Selecting the right RTU and SCADA System

James M DiNanno - Whitmor Company - Revere, Ma 02151 - jdinanno@whitmorcompany.com
Dominic de Changy – Technotrade S.a. Waterloo,Belgium dominic.dechangy@technotrade.biz

Abstract
The aspects to consider when selecting a RTU and SCADA platform for remote applications can be overwhelming. Today there is a broad choice of solutions for remotely controlled equipment and centralized monitoring systems. It is no longer necessary to use traditional and discrete devices such as a PLC, modem/dialer, data logger or SCADA PC and integrate them yourself. Hardware and software solutions that offer multiple and pre-engineered functions are now available with enough power and scalability to service any remote application. These new all-in-one Telecontrol products can often save substantial time in development and integration, which is the largest cost component of a project. Normally you would expect to pay a premium for products and software that offer multiple functions, but today this is no longer the case.
We will explore the evolution of traditional RTU and SCADA systems architectures versus new embedded and hybrid Telecontrol systems offering many new technological advancements. A guide to weighing the features and benefits will be provided to determine applicability. A case study is presented.

Change is good – sometimes

You know the routine. We have all been there before. When you know how to do something and are familiar with it you tend not to take the extra effort to explore or learn what new products or solutions may be available to replace it. You also feel comfortable because it works and it has been fairly reliable. And by the way just about everyone else is doing the same thing so it must be right. At least it is a safe choice.

Well this is exactly what the Big 5 Automation vendors want you to do, get complacent and follow the crowd. Now is that why you wanted to become an engineer? Wasn't it for the joy of exploring new technology and leveraging the best of the best or at least staying up to date with the state of the art?

Background

The 5 Big automation vendors all offer a wide range of general purpose products. Often these manufacturers do not look to offer the most efficient solution for vertical markets or applications but rather a broad product offering, serving many industries. Classical big company marketing practices drive the concept of product families and marketing mix. These policies drive the companies to segment features and functions into separate products so that they can sell more and justify their participation in their respective division. They very rarely take all of your application needs into consideration. They also like to bend your needs and requirements to align with their product concepts. The product categories we all have become familiar with are PLC, HMI, SCADA, Drives, etc.

A new paradigm

We are living in a new paradigm. Finally many consumer product companies have broken the traditional marketing mold to offer products and solutions that address needs from a customer's point of view. A cell phone with a camera and mp3 player. A microwave with a TV screen on the door. A refrigerator with a barcode scanner and display. This paradigm shift of thinking outside of the box or from the customer viewpoint has finally occurred in the industrial sector.

Centralized vs. de-centralized RTU

Traditional SCADA solutions have used personal computers and industrial controllers to manage outstations via dedicated and leased line connections. The remote stations had limited intelligence and relied heavily on the central station for process control, monitoring and alarm handling. Any breakdown in remote communications caused an immediate downtime of the outstation due to its dependency of the no longer connected central station. Additionally, the SCADA capability to interface with many outstations was limited by the direct wired connections available. To improve the capability to manage and monitor many stations the use of polling was introduced. This allowed RTU's at the outstations to be connected one at a time to the MCU (master control unit) to exchange any data for a short period. This had the limitation that if any critical events or alarms would occur, they would not be detected until the next polling cycle. In cases where many RTU's were deployed, the update rate at the SCADA operator interface would be fairly sluggish and not representative of the actual real-time events of the outstations.

Intelligent pre-processing

With the lower cost of memory devices and more powerful controllers it has now become practical to distribute processing and data logging operations at the remote stations. Events can be interpreted and acted on at a local level without interaction from the MCU. Data logging and trend analysis can also be provided locally thus eliminating the need for large amounts of remote data transfer. This capability greatly helps to improve data transfer efficiency because the MCU and SCADA must only consume the pre-processed data. Optionally, the events and data can be stored at both the local and remote station to add a second level of data integrity.

Push vs. Pull

Today with an advanced Telecontrol system, data, statistics and alarms can be transferred on event instead of relying on a polling scheme. In the past the limitation of the hardware and shared line interconnections made it difficult to use a push configuration. Today newer communication capabilities allow multiple remote stations to send information in an asynchronous manner without any concern for collisions or open connections at the MCU and SCADA. With a large number of outstations the push model better utilizes the available bandwidth.

Leveraging Internet technology

The Internet has finally become cost effective for remote monitoring and control as compared to telephone and leased lines. With the use of the Internet a highly flexible communications topology can be used to access many outstations effectively. Remote stations can dynamically and simultaneously send data via email, FTP or be monitored and controlled via a web browser. This data can then be consumed and displayed by a centralized SCADA system or individual users.

With the broad coverage of Internet access we have seen a drastic growth in Web services for industrial controls. Many vendors now offer subscription based services available to access remote equipment. This usually requires monthly service fees and contracted service charges to have custom Web pages developed.

A select few products offer the capability to embed HMI pages and access configuration features or the data in a RTU via the Internet or other direct connections.
These embedded Web servers reduce the need for monthly fees and allow flexibility to manage and configure the features more freely. Only a PC with Internet access and a Web browser are required thus eliminating the need for remote software such as PCanywhere ® to be purchased and installed.

Centralized vs. de-centralized SCADA and HMI

A traditional SCADA implementation uses a specific software and personal computer to collect data from remote stations and display it in various forms for the user via the HMI. This master PC acts as the eyes and ears of the system. For reliable operation this architecture requires that this PC be available at all times to serve data, display and take HMI request. To enable multiple users or remote access, additional software installed on the SCADA PC and remote PC is required. A nice feature of some new SCADA software is the web server feature. This allows many remote users to access the common SCADA and HMI views on remote computers which are served by the master SCADA PC. Going even further an advanced Telecontrol system may offer an embedded SCADA and HMI at the remote stations allowing both local and remote users the capability to access the individual outstations directly.

PC's role in SCADA system -

PC's are used quite often for the SCADA interface to the remote process. Many times a PC is located at the remote site for HMI, datalogging and charting purposes. Unfortunately, there is an added cost of PC hardware, software and engineering effort to create this type solution. Most importantly a low cost consumer PC does not meet the criteria of reliability or environmental robustness demanded by remote site applications. The PC's power supply and mechanical parts, such as fans and rotating media are the most common areas of failure. Additionally, standard consumer operating systems such as Microsoft Windows® are configured by default to run many software components and drivers that are non-essential and sometimes troublesome. This can cause instability, crashes and performance degradations that can adversely affect the SCADA and possibly shut down the process. Operating system updates, virus and security vulnerability, multi-communications management and power and reboot conditions can be cumbersome and costly to remedy.

Embedded hardware for SCADA AND HMI-

There are some industrial products on the market that offer the high reliability, robust performance and small size not provided by a PC. Devices vary from open or minimally packaged circuit board products, moderately packaged plastic PLC's to ruggedized metal housed gateways and Telemetry products. Most of these devices offer a specific function as part of a RTU or SCADA solution. The level of feature integration can vary widely depending on the product and manufacturer. A few solution based products offer multiple functions in a single device or modular platform.

Discrete devices vs. integrated Hybrid solutions

Using a traditionally deployed RTU, MTU and SCADA system involves the use of many different devices which are interconnected and integrated together into a system. Often, the devices are from different vendors, have varying form factors, separate software or configuration utilities and various levels of interoperability. A combination of communication ports, drivers, protocols and database interfaces are needed for all the components to work together. An experienced integration contractor, comprehensive system specifications and strong adherence to the requirements is a must with this type of solution.

Some multi-function or hybrid devices offer varying levels of capability focused on one of the main 3 functions of a system – that being control, telemetry or HMI/SCADA . A limited number of products offer a complete out of the box solution for Telecontrol applications. Benefits include single or streamlined software, plug and play functionality for all system components, consistency in hardware form factor, interoperability and vastly reduced integration and wiring effort. Embedded HMI and SCADA solutions are even provided allowing access to the process from a standard web browser at any location without the need for costly or proprietary SCADA software installed on a dedicated PC.

Availability / Redundancy -

High availability of a system is often a consideration for remote process operations. Availability is a consideration in 2 domains – the remote process being controlled and monitored and the communication interface at the operator or SCADA point of view. To improve availability of the remote communications, redundant interfaces or mediums may be used – ie: self healing fiber optic Ethernet ring, radio, telephone modem, etc.

To provide high availability of the process, the use of redundant controllers, IO and power supplies may be used. Power management and surge protection is also a critical factor to consider. Lightning strikes and power failures can damage equipment causing critical downtime and costly equipment replacements. A battery backup system allows the RTU to ride through short power failures, manage an orderly shutdown of the process and to send remote alarms when these conditions occur. The process being controlled will dictate the level and complexity of the redundancy solution used. Cost and system complexity can rapidly escalate when redundancy is a requirement.

Security

With the openness and availability of the Internet and other growing range of wireless forms of communication it is imperative to limit access to data and functionality of the remote systems from unauthorized users. Password protection with multi-layers of access level should be provided to manage viewing vs. control access and changes of the system. Configurable firewall can also aid to reduce unsolicited communications and filter unwanted traffic from affecting the systems performance and capability to communicate.

Scalability and portability

Scalability is the capability of the hardware and software architecture to support a wide variety of outstation and SCADA configurations with a high degree of commonality and ease. Since outstations may vary in size and demands, the scalability of the solution can become an important factor. One common but costly practice is to base your hardware and software solution on your worst case or largest outstation. For many PLC products this means using a control platform and software tools that are a vast overkill in cost and expansion capability for the remote process that you may be controlling or monitoring.

Key factors to consider:

- Select a control platform that uses a common software development environments that allows porting the application from and to the various hardware devices needed to service all outstations.
- Since the majority of outstations have less than 100 I/O points and devices you should select a hardware platform that allows you to optimize for the majority of these configurations.

Data and protocol translation

Remote applications and SCADA systems are communications intensive and usually require many communications ports and remote access options. Additionally many devices may speak different protocols and have varying hardware interfaces. The most common protocol is Modbus (the defacto industry standard for serial communication) for general devices and a small variety of others being mostly industry specific. Examples include – DNP3 for the power substation sector and LON and BacNet for building automation. The use of Ethernet and Modbus TCP/IP is also becoming a popular choice for system wide and remote communications. Many other devices have special serial protocols unique to their manufacturer. The capability to support multi-port communications and protocols can be critical to the success and longevity of your chosen platform across various applications.

Remote Communications

Today there are many options to select when remotely communicating to a site. It is no longer necessary to have dedicated wiring or leased lines to monitor or control outstations. In cases where high rates of data or always on-line communications are required a multi-drop communication network may be used. This includes RS-485, Ethernet or others. The network allows multiple stations to be connected and for various data points to be shared. For locations where hard wiring is impractical a wireless interface may be used. Many wireless methods are available such as traditional licensed band radio, non-licensed spread spectrum radio, cellular, satellite, and a variety of other short range technologies such as 802.11G . These methods all have their specific benefits and limitations and must be considered when selecting a solution. The use of GSM cellular technology has now become a practical option allowing an outstation to leverage the vast GSM based cellular networks and land line interfaces to reach across the globe at very reasonable rates without the need for any specialized and costly hardware or service contracts. On the horizon is 3G based communications which will extend the bandwidth capability to enable live video transmission.

The following matrix shows a basic overview of strengths, limitations and pluses and minuses of a variety of communication methods.

Method	Initial Cost	Operating Cost	Operating Benefit	Distance	Operating Limitation	Plus	Minus
Hard Wire	**$$$$$**		Dedicated on-line	Up to 10 miles or more	Single device/ limited data	Simple to implement	Site installation
Hard Wire Network	**$$$$$**		Dedicated on-line	Up to 10 miles or more	Multi-device & data	Easy to change data	Site installation
Leased Tel Line / Modem	**$**	**$$$**	Dedicated on-line	100s of miles or more	performance depends on public utility	Simple to implement	Initial an Monthly Fee
Public Tel Line / Modem	**$**	**$**	Wide availability	100s of miles or more	performance depends on public utility	Simple to implement	Initial and Monthly Fee
UHF Single Band Radio	**$$$$**	**$**	Fair / good reliability	Up to 20 miles or more	Limited data rates	Any location	Requires License / fees
Spread Spectrum Radio	**$$$**		Fair / good reliability	Up to 10 miles	Limited data rates	Any Location	Performance depends on geography and weather
Cellular / GSM Phone	**$$**	**$**	Fair / good reliability	Up to 10 miles to local tower	In service Area	Wide availability	Initial and Monthly Fee
Satellite	**$$$$$**	**$$**	High data rates	Around the world	Line of sight	Wide availability	High latency

Integration

Since many field devices may need to be interconnected in a Telecontrol solution, it is necessary to support a variety of signal types. The most common field device interface are via contact closures, standard digital discrete signals or via analog the most common being 4-20ma. Smart devices with a high level of data values may also support serial or other communication interface. A big consideration in developing and maintaining the solution is the ease and level of integrating the devices and functions required. Communications interfaces can be the most complex to integrate especially when there are varied protocols, different vendors and an array of cabling interfaces.
Working with different vendors and products can also impact integration efforts due to some inconsistencies in signal interfaces and protocols. All too common is the problem of finger pointing. This occurs when multiple vendors and integrators shift accountability to the other guy when the system components won't talk to each other.

Key Points to consider:

- Minimize complexity in the system integration by choosing pre-tested and highly integrated solutions
- When using systems integrator, be sure of their experience and qualifications.
- Assign a single point of contact to be accountable for the complete integration effort.

Risk and Reliability

Many factors play into the reliability of a system and the risk of success when deploying a system. We will consider 4 primary factors affecting reliability and risk for success. The 4 factors are maturity of the hardware, maturity of the software and firmware, complexity of the integration effort and experience in integrating the components. Today the state of the art manufacturing technology allows most vendors to produce products consistently. The real difference can be seen with the design methodology, experience and choice of materials and enclosures.

The following matrix shows the risk associated with major 4 factors of concern.

Risk factor	Hardware	Software	Integration Complexity	Engineering Experience
Low	Existing/Proven	Existing/Proven	Simple design	High Experience
Moderate	Existing/Proven	Existing/Proven	Simple design	Moderate Experience
Moderate	Existing/Proven	Existing/Proven	Moderate Complexity	High Experience
Medium	Existing/Proven	Existing/Proven	Moderate Complexity	Little Experience
Medium	Existing/Proven	New Software	Moderate Complexity	High Experience
Medium	New technology	Existing/Proven	Significant Complexity	Moderate Experience
High	Existing/Proven	Existing/Proven	Significant Complexity	Little Experience
High	Existing/Proven	New Software	Significant Complexity	Little Experience
High	New technology	New Software	Significant Complexity	Moderate Experience
Very High	Existing/Proven	New Software	Very Complex	Little Experience
Very High	New technology	New Software	Very Complex	Moderate Experience

Key Points to consider:

- Well proven hardware and software designs can greatly reduce the risk of failure of a system once it is operational but the complexity of integration and number of system components can have a negative impact.
- Highly integrated solutions reduce risk in both development and in operation especially when it comes to deploying advanced remote communications functions.
- Modularity may aid in quick recovery if a component of the system fails.

Total cost of ownership and life cycle costs

When considering the costs and time to justify RTU and SCADA installations you should look at all aspects of the life cycle. This includes the specification, design, implementation, documentation, start-up/commissioning, maintenance, operation and downtime, evolutions, and end of life. Traditionally implemented RTU and SCADA solutions have been determined to be fairly equal in costs regarding hardware, integration and the installation effort. Since many remote applications are very specialized or specific, the engineering and integration component of the project can often become the largest cost factor. Selecting hardware and software solutions that offer multiple and pre-engineered functions, can often save substantial development and integration dollars on the project.

Case Study

A water utility client is installing a new waste water lift station and is requesting the following features to control and monitor the dual wet well pumping station.
The remote site will not be manned and will only be physically checked on a once a week basis or when a critical condition occurs.

- Dual pump control with variable speed drives depending on demand and level.
- Well level monitoring with analog pressure level sensor and high and low level float switches.
- Pump and field sensor monitoring – overheat, seal fault
- Manual and automatic pump run options
- PID loop control
- Remote monitoring and control capability
- Local and remote Alarming with modem and programmable dialer
- Local HMI via Ethernet
- Local data logging
- Local printer
- Building motion sensors and access door keypad and control

The engineering firm hired by the Utility has specified the use of traditional and discrete devices and a SCADA to be integrated into the outstation based on a previous project of 5 years prior. The Utility also has a project cost budget of only $75,000 for the electrical and instrumentation design, integration and installation and has already signed off $25,000 to the engineering firm for the specification development and project management. The utility decides to purchase the variable speed drives directly from the manufacturer to save some cost for $20,000. This leaves $30,000 available for the electrical equipment, installation and integration.

A traditional SCADA and RTU solution was quoted based on the specified components.

The outstation includes:

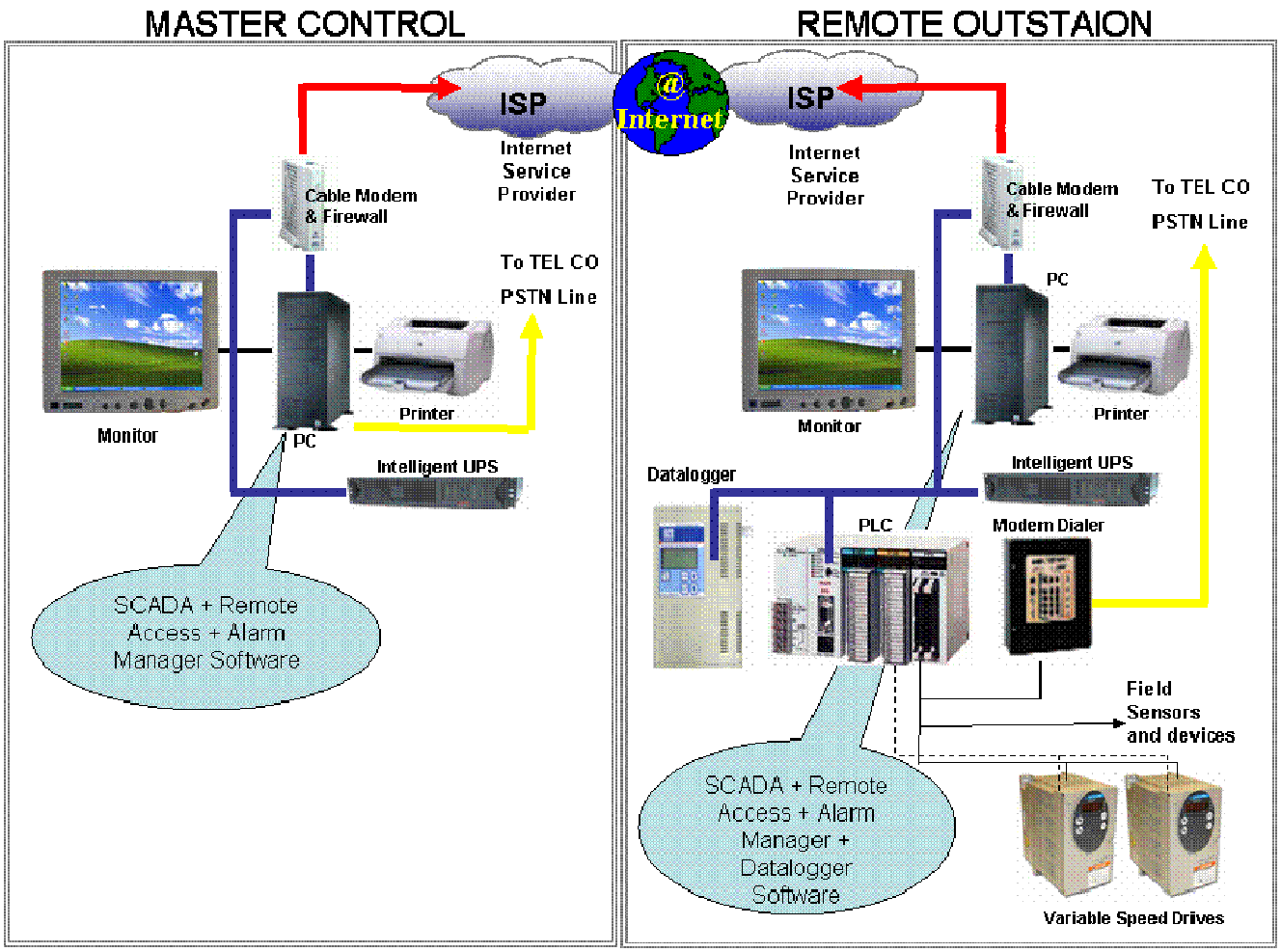
• A modular PLC with power supply , processor and IO modules from Vendor A	$ 4,500
• PLC Programming software and cables from Vendor A	$ 2,500
• A stand alone modem/dialer with 4 discrete alarm inputs from Vendor B	$ 600
• A datalogger / digital chart recorder from Vendor C	$ 1,800
• Configuration software for datalogger from Vendor C	$ 250
• A PC, operating system ,display and printer for local interface from Vendor D	$ 1,200
• SCADA HMI Software from Vendor E	$ 1,500
o Optional – Trend / graphing software	$ 400
• Alarming Software from Vendor F	$ 400
• Remote Access Software from Vendor G	$ 80
• Cable Modem and Firewall from Vendor H	$ 250
• Internet Access account with local ISP –from Vendor H - monthly cost	$ 50
• 120V Intelligent UPS System – Inustrial with Ethernet	$ 800

The Master SCADA included:

• A PC, operating system ,large display and Printer for local interface from Vendor D	$ 2,500
• SCADA HMI Software from Vendor E	$ 1,500
o Remote communication Driver Master	$ 500
o Optional – Trend / graphing software	$ 400
• Alarming Software from Vendor F	$ 400
• Remote Access Software from Vendor G	$ 80
• 120V Intelligent UPS System – Inustrial with Ethernet	$ 800

Engineering, Integration, Panel enclosures, piping and wire and system installation and Start-up	$ 25,000
Sub-Total	**$45,560**
Over Budget	**$15,560**

Figure 1: *Traditional SCADA and RTU System Architecture*



After the submittal of the project cost the Utility asked what features could be eliminated or what alternatives could be offered to meet the budget. Since the system specification identified specific vendors and products it was not possible to meet the budget while complying to the specification. A specification change was requested and issued allowing an equal or alternative solution to be offered. This allowed the Integrator to submit a new proposal based on a new Telecontrol solution with many of the features and functions built into a single product. The cost of hardware and software was dramatically reduced while also eliminating much of the integration efforts.

A new multi-function SCADA and Telecontrol solution was quoted based on the following components.

The outstation includes:

- A modular Telecontrol with power supply, processor and IO modules from Vendor A $ 4,000
  Standard embedded features include
  - PSTN modem /dialer and alarm management
  - Ethernet
  - Programmable controller supporting IEC 61131 programming
  - Data logger
  - Email and FTP
  - Embedded Web Server
  - 12V battery Charger for backup operation
- Single Programming and Config software for all Telecontrol features from Vendor A $ 1,200
- A PC, operating system ,display and printer for local interface from Vendor B $ 1,200
  - Web Browser Software from Vendor B $ Free
- Cable Modem and Firewall from Vendor C $ 250
- Internet Access account with local ISP – monthly cost Vendor C $ 50
- 12V Sealed Lead Acid battery for Telecontrol backup operation $ 30

The Master SCADA included:

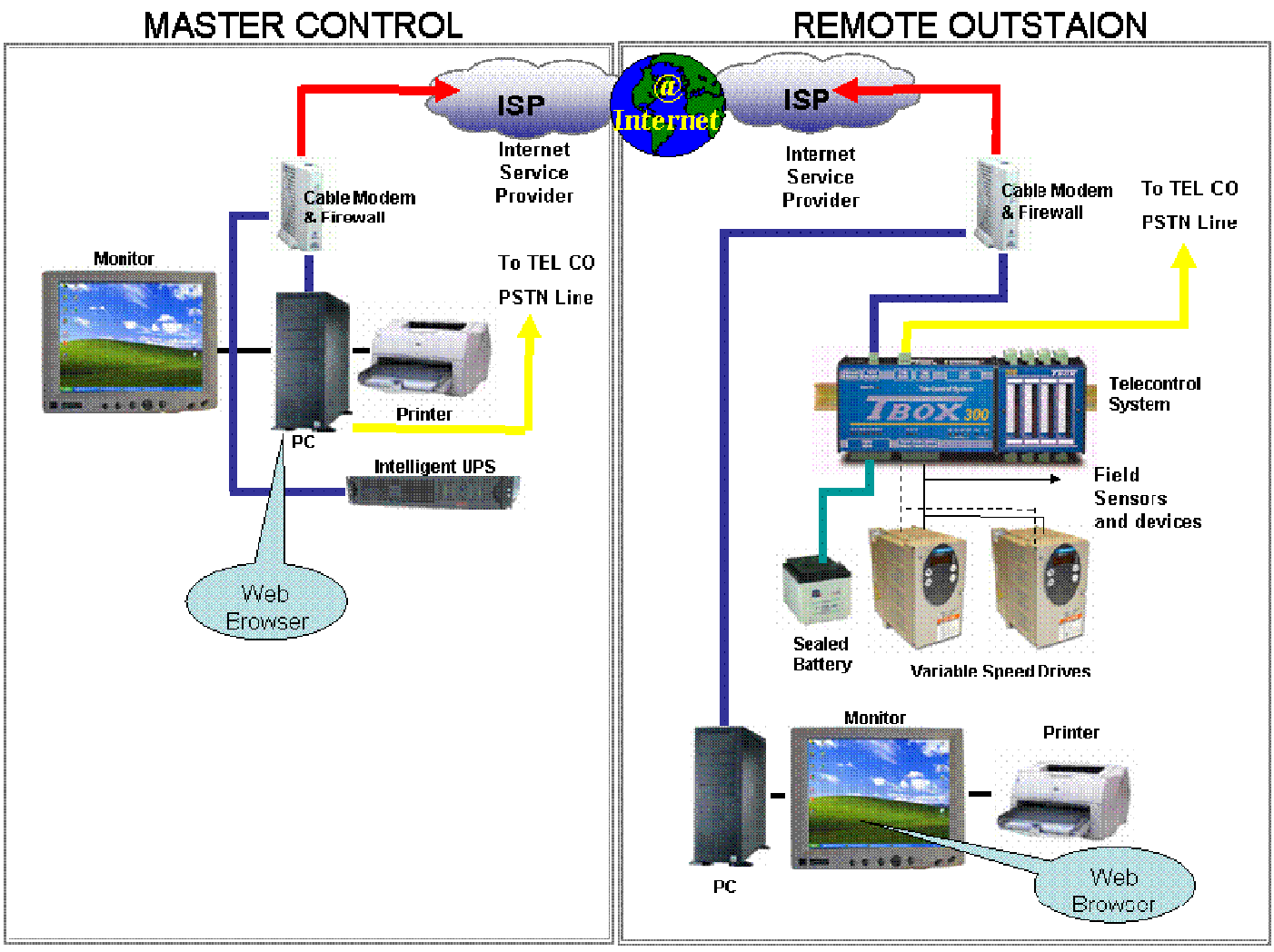
- A PC, operating system ,large display and Printer for local interface from Vendor B $ 2,500
  - Web Browser Software from Vendor B $ Free
- Cable Modem and Firewall from Vendor C $ 250
- Internet Access account with local ISP – monthly cost Vendor C $ 50
- 120V Intelligent UPS System – Inustrial with Ethernet $ 800

Engineering, Integration, Panel enclosures, piping and wire and system installation and Start-up $ 18,000

Sub-Total **$28,330**

Under Budget **$ 1,670**

Figure 2: *New Multi-function Telecontrol System Architecture*



Conclusion

A traditional implementation of a RTU, MTU and SCADA system can be a complex and overwhelming system to integrate and maintain costing more than $40,000 per station when considering the specification, integration engineering and hardware costs.

With the advent of multi-function Telecontrol solutions specifically designed for remote applications many advantages and benefits may be achieved vs. traditional solutions:

- Capital investment costs savings – typically 30 - 50%.
- Reduction in programming and integration efforts across the system - typically 30 % or better.
- Single software interface to develop and maintain system via one common connection to access all system functions.
- Easy to adapt – especially SCADA HMI views - most can be done by end user.
- No subscription based Internet SCADA service required to access or modify your remote stations.
- No complex AT command programming required for modem communications.
- Common form factor and plug and play operation of system devices and functions.
- Pre-designed and tested solutions for peripheral functions.
- Better autonomy of individual sites especially regarding historical data archiving and remote SCADA capabilities. No dependency on central SCADA system.
- Powerful, scalable and open solutions are now available offering common interfaces to existing and new installations – ie Standard IO, Modbus, DNP3.

Glossary

CTU – Central terminal Unit - The master control station of a 2 part remote control system

DNP – a protocol developed by GE Harris Energy Control Systems for distributed electrical and power devices hence called the Distributed Network Protocol has become the defacto standard for the power industry. The standard has now been turned over to the DNP users group. More information available at www.dnp.org.

HMI – Human Machine Interface - Point at which dynamic information can be monitored or entered to interact with the process – usually graphically based display system.

LONWORKS – a protocol and hardware devices developed and owned by Echelon Inc. which leverages the concept of distributed intelligent devices and supports transmission over standard twisted pair and power lines. More information available at www.echelon.com

Modbus – a data transmission protocol originally developed by Modicon which is the defacto standard for industrial automation devices using serial RS-232 and RS-485 interfaces. The standard is now managed by an open industry trade organization called the Modbus-IDA . More information available at www.modbus.org

Modbus TCP/IP – a data transmission protocol originally developed by Modicon / Schneider Electric which is the defacto standard for industrial devices using Ethernet interfaces. More information available at www.modbus.org

MTU – Master Terminal Unit – The master control station of a 2 part remote control system

OI – Operator Interface – Point at which dynamic information can be monitored or entered to interact with the process.

PLC – Programmable Logic Controller – A term used generally in the industrial automation sector . Originally developed by Modicon in conjunction with General Motors.

RTU – Remote Terminal Unit - The slave or remotely located station of a 2 part remote control system

SCADA – Supervisory Control and Data Acquisition – The hardware and software providing visualization and overall management of a process. Usually a graphic based system.

Tag – refers to a data point either in dynamic or historical which is derived from the process being controlled or monitored.

TBOX – A range of multi-function advanced Telecontrol systems developed by Technotrade SA Waterloo, Belgium and represented in the USA by The Whitmor Company Revere, Ma. More info at www.tbox.us

Telecontrol – a system providing the capability to control a process locally and remotely.

Telemetry - a remotely accessible system (RTU) with local control and automation functionality.