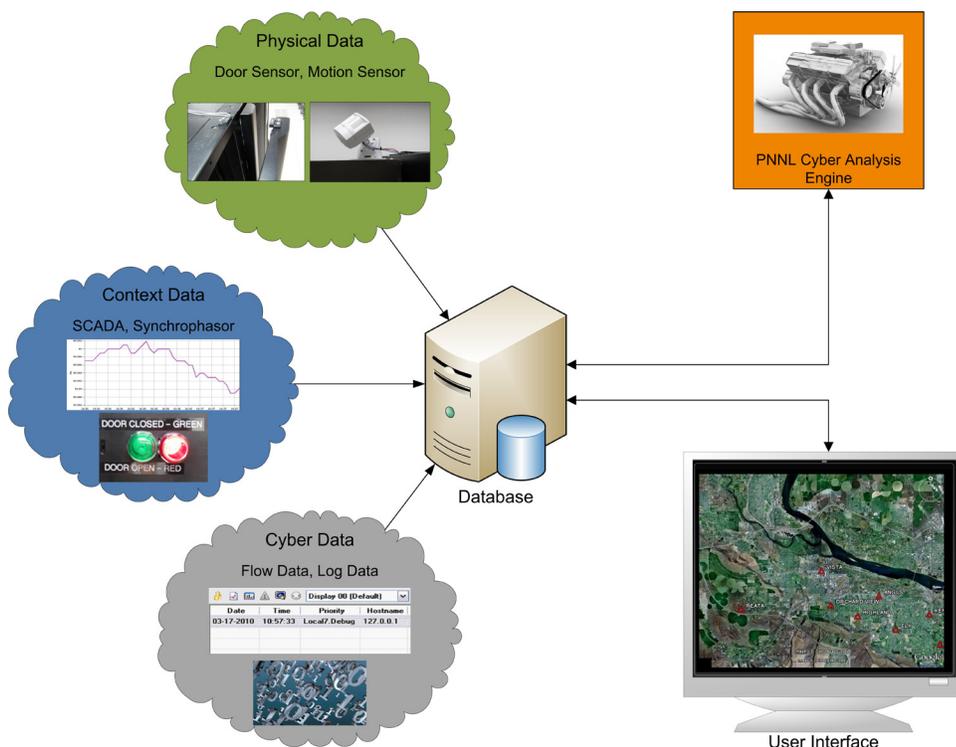


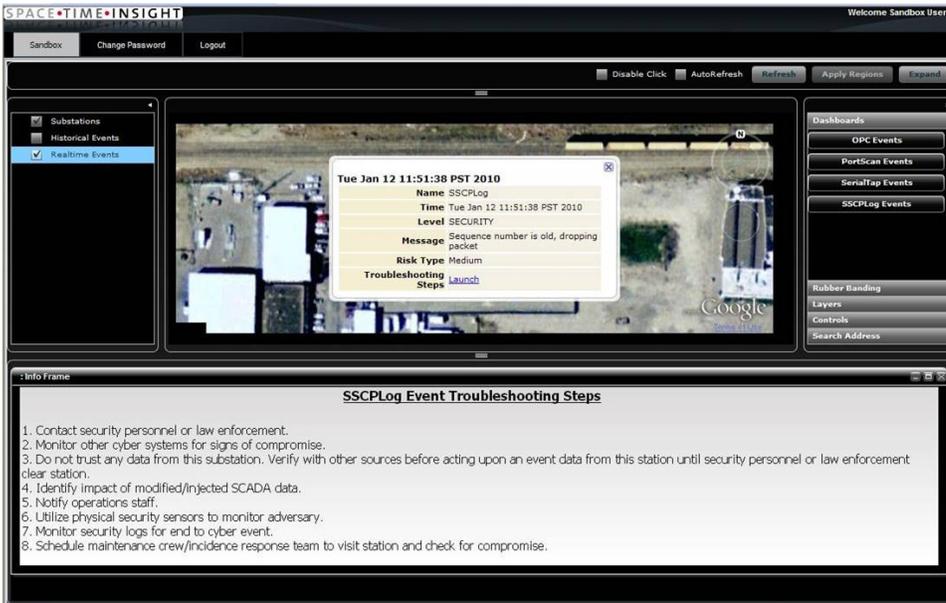
# Real-Time Security State Visualization Tool

Process control networks are composed of control system, physical sensor, and security data. All of these applications are silos that do not interoperate and use data from each other. These heterogeneous data sources need to be collected into a centralized repository, analyzed, and reported to control system operators and engineers to provide true real-time situational awareness.

Security events can no longer be considered an IT enterprise concern. These events also cannot be evaluated alone. Control system security events need to be brought to the attention of those who

Control system operators and engineers require real-time system state awareness to manage the power grid efficiently and effectively. With the advent of smart grid technologies and the integration of physical and cyber security controls, the ability to aggregate and assimilate the various data feeds manually is becoming intractable. A system that automates these tasks and provides an intuitive user interface to the data is necessary to maintain a secure and stable smart grid of the future.





operate and manage it. However, for this data to be of value to their daily concerns, it must be presented within the context of the environment. Aggregating data from control system operations with physical and cyber data will enable presentation of the data to users within the context of their area of concern. Operators can be notified of security events that may have consequences on the stability of the grid. Engineers can be notified of security events so they can handle the incident and contact incidence response teams and law enforcement as necessary. The real-time situational awareness provided by bringing together these disparate data types will enable dynamic response to all events instead of solely disaster recovery efforts after a serious compromise has occurred.

## PROBLEM DOMAIN

- » Control system operators and engineers lack awareness of cyber security events
- » Control system flow data alone is insufficient to detect all malicious activity

- » There is a lack of analysis of cyber security data in control system environments
- » Control systems have heterogeneous data feeds that are not aggregated for analysis and action

## SOLUTION

- » Aggregate heterogeneous data types in central repository
- » Perform both real-time and forensic cyber analytics on data to detect events
- » Utilize a geographical user interface to present the data within the context of the environment for monitoring and response to events
- » Contextual role-based access and operations to ensure proper need-to-know access to information

## PNNL APPROACH

- » Focus on local utility data then scale up to regional and national level analysis
- » Concept environment selection
- » Utilize industry advisors to ensure the needs of the industry are met
- » Attempt to design the solution around commodity products for faster time to commercialization transfer and market

## WHY THIS SOLUTION IS BETTER

- » Provides a combined view of physical, cyber, and operational data
- » Supports both routable and serial architectures
- » Information is presented within the context of environment and the users concerns
- » Provides event troubleshooting guidance to the user

## INDUSTRY COLLABORATORS

- » Space-Time Insight
- » Siemens

For more information, contact:

**Tom McKenna**

Pacific Northwest National Laboratory

Thomas.McKenna@pnl.gov

**NSTB**  
National SCADA Test Bed

  
**Pacific Northwest**  
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965