REMOTE
Site & Equipment Management
June/July 2005 Volume 5, Issue 4 a webcom publication

Optimizing Remote Site Equipment Configuration, Monitoring and Control

By Talbot Hack
Eastern Research

Most large network operators - including mobile wireless service providers, wireline telecoms, infrastructure-based service providers, government agencies, utilities, energy companies and other critical infrastructure operators - are under constant financial and competitive pressure to improve the quality, breadth and profitability of the services they offer. Yet the complexity in operating, maintaining and securing wide-area telecom and data control networks has only increased over time. Network administrators must monitor and control numerous heterogeneous network elements at what are typically remote, unmanned locations with limited connectivity. The remote elements at these sites - often spanning multiple generations of equipment and overlay network infrastructure - may each require a separate management platform and legacy communication protocol, driving up site access equipment needs and overall operational costs.

To alleviate these limitations and improve operational efficiency, an effective and flexible remote configuration, monitoring and control or telemetry solution must allow "plug and play" operation to quickly accommodate future services, enable quick, trouble-free access to remote network elements, support IP connectivity to each site and each device, permit protocol/topology segmentation for security reasons, and should integrate easily with network performance monitoring platforms such as NetCool, NetBoss, Micromuse and others.

Common examples include the telemetry needs at mobile wireless cell sites and SCADA-based monitoring and control of remote sub-stations within utility networks. Figure 1 illustrates a mobile operator's base station telemetry environment, showing management data connectivity back to a network operations center (NOC).

Example Network Elements & Requirements

There are numerous examples, spanning multiple industries, of remote network elements (and control protocols) that can be operated more efficiently - and operational procedures that can be streamlined - utilizing an intelligent, integrated remote management strategy, including:

-- Power Management Systems - Monitoring power distribution, battery back-up systems and rectifiers (via dry input/output contact alarms and relays; asynchronous data)

-- Heating, Ventilation & Air Conditioning Systems - Measuring temperature and humidity stability for environmentally sensitive site equipment (via IP, serial data)

-- Fire, Security & Access Control Systems - Enabling alarm relays, entry and exit control systems, door locking mechanisms and logging software to record who entered/exited the site and when (via asynchronous data)

-- Surveillance Systems - Closed-circuit video and Ethernet-based webcams to provide 'active' remote security and visually identify visitors before permitting site access (via streaming Ethernet/IP data)

-- Back-up Generators - controlling generator start/stop circuitry during power failures and restoration (via dry input/output contact alarms and relays)

-- Technician Access - providing intranet, email and diagnostics access to remote technicians conducting onsite maintenance (via streaming Ethernet/IP data)

-- Smart Devices - Smart antennas and location-based servers being deployed by mobile operators (via Ethernet/IP streaming data)

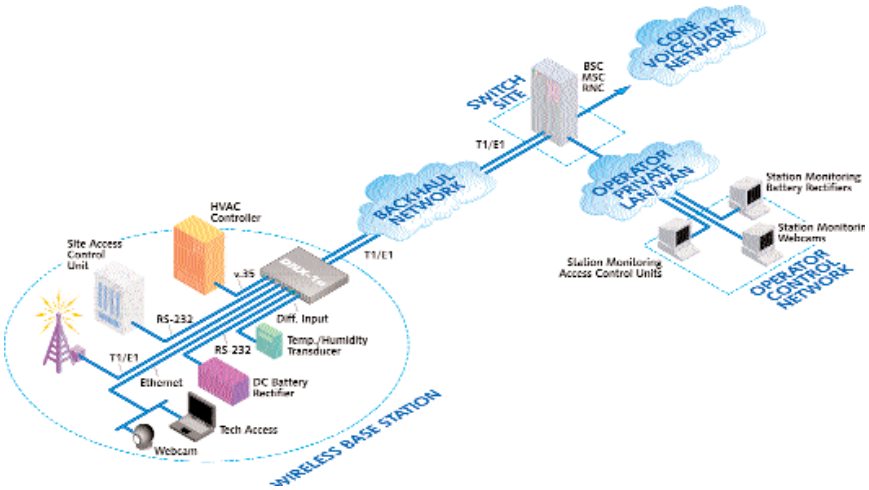

Figure 1 - Typical Mobile Operator Base Station Telemetry Environment

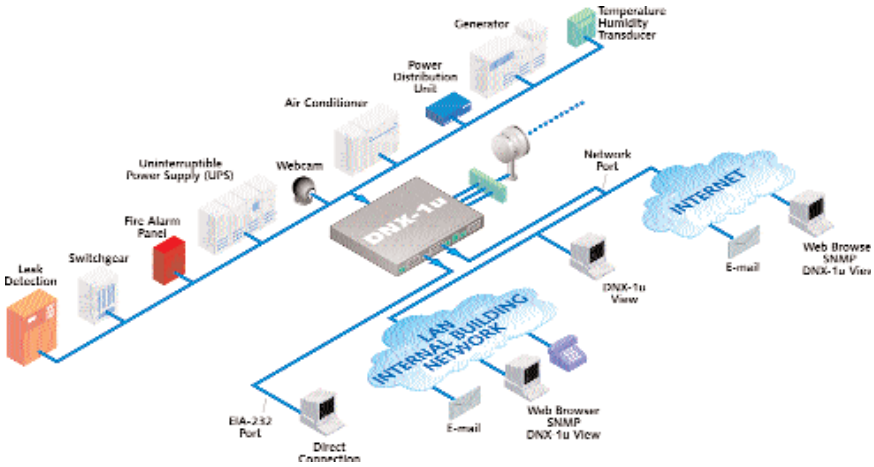

Figure 2 - Eastern's Versatile and Compact DNX-1u Solution for Today's Telemetry Needs

Benefits of an Integrated, IP-Based Management Approach

From a technical perspective, wide-area telecom and data control network service nodes and substations are frequently unmanned locations with limited connectivity options. These sites can be located far from service and dispatch centers, making scheduled (and especially unscheduled) maintenance and service upgrades difficult and expensive. From a business perspective, network operators are under constant pressure to extract operational expense and improve profitability. Key opportunities for efficiency gains include network field operations, administration, maintenance and provisioning, reducing 'windshield time' for field technicians and improving their productivity per site visit.

The business case for an integrated remote management strategy starts to take shape when these technical and financial factors are combined. First, cohesive remote management enables the NOC to have greater visibility and be better informed, since alarm isolation, fault diagnosis, trouble-shooting and analysis can take place prior to dispatch. Second, truck rolls and unnecessary visits to unmanned facilities can be reduced and in many cases eliminated due to improved site monitoring. Routine system maintenance and upgrades can in many cases be performed remotely as well. Third, it enables faster restoration of service because problems can be diagnosed and resolved in minutes rather than in hours. Fourth, greater NOC visibility can yield significant operational cost savings due to fewer truck rolls, reduced travel and onsite time, lower administrative and overhead support costs and even reduced fuel costs due to fewer instances of back-up power generation being required. Last but not least, remote intruder detection, site access control and 'lights out' surveillance from the NOC can dramatically improve site security, minimizing capital losses from theft and vandalism.

Reprinted from the June/July 2005 issue of Remote Site & Equipment Management Magazine

Significant 'soft savings' can also be derived from an integrated remote management solution: stemming revenue losses due to service outages or dissatisfied customers; minimizing regulatory fines due to inoperative aircraft warning lights on major structures such as radio towers, antennas and smokestacks; consolidating legacy equipment and re-claiming valuable rack space (which can be especially important in remote collocation facilities, equipment huts and sub-stations with limited or no room for equipment growth).

Real-World Applications

Real-world examples of this strategy in action include major mobile network operators in the US, South Africa and Turkey as well as forward-thinking North American utilities.

The mobile operators must manage complex, geographically dispersed radio access networks representing a significant portion of their recurring operational expense. As a result, they have significant incentives to improve operational efficiencies by concentrating management of everything from base station intruder detection and access control systems to battery and rectifier management systems, environmental control systems, tower aircraft warning light controls, technician IP access and microwave backhaul control systems onto an intelligent telemetry aggregation platform at each base station. This platform then enables consolidated IP-based data communication in-band over existing T1/E1 transmission facilities to their regional NOC.

North American utilities must also manage extensive private networks, in their case SCADA-based control of valves, transfer pumps, leak detection systems, reservoir and tank monitoring systems, microwave systems, etc., but much of the underlying communications and telemetry infrastructure at hubs, sub-stations and remote terminals is woefully inadequate for remote diagnostics and configuration. This lack of visibility often leads to unnecessary truck rolls and misdiagnoses. Increasing disaster recovery regulation and security concerns at the State and Federal levels is putting further pressure on the industry to upgrade their SCADA network capabilities. The response has been similar: deploy an intelligent, integrated remote supervisory node to replace multiple legacy communications devices, consolidate alarming over a single IP (SNMP) channel and provide technician network access during site visits.

Integrated Telemetry Concentration Solution

Eastern Research's answer to the telemetry challenge is the DNX-1u Access Gateway, an intelligent platform combining sophisticated telemetry capabilities with multiple transmission interfaces and flexible cross-connect functionality. Whether a DNX-1u is installed in a mobile network cell site, a utility sub-station or a carrier POP, virtually every remote element deployed at that location can be managed from a centralized location.

The DNX-1u provides analog inputs to monitor signal levels and generate alarms when configurable thresholds are exceeded. Contact closures can be configured as general purpose outputs and remotely toggled, enabling recycling of devices. The DNX-1u can also send alarm notifications via SNMP for integration with other network performance, monitoring and management tools.

For improved operational efficiency, a field technician can quickly and easily access the central network via the DNX-1u's Ethernet/IP connection to get email, check a work order, or conduct a remote diagnostic test.

Talbot Hack is the Product Line Manager for access & telemetry platforms at Eastern Research Inc. (www.erinc.com) Talbot is responsible for management of Eastern's access portfolio, and brings nearly 20 years' experience in high-tech and the telecom industry - including management positions with equipment vendors such as Network Express, Cabletron Systems, Enterasys, and Avail Networks.

Reprinted from the June/July 2005 issue of Remote Site & Equipment Management Magazine

www.erinc.com

Reprinted from the June/July 2005 issue of Remote Site & Equipment Management Magazine