Impact of SCADA on Research Projects at the Center for Petroleum Security at the University of Texas at Tyler

Nary Subramanian
Assistant Professor
Department of Computer Science
The University of Texas at Tyler
nsubramanian@uttyler.edu
Phone: 903-566-7309
Texas is the leading crude oil-producing State in the Nation (excluding Federal offshore areas, which produce more than any single State).

The State’s signature type of crude oil, known as West Texas Intermediate (WTI), remains the major benchmark of crude oil in the Americas.

Texas’s 27 petroleum refineries can process more than 4.7 million barrels of crude oil per day, and they account for more than one-fourth of total U.S. refining capacity.

Approximately three-tenths of total U.S. natural gas production occurs in Texas, making it the Nation’s leading natural gas producer.

(Source: US Energy Information Administration)
Petroleum Map of Texas
Petroleum Industry in East Texas

- Referred to as Cotton Valley
- Covers East Texas and Northern Louisiana
- The East Texas Field was 43 miles long and five miles wide and extended into five counties: Rusk, Gregg, Upshur, Smith, and Cherokee.
- At its peak, this field would produce 60 percent of all Texas oil, 37 percent of the oil in the United States, and 22 percent of the oil in the world.
- There are eight treatment plants and seven processing plants
- Several pipeline systems go through East Texas
Security Issues in Petroleum Industry

- Physical damage to infrastructure including pipelines
  - Physical access control for plants
  - Maps and notices for pipelines
  - Accidents or intentional damage
Security Issues in Petroleum Industry

- On June 7, 2010, a gas pipeline in Johnson County, Texas. Caused by workers installing poles for electrical lines. One worker killed, six injured.

- On September 9, 2010, a high pressure gas pipeline exploded in San Bruno, CA, a suburb of San Francisco. The blast destroyed 38 homes and damaged 120 homes. Eight people died and many were injured. Ten acres burned in total
Security Issues in Petroleum Industry

- Logical systems vulnerability
  - DCS
  - SCADA
  - PLC’s, RTU’s

Example:
In 1999 a 16-inch gas pipeline ruptured in Bellingham, Washington, because a SCADA system fault locked out engineers from the control room preventing them for relieving pressure on valves in the pipeline.
What is SCADA?

- **SCADA** is the abbreviation for *Supervisory Control And Data Acquisition*.

- It generally refers to an industrial control system: a computer system monitoring and controlling a process.

- The process can be industrial, infrastructure or facility
Industrial processes include:
- manufacturing,
- production,
- power generation,
- fabrication, and
- refining.
Infrastructure processes include

- water treatment and distribution,
- wastewater collection and treatment,
- oil and gas pipelines,
- electrical power transmission and distribution, and
- large communication systems.
SCADA Systems

- Facility processes include
  - buildings, airports,
  - ships, and
  - space stations.

- They monitor and control HVAC, access, and energy consumption.
What is SCADA?
SCADA Architecture

- Archive
- Gas Inlet Valve
- Control Computer
- Archive
- Operator
- Furnace
SCADA Architecture

RTU

RTU

RTU

Oil Pipeline

Communication Links

Master Station
Levels of Control

- Geographical distribution
- More Control automation
- Equipment reliability
- Software reliability
- Security

Level 4

- Control Automation
- Equipment Reliability
- Programmability of controls
- Bandwidth requirements

Level 3

- Equipment Reliability
- Reduction of operators
- Remote controllability

Level 2

- Controllable
- Operator Dependability
- Communication Requirements

Level 1

- Simplicity
- Functional
- Cost Effective
- Automation of Manual Labor

Level 0
SCADA Market

- Oil and gas: to grow at 9% over next five years; to reach almost $1.5 Billion by 2012
- Water and wastewater: to grow at 5% over next five years; to reach almost $300 Million by 2012
- Electric power: to grow at 6% over next five years; to reach almost $2 Billion by 2012
Major Players

- GE
- HP
- Harris
- Siemens
- IBM
- Sun Microsystems
- ABB
- And many others
• Critical infrastructure protected by SCADA systems
• Reliability of SCADA extremely important
• Security of SCADA extremely important
• Very little standardization
• Monitor flow of crude oil through pipelines
  o from source to destination
  o from source to storage tank farms
  o typically rate of flow is the main item measured
    ▪ low bandwidth of communication
    ▪ sufficient to have sensors at start and end points
SCADA Usage in Petroleum Industry

- Monitor flow of natural gas through pipelines
  - typically rate of flow and pressure are measured
  - "packing" and "unpacking" occurs to meet elastic demand
- Pipe segments are geographically distributed and could be tens to hundreds of miles long
DCS Usage in Petroleum Industry

- DCS used in:
  - offshore oil rigs
  - DCS used in tank farms
  - DCS used in oil refineries
- In a refinery, storage tanks separate SCADA and DCS
- In a refinery, the most important inputs to a DCS are temperature, pressure, flow rate, and level
- Sometimes conveyor belts are controlled and in that case speed is an important input
- In a refinery, control is almost always a valve.
- Another item controlled is pump start/stop.
SCADA Parameters Evaluated

- Physical Parameters Measured:
  - Flow rate
  - Pressure
  - Temperature
  - Level
  - Speed
  - Valve status
  - Pump status

- Properties that are important
  - Reliability
  - Security
  - Redundancy
Important Research Issues

- DCS does not use wireless sensors most of the time
  - problems include:
    - reliability
    - metals (usually steel) interacts with wireless
    - power supply
    - wiring wireless sensors costs $10/feet
  - some refineries trying out wireless sensors for flares monitoring
    - measures flow and gas analysis
    - transmits data to a WiFi access point
Important Research Issues

- Internet based control is not supported
  - chief problem is reliability
  - practitioners prefer complete separation of DCS system from enterprise system
Academic Research Centers for Petroleum Engineering

- UTA's Center for Petroleum and Geosystems Engineering
  - http://www.cpge.utexas.edu
  - encourage and develop interdisciplinary research in petroleum and geosystems
Academic Research Centers for Petroleum Engineering

- Texas Tech's Center for Applied Petrophysical and Reservoir Studies
  - http://www.depts.ttu.edu/pe/dept/research/caprs.php
  - to promote interdisciplinary research in petroleum industry
Academic Research Centers for Petroleum Engineering

- University of Houston's Composites Engineering and Application Center
  - http://www.egr.uh.edu/CEAC/
  - to undertake research in support of the reliable and the economical use of composite materials in onshore and offshore operations.
Center for Petroleum Security Research

- CPSR to be set up at UT Tyler
- Funded by Department of Justice
- Will be interdisciplinary
- Will be supported by local industry including Delek Refining at Tyler
- Will focus on SCADA and DCS security research
Impact of CPSR on Research

- Considering SCADA systems of systems
- Evaluating SCADA NFRs
- Automating SCADA designs
  - Synthesis
  - Analysis
SCADA systems of systems

- System Security Control
- Power Grid
- Network Management
- SCADA/DCS
- Physical System
Impact of CPSR on Curriculum

• CPSR can aid curriculum development

• Serve as the location for lab experiments

• Serve as the training place for faculty members

• Potential impact on Computer Information Systems Program – SCADA security management?

• Potential impact on Computer Science Program – SCADA security?
Typical Approach to Introducing SCADA in CIS

- Programming covered in first year
- Networking part of senior year
- Project management part of senior year capstone course
- SCADA basics could be an elective (junior/senior)
- SCADA lab could be an additional 1 credit elective (junior/senior)
SCADA Course

- Basics
- Protocols (ModBus, FieldBus, ProfiBus, DNP)
- RTU Technologies
- Master Station Technologies
- HMI
- System Architecture
- System Integration
- Project
- Presentation
SCADA Lab

- SCADA System Design
- SCADA System Implementation
- Interfacing systems using standards
- Development of HMI
- PLC implementation
- Integrating PLC to SCADA System
- Simulations of SCADA System
- Extensions
Sequence for SCADA Minor

- C++/C# .NET programming (COSC 1137, COSC 4309)
- HMI (COSC 4309)
- Project management (COSC 4375)
- Networking (COSC 4325)
- Elective: SCADA + Lab
- Security (COSC 4361)
- Total: 19 credit hours
CPSR Development

- Hire researchers in SCADA security
- Collaborate with other research centers
- Collaborate with other Universities: SMU, for example
- Collaborate with industry
Challenges

• Industry collaboration is almost a must
  • Problems solved by the Center should be relevant
  • Solutions should be testable in an industrial environment
  • Different sections of the industry – drilling, transportation, and refining – will need to participate
• Academia should introduce certificates, minors, and programs
  • Relevant texts
  • Home department?
  • Industry needs have to be addressed
  • Standardization – on the lines of ABET
Conclusions

• SCADA is a rapidly growing industry segment
• SCADA for petroleum industry is a rapidly growing niche
• Few centers for petroleum research consider SCADA
• CPSR to be set up at UT Tyler with DOJ funding
• CPSR will include SCADA research as a major component
• CPSR will drive both research and curriculum development
References

