

# **OPSAID: Secure IP-Based PCS Architecture**

## **A Department of Energy National SCADA Test Bed Project**



# DOE National SCADA Test Bed

- ◆ **Joint Government - Industry Collaborative Effort**
- ◆ **Improve SCADA security in Energy Sector**
  - Per the *Roadmap to Secure Control Systems in the Energy Sector* document
- ◆ **Sandia National Laboratories**
  - Center for SCADA Security



**Sandia National Laboratories**



Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

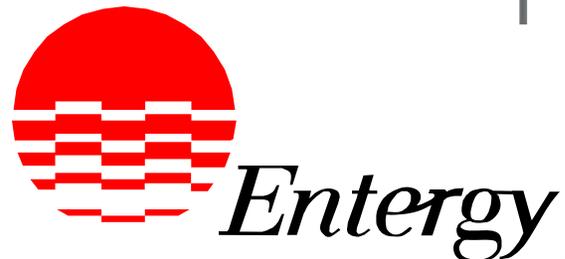




(**Open** PCS Security **Architecture** for **Interoperable**  
**Design**)

## OPSAID Industry Partners

- ◆ Entergy – 5<sup>th</sup> Largest Power Utility in US
- ◆ Teltone – Vendor, SCADA Networking
- ◆ Schweitzer Engineering Laboratories, Inc– Vendor, SCADA Networking
- ◆ Industry Panel Members



## Introducing the Panel

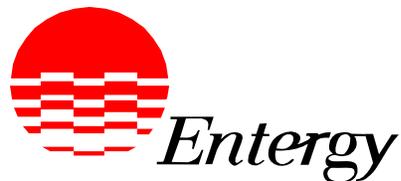
- ◆ **Dave Norton, Entergy**
- ◆ **Jason Stamp, Sandia National Laboratories**
- ◆ **Rhett Smith, Schweitzer Engineering Laboratories**
- ◆ **Ori Artman, Teltone**
- ◆ **Dave Teumim, Teumim Technical, LLC (Moderator)**

## Session Overview

- ◆ What is the problem to be solved ? (Norton)
- ◆ The solution: OPSAID (Stamp)
- ◆ Vendor participation in OPSAID (Smith, Artman)
- ◆ Audience Q & A

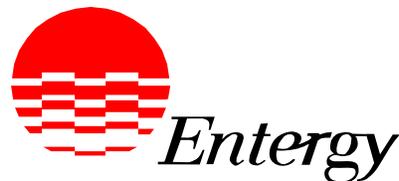
# Forces Affecting Control System End Users

- **Known threats demand secure control systems**
  - Unfriendly actors; systems run amuck; human error
  - Accordingly... Increasing sector-specific regulatory oversight
- **Need for operational “time and distance compression”**
  - Reducing Asset Management costs greatest impact to bottom line
  - “Through fault monitoring”; synchrophasor measurement; AMR
  - Distributed computing: IEC 61850 Substation automation/LAN
  - Wider access to Op and non-Op controls data for decision support
  - Remote video for both Ops and security monitoring
  - User access *from* remote field sites to info stored “anywhere”



## Forces Affecting Control System End Users

- ◆ **More interconnectedness // “situational awareness”**
  - NERCnet; NASPI; HSIN; Corporate IT; Internet... Dial-up...
  - But with only modest appreciation for CI sector interdependencies
- ◆ **“Generation gap” realities...**
  - Aging technology & work force technical skill sets
  - Just learning InfoSEC; Field IED asset management: new ballgame
  - Modernization hamstrung: IOU’s, PUC rate making; Federal law
- ◆ **Entering new vendor “gold rush” era in terms of both very new control system solutions, and, their security**



## Summary Status View from 80,000 Feet...

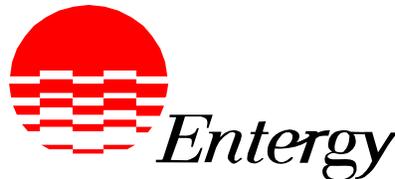
### ◆ Serial/Dial Solutions Exist // Need New IP Conventions

- New applications demand high speed and interoperability
- Regulators require 21<sup>st</sup> century CyberSEC measures
- Telecom/users want to retire vintage analog serial lines
- Link encryption can serve serial line needs until IP transition
- Dial-up: need IP infrastructure integration; key management
- Can't "IP field upgrade" old remote IED – no horsepower
- New "gateways" now in use to IP-encapsulate serial traffic
- New IP-ready IED coming to market; often COTS web based
- Vendors now *independently* implementing current COTS-based IP for host and IED alike, some with proprietary tweaks, and are rushing to market



# From This, What Can We Conclude?

- PCS not as yet IP-environs; but are moving swiftly forward with garden variety 'Internet' IP (and baggage)
- Greatest need: Next-generation PCS secure IP stack; related utilities needed to run data comm. infrastructure
- OPSAID is 1<sup>st</sup> step in a “green field” opportunity:
  - define a standards-based secure IP reference model;
  - develop tangible open-systems IP code set using open-source and public domain resources; and,
  - Make it available to PCS vendors world wide
- Fringe benefit: Eventually, can create an opportunity for cross sector controls interoperability



# Sandia Center for Control System Security and the National SCADA Test Bed

- ◆ PCS security R&D across industries
- ◆ Technology assessments
- ◆ System assessments
- ◆ Current projects:
  - Virtual Control Systems Environment
  - OPSAID
  - Security metrics
  - Threat assessment

# OPSAID Project Sandia Team

- ◆ **Jason Stamp: National SCADA Test Bed Tech Lead, Project Principal Investigator**
- ◆ **Adrian Chavez: Project Tech Lead**
- ◆ **Steve Hurd: Project Coordinator**
- ◆ **Regis Cassidy: Project Technical Development**
- ◆ **Bob Pollock: National SCADA Test Bed Lead**



# OPSAID Features and Benefits

## ◆ Need:

- Cost-effective and easy-to-implement PCS security improvements

## ◆ Approach:

- Help develop PCS security technology
- Organize an industry advisory group (including vendors and owner/operators)

## ◆ Benefits:

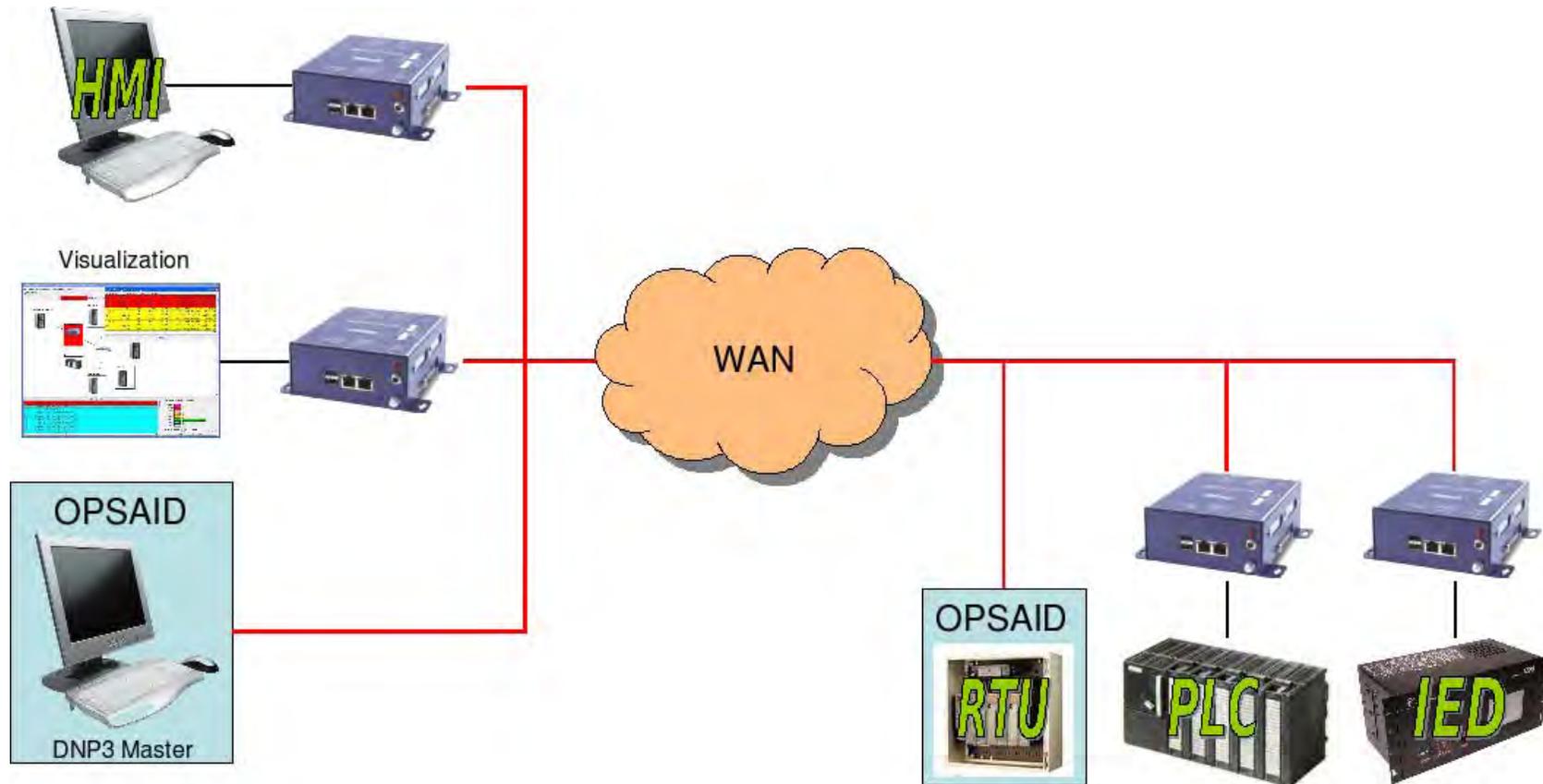
- Accelerate the availability and deployment of comprehensive security technology for PCS
- Provide building blocks to develop add-on security devices
- Define a path for the development of PCS elements with built-in security



# OPSAID Technical Approach

- ◆ **Open-source development**
  - Prefer configuration over coding
  - Royalty-free distribution
  - Strong code base leveraging Linux software
- ◆ **Design reports and specifications freely available**
- ◆ **Technology available either as modules or an entire installation profile**

# OPSAID Application



# OPSAID Progress

## ◆ Field devices:

- Key exchange and management using certificates and OCSP
- Encrypted syslog-ng security reporting
- Strongswan key exchange
- Encryption for operational communications
- Basic NIDS and HIDS
- SSH redirection to serial configuration ports
- Configuration session capture
- Reference implementation using subset of Ubuntu distribution on mini-ITX platforms



# OPSAID Progress

## ◆ Centralized repository:

- Database schema for raw field security reporting
- Second database for processed security information
- Basic, proof-of-concept implementation of security visualization

## ◆ Testing:

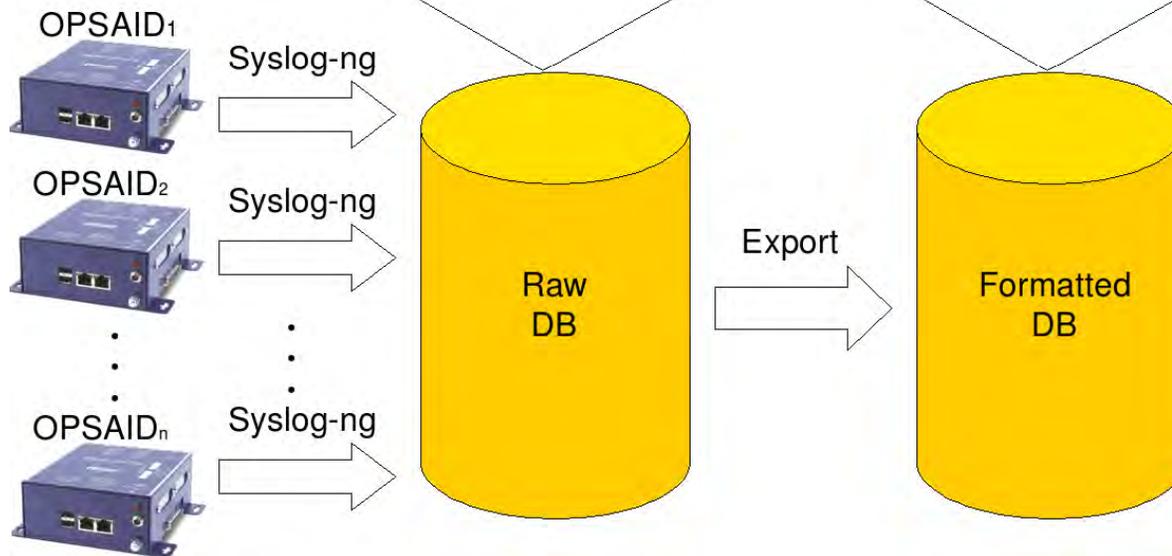
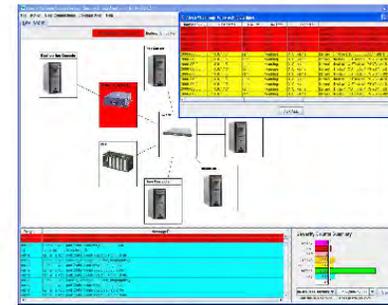
- Sandia lab testing for basic capability development
- Internet connectivity for testing between NM and CA facilities
- Lab testing at Entergy using standard industry components
- Long haul connections to SEL facilities with operational DNP3

# OPSAID Technology Applications

PHP Syslog-ng

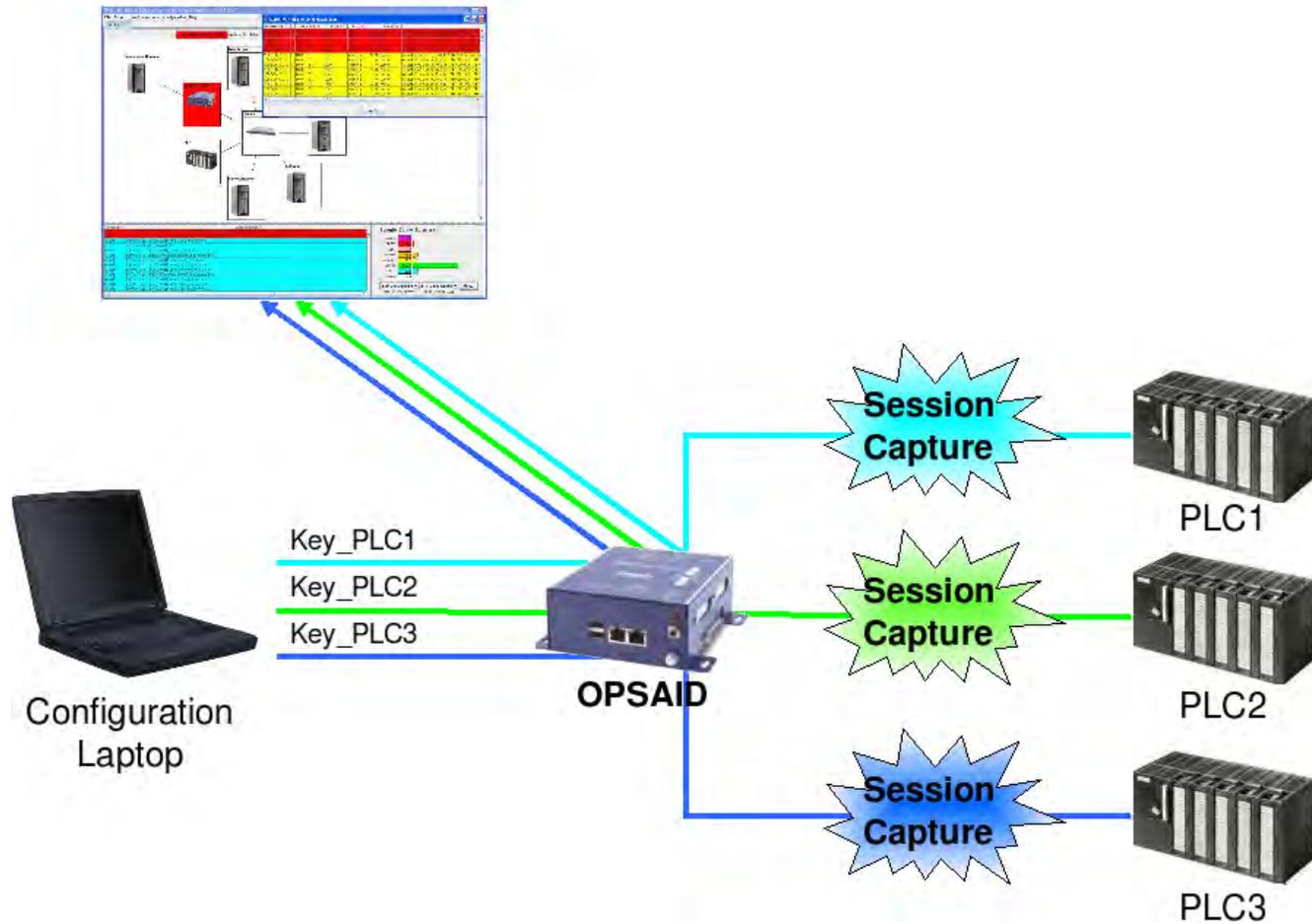
ID	HOST	PRIORITY	DATE	TIME	MESSAGE
1	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the ASP.NET (ASP) service are being assigned to this service.
2	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the IIS (IIS) service are being assigned to this service.
3	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Distributed Management and Automation (DMA) service are being assigned to this service.
4	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Remote Storage (RemoteStorage) service are being assigned to this service.
5	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Management Console (MMC) service are being assigned to this service.
6	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Distributed Transaction Coordinator (MSDTC) service are being assigned to this service.
7	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Exchange Information Store (MSExchangeIS) service are being assigned to this service.
8	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Exchange Transport (MSExchangeTransport) service are being assigned to this service.
9	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Exchange Search (MSExchangeSearch) service are being assigned to this service.
10	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Exchange Mailbox (MSExchangeMailbox) service are being assigned to this service.
11	172.19.2.29	3	2005-08-08	15:05:11	Bricklog: Performance counters for the Microsoft Exchange Mailbox Assistants (MSExchangeMailboxAssistants) service are being assigned to this service.

Network View Visualization



# OPSAID Technology Applications

Alarms Visualization



# Future OPSAID Work

- ◆ **Distribute PCS security technology**
- ◆ **Develop security capabilities currently not available**
  - PCS application proxies
  - Advanced HIDS/NIDS for PCS
- ◆ **Greater industry participation, ownership, and direction**
- ◆ **Lab and field testing with industry partners**
- ◆ **Reference implementation for interoperability testing**



# Vendor Participation



# Schweitzer Engineering Laboratories, Inc.

- **SEL:**

- Systems, Services, and Products for the Protection, Monitoring, Control, Automation, and Metering of Utility and Industrial Electric Power Systems Worldwide.
- *Our Mission...*

***Making Electric Power Safer, More Reliable,  
and More Economical®***

- **What we see on the horizon:**

- Increase in interconnected systems within and across sectors
- Heightened regulatory cyber security oversight
- Increasing need for remote management of field cyber-based assets

- **Why we are participating in OPSAID:**

- Maintain industry leadership position
- Validation on security models



# Schweitzer Engineering Laboratories, Inc.

## ◆ Participation:

- OPSAID security core uses standard security practices
- Easy qualitative testing with expert resources at Sandia
- Knowledge that our solution is interoperable

## ◆ Improvement options to OPSAID

- Easy configuration wizard
- Baseline of ACL's
- Clearly defined interoperability testing





- Who we are:
  - Teltone has been in the utility market for 12 years developing dial-up line sharing devices which are in 95% of the substations in US and Canada
- What we saw on the horizon:
  - In 2005 Teltone identified a lot of confusion in the market place. Many utilities realized that the old equipment is exposed
- Existing product for dialup line sharing and IP:
  - Jan 06 Teltone released Gauntlet, a dial-up solution for all communication within the utility with emphasis on the substation. Gauntlet was designed from the ground up to aid in NERC CIP compliance
  - In Feb 07 Teltone extended the Gauntlet to IP via partnership with RuggedCom and renamed the solution RuggedCom Gauntlet





- Why we joined OPSAID:
  - The OPSAID project offered a vehicle to use even more off the shelf software and hardware as well as leverage other vendors modules - like logs, alarms etc
  - Opportunity to team with our established customer
  - Saving on R&D expenses while expanding our product line
- Expansion in Product Line Teltone may develop OPSAID compatible modules:
  - Reporting module for activities, standards compliance etc
  - Configuration and management module
  - Generic interface - mediation services



# Benefits to Industry



## ◆ Benefits to End Users:

- Simple to integrate with existing environment
- Greater interoperability of vendor security solutions
- Industry tested approach

## ◆ Benefits to Vendors:

- Tested open security technology to adopt for your products
- Multi-vendor interoperability
- Greater customer acceptance

**Join Us !!!**



# Questions ?