

Barry Baker, P.Eng.

Pipeline SCADA Local vs. Hosted SCADA

▶ achieve more

Agenda

- 1. Introduction (Make sure you have completed Pre-test)
- 2. Classical SCADA System Definition
- 3. The rise of IP connectivity New SCADA system options
- 4. General Cellular communications overview
- 5. Hosted Systems Overview
- 6. Hosted System Communications The devil is in the details
 - Public vs. Private IP's
 - VPN's
 - Achieving redundancy
- 7. Hosted Systems Operations
- 8. Case Studies with live demos.
- 9. Summary review
- 10. Q&A
- 11. Post-test.

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 been providing hosted systems for others (not directly to end-customers) for over 12 years. These span a variety of solutions, with the largest system to date monitoring approximately 20,000 RTU's worldwide.
- Having provided both local and hosted systems for over a decade (and some hybrids), we wish to share our knowledge on the "lessons learned" in contrasting the two SCADA delivery methods.



What is a traditional (Local) SCADA System?

Every SCADA application is different. However, most share the following core elements:

- 1. Devices to collect data and control equipment (e.g. PLCs, RTUs).
- 2. A communication network to relay commands and bring back process data.
- 3. Human machine interface (HMI) software to provide a graphic interface to users.
- 4. A database of historical process information logged by the system.
- 5. A reporting package to generate scheduled or ad-hoc reports.
- 6. An alarm management system to alert personnel to system problems.



Advantages of Traditional (Local) SCADA Systems

- 1. Historical data, configuration files and security settings are stored locally.
 - Sensitive information is <u>only</u> known "inside" the corporate walls.
 - Easier compliance with the corporate security requirements.
- 2. Direct control of <u>all</u> security accounts.
- 3. In-house staff can customize applications without worry of interference on shared resources.
- 4. Direct SCADA related trouble-shooting abilities (Ping tests and other network tests).
- 5. More communications options (e.g. radio, serial, cellular IP, etc.).
- 6. Generally a "master of your own domain"!



KROHNE

achieve more



Potential Problems of Local SCADA Systems

All Projects fall into three classical "modes": Build, Operate, Maintain

- 1. Build:
 - Selecting a technology or solution can be daunting. Hiring consultants can help but increases cost with no guarantees.
 - Project time line is extended while alternatives are explored can possibly delay ROI affecting business case.
 - Higher capitol cost to deploy since purchasing all elements.

2. Operate:

Hosted systems are generally "cloud connected" by nature, and thus fewer unknowns when dealing with external access to data or operations (i.e. field deployed tablets, smart phones). In contrast, operating a secure network with outside access for a local system can be expensive and time consuming due to ever-emerging threats.

1. Maintain:

- Continual maintenance of PC hardware and software. Life cycles for servers and operating systems average 3 to 5 years, while SCADA software should be 10 15 years before major changes are needed.
- Once installed, system elements require periodic upgrades for new features and improved security. Failure to do so can prove to be costly due to lost production or downtime.
- Additional responsibilities for over taxed IT departments.





The Hosted SCADA Model

- 1. Remote monitoring & control devices collect data and control equipment.
- 2. A communication network (typically cellular) transmits commands and carries data back to a third-party SCADA host.
- 3. For a monthly fee, the host provides access to application displays via (thin) Internet clients. Predictable low cost is generally the key selling principle!
- 4. The host assumes responsibility for providing all hardware/software maintenance, automatic failover, data backup, and security accounts.





Hosted Systems

A common attribute of hosted systems (or SaaS – Software as a Service) is that they utilize thirdparty infrastructure such as the internet and/or cellular phone networks to keep costs low (i.e. Infrastructure capitol costs are distributed over millions of users).

Their emergence can be linked to the falling costs and greater capabilities of these elements as the adaptation of cellular data continues.

• Data growth over the last 5 years



Projected Data Growth



Source: Cisco VNI Mobile, 2011



Cellular Technologies: Many players & evolving standards

The lay of the land...

- There are over 180 facilities-based wireless service providers in the US.
- The total number of <u>current</u> subscribers of the top 8 carriers (AT&T, Verizon, Sprint Nextel, T-Mobile, TracFone, MetroPCS, U.S. Cellular, Leap Wireless) is estimated to be 336 Million.
- Of this number, no carrier has more that 33% of the total.
- The two historic data communications technologies were CDMA and GSM.
- LTE (Long Term Evolution) Marketed as "4G LTE" is seen as a possible convergence.
- "LTE-Advanced" and "WiMax-Advanced" are defined as "True 4G" by ITU (International Telecommunication Union).

What does the really mean?

- Varying providers and capabilities by geographic region.
- A hosted system tied to a single carrier or technology risks obsolescence as markets and competition evolve in key infrastructure.



achieve more

Coverage is not uniform when you look closely ..



- AT&T Coverage Map 2013
- http://www.wireless.att.com/coverageviewer/#?type=data

▶ achieve more

Verizon Coverage



Map Legend

Digital Coverage

Extended Digital Coverage

No Coverage



Hosted Systems: Pros

Simple Deployment

- Only RTU's and modems need be installed on site.
- Host provides standardized industry-specific pages and reports.
- Turn-key solution can be up-and-running in days not months or years.

Low Up-Front Financial Risk

Pricing Models

- Predictable monthly costs.
- Customers use what they need.
- No need for end-user to build for peak usage. Host can build for peak usage across multiple systems assuming user peaks will not occur simultaneously.

Reduced End-user Knowledge Requirements

• IT, SCADA, Security, Communications

Low Real-World Evaluation Commitment

• Customers can more easily abandon approach since lower capitol investment.

Support

• Host support is consistent while local SCADA support may shift to a lower-tier after commissioning and internal engineering resources align to other endeavors.

Hosted Systems: Cons

- Can be more difficult to customize applications and reports.
- Host company may go out of business, as start-up investment requires large numbers of users to make business case.
- Sensitive data is stored at third-party site(s).
- Remote hardware security. SaaS requires devices to be accessible over public networks.
- Host company may rely on third-parties for part of solution (i.e. cloud servers which are not without failure, i.e. Amazon Servers & Netflix outage on Dec 24 2012).
- Data throughput can suffer outages caused by external and unrelated events.
- To keep costs low, hosted servers <u>can</u> be shared amongst customers, which can result in reduced performance.
- Be aware that Virtual servers are a fraction of a real server. They do not work well with highvolume real-time data communications.
- Generally more links in the chain from measurement to delivery.





Hosted Systems: Dynamic vs Static IP Addresses

Dynamic Public IP: The device is assigned a public IP on connection or re-connection to the network. This is usually the cheapest option. Since the device address may change, the hosted solution requires some mechanism to determine the IP of a given RTU. This typically requires some type of DDNS (Dynamic Domain Name Server) infrastructure to added to the solution.

Static Public IP: The device is permanently assigned a public IP which gives a fixed address to the RTU. This simplifies the connection configuration. However, most carriers have an additional charge for static IPs.

Both have the advantage and disadvantage that any other device on the Internet can connect with the RTU.

Advantage:

- No additional configuration is required for a hosted server to connect to an RTU.
- Technicians and administrators can use any public IP connection to configure or manage RTUs.

Disadvantage:

- Network security depends on fire-walling built into the cellular modem (anybody could access the RTU).
- Data to and from the device is sent over the public internet (data can be intercepted by another party).

Hosted Systems: RTU Polling Schemes and IP Protocols

Depending on the RTU and communication protocol, the system may be configured so that either:

- The RTU is periodically polled to determine current process values and states. The IP connection is initiated by the hosting server.
- The RTU is configured to initiate a connection to the hosted server when an input value changes ("Report by Exception"). The RTU must be configured with the IP of the hosted server.

The polling approach simplifies RTU configuration and allows multiple hosted server locations at the expense of additional data bandwidth use. To provide hosted server redundancy "Report by Exception" requires either an RTU with the capability of connecting to backup servers or load balancing/routing solutions in the event of primary server failure.

RTU protocols can use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) as the transport layer for communication. In practice either will work well but UDP protocols can reduce the cellular data use by up to 50% depending on the protocol and amount of data transmitted.

Hosted Systems: Virtual Private Network (VPN) Options

To address network security and data privacy issues, many providers have VPN options.

- Uses secure connections between the hosted solution site and the cellular carrier.
- Ensures that only the hosted servers can connect with the RTUs and that any traffic over the public internet is encrypted and therefore private.
- Usually requires a technical negotiation between the hosting IT infrastructure and cellular providers to develop a suitable secure solution.
- VPN architecture may be complex if both the hosted solution provider and the cellular carrier have backup data sites.
- Redundant VPN links between two hosted solution sites and two cellular provider network centres may require dynamic router paths and additional load balancing hardware.

achieve more

Typical Redundant Hosted Data Center/ Redundant VPN Provider Network Arrangement





Hosted Systems: Other Communication Concerns

Not all Telemetry devices\protocols work well with cellular networks:

- Delays in connection
- · Changes in IP addresses or access points
- Dropped calls & recovery
- Data costs with Polling vs. Exception based reporting

Cellular carriers can obsolesce communication technology faster than the telemetry hardware life-cycle.

• One large customer found that after struggling with GSM coverage and varying standards, CDMA was more reliable and consistent – But slower and destined for replacement.

Data plans must be carefully managed

- Costs are dropping, but the mentality of \$/byte must be observed (or big surprises can emerge).
- Data packet plans can include the cost of the telemetry data + <u>IP packet overhead</u>.



Operations with Hosted Systems

What do they look like, how do they differ from a local system?

For the lower cost, do I get what I need?

Depends upon the "type" of Host system offering:

Database driven forms vs. Full Function HMI's

Database form based solutions (Active Server Pages, JAVA applets, etc.):

Tend to tabular in nature, with generic display elements similar to those found in MS Excel, etc. Delivered via HTML and/or Java.

Work on a client request to server then response.

Tend to work well with varying screen resolutions.

Generally leverage OS API's so server updates can introduce new "styles"

Achieving fault-tolerance using redundancy can be limited due to underlying DB technology and limited client-side processing.

Full Function HMI Hosted systems

- Display Process displays similar (or identical) to SCADA HMI (i.e. Pipe layouts, maps, alarm lists, Historian, etc.).
- Leverage fault-tolerance of HMI product.
- Can have issues with varying resolutions of client screens (i.e. Aspect ratios, like TV's).
- Look & feel is largely dependent upon HMI changes vs. OS updates.

Client Sides generally come in two "flavours" :

- "Light" Program working in conjunction with Server (i.e. Thin-Client).
- Client side via Remote Terminal Session of Server.



Case Study #1: SJRWMD

Need: The St. Johns River Water Management District (SJRWMD) is responsible for operating flood control structures and protecting water quality for roughly five million people in Northeast and North Central Florida.

After two hurricanes in 2004 cut network access to two of their remote monitoring sites, the district's Engineering Division decided to implement a redundant cellular-based SCADA system to take over when the primary is unavailable.

Result: A Hybrid solution was adopted, where critical elements were monitored via the installed local system AND a hosted system.

The remote system was required to be located outside the state of FL, AND not have any infrastructure elements installed in the historic hurricane paths that could affect the district.



Case Study #2: Southwest Florida Water Management^{achieve more} District (SWFWMD)

Background: FL Water Management Districts are required by State law to publicly disclose their Hydrological data so that interested parties may review the data collected by their SCADA system. This is to permit oversight and/or provide information to review or contest decisions made by these government bodies with regards to public resources.

Live Example of Public Facing SCADA System – example of full-function HMI via Internet.





Case Study #3: Live Demo

Example of operations & display on a attendees computers, tablets and Smart phones.





Summary: Selecting a Hosting system Vendor

Things to consider when selecting a Hosted system host:

- Ensure proper support and diagnostics assistance will be provided, since you are giving up some control of your system.
- Choosing a nearby host can help reduce latency.
- Ask how data backup is handled?
- Ask how redundancy is achieved for critical infrastructure?
- Clarify who "owns" the telemetry data collected?
- Demand the host provide availability reports measured by third-parties (i.e. Website Pulse, etc.).
- Check host policy with regards to eligibility for product upgrades and new features over time. Some vendors are not very backward compatible.
- Investigate the export tools available (data and configuration) in any SAAS system you may select. This will help you move to a different vendor if you are not satisfied with the service.
- Be wary of telemetry hardware + carrier packages that may leave you exposed when the cellular infrastructure evolves at a faster pace than your business application (People now update\change cell phones on average every 2 to 3 years!)

Summary: Other Considerations

- Owning a local system means you are responsible for making sure it works.
- Subscribing means you rely on someone else to make sure it works.
- Large corporations typically have very knowledgeable IT staff with little to no SCADA knowledge. Solutions can be IT driven which may not be the best solution for an engineering problem, and the lack of knowledge can result in external support being hampered by lack of IT credentials.
- Investigate overhead costs of communication service. Cellular/sat data can be very expensive. Determine your data requirements in terms of bandwidth and your sensitivity to data age.
- Local SCADA systems have the option to outsource work and take advantage of competition between vendors. When locked into SAAS system, you will likely have few or sole-source integrators.
- Rather than accessing SaaS over the open internet, you can use a VPN to access your host's network to ensure an extra layer of security.



Q&A

Your turn to speak !





Post-test

Were you taught anything?

