You may delete this page from the document that follows after reading.
It contains plain language about the copyright we've adopted from **Creative Commons**.

It also contains a link to the summary for our copyright license. This summary should be consulted if you intend to copy and redistribute this material in any medium or format, or adapt, remix, transform, or build upon this material.

Click Here for information on the Creative Commons License we've adopted.

From **Creative Commons**:

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** — You may not use the material for commercial purposes.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

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.

Introduction to SCADA for Renewables
(A Six Module Course)

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

Introduction to SCADA for Renewables

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 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

- https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

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

- https://www.cisco.com/c/en/us/products/security/what-is-network-security.html#~types

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

- https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm

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

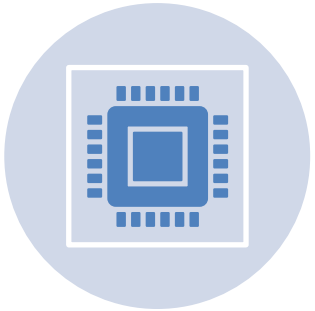
Network Communications

- 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 (1)



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 (2)

- 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://realpars.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?