History, Evolution, and Future of the Substation RTU

Mark Peterson, PE
GE Technical Application Engineer

Power & Energy Conference - 2020
Biggest Machine on Earth

America’s Power System:

- 10,000 power plants
- Half a million miles of transmission
- Millions of miles of distribution
- 55,000 substations
Biggest Machine on Earth

The goal is to optimize the power production and delivery process.

The collection, secure transfer, and analysis of end-to-end system information is required in order to achieve that goal.
SCADA

- Supervisory Control and Data Acquisition

- Purpose of SCADA
  - Process optimization
  - System situational awareness
  - System control
  - Without it, essentially running blind, must rely upon:
    - Dispatched workers
    - Staffed substations
    - Phone call reporting
Healthcare Analogy

Monitor: Critical Real Time Data

Frequency: Constant/Short Interval

Actions: Immediate

Goal: Keep Patient Alive

Emergency Room
Power Production/Delivery System

Energy Management System

Monitor: Critical Real Time Data

Frequency: Constant/Short Interval

Actions: Immediate

Goal: Keep System Alive and Operational
SCADA History (Early to Mid 1900’s)

• Power plant control rooms were first “control centers”
  – Extended to nearby substations for SCADA functionality
  – Directly-connected data sources
    – Device contacts
    – Electromechanical meters
    – Transducers
SCADA History (Early to Mid 1900’s)

- Power plant control rooms were first “control centers”
  - Essentially extended instrumentation
  - Dedicated discrete data indication and display board
    - Meters
    - Lamps
SCADA History (Early to Mid 1900’s)

- Extended instrumentation impractical for distant stations
- Alternative manual methods
  - Staffed stations
  - On-call local area workers
  - Public
- Progressive application of telemetry
  - Simple schemes
  - Limited to crucial data
SCADA History (1960’s -1970’s)

- SCADA acronym came into use
- Early implementation
  - Field devices, predominantly at subs
  - Remote Data Equipment (RDE)
    - Standalone, independent
    - Dedicated function
    - Perform data acquisition
    - Execute control actions
SCADA History (1960’s - 1970’s)

• Remote Data Equipment (RDE)
  – Hardware
    – Discrete electronics
    – Hardware based logic
    – Often wire-wound connections
    – Multiple large low-density PCBs
    – Common card-cage format
SCADA History (1960’s - 1970’s)

• Hard IO
  – Card based
  – Local to RDE
  – Low-level analog inputs (AIs)
    – Typically +/- 1mA transducer
  – Status inputs (DIs)
    – Typically equipment contacts
  – Control outputs (DOs)
SCADA History (1960’s - 1970’s)
SCADA History (1960’s -1970’s)

- Energy Management System (EMS) master
  - Computer / data processor
  - Communications processor
    - Communication with system devices
    - Protocol / language
  - Simple limited interface
  - Modifiable display board
  - Highly dependent on local area workers
SCADA History (1960’s -1970’s)

• Communications
  – Protocol / language
    – Move data
    – Typically poll-response scheme
    – Optimize bandwidth usage
    – Minimize impact on processor and memory

    – Typically RDE and Master sourced from common vendor and utilized proprietary vendor-specific protocol, e.g. Conitel, CDC, Telegyr
    – Near zero concern for interoperability
    – Bit and byte orientations
    – Often hardware-associated
SCADA History (1960’s - 1970’s)

- Often hardware-associated
  - Message segments match hardware I/O cards
  - e.g. Leeds & Northrup RDE – Conitel protocol

<table>
<thead>
<tr>
<th>MSB</th>
<th>INFORMATION SECTION A</th>
<th>A</th>
<th>INFORMATION SECTION B</th>
<th>B</th>
<th>BCH</th>
<th>EOM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>13</td>
<td></td>
<td>26</td>
<td>27-31</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14</td>
<td></td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td>25</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SCADA History (1960’s - 1970’s)

- Communications Media
  - 4-wire leased party phone lines
  - Microwave
  - Radios
  - Typically FSK via 1200 baud modem
**SCADA History (1980’s - 1990’s)**

- Remote Terminal Unit (RTU)
  - Microprocessor based
  - Firmware based logic and processing
  - Implement advanced functionality
    - PLC, multiple master support, calculator, etc.
  - Communications to Master
    - Leased phone lines
    - Microwave
    - Radio, licensed and spread spectrum
    - Fiber, mostly multiplexed serial channels
SCADA History (1980’s - 1990’s)

- IO
  - Predominantly local hard IO
  - Distributed IO for large stations

- Utilize data in IEDs
  - Meters
  - Relays
  - Controls (e.g. LTC, regulator, etc.)

- Communications media to IEDs:
  - RS232 serial
  - RS485 serial
  - Some fiber serial
  - Some Ethernet, copper and fiber
SCADA History (1980’s - 1990’s)

- Communication Protocols
  - Vendors started to emulate other vendors’ protocols
    - Eliminated vendor hardware limitations
    - Increased competition
  - Westronic created DNP protocol
    - Interoperable
    - Critical need for RTU-to-IED comms
    - Publicly released to DNP Users Group
    - Industry game changer
SCADA History (1980’s -1990’s)

• **Energy Management System (EMS) master**
  – Increased processor and memory
  – More remote stations monitored
  – **Advanced Graphical User Interface (GUI) display board**
    – CRT
    – Projection
SCADA Recent Evolution (00’s-Present)

- Energy Management System (EMS) master
  - Many continued to utilize vendor-specific protocols
  - Progressively implemented DNP
  - Implemented advanced functionality
    - Load control
    - State estimators
SCADA Recent Evolution (00’s-Present)

• Energy Management System (EMS) master
  – GUI
SCADA Recent Evolution

- Remote Terminal Unit (RTU)
  - Moved toward substation Gateway design/concept
    - Hard IO agnostic - Use IED data or 3rd party IO modules
    - Data primarily sourced from IEDs
      - Operational real time data
      - Classic status and analog values
      - Non-operational data
        - Events
        - Logs
  - Communications media
    - Move to more Ethernet – copper and fiber
SCADA Recent Evolution

- Substation Gateway
SCADA Recent Evolution

- Substation Gateway
  - Communications Protocols
    - Evolution of interoperable protocols
    - DNP additions
    - UCA evolution to, and development of IEC 61850
      - Specifies how data shall be moved
      - Manufacturing Message Specification (MMS)
        - Client/Server scheme
      - Generic Object Oriented Substation Event (GOOSE)
        - Publisher/Subscriber scheme
SCADA Recent Evolution

• Substation Gateway

  – Communications
    – Drastic reduction in bandwidth constraints
      – Serial: 1200 baud to 56 kbaud channels
      – LAN: 1MB to 1GB
      – Frame relay, SONET, MPLS, etc.
    – Drastic reduction of communication costs
      – Standards such as Ethernet and TCP/IP
      – Explosion of communications market
      – Advances in hardware capabilities
SCADA Recent Evolution

- Multiple Functions on Common Platform

**Advanced Gateway**
Data collection from substation IEDs for control & secure monitoring

**Advanced Automation**
Automate substation procedures using IEC 61131 compliant tools

**Fault Recording & Data Logging and File Retrieval**
Extract valuable data such as digital fault records and event files

**Embedded HMI**
Customizable local or remote HMI with multiple windows

**Secure Remote Access**
Securely access substation device locally and remotely

**Redundancy**
Hot & Warm-standby, PRP and HSR
SCADA Future

- Impacts of technology
  - Wide variety of communications technologies available
  - Bandwidth costs no longer the driver they used to be
  - Greater system and device intelligence and need for situational awareness requires:
    - More points to be monitored and reported
    - More data to be obtained and processed
    - Increased complexity in applications
    - Focus is shifting from data acquisition to data management
SCADA Future

• Focus shifting from data acquisition to data management

  – Manage huge amounts of data and datasets
  – Configuration of devices and applications
  – Maintenance of devices and applications
  – Updating devices
  – Securing devices and configurations

  – These will be the main cost drivers
SCADA Future

• Impacts of technology
  – Application of data analysis tools
  – Process boatloads of data into information
  – Mine data for useful information
  – Efficient reporting of data to those who need it
SCADA Future

• Data Management
  – Higher commissioning costs
  – More applications accessing data
  – Deregulation adds complexity due to increased sharing
SCADA Future

• Traditional SCADA data management
  – Goal was to move points with minimal overhead
  – Meanings of points maintained in multiple places
    – Configuration of RTU and IEDs
    – Configuration of databases
    – Configuration of applications
    – Protocols were primarily register based
SCADA Future

- Traditional SCADA data management
  - Validation is costly and time consuming
  - e.g. Move point 3851 from source to multiple destinations
    - People need to manage and validate that point
    - Expensive effort
SCADA Future

• Communication and Data Management Trends
  – Industries moving toward Object-Oriented protocols
    – Data organized by function
    – Simplifies distributed applications and their management
    – Standardized objects for interoperability
    – Self-description and Meta-Data allow for online validation
      – Objects aren’t just bytes of data but also descriptions
    – Bandwidth is the tradeoff
      – Connecting applications to data is bigger effort/obstacle than the bandwidth to move it
SCADA Future

- Modern Object-Oriented Protocols

  - Goal: Reduce data management while maintaining high integrity and reliability
  - IEC 61850 standard objectives
    - Address data management costs via modern communication techniques
    - High degree of interoperability via standard objects
    - Simplify config effort via common config language
    - On-line validation of comm via Meta-Data and self-description
SCADA Future

• Scope of IEC 61850
  – Much broader than traditional protocols
  – Multiple protocols
    – GOOSE, MMS, Sampled values
  – Standardized configuration language
    – SCL - Substation Configuration Language
    – XML - Extensible Markup Language
  – Standard and extensible objects
    – Naming
    – Data types
SCADA Future

```xml
<?xml version="1.0"?>
  <Header id="GE" version="0" revision="1" toolID="DAPStudio" nameStructure="IEDName" />
  <Communication>
    <SubNetwork name="IOLAN">
      <ConnectedAP iedName="IED9" apName="AccessPoint5">
        <Address>
          <P type="IP">0.0.0.0</P>
          <P type="IP-SUBNET">255.255.255.0</P>
          <P type="IP-GATEWAY">0.0.0.0</P>
        </Address>
      </ConnectedAP>
    </SubNetwork>
  </Communication>
  <IED name="IED9">
    <AccessPoint name="AccessPoint5" router="false" clock="false">
      <Server timeout="30">
        <Authentication none="true" password="false" weak="false" strong="false" certificate="false" />
        <LDevice inst="TransfixA">
          <LN0 lnType="DAP_LLNO" lnClass="LLNO" inst=""/>
          <DataSet name="DataSet1">
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="Tmp" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="H2O" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="H2ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="N2ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="COppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="CO2ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="CH4ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="C2H2ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="C2H4ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="C2H6ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="O2ppm" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="1" doName="CmbuGas" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="2" doName="Tmp" fc="MX"/>
            <FCDA ldInst="TransfixA" prefix="" lnClass="SIML" lnInst="2" doName="H2O" fc="MX"/>
          </DataSet>
        </LDevice>
      </Server>
    </AccessPoint>
  </IED>
</SCL>
```
SCADA Future

- **Gateway Evolution**
  - Advanced Functionality
  - Time synchronization and distribution: IRIG-B, SNTP, PRP
  - Programmable logic
  - Non-operational file gathering and reporting

- **Processing platform**
  - Virtual machines
  - Multiple OS environment
  - Container based technology
SCADA Future

- Security
  - Secure perimeter access point and gateway
  - Authentication, authorization, and audit trails
  - Password management
  - Firmware management
  - Remote tunneling (pass-through) connection to IEDs
  - Automated retrieval and reporting
Summary

• Substation RTU
  – Moving toward multifunction gateway platform

• Substation Data
  – Volume will increase, primarily non-operational data
  – Efficient, reliable, and secure management of data will be main objectives
Summary

• Communications
  – Industry is moving toward object-oriented communications and protocols
  – Interoperability, validation, self-identification will be key objectives

• Cybersecurity
  – Critical infrastructure protection will be crucial focus
  – Authentication, authorization, and audit trails
  – Compliance with mandates from governing bodies