SCADA System

TCIPG RG 1
SCADA: Supervisory Control and Data Acquisition
The SCADA system monitors and {automatically or manually} controls the an industrial process.
Types of Processes

• Power generation and transmission
• Oil and Gas
• Air traffic and railways
• Water management
• Manufacturing
In real life SCADA controls...

• The power in your home
• The water in your home
• Where the water goes from your home
• The traffic lights on the way to the office
• The commuter train controls
• The air conditioning system in your office building
• The phone system to your home
SCADA topology

OpenControl SCADA Network Architecture
Another Example
Human-Machine Interface (HMI)
Power Utility
Protocols Used

• Raw binary protocols
  – DNP3 and modbus
  – Designed for serial links
  – Reads data and sends commands and alerts

• High-level data protocols
  – ICCP
  – Uses XML for communication
  – Human readable
DNP3

DNP 3.0 Application Layer message (12 bytes)
Security Issues

• SCADA does not authenticate users or devices
  – All SCADA protocols do not implement authentication. Trust assumption

• Patching is really hard
  – Devices have to be taken offline for patching

• Believe they are not connected
  – Laptops roam around (WiFi)
  – Ex. Historians are a possible leak

• Old Modems
SCADA Functions in Power Systems

• Another commonly used term is energy management system (EMS), which is a broader concept.
  – An energy management system (EMS) is a system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system.
  – The monitor and control functions are known as SCADA; the optimization packages are often referred to as "advanced applications". They are closely related.
SCADA: Monitoring

- State estimation is the core
State Estimation

- Typical measurements used for state estimation:
  - Real and reactive power flows on the lines; Bus voltage magnitudes at generation;
  - Transformer tap settings; Real and reactive power loads at load buses;
- System state
  - Voltage magnitude and angle
- Example:
  - 21 measurements,
  - 7 state variables
State Estimation

• Basic assumption
  – Power system is in the quasi-steady-state condition

• Problem formulation
  \[ z = h(x) + \nu \]  
  Power flow equations

• Estimation method
  – weighted least-squares (WLS) estimation

• Security consideration
  – bad data detection (incorporation of PMU data)
SCADA: Control

- In EMS, the time hierarchy for operations and control decisions

<table>
<thead>
<tr>
<th>Time Scale</th>
<th>Load Variations</th>
<th>Function in EMS</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>small, random</td>
<td>automatic control</td>
<td>Match the on-line generation with the load</td>
</tr>
<tr>
<td>minutes</td>
<td>large</td>
<td>economic dispatch</td>
<td>Allocate economically load among the committed generating units</td>
</tr>
<tr>
<td>days and hours</td>
<td>wide</td>
<td>unit commitment</td>
<td>Start-up and shutdown of units</td>
</tr>
<tr>
<td>weeks</td>
<td>very wide swings</td>
<td>Fuel, hydro, and maintenance scheduling</td>
<td>Meet load with the installed resource mix</td>
</tr>
</tbody>
</table>
SCADA: Control

• SCADA control mechanisms:
  – Voltage control:
    • Var compensation, in-phase transformer tap settings
  – Frequency control: AGC
  – Topology change: line switching
  – Load shedding: the last resort
  – Protection device (e.g., relays) parameter setting

• Security consideration:
  – The impact of malicious control command is hard to evaluate.