

Smart Remote Connected Sites

Using Cellular Automation to Monitor & Control Assets

Smart Remote Connected Sites

While every business strives to ensure uptime and availability for customers, operators within the utilities space have additional regulatory and monitoring requirements that must be adhered to as well. For both financial and safety reasons, utility companies are building high-availability smart sites to help minimize unscheduled downtime and time to repair. This white paper will discuss how cellular automation enables cost-effective monitoring and control of data at remote sites.

Table of Contents

Introduction	3
Monitoring & Controlling Data at Remote Sites	3
Using Cellular Automation to Access Data	4
Comparing Alternative Solutions	4
Using an Integrated Software Development Kit	5
Creating Smart Remote Connected Sites	5
The Red Lion Advantage	4

Introduction

Today's utilities operate in highly productive business environments that are very competitive. As such, these organizations need to comply with stringent regulatory requirements to prevent downtime that may negatively impact customers. A slight failure of equipment can translate to immediate consequences from both a financial and safety perspective. These pressures are driving utility companies to build high-availability smart sites that help minimize unscheduled downtime and time to repair.

A direct result of this trend is the deployment of equipment to facilitate remote access, regardless of geographic location. To help enable remote connectivity, utilities are integrating legacy serial equipment with IP networks. Despite the many benefits this offers, the move to IP networks may add a level of complexity as it becomes increasingly more important to securely connect critical industrial infrastructures. This white paper will discuss how cellular automation enables cost-effective monitoring and control of data at remote sites.



Monitoring & Controlling Data at Remote Sites

Remote sites are typically located in places that are difficult to access due to long distances, harsh conditions or limited field staff availability. Accessing critical information, such as equipment status and operational data, at remote sites can be time consuming and costly. Additionally, given today's aging industrial infrastructures, monitoring and controlling the data within these sites is more critical than ever. In fact, organizations are beginning to witness the consequences of not updating and maintaining outdated networks. Consequences may include utility blackouts and gas pipeline explosions.

Keeping a closer eye on these infrastructures is necessary not only to prevent loss of revenue, but also loss of life. Unfortunately, communicating with these remote sites to proactively prevent equipment degradation is far from an easy task, and in some cases may require lengthy helicopter rides to isolated locations. In order to proactively monitor and control remotely-located assets, users must be able to access local sensor-level data. The most cost-effective and intelligent way to do this is through cellular automation.



"In order to proactively monitor and control remotely-located assets, users must be able to access local sensor-level data."

Using Cellular Automation to Access Data

Cellular automation is the concept of adding cellular connectivity to Remote Terminal Units (RTUs) to facilitate access to data in hard-to-reach locations. Cellular connectivity provides reliable, easy data access that enables organizations to monitor and control critical applications at remote sites.

Remote access to data, however, requires enhanced security measures be taken. In some cases, this is new ground for many users. Data security is something that many customers have yet to focus on because they are using direct circuit connections via modem banks or private radio networks. These types of connections do not have the same stringent security standards as cellular connections over IP networks. Therefore, as organizations migrate towards IP networking where data security is mandated, sourcing and implementing new technologies to support increasing security demands becomes necessary.

In addition to addressing more stringent security requirements, industrial users also have the added complexity of managing multiple devices when implementing an effective remote monitoring and control solution over IP. The challenge in this scenario is figuring out the additional products that they will

require in addition to their existing RTUs. For instance, it may be necessary to have a cellular modem, a Modbus gateway and a security VPN client, all of which are costly to deploy and complicated to administer and maintain. Deploying a cellular automation solution dramatically simplifies this task by integrating automation, routing, security and cellular technologies into one hardened package. A built-in Modbus gateway easily interfaces with existing RTUs and PLCs to provide real-time access to data from pumps, valves, reclosers, transformers, capacitor banks and meters.

For industrial networks such as oil & gas, power, utilities and water/wastewater applications, accessing data in real time and keeping networks up and running is critical. More stringent security requirements, such as EPA and NERC, must also be supported as the network continues to evolve and grow. Additionally, an integrated firewall that provides stateful packet inspections, as well as filtering of IPs via access control lists or NAT, is needed to avoid new threats. More specifically, it is necessary to have integrated user firewall configuration rules that restrict the type and duration of access to authorized individual user-based permissions and encryption of data to provide adequate security for business-critical applications.

Comparing Alternative Solutions

Short Messaging Service (SMS) based solutions are another lower-cost alternative that some companies have chosen to implement. Although this approach may be effective and easy to use, it has inherent risks. Text messages are a powerful means of attack because the devices that receive them generally cannot refuse delivery. The problem is that organizations cannot block unauthorized texts, which may include unwarranted command execution.

Adding a standalone cellular modem to existing equipment presents another approach that may be considered. While this alternative offers remote connectivity, the lack of security options on most cellular modems leaves the network open to attacks and adds complexity when managing several remote devices.

In comparison, an effective cellular automation solution based on TCP/IP networking provides anywhere, anytime connectivity

while offering security features that meet stringent mandates. Cellular automation cost-effectively solves remote monitoring problems by integrating cellular data networking to enable SCADA data to be securely communicated from the remote site back to the control center. This approach helps to improve safety, productivity and security while driving profitability.

Today, most—if not all—remote sites contain legacy serial devices that require connection to IP-based services. Serial-to-IP conversion can be difficult due to speed and protocol differences. Cellular automation simplifies this process by connecting RTUs, PLCs and other HMI equipment and gives organizations real-time access to data at remote sites. This solution also eliminates costly visits to remote sites for minor software changes or data collection, which can translate to large savings for organizations.

¹ http://www.strategosinc.com/toyota_production.htm

Using an Integrated Software Development Kit

Another critical element of an effective cellular automation solution is an integrated Software Development Kit (SDK) that enables application customization. Today's highly efficient environments demand flexibility that allows users to customize features to meet specific site requirements while providing software tools that integrate proprietary applications. An example of this would be the development of custom software code, which is designed to extract specific types of data and formatting for special reports. In the absence of using an SDK, additional time and resources would need to be dedicated to application support.

To efficiently address the remote monitoring and control challenges of today's industrial networks, an integrated and cost-effective solution that supports both legacy serial-based

equipment (Modbus RTU) and next-generation IP based (Modbus TCP) environments within a single hardened platform is required. Furthermore, the additional complexities of managing multiple locations require remote sites to have easy-to-configure software. The goal is to allow remote users to do everything that they would typically do on site. This means that robust device management software should provide everything from health status and connectivity information to remote and mass device configuration. A smart remote site connected via a cellular automation solution with an integrated SDK provides users the ability to monitor, reboot and control equipment without requiring a technician to be sent to the field.

Creating Smart Remote Connected Sites

Smart remote connected sites protect RTUs, PLCs, HMIs and process control equipment using a secure, easy-to-configure solution that is integrated into one cellular automation device. Red Lion Controls is leading the way to cellular automation with its Sixnet® series RAM® 6000 and 9000 industrial cellular RTUs. Red Lion's RAM RTUs combine a built-in Modbus gateway and state-of-the-art firewall with full router functionality and 4G LTE cellular connectivity to provide a compact, industrially-hardened device that can easily be implemented without disturbing the existing environment. Having all this intelligence built into a single cellular automation platform provides an optimal solution for creating smart remote connected sites. Visit www.redlion.net/RAM to learn more.



The Red Lion Advantage



As the global experts in communication, monitoring and control for industrial automation and networking, Red Lion has been delivering innovative solutions for over forty years. Our automation, Ethernet and cellular M2M technology enables companies worldwide to gain real-time data visibility that drives productivity. Product brands include Red Lion, N-Tron® and Sixnet®. With headquarters in York, Pennsylvania, the company has offices across the Americas, Asia-Pacific and Europe. Red Lion is part of Spectris plc, the productivity-enhancing instrumentation and controls company. For more information, please visit www.redlion.net.

©2015 Red Lion Controls, Inc. All rights reserved. Red Lion, the Red Lion logo, N-Tron and Sixnet are registered trademarks of Red Lion Controls, Inc. All other company and product names are trademarks of their respective owners.



Americas
sales@redlion.net

Asia-Pacific
asia@redlion.net

**Europe, Africa
Middle East**
europe@redlion.net

+1 (717) 767-6511

Connect. Monitor. Control.

www.redlion.net

ADLD0440 111115