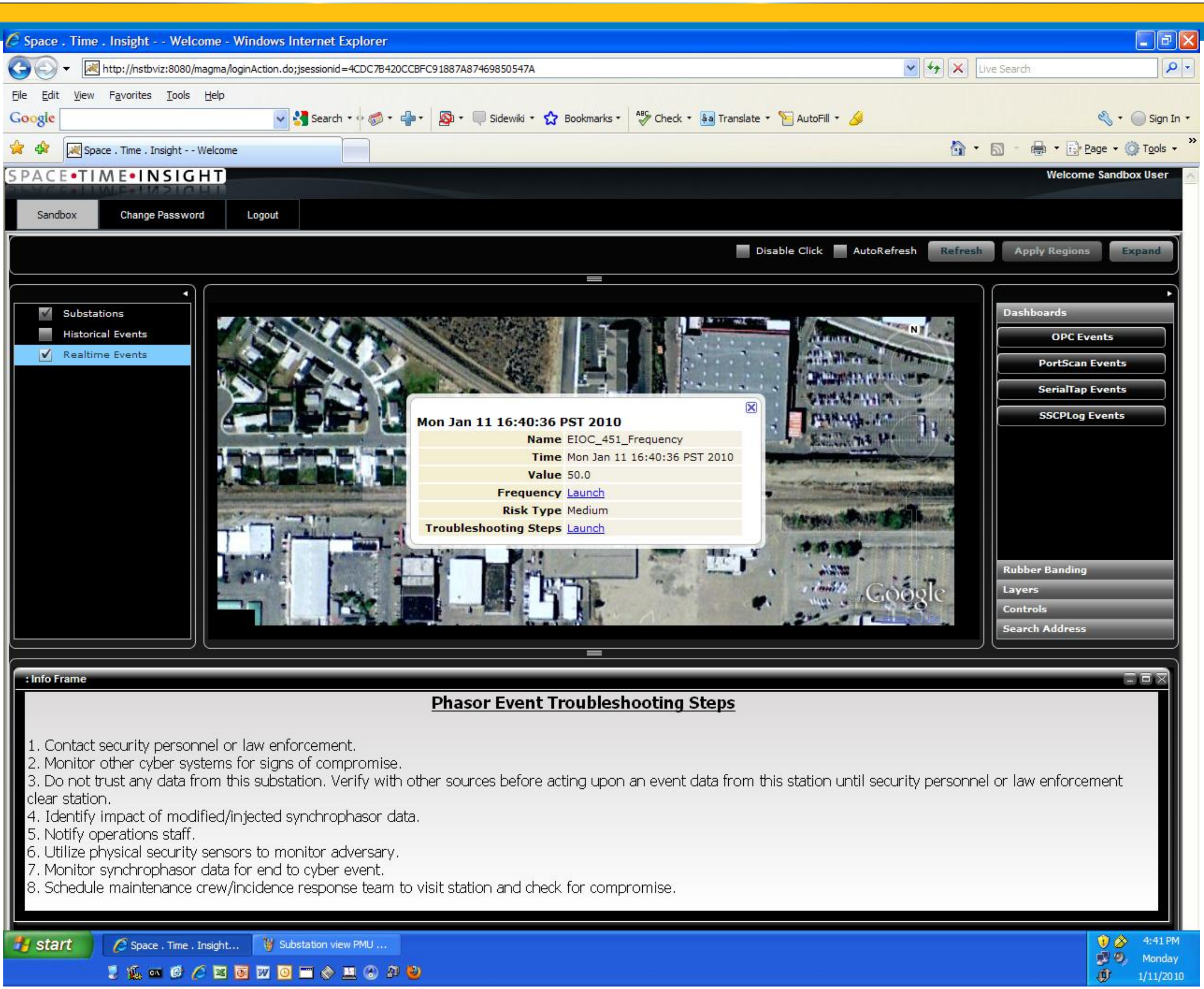
sid	cid	signature	timestamp
2	6833	1	Tue Jan 12 10:12:10
2	6834	1	Tue Jan 12 10:12:10
2	6835	1	Tue Jan 12 10:12:10
2	6830	1	Tue Jan 12 10:12:00
2	6831	1	Tue Jan 12 10:12:00
2	6832	1	Tue Jan 12 10:12:00
2	6828	2	Tue Jan 12 10:11:18
2	6829	2	Tue Jan 12 10:11:18

Synchrophasor Attack



```
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
Injecting frequency of 50.000
Injecting frequency of 50.000
Injection successful.root@wd55630-laptop:/home/wd55630/pmu# 
```

Synchrophasor attack event



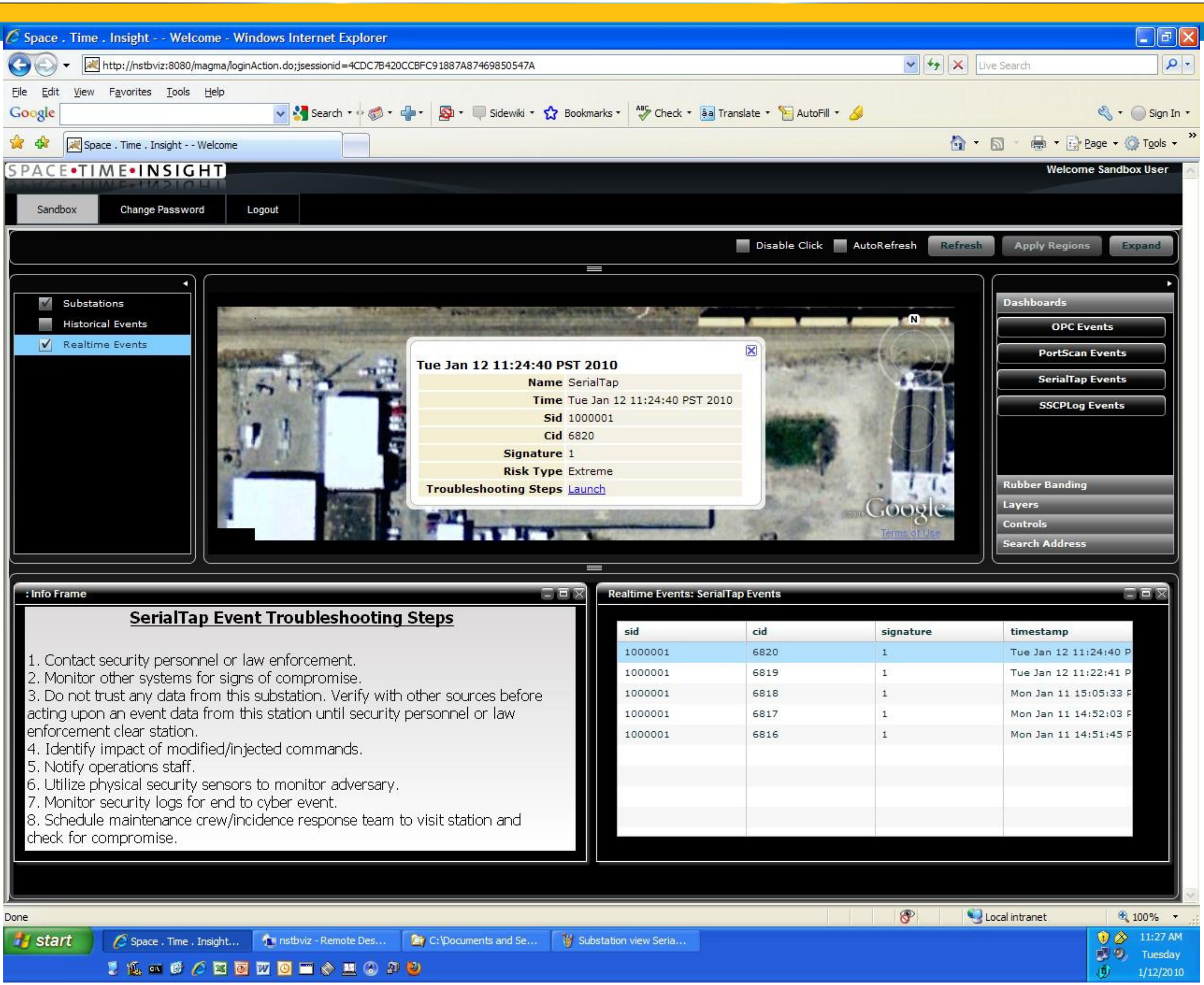
Mon Jan 11 16:40:36 PST 2010

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

Phasor 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 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.

Serial Tap Event



☑ 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

SerialTap Event Troubleshooting Steps

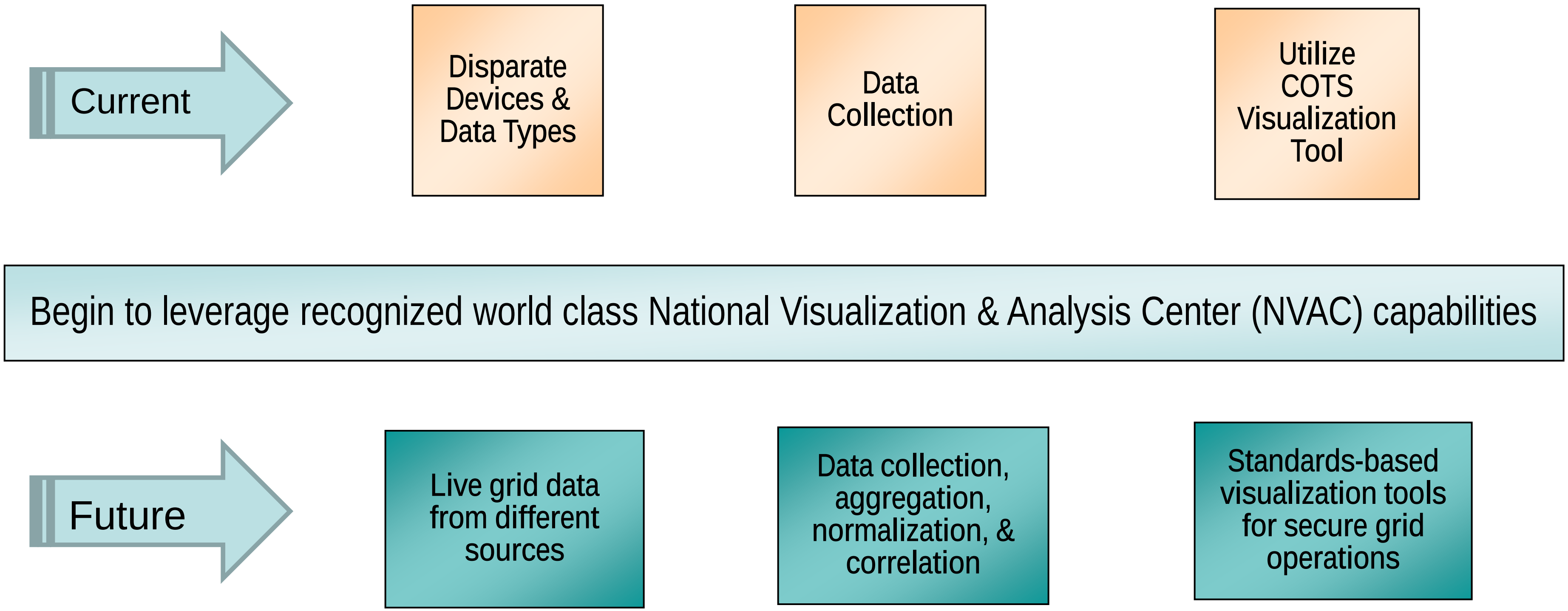
1. Contact security personnel or law enforcement.
2. Monitor other systems for signs of compromise.
3. Do not trust any data from this substation. Verify with other sources before acting upon an event data from this station until security personnel or law enforcement clear station.
4. Identify impact 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.

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 F
1000001	6817	1	Mon Jan 11 14:52:03 F
1000001	6816	1	Mon Jan 11 14:51:45 F

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



Current

Disparate Devices & Data Types

Data Collection

Utilize COTS Visualization Tool

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

Future

Live grid data from different sources

Data collection, aggregation, normalization, & correlation

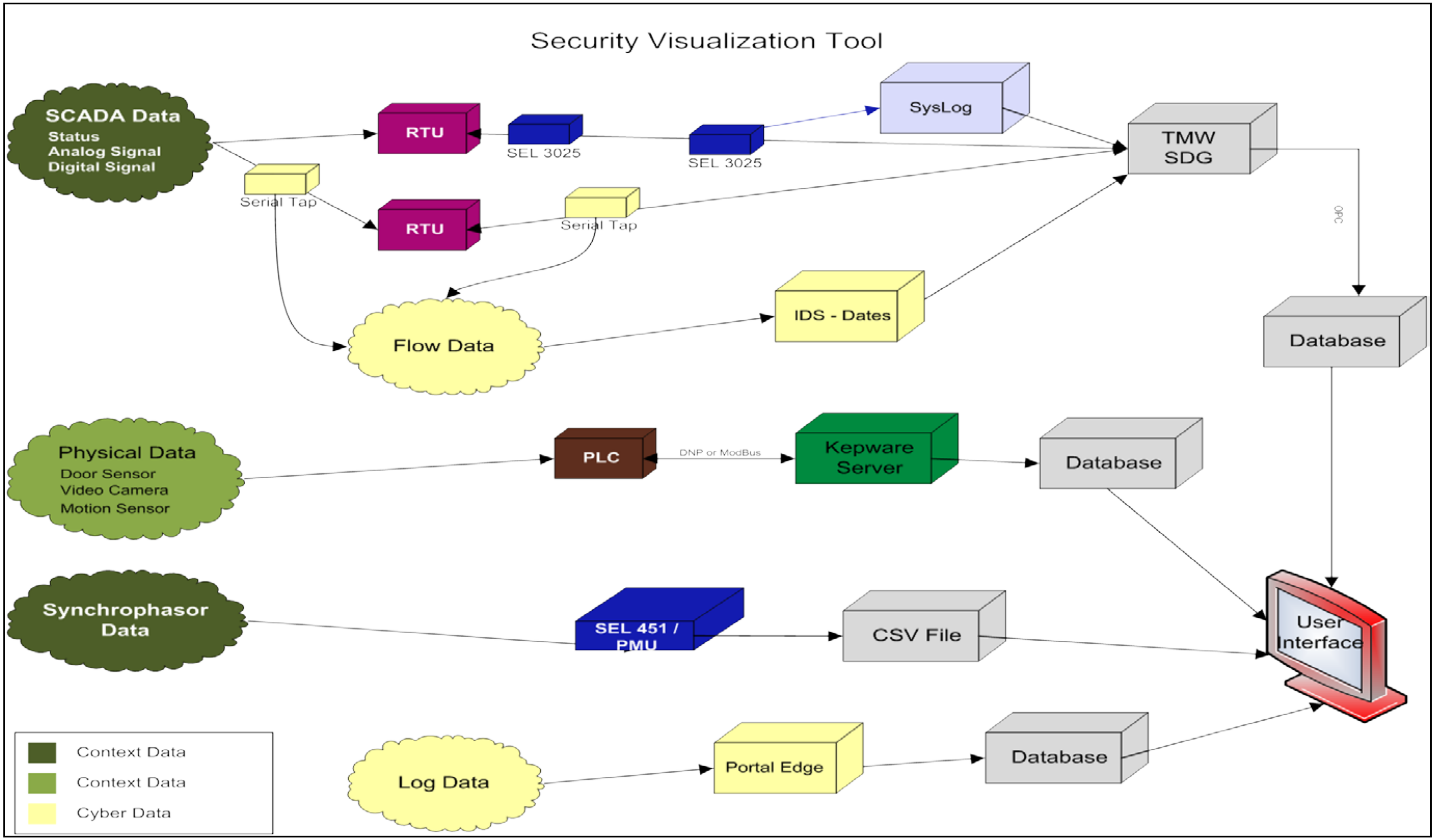
Standards-based visualization tools for secure grid operations

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



Security Visualization Tool

SCADA Data
Status
Analog Signal
Digital Signal

RTU

SEL 3025

SEL 3025

SysLog

TMW SDG

Serial Tap

RTU

Serial Tap

OPC

Flow Data

IDS - Dates

Database

Physical Data
Door Sensor
Video Camera
Motion Sensor

PLC

DNP or ModBus

Kepware Server

Database

Synchrophasor Data

SEL 451 / PMU

CSV File

User Interface

Log Data

Portal Edge

Database

🟩	Context Data
🟩	Context Data
🟨	Cyber Data