SCADA On-line over the Internet

May 6, 2011
2011 PNWS-AWWA Conference
Boise, Idaho

Presented by

Garre L. Biladeau P.E.
President
Smarter Process Inc.

Email: garre@smarterprocess.com

Topics of Discussion

- SCADA – Options for Supervisory Control and Data Acquisition
- COMUNICATION & CONTROL - Talking to Remote Locations
- INTERFACE PROTOCOLS – Formats for sending data
- USING THE INTERNET –With IP, Ethernet, and Broadband
- SAFETY AND SECURITY –Is it safe to use the Internet?

SCADA Systems

- Historical Technology – Hard Panels
  - Basic Control Panel - Push Buttons and Lights
  - Analog Data Logging - Tape Machines

- Today's Technology - Computers
  - PLC's - Programmable Logic Controllers
  - HMI - Human Machine Interface Displays
  - Touch Screens
  - Digital Data Logs
  - PC's Personal Computers

COMMUNICATION and CONTROL

- CONTROL STRATEGY
  - Local Control – Basic
  - Central Control – Legacy Computer
  - Distributed Control – Today's Strategy
    - PLC for Local and Computer for SCADA

- COMMUNICATION over Distances
  - Hard Wired – Distance Limited
  - Telephone – Slow Data Transmission
  - Radio – Slow Data Transmission & Distance Limited
  - WiFi – Distance Limited
  - Broadband - Unlimited

COMMUNICATION PROTOCOLS

- SERIAL (RS-232-C, RS-422, RS-485) - Slow
  - Telephone
  - Radio
- PROPRIETARY or INDUSTRIAL
  - Often Related to a Specific Vendor
  - Usually are hard wired
- INTERNET PROTOCOL - (Internet Broadband and WiFi)
  - Becoming the standard for the Internet and Industry
  - Open standard and readily available

INTERNET PROTOCOL

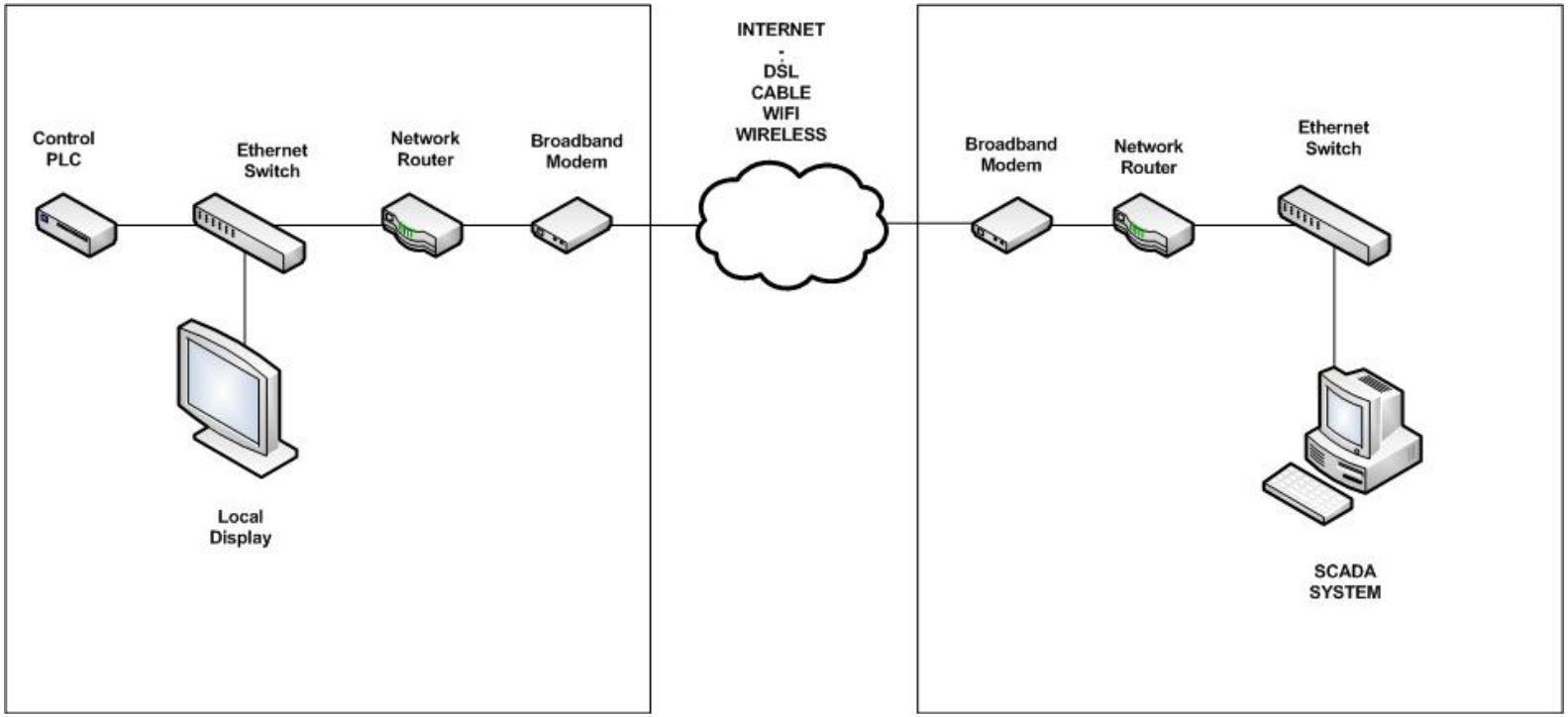
- INTERNET 12 DIGIT NUMBER
  - Think of it like a telephone number (NNN.NNN.NNN.NNN)
    - > 4 billion unique numbers
    - A New version has over a billion, billion, billion, billion unique numbers
  - Dynamic IP
    - Assigned each time you login to your Internet Service Provider (ISP)
  - Static IP
    - Never Changes
  - Domain Name
    - Assigned to Static IP by Domain Name Server (DNS)

Basic Internet Security

- ROUTING (Basic Security Fire Wall to Primary Network)
  - Subnet Addresses
  - Network Access Translation (NAT)
    - Ports
      - Numbers for functions to be directed to Subnet Addresses
        - Website (80)
        - Email (25)

- PORT Numbers Route Data at Both Ends of Communication
  - Router sends Port Functions to SCADA Computer at one end
  - Router sends Port Functions to PLC at the other end
  - Usually requires multiple different ports for SCADA

INTERNET BROADBAND CONNECTION



SECURITY PRACTICES

- Use Routers with NAT
  - Isolate SCADA PC's and PLC's from the Internet and corporate networks.
- Keep PC Operating System Security patches up-to-date.
- Use Anti virus and malware software on all SCADA PC's.
  - Keep Anti Virus software up-to-date
- Use Dedicated SCADA PC's
  - Do not allow Internet Access through Browsers or Email
  - Any other PC Function (Games, Word Processing, etc.)
  - Do not allow use of unapproved Flash Drives, CD's or DVD's

IS THE INTERNET SAFE FOR SCADA?

- YES - If you follow good security practices
- WHAT IS MY BIGGEST THREAT?
  - Disgruntled Employee
- WHAT ABOUT THE "STUXNET" OR OTHER VIRUS?
  - Wasn't "Stuxnet" designed to attach Siemens PLC's?
    - YES, but attached through the PC software interface to the PLC
    - Designed for Specific System Configuration (9 Siemens PLC system)
      - Pakistani Nuclear Centrifuges owned by Iran
      - Designed by INL, CIA and Israeli government (Professionals)

SUMMARY

- SCADA / PLC – Use Distributed Control
- BROADBAND over the INTERNET– Better performance for cost
- INTERFACE PROTOCOLS – Use Ethernet standard
- INTERNET –Use NAT Routers
- SAFETY AND SECURITY – Up-to-date and dedicated systems