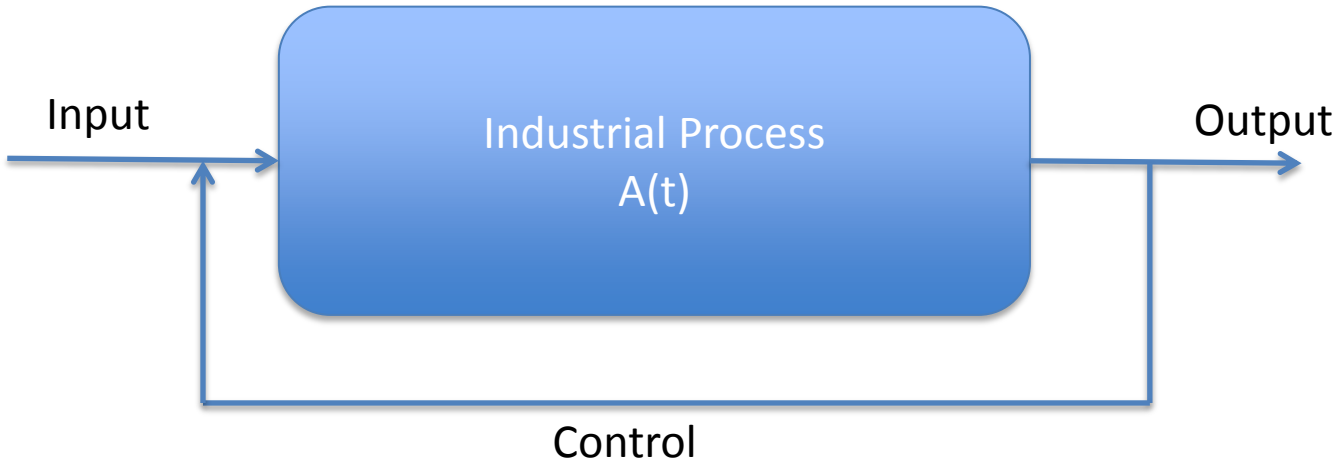
# SCADA System

TCIPG RG 1

# Industrial Systems




**SCADA**: Supervisory Control and Data Acquisition
The SCADA system monitors and {automatically or manually} controls the an industrial process.

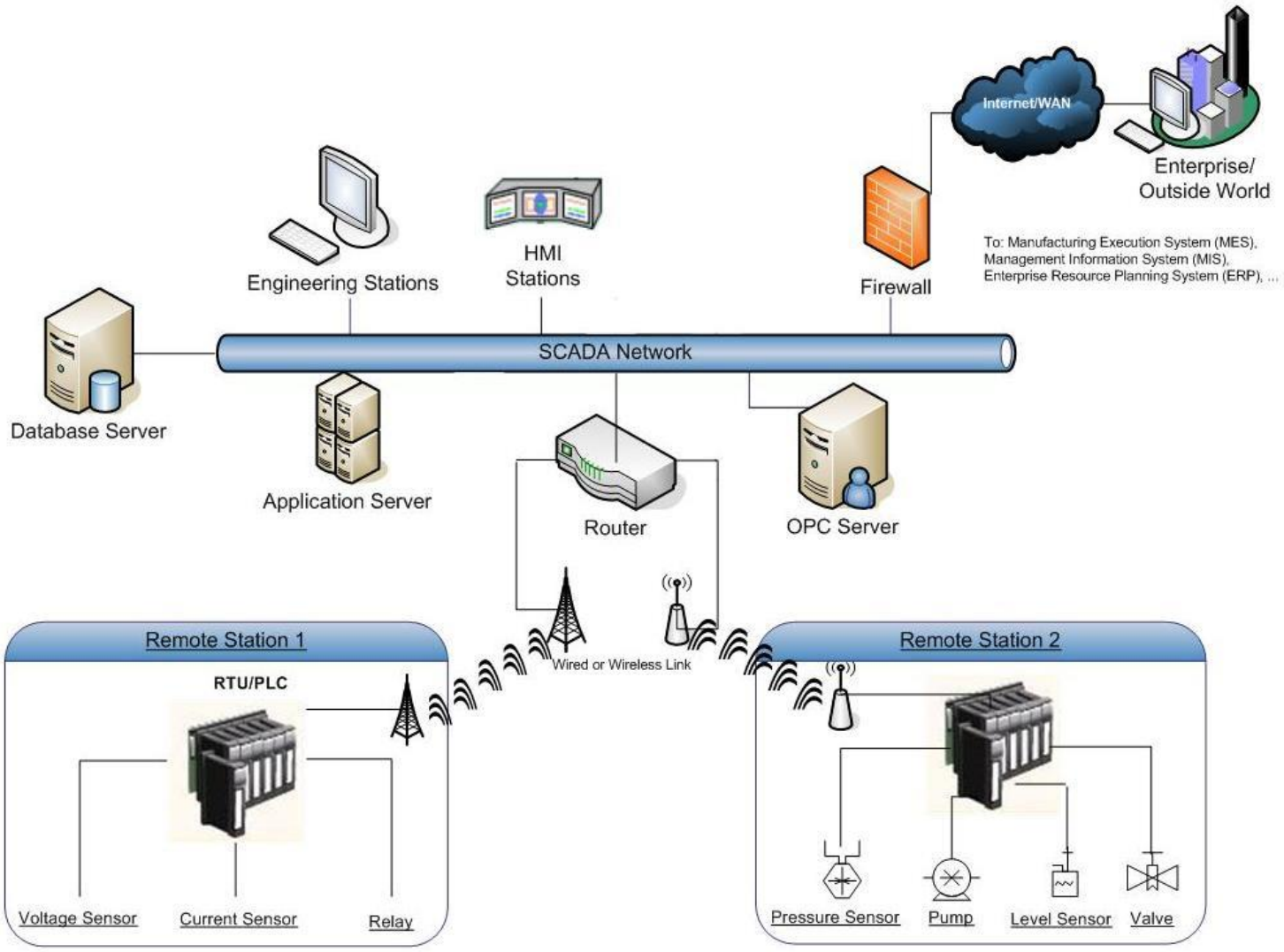
# Types of Processes

- Power generation and transmission
- Oil and Gas
- Air traffic and railways
- Water management
- Manufacturing

# In real life SCADA controls…

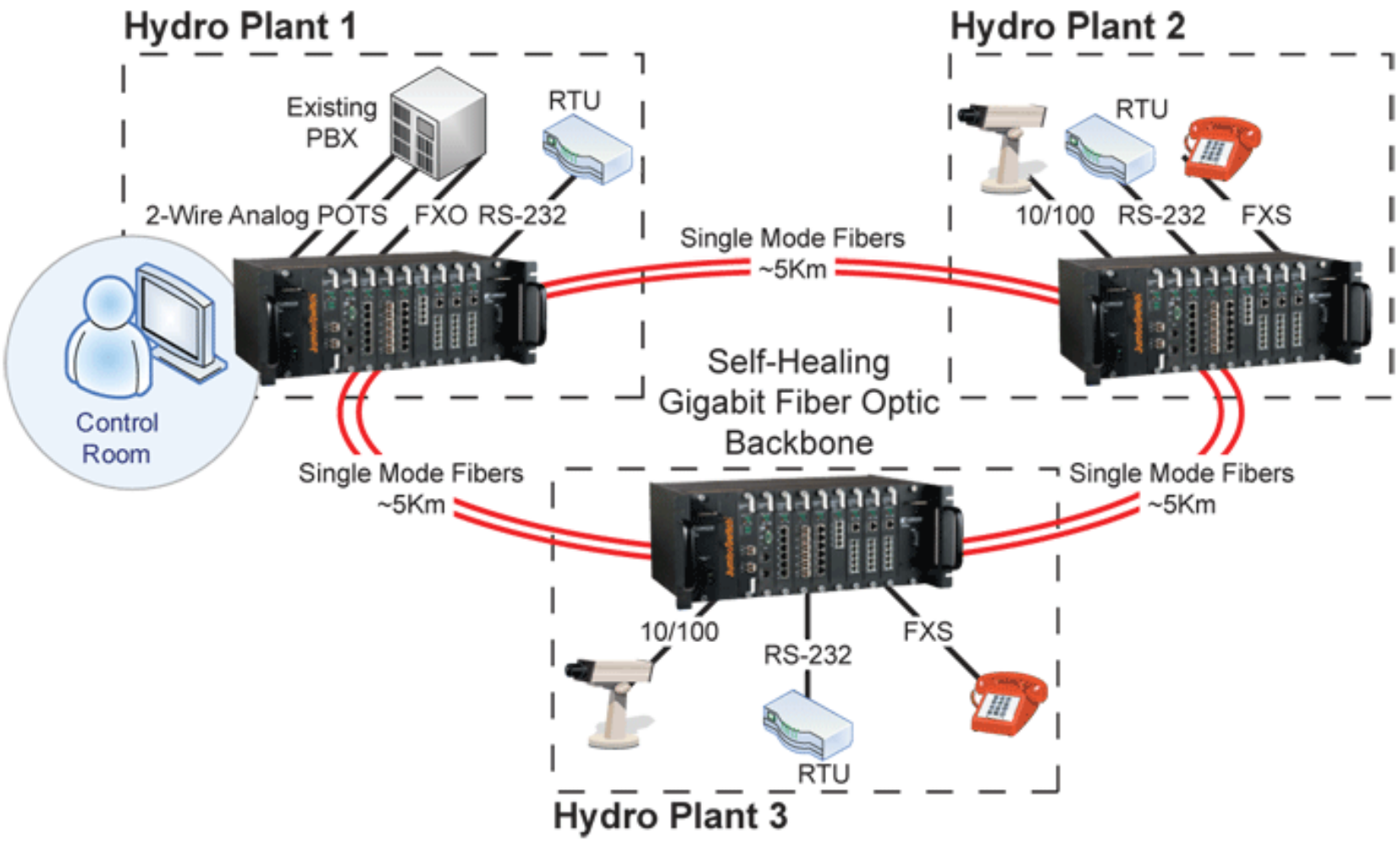
- The power in your home
- The water in your home
- Where the water goes from your home
- The traffic lights on the way to the office
- The commuter train controls
- The air conditioning system in your office building
- The phone system to your home

# SCADA topology



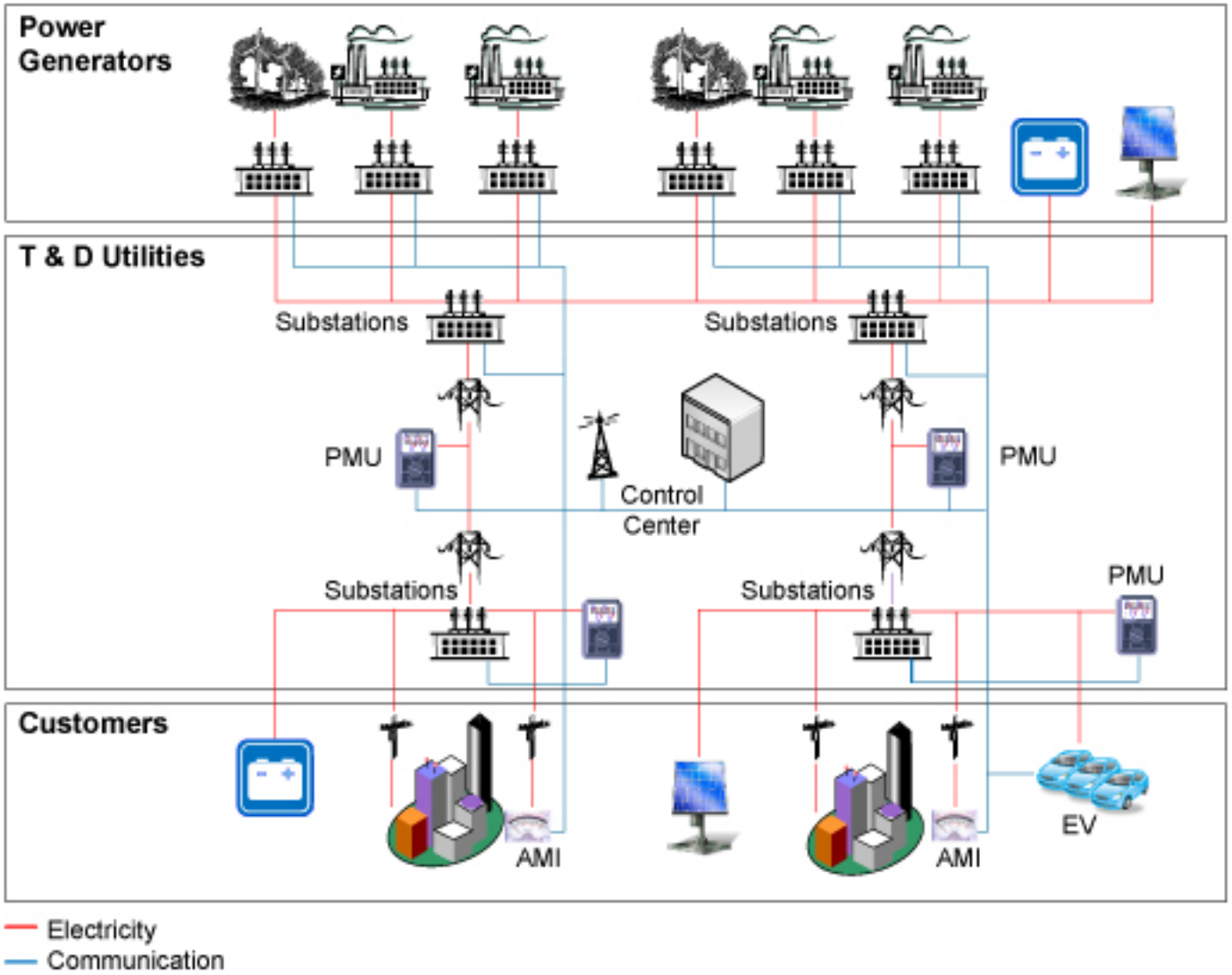

**OpenControl SCADA Network Architecture**

# Another Example

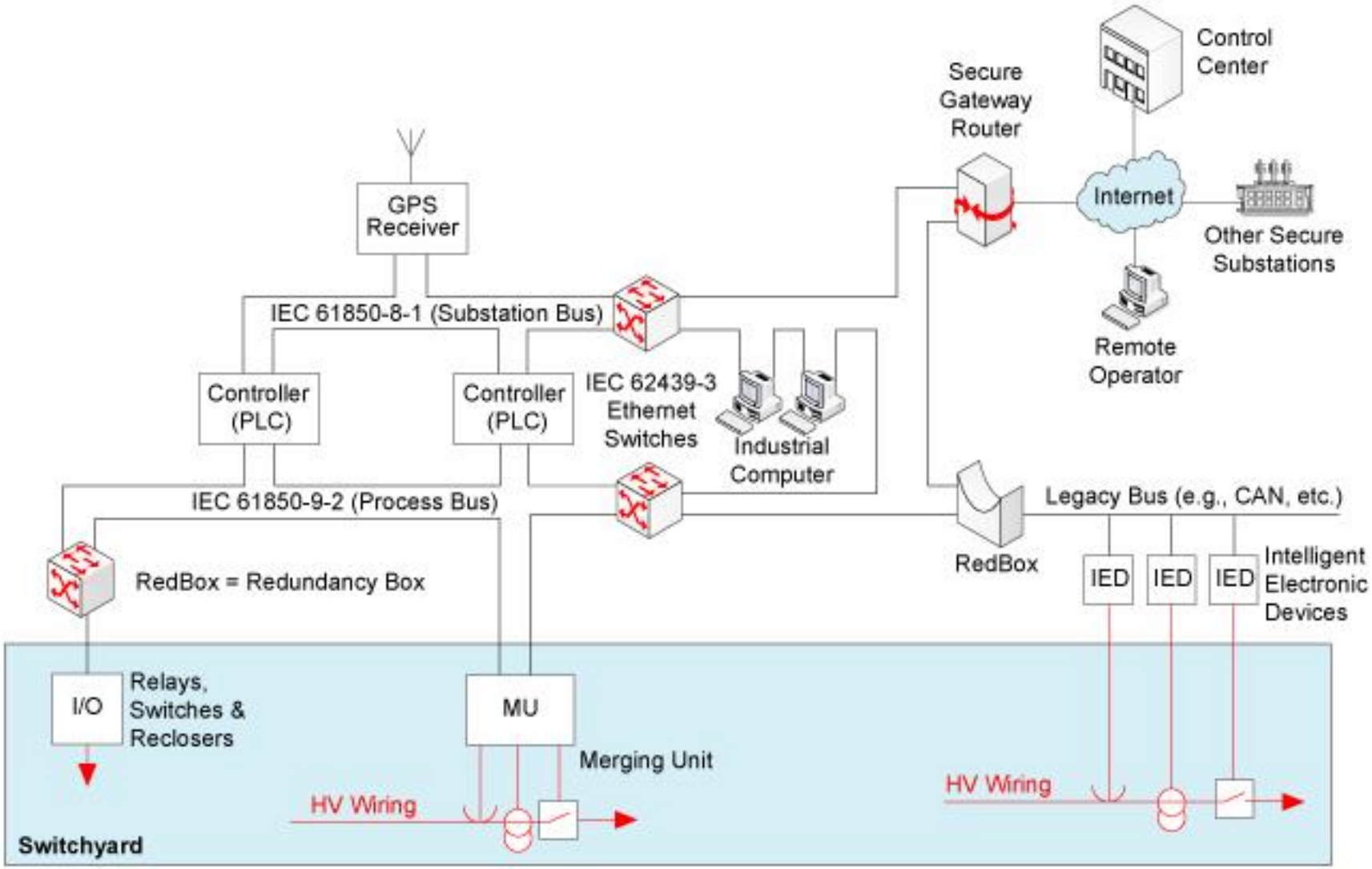


# Human-Machine Interface (HMI)

# Power Utility



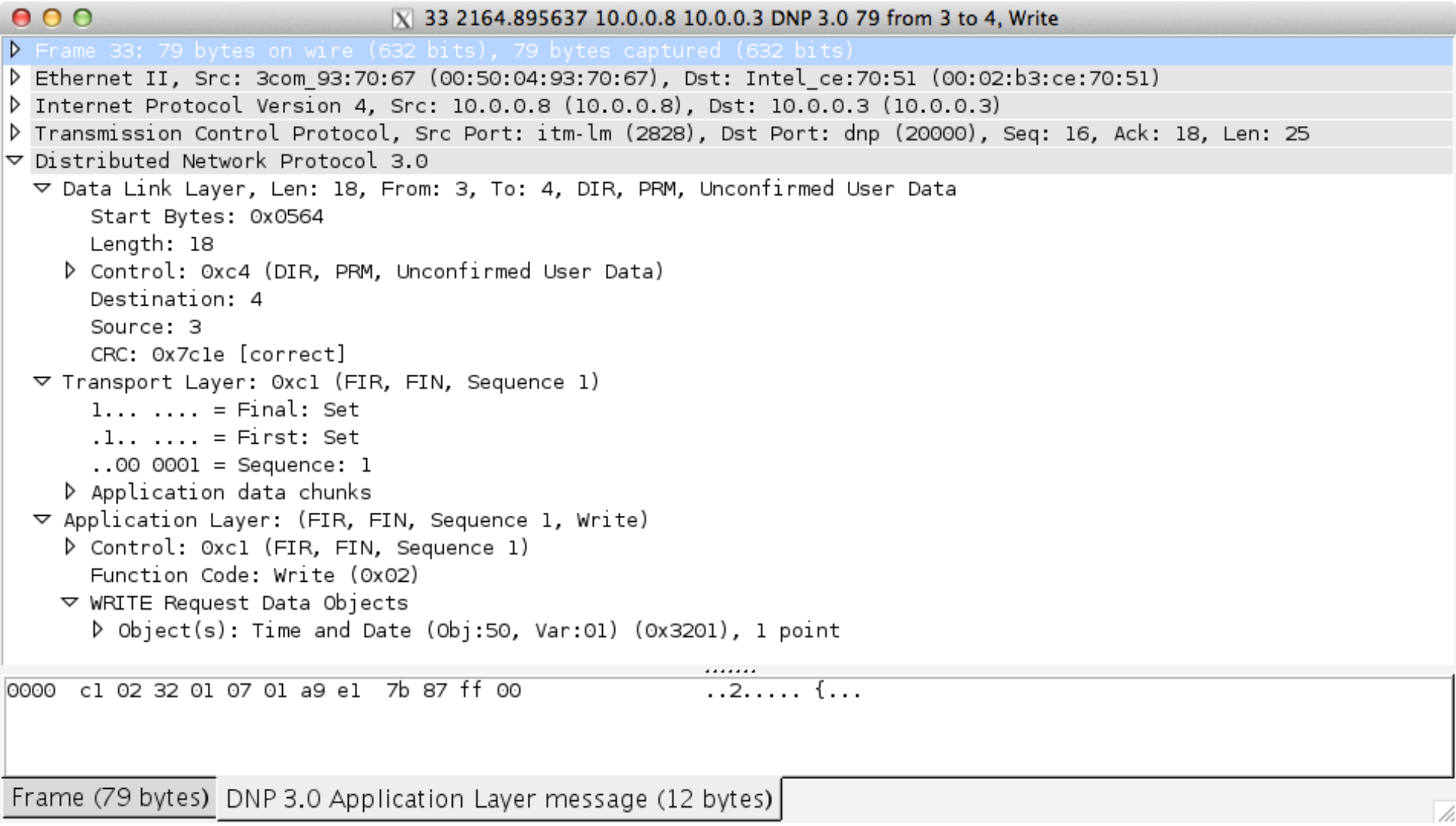
# Substation Connection



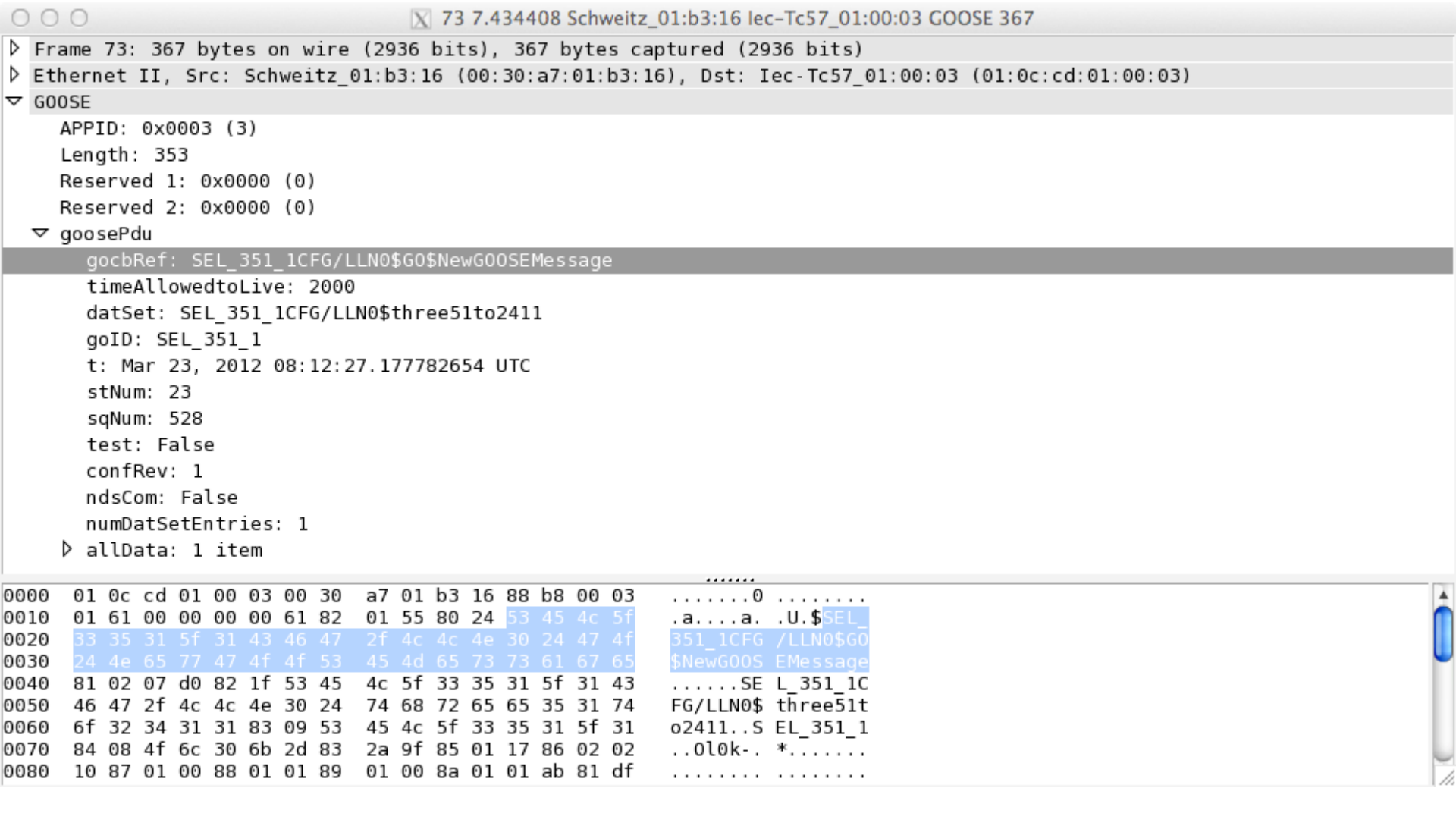
# Protocols Used

- Raw binary protocols
  - DNP3 and modbus
  - Designed for serial links
  - Reads data and sends commands and alerts
- High-level data protocols
  - ICCP
  - Uses XML for communication
  - Human readible

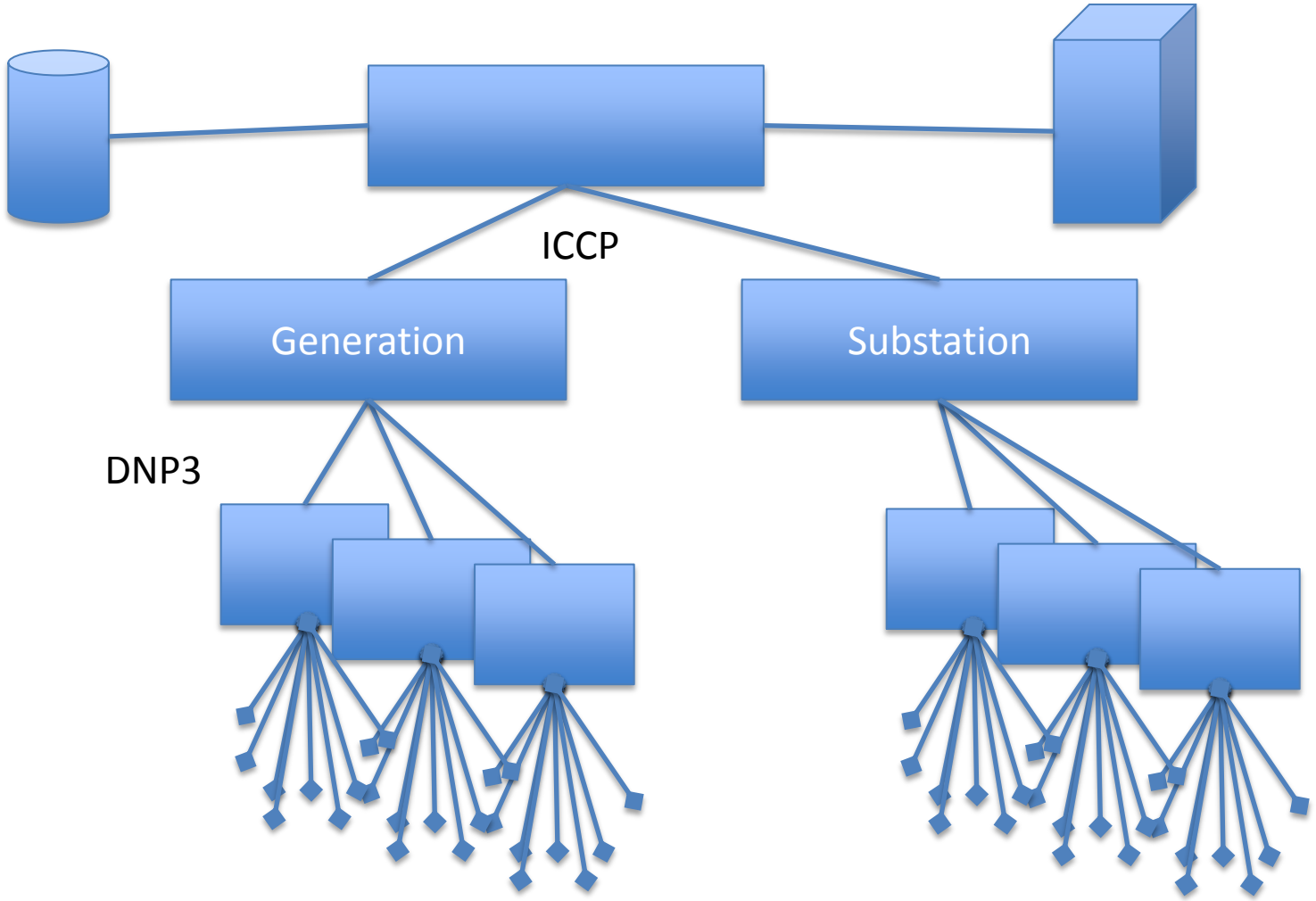
# DNP3


33 2164.895637 10.0.0.8 10.0.0.3 DNP 3.0 79 from 3 to 4, Write
Frame 33: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
Ethernet II, Src: 3com_93:70:67 (00:50:04:93:70:67), Dst: Intel_ce:70:51 (00:02:b3:ce:70:51)
Internet Protocol Version 4, Src: 10.0.0.8 (10.0.0.8), Dst: 10.0.0.3 (10.0.0.3)
Transmission Control Protocol, Src Port: itm-lm (2828), Dst Port: dnp (20000), Seq: 16, Ack: 18, Len: 25
Distributed Network Protocol 3.0
Data Link Layer, Len: 18, From: 3, To: 4, DIR, PRM, Unconfirmed User Data
Start Bytes: 0x0564
Length: 18
Control: 0xc4 (DIR, PRM, Unconfirmed User Data)
Destination: 4
Source: 3
CRC: 0x7c1e [correct]
Transport Layer: 0xc1 (FIR, FIN, Sequence 1)
1... .... = Final: Set
.1.. .... = First: Set
..00 0001 = Sequence: 1
Application data chunks
Application Layer: (FIR, FIN, Sequence 1, Write)
Control: 0xc1 (FIR, FIN, Sequence 1)
Function Code: Write (0x02)
WRITE Request Data Objects
Object(s): Time and Date (Obj:50, Var:01) (0x3201), 1 point
0000 c1 02 32 01 07 01 a9 e1 7b 87 ff 00 ..2..... {...
Frame (79 bytes)
DNP 3.0 Application Layer message (12 bytes)

# GOOSE


73 7.434408 Schweitz_01:b3:16 Iec-Tc57_01:00:03 GOOSE 367
Frame 73: 367 bytes on wire (2936 bits), 367 bytes captured (2936 bits)
Ethernet II, Src: Schweitz_01:b3:16 (00:30:a7:01:b3:16), Dst: Iec-Tc57_01:00:03 (01:0c:cd:01:00:03)
GOOSE
APPID: 0x0003 (3)
Length: 353
Reserved 1: 0x0000 (0)
Reserved 2: 0x0000 (0)
goosePdu
gocbRef: SEL_351_1CFG/LLN0$GO$NewGOOSEMessage
timeAllowedtoLive: 2000
datSet: SEL_351_1CFG/LLN0$three51to2411
goID: SEL_351_1
t: Mar 23, 2012 08:12:27.177782654 UTC
stNum: 23
sqNum: 528
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 1
allData: 1 item
0000 01 0c cd 01 00 03 00 30 a7 01 b3 16 88 b8 00 03 .....0 .....
0010 01 61 00 00 00 00 61 82 01 55 80 24 53 45 4c 5f .a....a. .U.$SEL_
0020 33 35 31 5f 31 43 46 47 2f 4c 4c 4e 30 24 47 4f 351_1CFG /LLN0$GO
0030 24 4e 65 77 47 4f 4f 53 45 4d 65 73 73 61 67 65 $NewGOOS EMessage
0040 81 02 07 d0 82 1f 53 45 4c 5f 33 35 31 5f 31 43 ......SE L_351_1C
0050 46 47 2f 4c 4c 4e 30 24 74 68 72 65 65 35 31 74 FG/LLN0$ three51t
0060 6f 32 34 31 31 83 09 53 45 4c 5f 33 35 31 5f 31 o2411..S EL_351_1
0070 84 08 4f 6c 30 6b 2d 83 2a 9f 85 01 17 86 02 02 ..Ol0k-. *.....
0080 10 87 01 00 88 01 01 89 01 00 8a 01 01 ab 81 df ..... .....

# Protocols



# Security Issues

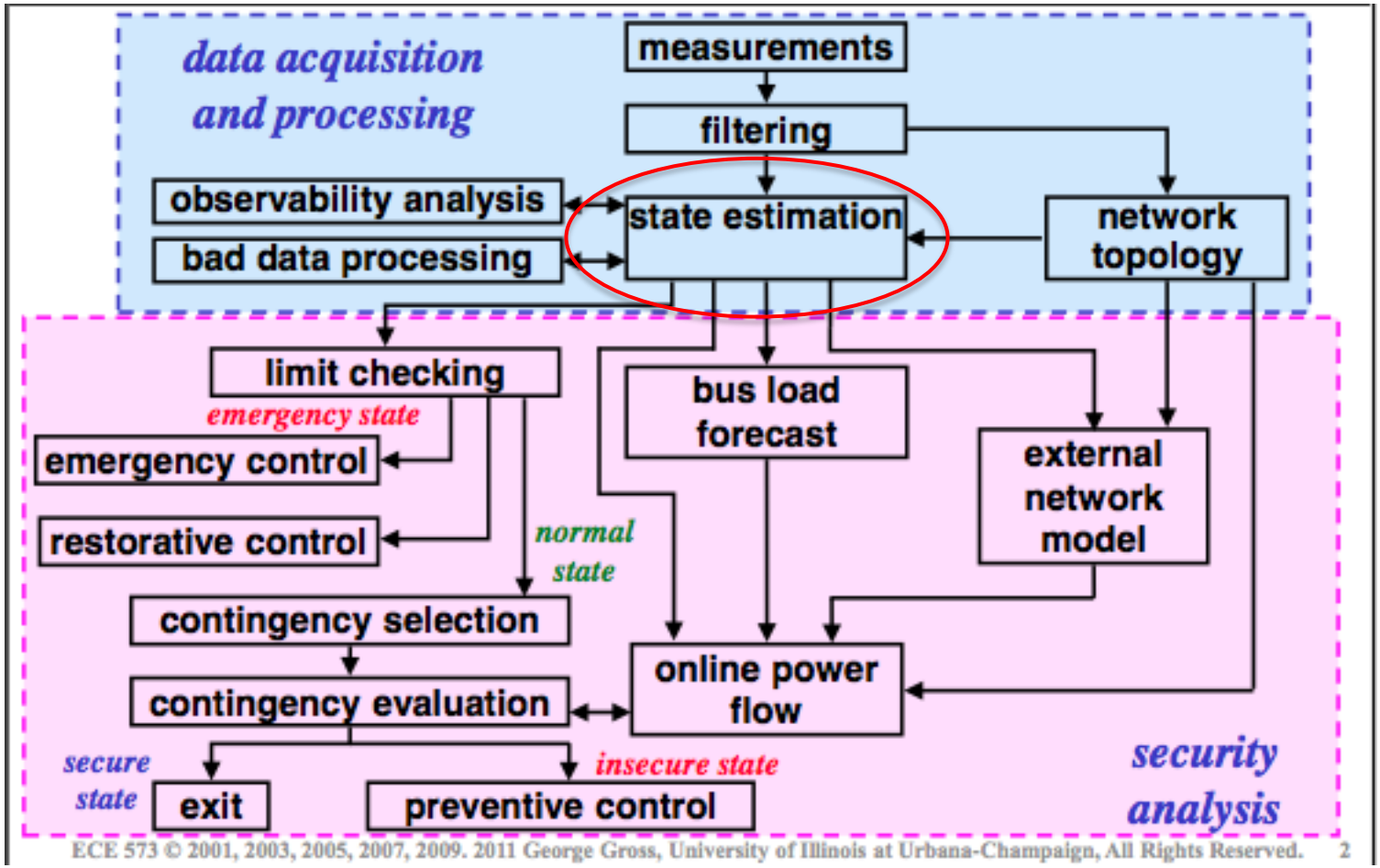
- SCADA does not authenticate users or devices
  - All SCADA protocols do not implement authentication. Trust assumption
- Patching is really hard
  - Devices have to be taken offline for patching
- Believe they are not connected
  - Laptops roam around (WiFi)
  - Ex. Historians are a possible leak
- Old Modems

# SCADA Functions in Power Systems

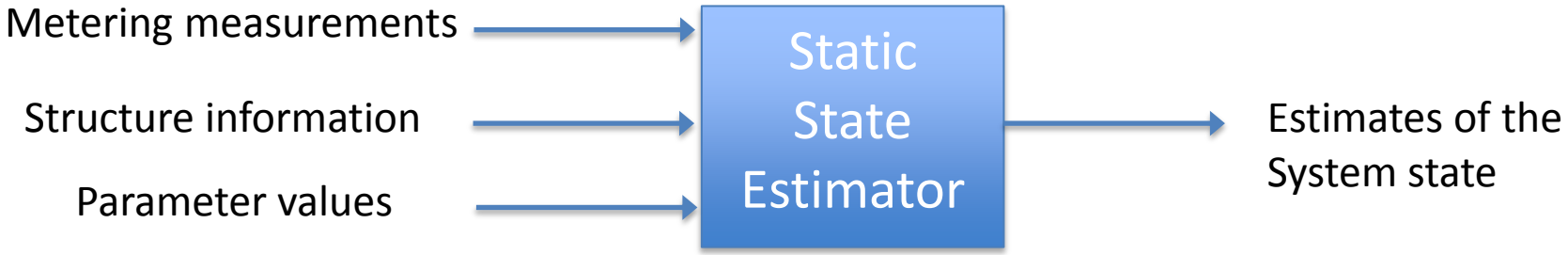
- Another commonly used term is *energy management system (EMS)*, which is a broader concept.
  - An energy management system (EMS) is a system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system.
  - The monitor and control functions are known as SCADA; the optimization packages are often referred to as "advanced applications". They are closely related.

# SCADA: Monitoring

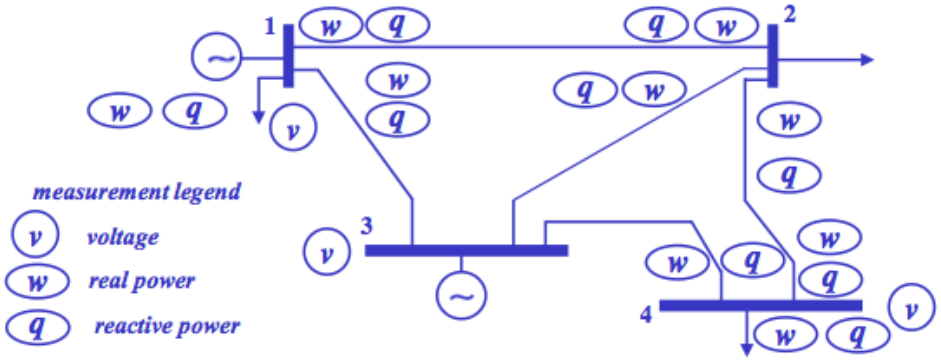
- State estimation is the core



# State Estimation




- Typical measurements used for state estimation:
  - Real and reactive power flows on the lines; -Bus voltage magnitudes at generation;
  - Transformer tap settings; -Real and reactive power loads at load buses;
- System state
  - voltage magnitude and angle
- Example:




- 21 measurements,
- 7 state variables

# State Estimation

- Basic assumption
  - Power system is in the *quasi-steady-state* condition
- Problem formulation

$$z = h(x) + \nu \Longleftrightarrow$$ Power flow equations

- Estimation method
  - weighted least-squares (WLS) estimation
- Security consideration
  - bad data detection (incorporation of PMU data)

# SCADA: Control

- In EMS, the time hierarchy for operations and control decisions

| Time Scale | Load Variations | Function in EMS | Decision |
|---|---|---|---|
| seconds | small, random | automatic control | Match the on-line generation with the load |
| minutes | large | economic dispatch | Allocate economically load among the committed generating units |
| days and hours | wide | unit commitment | Start-up and shutdown of units |
| weeks | very wide swings | Fuel, hydro, and maintenance scheduling | Meet load with the installed resource mix |

# SCADA: Control

- SCADA control mechanisms:
  - Voltage control:
    - Var compensation, in-phase transformer tap settings
  - Frequency control: AGC
  - Topology change: line switching
  - Load shedding: the last resort
  - Protection device (e.g., relays) parameter setting
- Security consideration:
  - The impact of malicious control command is hard to evaluate.