HANDS-ON
DATA COMMUNICATION, NETWORKING AND TCP/IP TROUBLESHOOTING

YOU WILL LEARN HOW TO:

- Set up, configure and troubleshoot RS-232and 2-wire as well as 4-wire RS-485 links
- Set up and configure basic Ethernet networks containing hubs, switches and routers, and troubleshoot these networks down to the packet level
- Configure IP parameters, and do basic TCP/IP troubleshooting down to the packet level by means of DOS and Windows utilities such as IP address and port scanners as well as protocol analysers
- Troubleshoot Modbus serial and Modbus TCP systems down to byte level
- Set up IEEE802.11 Access Points in Infrastructure and Point-to-Point mode, do site surveys and sniff packets
- Implement authentication and encryption on IEEE 802.11Wireless LANs

WHO SHOULD ATTEND:

This workshop is designed for personnel with a need to understand the techniques required to use and apply industrial communications technology as productively and economically as possible. This includes engineers and technicians involved with:

- Control and Instrumentation
- SCADA and Telemetry Systems
- Process Control
- Electrical Installations
- Consulting
- Design
- Process Development
- Control Systems
- Maintenance Supervisors
- Project Management
- Instrumentation

The Workshop

Data Communication is given high priority in today's industrial environment. This course is designed to be hands-on, providing the participants with essential knowledge and helping them to understand and troubleshoot systems.

This is a comprehensive two-day hands-on workshop that covers practical aspects of Data Communication such as serial communications, Ethernet networking, TCP/IP, Modbus, wireless communications and security.

This course is for enthusiastic engineers and technicians who wish to develop and enhance their practical knowledge in the field of data communications and networking. It will help them to understand the concepts behind data transmission, the various protocols involved, and the topologies that govern data exchange among various systems in industry. It will also equip them with the skills and tools to design and/or maintain these systems on an ongoing basis.

Pre-requisites:

This course is for enthusiastic engineers and technicians who wish to develop and enhance their practical knowledge in the field of data communications and networking. It will help them to understand the concepts behind data transmission, the various protocols involved, and the topologies that govern data exchange among various systems in industry. It will also equip them with the skills and tools to design and/or maintain these systems on an ongoing basis.

The Program

1. SERIAL DATA COMMUNICATIONS

- Asynchronous serial communication basics

PRACTICAL EXERCISES

- RS-232, RS-485 basics
  - Setting up the software
  - RS-232 basics
  - RS-232 point-to-point communication
  - RS-232 via Virtual null modem
  - RS-485 basics (2W and 4W) using Listen 32 software, voltmeter and oscilloscope (if available)

2. ETHERNET AND TCP/IP NETWORKING

NETWORKING BASICS (BRIEF REVIEW)

- Ethernet
- TCP/IP protocol suite
- Internet layer (OSI Layer 3) protocols: IP, ARP, ICMP
- Host-host layer (OSI Layer 4) protocols: TCP, UDP
- Application layer (OSI Layer 5/6/7) protocols: FTP, HTTP, Telnet
- Utilities
- Network components

NETWORK CONSTRUCTION

PRACTICAL EXERCISES

- Constructing a simulated Wide Area Network simulation with hubs/switches and pre-configured Cisco 2500 routers
- IP configuration (IP addresses, Subnet Masks, Default Gateways) of hosts

BASIC SYSTEM CHECKS

PRACTICAL EXERCISES

- IP configuration checks (ipconfig, wntipcfg)
- Router configuration checks using IOS commands via Telnet
- Switch configuration checks using browser
- Connectivity checks (ping, arp, tracert)
- Name resolution (Hosts file, Lmhosts file)

TROUBLESHOOTING THE MEDIUM

- Fiber connectivity – basic checks
- Cat5 connectivity (damaged and mis-wired cabling, with cable tester)

TROUBLESHOOTING AT LAYER 2

- Ethernet packet analysis with Wireshark
- Checking Ethernet NIC driver configuration

TROUBLESHOOTING AT LAYER 3

PRACTICAL EXERCISES

- Checking stack operation with loop-back test
- Tracing Ethernet packet contents between subnets with Wireshark
- Detecting duplicate IP addresses
- Automatic IP address allocation (DHCP server down)

2. ETHERNET AND TCP/IP NETWORKING (CONT.)

TROUBLESHOOTING AT LAYER 4

PRACTICAL EXERCISES

- Checking TCP connections, observing TCP sequence numbers and acknowledgements with Wireshark
- Scanning ports on hosts with advanced ports scanner
- Scanning ports on hosts with NMap
- Checking TCP/UDP delay and data rate between hosts on WAN with IXIA QuickCheck

3. INDUSTRIAL PROTOCOLS: MODBUS

MODBUS SERIAL

- Basic client/server concept
- Addressing scheme
- Message structure

PRACTICAL EXERCISES

- Master/Slave simulation over null modem

MODBUS TCP

- Basic concept
- Message structure

PRACTICAL EXERCISES

- Master/Slave simulation over Ethernet and TCP/IP
- Modbus Serial/TCP gateway (Moxa Nport 6110)

4. WIRELESS

- IEEE802.11 Wireless LAN Overview

PRACTICAL EXERCISES

- Setting up Cisco Aeronet Access Point
- Configuring an access point as Workgroup bridge to establish a point-to-point link (wireless bridge) with two Cisco Aeronet access points
- Sniffing wireless packets with Wireshark
- Quick site survey
- Measuring Signal-to-Noise ratio with Netstumbler

5. SECURITY

- Basic security issues
- WPA2 encryption (AES)
- WPA2 authentication
  - Personal mode
  - Enterprise mode

PRACTICAL EXERCISES

- Enabling encryption (AES) on a Wireless LAN
- Authentication via RADIUS server

SUMMARY, OPEN FORUM AND CLOSING