History, and Evolution of SCADA

Origin and Purpose of SCADA


One of the
Biggest Machine on Earth - America's Power System
10,000
Power Plants
½ Million
Miles of Transmission
Millions
Of miles of distribution
55,000
Substations

Biggest Machine on Earth

Goal is to **optimize the power production and delivery process**

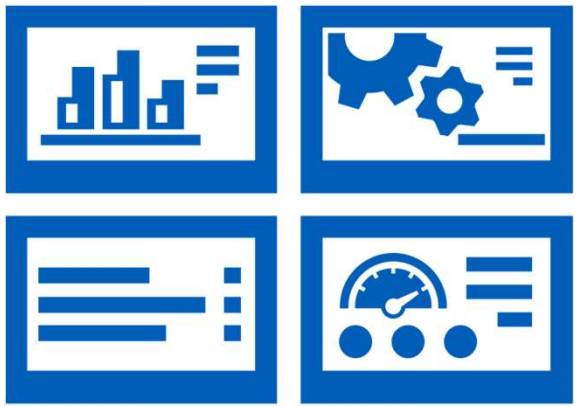
The collection, secure transfer, and analysis of end-to-end system information is required in order to achieve that goal

SCADA: Supervisory Control and Data Acquisition

TECHTALK

Purpose of SCADA

- Process optimization
- System situational awareness
- System control
- Without it, essentially running blind



System state knowledge is crucial

Healthcare Analogy – Wellness Care

Monitor

Various real and long-term data

Weight, heart rate, insulin level

Frequency

Periodically, relatively long interval

As reasonable, appropriate and directed

Event based

Goal: Find and correct health issues

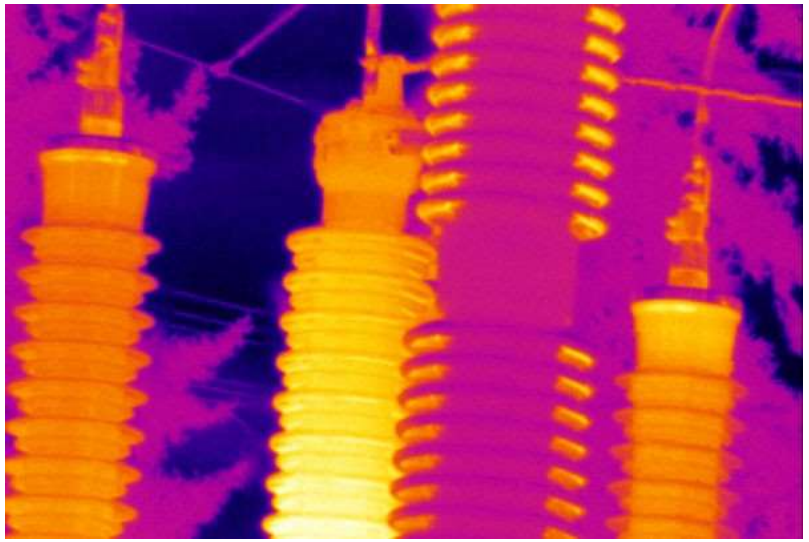
Maintain and optimize health

Power Production/Delivery System – Maintenance

Monitor

Various real and long-term data

Temperature, power, gas concentration



Frequency

Periodically, relatively long interval

As reasonable, appropriate and directed

Event based

Goal: Find and correct issues

Maintain and optimize system health

Healthcare Analogy – Emergency Room

Monitor
Critical real-time data
Heart rate, blood pressure, breathing rate

Frequency
Constant, short Interval

Actions: Immediate

Goal: Keep patient alive

Power Production/Delivery System - SCADA

Monitor

Critical real-time data

Volts, amps, power, loads

Generation availability, breaker statuses

Frequency

Constant, short Interval

Actions: Immediate

Goal: Keep system alive and operational

Initial Implementations: Early to mid-1900s

Power Plant Control Room

Power plant control rooms were first “control centers”

Extended to nearby substations for SCADA functionality

- Directly-connected data sources
- Device contacts
- Electromechanical meters

Moran Generating Station
Courtesy of the Burlington Electric Department
Burlington, Vermont

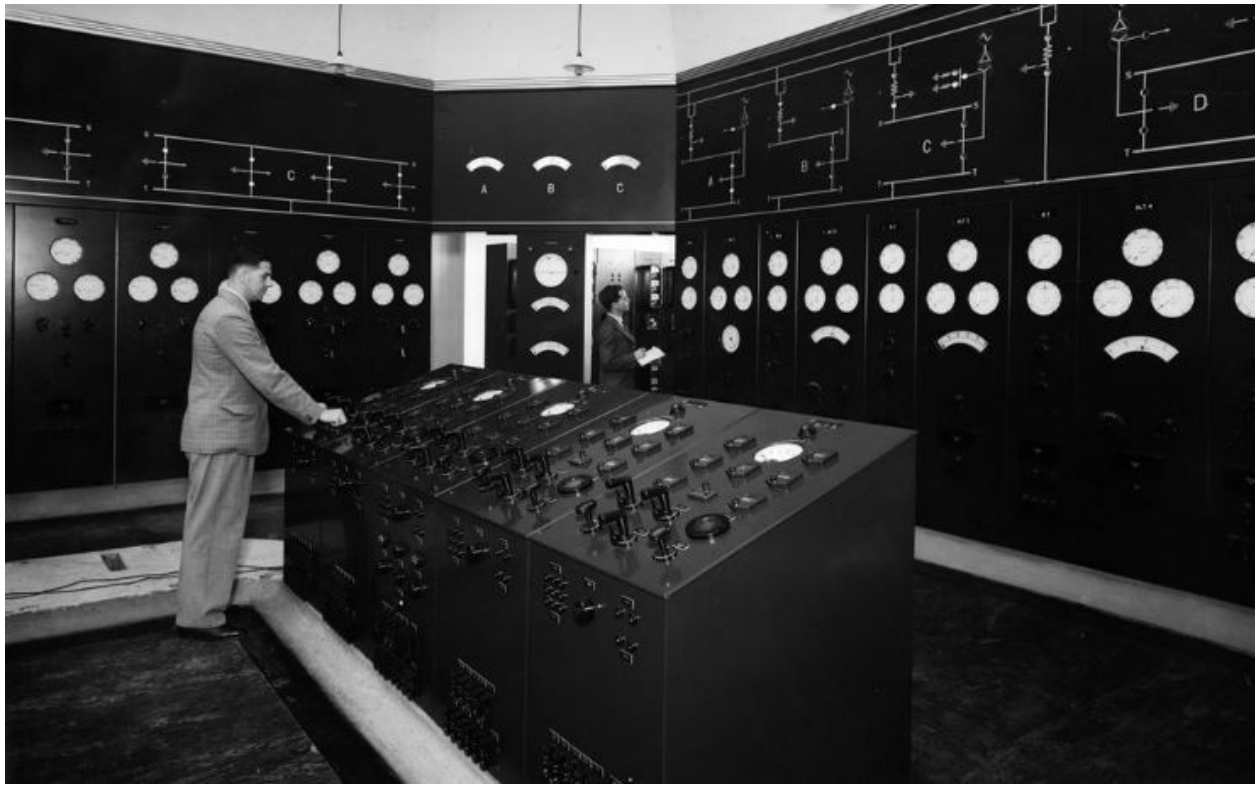
State knowledge limited to immediate facilities

Power Plant Control Room

Power plant control rooms were first “control centers”

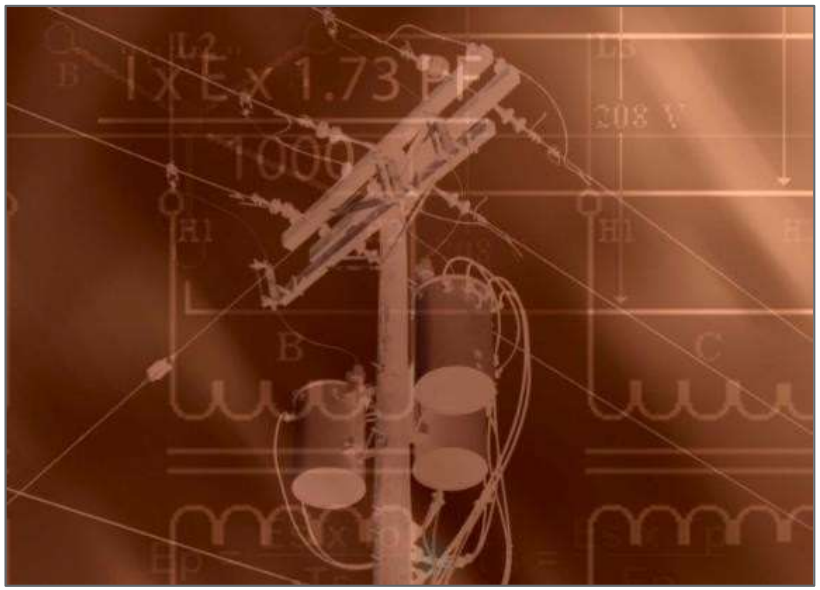
Essentially extended instrumentation

- Dedicated discrete data indication and display board
- Meters
- Lamps



Sources and Provision of Data

- 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



Electronic-Based Systems: 1960s-1970s

Supervisory Control and Data Collection

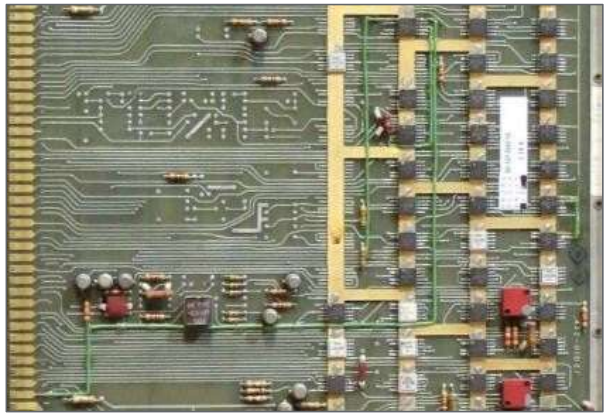
- SCADA acronym came into use
- Early implementation
  - Field devices, predominantly at subs
  - Remote data equipment (RDE)
    - Standalone, independent
    - Dedicated function
    - Perform data acquisition
    - Execute control actions

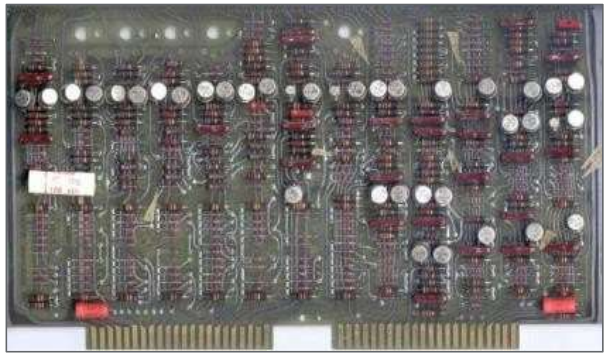
Remote Data Equipment (RDE)

TECHTALK

Hardware

- Discrete electronics
- Hardware-based logic
- Often wire-wound connections
- Multiple large low-density PCBs
- Common card-cage format





Local Input/Output (I/O)

Hard IO

- Card-based
- Local to RDE
- Low-level analog inputs (AIs), typically +/- 1mA transducer
- Status inputs (DIs), typically equipment contacts
- Control outputs (DOs)

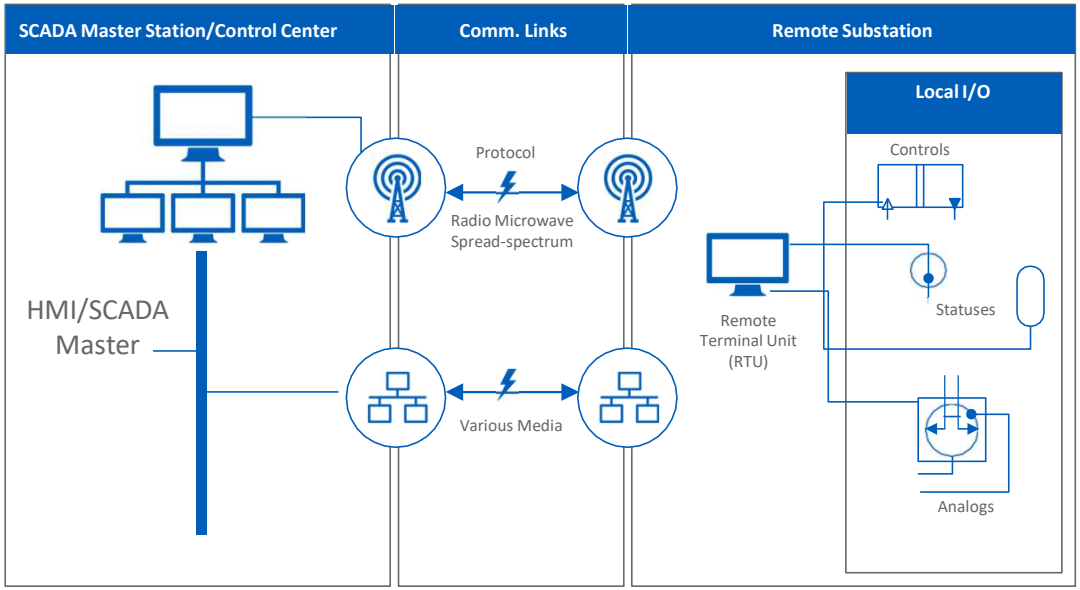
Energy Management System (EMS) Master

- Computer / data processor
  - Communications processor
  - Communication with system devices
- Protocol / language
- Simple limited interface

Orpheum Electric building
Courtesy of Iowa Electric
Sioux City, Iowa

Master-to-RDE Communications

- Objectives
  - Move data
  - Optimize bandwidth usage
  - Minimize impact on processor and memory
- RDE and master sourced from common vendor using proprietary vendor-specific protocol, e.g., Conitel, CDC, Telegyr
- Near-zero concern for interoperability
- Protocol / language
  - Poll-response scheme
  - Bit and byte orientations
  - Often hardware-associated



Protocol Hardware Association

Message segments match hardware I/O cards

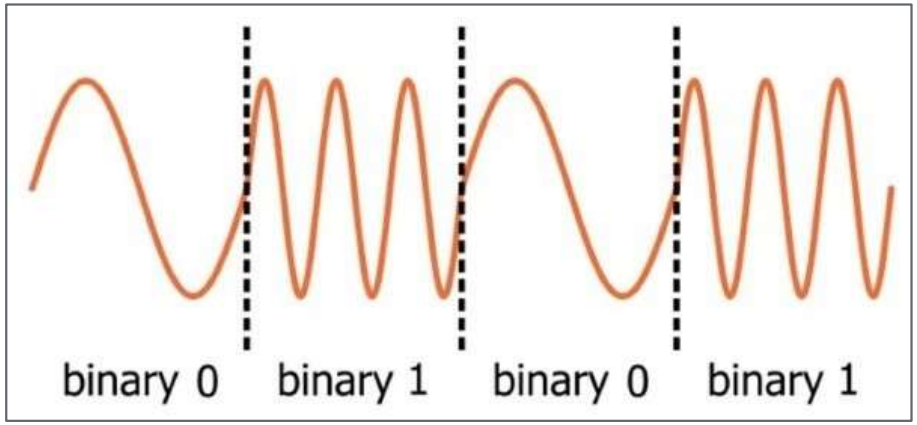
e.g., Leeds & Northrup Conitel protocol

MSB LSB

INFORMATION SECTION A	A	INFORMATION SECTION B	B	BCH	EOM
1 ---------- 12	13	14 ---------- 25	26	27-31	32

Communications Media

- 4-wire leased party phone lines
- Microwave
- Radios
- Typically FSK via 1200 baud modem



Microprocessor-Based Systems: 1980s-1990s

Remote Terminal Unit (RTU)

TECHTALK

- Microprocessor-based
- Firmware based logic and processing
- Implemented 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

I/O and Local Communication

TECHTALK

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

Communication Protocols

- Vendors started to emulate other vendors' protocols
  - Meters
  - Relays
  - Controls (e.g., LTC, regulator, etc.)
- Westronic created DNP protocol
  - Interoperable
  - Critical need for RTU-to-IED comms
  - Publicly released to DNP Users Group
  - Industry game changer

TECHTALK

dnp
Distributed
Network
Protocol

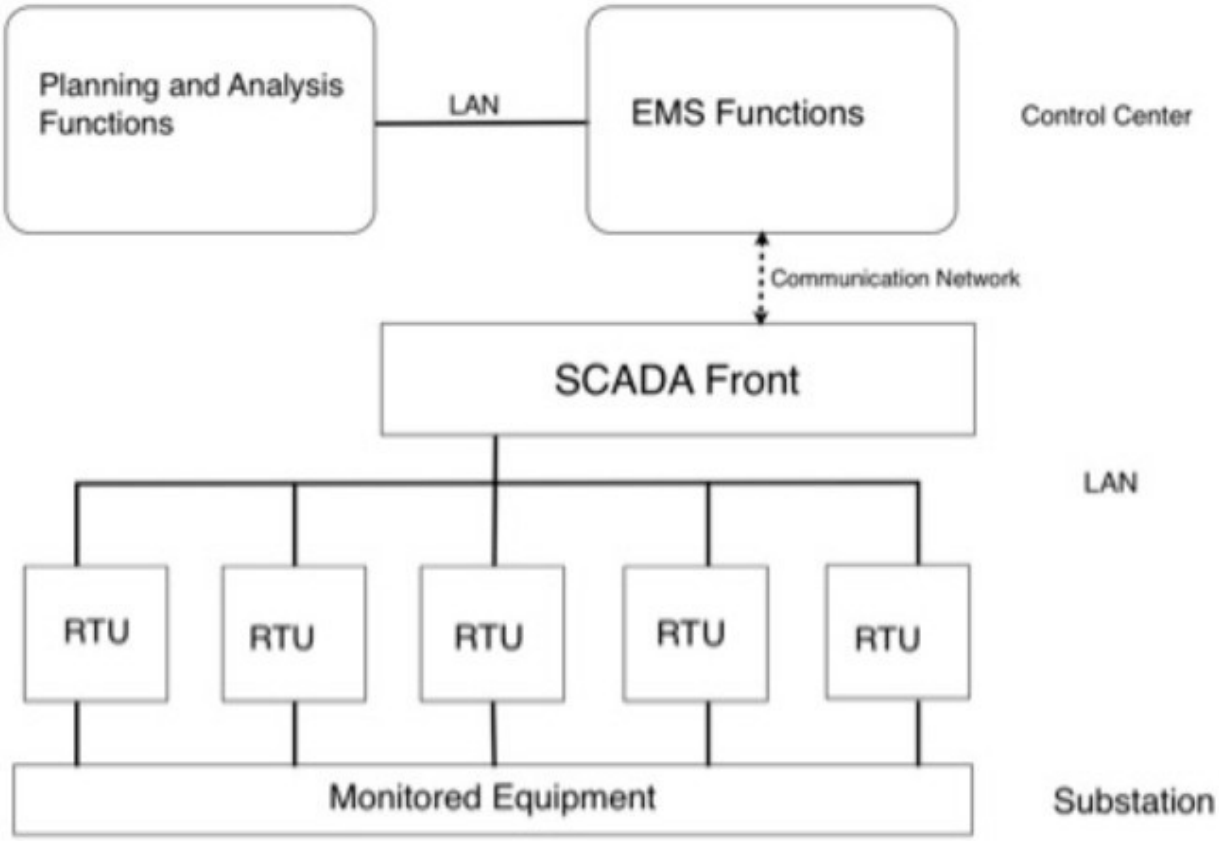
Energy Management System Master

- Increased processor and memory
- More remote stations monitored
- Advanced graphical user interface (GUI) display board
  - CRT
  - Projection

Current Systems of the 2000s-2010s and the Migration to Multifunction Gateways

Energy Management System Master

- Many continued to utilize vendor-specific protocols
- Implemented advanced functionality
  - Load control
  - State estimators



Energy Management System Master

TECHTALK

- Advanced Graphical User Interface (GUI)

Remote Terminal Unit (RTU) / Gateway

TECHTALK

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

Gateway Multifunctionally

TECHTALK

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

Embedded HMI
Customizable local or remote HMI with multiple windows

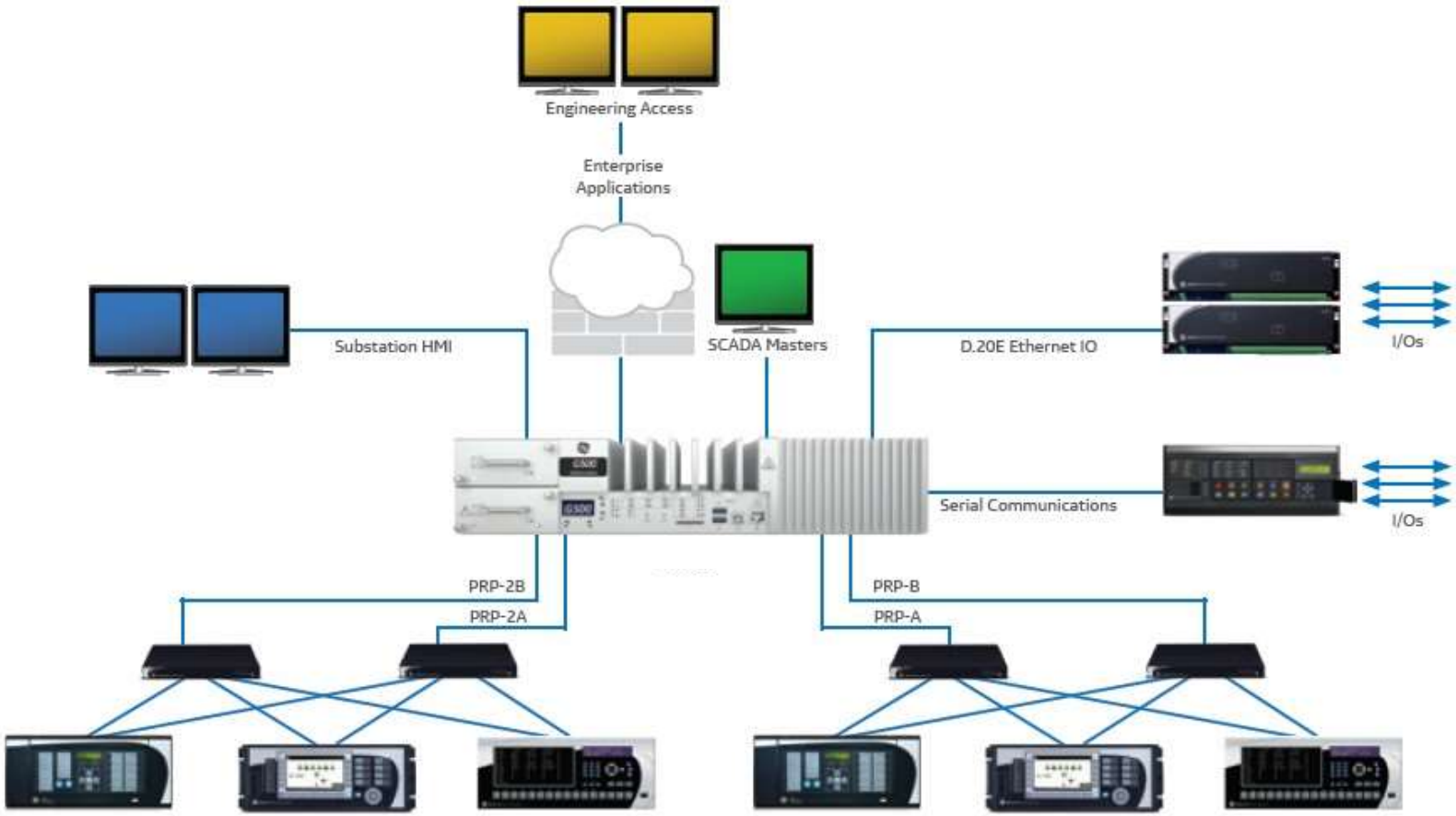
Advanced Automation
Automate substation procedures using IEC 61131 compliant tools

Secure Remote Access
Securely access substation device locally and remotely

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

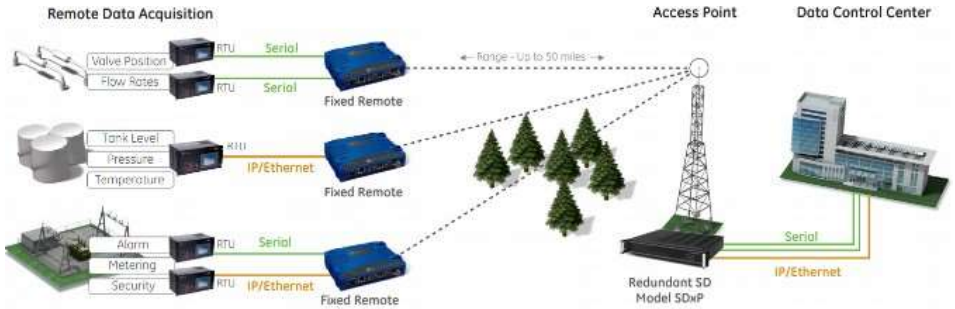
Redundancy
Hot & Warm-standby, PRP and HSR

Gateway Multifunctionally



Communications Media

- 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



Communications Protocols

TECHTALK

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

Future Implementations and Direction of SCADA

Impacts of Technology

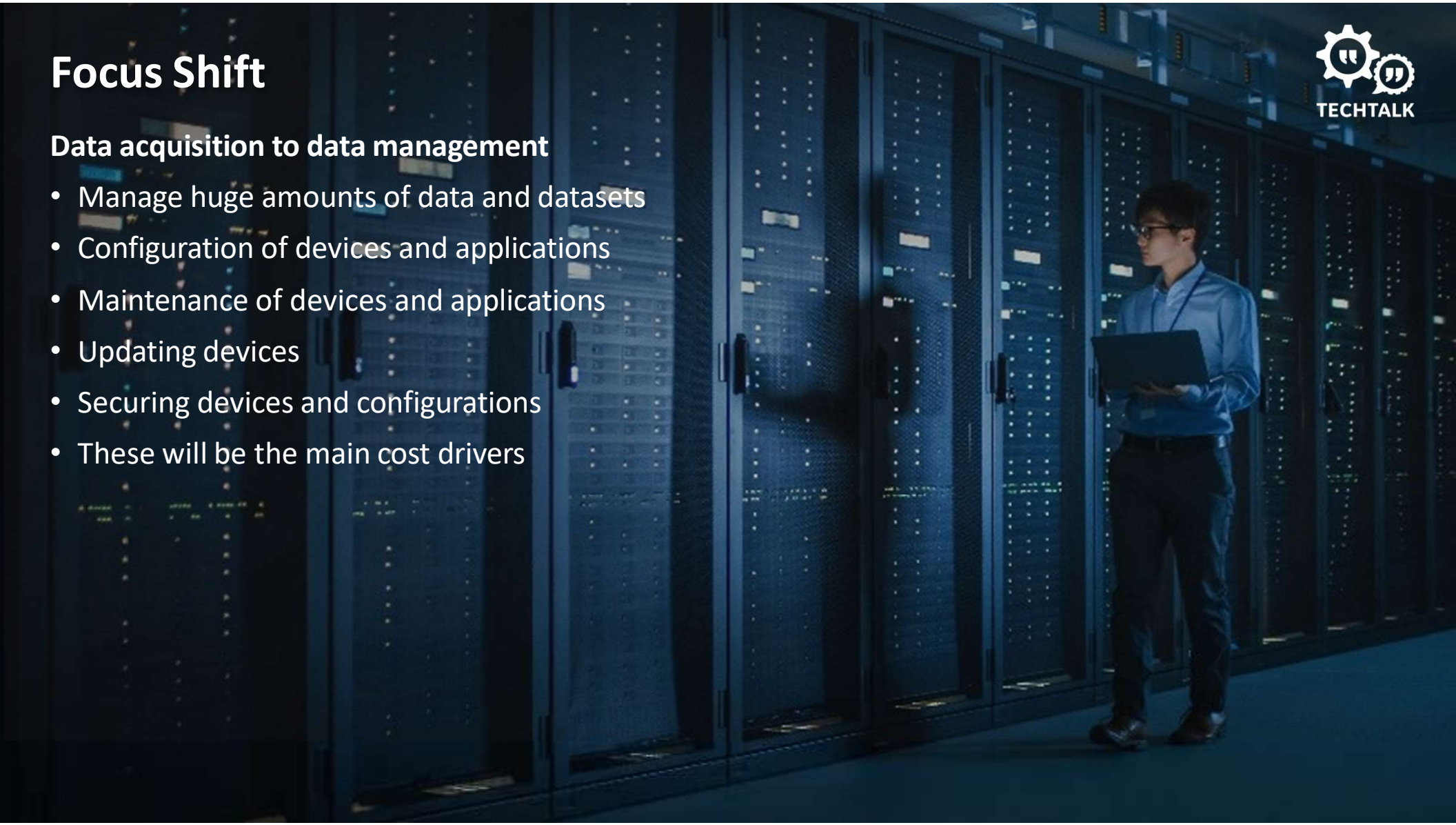
TECHTALK

- 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

Focus Shift

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



Impacts of Technology

TECHTALK

Application of data analysis tools

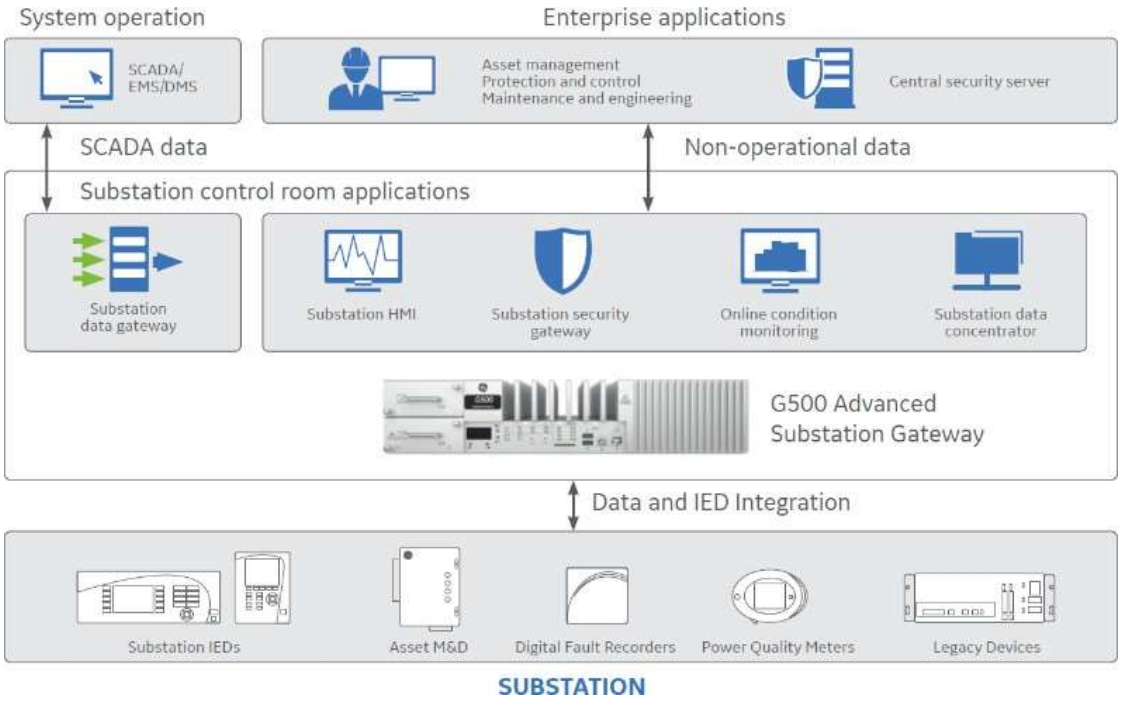
- Processing boatloads of data into information
- Mining data for useful information
- Efficient reporting of data to those who need it

Data Management

- Higher commissioning costs
- More applications accessing data
- Deregulation adds complexity due to increased sharing

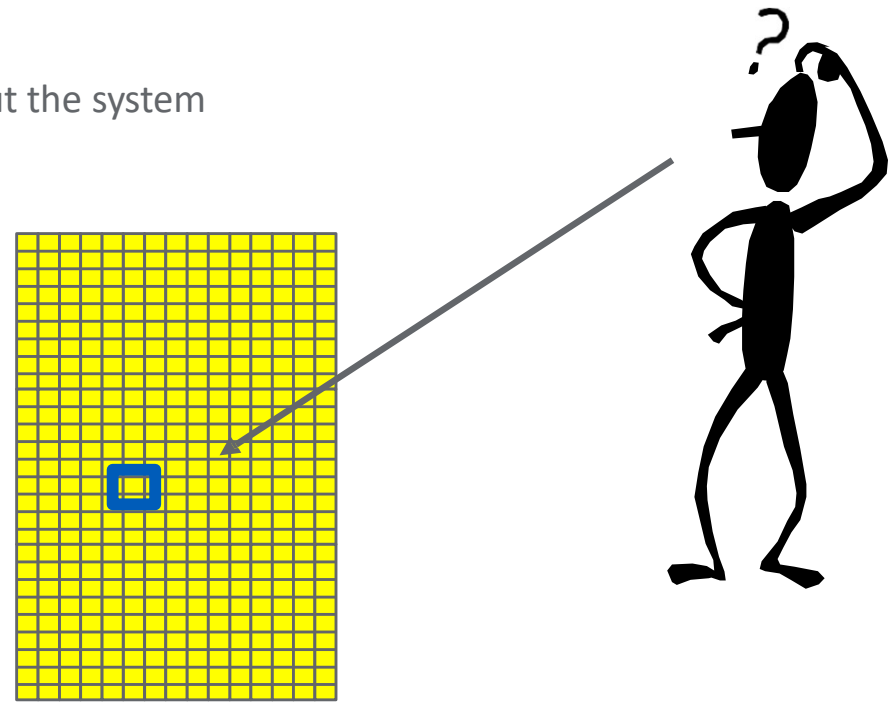
Traditional SCADA Data Management

- Meanings of points maintained in multiple places
- Configuration of RTU and IEDs
  - Configuration of databases
  - Configuration of applications
  - Protocols were primarily register based



Traditional SCADA Data Management

- Validation is costly and time consuming
- Example: Move point 3851 from its source to multiple destinations
  - The point is referenced by its stack location
  - A meaning must be assigned to the point
  - The meaning must be consistent and tracked throughout the system
  - The point must be manually managed and validated
  - The effort is complex and expensive



Communication and Data Management Trends

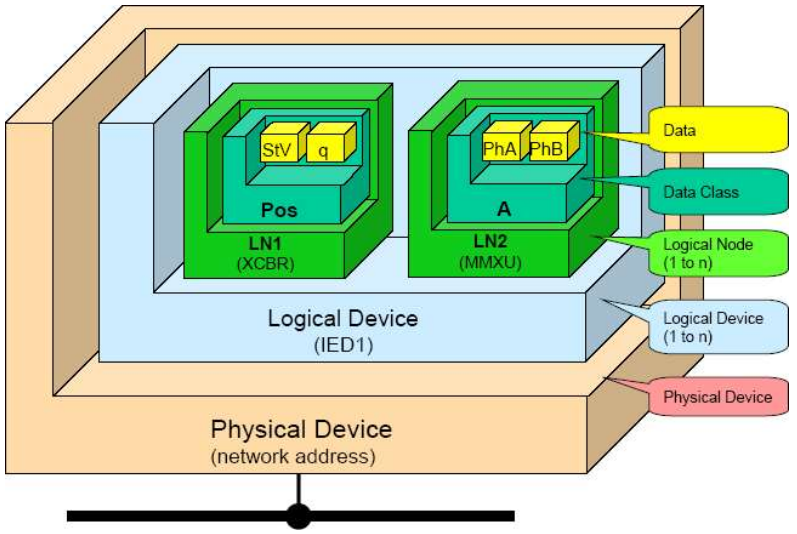
TECHTALK

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

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 metadata and self-description



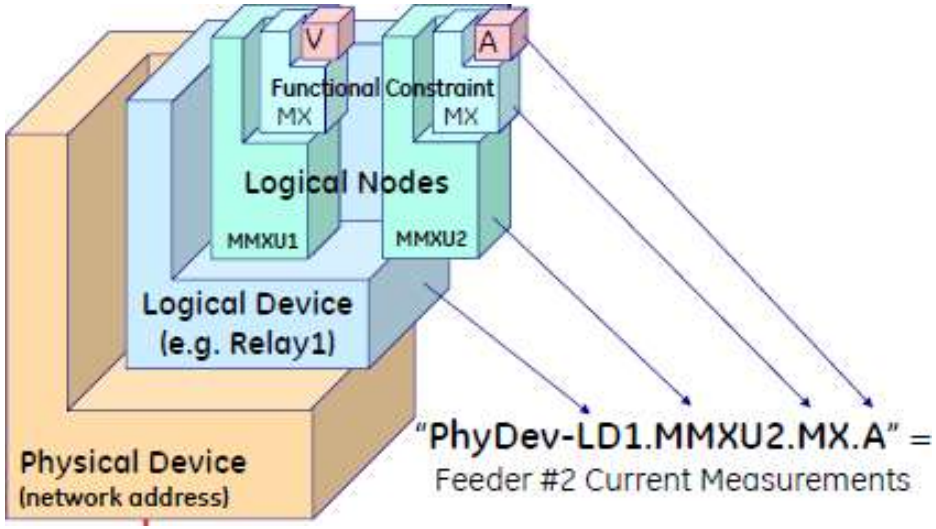
Source: "UCA & 61850 for Dummies." – Douglas Proudfoot

Modern Object-Oriented Protocols

TECHTALK

IEC 61850

- Much broader than traditional protocols
- Multiple protocols
  - GOOSE, MMS, Sampled values
- Standardized configuration language
  - Substation Configuration Language (SCL)
  - Extensible Markup Language (XML)
- Standard and extensible objects
  - Naming
  - Data types



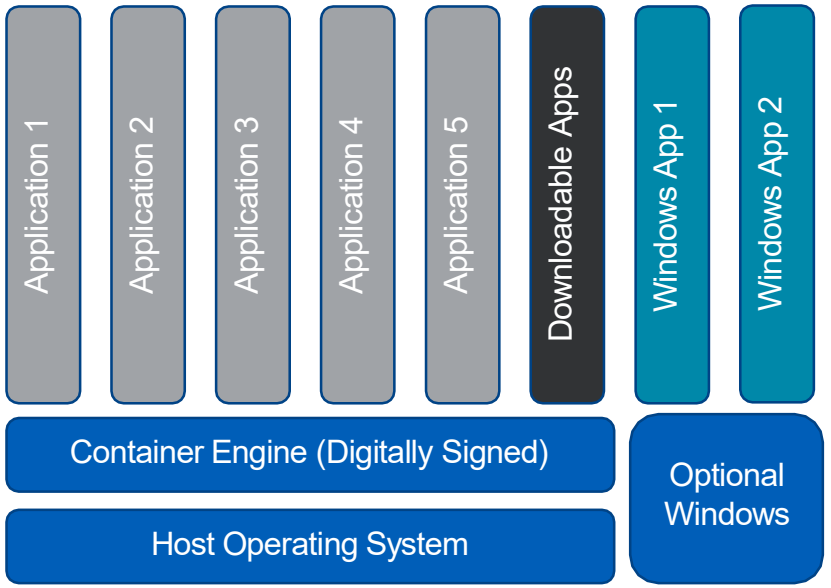
SCL CID Example File

TECHTALK

```
<?xml version="1.0"?>
<SCL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" x
http://www.iec.ch/61850/2003/SCL">
  <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_LLN0" lnClass="LLN0" 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" />
```

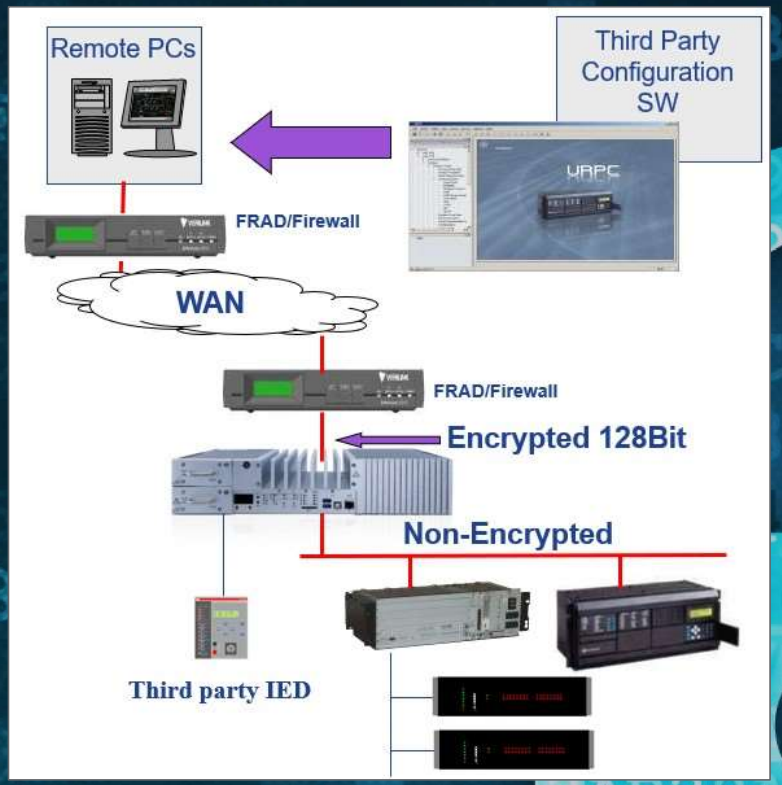
Advanced Functionality

- Gateway Evolution
  - Advanced functionality
  - Time synchronization and distribution: IRIG-B, SNTP, PRP
  - Programmable logic
  - Non-operational file gathering and reporting
- Advanced processing platform
  - Virtual machines
  - Multiple OS environment
  - Container-based technology



Gateway Security

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



Summary

- **Substation RTU**
  - Moving toward a multifunction gateway platform with advanced functionality

- **Substation Data**
  - Volume will increase, primarily non-operational data
  - Efficient, reliable, and secure management of data will be main objectives
  - Application of analytical tools to convert data to useful information

Summary

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

XCBR1.Loc.stVal[ST]

- **Cybersecurity**
  - Critical infrastructure protection will be crucial focus
  - Automated management of firmware and passwords is key
  - Compliance with mandates from governing bodies