Introduction to SCADA

Most of the slides are from ECE 450/CSE 450 (Fall 2010) taught at Lehigh University by Dr. Liang Cheng and Dr. Shalinee Kishore.

Motivation for SCADA

- Suppose you have a simple electrical circuit consisting of a switch and a light
- This circuit allows an operator to watch the light ( ) and know whether the switch is open or closed. The switch may indicate that a motor is running or stopped, or whether a door is open or closed, or even whether there has been a fault or the equipment is working.

Motivation: Telemetry

- Now imagine that the switch and the lamp were 100 kilometres apart. Obviously we couldn't have an electrical circuit this large, and it would now be a problem involving communications equipment.
- Now complicate the problem a bit further: Imagine we had 2000 such circuits. We could not afford 2000 communications circuits. However someone found that we could use one communications circuit by sharing it.
  - First we send the status (open/closed or 0/1) of the first circuit.
  - Then we send the status of the second circuit, and so on. We need to indicate which circuit the status applies to when we send the data.

Motivation: Automation

- The poor operator at the other end still has a problem. He has to watch all 2000 circuits.
- To simplify his task, we could use a computer: monitor all circuits, and tell the operator when he needs to look at a particular circuit.
- Computer will be told what the normal state of the circuit is and what state is an "alarm". It monitors all circuits, and informs the operator when any circuit goes into alarm.
- Some circuits may contain "analog" data. In these cases the computer will be told a top and bottom level value that are to be considered normal. When the value goes outside this range, the computer will consider this an alarm, and the operator will be informed.
- We could also use the computer to present the information in a graphical manner.

SCADA Possibilities

- A real SCADA system is more complex.
- There are more sites than one. Some have 30,000 to 50,000 "points".
- They usually have "analog" information as well as digital or status information (e.g., numbers such as level of fluid in a tank).
- They can send a status value (e.g., start a pump) as well as receive it (the pump is started).
- And the power of the computer can be used to perform complex sequencing of operations. e.g., OPEN a valve, then START a pump, but only if the pressure is greater than 50.
- Computer can be used to summarize and display the data it is processing. Collecting data and summarising it into reports for operators, and management are normal features of a SCADA system.

SCADA Possibilities (Cont'd)

- Does your equipment need an uninterrupted power supply and/or a controlled temperature and humidity environment?
- Do you need to know — in real time — the status of many different components and devices in a large complex system?
- Do you need to measure how changing inputs affect the output of your operations?
- What equipment do you need to control, in real time, from a distance?
- Where are you lacking accurate, real-time data about key processes that affect your operations?

More Possibilities

- Access quantitative measurements of important processes, both immediately and over time
- Detect and correct problems as soon as they begin
- Measure trends over time
- Discover and eliminate bottlenecks and inefficiencies
- Control larger and more complex processes with a smaller, less specialized staff

SCADA

- SCADA: Supervisory Control And Data Acquisition
- SCADA: An industrial measurement and control system consisting of
  - a central host or master (usually called a master station, master terminal unit or MTU);
  - one or more field data gathering and control units or remotes (usually called remote stations, remote terminal units, or RTU's); and
  - a collection of standard and/or custom software used to monitor and control remotely located field data elements.

The SC and the DA

- Supervisory Control: Giving an operator the ability to control processes and equipment without having to run out in the field and do everything manually.
- Data Acquisition: Collecting process information from all over your plant, displaying it, and storing it for future reference.

So What is SCADA?

- Used to monitor and control plant or equipment.
- Control may be automatic, or initiated by operator commands.
- Data acquisition is accomplished firstly by the RTU's scanning the field inputs connected to the RTU (it may be also called a PLC - programmable logic controller)…typically this is done at a fast rate.
- Central host will scan the RTU's (usually at a slower rate.)
- Data is processed to detect alarm conditions, and if an alarm is present, it will be displayed on special alarm lists.

"DART"

- Displays
  - See everything in ways that make sense to the people who run the place. "Mimic" graphics, trend charts, etc.
- Alarms
  - Monitor process and alert staff
  - Audit logs
- Reports
  - On demand, or generate automatically at the end of the shift/day/week/month/year.
- Trending (Historical data logging; chart recording)
  - Visually analyze process over time
  - Instantaneous recall

What is SCADA? (Cont'd)

- Generally refers to industrial control systems: computer systems that monitor and control industrial, infrastructure, or facility-based processes:
  - Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may 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, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

SCADA Functions

- A SCADA system performs four functions:

1. Data acquisition
2. Networked data communication
3. Data presentation
4. Control

SCADA Subsystems

- A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- Sensors (either digital or analog) and control relays that directly interface with the managed system.
- Remote telemetry units (RTUs). These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.
- SCADA master units. These are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs.
- The communications network that connects the SCADA master unit to the RTUs in the field.

SCADA & DCS

- Contemporary SCADA systems
  - exhibit predominantly open-loop control characteristics
  - utilize predominantly long distance communications, although some elements of closed-loop control and/or short distance communications may also be present.
- Systems similar to SCADA systems are routinely seen in factories, treatment plants etc.
  - Often referred to as Distributed Control Systems (DCS).
  - Have similar functions to SCADA systems, but field data gathering or control units are usually located within a more confined area.

SCADA v DCS

- Communications may be via a local area network (LAN), and will normally be reliable and high speed.
- A DCS system usually employs significant amounts of closed loop control.
- SCADA systems on the other hand generally cover larger geographic areas, and rely on a variety of communications systems that are normally less reliable than a LAN.
- Closed loop control in this situation is less desirable.

Evolution of SCADA

- First generation: Monolithic
  - Computing was done by mainframe computers. Networks did not exist at the time SCADA was developed.
- Second generation: Distributed
  - The processing was distributed across multiple stations which were connected through a LAN and they shared information in real time.
- Third generation: Networked
  - Use standard protocols
  - Many networked SCADA systems are accessible from the Internet

More SCADA Basics

- Data can be of three main types.
  - Analog data (i.e., real numbers) will be trended (i.e., placed in graphs).
  - Digital data (on/off) may have alarms attached to one state or the other.
  - Pulse data (e.g., counting revolutions of a meter) is normally accumulated or counted.
- Interface to the operator is a graphical display (mimic) which shows a representation of the plant or equipment in graphical form.
- Live data is shown as graphical shapes (foreground) over a static background. System may have many such displays, and the operator can select from the relevant ones at any time.

Data Storage

- Distributed database (tag database)
  - Points are normally stored as value-timestamp pairs: a value, and the timestamp when it was recorded or calculated.
  - A series of value-timestamp pairs gives the history of that point.
- A point represents a single input or output value monitored or controlled by the system.
  - A hard point represents an actual input or output within the system
  - A soft point results from logic and math operations applied to other points.

SCADA Simulation

- To see an example SCADA system, visit:

  http://members.iinet.net.au/~ianw/simulate.html
- It shows a simple simulation of a SCADA system being used to control a small water supply system.
- System consists of a number of bores (or water wells) pumping to a collector tank.
- A transfer pump station pumps to a larger storage tank, and the town is supplied by gravity from the storage tank.

Simulator Explanation

- The bores are organized in two "banks" and are controlled by the level in the collector tank. Bank 1 (bores 1 and 3) are the first to operate as the tank level falls. If the level continues to fall Bank 2 (bores 2 and 4) will operate. The display of the "Tank RTU" for the collector tank shows when the RTU is calling for bank 1 or bank 2.
- The main transfer pump station consists of a duty/ standby pair of pumps, which alternate duty to spread the wear. They cannot be operated together. This pump station is controlled by the level in the main tank. The display of the "Tank RTU" for the storage tank shows when the RTU is calling for the pump station to operate.

What to look for in SCADA System?

- **Sufficient capacity to support the equipment at site** … but not more capacity than actually will be use. At every site, you want an RTU that can support expected growth over a reasonable period of time, but it's simply wasteful to spend budget on excess capacity that won't be use.
- **Rugged construction and ability to withstand extremes of temperature and humidity.** SCADA system needs to be the most reliable element in the facility.
- **Secure, redundant power supply.** SCADA system will be up and working 24/7, no excuses. RTU should support battery power and, ideally, two power inputs.

More Things to Look for

- **Redundant communication ports.** Network connectivity is as important to SCADA operations as a power supply. A secondary serial port or internal modem will keep RTU online even if the LAN fails. Plus, RTUs with multiple communication ports easily support a LAN migration strategy.
- **Nonvolatile memory (NVRAM) for storing software** and/or firmware. NVRAM retains data even when power is lost. New firmware can be easily downloaded to NVRAM storage, often over LAN — so RTUs' capabilities can be up to date without excessive site visits.

More Things to Look For

- **Intelligent control.** Sophisticated SCADA remotes can control local systems by themselves according to programmed responses to sensor inputs. This isn't necessary for every application, but it does come in handy for some users.
- **Real-time clock** for accurate date/time stamping of reports.
- **Watchdog timer** to ensure that the RTU restarts after a power failure.

What to Look for in the Master Unit?

- **Flexible, programmable response to sensor inputs.** A system that provides easy tools for programming soft alarms (reports of complex events that track combinations of sensor inputs and date/time statements) and soft controls (programmed control responses to sensor inputs).
- **24/7, automatic pager and email notification.** There's no need to pay personnel to watch a board 24 hours a day. If equipment needs human attention, the SCADA master can automatically page or email directly to repair technicians.
- **Detailed information display.** Display reports in plain English, with a complete description of what activity is happening and how to manage it.

What to Look for…

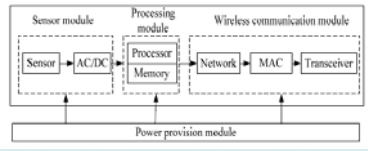
- **Nuisance alarm filtering.** SCADA master that includes tools to filter out nuisance Alarms.
- **Expansion capability.** A SCADA system is a long term **i**nvestment that will last for as long as 10 to 15 years.
- **Redundant, geodiverse backup.** The best SCADA systems support multiple backup masters, in separate locations.. If the primary SCADA master fails, a second master on the network automatically takes over, with no interruption of monitoring and control functions.
- **Support for multiple protocols and equipment types.** Early SCADA systems were built on closed, proprietary protocols. Single-vendor solutions aren't a great idea — vendors sometimes drop support for their products or even just go out of business. Support for multiple open protocols safeguards SCADA system against unplanned obsolescence.

Example: SCADA for Wind Farms

- SCADA system for wind plant is the process control and schedule system of wind power generation.
- It can realize automatic surveillance of wind speed, wind direction, the long-distance online diagnosis and control of wind generator, which provides safeguard for safe and effective running of wind power plant.
- SCADA can
  - guarantee system information integrity,
  - grasp the wind power systems' operation condition exactly,
  - quicken the increase production and the maintenance decision-making,
  - enhance production efficiency, and
  - help correctly diagnoses the system failure condition fast

Wireless SCADA for Wind Farms [1]

- [1] uses Wireless Sensor Networks (WSNs): large number of sensor nodes (deployed on top of wind power generator) which consist of sensor (for measuring wind velocity, direction, generator running status, etc), data processing, power provision and communication modules:



[1] Bai, Meng, Du, Gong, Hu "Design of Wireless Sensor Network in SCADA System for Wind Power Plant," IEEE International Conf. on Automation and Logistics, 2008.

Wireless SCADA for Wind Farms [1]

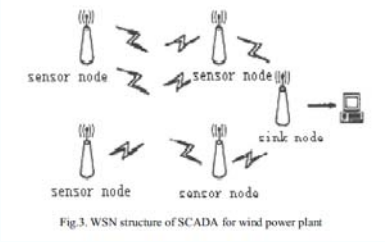
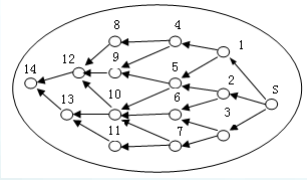


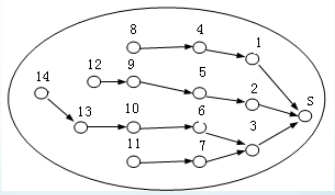
Fig.3. WSN structure of SCADA for wind power plant

- Sink node: receives data from various sensor nodes located in monitoring areas and is responsible for communication with surveillance center through (e.g.,) Internet link.
- Hardware of sink node: CPU, storage unit, RF transceiving modules and GSM wireless communication module.

- [1] is concerned with designing the WSN protocols to enable the SCADA system to operate.
- In particular, the routing of collected data to the MTU.



Task Diffusion from Sink



Set up of transmission route