

## Achieving the Always-Available Network: Ensuring Constant Network Availability and Control Through Secure Remote Management

Barry Cox, CTO  
Uplogix

Like many industries, the oil and gas industry has long been faced with the challenge of how to securely manage its distributed network infrastructure and remote locations. Maintaining availability of communications equipment and network infrastructure on offshore oil rigs is essential in order for companies in this industry to thrive. In many cases, these offshore oil rigs are outfitted with elaborate network infrastructures and computing systems that enable operators to do everything from maintain the rig's position to transmit production data in real time to company management, geophysicists, sales associates and engineers.

But when network problems arise and connectivity is lost, a critical link is severed between the offshore rig and the rest of operations, which can result in lost production. And in an extremely competitive business such as the oil and gas industry, a few hours of lost production can translate into significant lost revenues, and potentially market share.

However, a solution to this complex problem currently exists and is enabling proactive enterprises, including those within the energy sector, to more easily manage their remote locations while also saving money and time. By employing secure remote management solutions locally, oil and gas businesses can better rely on the network to always be available, reliable and performing well. Additionally, this solution can increase business efficiency by reducing maintenance and other costs, and decrease the problems that arise when companies rely solely on their IT staff to diagnose and fix common network-related problems.

Historically, the energy industry has had to make due with unreliable, passive network and systems management tools that were not specifically designed to handle today's remote management costs, complexities and risks. For instance, an oil and gas service company with a rig stationed off the coast of Africa relies on that rig's ability to pump oil and gas out of the depths of a well. It is essential that the information about the well system and the rig's

critical equipment is accessible by company management from thousands of miles away. Off-site analysts pouring over data may determine that oil production may increase if the oil rig's drill bit is moved two feet to the left of its current position. However, if and when network connectivity is lost, analysts, as well as company managers and engineers, are suddenly in the dark; they have no way of tracking or manipulating the rig's systems.

At this point, the service company's IT staff goes to work. But the IT technician who can best solve the problem may be hundreds or thousands of miles away. Worst case, a technician might embark on a journey around the globe in order to fix what may be a minimal IT problem. By the time the technician arrives at the oil rig and fixes the network problem, it is likely that hours or even days have passed without the rig being able to communicate with onshore analysts and engineers. Unfortunately, oil and gas service companies face this problem on a regular basis. An outage like this can translate into a costly situation for any oil and gas company, not to mention the exorbitant cost required to physically transport the IT technician to the remote oil rig.

However should the same oil and gas service company employ a secure remote management solution, the company can save the time and expense of sending that IT technician, and minimize the production downtime caused by that lost connectivity and communication.

### An Intelligent Gateway

Many oil and gas companies are proactively taking a new approach by implementing secure remote management solutions. These solutions are deployed as part of the network and communications infrastructure directly on the rig, where they act as a local administrator's eyes, ears and hands, ensuring the network consistently stays up and running and doing what it is designed to do.

The secure remote management platform can also act as a gateway for all the systems onboard the rig. And because it is connected to a secondary, cost effective network that is operated through a satellite-based communication system, an authorized operator can remotely access important information about the rig, or even manipulate

any of the rig's communications equipment, since all actions are routed through the local management device. This provides remote access and control to any of the rig's network infrastructure components that are connected to the WAN (wide area network).

IT administrators and operators can remotely access, monitor and control hybrid satellite and terrestrial networks, and all other connected equipment including routers, switches, firewalls, GPS devices, power controllers and other management and control systems. If and when there is a network outage, the remote management platform is able to "call home" via a secure, satellite-based out-of-band connection to a central management station so that connectivity and control is constantly ensured.

The secure remote management solution also has the ability to diagnose and fix common technical problems with the communications infrastructure while also performing maintenance tasks and necessary upgrades. It is essentially a self-sufficient remote technician and remote administrator in a box.

By minimizing the challenges of managing remote sites and other highly distributed infrastructure, secure remote management solutions enable enterprises to overcome the limitations associated with console servers and network-dependent monitoring tools to deliver the active, secure management required to keep remote sites online and under control.

### Automated Problem Resolution

Whether IT staff is sent to remote locations in order to fix network problems like restoring unresponsive devices, or just to perform routine system maintenance such as OS upgrades or configuration changes, companies are forced to invest the time and money associated with having to deploy valuable and scarce IT staff to remote locations throughout the world. This time and cost can be recouped by simply relying on the intelligent automation capabilities that a secure remote management solution can provide. Additionally, the use of automation helps reduce operator errors that may arise when relying on technicians to maintain and fix problems at remote sites.

According to Nemertes Research, IT staff at large enterprises spend between 30 and 50 percent of their time troubleshooting and fixing problems at remote locations. As oil and gas service companies continue to add more remote sites, IT staff is only spread more thin. And delays in reaching these remote locations can mean more production time is lost. This problem, says Robin Gareiss, executive vice president, Nemertes, can easily be resolved by replacing the manual processes of IT staff with automated management tools.

"IT staffs must manage a growing number of remote locations without increased headcounts. With 11 percent annual growth in the number of branch offices, it's imperative for them to have both local and centralized management tools to help deliver consistent and cost-effective application performance over the WAN," says Gareiss. "In our research, the more sophisticated IT executives who run aggressive IT organizations consistently place 'automated problem/resolution' as a key item on their wish lists. They want tools that replace manual processes for maintenance and recovery with automation. We expect a growing number of IT staffs to look for these capabilities."

Secure remote management solutions have the ability to automate hundreds of routine network

**Now Available Electronically!**

**SUBSCRIBE TODAY TO GET  
THE LATEST NEWS ABOUT**

**REMOTE**  
Site & Equipment Management



**New Products, Companies,  
The Industry, Research &  
Development and Events.**

For a new subscription, or to renew your current subscription go to:

[www.RemoteMagazine.com/r-sub.php](http://www.RemoteMagazine.com/r-sub.php)

and select Print or Electronic Edition

maintenance and recovery tasks. These include detecting and correctly diagnosing equipment and communications failures, executing pre-defined, best-practice recovery procedures, provisioning and re-provisioning services, configuring devices via remote administration, and measuring and managing both application and network service levels from a remote perspective.

As the demand for skilled remote IT staff increases, many industries and business sectors are deploying secure remote management solutions. Some oil and gas service companies have been able to automate more than 75 percent of their routine network support and maintenance tasks. Additionally, these companies have been able to grow faster without having to increase or overextend IT staff. They have also been able to minimize expensive tech support trips and lower remote support costs in the process.

### Security and Compliance

Being able to effectively manage a remotely located oil rig is paramount for oil and gas companies. But just like in the data center, security and management policies aboard a rig need to always be enforced, even during a network outage or other maintenance window. System administrators need to be able to control who has access to devices on the network, what they are doing while accessing the devices, and be able to accurately report on all user interactions in order to satisfy security and compliance requirements. Thanks to secure remote management technology, meeting all of these requirements has become possible.

In order to effectively, efficiently and securely manage remote locations, solutions need to be deployed where they are needed most: at the edge of the network. Historically, when outages have occurred at a remote location, in-house or out-sourced support staff would likely be given root-level access to systems and applications in order to quickly restore them. But this can unnecessarily expose an organization to potential security risks and threats. In order to satisfy strict compliance requirements, IT administrators must be able to identify information about what changes are being made in the network, who is making them, and what the impact of those changes will be. And they must do it all quickly and correctly.

Through the use of remote management technology, end-to-end management security is absolute by providing encrypted access to all managed devices, enforcing authorization and authentication policies while also auditing all user interactions and configuration changes. And the intelligent architecture ensures both internal and regulatory security standards will be enforced at all times, even during a network outage or service disruption, addressing the problem without new costs and complexity to adhere to those policies.

By implementing secure remote management within their enterprise network, IT administrators can collect all device interactions and configuration changes for each managed device in the network, including satellite communications equipment. Once again, because of the management system's direct connectivity to each device, compliance requirements can be met, even during network outages and disruptions, since the system is not dependent on the network itself to gather and report this information.

### Meeting All the Requirements

With remote management already being adopted within many business sectors, including the financial services, health care and retail industries, the oil and gas sector in particular can benefit from the capabilities of this customer-

centric technology approach to the problem. IT staff and administrators have 24-hour access to and control over their remote network infrastructure, even during network disruptions.

By co-locating management technology at a remote site, a secure remote management solution can perform the majority of the routine administration, maintenance and recovery tasks that an on-site technician would normally perform, but in a quicker, error-free manner and at a fraction of the cost. And by diagnosing and fixing problems locally, automating routine maintenance tasks, and controlling who has access to networked devices from a centralized location, support costs and incidences of downtime are dramatically reduced.

So the next time communications is lost with that oil rig

off the coast of Africa, IT administrators can relax. Companies no longer need to foot the cost and risk of sending a technician across the world and worry about lost production time. Getting communications with the rig back up and running can be done quickly, automatically and error-free with a secure remote management solution.

*Barry Cox is currently the Chief Technology Officer at Uplogix and can be reached at [bc Cox@uplogix.com](mailto:bc Cox@uplogix.com). Uplogix is privately held and headquartered in Austin, Texas with European offices in Canary Wharf, London, U.K. For more information please visit [www.uplogix.com](http://www.uplogix.com).*

# Remote 2008

## CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

### 2008 Call for Papers Deadline April 25th, 2008!

No other industry conference brings together technology users that manage remote sites like the Remote 2008 Conference and Expo. Over 50 conference sessions will provide cutting-edge technology direction and application strategies from the companies and users driving the growth in SCADA, M2M, device networking, data communications, system & site security, emerging wireless technology, remote monitoring and automated control, and onsite powering of distributed equipment, networks and facilities.

### Subjects Areas Include:

- |  |  |
|--|--|
| Emerging SCADA Technology                        | Back-up and Stand-by Power Solutions                   |
| Mesh Networking                                  | Gen-sets, Fuel Cell and Other Onsite Power Solutions   |
| Designing and Implementing New Networks          | Renewable Energy as a Remote Power Source              |
| Adapting and Upgrading Existing Networks         | Power Reliability for 24/7 operation                   |
| Device and System Capabilities & Testing         | Dual Redundancy of Power for Critical Operations       |
| Selecting the Right System for Your Application  | Low Power Systems for Monitoring and Communications    |
| Network Reliability and Accountability           | Power Protection Systems                               |
| Basic Networking Configuration                   | Substation Automation                                  |
| Network configuration in a static environment    | ROI on Monitoring Technologies                         |
| Basic RF troubleshooting                         | Integrating Wireless Technology into existing systems  |
| Standards (ISA100, 1451, NERC)                   | New Wireless Technology for Remote Sites and Equipment |
| Basic network design including IP configurations | Security (Cyber and Physical)                          |

For more information about submitting a proposal contact Nick Depperschmidt at: [Nickd@infowebcom.com](mailto:Nickd@infowebcom.com) or 800-803-9488 x.111 or visit [www.remotemagazine.com/rem08\\_call.php](http://www.remotemagazine.com/rem08_call.php)

For more information about sponsoring or exhibiting contact Scott Nash at: [ScottN@infowebcom.com](mailto:ScottN@infowebcom.com) or 800-803-9488 x.114

NOVEMBER 5-6, 2008 - ATLANTA, GA.