SCADA
Supervisory Control And Data Acquisition

Goal: Integrate 21st century SCADA technology into existing Renewable Energy programs

- Develop an open source SCADA platform
- Deploy SCADA hardware on RE installations at two-year colleges
- Develop SCADA curriculum and instructional materials
- Provide faculty professional development in SCADA technology

Award # 1901852

This material is based upon work supported by the National Science Foundation under Grant # 1901852. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
HITEC Session Title and Description:

**SCADA Modularized Curriculum, Hands-On Labs, and Job Task Analysis for Renewable Energy**

The CREATE Energy Center’s SCADA (Supervisory Controls And Data Acquisition) project has developed a job task analysis, a set of six curriculum modules, and seven hands-on labs designed to advance renewable energy education by enabling faculty leaders to integrate SCADA into existing energy technician education programs.

Viewers of this session see the SCADA job task analysis, modules, and labs segmented by learning objectives and learn about upcoming faculty professional development to help integrate these materials into existing energy technician and other technology programs. **Benjamin Reid**, Co-PI/Project Manager, CREATE SCADA, Madison Area Technical College, Madison, WI; **Kenneth Walz**, Director and PI; Science, Engineering and Renewable Energy Instructor, CREATE, Madison Area Technical College, Madison, WI; **Kevin Cooper**, PI, Dean of Advanced Technology, RCNET, Indian River State College, Fort Pierce, FL; **Kathleen Alfano**, Co-PI, CREATE, College of the Canyons, Santa Clarita, CA
Contents:

- Part 1: SCADA – Job Task Analysis
- Part 2: SCADA for Renewables: A Six Module Course
  - 1. SCADA Overview
  - 2. Components and Functionality
  - 3. Basics of SCADA Communications
  - 4. Human/Machine Interface
  - 5. Applications within Renewable Energy Industry
  - 6. Emerging Trends in SCADA for Renewables
- Part 3: SCADA Control Board Labs (4)
- Part 4: SCADA Computer Based Labs (3)
Part 1: SCADA – Job Task Analysis

The scope of this JTA encompasses the knowledge and fundamental principles across five content domains of SCADA systems for renewable energy applications:

• Application
• Installation
• Operation & Maintenance
• Data Analytics
• Cybersecurity

The SCADA – Job Task Analysis is a 9 page document best viewed here: https://createenergy.org/job-task-analysis
Page intentionally left blank
Course Learning Objectives

1. **Describe** SCADA system basics and important differences with other control systems
2. **Demonstrate** competency of the key components of a SCADA system and their functions
3. **Describe** the different communication systems used in SCADA
4. **Demonstrate** competency of the role and capabilities of operator interfaces
5. **Demonstrate** competency of implementing SCADA in real world applications, specifically renewable energy applications (install, operation, maintenance)
6. **Identify** emerging technical trends, shifts, and innovations impacting SCADA and its application in the renewable energy sector
SCADA for Renewables: A Six Module Course

Course Outline / Curriculum Learning Modules:

Module 1  SCADA Overview
Module 2  Components and Functionality
Module 3  Basics of SCADA Communications
Module 4  Human/Machine Interface
Module 5  Applications within Renewable Energy Industry
Module 6  Emerging Trends in SCADA for Renewables
Module 1 – SCADA Overview
Learning Objectives

• **Understand** the course intent and the study topics to become versed in SCADA
• **Understand** the history of SCADA
• **Understand** the fundamentals of industrial control systems, distributed control systems, and their core components
• **Understand** the definition of a SCADA system, why SCADA is important
• **Understand** characteristics, strengths, and weaknesses of SCADA systems versus other control systems, i.e. DCS
• **Understand** the terminology associated with SCADA systems for monitoring power systems (solar, wind, energy storage, etc.)
• **Understand** the key devices and components and their purpose in a SCADA system; especially for monitoring power systems (solar, wind, energy storage, etc.)
• **Understand** the basic communication structure for a SCADA system
• **Understand** the difference between Proprietary vs Open or Mix and Match systems
• **Understand** the differences between data collection, process monitoring, and process control
• **Describe** types of SCADA system applications for the Renewable Energy (RE) Industry
• **Identify** key features and benefits of the integration of RE and SCADA systems
• **Understand** how SCADA facilitates data analysis to improve RE operating performance
• **Observe** SCADA system in use, if possible, at a power facility – SCADA design considerations, operating philosophy and requirements, end-user operation of the SCADA system
References and Additional Learning Material

- https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/
  Overview article on SCADA systems

- https://www.affinityenergy.com/avoid-solar-energy-loss/
  How SCADA can be used to improve solar power system operations

  Advanced features that can be leveraged in SCADA for solar power systems

- https://www.youtube.com/watch?v=rmDdK38w-uw
  Short video of SCADA for wind power application

- https://blog.norcalcontrols.net/solar-pv-plant-operations
  Resource blog for SCADA solar applications
What is SCADA

A range of process control systems and formats are used to operate industrial processes:

- Local Control – controls located at the machine or at the point of use
- DCS – Distributed Control System
- SCADA – Supervisory Control and Data Acquisition
Importance of SCADA

At the site or operator level, a SCADA system enables operators to:

• Manage the day-to-day performance of a process or plant site as efficiently and profitably as possible
• Prevent failure, damage, or other costly equipment issues by alerting operators of problems, maintenance needs, and operational anomalies.
• Monitor processes, adjust to changes, and troubleshoot issues by providing real-time data at their fingertips

At the enterprise level, a SCADA system enables business owners or stakeholders to:

• Leverage process data to make more informed projections and financial decisions
• Efficiently manage a network of plants or assets to maximize overall profitability
What is SCADA?
Comparing DCS and SCADA

Both DCS and SCADA systems are similar in that they are a collection of software and hardware components that:

- Gather and present data to operators from remote devices and processes (temperature, flow rate, voltage, position indication, etc.)
- Allow supervision and control of plant operations, locally and remotely
- Make decisions about processes with the aid of operator input
- Allow a human to manually take over in unusual circumstances

Source: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/
Comparing DCS and SCADA

But they are different in that DCS emphasizes process level operations while SCADA is event driven and based on data gathering.

Additionally:

• DCSs have built-in operator interface software with tag databases, while SCADA requires additional software to set up the interface and tags
• SCADA is not recommended for safety systems. If safety is a primary concern, then DCS offers advantages
• For time-sensitive processes, SCADA systems may have a slight advantage as the processing time is generally faster than DCS, but the gap has narrowed
• SCADA is often network based, i.e. LAN or WAN
• Requirements or needs for an open communication architecture favor SCADA
• SCADA is generally more scalable and flexible for use across multiple sites or remote locations

DCS and SCADA can also be merged into a singular supervisory system leveraging the best of both
Basic Functions of a SCADA System

- Monitor and gather process data in real-time
- Interact with field devices and control stations via Human Machine Interface (HMI)
- Record system events into a data file
- Enable virtual monitoring and control of operations and processes
- Provide information storage and reporting
SCADA System Diagram Example

- Solar Array A
- Solar Array B
- Solar Array C
- Energy Storage 1
- Meter 1
- Field Device/IED 1
- Field Device/IED 2
- RTU Z
- MTU
- Communication Network
- Remote HMI / Workstation
- Control center
- Utility substation
- Local HMI
- Communication Network
- RTU / PLC A
- RTU / PLC B
- RTU / PLC C
- RTU / PLC 1
- Meter 1
- Field Device/IED 1
- Field Device/IED 2
- RTU Z
- MTU
- Communication Network
- Remote HMI / Workstation
- Control center
- Utility substation
- Local HMI
- Communication Network
- RTU / PLC A
- RTU / PLC B
- RTU / PLC C
- RTU / PLC 1
- Energy Storage 1
SCADA is a collection of hardware and software components:

- Sensors, switches, meters, etc.
- Remote Terminal Unit (RTU), Programmable Logic Controller (PLC)
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
- Communication protocols
Basic operation of a SCADA System

• Field devices, such as sensors and switches, provide real time process signals to a RTU or PLC

• The RTU or PLC uses these inputs in its logic algorithms to manage or control process systems and communicate back and forth with both field devices and the MTU

• The computer-based core of the system, the MTU, initiates communication with the RTUs and/or PLCs, collects and stores data, supports the operator interface, and communicates with other systems

• HMIs enable system operators, maintenance personnel, engineers, and other stake holders to monitor and manage the process system or process network
Communication between field devices and RTUs/PLCs can be analog or digital.

Communication between the MTU and the RTUs/PLCs is a critical part of a SCADA system.

-- Can be wired or wireless (radio, cellular, satellite), usually a combination of both are used.

Communication protocols

-- Range of proprietary, vendor specific communication protocols and open communication standards exist.
Proprietary vs Open SCADA

• An **Open** SCADA System is a system where the major components all comply to certain industry standards to enable interoperability.

• A **Proprietary** SCADA System is a system where all major components come from one vendor/manufacturer and the standards are usually specific to that system and vendor.
Proprietary vs Open SCADA

Examples of proprietary vendor protocols
- SAP-bus (ABB)
- Conitel (Leeds&Northrup)

Examples of open protocol standards
- Modbus
- Profibus
- IEC 60870-5-101 or 104
- IEC 61850
- DNP3 (used commonly for utilities)
Applications of SCADA in RE

- Monitor and control of operations at RE generation sites, such as solar farms and wind farms, or even a network of distributed RE generation sites
- Integration of RE generation sites with the power grid
- Integration of energy storage systems with both RE generation site(s) and the power grid
Examples of SCADA Architecture in RE

Source: Communication Architecture for Grid Integration of Cyber Physical Wind Energy Systems - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Proposed-architecture-of-the-cyber-physical-wind-energy-system-SCADA-supervisory_fig6_320112821

SCADA Systems: Challenges for Forensic Investigators - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Layers-of-a-SCADA-system_fig3_234138890 [accessed 27 Sep, 2020]
Advances in SCADA for RE

With new technologies, improving system integration, and more powerful analytics SCADA enables:

- Finite system performance management down to the device level (i.e. individual inverter or panel)
- Intelligent alarm processing
- Advanced predictive maintenance to minimize outages and downtime
- Automatic power generation control
- Predictive system output incorporating multiple weather data and weather forecast sources for operations planning and financial optimization
- System coordination with utility energy management systems (EMS)
- Real time performance optimization of a network of distributed operating sites
- Real time theoretical vs actual power output analytics
- Real time production value calculations and financial optimization
- Event sequence recording and reporting, document management, and report generation
QUESTIONS?
Module 2 – SCADA Components and Functionality

Learning Objectives

• **Identify** common field instruments and sensors and understand how they are used in a SCADA system
• **Discuss** syncing and sourcing sensor devices and actuators
• **Wire** intelligent electronic devices and controllers
• **Understand and evaluate** various PLC and RTU controller functions and programming
• **Configure** controllers for basic communication to workstations and wider networks
• **Program** controllers and smart devices (write program, perform calculations, perform scaling operations, perform tagging operations, etc.)
• **Configure** and program a RTU to communicate with the master system
• **Understand** role of the Master Terminal and how it monitors and/or controls other components
• **Configure** and program a Master Terminal to communicate with various system components
• **Understand** role of the HMI in communicating information to/from the user/operator and design and configuration best practices for a HMI
• **Distinguish** between proprietary systems and standards based general purpose communications networks
• **Investigate** communications between smart sensors and various controller devices
• **Discuss** standard TCP/IP network equipment such as switches and routers
Module 2 – SCADA Components and Functionality

Pre-requisites

Students should have completed the following courses prior to taking Module 2 or have equivalent work experience:

• Introductory DC/AC Electrical Circuits

• Digital Electronics Fundamentals

• Programmable Logic Controllers (recommended)
References and Additional Learning Material

• [https://blog.norcalcontrols.net/solar-pv-plant-operations](https://blog.norcalcontrols.net/solar-pv-plant-operations)
  Resource blog for SCADA solar applications


SCADA System Components

SCADA is a collection of hardware and software components:

• **Sensors, meters, switches, etc.**
• **Remote Terminal Unit (RTU)**
• **Programmable Logic Controller (PLC)**
• **Master Terminal Unit (MTU)**
• **Human Machine Interface (HMI)**
• **Communication networks and protocols**
Basic SCADA System Components

• SCADA enables data collection from one or more distant facilities and facilitates sending control instructions to such facilities.

• SCADA was developed to monitor and control very large distributed process facilities such as energy grids, remote gas or oil pumping facilities, etc.

• SCADA typically is NOT used for factory control and monitoring – PLCs (Programmable Logic Controllers) or DCSs (Distributed Control Systems) work better for the factory control.
## SCADA System Components Purpose

<table>
<thead>
<tr>
<th>Hardware / Software Components</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Field Devices: sensors, switches, meters, etc.</td>
<td>To perform data collection.</td>
</tr>
<tr>
<td>Output Field Devices: Motor controls, valve controls, etc.</td>
<td>Devices that can be controlled remotely.</td>
</tr>
<tr>
<td>Remote Terminal Units (RTU), Programmable Logic Controllers (PLC)</td>
<td>Receives instructions and performance targets from MTUs. Performs immediate control of field devices. Collects data from field devices and communicates data (or totalized data) to MTU.</td>
</tr>
<tr>
<td>Master Terminal Unit (MTU)</td>
<td>Sends process targets to RTUs. Monitors data from RTUs to ensure that targets have been reached. Alerts operator about system conditions.</td>
</tr>
<tr>
<td>Human Machine Interface (HMI)</td>
<td>Display system components status. Relay operator input to MTUs.</td>
</tr>
<tr>
<td>Communication networks and protocols</td>
<td>Enable communication between: RTU/PLC and field devices; RTUs and MTU; MTU and HMI</td>
</tr>
</tbody>
</table>
SCADA System Components

SCADA is a collection of hardware and software components:

These are the various components mentioned below:

• **Sensors, meters, switches, etc.**
  • Remote Terminal Unit (RTU), Programmable Logic Controller (PLC)
  • Master Terminal Unit (MTU)
  • Human Machine Interface (HMI)
  • Communication networks and protocols
SCADA System Diagram Example

- Solar Array A
- Solar Array B
- Solar Array C
- Energy Storage 1
- Remote HMI / Workstation
- Local HMI

Communication Network

- Field Device 1
- Field Device 2
- RTU / PLC A
- RTU / PLC B
- RTU / PLC C
- RTU / PLC 1

RTU Z
MTU
Input Field Devices: Discrete vs Analog

• Input field devices, such as sensors and switches, provide real time process signals to a RTU or PLC.

• Input filed devices can produce discrete or analog inputs to RTU/PLC:

**Discrete inputs** - can only have two states – ON and OFF (binary 1 or 0). Discrete inputs are typically powered by 24VDC or 120VAC power supplies. Examples of discrete inputs are from switches and some sensors.

**Analog inputs** - are typically produced by sensors and meters and provide continuous DC voltage (0-5V, 0-10V) or DC current (0 – 50mA, 4 – 20mA) values. Analog inputs require specialty analog input cards (for PLCs) with built-in A/D converters.
Input Field Devices: NO vs NC Switches

• Normally Open (NO)
  OPEN - WHEN INACTIVE
  CLOSED - WHEN ACTIVATED

Normally open switches are open when inactive and closed when activated.

• Normally Closed (NC)
  CLOSED - WHEN INACTIVE
  OPEN - WHEN ACTIVATED

Normally closed switches are closed when inactive and open when activated.
Input Field Devices: Examples of Discrete Mechanically Operated Switches

- **Limit switch**
  Limit switch position control is used to
  - Govern carriage
  - movement range Count parts
  - Parts tracking / zones and
  - Initiate operating sequence

- **Temperature Switch**
  Temperature switch can be bi-metallic, liquid, or vapor based. Most have adjustable preset adjustable actuation point. Some may also have separate de-activation point.
Input Field Devices: Examples of Discrete Mechanically Operated Switches

• **Pressure switch**
  Limit switch position control is used to:
  - Govern carriage movement range
  - Count parts
  - Parts tracking / zones
  - Initiate operating sequence

• **Level Switch**
  Level switch is activated by level change in liquids. The switch uses a float to determine the action. Below curtain level, fluid is added to the chamber. Above curtain level, fluid entry stops. It can be used to control pump motor action or solenoid pipe valves.
Input Field Devices: Examples of Discrete Mechanically Operated Switches

FLOW SWITCH:

- Flow switch is activated by a CHANGE in flow of liquid or gas.

- A flap in a pipe or passage is rotated or pushed aside by moving fluid.

- All of these are examples of DISCRETE (ON/OFF) inputs.
I/O Field Devices: Examples of Discrete Electro-Magnetically Operated Switches

I/O Field devices- examples of Discrete Electro Magnetically Operated switches:

• **Relays**
  Relay is an electro-magnetic switch controlled by the PLC/RTU with moderate currents (0.3A to 10A) and voltages (up to 240 V).

• **Contactors**
  Contactor is an electro-magnetic switch controlled by the PLC/RTU. It is used to provide ON/OFF contacts for circuits with heavy current loads (10A to 100’s A).
Input Field Devices: Sensors

• SENSOR – is a transducer that receives and responds to a signal or stimulus from a physical system AND produces a signal which could be used by a control system.

Sensors can detect the following properties: mechanical, electrical, magnetic, thermal, optical, chemical, audio, atomic, etc.

• Examples: proximity detectors (inductive or capacitive), light/optical/IR sensors, light/dark level sensor, pressure sensor, temperature sensor and many more.

• Sensors can produce both discrete and analog electrical signals.
Output Field Devices: Actuators

OUTPUT FIELD DEVICES:

• ACTUATORS:

ACTUATOR is a device that is responsible for moving or controlling a mechanism or system. It is controlled by a signal from a control system or manual control.

Examples:
• Pneumatic valve actuator; Motor starter etc.
SCADA System Components

SCADA is a collection of hardware and software components:

- Sensors, meters, switches, etc.
- **Remote Terminal Unit (RTU)**
- **Programmable Logic Controller (PLC)**
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
- Communication networks and protocols
Remote Terminal Unit (RTU)

Remote Terminal Units (RTUs) are microcomputer-based with special equipment to:

• Interface with the long-range communications link to MTU (Master Terminal Unit)

• To interface with the sensors, actuators, and perform calculations in the process.

Since modern RTUs need to perform some control functions, as well as interface functions, Programmable Logic Controllers (PLCs) can be used in place of RTUs in SCADA systems.
RTU/PLC Functions

Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC) performs the following main functions:

• Communicates with MTU (Master Terminal Unit):

  When MTU requests, RTU sends signals to open/close valves, turn switches on/off, start/stop motors, outputs analog or digital signals (such as set points) or outputs pulse trains to move stepper motors.

• Communicates with each of the field sensors and actuators that it is connected.
• Gathers information from the field: analog or digital values, alarm and status points, metered amounts.
• Converts data into digital form and keeps this information available for MTU.
• Solves algorithms to act as controller or a pulse totalizer for functions that cannot wait for decision from MTU.
Initially, RTUs (analog RTUs) performed only the first two functions. Now, electrical controllers, such as PLCs (Programmable Logic Controllers), can be used in place of dedicated RTUs that allow additional functionality:

• Fluid flow totalizing or electrical energy flow totalizing

• Interactive valve positioning or interactive pneumatic controls positioning

• Other control functionality such as PID loops (example – PID loops in oil refining process) that require powerful CPU processing capabilities
Programmable Logic Controllers

PLC System

Input module
Central processing unit (CPU)
Memory
Program data
Output module
Optical isolation
Output load devices
Programming device

Power supply

Input sensing devices
Programmable Logic Controllers

PLC is essentially a computer with similar components, architecture, operation, but with enhanced handling of input/output field devices. PLC has:

- Central Processing Unit (CPU) with ALU, registers, instructional decoder, clock and control signal circuit.
- Memory to store firmware, program and data.
- I/O modules (input/output) – AC or DC discrete I/O, AC or DC analog I/O. specialty I/O.
- Power supply (5 VDC for CPU, limited 12/24 VDC for I/O.
- Base (Rack or Backplane or Chassi) provides electrical contacts and databus on the back of the rack.
- Specialty modules – I/O modules with separate CPU, such as high speed counter or Ethernet module.
Programmable Logic Controllers

What really separates PLC from a regular computer and makes it suitable for harsh industrial environment is presence of isolation boundaries as shown on this figure.

Source: www.AutomationDirect.com
Programmable Logic Controllers

• Electrical isolation between primary / secondary / field sides and different I/O is important for safety, so that fault in one area does not damage another area.

• A transformer in the power supply provides magnetic isolation between primary and secondary sides.

• Opto-couplers in I/O modules provide optical isolation between CPU and I/O in the input/output circuits. This isolates logic circuitry (CPU) from the field side (machinery).

Discrete inputs are isolated from discrete outputs as well.
PLC: Sinking vs Sourcing

- Sinking/Sourcing is only applicable to DC powered field devices.

- For example, **Sinking** PLC input is defined as input circuit with uninterrupted path to supply ground.

Source: www.AutomationDirect.com
I/O Field Devices: Sinking vs Sourcing

- **Sourcing** PLC input is defined as input circuit with uninterrupted path to supply source (positive terminal).
I/O Field Devices: Sinking vs Sourcing

- Many newer PLCs with DC inputs can be wired as either sinking or sourcing due to dual diodes in the opto-isolator.

Source: www.AutomationDirect.com
I/O Field Devices: Sinking vs Sourcing

- Most Sourcing PLC discrete input circuits can be paired up with Sinking Field Devices, such as sensors (except AB PLCs which use terminology of sourcing PLC inputs being paired up with sourcing field devices).
I/O Field Devices: Sinking vs Sourcing

• Vice versa, Sinking PLC discrete input circuits can be paired up with Sourcing Field Devices, such as sensors.

Source: www.AutomationDirect.com
I/O Field Devices: Sinking vs Sourcing

- Similar to DC PLC inputs, DC PLC outputs can be wired as sinking or sourcing (using 12VDC or 24VDC typical power supplies):

![Diagram of Sinking and Sourcing Outputs](https://www.automationdirect.com)
Input Field Devices: AC vs DC

• **Only DC PLC Inputs** – sinking, sourcing or both. PLC DC input circuits are usually built using solid-state electronic components.

• **Only AC PLC Inputs** – are typically built using solid-state electronic components. Sinking and sourcing is NOT applicable to AC inputs.

Source: www.AutomationDirect.com
Output Field Devices: AC vs DC

- **Only DC PLC Outputs** – sinking or sourcing. PLC DC output circuits are usually built using solid-state transistor components.

- **Only AC PLC Outputs** – are typically built using solid-state triacs as part of the output circuitry. Sinking and sourcing is NOT applicable to AC outputs.

- **AC or DC PLC Outputs** – are built using relays in the output circuitry which allows them to use outputs powered by either DC or AC power supplies.
I/O Field Devices to PLC Wiring

- **Wire sizes**— AWG 14 – AWG24, usually AWG 20 – 24.
- **Energizing I/O** – AC or DC power supply must be used with inputs and outputs (need to check specs to choose appropriate power supply). PLC may provide auxiliary power supply to power inputs and limited number of low-power outputs.
- **Wire Tagging** – each wire should be tagged/labelled to indicate which switch/sensor or load and which PLC input/output port it is connected to. This is very important for system troubleshooting.
- **Copper Wire** is usually used since signals are low-voltage electrical. In some applications, **Shielding** needs to be added over the copper wire to prevent electromagnetic interference or noise.
PLCs: Programming

PLCs are programmed by using one of the following programming methods:

- Ladder Logic – is a graphical language that resembles relay ladder logic used by electricians. This is the most widely used PLC programming language.
- Structured text.
- Instruction lists.
- Sequential function charts.
- Function blocks.
PLCs: Ladder Logic Programming

The following two examples show relay ladder logic vs PLC ladder logic diagrams (both look like “rungs” of the ladder):

PB – push button
CR – control relay
PLCs: Ladder Logic Programming

• Left rail represents power rail.

• Right rail – ground rail.

• Outputs are energized when logic contacts provide closed path for the electrical current to flow from left rail to right rail.

• If PLC is in the run mode, it will:
  – scan all inputs (and record input status values in PLC memory),
  – scan and perform all ladder rungs (use status of each input stored in the memory and update all memory location corresponding to the outputs),
  – update physical outputs (open or close output relay or solid state switches that will energize/de-energize field devices).

• If PLC in the program mode, it will only scan inputs and update input memory locations.
PLCs: Configuring/Programming Discrete Inputs / Outputs

• There is no special config required for discrete inputs or outputs.

• If push button PB1 is connected to input terminal X001 of the PLC, memory location X001 can be used in the ladder logic program to address this input.

• If motor starter is connected to discrete output Y1, it can be addressed in ladder logic as Y1 for output coil or set/reset instructions.

PB – push button
CR – control relay
PLCs: Hardware / Configuring/Programming for Analog Inputs / Outputs in DL06 PLC

• Analog inputs and outputs typically require special I/O cards.
• Diagram shows wiring diagram for the 0.0 - 1.0 V PV Irradiance Sensor connected to the Analog Voltage Input card for DL06 PLC. PV Irradiance Sensor serves as a power source since it generates DC voltage between 0.0V and 1.0V for irradiance level between 0 W/m² and 1000 W/m². The analog input card is rated for 0 – 5VDC input voltage.
PLCs: Hardware / Configuring/Programming for Analog Inputs / Outputs in DL06 PLC

- Analog inputs/outputs require special configuring.

- Ladder logic code for DL06 PLC below configures format (BCD or binary) of the incoming data and number of active channels on the card (0 – 8). K100 that is stored in memory location V700 indicated 1 channel in BCD format.

- It also stores address of memory location where data from this input card (O2000) in the memory location V701 assigned to the input card located in slot 1.
PLCs: Hardware / Configuring/Programming for Analog Inputs / Outputs in DL06 PLC

- Next ladder logic block inputs and stores multiplication constants that will be used in the rescaling calculations.
- A/D converter in the analog input card is going to take the voltage between 0V and 5V and convert it to the numerical value between 0 and 65535.
- We need to convert this abstract number to the corresponding irradiance level with 65535 corresponding to irradiance level of 5000 W/m².
PLCs: Hardware / Configuring/Programming for Analog Inputs / Outputs in DL06 PLC

- The last block of ladder logic performs re-scaling calculations and store value in units of W/m² in the memory location V2100.
PLCs: Hardware / Configuring/Programming for Analog Inputs / Outputs in DL06 PLC

- Finally, the value of solar irradiance, stored in V2100, can be used to energize/de-energize water pump (connected to output Y11) and to update status of control bit (C2) to be displayed on the operator touch-screen panel.

- Configuring/Programming instructions syntactics shown here is specific to DL06 PLC, but similar programming steps would need to be done on other PLCs to process analog I/O.
SCADA System Components

SCADA is a collection of hardware and software components:

- Sensors, meters, switches, etc.
- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
- Communication networks and protocols
The center of SCADA system is Master Terminal Unit (MTU) which:

- Issues all commands to communication equipment and RTUs
- Receives information requested from RTUs
- Gathers all data from RTUs
- Stores some information (usually in totalized form)
- Passes information to associated systems
- Interfaces with operators via HMI (Human Machine Interface hardware)
MTU Communications Interface

Communications Interface Requirements:

• Use the same communications medium that RTU uses to send information to MTU
• Use the same protocol as the RTU (usually proprietary protocols)
• In MTU-RTU communications, usually utilizes Master-Slave communications with MTU being a master (that initiates all communications) and RTU being a slave (cannot initiate communications)
• In communications with printers and operator screens/HMI, utilizes regular computer communications techniques using open protocols and standard equipment. This is typically done with peer-to-peer communications via local area networks or LANs.
• May pass data to accounting computers, corporate business computers or computer networks.
SCADA System Components

SCADA is a collection of hardware and software components:

• Sensors, meters, switches, etc.
• Remote Terminal Unit (RTU)
• Programmable Logic Controller (PLC)
• Master Terminal Unit (MTU)
• **Human Machine Interface (HMI)**
• Communication networks and protocols
Human Machine Interface (HMI)

Operator can interact with MTU and/or RTU using the following Human Machine Interface (HMI) devices:

- **Programming devices:** computers and hand-held devices (legacy systems).
- **Operator interface devices:** data entry units, touch-screen panels or larger operator screens.

Data entry unit

Touch-screen panel/screen
Human Machine Interface (HMI)

HMI operator interface devices can be connected to MTUs and/or RTUs using:

- serial communication cables RS-232
- Ethernet cables

HMI operator interface devices can be connected to programming devices (computers) using:

- USB connectors
- Ethernet cables

Depending on the connection type, appropriate communication protocols must be utilized.
Human Machine Interface (HMI)

HMI Video Resources:

• What is HMI?
  https://www.youtube.com/watch?v=kujHQgK352o

• Example of C-More Touch Screen panel setup and programming using DO-More PLC Software:
  https://www.youtube.com/watch?v=fq5ScU0BI-k&t=183s
SCADA System Components

SCADA is a collection of hardware and software components:

- Sensors, meters, switches, etc.
- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
- Communication networks and protocols
Communication Networks and Protocols in SCADA Systems

Three rules of communication:

1. Talker and listener must use the same communication medium.

2. Talker and listener must use the same language (communication protocol).

3. Talker must not talk when someone else is talking (communication protocol).
Communication Networks and Protocols in SCADA Systems

Communication network/protocols can be:

Closed or Proprietary

• Convenient for connecting hardware from the same manufacturer
• Examples: Proprietary protocol for a barcode reader using an RS-232 point-to-point connection or RS-232C or RS-422 physical layer network with the DirectNET protocol

Open Systems

• Are needed to connect systems components from different manufacturers.
• This lead to the development of Open System Interconnection model (first for computers, later for PLCs)
OSI (Open System Interconnection) Model

1. Physical
   - Copper
   - Fiber
   - Wireless
   - Transmission Media

2. Data Link
   - Ethernet
   - DLL

3. Network
   - IP
   - ARP
   - ICMP

4. Transport
   - TCP
   - UDP

5. Session

6. Presentation
   - HTTP
   - FTP
   - SMTP
   - Modbus
   - DNS
   - SNMP

7. Application

Source: https://library.automationdirect.com/plc-communications-coming-of-age/
OSI (Open System Interconnection) Model

“The physical layer defines how to connect the upper data link layer in the OSI communications model within a computer/PLC to physical devices. It is basically the hardware requirements with schematics and specifications for successful bit-level communication to different devices.”

The physical layer defines:
• bit rates,
• transmission electrical, light or radio signals,
• flow control in asynchronous serial communication,
• types of cables (communication standards) and the shape of connectors.

Source: https://library.automationdirect.com/plc-communications-coming-of-age/
Serial Communication Standards

RS-232 Standard:
- Introduced in 1962. RS stands for recommended standard
- Other names include
  - TIA-232 (Telecom Industry Association – 232)
  - EIA-232 (Electronics Industry Association – 232)
- This is unbalanced wire (made of single wire, not twisted so that noise does not cancel out equally).
- Max length 50’ (at max data rate of 20 Kbps)
- Voltages: High (mark) (1) : -3V to -25V
  - Low (space) (0) : +3V to +25V
- Typical computer voltages: +/-5V (CPU), +/-12V (ex – to run fan motors and other operations)
- Max data rate is 20 Kbps (kbits per second)
Serial Communication Standards

• RS-232 is used for point-to-point communications.
• Such communications have master/slave designation.
• Example: computer/PLC to modem communication

Modem stands for modulator / demodulator:
• was very slow 300 bits per second
• communication byte included start bit + 8 bits data + stop bit, this resulted in transmission speed of about 30 characters per minute.
• Eventually modems went to speeds of 1200 character and 1600 characters per minute.

DIAGRAM:
- COMPUTER
- MODEM Printer
- DCE – data communication equipment
- DTE – data terminal equipment
Serial Communication Standards

RS-232 were used in Star Topology computer network systems (still point-to-point, still fairly short distances)

To go longer distances – need more current I
Serial Communication Standards

RS/EIA/TIA-423 Standard:

• This is still unbalanced wire (made of single wire, not twisted so that noise does not cancel out equally).

• It is used for point-to-multipoint communications

• Maximum length is 4000’ (at max data rate of 100 Kbps)

• Maximum line voltage is +/- 6V, but currents are higher than for RS-232

• Max data rate is 100 Kbps
Half Duplex vs Full Duplex

- **Half duplex** – only transmit or receive (but not both) can be on the same line at the same time.

- **Full duplex** – transmit and receive can happen at the same time on the same line. For full duplex, two dedicated RS-423 wires are needed.

Source: https://study-ccna.com/half-duplex-and-full-duplex/
Serial Communication Standards

RS/EIA/TIA-422 Standard:

• This is still balanced wire (made of twisted pairs resulting in the same noise cancellation on both wires in the pair). Problem – you need 2 wires for each pin.

• Maximum data rate is 10 Mbps

• Maximum length is 4000’ (at max data rate of 10 Mbps):
  (length x data rate should be less or equal to 1 x 10^8)

• Line voltages are -0.25V to +6V

• used for point-to-multipoint communications (1 driver/master to up to 10 receivers/slaves)
Serial Communication Standards

STANDARDS: RS/EIA/TIA-422

- Master / Driver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver
- Slave / receiver

Up to 10 receivers

Up to 10 receivers
Serial Communication Standards

RS/EIA/TIA-485 Standard:

- This is a balanced wire (made of twisted pairs resulting in the same noise cancellation on both wires in the pair). Problem – you need 2 wires for each pin.

- It is used for multipoint-to-multipoint communications:
  - up to 32 drivers
  - up to 32 receivers

- Maximum length is 4000’ (at max data rate of 10 Mbps)
- Line voltages are -7V to +12V (and has highest currents)
- Slow – for example, with 90 devices, it takes up to 1 sec to communicate with all

Daisy-chain configuration

Standard configuration
OSI Model: Datalink Layer

- **DATALINK LAYER**
  - node to node data connection / transfer
  - Media Access Control (MAC) for Ethernet: MAC address is unique number assigned to each piece of hardware by manufacturer
  - Logical Link Control (LLC)

- **Examples:**
  - PPP (point-to-point-protocol)
  - IEEE 802.3 (standard devices Ethernet card)
  - Appletalk IEEE 802.11 b/g/n (for wireless)
OSI Model : Network Layer

- **NETWORK LAYER** – functional and procedural rules for transferring variable length datagrams or packets

  IPv4 – Internet started with this
  IPv6 – current Internet IP addressing rules (allows for more / addresses)
  IPX/SPX – old Novel standard (Novel was leader in LANs, invented expandable token ring configuration)

- **TRANSPORT LAYER** – functional and procedural rules for transferring datagrams/packets from a source to a destination via one or more networks
OSI Model : Transport Layer

• TRANSPORT LAYER - Functional and procedural rules for transferring datagrams/packets from a source to a destination via one or more networks

TCP – transport control protocol (most common)

UDP – universal datagram protocol

Note: LINUX, UNIX, MAC OS – can run network on any physical layer; Windows – is more restrictive
Serial Communication Protocols

A protocol is a set of rules for communication among networked devices. Proprietary protocols are not part of OSI mode. Some examples of proprietary serial protocols are (this is not a complete list):

- Modbus RTU or K-Sequence (usually runs on RS-485 serial network)
- DirectNet (runs on RS-232C or RS-422 physical layer network) for PLC-to-PLC and PLC-to-HMI communications

Disadvantage – they are SLOW and will not work for applications demanding high speed or having high data volume.
Ethernet Communication Protocols used with PLCs

Some of the Ethernet protocols that are often used in PLC communications:

- ETHERNET/IP
- ETHERNET TCP/IP
- MODBUS TCP/IP
- PROFINET
Early Ethernet Models

In early days, coax cables were used for token ring configurations. In a token ring configuration, only 1 computer could talk at a time, then token was passed.

75 Ω termination is needed to prevent reflections if connecting to another ring.
Later Ethernet Models – with HUB

• At a later time, Ethernet was configured using HUBs.

• Every device was connected to the same HUB

• Each device broadcasted to all devices in the network.
Later Ethernet Models – with Ethernet Switch

• At the present time, Ethernet uses Ethernet switches.

• Every device is connected to the same switch.

• Switch can provide communication between 2 devices without broadcasting.
Later Ethernet Models – with Ethernet Switch

How Ethernet Switch switches between devices:

• TDMA/CD – time division multiple access
• CDMA/CD – carrier division multiple access (Internet uses mostly this)
• FDMA/CD – frequency division multiple access
• WDMA/CD – wavelength division multiple access (for fiberoptic cables)

CD – (optional) collision detection
Communications between MTUs, RTUs/PLCs, HMIs and field instruments

Communications between SCADA system components can use:

• Twisted copper wire (serial communications, typically used to connect PLCs to field devices)

• Ethernet cables CAT-5 and 5e, CAT-6 and 6a, CAT-7, CAT-8 and the RJ-45 connectors

• Optical fiber (Ethernet communications mostly)

• Small dedicated radios and/or UHF radios (note, UHF radios only work in the line-of-sight)
Communications between MTUs, RTUs/PLCs, HMIs and field instruments

You will learn more about communications between SCADA system components in Module 3 of this course.
SCADA System Components

Review

SCADA is a collection of hardware and software components:

- Sensors, meters, switches, etc.
- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
- Communication networks and protocols
QUESTIONS?
Module 3 – Basics of SCADA Communications
Learning Objectives

• **Distinguish** between proprietary and standards based general purpose communication networks.

• **Establish** communications for a SCADA network.

• **Integrate** sensors and data sources within the SCADA network.

• **Understand** and configure various communication applications.

• **Understand** cybersecurity risks.

• **Understand** measures taken to minimize cybersecurity risks.

• **Understand** basic types of network security.

• **Understand** basic types of data encryption.
References and Additional Learning Material

  21 things that can be done to secure SCADA systems with explanations

  Additional ways to secure networks including short videos.

- https://download.schneider-electric.com/files?p_Doc_Ref=998-2095-04-09-12AR0_EN
  Explains how vulnerabilities in SCADA systems have led to NERC-CIP standards

  Article on the importance of cybersecurity on SCADA systems including our nation’s electric grid.
SCADA Communication

• Communication between field devices and RTUs/PLCs can be analog or digital

• Communication between the MTU and the RTUs/PLCs is a critical part of a SCADA system
  – can be wired or wireless (radio, cellular, satellite), usually a combination of both are used

• Communication protocols
  – Range of proprietary, vendor specific communication protocols and open communication standards exist
Network Communications

• Network: two or more devices that exchange information (communicate).

• Networks can be wired or wireless.

• For communication to occur between field equipment and MTUs, there must be a protocol in place.
Protocols

• A protocol is a set of rules in which data is transferred on a network.

• In order to communicate, there must be a language chosen; that language is a protocol.

• There are many types of network protocols.

• Multiple protocols can be combined into a suite, such as TCP/IP.

• Some protocols are proprietary, meaning that they are owned and/or exclusive to a company.
Proprietary vs Open SCADA

An **Open** SCADA System is a system where the major components all comply to certain industry standards to enable interoperability.

A **Proprietary** SCADA System is a system where all major components come from one vendor/manufacturer and the standards are usually specific to that system and vendor.
Proprietary vs Open SCADA

• Examples of proprietary vendor protocols
  – SAP-bus (ABB)
  – Conitel (Leeds&Northrup)

• Examples of open protocol standards
  – Modbus
  – Profibus
  – IEC 60870-5-101 or 104
  – IEC 61850
  – DNP3 (used commonly for utilities)
Out of Many, Comes One

- In the 1980’s, there were many competing and proprietary communication protocols used in SCADA.

- Standardization of these protocols became important for SCADA systems integration.

- For example, the MODBUS protocol was a proprietary protocol introduced by Modicon in 1979.

- Today, MODBUS is an industry standard communication protocol used in many SCADA systems.
MODBUS Video

https://realsars.com/modbus/
SCADA and Security

• Allowing SCADA systems to be controlled on a network leads to unintended consequences of security risks.

• Security risks can come from external intruders or hackers as well as internally within the corporate LAN.
Network Security

- Network security refers to measures that are taken to protect the network and the data contained within.

- There are many ways to secure a network. Here are a few:
  - Firewalls
  - access control
  - IPS (Intrusion Prevention Systems) and
  - VPN (Virtual Private Networks)
Firewalls and Access Control

• Firewalls are the barrier between what gets in and out of a network.

• Firewalls are implemented in SCADA systems to keep unwanted traffic out of the network.

• In addition to firewalls, who can access the SCADA network is vital to its security; this is known as access control.

• Devices or users that are not known are given limited or no access to the network.
IPS and VPN

- IPS or Intrusion Prevention Systems are in place within SCADA systems to block malware or suspicious activity.

- Virtual Private Networks or VPNs allow data to be encrypted and to be sent over the internet.

- VPNs are a crucial network security tool that allows a user or operator the ability to have remote access to devices or information on the SCADA system.
Data Encryption

• Encryption is the process of encoding data so that it remains hidden or inaccessible to unauthorized users.

• Encryption is vital to the security of SCADA systems and networks.
Cybersecurity

- Cybersecurity is the protection of company assets from malicious network attacks or intrusion.

- The North American Electric Reliability Corp (NERC) created standards known as Critical Infrastructure Protection (CIP) to secure networks and energy assets for utility
QUESTIONS?
Page intentionally left blank
Module 4 – Human/Machine Interface

Learning Objectives

- **Understand** key elements of an HMI and its purpose for a SCADA network
- **Understand** how HMI facilitates continuous monitoring, data collection, automatic alerts, reports, etc.
- **Create/configure** a Human Machine Interface
- **Leverage** HMI to address alarms and alerts
- **Troubleshoot** faulty equipment with HMI tools
- **Understand** data formats and database organization
- **Understand** data sources and storage
- **Understand** data visualization
- **Understand** statistics and trend analysis
- **Leverage** data collection and analytical tools to generate various reports
References and Additional Learning Material

- [https://www.pas.com/resources/white-papers/high-performance-hmi](https://www.pas.com/resources/white-papers/high-performance-hmi)

  ISA 101 standard on HMI for process automation systems.

- [https://www.marinetech.org/files/marine/files/Curriculum/IROV/Module13/gruhnhmidesig
  nreviewed-110722135448-phpapp02.pdf](https://www.marinetech.org/files/marine/files/Curriculum/IROV/Module13/gruhnhmidesig
  nreviewed-110722135448-phpapp02.pdf)
What is a **Human Machine Interface?**

• At its most basic, a HMI is the link between a human operator and an automated process
  • Information is passed back and forth between the user through the HMI and the process controller (PLC, MTU, etc.) via the communication protocol (Modbus, etc.)

• HMI has and can take a variety of forms

• HMI continues to constantly evolve with technology
Various HMI Examples

Local Push Button Control Panel

Remote Workstation

Local Touchscreen Control Panel

Mobile Device HMI

Source: atex delvalle

Source: mjk.com

Source: nebb.com

Source: Totally Integrated Automation
Basic Functions of a HMI

• **Monitoring** – display real time operating status of the equipment or system

• **Supervision** – along with monitoring, the ability to make changes to the operating conditions directly through the HMI

• **Alarm** – recognize unusual events and report them

• **Control** – ability to apply algorithms to the operating process to control key variables within a desired target range

• **Historian** – storage of operating data for analytic or diagnostic purposes
Design intent – Who’s the Audience?

Target audience – sets design/functionality requirements

• In HMI design, the target audience is the system operator

• Additional layers and details can be accessible for other audiences (maintenance personnel, engineers, etc.) but in a format that does not create inefficiency or issues for the operator
HMI Design Evolution

• HMI continues to evolve with technology
• From hardware controls to digital versions of a P&ID with poor/confusing style to more modern, intuitive designs leveraging IOT and cloud to make HMI mobile/wearable/etc.
Why is good HMI design important?

- **Concern**: Sophisticated computer-based control systems being operated with ineffective and/or problematic HMIs, designed without adequate knowledge.

- **Countermeasure**: Redesign these systems in accordance with proper HMI principles to greatly improve their functionality and effectiveness.

Proper HMI design Principles enable:
- Improved operator situational awareness
- Improved safety
- Reduced likelihood of expensive mistakes
- Reduced incident response time to abnormal conditions
Early era HMI examples with poor design...

P&ID style with data overload and poor color scheme. Hard to use and understand.

Overdone use of “realistic” graphics but not informative or intuitive to use and understand.
Modern HMI Design standards

• With advancing HMI technology, the need arose to set standards and best practices

• In 2015, the International Society of Automation (ISA) published ISA 101 HMI Design Standard

• This document lays out the principles and design standards for **High Performance HMI** design
...and newer, High Performance HMI designs

Provides critical information rather than simply data.

Consistent color scheme and visuals.
Display Hierarchy

High Performance HMI display hierarchy

- **Level 1:** Overall situational awareness
- **Level 2:** Detailed view (sub-system or more granular view)
- **Level 3:** Equipment level detail
- **Level 4:** Diagnostics
Display Hierarchy - Example

High Performance HMI display hierarchy

- **Level 1**: Overall PV power plant operation
- **Level 2**: Specific array or module operation
- **Level 3**: Detail on a specific inverter
- **Level 4**: Performance data and analytical tools
How an HMI uses Data

- Monitor and historize operating conditions and parameters over time
- Establish relationships between operating variables/conditions/etc.
- Enables troubleshooting, optimizing, etc. of the process
- Export data for further analysis with other software – e.g. Excel
Considerations with HMI Data

• Data storage – local data historian server(s) and cloud integrated storage

• Data synchronization – ability to merge and exchange data across historian servers

• Speed – data collection speed, auto-archiving capability

• Compatibility with open standards and new technologies

• Performance calculation ability and intelligent asset technology

• Data insertion capability – insert data into the historian

• HMI data visualization tools – analysis toolkit within the HMI software

• Extensive redundancy and system security – reduce/minimize chance of operating losses or performance issues
Creating the Ultimate SCADA System for Solar Energy | Inductive Automation
Trends in HMI

- Cloud connectivity (local, remote, mobile, etc.)
- IOT
- AI – big data analytics
- AR/VR and haptic technology for system operators
- UAV – unmanned aerial vehicle integration
Trends in HMI
QUESTIONS?
Module 5 – Applications in the Renewable Energy Industry

Learning Objectives

• **Understand** how SCADA functions and is utilized in various RE power generation applications
• **Create and operate** a basic SCADA system for a solar power application project under various scenarios
• **Demonstrate** troubleshooting of issues from solar power application project
• **Generate** data collection, analysis, and operating reports from the application project
• **Understand** how SCADA is used for energy storage applications
• **Understand** how SCADA for RE applications can be combined with energy storage systems
• **Configure** solar power project to include energy storage and operate project under various scenarios
• **Generate** data collection, analysis, and operating reports from the application project
• **Understand** how SCADA for RE applications and/or energy storage is used in grid response applications
• **Understand** positives and negatives of RE grid response with SCADA vs traditional grid response options
SCADA – How is it used in daily operations?

• Software is used to interface between the actual control and the human display

• Makes gathering data easy

• Makes control of the asset easy

• Makes monitoring many assets at one time possible
Data Acquisition

• Data can be processed into many different forms
  
  • Reports
  
  • Logs
  
  • Graphs
  
  • Lists
Users of Data

• System Operators
• Local Managers
• Technicians
• Utility Companies
System Operators

- Use Data to Monitor Power Production
- Dispatch Assets to Correct Faults
- Plan Work Schedules
- Plan Shutdown of Production for Maintenance
Local Managers

• Coordinate Scheduled and Unscheduled Maintenance
• Produce Daily Production Reports
• Produce Daily Availability Reports
• Monitor Performance of Assets
Technicians

- Gather Data to Troubleshoot a Fault
- Use Data from Other Machines to Compare
- Collect Parameter Lists for Comparison
- Use Data to Commission the Assets
Utilities and Grid Operators

• Use Data to Help Balance the Grid

• Meet Customer Demands for Electricity

• Set Pricing for Electricity

• Plan Generation Levels Day Ahead
Other Data

• Fuel Mix
• Import and Export
• Pricing and Demand
• Weather Related
• Data Collected From All Sources

• Renewable Production Varies

• More Wind = More Wind Power

• More Sun = More Solar Power
Day Ahead Forecasting

- Weather Predictions Determine Amount of Renewable Power Expected
- Bids are Placed by Generating Units Based on Expected Power
Planning for Import and Export

- Sometimes Excess Power can be Exported to Other Areas
- Sometimes Power Needs to be Imported from Other Areas
Data Capabilities

All Parts of the Grid have Data Capability

• Generation Source

• Substations

• Transmission Systems

• All used together to Make Grid Management Possible
Troubleshooting Remote

• Depends on Good Data Collection

• Individual Generation Assets Collect Data Continuously

• Data is Accessed and Used to Determine the Source of the Fault

• Technicians and System Operators Depend on Processed Data
Case Study

Pitch Servo Motor Overheat Fault

• Electric Pitch Control System in a Wind Turbine

• Servo Motor Temperature is Monitored by the Control System

• Parameters are Established Within the Controller to Protect the Motor

• Control System Takes Specific Actions When Temperature Reaches Set Point
Start of Event

• The Control System in the Wind Turbine Detects a High Temperature

• Alarm is Sent to the Monitoring Operator (Local and System Operators)

• The Operator can Acknowledge the Alarm and Start Working the Problem
Operator Action

• Operator Acknowledges the Alarm
Investigating the Cause

• The Operator (or Technician) Starts to Investigate Possible Causes

• Logs Into the Controller to Gather Data About the Fault
Logged Into the Control System

- Once Logged In the Control Menu Options Appear

<table>
<thead>
<tr>
<th>MAIN MENU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Info</td>
</tr>
<tr>
<td>User Account Info</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>System</td>
</tr>
<tr>
<td>Shutdown...</td>
</tr>
<tr>
<td>Alarm Server</td>
</tr>
<tr>
<td>Alarm Client</td>
</tr>
</tbody>
</table>

**Application WTG 60Hz**
Checking Parameters

• The Pitch Motor Temperature Parameter can be Checked
Referencing the Manufacturers Material

- Checking Documentation for Parameters

<table>
<thead>
<tr>
<th>PLU</th>
<th>PDU</th>
<th>Temp</th>
<th>SHH</th>
<th>xx °C</th>
</tr>
</thead>
</table>

- View: 99, Edit: 99
- Min.: 0, Max.: 150, Default: 60
- Max. temperature for the PLU pitch motors.
Checking the Fault Data

• Modern Machines Store Data Before and After a Fault

• This Data Can be Used to Gain Information About the Fault

• Can Be Compared to Other Data

• Data Used to Support Theories About Cause of Fault
Data Supported Theories

• Increased Torque on Motor Could Cause It

• The Motor Torque is Compared to the Other Blades

• Motor Torque is Higher on the Faulted Blade

• More Information is Required to Determine Cause
Other Theories

• Motor Brake Stuck On

• Blade Bearing Binding

• Pitch Gear Box Issue

• Worn Open Gear Teeth Requiring More Holding Torque

• All Motor Brakes Appear to Be Open
Root Cause Determined

• Technicians Dispatched to Machine

• Inspection Found Worn Teeth on the Open Gear

• Caused Increased Torque Demand

• Blade Open Gear Was Replaced
Case Study Summary

• The Control System Reported the Fault

• The System Operator Started Diagnostics

• Site Technicians Inspected Based on Theories Supported by Data

• Root Cause was Improper Heat Treatment on Gear
Supervisory Control

• Allows Control of Machine

• Can Be Local – at Machine Through Human Machine Interface (HMI)

• Can Be Remote – Through Software and Remote Connection

• Passwords Assign Different Levels of Privilege (access to control level)
Machine Control

• Software Allows for Control of Systems

• Changing Parameters

• Activating Motors and Heaters

• Changing Signals
Parameter Changes

• Adjusting Parameters

• Changing the Pitch Motor Temperature Parameter
Parameter Changes

• The Parameter is Selected
• The New Value is Typed In and Updated
Motor Control

• Motors Controlled Through Remote

• Grease Pump Motor Control
Turning the Unit On

• Turning the Unit On
Feedback Data

• Verifying the Unit is On

• Uses a Sensor to Indicate the Piston is Moving From Grease Moving
Curtailment – Local and Remote

• Wind Turbines Are Able to Be Turned Up and Down Easily

• Can Adjust Output Levels Quickly

• Used by Utilities and Grid Operators to Control Grid Levels

• Done Through Remote Signaling
Summary

• Supervisory Control and Data Acquisition (SCADA)

• Allows Remote Control

• Collects and Stores Data for Use Later

• Vital to Operations, Grid Control and Reporting Production
QUESTIONS?
Page intentionally left blank
Module 6: Emerging Trends in SCADA
Learning Objectives

• **Understand** how various emerging technologies impact RE and SCADA systems

• **Understand** smart grid architecture

• **Understand** distribution SCADA and advanced applications.

• **Discuss and describe** risks and benefits with advanced SCADA systems.

• **Understand** different types of cyber attacks and risk mitigation frameworks
Introduction

• **Smart grids** are essential to powering the green energy revolution.
  • They take advantage of a range of technological advances, from edge cloud computing and artificial intelligence (AI) to sensors and smart meters, to more smoothly integrate the increasing volume of decentralized and intermittent renewable energy flows.

• However, the more assimilated the energy network becomes with connected Internet of Things (IoT) technology, the greater the risk of cyber attacks.

• In particular, the fast data flows needed to pass across highly interconnected communication networks, often facilitated by a mixture of new and legacy infrastructure, can create vulnerabilities in smart grid systems, prompting the urgent need for robust cyber security protection.

• The digitization of the grid, along with renewable energy infrastructure such as solar and wind farms, will serve to enhance the performance, controllability and security of hugely important and strategic assets while building in reliability and resilience.
Smart Grid Architecture

• The backbone system includes SCADA for
  • Generation, transmission and distribution
  • Control centers
  ● Loads

• A backbone system augmented with “accessories”, such as
  • Distributed energy resources such as wind and solar
  • Microgrids
  ● PMUs
  ● Storage
  ● Demand response
  • Smart loads and appliances
  ● Electric vehicles

• The most effective Smart Grid can monitor/control residential home devices and renewable sources that are non-critical during peak power consumption times to reduce power demand and return their function during non-peak hours.
Smart Grid Architecture

SCADA/Smart Grid Integration

• SCADA empowers the electricity consumer by interconnecting energy management systems to authorize the customer to manage their own demand of energy and control costs.

• It allows the grid to be self-healing by automatically responding to power quality issues, power outages, and power system faults.

• SCADA optimizes the grid assets by monitoring and optimizing those assets while minimizing operations and maintenance costs.

• The Smart Grid, intelligence and control need to exist along the entire power supply chain.
  • This includes the electricity generation and transmission from beginning to delivery end-points at the customer’s side and includes both fixed and mobile devices in the SG architecture.

SCADA/Smart Grid Integration

Advanced SCADA in Smart Grid applications

Source: http://smartgridstandardsmap.com/
SCADA system – Current Status

• The **SCADA system** is a centralized system that monitors and controls the entire area.

• SCADA architecture is a supervisory system gathers data on the process and sends the commands control to the process.

• SCADA framework is an amalgamation of hardware components and software programs where hardware includes a “Remote Terminal Units (RTU)”, “Master Terminal Unit (MTU)”, actuators and sensors, and software includes “Human Machine Interface (HMI)”, a central database (Historian) and other user software.

• These software provide a communication interface between hardware and software.

• The physical environment is linked to the actuators and sensors which are further connected to RTUs.

• RTUs gather the information and data from the sensors and forward telemetry data to the MTU for observing and controlling the SCADA framework.
SCADA Network Framework

• Communication network provides communication services between various components in the SCADA network framework.

• The medium utilized can be either wireless or wired. Presently, wireless media is generally utilized as it interfaces geologically circulated areas and less available zones to communicate effortlessly.

• The advancement of communication paradigm is isolated into four primary ages,
  • First era: Monolithic
  • Second era: Distributed
  • Third era: Networked
  • Fourth era: Internet of things technology.
SCADA Network Framework

1\textsuperscript{st} generation: "monolithic"

2\textsuperscript{nd} generation: "distributed"

3\textsuperscript{rd} generation: "networked"

SCADA Paradigm

• **Monolithic SCADA systems:**
  • refers to those systems which work in an isolated environment and do not have any connectivity to the other systems. The motive of these systems is to work in a solitary way. Large minicomputers were used for SCADA system computing.

• **Distributed SCADA systems:**
  • systems that were inter-connected and confined inside small range network like Local Area Networks (LAN). This generation distributes the computation overhead on remotely located systems using LAN, i.e., some of the systems work as communications processors.
SCADA Paradigm

• **Networked SCADA systems:**
  • It utilizes networks and web broadly because of the standardization and cost-effective solutions for large-scale systems. This is also referred to as a modern SCADA system. In this design, SCADA systems may be geographically distributed.

• **Fourth generation:**
  • The industries have been utilizing the power of technology to build, monitor and control the systems. Integration of Internet of Things (IoT) innovation and economically accessible cloud computing with SCADA systems has considerably lessened its infrastructure and deployment costs.
Emerging trends in SCADA

• Cloud-based supervisory control and data acquisition (SCADA) systems
• Increased use of analytics
• Subscription/flex licensing: SCADA as a service
• High-performance Human-machine Interface (HMI) and HISTORIAN
  • Allows for pre-attentive processing
  • Provides predictive analytics and regression analysis that will alert your operator days or weeks before a system failure
  • Allows operators to learn from and analyze data without the help of a programmer
• Cellular and 5G
  • seen as reliable backups for primary fiber communication and alternative to traditional radio communications
• Virtualization
  • Reduces capital and operating costs, Allows for system redundancy, Minimizes or eliminates downtime and Simplified data center management
Advanced Smart grid & SCADA Application: Distribution Automation

Distribution Automation technologies and systems can achieve substantial grid impacts and benefits:

• Improvement in location of fault, isolation, and service restoration capabilities

• Improved distribution system resilience to extreme weather events

• More effective equipment monitoring and preventative maintenance that reduces operating costs

• More efficient use of repair crews and truck rolls that reduces operating costs

• Improved grid integration of selected distributed energy resources (DER) such as thermal storage for commercial and municipal buildings
Application of advanced distribution Automation in SCADA

The most important application of the Advanced Distribution Automation is fault diagnosis by monitoring the faults in the grid, then identifying the root cause of the occurred fault and then restoring the system.

Distribution Automation can be grouped into 5 major subgroups:
1. SCADA
2. Integrated volt self var control (IVVC)
3. Equipment health monitoring
4. Fault location, isolation and service restoration (FLSR) systems.
5. Integration of renewable energy sources.
Components and Applications of SCADA in Distribution Automation

Improving Power distribution network with SCADA

With customers relying on continuous power supply, electricity distribution authorities need to provide power that meets customer needs by ensuring distribution infrastructure, including substations and transformers, are efficiently managed, operated and maintained.

Automating power distribution networks by installing, or upgrading, a SCADA system is a cost-effective solution to minimize power disruptions and provides greater visibility and improved control of the distribution network.

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/
Improving Power distribution network with SCADA

Minimize disruptions and improve operations:

• SCADA system’s function in the power distribution network is to
  • monitor and control distribution sectors,
  • optimize overall network efficiency, and
  • provide greater system reliability and sustainability.

• SCADA does this by
  • Collecting data from the distribution system, most of it originating from substations.
  • Typically, substations are controlled and monitored in real time by Programmable Logic Controllers (PLC) or Remote Telemetry Units (RTU) along with other devices such as circuit breakers and power monitors.
  • Devices that collect data transmit it back to a central SCADA node located at the substation; this node is connected to the main Control Centre.

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/
Improving Power distribution network with SCADA

• Reducing Manual labour requirements:
SCADA reduces the need for workers to physically complete the task themselves. This allows workers or operators to undertake specific tasks in a much safer and more efficient manner than if they were to do them manually.

• Reaping the benefits of SCADA:
Automation IT covers all aspects of SCADA power control and monitoring, from large distribution transformers and high voltage switchgear through to complete renewable energy power stations, solar farms, wind turbines, gas turbines and reciprocating engines.

Other functions performed by SCADA include:
• Controlling transformer voltage taps to improve network efficiency
• Control and monitoring of sectionalizers and reclosers
• Continuous monitoring and controlling of electrical parameters
• Trending and alarming to alert operators to power supply, quality or safety issues

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/
Benefits of integrating technologies to SCADA

• **Proactive Maintenance:**
Proactive maintenance involves preventive maintenance measures that will allow you to correct the root causes of failures and avoid downtime caused by underlying equipment problems. The main goal of proactive maintenance is to be able to anticipate machine failures and eliminate them before they develop.

• **Quick response to issues:**
A quick response is critical when SCADA system emergencies happen. In fact, depending on the issue, a quick response may be the difference between correcting the situation and a disaster. That's why receiving notifications in a timely manner is so important - emergencies could occur at any time.

• **Automated Controls:**
Having notification flexibility is very important, but sometimes it is not enough. Usually, SCADA systems allow you to remotely control just about any piece of equipment through control relays outputs in your RTU.
Benefits of integrating technologies to SCADA

• **Customized Alerts:**

Your SCADA should be customizable in order to allow you to avoid receiving irrelevant alarms. Getting notifications for every little thing that happens in your network triggers the slippery slope of operator indifference towards all alarms. Another important custom option that is important to have is the need-to-know based alerts.

• **Detailed reporting:**

SCADA systems are always collecting data from your remote equipment and processes. All of this information is usually stored in a central master station. Efficient master stations are able to compile a detailed reporting document about your network equipment.

• **Integration with your current Equipment:**

The result of integrating incompatible devices is that issues are dealt with more quickly and with a better level of consistency. The systems will allow for the integration of your current equipment to best in class SCADA increase efficiency.
Risk while integrating technologies into SCADA RE systems

• The need for a powerful and collaborative risk management framework for SCADA systems has become urgent to identify, evaluate, and treat various types of risks targeting SCADA systems. All possible scenarios that may happen and affect the system either directly or indirectly should be well described according to a set of parameters. Some of them are:

• Giving a detailed level of identifying the risks and classifying them based on the nature of the risk agents, their action’s motivation, and the penetration tools/techniques that can be used to cause a risk on a SCADA system.

• Providing all possible components that formulate a SCADA system and state all known vulnerabilities that can be used by attackers to perform the attack.
Risk while integrating technologies into SCADA RE systems

• Mapping between risks, vulnerabilities, and system components by linking each risk with all possible vulnerabilities of system’s components that an attack agent can utilize to achieve the risk goals. A description of the estimated impact on that component as a result of an attack is also missing.

• Description of the interdependency among threats that can be used to present the possible attack path scenarios. The main point in this work depends on the hierarchal based method. The relation among related parameters is converted into matrices, which are linked synchronously to construct an augmented matrix with six dimensions, which is analyzed.
Cyber Threats

• There are several technical threats that could affect to the digital infrastructure because of the need to connect remotely.

• This involves unencrypted connections, technical known vulnerabilities and exposures from systems on site that could enable malwares, backdoors and many other techniques to affect to current or future behavior of digital components.

• Or even worse botnets and advanced persistent threats could disrupt normal operation and affect to the energy assets as well.
Cyber Threats

• Internal technical threats because of unsafe network designs, communication protocols chosen, software dependencies, lack of patch management policy or simply information risks because of bad human habits can make useless any cyber protection.

• It is well known that a system is only as strong as the weakest link, and this involves people as well, so social engineering needs to be considered as an important threat too.
Cyber Threat for Critical Infrastructure

Cyber-Based Attacks

- Protocol Attacks
- Social Engineering
- Intrusions
- Worms / Spyware / Malware
- Denial of Service (DoS)
- Insider Threats

Threats to Critical Infrastructures
(Power Grid, Oil & natural gas, Water distribution, Transportation, ..)

Source: Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu), March 2018
Cyber threat: Actors & Impact in electric power sector

The cyber threat profile for the US electric power sector is highest from three key actors:

- **Very high**
- **High**
- **Moderate**
- **Low**

<table>
<thead>
<tr>
<th>ACTORS</th>
<th>Financial theft/fraud</th>
<th>Theft of customer data</th>
<th>Business disruption</th>
<th>Destruction of critical infrastructure</th>
<th>Reputation damage</th>
<th>Threats to life/safety</th>
<th>Regulatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organized criminals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nation-states</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insiders/partners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacktivists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skilled individuals hackers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Deloitte analysis.
Types of Cyber Threats

- **Malware**: means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer.

- **Spyware**: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

- **Ransomware**: Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

Types of Cyber Threats

• **SQL injection**: An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

• **Phishing**: is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information.

• Full list of significant cyber incidents in US since 2006:

  https://csis-website-prod.s3.amazonaws.com/s3fs-public/210326_Significant_Cyber_Events.pdf?ZKJldGVXdQd2vXW.gFEcFQs2Ay7cDipt

Utilities Worldwide Menaced by Cyberattacks As Pandemic Stretched Into the Summer Months

Distributed denial of service attacks on utilities around the globe increased almost seven-fold compared to the year-ago period, NETSCOUT data shows.

Best practices approach on Cyber security at Project/Component level

• Each control with physical or cyber access presents an intrusion point.

• Access must be controlled, and data integrity must be maintained at each accessible point.

• Examples of components: Wind farm reference architecture with secure best practice approaches like Network Segmentation, Zoning, Monitoring, and Intrusion Detection and Prevention System (IDS/IPS) for control and SCADA environment.

Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020
Best practices approach on Cyber security at Project/Component level

Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020
Tools for Cyber security

• **Network threat monitoring:**

Network monitoring tools that randomly check data samples to see if traffic is going to suspicious locations in and around a network can identify and stop an attack like this in its respective tracks.

• compare the data flow samples to an in-house extensive threat library and

• decipher suspicious patterns and

• potential security gaps that may be early indicators of a compromise, network problem or misconfiguration.
Tools for Cyber security

• Managed Security Analysis:
  Advanced analytics of systems can help single out potential attacks early, providing confidence as the digital footprint of the utility and grid expands.
  • single out critical threat data and help organizations act before there is a serious impact on operations.
  • incident data can be quickly generated for analysis through a simple portal, with actionable information from logs or events made available so the most imminent threats can be escalated for action.
Tools for Cyber security

• **Mobile Security:**
Operators and engineers out in the field are increasingly making use of tablets and other mobile devices that, if not managed, can also be vulnerable entry points for attackers. Mobile security allows businesses to secure employee and associate devices, whether they're at their desks, in the field or nearly anywhere in between.

• **Cyber risk monitoring:**
Cyber risk monitoring can provide an easy 360-degree view of the overall security landscape, make regular risk assessments and benchmark specific security information. The technology will provide regular updates in clear language, making it easier to manage and understand. This can help businesses identify security gaps and ultimately develop a focused action plan so money can be spent where it's needed most.
Tools for Cyber security

• Smart energy Cyber Security:

These are intelligent and robust solutions to keep smart energy and smart grids secure and operational. Together these solutions provide flexibility and scalability when it comes to cyber security management, which is key for an industry that is critical to national infrastructure but also undergoing dramatic and rapid changes.
Points to Consider to develop a cyber security Plan

• Industry needs to adopt cybersecurity best practices and develop a risk management culture; cybersecurity regulations are important, but because there is a delay in developing and implementing them, regulations lag behind evolving threats.

• It is important to rapidly share information about cyber threats while respecting privacy guidelines.

• Good cybersecurity requires skilled teams to understand baseline operations, detect and respond to anomalous cyber activity, reduce the “dwell time” of cyber attackers, and implement layered cyber defenses.

• The is a need to understand and increase system resilience to avoid prolonged outages and better recover from cyber attacks.

• In the future, utilize advanced cybersecurity technologies, international approaches to cybersecurity, and machine-to-machine information sharing so the response to cyber incidents takes place in milliseconds—not months.
# NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Identify</th>
<th>Asset Management</th>
<th>Business Environment</th>
<th>Governance</th>
<th>Risk Assessment</th>
<th>Risk Management Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect</td>
<td>Access Control</td>
<td>Awareness and Training</td>
<td>Data Security</td>
<td>Info Protection Processes and Procedures</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
<td>Security Continuous Monitoring</td>
<td>Detection Processes</td>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td>Communications</td>
<td>Analysis</td>
<td>Mitigation</td>
<td>Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td>Improvements</td>
<td>Communication</td>
<td>Improvements</td>
<td></td>
</tr>
</tbody>
</table>

Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020
Defense In Depth Strategy

To Minimize the impact of these attacks, it is important to have multiple layers of cyber security protection.

QUESTIONs?
Page intentionally left blank
Part 3: SCADA Control Board Labs (4)

Learning Objectives

1. Understand the purpose and functions of the SCADA Control Board
2. Describe the layout and function of components on the SCADA Control Board
3. Analyze the data flow paths through the SCADA Control Board
4. Investigate wiring techniques for connecting components on SCADA Control Board
5. Discuss SCADA software and installation steps
Control Board -- Labs 1 & 2 Overview

**Lab1** Network Configurations Using Serial and Internet Protocol Communications

- Lab1 explores various communication protocols that are common to SCADA systems and are supported by the SCADA Control Board. Completing this lab will develop fundamental skills in configuring Serial and Internet Protocol based communications. Completion of Lab1 is necessary to complete Lab3 or Lab4.

**Lab2** Analog Sensors and Analog to Digital Conversions

- Lab2 investigates the SCADA board’s OceanControls WeatherStation conversion of the Voltage and Current Sensor data. Detailed mathematical analysis of the conversion process is used to help predict and correctly display data used in Lab3 SCADA HMI (Human Machine Interface) software.
Control Board -- Labs 3 & 4 Overview

Lab3 Investigating Scada Weather and Power Monitoring HMI Software

• Lab3 utilizes the communications set up in Lab1, and the sensor data scaling function table generated in Lab2, to accurately present Voltage, Current, and Power of sensor measurements. Modifications to SCADA HMI screens and verification of communications parameters help give an understanding of how data is transmitted and displayed in the SCADA software.

Lab4 Working with PLC Ladder Diagrams and Passing Modbus Data to and from SCADA HMI’s

Lab4 builds on Lab1’s communication configurations and introduction to Programmable Logic Controller (PLC) programming. It provides a more in-depth discussion of programming and bidirectional Modbus Communications using a simulated Motor Control HMI screen.
CREATE SCADA Control Board and Labs
Status as of July 1, 2021

8 CREATE SCADA Control Boards have been built and disseminated to faculty at 8 community colleges, who have assembled the control boards and run the associated labs as part of a lab review committee, which itself was an extension of the curriculum review and development.

10 additional CREATE SCADA Control Boards are being delivered to an additional 10 community colleges during summer/fall 2021. Currently the 4 Control Board Labs are being revised; they will be put though the CREATE review process again; and are planned for broad distribution in 2022.

IF YOU ARE INTERESTED IN BEING ONE OF THE TEN FACULTY RECIPIENTS OF THIS CREATE SCADA CONTROL BOARD, PLEASE EMAIL BEN REID AT: SCADA@IMPACTALLIES.COM
Page intentionally left blank
CREATE SCADA commissioned the development of an open source SCADA platform. This system serves two purposes:

1) Colleges can connect their renewable energy assets to it to monitor and share their own energy generation and local conditions, and

2) It is computer-based, allowing students anywhere to freely and without physical equipment understand and work with SCADA systems from a renewable energy technicians point of view.

This simulation software program is available at this URL:
https://scada-student.irsccsdept.org
## SCADA Computer Based Labs (3)

<table>
<thead>
<tr>
<th>Computer-Based Lab:</th>
<th>Related SCADA Curriculum Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 SCADA &amp; HMI Planning and Preparation</td>
<td>Compliments Module 1 (SCADA Overview)</td>
</tr>
<tr>
<td></td>
<td>Integrates with Module 4 (HMI)</td>
</tr>
<tr>
<td>#2 Create Solar Project</td>
<td>Compliment Module 1 (SCADA Overview)</td>
</tr>
<tr>
<td>HMI Simulation</td>
<td>Integrate with Module 5 (Applications in RE Industry)</td>
</tr>
<tr>
<td>#3 Alarm Conditions, Equipment Failure, Output Impact</td>
<td></td>
</tr>
</tbody>
</table>
Before an HMI is created in a software SCADA system, the HMI must be planned. The planning process includes gathering information regarding the available devices, data points, and needs of the operator/user. Then, the levels of display hierarchy must be planned, and data points mapped to each level. This lab builds from the best practices presented in lecture, then plans a two-level HMI display using pen and paper for initial drafts, then Microsoft Paint, and concluding the plan within the simulation software.
Example two-level HMI display with Level 1 displaying the overall plant/system and Level 2 displaying detailed information about the weather station.

<table>
<thead>
<tr>
<th>Device</th>
<th>Data Point</th>
<th>Data Type</th>
<th>Units/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>12v-battery</td>
<td>voltage</td>
<td>number</td>
<td>volts</td>
</tr>
<tr>
<td></td>
<td>current</td>
<td>number</td>
<td>amps</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>discrete</td>
<td>charging, charged, discharging</td>
</tr>
<tr>
<td>basic-inverter</td>
<td>power</td>
<td>number</td>
<td>watts</td>
</tr>
<tr>
<td></td>
<td>fan</td>
<td>number</td>
<td>rpm</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>discrete</td>
<td>charging, charged, discharging</td>
</tr>
<tr>
<td>solar-panel</td>
<td>voltage</td>
<td>number</td>
<td>volts</td>
</tr>
<tr>
<td></td>
<td>current</td>
<td>number</td>
<td>amps</td>
</tr>
<tr>
<td>weather-station</td>
<td>irradiance</td>
<td>number</td>
<td>watts</td>
</tr>
<tr>
<td></td>
<td>temperature</td>
<td>number</td>
<td>fahrenheit</td>
</tr>
<tr>
<td></td>
<td>wind-speed</td>
<td>number</td>
<td>mph</td>
</tr>
<tr>
<td></td>
<td>wind-direction</td>
<td>number</td>
<td>N, NE, E, SE, S, SW, W, NW</td>
</tr>
<tr>
<td></td>
<td>humidity</td>
<td>number</td>
<td>relative humidity</td>
</tr>
</tbody>
</table>
Implement in the simulation software:
Operator (student) creates new project (PV solar system) with the HMI simulation. Student then creates and installs two new devices within the project simulation – one device for an inverter and one device for a weather station – and configures each device with alarm setpoints for critical outputs. Once the devices are created and configured the student will run the data simulation and note any alarm conditions that were triggered.
SCADA Computer-Based Lab
#2 Create Solar Project HMI Simulation

Learning Objectives

• Create a new HMI project
• Understand how to create new devices within the HMI (i.e. weather station and inverter)
• Understand how to set alarm points for different devices and/or data points within a device (i.e. low output, high temperature, etc.)
• Recognize alarm state and be able to identify what alarm condition was triggered
SCADA Computer-Based Lab
#3 Alarm Conditions, Equipment Failure, Output Impact

Operator receives alarm conditions for the inverter for low output. Identify specifics of the equipment failure (what, where,) and the impact to the overall system output.

Learning Objectives:
• Demonstrate use of SCADA data analysis and trend tools
• Demonstrate ability to export data for further/detail analysis
• Utilize troubleshooting skills to identify root cause of decrease in system output
• Utilize data analysis/troubleshooting skills to issue operators report/log of findings and escalate system issue for maintenance and/or engineering follow-up
SCADA Computer-Based Labs

The SCADA Computer-Based Labs are contained in this 21 page document best viewed here:

https://drive.google.com/drive/folders/11NlyFzpKDi5yhr5ymbIF4nlnzvgLRJzu?usp=sharing

Again, the simulation software program is available at this URL:

https://scada-student.irsccsdept.org
End of Presentation

THANK YOU!

Please visit us at:

www.createenergy.org