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

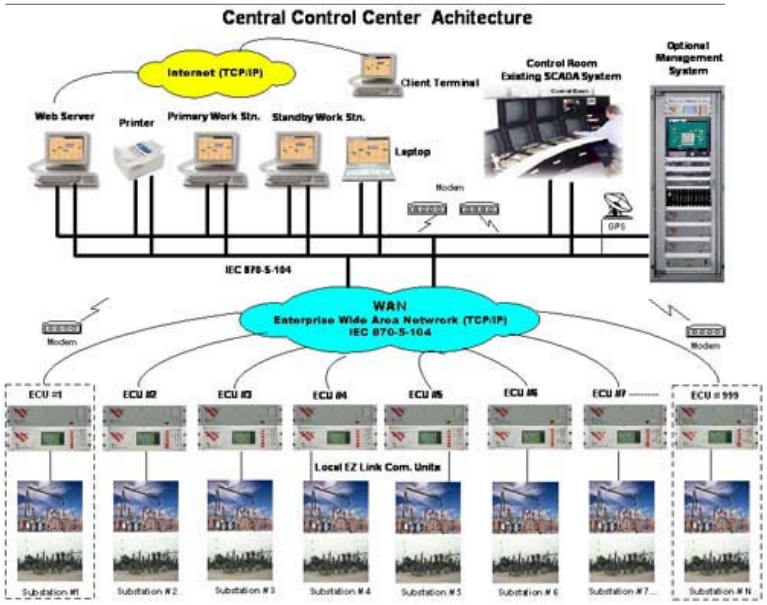
Loren Toole & Andy McCown

Los Alamos National Laboratory

Right-Sized SCADA Communications

Summary Slide: Right-Sized SCADA Communications

- **Outcomes:** Scalable, cost-effective security solutions for new architecture designs and communication methods applicable to new systems as well as legacy-system upgrades
- **Roadmap Challenge:** Limited resources available within businesses to address security needs
- **Major Successes:** End-to-end description of EP SCADA systems; survey of literature for SCADA system metrics



- **Schedule:** Detailed analysis of SCADA system 10/30/2010; System metrics 11/30/2010; Detailed specifications document 1/31/2011
- **Level of Effort:** $200K
- **Funds Remaining:** $150K
- **Performers:** LANL

Technical Approach and Feasibility

- **Approach**
  - Analyze SCADA functions and uses
  - Leverage LANL SCADA database
  - Start with substation / field / control center components; phone / radio / microwave / fiber / satellite transmission media
  - Advance to generation systems, protocols, smart metering
  - Identify metrics for SCADA system
  - Write detailed specifications document

Technical Approach and Feasibility

- **Metrics for Success**
  - Compiled list of SCADA components
  - Completion of SCADA schematic and analysis
  - Definition of metrics for SCADA system
  - Input data from suppliers on specifications/cost
  - Completion of specifications document that will feed development of cost-benefit analysis decision-support tool

Technical Approach and Feasibility

- **Challenges to Success**
  - Complexity of system
    - Break into small pieces
  - Reluctance of utilities to divulge information
    - Cultivate utility relationships
  - Complexity of developing security standards
    - Capture utilities' response and incorporate
- **Technical Achievements to Date**
  - Completion of SCADA component diagram
  - Survey of literature for SCADA system metrics

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Need cost and specification data from SCADA suppliers
  - Need utility input to scope SCADA system requirements
  - Have already developed relationships with several utilities over the years
  - Must develop relationships with SCADA suppliers
- **Plans to transfer technology/knowledge to end user**
  - End user will be SCADA system designer/developer
  - Tool will provide cost/bandwidth/security tradeoff capabilities
  - Tool will ultimately be piloted by comparison with system upgrades at local utility

Next Steps

- **Approach For Remainder FY-10 and FY-11**
  - Complete SCADA analysis
  - Finalize metric evaluation
  - Write specifications document
  - Build cost-benefit analysis decision-support tool (FY-11)
- **Potential Follow-on Work**
  - Outreach to develop large industry audience
  - Possible incorporation into other tools under development or in use

Analysis of SCADA System

- 28 SCADA functions identified in typical electric power system

SCADA Functions Listed by Electric System Level

System Level	SCADA Function
Distribution	RTU, Line switch, Throwover switch, Tie switch, IEDs, RAS, Service restorer, Line monitor
Generation	Regional interties, Capacitor bank switching, Remote load control, Cogen RTUs, Peaker telemetry, PQ control
Transmission	RTU, IEDs, Line/load monitor, Switching center functions, Protective relay
T/C	Dialup modem pool, WAN to sub-station, Substation telephone, Data warehouse, Sub-station alarms, Intertie/generation coordination, Field crew radio dispatch, Disaster communications

Abbreviations:
IED Intelligent Electrical Device; T/C Telecommunication; RTU Remote Terminal Unit; RAS Remedial Action Scheme; PQ Real/Reactive power

Analysis of SCADA System

- 10 telecom modes identified in data transfer and controls

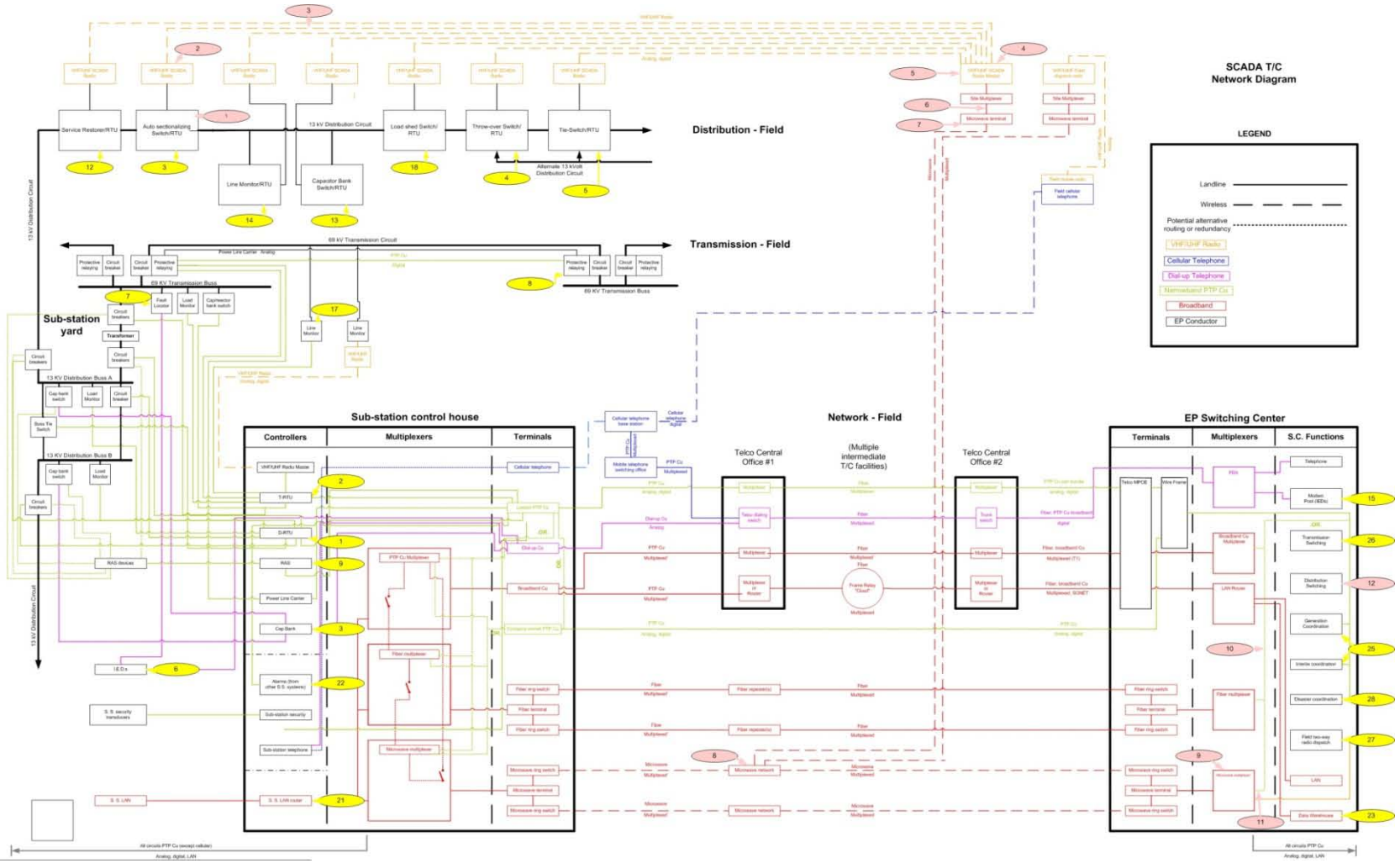
Telecommunications Modes In Use

Mode	Typical use
Broadband PTP copper	Standard upgraded phone circuits
Broadcast sub-carrier	Radio device, infrequent use for load control
Cellular phone	Expanding rapidly
Dial-up telephone	Standard dial-up service
Fiber optic	Standard broadband circuits
Microwave	Losing favor in many places as broadband circuit availability grows
Narrowband point-to-point copper	Standard direct phone circuits
Paging	Not common, but still in use – not that dissimilar to radio
VHF/UHF radio	Still fairly common in many areas – remote, low-data rates
VSAT	Satellite not common

Abbreviations:
PTP Point-to-point; UHF ultra-high frequency; VHF very-high frequency
VSAT very small aperture terminal

SCADA Component Diagram

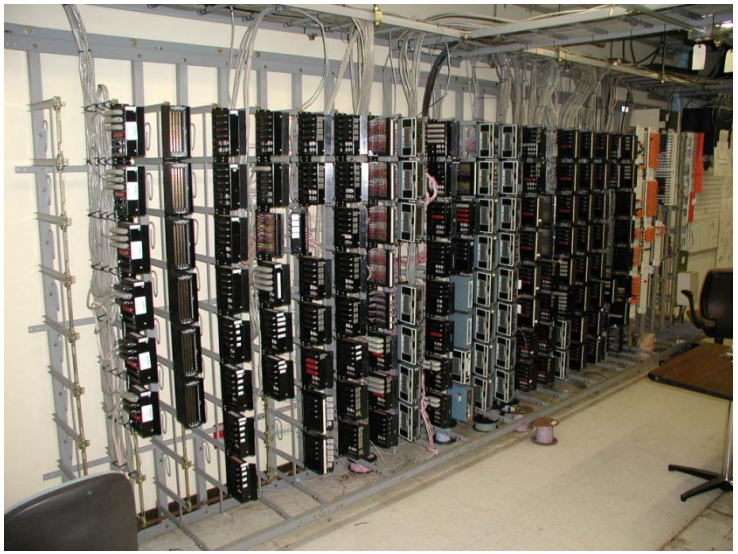
Substation components --- Field components --- Telecommunications --- Control center



Substation yard --- Substation control house --- Telecommunications --- Control center

SCADA Components

Field components with radio antennas



Plain old telephone service inside control center

Operator's console

Substation RTUs

SCADA Components Database

Current effort leverages work that was performed previously.

In-house database was designed, constructed, and populated with SCADA component data and images.