



GAINING CONTROL OF REMOTE INFRASTRUCTURE WHITEPAPER

KENTROX

REMOTE SITE MANAGEMENT

TABLE OF CONTENTS

> Executive summary	1
> A confluence of priorities	1
> Remote sites: the weakest link	3
> Challenging delays	4
> Remote operations: more than meets the eye	4
> The remote site: what it takes to manage it	6
> Creating a sound, flexible architecture	6
> More than technology	9
> Tangible results: the “intelligent dispatch”	10

EXECUTIVE SUMMARY

Increased competition for wireless subscribers is forcing network operators to expand advanced technology support and services to larger geographical areas. Significant investments are being made to deliver on these priorities while budgets and resources are being maintained or reduced for maintaining infrastructure quality.

The management and protection of critical infrastructure such as communications, utilities, and transportation systems is a challenging task because literally millions of core cellular network elements are at un-staffed remote, rural, and underground locations. Generations of disparate technologies are at these sites, raising complexity, causing interoperability issues and risking availability and security. The operations and management teams responsible for the distributed equipment and facilities at these sites are faced with reduced budgets along with increasing expectations for infrastructure maintenance, performance and security. Innovative operational strategies are the only chance at gaining control, improving efficiencies, and reducing costs.

The case study contained in this document will show how advanced operational strategies for remote site management can reduce the time spent on travel and troubleshooting by as much as forty percent (40%). In addition, these strategies can increase network infrastructure availability and quality, improve preventative maintenance and resource efficiencies, and triple the time available for infrastructure improvement and expansion.

A CONFLUENCE OF PRIORITIES

The management and protection of the world's communications infrastructure is arguably one of the most critical challenges we face in a globally networked world. We must be prepared to provide life-saving service during emergencies and provide 24x7 availability for utilities, transportation and national security related systems.

Communications infrastructure providers are being pressured to enhance performance and improve security levels. Combine this with burgeoning infrastructure build-outs in a highly competitive race to capture new cellular and internet subscribers from an expanding geographic service area (see Figure 1). The need to be flexible in technology roll-outs and corresponding marketing incentives for new "triple play" and "quad play" bundles of voice, Internet, TV/video and wireless content services has completely changed the industry's leader board.

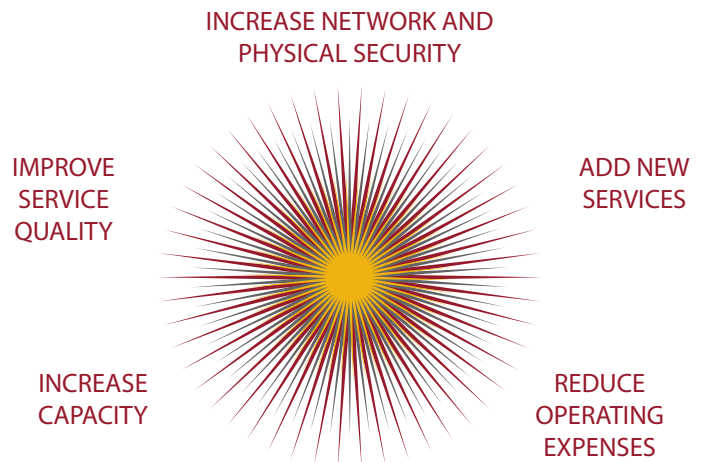


Figure 1: Challenges for remote sites

Unprecedented mergers and acquisitions among wireline, wireless, cable and satellite providers are producing a small set of key players. Traditional telecommunication providers are spending vast amounts of capital to build out fiber-to-the-home (FTTH) networks for high-speed broadband; wireless providers are evolving to deliver 3G and 4G networks for robust data and innovative new services; and cable and satellite providers are expanding their competitive high-speed internet services into areas such as voice-over-IP (VoIP).

Subscribers now demand better service or threaten to switch providers. Virtually all competitive barriers have been removed, leaving major players in a fight for the same communications market share.

The utilities and transportation industries are faced with similar infrastructure management issues, resource constraints, tight margins and competitive market forces. The relentless increase in sophistication of threats to oil and natural gas pipelines as well as major railroads (see Figure 2) has created a new category of infrastructure—critical transportation infrastructure. The United States alone maintains 120,000 thousand miles of railroads and two million miles of oil and gas pipelines. Remote infrastructure such as rail depots, stations, terminals, oil platforms, pipeline networks, pumping stations, power plants, and all types of control centers are being outfitted with new technology to enhance the performance and efficiency of their infrastructure. The U.S. Department of Energy has received international attention for its efforts in avoiding energy disruption and ensuring preparedness for attack. Significant research spending will find ways to reduce the vulnerability of control networks and increase “secure wireless communications,” since much of the existing Supervisory Control and Data Acquisition (SCADA) systems use wireless technologies.

With the consolidation and rapid introduction of new communication services and distributed facilities, and the increased security threats, this much is clear:

- Remote site technology is on a permanent growth path.
- The security and availability of these sites is paramount to the performance of the entire critical infrastructure.
- Outage costs rise quickly from several potential sources, including lost revenues, regulatory fines, service level agreement penalties, customer dissatisfaction, and public reputation resulting from media attention.
- Sites are interwoven with heterogeneous legacy and next-generation network equipment, power systems and environmental sensors from a multitude of vendors.
- Increased technical complexity is draining operations resources, especially at the most rural un-staffed locations.

CRITICAL INFRASTRUCTURE THREATS

NATURAL DISASTERS

Fires, Floods, Storms, Earthquakes

HUMAN CAUSED DISASTERS

HAZMAT spills, Major Traffic Crashes

SOCIAL, CRIMINAL and TERRORIST ACTIVITIES

Vandalism, Sabotage, Civil Unrest, Riots, Strikes, Attacks Using Chemical, Biological, Nuclear or Explosive Weapons

OTHER

Deferred Maintenance, Neglect, and Energy Material Shortages

Figure 2: Potential threats to critical infrastructure

- Financial budget constraints are increasing the number of sites per remote technician, in direct conflict with the demand for operational excellence.

Maintaining critical infrastructure at rural un-staffed locations, cell towers, small central offices, controlled environmental vaults (CEVs), huts, pumping stations, and oil platforms require significant labor expenditures. Limited connectivity options, mountainous terrain and inclement weather add to the challenge. For this reason, monitoring solutions are deployed at central network operations centers (NOCs) and master control stations. Because the personnel at these central locations maintain responsibility for the entire infrastructure, they generally monitor remote equipment only for critical failures. Ambiguous information often requires further troubleshooting by regional field technicians. Too often, costly physical site visits are the only option—in fact 80% of remote site problems today still require physical site visits.

The solution lies in a more efficient approach to complete, intelligent remote site management—one designed specifically to address the unique diagnostic, recovery and preventative maintenance activities of regional operations personnel and field technicians. This approach embraces the opposing market forces by improving operational efficiencies and freeing up resources to support new capacity expansion and service roll-outs. In fact, studies show that improved operations management using intelligent remote site monitoring solutions can eliminate up to 40% of site visits and can drastically reduce Mean Time to Repair (MTTR) resulting in reduced operational costs, better-than-ever network quality, and reduced churn.¹



REMOTE SITES: THE WEAKEST LINK

Remote infrastructure is experiencing explosive growth as communications, utilities and transportation operators bring better service and more resources closer to their customers. The personnel responsible for the daily security, upkeep, preventative maintenance, and evolution of technology has hardly risen. Remote site field technicians are over-taxed like never before—and the leveling off of site-to-technician ratios is nowhere in sight. Wireless mobile service providers report these ratios today range from 30 to 75 locations per technician (depending on geographic dispersion), compared with 5 to 15 sites just 5 or 6 years ago.

Remote field technicians need in-depth site intelligence. The latest IP networking and security technologies are being deployed as quickly as possible, but there are few “green field” infrastructures. New and old systems alike must be supported in a consistent way. Otherwise, technicians are blindly heading to locations to isolate

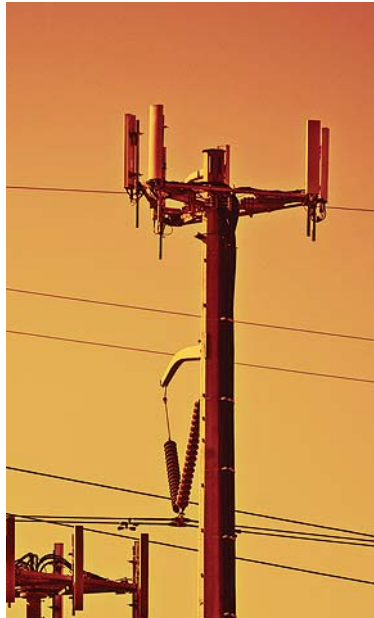
¹ Kentrox Inc. customer research statistics

problems perhaps lacking the correct parts or skill sets. Supplemental remote site systems—power, backup power, environmental sensors, access control and more—are just as critical to optimal infrastructure operations. If ignored, failures within these systems often can be even more damaging than core infrastructure failures. Management of these disparate systems from multiple equipment suppliers is complex. Newer ones are likely SNMP-based, but older telemetry systems use simple contact closures as good/bad indicators to provide limited, yet critical, information.

CHALLENGING DELAYS

The challenge with recovering from remote site failures is the race against time, and time is money. Let's break down the process to see where time and money are lost:

- If the NOC receives an alarm but cannot quickly identify or notify the most appropriate resource to fix the problem, time will be lost.
- Without remote diagnostic tools, problems cannot be prioritized. Every problem is assumed to be major. Hence, time is lost on the most critical problems.
- Travel time averages one hour to most remote sites and easily runs three hours or more in rural locations. Traffic and weather delays compound the issue. In cases such as microwave radios, multiple technicians are even sent to separate sites just to determine where the root cause problem is located.
- Once on site, valuable time is spent determining the actual problem. Is it a network equipment failure alone, or was the failure caused by an environmental problem, such as temperature or water? Was a door alarm caused by weather or an intruder?
- Depending on the diagnosis, the technician must determine if the problem can be repaired at the time of the initial dispatch or if third party assistance is necessary. The technician must also determine what equipment components or parts will need to be delivered to the site.



The bottom line is that dispatches are costly. Repair times are long and added travel, vehicle insurance and maintenance costs, unproductive technician “windshield time” and ever-increasing fuel costs add to the total cost. Considerable cost savings is possible if tools and expertise could be applied before a dispatch is ordered, or if problems could be fixed without a single dispatch.

REMOTE OPERATIONS: MORE THAN MEETS THE EYE

The optimal solution for eliminating operations management costs is using solutions designed specifically for the challenges of regional operations personnel. Fixed line and wireless mobile communications providers, as well as private operators of utilities, pipelines, railways and other transportation, are faced with securing and maintaining critical infrastructure at un-staffed locations. Providers have an unprecedented opportunity to improve operations and reallocate personnel from problem solving to top-line-growth initiatives. The end result is more reliable infrastructure and new, competitive services.

Complex problems require flexible solutions. Consider these business requirements:

- Eliminate costly dispatches—fix problems and collect maintenance statistics remotely.
- Improve quality of service—provide regional personnel access to more information firsthand, facilitating a correct diagnosis to identify where and what the problem is before dispatch. With this intelligence, the proper equipment is available, ensuring first call success, reducing repair cycles and increasing network and service availability.
- Reinstitute the discipline of preventative maintenance—automate tests.

- Facilitate regulatory adherence—automate reports and these operations management requirements
- Deliver information directly to the resources that need it. NOCs and master stations need it, but so do regional personnel—without losing critical minutes or hours.
- Inspect the problem remotely through all possible means. Although telemetry-based systems are not manageable through classic techniques such as SNMP, innovative protocol mediation can convert simple contact closures into a single stream of SNMP messages, consolidating them with those from a wide range of products. The more information that is forwarded to a management tool, the greater intelligence you will have before dispatching to the site.
- Consolidate remote equipment and facility management as much as possible onto one powerful platform. Point solutions can clutter space-constrained infrastructure and leave technicians with information that is as disparate as the systems themselves.
- Provide correlation to help technicians recognize root causes to complex problems. Equipment failures caused by power outage, or low tank levels caused by pipeline leakage are more easily detected through analysis of information that is provided through a single system.
- Fix problems remotely whenever available. Console port pass-through access to native devices at remote locations is an invaluable attribute of any remote management solution.
- Design products for extreme use, including environmental hardening.
- Create a flexible architecture with diverse connectivity to meet the needs of any place on Earth.
- Ensure complete physical and logical security into and out of the facility.
- Automate preventative maintenance checks and regulatory statistic reporting; store results for historical trend analysis.
- Maintain a consistent inventory record of disparate remote site equipment.

The promise, ultimately, is shorter MTTR, better service and lower costs through the following:

- Elimination of a significant number of site visits through remote management techniques
- Reduced time on site when a dispatch is required by being better informed and prepared with proper equipment

The challenge in managing the multitude of remote site technologies is illustrated here with just a sample of possible remote site equipment. Although no one infrastructure contains all of these, all utilize several of the same facility support systems. Just a few typical alarms that can be monitored remotely indicate:

- Tower light failure
- Power failure
- Low fuel level
- HVAC failure
- Water on floor
- High/low temperature
- Smoke or hazardous gas detection
- Failed changeover to backup power
- Intrusion (door/cabinet) detection
- Pipeline failure or corrosion leakage

Remote monitoring alone for these and other failure conditions can improve recovery times by diagnosing where the problem is and what equipment has failed. Even greater value is achieved with remote site access to devices for problem recovery. Figures 3 and 4 show real examples of alarm and event monitors, problem resolution activities, and preventative maintenance that can be performed remotely. The list is not exhaustive but illustrates the strength of remote management solutions. Specific capabilities that operators can expect will vary, depending on the site equipment as well as the capabilities of the management equipment selected.

THE REMOTE SITE: WHAT IT TAKES TO MANAGE IT

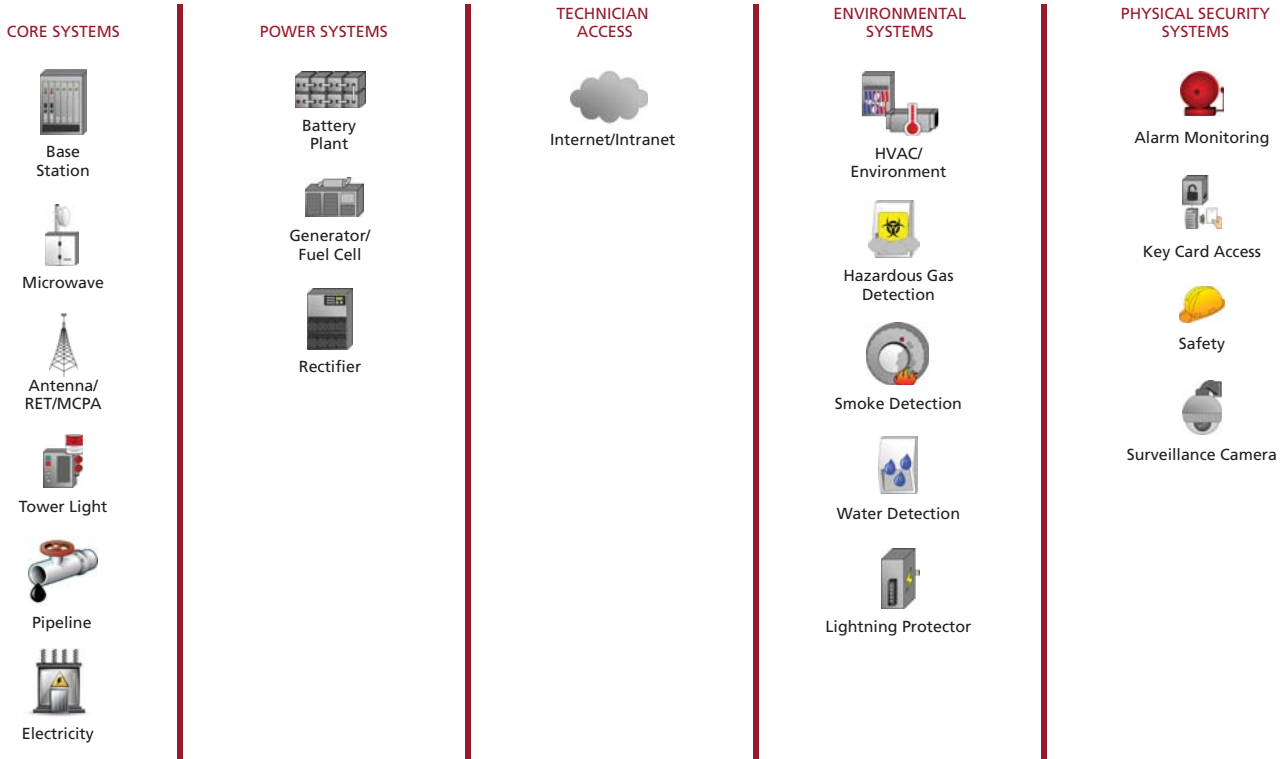


Figure 3: What needs to be managed at remote sites

CREATING A SOUND, FLEXIBLE ARCHITECTURE

A flexible architectural design paired with powerful products gives wireless network operators the ability to implement components on an as-needed basis.

Remote Device—The true workhorse of any wireless site management solution is a remote device that has a small footprint for space-constrained locations. It also:

- Consolidates bi-directional communications between the remote site devices and the operations center or technician supports a multitude of secure fixed line and wireless IP WAN technologies—fiber, T1, fractional T1, CDMA, GSM/GPRS/HSDPA, DSL, dial and more.
- Converts simple input/output contact closure alarms from remote site devices into intelligent messages in either TL-1, SNMP or other format.
- Translates legacy alarm and status collection protocols to simplify integration of Supervisory Management (SCADA) systems.

- Has been environmentally hardened to sustain extreme conditions.
- Is designed and certified for industry use, such as NEBS.
- Offers the necessary density to support diverse device connections.
- Provides a secure Ethernet port with network authentication so that dispatched technicians can access their corporate information to assist with on-site problem recovery.
- Can be customized to assimilate new and unique devices for a wide range of applications.

A robust appliance is best. Single-function devices may offer some similar capabilities, but they are often vendor-specific, vary in reporting capability, use more space and become additional points of failure.

	EQUIPMENT EXAMPLES	TYPICAL EVENT	REMOTE MANAGEMENT	PREVENTATIVE MAINTENANCE
NETWORKING	Router Switch Firewall Transmission device	SNMP MIB variables Hardware failures Performance capacity threshold exceeded Firewall attack	Device configuration or policy change and/or restoral Software patch loads Equipment reboot Diagnostic testing	Continuous collection of performance utilization for capacity planning Routine testing
TELECOM	Base Transceiver Station Channel bank Microwave radio Remote Electrical Tilt (RET) antenna	Equipment failure Circuit degradation/failure Service availability alarms Customer experience degradation	Console port access Control antenna tilt Access to multi-vendor applications typically only accessible locally	Routine network upgrades Continuous collection of performance statistics Continuous measurement of customer experience
PIPELINE CONTROL	Pump Valve Tank Leakage detection system	Tank level out-of-spec Leak detected	Change valve position Transfer pump speed control	Automatic flow measurement with daily reports Continuous measurement of tank levels with historical reports
FAA OBSTRUCTION	Tower lights	Light failure	Site visit to appear	Continuous automated check with stored results Quarterly (minimum) result report for FAA regulatory compliance
COMMERCIAL POWER	Rectifier Automatic transfer switch	Power failure Power switched from primary to back-up source Power restored to primary source Power switchover failure	Manual switchover Power on/off	Scheduled automated switch from primary to backup power Logging of commercial power outages for service level agreements with power provider
BACK-UP POWER	Battery plant Generator Fuel cells	Battery voltage high/low, temperature, discharge, out-of-tolerance Generator fuel level low Maximum generator run-time exceeded	Telcordia battery analysis: load, voltage, ambient temperature Battery and generator current run-time, estimated remaining run-time	Routine collection of battery cell and overall voltage Routine generator start/stop test Data storage and reporting for government safety and environmental regulations Routine audit of backup power capacity
ENVIRONMENTAL CONTROL	Temperature controller Heating, ventilation, air conditioning (HVAC) equipment Gas, smoke, water detector	Equipment failure Temperature high/low alarm Humidity alarm Gas, smoke, water detected	View/set temperature	Continuous trending of temperature and HVAC efficiency Regular reminders for HVAC filter changes Automated routine alarm-test procedures
ACCESS CONTROL	Surveillance camera Door entry/exit control system Window alarm relay Motion detector	Equipment failure Unauthorized entry/exit Motion sensed	Adjust pan-tilt-zoom camera Turn camera on/off Recording start/stop/storage	User account administration (changes/adds/deletes) Verify "passable" terrain prior to site visit

Figure 4: What needs to be managed at remote sites

Management Tools—The remote device’s capabilities are maximized when they are combined with a management tool that interprets the wealth of information forwarded from the remote site (see Figure 5). Alerting, control, security and reporting provide the integrity and intelligence that remote support personnel require, such as the following:

- Collects and correlates events from all devices onto single platform; correlation helps discern the difference in a temperature increase resulting from an HVAC failure versus an open door.
- Differentiates alarms indicating failure or compromised functionality from events and statistics that indicate “good” conditions and early warning signs; all messages are important, but some are more urgent.
- Manages the WAN security; both private and public infrastructures must prevent unauthorized access to remote site architecture; certification key administration between the management platform and the remote appliance provides a strong authentication mechanism.
- Provides authenticated pass-through control terminal access to remote site devices using TACACS+ and RADIUS RAS protocols and maintains user profiles defining command level access permissions and full RAS accounting support; even simple pass-through control is powerful if it can avoid a site visit.
- Supports detailed access level configurations to provide security for contract support staff so that only specific required functions are permitted while protecting access to other critical resources.
- Stores and displays inventory information for all equipment.
- Offers an intuitive user interface for navigating to each device without the need to memorize or look up IP addresses; access is provided via vendor-specific applications.

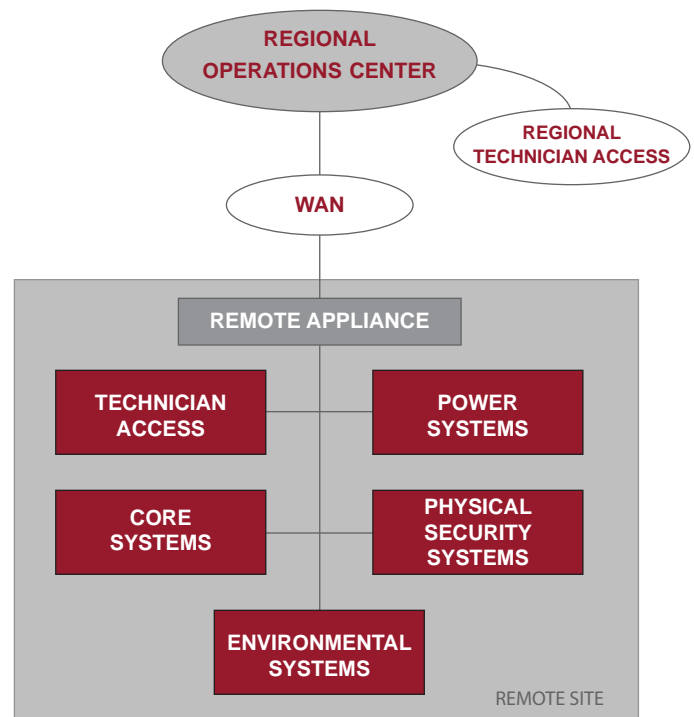


Figure 5: What a remote device should allow

- Facilitates reporting for internal tracking and measurement, as well as service level agreements (SLAs) and regulatory compliance.
- Uses client-server software so regional operations centers and technicians have secure remote management capability.

End-to-End Security and Flexibility—It sounds contradictory—security and flexibility, but for remote site management, they must work together. Features to look for include:

- Secure network connectivity into and out of the remote site. Firewalls, authentication and robust network security schemes should preclude unauthorized users from gaining access to the management tools, connecting to remote site equipment, accessing the corporate network from within the remote site, and tampering with the

management traffic being carried over the wide area network. Audit files of user access and functions performed should be inspected on a regular basis and retained for regulatory compliance.

- Physical site security through access control systems and surveillance techniques are critical. Monitoring these systems to ensure proper operation is an important piece of the solution.
- Flexible architecture with plug and play operation. Telemetry-based and IP-based systems can—and must—co-exist in a system that evolves to new technology over time. Every deployment has unique characteristics, either in the technology used or the operational process. Solution providers and their products must be able to assimilate quickly to the specific requirements of each customer. Innovative product designs and a keen understanding of the customer's operation are mandatory.

MORE THAN TECHNOLOGY

To this point, we have focused on the technology available to gain control of remote site infrastructure. While many companies strive for remote monitoring solutions, they

later discover that internal processes are established to support a centralized infrastructure management approach. Significant savings await those who augment the process of centralized NOC and master control station alarms and site visits with increased intelligence and automation at the regional level.

Technology can provide the tools, but the facilities, systems, and functions that comprise critical infrastructures are highly sophisticated and complex. They include human assets and physical systems that work together in a highly interdependent way. Adopting a complete remote site management strategy likely requires procedural changes as well. More information and control can be made available to regional operations centers and technicians from wherever they are located. Changing the “normal routine,” however, takes time and retraining technicians to use the tools that can make a proper diagnosis isn't always as easy as implementing the technology. Operators of critical infrastructure must be committed to constant improvement if they are to reap the rewards, and the suppliers of the solution need to be prepared to assist them with proper training at all levels of the organization.



TANGIBLE RESULTS: THE “INTELLIGENT DISPATCH”

The payback is tremendous: eliminating a significant percentage of physical dispatches, and increasing first-call success rates. In addition, measured customer results demonstrate that the right information prior to a site visit can reduce repair time by as much as 40%.

The time study results in Figure 6 show how the operational model can be changed with the addition of intelligent remote infrastructure management:

- **Travel**—By eliminating truck rolls (dispatches) for most problem diagnosis and preventative maintenance, plus a portion of problem recovery activities, travel time can be reduced by 40%.
- **Troubleshooting**—Tools and event correlation cut diagnostic time in half.
- **Preventative maintenance**—This one is debatable. As discussed earlier, some operators have stated that the important task of preventative maintenance has been neglected because problem management, new build-outs, and technology advancements take precedence.

Others say these tasks can consume as much as 40% of a technician’s time. Either way, automated maintenance routines such as system checks, backup power checks, disaster recovery testing, monitoring fuel levels and more can reduce the time spent on routine maintenance. Perhaps more beneficial is the gain in problem prevention. Even organizations that routinely perform preventative maintenance do so only annually at best, which rarely provides early detection of problems.

Automated routines provide more accurate information and are performed more frequently at no additional cost. In this study, the customer increased the level of preventative maintenance activity while simultaneously reducing the time spent by 30%.

The time gained from these activities helps by improving and expanding network availability. The activities which, as a result, are allocated more time contribute to top line revenue growth from service reach and higher customer satisfaction. They are:

Time Study of Remote Field Technicians Before/After Remote Site Management Solution

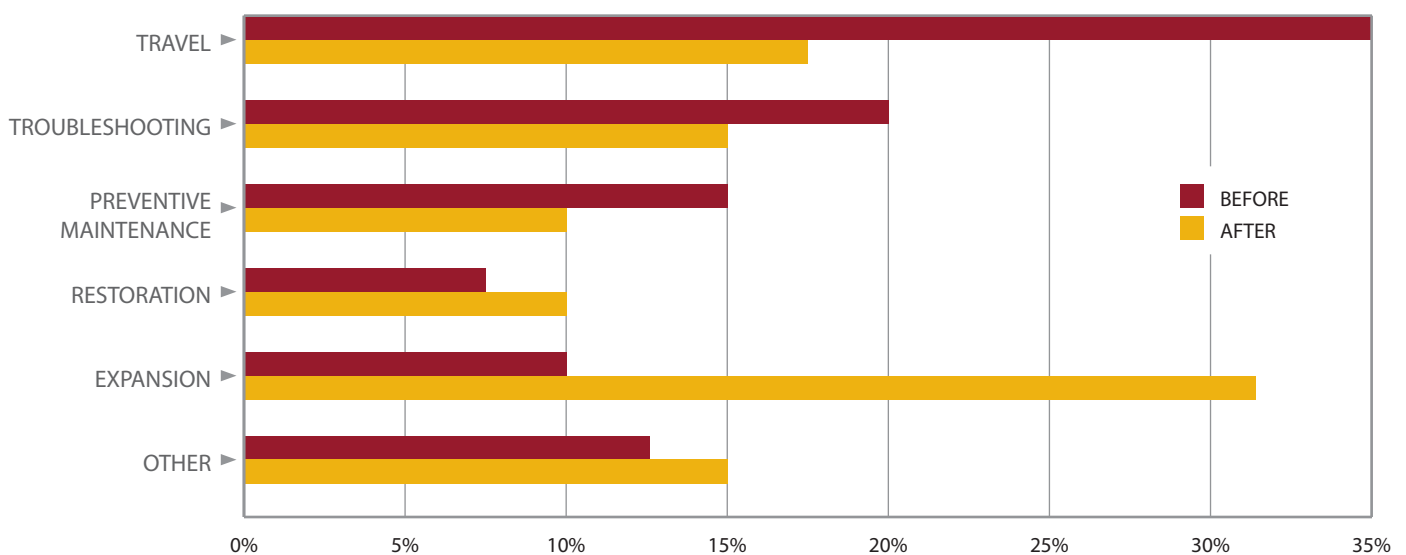


Figure 6: Results from implementing a site management solution

REMOTE SITE MANAGEMENT

Increase Network and Physical Security	Improve Service Quality	Increase Capacity	Add New Services	Reduce Operating Costs
Immediate remote intrusion alerts	Identify and correct problems before customers experience disruption	Network consolidation is eased	Organization free to focus more on revenue-generating activities, less on maintenance	Fewer truck rolls
Physical and logical authentication embedded into design	Higher availability	Able to proactively manage and monitor new network elements	Able to proactively manage and monitor new equipment required by new services	Lower MTTR
	Improved customer retention	Efficiencies are magnified as network grows		Faster upgrades
				More efficient use of labor

Figure 7: Benefits of a remote site management solution

- Problem restoration—While problem restoration is important in all cases, more time is allocated to solving minor problems before they become major.
- Service Expansion—The greatest buy-back of time is in capacity expansion, whether expanding the existing infrastructure to new geographic areas or rolling out new technology.
- Other—These additional tasks receive more focus:
 - Detailed equipment inventory records are maintained.
 - Software and configuration management procedures are followed—new patches are installed and maintenance test schedules are altered and optimized through automation.
 - Truck fleet maintenance activities can prevent costly en route failures.

The bottom line is an optimized operational process that maximizes highly-skilled field technicians, as well as operational efficiency and revenue potential (see Figure 7). Only when you have control of the infrastructure quality and security—and the associated costs—can effort be allocated to activities that sustain the long-term health and growth of the business.



www.kentrox.com

800-733-5511 or +1 614 798 2000

03-00-004 11/11 Copyright © 2011 by Kentrox, Inc. All Rights Reserved. Kentrox is a registered trademark of Kentrox, Inc. All product names are trademarks or registered trademarks of their respective owners. Information published here is current as of the date of publication, and is subject to change without notice. You may verify information by contacting company headquarters. Kentrox is an Equal Opportunity/Affirmative Action employer.