WHAT IS SCADA Certification?

NREP certifications are recognized by many international, federal, state and local governmental agencies, the military and industry as identifying individuals with the capability, education and work experience to do the job right. NREP is a legally recognized certification and accreditation organization, which has as its mission to provide legal and professional recognition of individuals possessing education, training and experience environmental managers, engineers, technologies, scientists and technicians. Since 1983 to present date, NREP has provided the skilled professional a professionally recognized credential as one would advance in their career and receive appropriate recognition for their highly revered qualification.

NREP has been a leader in offering highly professional certification programs through experience, specialty verification, examination and mentorship that has given the greatest personal and professional benefits to our professional organization's members.

Our new certification for SCADA is in the NEW innovation area of technology that encompasses our environment, health, medicine, food and safety. It is time to look at the interfacing of our Environment to Human to Machine as professionals move into these new areas of engineering, science and medicine through the integration of technology.

SCADA (Supervisory Control and Data Acquisition) was originally a type of Industrial Control System (ICS) that has now branched out into medicine, pharmaceuticals, agriculture, academia, military and many other remote controlled computer systems of data for many other remote controlled computer systems of data storage, analysis and monitoring. The aspect of Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large scale processes that can include multiple sites, and long distances (Example: Earth, Satellite, Space and Cosmos). These processes include industrial, infrastructure and facility-based processes as described below:

Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and many run in continuous, batch, repetitive, or discrete modes.

Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.

Facility processes occur both in public facilities and private ones, including buildings, airports, hospitals, schools, ships and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access and energy consumption. In medicine, one may monitor data gathered from a human body remotely. Recent developments in nanotechnology, biomedicine and life sciences have now incorporated Nano-CMOS, Moffett and MITRI Advanced Computer Systems into an integrated advanced materials, software and data storage/monitoring.

An Outline of Topics to be covered in the NREP Study Guide for SCADA Certification Examination will consist of the following:

1. History of SCADA
2. Common System Components
3. Systems Concepts (Nano, Micro and WI FI)
4. Human-Machine Interface
5. Hardware Solutions (Supervisory Station, Operational Philosophy, and Communication Infrastructure and Methods)
6. SCADA architectures: First generation (Monolithic); Second generation (Distributed), Third generation (Networked) and Fourth generation (Cloud plus)
7. Security and Public Privacy Issues
8. SCADA Protocols
9. Deploying SCADA Systems: twisted-pair metallic cable, coaxial metallic cable, fiber optic cable, power line carrier, satellites, leased telephone lines, very high frequency radio (terahertz); Ultra High Frequency radio (point to point, multiple address radio systems, spread spectrum radio, microwave radio, and terahertz pulse)
10. Security Vulnerability of SCADA Systems (attacks against SCADA Systems and developing a SCADA Security Strategy)