SCADA AND TELEMETRY IN GAS TRANSMISSION SYSTEMS

AN OVERVIEW OF SCADA TELEMETRY, INFORMATION, SECURITY

AND USE IN THE TRANSMISSION SYSTEM

CHRIS J SMITH

INVENSYS PRODUCTION MANAGEMENT

THE FOXBORO COMPANY

38 Neponset Ave, Foxboro, MA 02035, USA

ABSTRACT

Modern business and security imperatives coupled with rapid technological change require key new architectural elements for SCADA systems These elements are discussed along with more traditional block diagram fundamentals, so that the reader might better understand migration and adaptation strategies for their transmission pipeline operations in the new millennium.

INTRODUCTION

Some SCADA system overviews might start with a general block diagram of a SCADA system. I'm taking a step back here and will start with the SCADA system as it appears in the business of the operation. In the new millennium, recognition of SCADA as an important functional unit in the overall business supply chain makes sense, as more and more business systems are more tightly integrated to the SCADA system. SCADA systems provide an operational platform to control and monitor the pipeline. The classic SCADA architecture consisted of a number of servers and network elements designed to provide a real-time representation of the field and its data as well as a control platform for closure of valves, and operation of pump or compressor set point.

An important step in the understanding of SCADA systems technology is to realize the placement of the SCADA system in the overall business and operational strategy of the pipeline. Pipelines are assets that need to be monitored and protected. The product transferred from supply to delivery point provides the economic justification of the pipeline.

The tradition of SCADA involves continuous and report-by-exception scanning of low-level data from RTUs, Flow Computers, Gas Chromatographs and PLCs. This data is elaborated with locally and remotely hosted configuration information to become basic real-time, historical and measurement data for the operation of the pipeline.

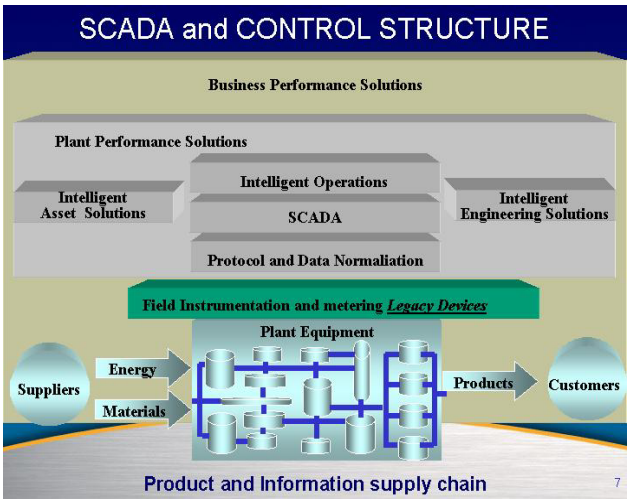

Figure 1 Pipeline Product and SCADA Information Supply Chain

So in a SCADA system all the technology required to get the data from the field, elaborate the data, store it, display it, alert the operator, and provide real time information to applications is provided. The SCADA system is an essential component in normalizing and centralizing data for the operational and business systems that depend on it as well as the basis for protection and control of the pipeline asset over its lifetime. At a higher level, once information is available, energy costs can be optimized relating to the actual transfer of product in the pipeline.

This paper looks at the variety of engineering and business requirements, which form the basic architectures of SCADA relating to gas transmission pipelines. The paper is an overview, it will raise more questions than it answers, however it should provide a framework for understanding and development of knowledge in the field for those who are possibly newcomers to the field.

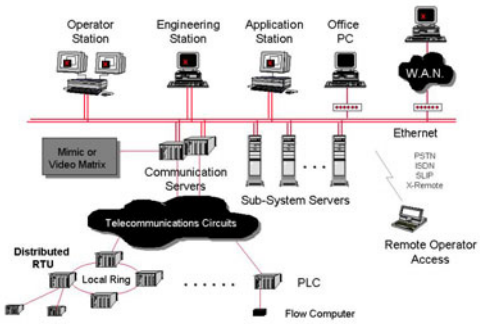

Figure 2 Functional elements of SCADA Block Diagram

BLOCK DIAGRAMS

The SCADA master is set up to provide a working operational interface to allow operators, and master sequence controls to create on-demand supervisory controls which--when transmitted to the RTUs, switch plant in or out of service and adjust operational conditions to suit the requirements of the moment. This relatively simple task involves the use of a wide range of technology and interfaces spanning large distances.

Now looking at the functional block diagram in figure 2, it is generally designed to show the physical connection and communications from the field through to the control room. When specifications are written and quoted, this is generally what vendors and purchasers use to gain a rapid understanding of the overall physical requirements and communications interfaces of the SCADA system. Key elements in Figure 2 are: -

- Engineering Workstation
- Operator Console
- Dual Database Servers
- Applications Station, Office PCs
- Dual Local Area Network
- Communications to field devices, PLCs, RTUs
- Diverse set of field devices such as flow computers, PLCs for compressor stations, and remote terminal units

You do not get a great sense of 'why'. What are the requirements this block diagram satisfy? Connectivity is one; with this you can see what is connected to what. Availability is another. With this you can see, if an element fails, which other element might take its place. Note the dual network and diversity of communications. In this case there is one communication path to a remote terminal unit. There are often two, a main and backup. Communications paths are expensive, so often the backup is high cost, possibly a dial up line. Consider an alternate block diagram Figure 3 In this example a pig receiving station. Traditional SCADA system architectures were developed to account for significant data speed and reliability problems associated with low speed long distance analog radio telemetry and transmission. Radio communications are still used today, however much more flexible and high bandwidth solutions are available with the use of high-speed microwave, VSAT, and fiber optic communications. The advent of TCP/IP protocols and their logical connectivity, has allowed multiple application requirements to coexist in the same communications pathway. A layered communications protocol requires much more bandwidth, but in turn allows for much more flexible implementations and diversity of technology.

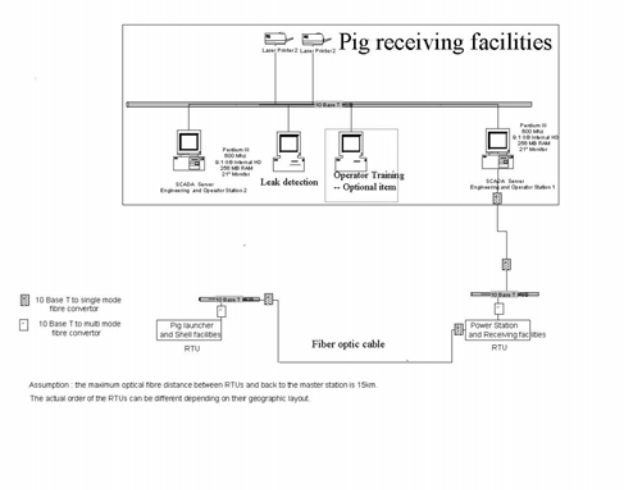

Figure 3 Pig receiving facilities block diagram

So the block diagram tells us about performance, reliability, connectivity, availability and partition of function in the control room. SCADA system designs in the 20th century had to contend with reliability of computing and communications equipment and pathways. Low bandwidth radio channels were used and thus block diagrams depicted solutions to the problems of the era. Another important point is that the main functional focus is one of operations and engineering. These are the basic requirements of SCADA. A system that will continually provide and operations interface for day-to-day operations and protection of the pipeline and pipeline network.

BUSINESS and OPERATIONAL REQUIREMENTS

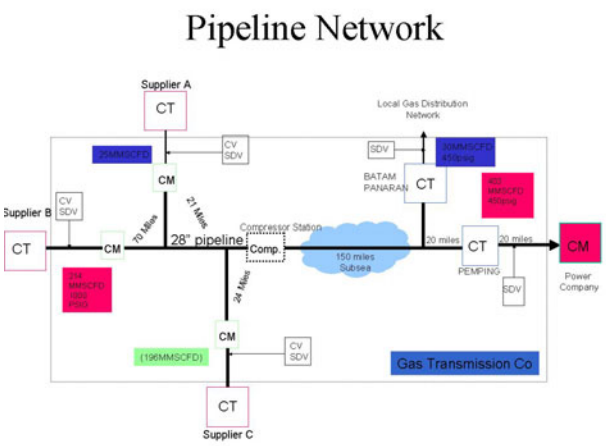

Figure 4 Example Supplier Consumer Pipeline Network

The simple pipeline network in Figure 4 represents a typical business oriented arrangement between a number of suppliers and consumers of Gas. In this case connected by an undersea pipeline of about 150 miles. The Gas Transmission Company develops a SCADA system for the above network to satisfy the following business oriented requirements.

- Monitor, analyze quality, quantity of sales gas from each receiving point up to delivery point
- Monitor and control the contracted quality throughput (gas quantity and quality) delivered to gas buyer (s)
- Manage hydraulic capacity to accommodate gas buyer's swing requirements in real time.
- Develop gas balance system for determining daily/weekly/monthly/quarterly/annual gas receipts and deliveries.

From this business-oriented set of requirements, a further set can be developed: -

1. The software must have capability to collect data from Gas SCADA, Gas metering, Gas Chromatograph and instrument analysis.

2. From entire data, the software must produce:

- Phase envelope analysis every 5(five) minutes
- Hydrate formation Detection and location.
- Composition tracking
- Pipeline transient modeling including:
  - What-if analysis
  - Look ahead analysis
  - Survival time
  - Line pack calculation
  - Process analysis
  - Leak Detection
  - Pipeline optimization
  - Fire & safety analysis
  - Pipeline optimization

3. Metering and Tariff Calculations

4. Management reporting

   - Daily
   - Weekly
   - Monthly
   - Annually

It would be reasonable to assume the block diagram in Figure 2 could be applied to help solve the business requirements in Figure 4. In engineering SCADA systems, there are many more architectures involving data structures and interfaces, which would couple these two sets of requirements.

Engineers often contend with the data flow and timing between applications to provide a gradual value add of information relating to the pipeline state and the products entrained commercial value and composition. Engineers would require a data flow diagram like the one in Figure 5 This diagram shows the many interactions and data paths for data in a typical Gas pipeline SCADA system. The general grouping of applications is that of Real time SCADA applications, an Applications database, a measurement system, a real time modeling system, and a nominations tracking system. All these systems would generally run on the database and applications servers provided at the master station as shown in Figure 2

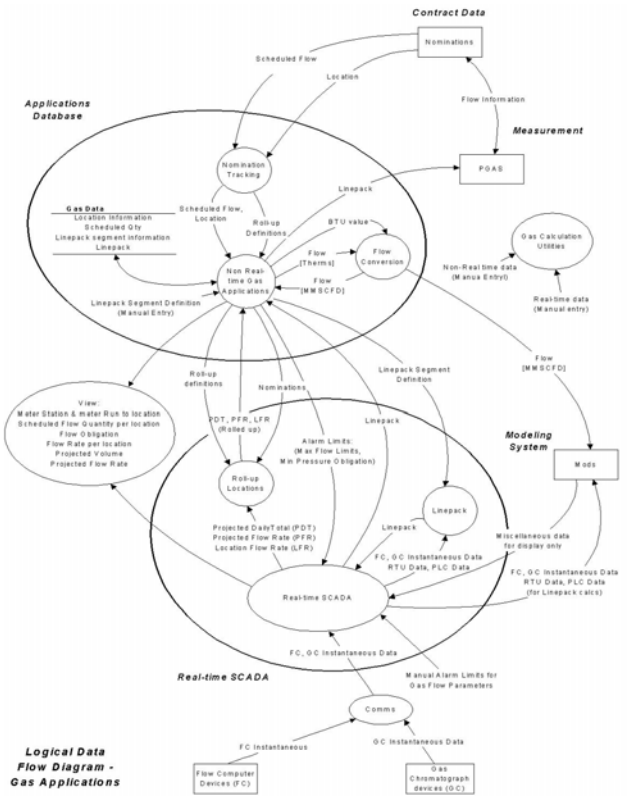

Figure 5 Logical Data Flow Diagram for Gas Applications

What Figure 5 depicts are generally the static and essential applications, often provided in the SCADA system and which would form the economic basis of operations in the system. There are many other applications that would be developed by the engineering and operational teams to aid and assist their work during the lifetime of usage of the SCADA system. This brings us to an important dynamic in information technology. Constant change. How is this then to be handled in static highly available systems?

In this paper I want to quickly bring to your attention, problems of the 21st century just starting. This will bring your overall understanding of SCADA systems to a realistic level for understanding the systems you will be seeing and working with. The requirements of availability, reliability and connectivity of Figure 2 are still important and provide the highest-level requirements of SCADA systems today.

SCADA SYSTEM TECHNOLOGY LIFETIMES

The case we are building here is one where it can be seen that the development of SCADA systems is a continuous process. The lifetime of some applications may be very short; the lifetime of the pipeline may be well over forty years. How do these two factors affect the operation and development of SCADA over the lifetime of the pipeline?

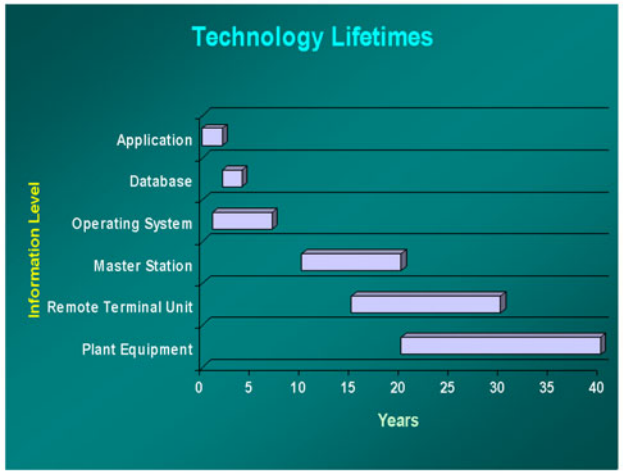

Figure 6 Technology Lifetimes in SCADA

Somewhere between the Database server and the field equipment is the point at which internet access and communications flexibility is required, which would help to match the lifetimes of measurement equipment and field installations and the SCADA data servers and enterprise demands.

ENTERPRISE INFORMATION DEMAND

This increasing demand for information relating to the operational and maintenance aspects of pipelines has outpaced the ability to upgrade field device installations and communications networks to supply the data. De-regulation, business mergers and acquisitions, and supply chain optimization require a point of flexibility to be created for supply of operational and field data. This point becomes a provider of a variety of data relating to the plant and equipment in the field, and therefore the controlled process. Whilst the revamp and extension of plant equipment may evolve slowly, the pace of business and business model change is extreme and its demands for data are only growing, not diminishing.

Whereas at some point in the near past, the demand for SCADA data was seen as only few clients, adoption of the internet has given new meaning to client server, leaving the server or data source, with now middle tier architectures, middleware, and web integration technologies to deal with before actually reaching possible the 'ultimate thin client' a voice activated control session on a normal telephone. There is however a clear point of demarcation which we can describe in terms of industrial electronic measurement technology and the realm of the Internet. For this purpose the Blue Water Blue Sky Line in introduced as in Figure 7.

The rapid pace of change in Internet technology is in contrast to the longevity and amount of installed industrial control and measurement equipment in the field. SCADA

system components like RTU s and Flow computers once installed tend to stay there and capture the state of the art of SCADA and measurement circa the installation date.

SCADA designers have had to come up with ways to connect the myriad of now almost museum grade technology installed since the 1970s boom in SCADA with the newer technologies whilst still providing the high levels of security, availability and now, operations responsiveness demanded by the fast changing internet fueled business environment

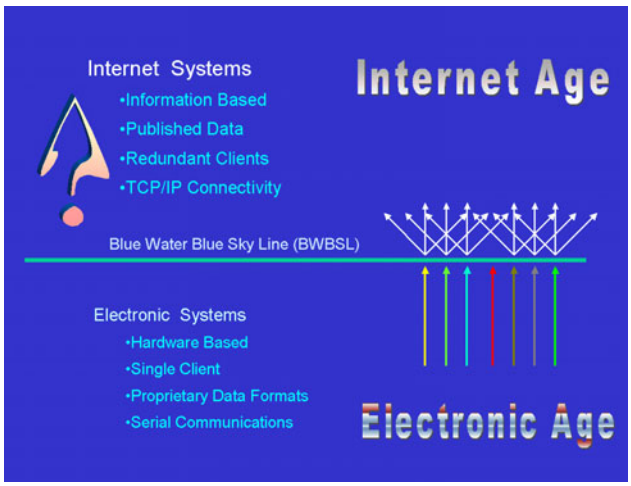

Figure 7 The Internet vs. Electronic age

An important realization in SCADA is generally in traditional architectures, there is an information hierarchy. The information is drawn up to a master station platform. The MTU provides the only real access point or gateway to the information. In the discussion on security this concept is important. Figure 8 shows what I call the SCADAspace.

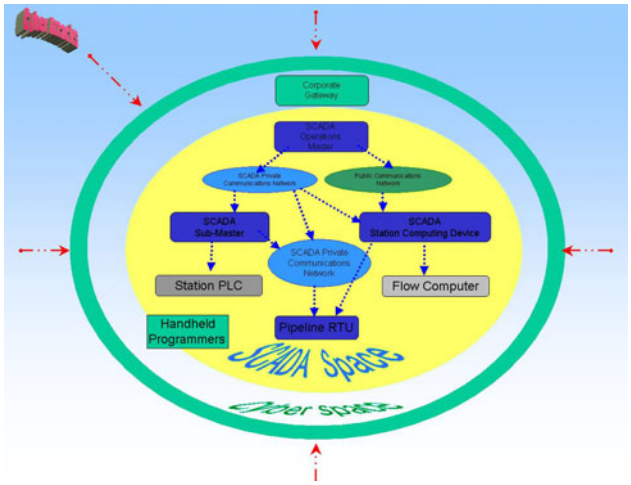

Figure 8 Defining the SCADA Information Space

Figure 3 details key components of a pipeline SCADA architecture located in relation to cyber and SCADAspace. The main communications pathways are also indicated. SCADAspace is defined as that area of information and technology, which is essentially private and not accessible to or from the public Internet. Cyberspace on the other hand is defined as the general realm of the public Internet and the network of computers and gateways serving it. One can see that in the SCADAspace, devices are generally fixed with low-level data structures, communications and information transfer protocols. In general the industry has suffered few security breakdowns due to the essentially private nature of SCADAspace.

Now you can see that the Internet is represented in **Figure 8** as Cyberspace. This is because it is generally not a space under the control of the SCADA engineer, designer, vendor, or anyone else. Whereas the SCADAspace is architecturally controlled by the pipeline operations people. Cyberspace is not. So why is it there? Why access it? Business drivers as well as the technology of the Internet are forcing engineers to include access to the Internet in more and more components of their SCADAspace. Business oriented measurement and information was often handled by means of paper reports and accumulations transferred from the SCADA operations control room to the one or two clients who needed it.

SECURITY DEMANDS and STANDARDS EVOLUTION

Since the 1990s, SCADA systems and cyberspace have become more widespread and sophisticated. As the security of infrastructure such as pipelines and utility equipment and services is now governed in part by the Department of Homeland Security in the USA, the development of component strategies such as those for SCADAspace is an important link in the strategy. All involved in the SCADA industry are, in part, responsible for its development. Initiatives associated with the new AGA Standard AGA12 are trying to capture these requirements for pipeline infrastructure.

Market forces are shifting the reach of cyberspace further into the low-level data hierarchy of SCADA. The advent of disaster recovery, web-enablement, and PDAs laptop computing, means that SCADA products will have a higher degree of Internet capability and services exposure at their access ports. Communications technologies are rapidly improving to allow a higher level of bandwidth and quality of packet information to be transmitted to the field. All of this brings the relatively insecure cyberspace into stronger and more elaborate contact with the SCADAspace.

The public communications system remained vulnerable, as did open analog communications, to a determined attacker. Successful attacks required some insider knowledge of the SCADA configuration and address schemes as well as in depth knowledge of the function

and operation of the station equipment, programmable logic controllers (PLCs) and RTUs.

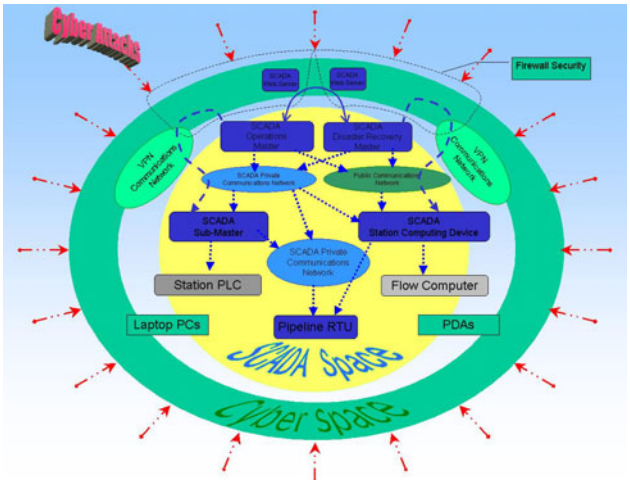

Figure 9 Current level of Cyber-SCADAspace Interoperation (2002)

Encroachment of cyberspace on the general operations, maintenance, and control of SCADA components is increasing in response to other user demands for SCADA. New business processes now demand accessibility and visibility of data at lower levels of the plant information hierarchy. The proliferation of laptop computing, windows and PDA equipment, brings permanent and intermittent contact with cyberspace into the general operation of SCADA and the once secure SCADAspace. Another development in the industry is the use of Disaster Recovery servers, and VPN channeling of communications, which use the Internet as the main transfer of information and control from site to site. Thus, the ease of use and flexibility of the Internet and cyberspace tools and techniques in SCADA operations, bring the attendant risk of security breaches and access to "deny SCADA service" to the pipeline infrastructure.

CONCENTRATION AND AGGREGATION OF DATA IN THE FIELD

Flow computer and or Remote Terminal Unit data can either be aggregated in the field or directly polled by a master station. Significant advantage can be gained by the installation of intelligent data concentrators in the field these would provide the following capabilities: -

- Give the remote site an IP Address
- Direct connect 10BaseFl, Dial-up connections
- Local polling and radio control in the legacy 'electronic age protocol'
- Multi-protocol handling
- Data normalization
- Report by exception to multiple masters with independent IP connections
- Remote configuration and download
- Brokered secure information to non controlling client applications such as measurement and asset data handlers
- A secure access point for low level data handling [AGA12-1]

The application of Internet Protocol (IP) and (IPsec) based data concentrators with speed, protocol, and data transformation features provides a pivotal point at which the legacy SCADA system components can be incorporated into a more modern Internet based system. These pivotal concentration points can be drawn on the imaginary BWBSL in the communications architecture.

The further into the field these devices can be placed, the more enhanced the visibility reach and security of the replacement SCADA system.

In this architecture, the scanning and communication modes below the BWBSL stay relatively fixed. Above the BWBSL alternate communications pathways can be established in real time to alternate centers and with OPEN standard protocols compatible with the Internet and standard networking equipment.

In modernizing SCADA system new data concentration equipment placed provide the following functionality desired by the newer architecture.

Communications Path Diversity

Whereby data trapped within a single or multi-drop path 'owned' by a particular channel master is made available to one or more masters using TCP/IP connections at the data concentrator. Use of TCP connectivity allows remote scanning to be done via Corporate Networks. Dial on Demand Routers can then be used to dial Remote terminal units, for which TCP/IP routed communications may have failed.

Information Diversity and speed matching

Whereby disparate types of information and records gained from multiple scanned legacy devices are normalized and made available to higher speed communications networks.

Protocol Diversity

Whereby legacy protocols are managed by the data concentrator, often in polled mode on local private networks, and thence after information normalization, made available to higher-level Internet age protocols and data messaging systems over generally leased and public communications networks using Open SCADA protocols to multiple masters.

Transparency and Pass through

Whereby file transfer aspects of legacy equipment and remote configuration functions can be accommodated by a pass through mode where the legacy protocol is handled over supporting internet transport and connection layers like TCP/IP.

STATION COMPUTING DEVICES

High power low cost computing technologies make it feasible to configure data concentrators for deployment to the field. A number of key features and benefits of these are described here.

Features

- Dual TCP/IP connections
- High performance processors
- Memory > 16MB
- Flash permanent memory- no moving parts
- Non Volatile Memory
- Environmental durability
- I/O Capability
- Central database
- Broker Technology
- Variety of legacy communications media and serial connectivity
- Configurable protocol stack selection and assignment
- Low cost

Benefits

- Enterprise access direct from the concentrator position
- Measurement system access direct to the concentrator
- Maintenance system access direct to the concentrator
- Better security of open access
- Alternate control room access to data
- Ability to service rapidly changing data needs and quantities
- Ability to incorporate standard or common information models close to the legacy source of data thus improving data consistency between clients

THE DISASTER RESPONSE

Newer SCADA architectures are able to transfer response from building to building, state to state, and country to country. The 'disaster' is generally defined to be something that prevents access to, disables, or destroys the main SCADA master station and communications infrastructure.

With the Internet age, the concept of operate from anywhere is now realized. Software operator console sessions can be created at the master station which may provide for visualization on a web browser from anywhere on the Internet.

Uncertainty in the connection and speed over a public Internet which itself may be impacted by the disaster makes the use of web based operations difficult to sustain as key steps in an emergency operations plan.

This difficulty means that emergency operations plans should be able to stand up without total reliance on web based remote operations.

The following general themes need to be considered in regard to disaster response and recovery.

- Transfer of Master Operations on reliable leased communications links.

Communications to a Control room building are probably the most critical element for transfer. If the control building can be networked to its communications equipment then that equipment should be reachable from an alternate control center. The placement of intelligent IP connected data concentrators in the field at key locations helps provide a means of communications transfer. The main and alternate master stations have independent and simultaneously active communication paths to the data concentration equipment. Health and readiness checks on the alternate communications pathways are required to ensure an emergency as well as restoration path capability is maintained.

- Transfer of Security to operate

With the extension of pipeline market areas by acquisition there is a requirement to handle a large number of operationally distinct areas, where individual personnel in those areas are qualified and with permission to operate. These areas of responsibility might overlap and change during the transfer of operations under disaster conditions.

The master station software and possibly the data concentration software must resolve the permissions of its clients for the area of responsibility both before during and after the transfer of control. With more open protocols and brokers allowing multiple subscribers and masters, arbitration as to the permissions is an issue that needs to be resolved as part of the design. It is no longer sufficient to assume that logon permissions cover operational permissions and that operational permissions relate directly to servers hosting operational sessions.

- Transfer of Engineering and Configuration

With the proliferation of numerous intelligent devices in the field, management of engineered solutions and configurations is becoming increasingly difficult. The incorporation of file access and transfer to each intelligent device from a single repository is key to the successful management of operations philosophy and equipment security.

- Getting back to normal…

An important point for SCADA software requirements is the ability to restore operations as well as handle the failure. A two-step process is used where the restoration of the operational system precedes a data re-synchronization phase and then final transfer of control back to its normal case. Care must be taken with transfer of operational permissions in the sequence.

SUMMARY

This paper provides a general overview of SCADA and telemetry and its use in the transmission system. Many broad concepts of architecture and design are introduced. Specific details of newer data concentration devices are introduced, as these newer architectural elements can aid in decoupling the business and disaster recovery problems from the long lifecycle field equipment measurement and communications infrastructure. Understanding of these concepts will bring the reader up to date with the requirements, market directions, and possible solutions available to the SCADA engineering community today.

AUTHORS BIOGRAPHY

Chris Smith M.E: University of NSW, Sydney, NSW, Australia. Mr Smith has been working in the SCADA Oil and Gas applications and modeling field for INVENYS since 1990. He has an extensive technical background and has held the position of SCADA system architect for Invensys. He also has extensive experience with real-time electric power SCADA applications and modeling. Currently Chris is the Invensys SCADA Products Manager and resides in Foxboro, Mass.

Email: Chris.J.Smith@Invensys.com

REFERENCES

[1] C. J. Smith, **Disaster Recovery in Pipelines,** *Article, World Pipelines, May June 2002*

[2] C. J. Smith, **Connection To Public Communications Increases Danger Of Pipeline Damage From Cyberattacks,** *Article, Oil and Gas Journal, February 2003*

[3] Dr A Stanford-Clark, Integrating monitoring and telemetry devices as part of Enterprise Information Resources March 2002, Websphere MQ development, IBM Software Group

[4] W. Rush – Gas Technology Institute, **AGA12-1 Can Reduce SCADA Cyber-Attack Risks at low cost**, A presentation to the AGA Operations Conference, April 28th 2003

[5] K. Smith, J Harrison, NiSource, **Use of Corporate Business Network for RTU Data Traffic,** proceedings of the AGA Operations Conference, April 28th 2003