ICS Research Projects
SANS SCADA Summit 2011

David Kuipers
Idaho National Laboratory

28 Jan 2011

www.inl.gov

Idaho National Laboratory

INL/CON-10-19389

INL Control System Situational Awareness Technology

- **Sophia Tool:** Provides users a thorough view of their control system and wired sensor networks, allowing a detailed review of all conversations that are occurring
- **Mesh Mapper Tool:** Collects all the routes taken by ICS wireless mesh network data messages and tracks them in such a way the operator can readily observe any abnormal behavior of wireless sensor networks
- **Intelligent Cyber Sensor:** Distinguishes between component failure and cyber security incidents and monitors the overall health of a system
- **Data Fusion System:** Identifies, reduces, and characterizes data, providing integrated situational awareness of the cyber and operational health of the control and sensor system
- **Network Access Policy Tool (NetAPT):** Provides standardized method of network information exchange.

Sophia Tool

Goal: Scalable architecture for capture and aggregation of information
  - Reads info from real-time network sources, archived PCAP files, netflow and syslog feeds
- Sortable communications tree to drill into hosts and services
  - Multi-user 3D interface
  - Fast forward, rewind and pause network displays
  - Customizable 3D network layout
  - GeoIP enabled to view interactions with internet based hosts
  - Protocols distinguished by color
- Working to complete Alpha software for site testing, develop commercialization partners
- Partners: INL, TBD Commercialization Partners, and multiple asset owner Alpha sites

Mesh Mapper Tool

- Passive collection of route information of a wireless mesh network (WMN). Graphically present this information for quick analysis.
  - **Goal:** Make Information available to higher level decision analysis tools that encompass more than just the wireless elements of a control system.
  - Define the Mesh Mapper Architecture
  - Develop a proof-of-concept prototype
  - Finalize development and establish commercialization partnership(s)
  - Perform an Alpha site test on a commercial system
  - Demonstrate with Tool Set.
- Partners: INL, TBD device vendor(s), Asset Owner POC sites

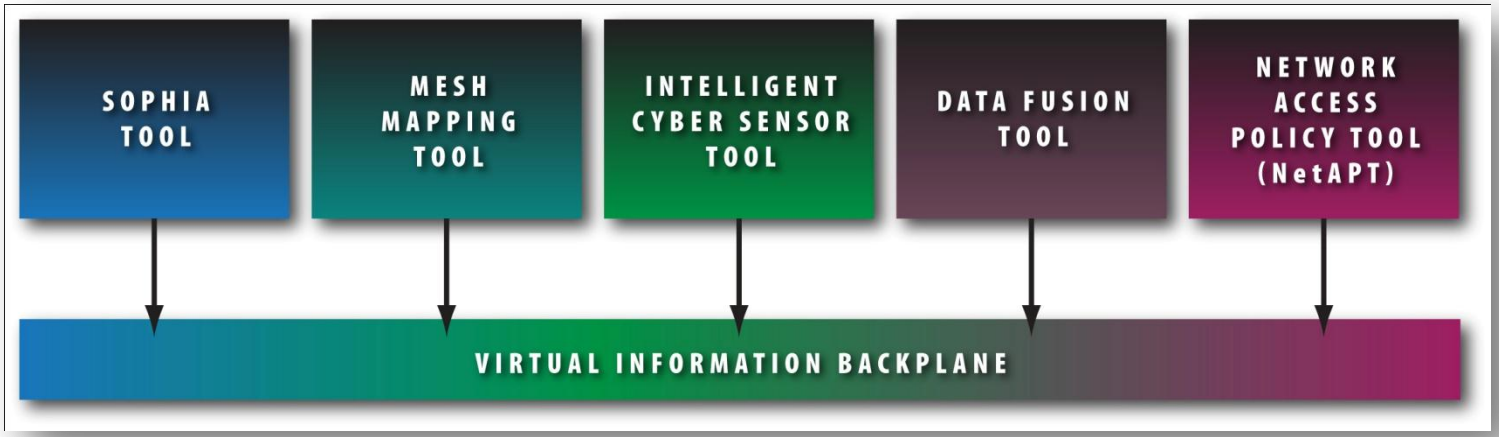
Intelligent Cyber Sensor

- Cyber sensor looks at smart grid sensor traffic with a highly efficient mechanism of monitoring and filtering network performance data.
- **Goal:** Create a new control system intelligent agent specification that contains anomaly detection and active autonomous responses.
  - Identify effective anomaly detection algorithms to implement within intelligent software agents to enhance reliability and survivability of control systems.
  - Create an intelligent software agent prototype capable of monitoring control system hardware and demonstrate its ability to detect and respond to anomalies.
  - Integrate with NetATP, ensures an effective implementation of security policy, flagging degradation trends in the associated sensor subsystem, and presenting information in an efficient, ergonomic fashion.
- Partners: University of Idaho, Univ of Illinois Urbana/Champagne, INL, Asset Owner POC sites

Data Fusion Tool

- Computational Intelligence (CI) Advanced Data Mining Techniques (ADMTs) combine multiple temporal/spatial, highly diverse data streams into a unified data model, then identify relationships and frequent data patterns that are common to ICS and sensor systems.
  - **Goal:** Achieve resilient data fusion (generation of actionable intelligence) via various CI techniques. The Data Fusion Tool will couple the cyber health and operational performance aspects of a sensor network to provide an overall network performance indicator.
  - Develop the ADMT architecture
  - Develop a proof-of-concept prototype
  - Integrate/demonstrate prototype solution with the Intelligent Cyber Sensor and other tools.
- Partners: University of Idaho, INL

INL Control System Situational Awareness Technology



4GL Microcontroller Implementation

Recent testing of various PLCs, RTUs, and IEDs suggest that many if not most of these devices can be easily exploited and controlled by hackers.

- The project: Port an existing high-level language to microcontrollers as its native operating environment. This environment would provide many advantages to the developer:
  - Far fewer exploitable coding mistakes
  - Sharp decrease in development time
  - Increased pool of developers to draw from
  - A wealth of already debugged modules already written for the language
- Selected Python language to implement on popular ARM processor
  - In Basic Prototyping Phase
- Project Length: 2 years
- Partners: Siemens Corp Research, TBD Asset Owner POC site

Honeywell: Role-Based Access Control

- Research, develop and commercialize a role-based access control (RBAC) –driven, least privilege architecture for control systems
- Project Lead: Honeywell International, Inc.
- Partners: University of Illinois, Idaho National Laboratory
- Kickoff scheduled for May timeframe

Contact:

Dave Kuipers
INL NSTB Program Manager
Ph: 208-526-4038
Email: David.Kuipers@inl.gov