Pipeline SCADA - Future Proofing

Prepared by Trihedral for KROHNE Academy 2013

Keith Donaldson

Agenda

1. Introduction (Make sure you have completed Pre-test)
2. Overview
3. SCADA and Telemetry Defined
4. Typical SCADA Upgrade Scenarios
5. Potential Problems
6. Suggested Solutions using SCADA Technologies
7. Combining Legacy and Current Equipment
8. Modernization Considerations
9. Summary
10. Q & A
11. Post-test

WELCOME !

Some housekeeping items before we get too far (and forget !)

Upon satisfactory completion of this course, you will receive CEU and/or CPE credits. Phoenix Contact is an authorized provider of CEUs licensed through the International Association for Continuing Education and Training (IACET).

Satisfactory completion requirements are as follows:

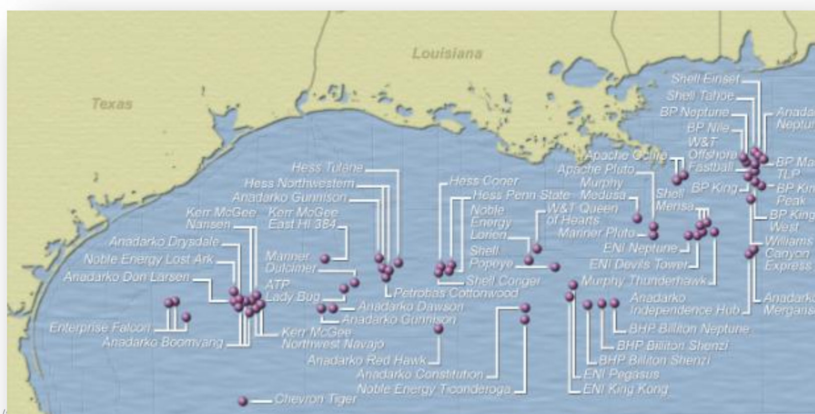
- Beginning of session – sign in sheet and pre-test
- End of session – post test and class evaluation

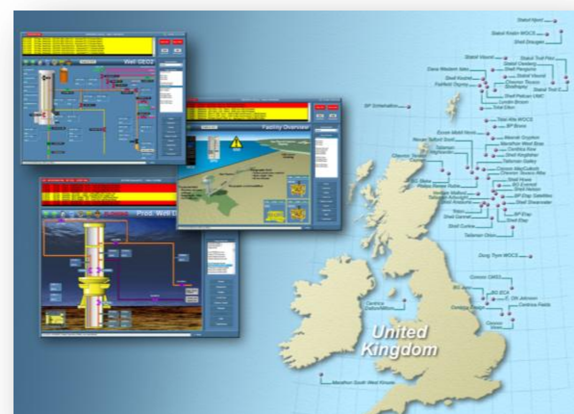
After completion of the course, the instructor will submit the class information to the corporate office training department.

CEU certificates will be mailed to each participant that fulfills the course requirements (meaning we need your mailing address!)

Trihedral Introduction

- Trihedral was founded in 1986 as an HMI (Human Machine Interface) software provider.
- Our software, VTS™ and VTScada™, is installed in thousands of applications worldwide, via direct and indirect sales. The oil & gas sector is largely served via OEM's who re-label the software as their own to serve a variety of specific applications.
- Trihedral has an active engineering group that supports end-customers and OEM's when they request custom SCADA developments. These endeavours can range from short "one-off's" to product or application "evolutions" over many years in various sizes. Since the average life of these systems is at least 10 years, it is not uncommon to encounter needs to change or upgrade SCADA hardware.
- Since Trihedral is hardware independent, we often become involved in designing solutions that permit inter-operability between competing hardware vendors. We would like to share with you the overall considerations and design possibilities that are possible.

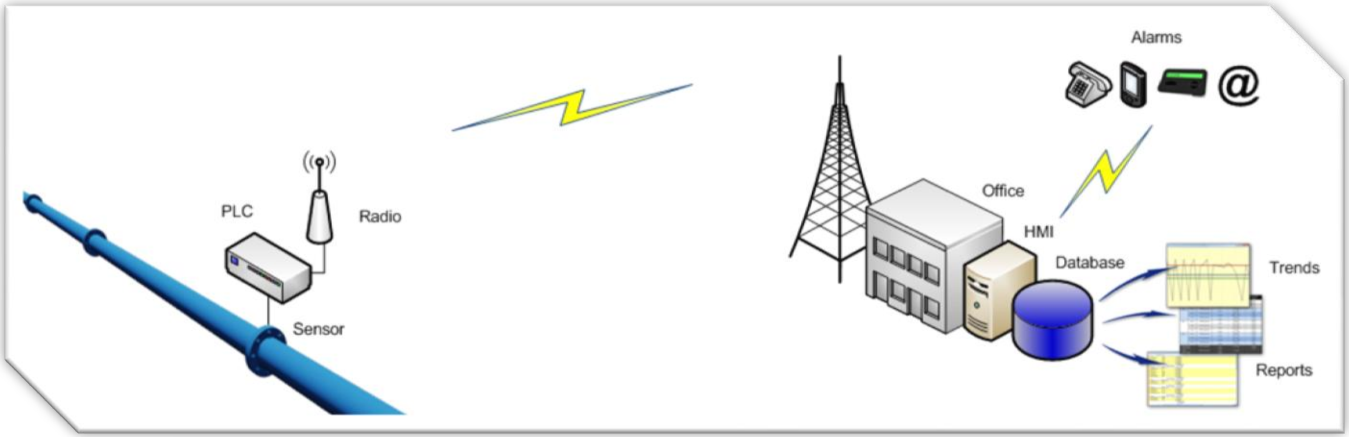




KROHNE
achieve more

Future Proofing - Overview

Replacing an aging SCADA system can be costly, even with working telemetry hardware. This seminar will outline several strategies for providing a cost effective upgrade path for your pipeline SCADA hardware.



An example of a common SCADA configuration.

SCADA Terms

- Supervisory Control and data Acquisition (SCADA)
- Programmable Logic Controller (PLC)
- Remote Telemetry Units (RTU)
- Human Machine Interface (HMI)

SCADA and Telemetry Defined

SCADA - **Supervisory Control And Data Acquisition**

- Computer controlled systems that monitor and control industrial processes
- Industrial Control System (ICS)
- Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote control devices (field devices)

Telemetry - Technology that allows data measurements to be made at a distance

- Commonly refers to wireless data transfer mechanisms (e.g. radio, infrared systems)
- Now encompasses data transferred over other media
- e.g. telephone or computer network, optical link or other wired communications

The definitions and functionality are converging.

Typical SCADA Upgrade Scenarios

Legacy Monitoring Equipment
Connect to existing remote monitoring and control devices

Pipeline Expansion
Add remote devices, similar to those existing, to an extension of your pipeline

Modernization
Replace all monitoring and control hardware and software

New SCADA
Brown field system installation (not upgrade)

Potential Problems

KROHNE
achieve more

Problems – Legacy Monitoring Equipment

Older devices are no longer supported by manufacturer

No redundant connectivity

No data redundancy

Cannot be maintained or…

Maintenance requires excessive downtime

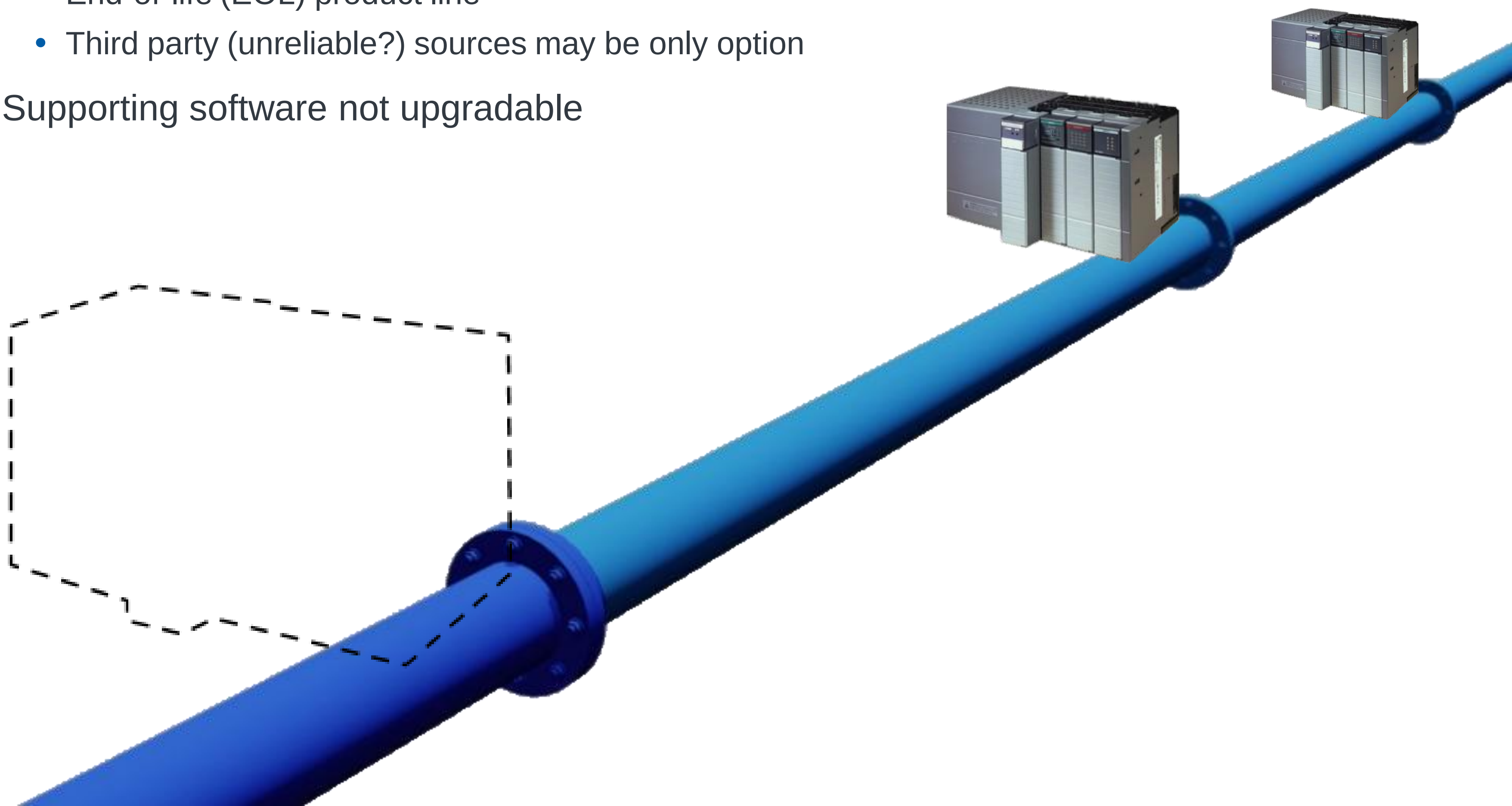
Lack of security

Problems – Pipeline Expansion (same SCADA equipment)

Difficult to find more of the same equipment

- Manufacturer may be out of business
- End-of-life (EOL) product line
- Third party (unreliable?) sources may be only option

Supporting software not upgradable



Problems - Modernization

Significant capital costs

- Hardware replacement/programming
- Software replacement/programming
- Network replacement

Lost monitoring time when doing one-shot replacement of all equipment

Difficult to replace a single asset and burn-in before moving the rest

KROHNE

achieve more

Suggested Solutions using SCADA Technologies

Hardware Abstraction

- Decoupling the Device Driver and the Transport Layer
- Allows the use of different types of communication medium
- No further changes to the Driver or SCADA system
- Data agnostic Transport Layer

Combining Legacy and Current Equipment

Hardware Extraction

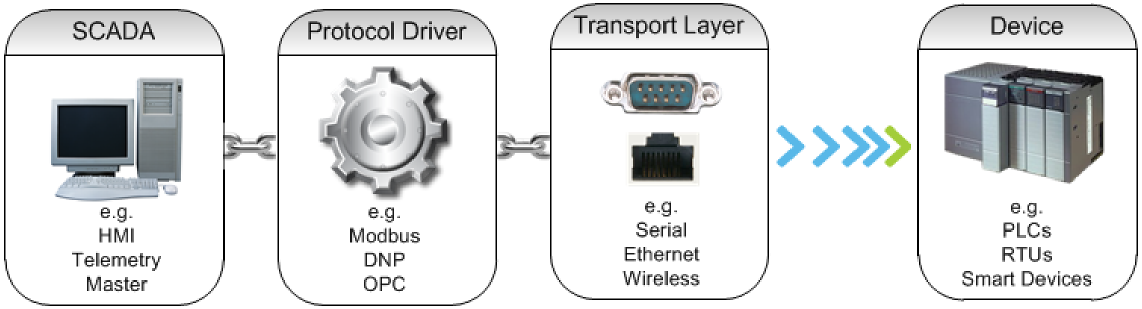
SCADA Communications Methodology

Device Drivers facilitate communications between SCADA software and field device

- Devices - PLCs, RTUs, Smart Devices
- Protocols - Modbus, DNP, OPC
- Transport layers
  - Serial RS232, RS485
  - Ethernet TCP/IP
  - Telephone PSTN/POTS, GSM
  - Wireless GPRS, WiFi

Drivers translate from the hardware device protocol to SCADA data values

Drivers are usually written to work with a specific transport mechanism



Hardware Abstraction – Protocol Driver

Breaks the link between

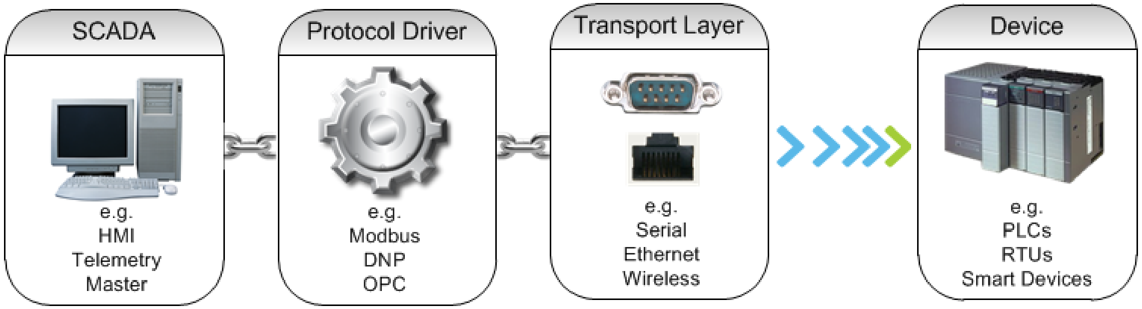
- Driver and Transport Layer
- Protocol and SCADA values

Provides transparent end-to-end communication

Driver is written to use an Application Programming Interface (API)

- Functions common to all transports
- Functions such as Connect(), Send() and Receive()

Driver interprets the protocol and extracts the data values



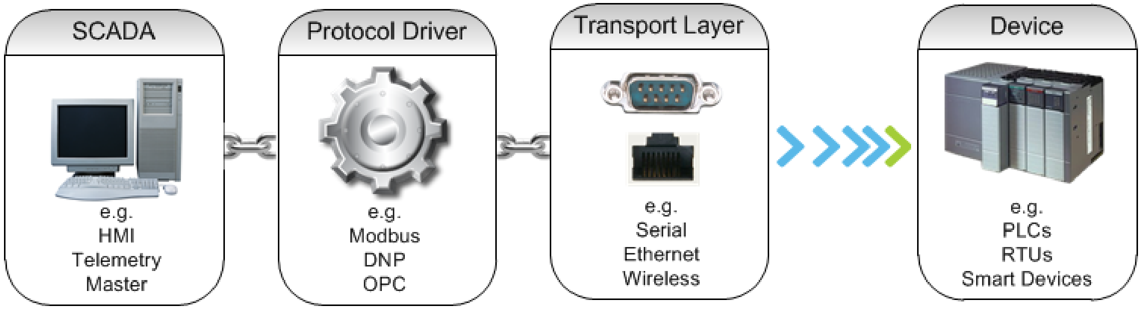
Hardware Abstraction – Transport Layer

Transport Layer is divided into Ports

Each is an abstraction of the Transport Layer that it uses

Must implement the same API

Data agnostic – does not understand the protocol, only delivers or receives data



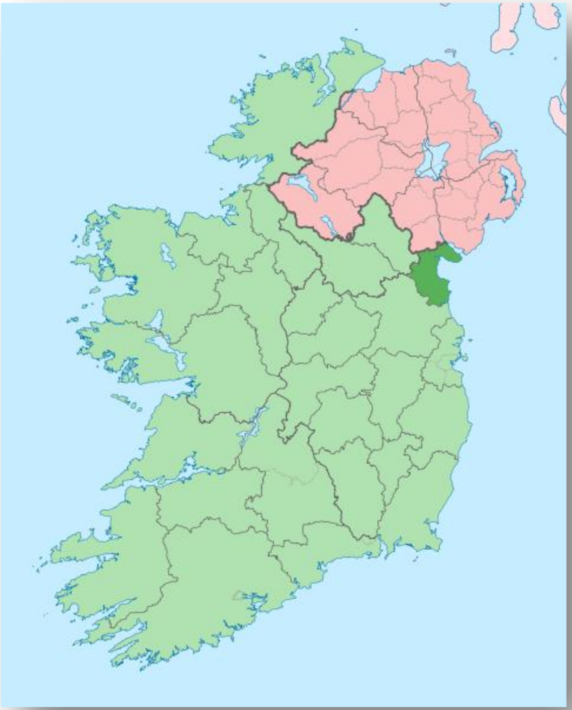
Case Study 1: No Telemetry Monitoring
County Louth Ireland Lift Station

A Lift Station controller (PLC) controls Duty and Standby pumps

RS232 port allows data access using MODBUS RTU protocol

No telemetry – operators visit site to check for problems

Spill events are only reported after an event has occurred



Requirement: Monitor the lift station from central SCADA

Concern: The control room is located some miles away

Case Study 1: Solution
County Louth Ireland Lift Station

Configuration details

- Low-cost GSM/GPRS Modem/Router connected to the RS232 Interface
- New Central SCADA configured with a MODBUS RTU Driver
- TCP/IP (Ethernet) Port configured for the MODBUS RTU (serial) Driver
- Device is polled once an hour for Lift Station status

Additional Benefit – Historical analysis identifies equipment fault

- Real-time data analysis identified Standby Pump running too frequently
- Site visit showed no abnormalities
- Subsequently pulling the Duty Pump revealed a broken impeller
- Couldn't have been identified without telemetry or physical intervention

Combining Legacy and Current Equipment

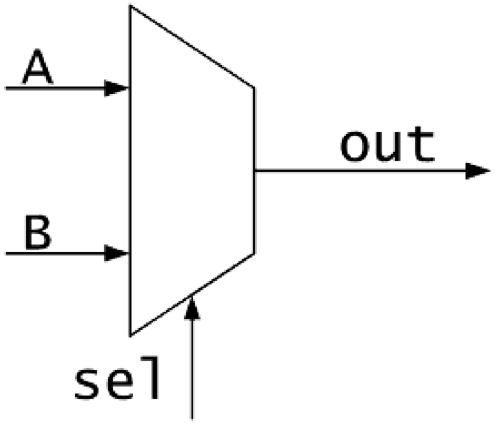
Multiplexing and Port Sharing

Multiplexing Overview

Method by which multiple communication streams are combined into one signal over a shared medium.

Options:

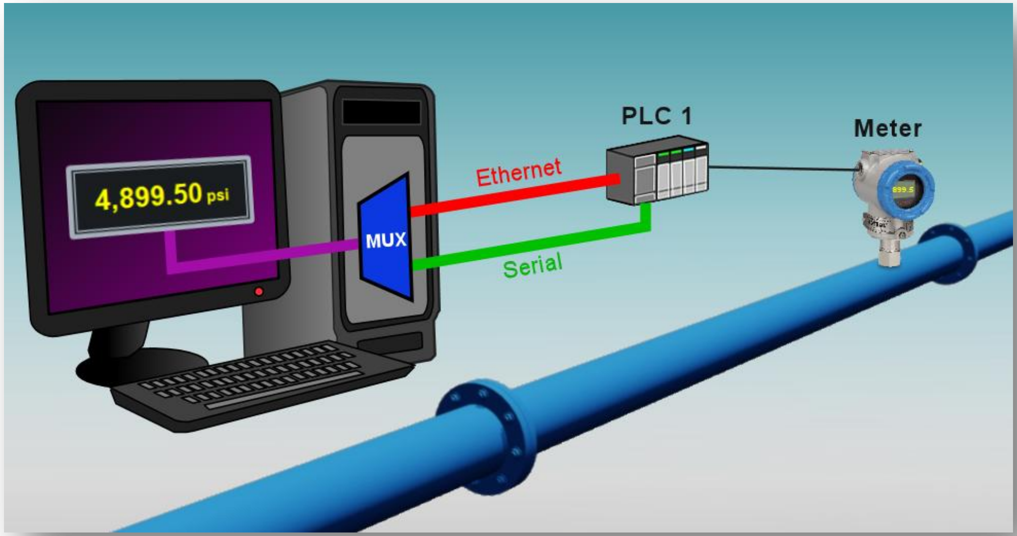
1. Establish redundant communications links to a PLC
2. Share the load between two communications links
3. Replace PLCs without losing SCADA connectivity
4. Establish communications links to redundant PLCs



Multiplexing – Option 1

Establish redundant communications links to a PLC

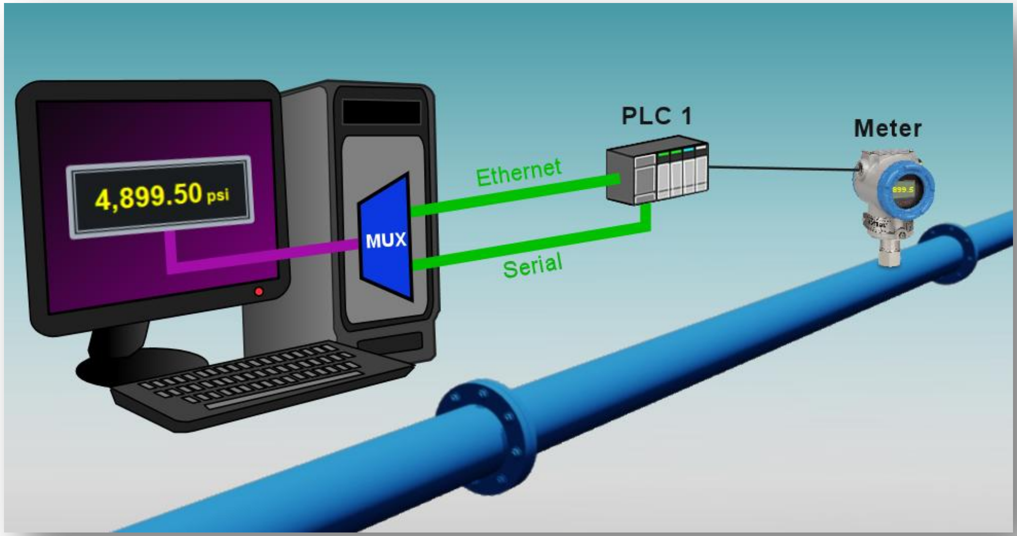
- Provide a hot backup should the primary link fail
- Automatically fail over from one communication path to another
- Transport layers can be physically disparate medium



Multiplexing – Option 2

Share the load between two communications links

- Use the maximum bandwidth of both communications links
  - Increases communication speed
  - Increases the amount of data that can be transferred
- Prefer a least cost routing or more reliable route

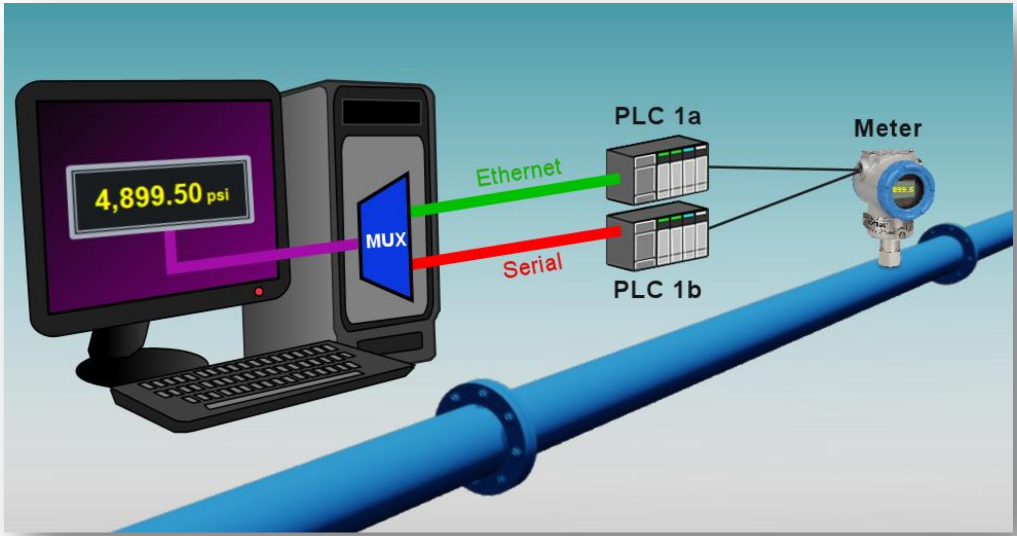


▶ achieve more

Multiplexing – Option 3

Replace PLCs without losing SCADA connectivity

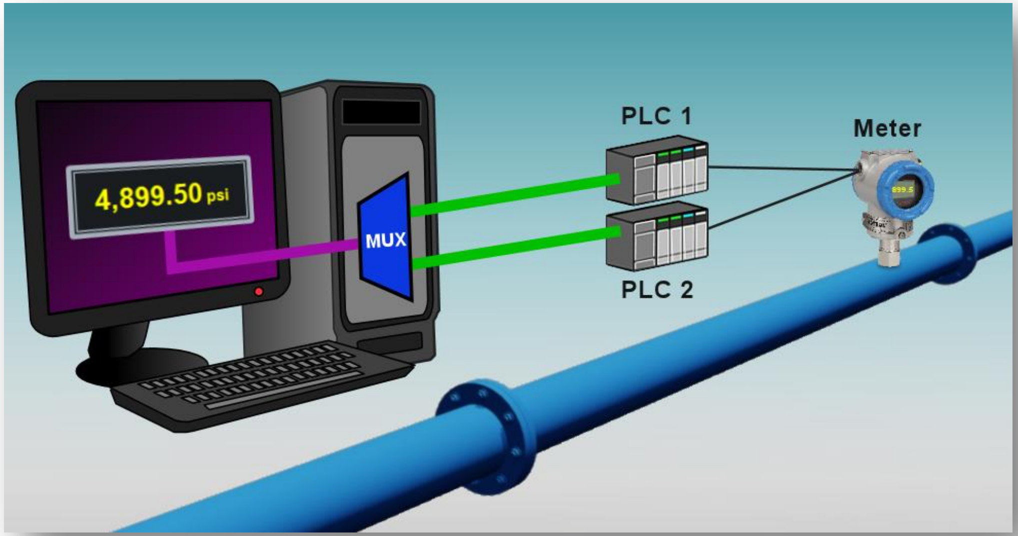
- Connect a new PLC in parallel with the existing
- Allows you to commission the new device in situ before switching communications
- Communications can be changed over when ready – without down time



Multiplexing – Option 4

Establish communications links to redundant PLCs

- Connect a new PLC in parallel with the existing
- Allows you to commission the new device in situ before switching communications
- Communications can be changed over when ready – without down time



Port Sharing

Communicate to different field devices using the same Transport Layer

Communicate using different protocols over the Transport Layer

Example:

- Existing telemetry system – VHF radio and legacy field devices
- Requirement - monitor additional field devices
- Problem 1: Legacy field device equipment unavailable
- Problem 2: New field device or different protocol typically requires second radio frequency
- Solution: Port sharing allows new device to be used on current radio system

Caution:

Erroneous protocol interpretation by another device could have adverse consequences!

Modernization Considerations

Communications and High-Availability Data

Data arbitration options

- Prefer A, Prefer B, Use A, Use B, Switch Every X Period
- Average Latest, Use Highest, Use Lowest

Advanced transport layer options

- Modems – provide transparent end-to-end communications
- Change PSTN for VOIP

Data hand-off to 3rd party systems

- SCADA system interrogated by DCS or other systems
- Data presentation as RTU or PLC

Front End Processor (FEP) elimination

Protocol conversion

Security

Ensure SCADA system is receiving data from the actual device (not spoofed)

Ensure that device only responds to commands from Central SCADA

Ensure end-to-end data privacy (no eavesdropping)

Transport Layer encryption (e.g. VPN tunnel)

Newer protocols with integrated security authentication/authorization

Modernization of Protocols

New protocols have richer data models

- Modbus limited to discrete values or 16-bit registers. Additional effort for 32-bit float values
- DNP supports 16-bit, 32-bit, Single, Double all with/without status (Quality) and Timestamp

Data can be reported on-event (on change) or by-exception (alarm)

Reduced bandwidth requirements

More open standards (hardware vendor independent)

Integrated security authentication/authorization

Case Study 2: Modernization
AkerSolutions Master Control Station

Master Control Stations (MCS) for Subsea Control of remote oil and gas wells

Communications to Subsea Electronics modules via umbilical up to 90 Kilometers

Electrical signaling using two-wire communications via proprietary BELL202 modems

The modems use RS232 serial interface

Pair of industrial PCs configured with hot redundant failover

Mechanical relays switch serial port pins from one PC to the other (Change-Over Rail)

Controlled via PC-mounted software driven Digital Output Board

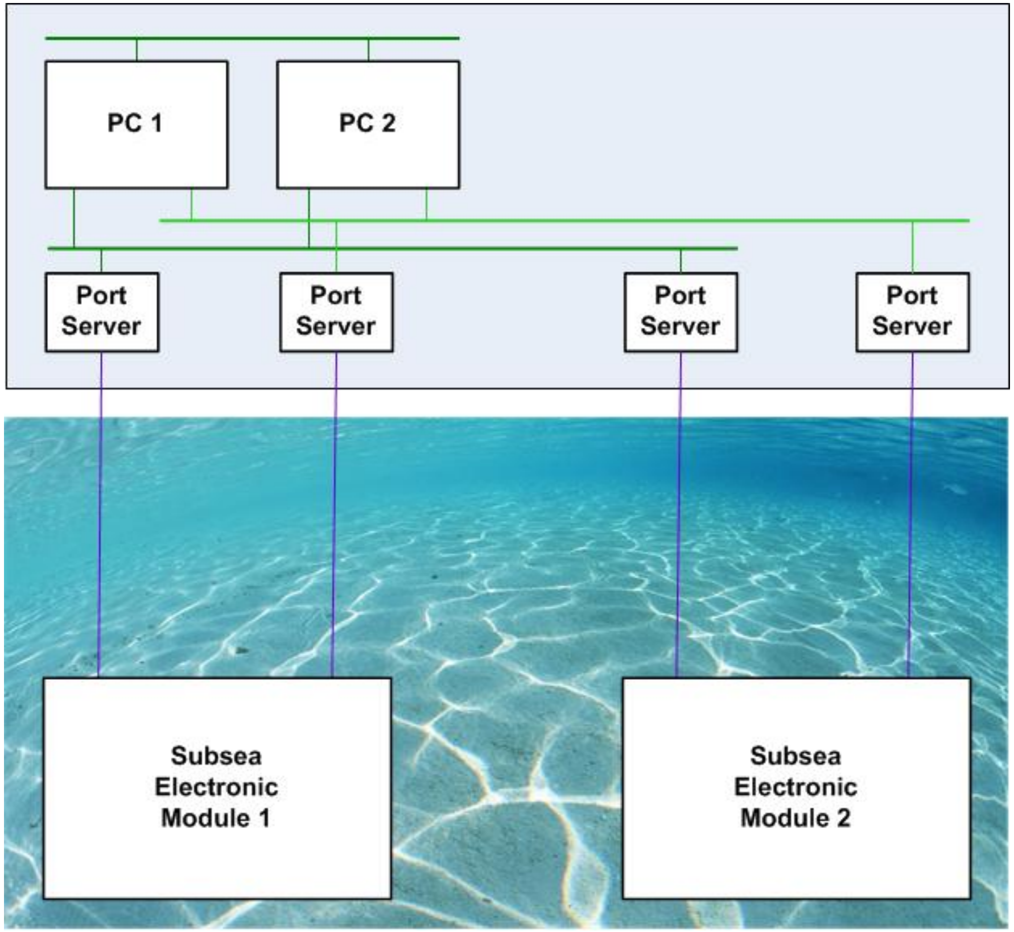
Problem: Change-Over rail was expensive to build and prone to failure

Problem: Complexity increased with number of modems and communications lines

Case Study 2: Modernization
AkerSolutions Master Control Station

Solution

- Replace the change-over rail with two port servers (IP over Serial)
- Each server PC fitted with two network cards
- Each port server was on a separate subnet
- Each PC has redundant path to port servers - additional level of redundancy



Summary

Replacing an aging SCADA system does not have to be a single step process.

- A multi-step upgrade and change over can be achieved
- Legacy hardware can be integrated in to modern system
- Additional functionality and redundancy can be achieved

Q&A

Your turn to speak !

Post-test

Did we teach you anything (useful) ??