Utility SCADA & Automation

- Chris Dyer, P.E.
- BSEE University of Idaho, 1997
- POWER Engineers, Inc., SCADA and Analytical Services (SAS) Department Manager, Boise, ID
- SCADA & Automation Engineer for 17 years
What is SCADA?

- S.C.A.D.A
  - Supervisory
  - Control
  - And
  - Data
  - Acquisition
What is SCADA?

• Transmitting and receiving logic or data (telemetry)
• Monitoring of processes
• Monitoring of equipment health
• Remote control
Why SCADA?

• Ability to manage large systems efficiently
• Area control and balance
• System reconfiguration
• Automation
  – Load shedding
  – Load transfer
  – Reactive compensation
What data?

- Breaker status
- Analog data
  - Voltage
  - Current
  - Real/reactive power
  - Load tap changer position
- Critical apparatus alarms
- Controls

University of Idaho
SCADA Evolution – Early History

• Pre-SCADA
  – Limited Technology
  – Local control limiting system size
  – Manpower required
  – Coordination became difficult
  – Slow response
  – Conservative operation
  – Longer, more frequent outages
SCADA Evolution – Early History

• “Homegrown” custom
• Proprietary systems
  – Distributed
  – Energy Management Systems (EMS)
  – Remote Terminal Units (RTU)
• Discrete hardwired components
  – Auxiliary contacts, DC inputs, AC current/voltage transducers with A/D converter
SCADA Evolution – Recent History

- Open (non-proprietary) RTUs
- Local Human Machine Interface (HMI)
  - Traditional annunciator/mimic
  - PC based
  - Web based
- Communication Infrastructure owned or leased
- EMS & associated systems
- Data repository
SCADA Evolution - Communications

- 1200 baud “Bell 202” standard lease-lines
  - Low bandwidth, high availability
- Traditional serial (RS232/RS485)
- Ethernet
- Microwave (and other RF communications)
- Owned Fiber Optic Networks (OPGW)
- Leased broadband circuits
SCADA Evolution - Protocols

- Set of rules defining the exchange of information utilizing digital data transmission between intelligent devices
- Software communication “languages”
- Hardware “handshaking”
  - RTS/CTS/DSR/DTR
SCADA Evolution - Protocols

- Proprietary based on manufacturer
- MODBUS industrial communications
- DNP V3.00 developed as an “open” protocol
  - Heralded in an era of “interoperability”
- UCA
- IEC-61850
  - GOOSE
  - MMS
  - Sampled Values
OSI Seven Layer Model

The 7 Layers of OSI

Transmit

Data

User

Application layer

Presentation layer

Session layer

Transport layer

Network layer

Data link layer

Physical layer

Receive

Data

Physical Link
SCADA Evolution – Modern Era

- IED (Intelligent Electronic Device)
- Digital microprocessor relays
- Additional microprocessor based IEDs
- Moore’s Law as applied to SCADA
- Communications and database additions
SCADA Evolution – Modern Era

• Communications systems advancement
  – Broadband technologies
  – Multiplexing
  – Interoperability
• Bandwidth capabilities
• Data analytics
SCADA = Visibility
SCADA = Visibility
SCADA Evolution – The Future

• Where do we go from here?
  – “Smart Grid”
  – Data analytics & Condition based maintenance
  – IEC-61850
  – Synchrophasors
  – Cybersecurity
The Smart Grid

- Many definitions driven by marketing
- Demand side data for customer use ("smart" meters)
- Distribution Automation
  - Load transfer
  - Load shedding/recovery
  - Volt/VAR control
The Smart Grid

• Distributed Generation
  – Distribution system design
  – Protection & stability

• Digital Substation
  – “Fly by wire”
  – Networked
  – High data availability
  – Redundancy
Condition Based Maintenance

• Definition
  – Real time monitoring of apparatus
  – Evaluation of data
  – Notification
  – Automated correction

• Traditional methods
  – Time based
  – Performance based (failure)
**Condition Based Monitoring**

- **Example: Power Transformer**
  - High cost, long lead
  - IED monitoring of:
    - Dissolved gases
    - Partial discharge
    - Cooling fan operation
    - Operation & stress
  - Trend analysis
  - “Uprating”
Condition Based Monitoring

• Benefits
  – Equipment expenditures
  – Labor & resource expenditures
  – Operational data
  – Event analysis
International Electrotechnical Commission
Set of standards
– System & project management
– Engineering tools
– Data modeling
– Hardware requirements
– Product lifecycle
– Communication structure
IEC-61850 Cont’d

• Station Bus
  – SCADA Protocols (MMS)
  – Protection Protocols (GOOSE)

• Process bus
  – Measured or Sampled Values
Object oriented standard for modeling substation and apparatus

Example:

- Logic Node: Circuit Breaker (XCBR)
  - Data Object: Position (Pos)
    » Data Attributes:
      • Control type, time
      • Status
      • Operations counter
      • Quality
      • Time stamp
IEC-61850
IEC-61850

- Factors impeding adoption
  - Room for interpretation of standards
  - Complex with integration of other standards
  - Integration of different skills sets
  - Limited interoperability
  - Brownfield site complexity
  - Training
  - Testing & Commissioning
  - Documentation (logic diagrams, etc)
  - Trust & confidence

- Technology and standardization will drive the implementation
Synchrophasors

- High frequency data sampling
- Time stamped voltage & current phasor measurements
- Synchronized utilizing GPS
- Instability detection
- Post mortem sequence of events
- Potential to allow dynamic power flow monitoring
Micro-grids

• What is a Micro-grid?
• What does a Micro-grid consist of?
• How is the operation different?
• Special considerations
  – Communications
  – SCADA
Cybersecurity – The Threat

• Stuxnet virus – the danger is real
• NERC CIP-14
  – Central California physical security attack
• Recent hacks
  – Retail industry (Target)
  – Sony Studios
  – Federal government (OPM)
• Is your local utility next??

University of Idaho
Cybersecurity – Response

- NERC (North American Electric Reliability Corporation)
- CIP (Critical Infrastructure Protection)
- Reliability & security
- Critical Assets Definition
- Compliance & penalties
Cybersecurity – Actions

• Policies & procedures
• Training
• Situational awareness
• Configuration management
• Monitor & detection
• Response and recovery
Substation of the future??
Questions?

- Thanks for your attention.
  – Chris