SCADA: A Deeper Look

Jeff Dagle

Pacific Northwest National Laboratory

P.O. Box 999, M/S K5-20; Richland WA 99352

509-375-3629; Fax: 509-375-3614;
jeff.dagle@pnl.gov

Battelle

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

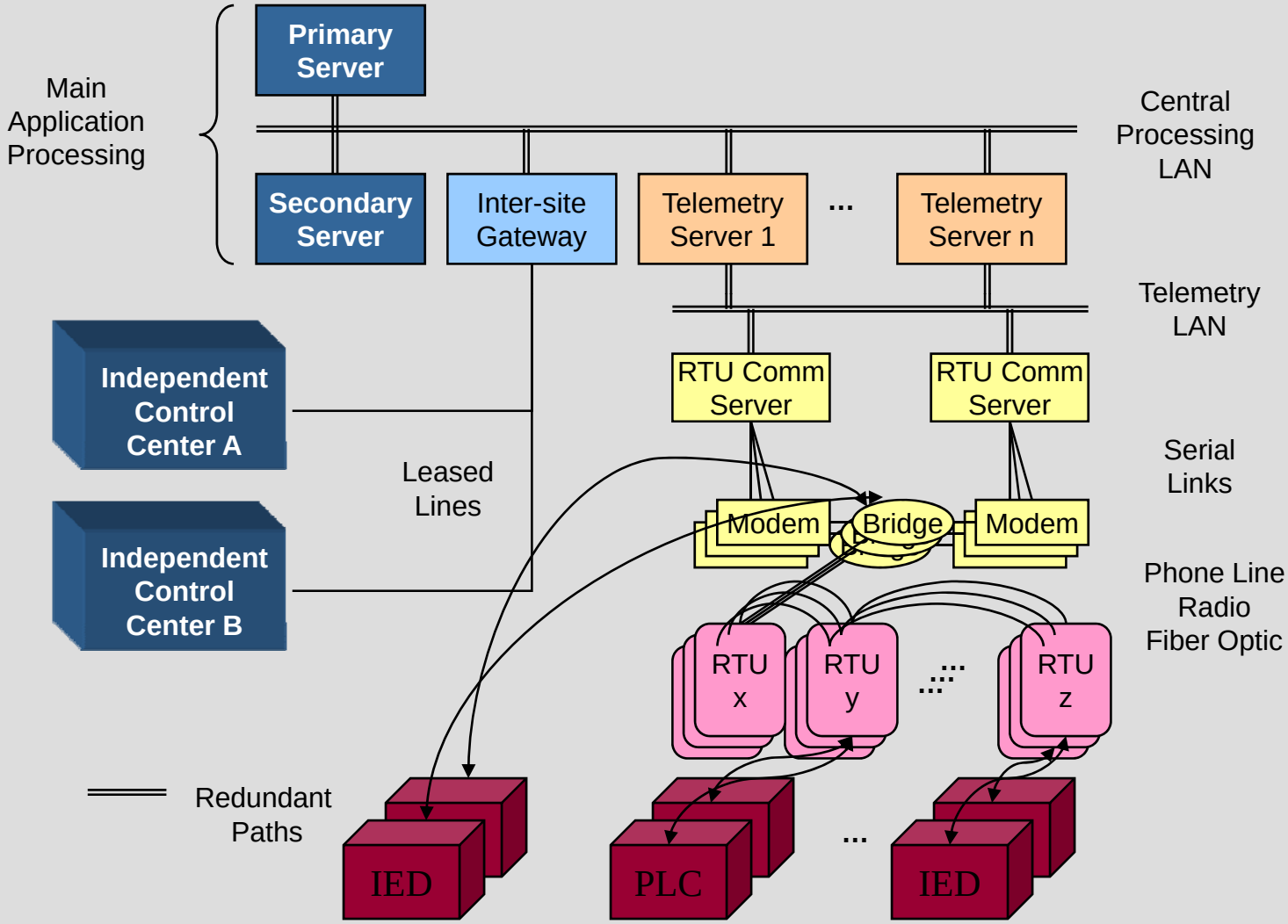
Outline

- Vendors
- Protocols
- DNP 3.0 Protocol Example
- Demonstration

SCADA Principles of Operation

- Interface with Physical Devices
  - Remote terminal unit (RTU)
  - Intelligent electronic device (IED)
  - Programmable logic controller (PLC)
- Communications
  - Directly wired
  - Power line carrier
  - Microwave
  - Radio (spread spectrum)
  - Fiber optic

Typical SCADA Architecture



Major SCADA/EMS Vendors

- Asea Brown Boveri (ABB)
- Siemens
- Alstom ESCA
- Telegyr Systems
- Advanced Control Systems (ACS)
- Harris
- Bailey

SCADA Protocols (Partial List!)

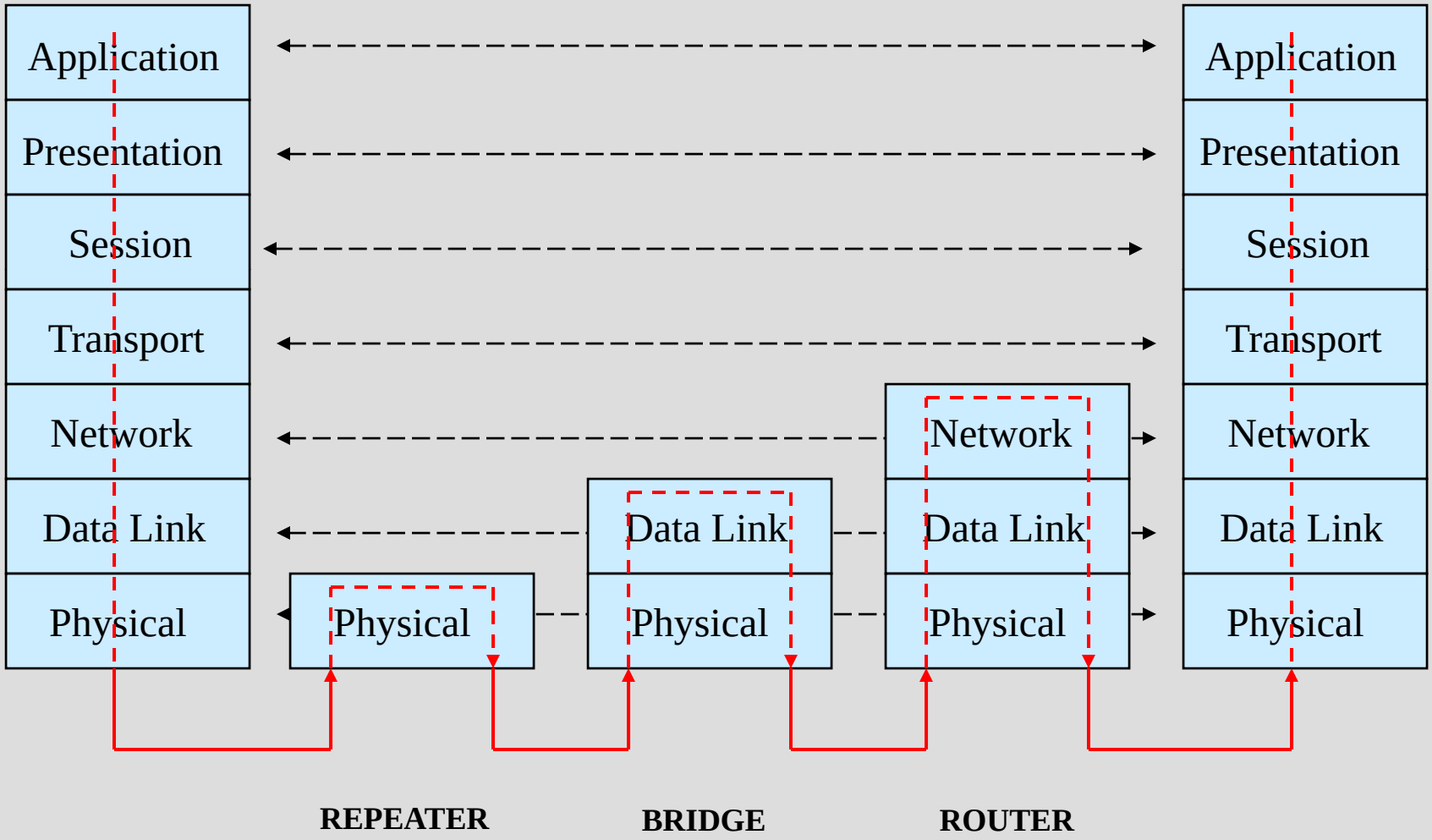
- ANSI X3.28
- BBC 7200
- CDC Types 1 and 2
- Conitel 2020/2000/3000
- DCP 1
- DNP 3.0
- Gedac 7020
- IBM 3707
- Landis & Gyr 8979
- Pert
- PG&E
- QEI Micro II
- Redac 70H
- Rockwell
- SES 91
- Tejas 3 and 5
- TRW 9550
- Vancomm

Protocol Background

International Standards Organization Open System Interconnection Reference Model
ISO OSI Reference Model (protocol stack)

7 Application	Provides interface to application services
6 Presentation	Data representation
5 Session	Starts, maintains, and ends each logical session
4 Transport	End-to-end reliable communications stream
3 Network	Routing and segmentation/reassembly of packets
2 Data Link	Transmit chunks of information across a link
1 Physical	Transmit unstructured bits across a link

Intermediate Nodes



Simplified Protocol Stack

International Electrotechnical Commission (IEC)
Enhanced Performance Architecture (EPA)

3 Application	Provides interface to application services
2 Data Link	Routing and segmentation/reassembly of packets
1 Physical	Transmit bits of information across a link

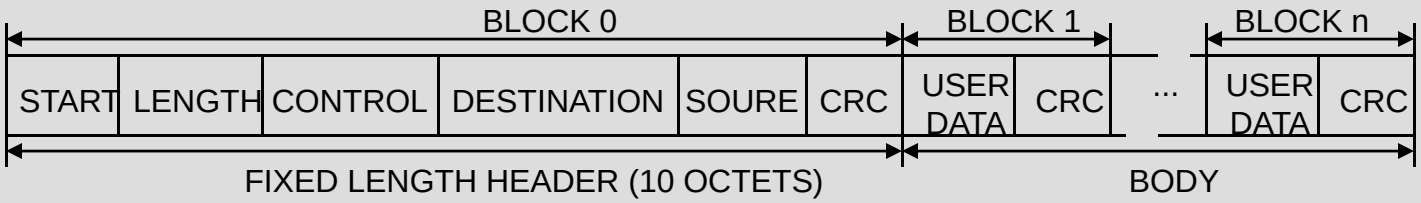
SCADA Protocol Example

- Distributed Network Protocol (DNP) 3.0
- SCADA/EMS applications
  - RTU to IED communications
  - Master to remote communications
  - Peer-to-peer instances and network applications
- Object-based application layer protocol
- Emerging open architecture standard

DNP 3.0 Data Link Layer

- Interface with the physical layer
  - Packing data into the defined frame format and transmitting the data to the physical layer
  - Unpacking frames received from physical layer
  - Controlling all aspects of the physical layer
- Data validity and integrity
  - Collision avoidance/detection
  - Perform message retries
- Establish connection, disconnection in dial-up environment

DNP 3.0 Data Link Layer

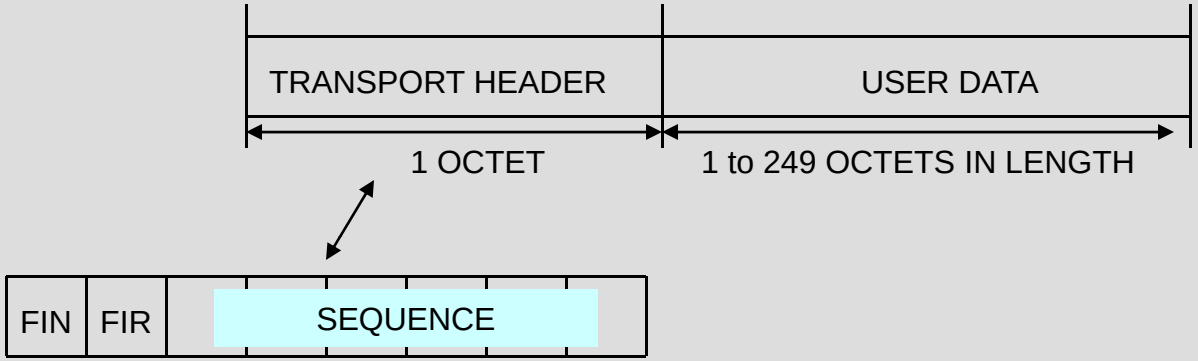


START	2 starting octets of the header
LENGTH	1 octet count of USER DATA in the header and body
CONTROL	1 octet Frame Control
DESTINATION	2 octet destination address
SOURCE	2 octet source address
CRC	2 octet Cyclic Redundancy Check
USER DATA	Each block following the header has 16 octets of User defined data

DNP 3.0 Transport Function

- Supports advanced RTU functions and messages larger than the maximum frame length in the data link layer
- Additional data integrity verification
- Packs user data into multiple frames of the data link frame format for transmitting the data
- Unpacks multiple frames that are received from the data link layer
- Controls data link layer

DNP 3.0 Transport Function



FIN	0 = More frames follow
	1 = Final frame of a sequence
FIR	1 = First frame of a sequence
	0 = Not the first frame of a sequence
SEQUENCE	Number between 0 and 63 to ensure frames are being received in sequence

DNP 3.0 Application Layer

- Communications Interface with Application Software
- Designed for SCADA and Distributed Automation Systems
- Supported functions include
  - send request
  - accept response
  - confirmation, time-outs, error recovery, etc.

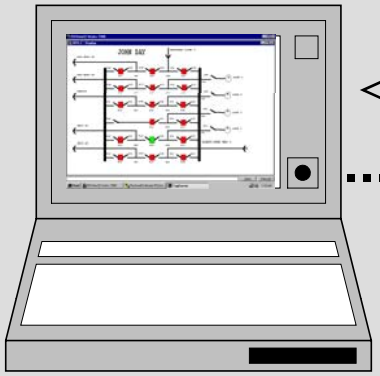
SCADA Trends

- **Open protocols**
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- **Interconnected to other systems**
  - Connections to business and administrative networks to obtain productivity improvements and mandated open access information sharing
- **Reliance on public information systems**
  - Increasing use of public telecommunication systems and the internet for portions of the control system

Vulnerability Concerns

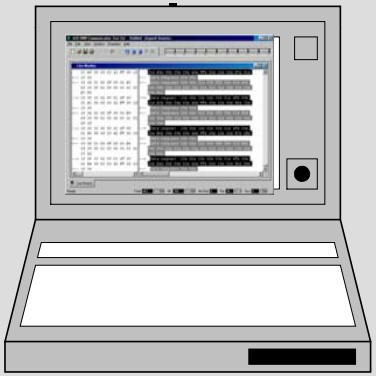
- **Confidentiality**
  - Protecting information from unauthorized access
  - Important for deregulation, competitive intelligence
- **Integrity**
  - Assuring valid data and control actions
  - Most critical for real-time control applications
- **Availability**
  - Continuity of operations
  - Important for real-time control applications
  - Historically addressed with redundancy

Laboratory SCADA Vulnerability Demonstration

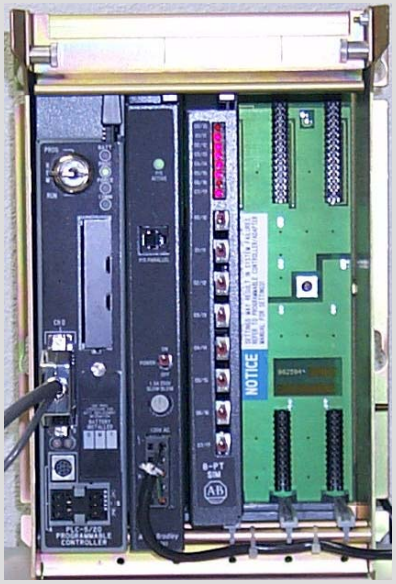


SCADA Protocol (DNP 3.0)

Operator Interface



Protocol Analyzer (Intruder)



Field Device

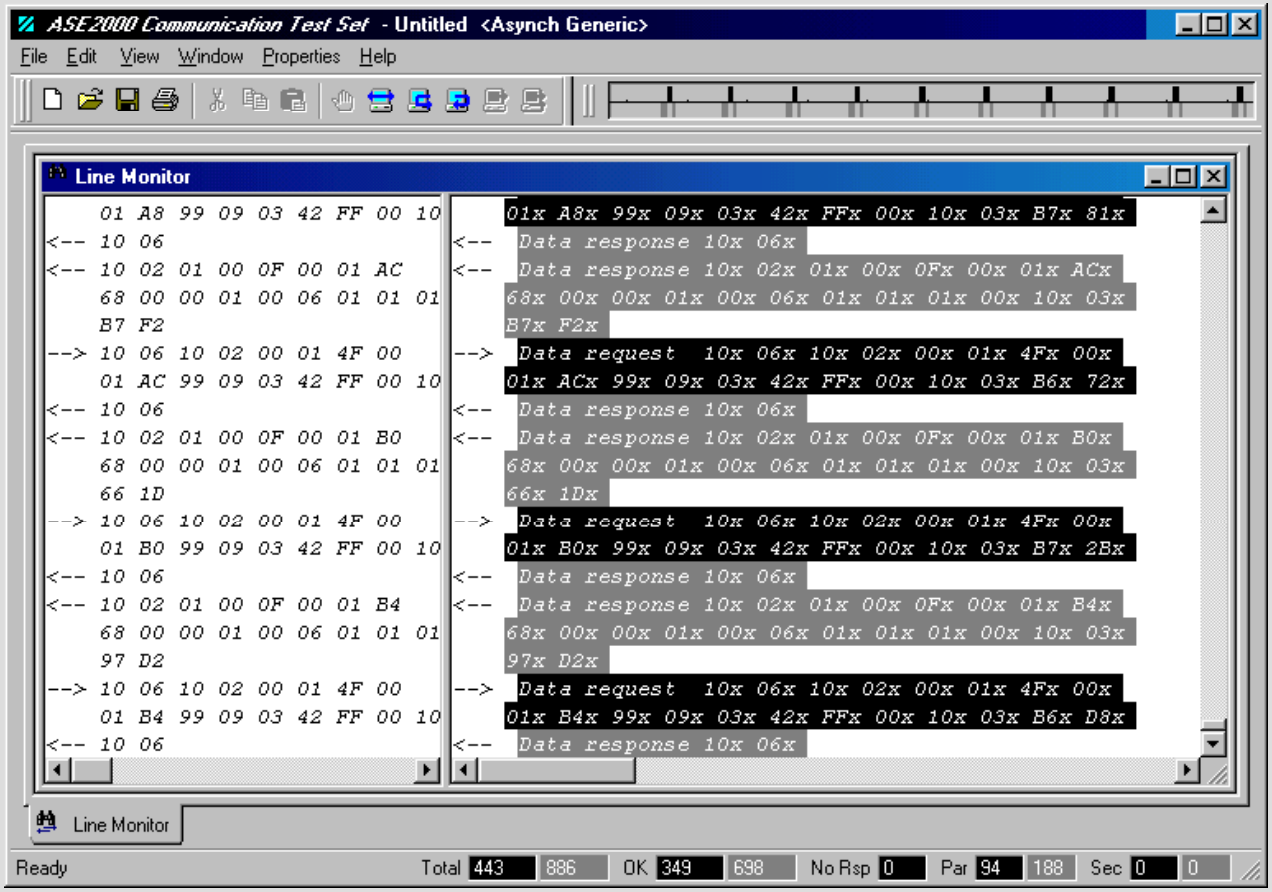
- Remote Terminal Unit (RTU)
- Intelligent Electronic Device (IED)
- Programmable Logic Controller (PLC)

Scenarios

- Denial of service
- Operator spoofing
- Direct manipulation of field devices
- Combinations of above

Vulnerability implications vary significantly depending on the scenario and application

SCADA Message Strings



Repeating easily decipherable format

Captured by RTU test set

Mitigation Strategies

- **Security through obscurity**
  - Poor defense against “structured adversary”
- **Isolated network**
- **Communication encryption**
  - Concerns over latency, reliability, interoperability
  - Vendors waiting for customer demand
- **Signal authentication**
  - May provide good defense without the concerns associated with full signal encryption

IEEE Standard 1402-2000

- IEEE Guide for Electric Power Substation Physical and Electronic Security
- Provides definitions, parameters that influence threat of intrusions, and gives a criteria for substation security
- Cyber methods considered:
  - passwords
  - dial-back verification
  - selective access
  - virus scans
  - encryption and encoding

Additional Countermeasures to Consider

- Implement access control with strong passwords
- Implement automatic reporting/intrusion detection features
- Create a multi-tiered access hierarchy
- Implement application level authentication and packet level data encryption
- Consider implementing public key infrastructure (PKI)
  - When properly implemented, PKI certificates enable authentication, encryption, and non-repudiation of data transmissions
- Implement properly configured firewalls and intrusion detection systems
- Have a defined Enterprise-level computer network security policy

Ref: *Concerns About Intrusion into Remotely Accessible Substation Controllers and SCADA Systems*, Schweitzer Engineering Laboratories, www.selinc.com

Steps for Enhancing SCADA Security

- Establish a robust network architecture
- Eliminate trusted remote access points of entry
- Evaluate and deploy technology and approaches to enhance confidentiality, availability, and integrity
- Implement rigorous configuration management
- Provide adequate support and training
- Never become complacent!

Conclusions

- Vendors
  - Relatively few
  - Mostly foreign
- Protocols
  - Several protocols being used
  - Trend toward open protocols
- DNP 3.0 Protocol Example
  - Emerging standard in the electric SCADA industry