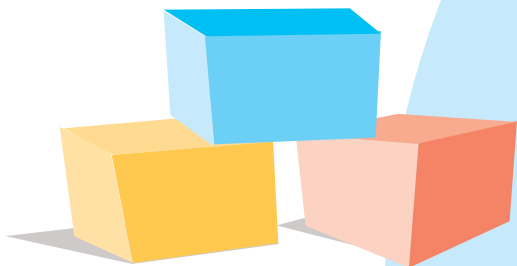


Network Alarm Monitoring Fundamentals

A solid introduction to alarm monitoring essentials:

- What equipment you must monitor
- How to design an alarm system to meet your current and future needs
- How to minimize transition costs



Version 1.6
Released March 15, 2006

www.dpstelecom.com · 1-800-622-3314

“We protect your network like your business depends on it”™

How This White Paper Will Help You

If you're just starting with network alarm monitoring, you probably have lots of questions. What equipment do you really need for an effective alarm system? How do you balance the need for network visibility against the need to reduce costs?

This White Paper will help you answer these questions for yourself. It covers how to analyze your network and determine your specific monitoring needs and create a system that fits your requirements and your budget.

Contents

Section I: Alarm Monitoring — Where Do You Start?	3
Learn Monitoring The Easy Way: Attend DPS Telecom Factory Training	3
DPS Telecom Remote Site Survey	4
Let DPS Help You Survey Your Network.	5
What RTU Features Do You Need?	6
This RTU Grows with Your Network.....	6
Section II: How Do You Monitor It?	7
3 RTUs to Fit Your Spec and Budget	7
If It Prints, You Can Monitor It.	8
RTU Choice: NetGuardian 832A	8
The Flexible RTU That Handles All Your Transports	9
Section III: How to Plan Your Alarm Monitoring Upgrade.	10
How DPS Telecom Can Help You	11

Section I: Alarm Monitoring — Where Do You Start?

You've just been put in charge of purchasing, selecting or recommending a new network alarm system for your company. Where do you start? What alarm equipment do you need? What monitoring features are essential, and which can you live without? How can you make sure your network is fully protected, without spending too much on equipment you won't use?

This White Paper is a quick guide to how you can answer these questions for yourself. This paper will NOT tell you, "Just buy this system and everything will be fine." Every network is different. A one-size-fits-all system won't provide the specific coverage you need and may cost more money than you really need to spend.

Instead, this White Paper will show you the right questions to ask. Before you can decide what alarm system to buy, you need to analyze your network and determine its specific monitoring needs. Figuring out what you really need your alarm system to do is your first step to designing a "perfect fit" system — one that's custom-designed for your network equipment, your available data transport ... and your budget, too.

The 3 Step Plan for Creating a Perfect Fit Alarm System

If you call DPS Telecom and ask what kind of alarm system you need, the DPS sales engineer won't make a

quick recommendation of "Buy this! Everyone has it. You should have it too!" Instead, your phone call starts a consultation in which your sales engineer will help you identify the network elements you need to monitor and the most effective way to monitor them.

This White Paper will take our through the same 3 steps as the DPS Telecom consultation process:

- 1. Survey where you are now:** What alarm monitoring do you currently use, if any? What equipment do you need to monitor? What data transport is available in your network?
- 2. Define your monitoring goals:** what would your ideal alarm system — the alarm system that does everything you need and want — look like? Do you need 24/7 pager and email notification? Do you want to integrate several different alarm systems onto one user interface?
- 3. Plan your alarm system upgrade:** How do you get from where you are now to where you want to be? Is upgrading at once feasible and within your budget, or should you phase your upgrade over several budget cycles? What alarm capabilities do you need right now, and which can wait?

Start Here: Network and Remote Site Survey

Your first step to get your alarm monitoring upgrade rolling is a complete survey of your current network and remote sites. This survey will document your existing alarm monitoring situation, in order to build a road map for your upgrade.



Learn Monitoring the Easy Way: Attend DPS Telecom Factory Training

"DPS Factory Training is a big help in not feeling intimidated by your network monitoring system. It's excellent — presented in the right way and tailored to the needs of the class."

— Bill Speck, 3 Rivers Telephone

Learn network alarm monitoring in-depth in a totally practical hands-on class. The DPS Telecom Factory Training Event will show you how to make your alarm monitoring easier and more effective. You'll learn SNMP alarm monitoring, ASCII alarm processing, Derived Alarms and Controls, and how to configure automatic email and pager notifications. DPS training is the easiest way to learn alarm monitoring, taught by technicians who have installed hundreds of successful alarm monitoring deployments

For dates and registration information, call 1-800-693-3314 today or go to www.dpstelecom.com/training.

In your site survey, you're looking for three things:

1. The equipment you need to monitor and the number of alarm points you'll need to monitor it.
2. The currently available data transport between your remote sites and your Network Operations Center (NOC) — the office where your alarm presentation master is located.
3. Any existing alarm collection and presentation equipment you already have. You may be able to save money by incorporating your existing alarm equipment into your new, upgraded alarm system.

(DPS Telecom offers a five-page Remote Site Survey template that will help you organize your network and remote site survey. See box: "DPS Telecom Remote Site Survey.")

Now let's look at what kind of network equipment you should be monitoring.

What Do You Need to Monitor?

It takes a lot of equipment working together correctly to keep your network running, and you need accurate information about every element involved.

That means monitoring not only your base telecom equipment, but also all the equipment that supports it and the environmental conditions that all your equipment requires to operate correctly.

The things you need to monitor fall into four categories:

- 1. Telecom and transport equipment: switches, routers, SONET equipment, fiber optic equipment, microwave radios, etc.**



Power supplies are some of the most critical equipment you need to monitor.

Don't settle for monitoring your revenue-generating equipment with simple summary alarms that just tell you whether the equipment is up or down. Ideally, you want a comprehensive series of alarms that identify problems down to the card level.

- 2. Power supplies: commercial AC power, battery plants, rectifiers, backup generators, UPS systems, etc.**

Monitor your power supplies as thoroughly as possible —

DPS Telecom Remote Site Survey

RTU Capacity and Function

1. How many remote sites do you need to monitor?
2. Do you want video surveillance at those sites?
3. Do you want a building access control system to manage entry to those sites?
4. How many alarm points do you need to monitor at each site?
5. How much growth, in sites and alarms at each site, do you anticipate over the next 5 years?
6. Do you need any analog inputs (e.g., voltage, temperature, humidity, signal strength)?
7. How many ASCII device (e.g., switches, routers, etc.) will you monitor at your remote sites?

Installation

1. How do you currently connect to your remote sites? (LAN, overhead, digital or analog circuit, terminal server, microwave?)
2. Do any of your sites support an alternate path communications link?
3. What type of power do you have at the master and remote sites? (-48 VDC, 110 VAC, other?)
4. How do you want to mount your RTUs? (23" rack, 19" rack, wall, tabletop?)
5. Who will install your RTUs?

This is just a small sample of the DPS Telecom Remote Site Survey. The full Remote Site Survey is a complete 5-page guide to evaluating your network alarm monitoring needs. For your copy of the Remote Site Survey, call DPS Telecom at **1-800-622-3314**.

power outages are the most common cause of remote site failures. Just as your power supply has multiple fail-safes and backup systems, every one of those backups should be monitored.

At the basic level, you must monitor commercial power availability and battery level. Getting more advanced, it's also a good idea to monitor rectifiers and generators, including whether the generators perform their regular self-start tests. If you want the earliest possible warning of any problem that might interrupt your power supply, monitor every link in the power supply chain, right down to the fuel levels in generator diesel tanks.

3. Building and facility alarms: intrusion, entry, open door, fire, smoke, flooding, etc.

It's vital to monitor the physical safety of the buildings that house your essential equipment. Since remote sites are usually unmanned and often in isolated locations, they're highly vulnerable to vandals and intruders. Accidents like short circuits and small electrical fires, even if they're small, can become disasters if you don't have any way to detect them and intervene in time.

Your facility monitoring should begin with at least monitoring open doors and fire alarms. For added security, you may want to consider integrating an electronic building access control system and video surveillance to your alarm system.

4. Environmental conditions: temperature, humidity, etc.

Most electronic equipment operates best within a defined range of temperature and humidity — monitoring these factors will give you early warning of potential problems.

You'll probably want to monitor different environmental conditions, depending on the physical location of the remote site. If the remote site is in a desert, humidity might not be a concern to you, but temperature probably will be. On the other hand, if your remote site has to function through an Iowa summer, humidity may be a major concern to you.

Another consideration is the sensitivity of your equipment. If it's rated to operate under extreme ranges of temperature and humidity, you won't have to monitor environmental factors quite so closely, but you'll still want to make sure the site stays within the range specified for your equipment.

If your remote site is an environmentally controlled facility, you have a different set of factors to worry about. You need to monitor the continued operation of the heating, ventilation and air conditioning (HVAC) equipment that

Let DPS Help You Survey Your Network — A Free Consultation at No Obligation to You

Determining your alarm monitoring needs can be tough. If you've got a busy job with lots of responsibilities, you don't have a lot of time to evaluate alarm systems and survey your remote sites.



Rick Dodd
Director of Sales
DPS Telecom

So why not get help from experts you can trust? DPS Telecom will help you survey your remote sites step-by-step, making sure you don't miss any opportunities to make your network monitoring simpler, more effective — and easier on your budget.

"We're not your typical sales department," says Rick Dodd, DPS Telecom Director of Sales. "We're design consultants, and a lot of the time we propose solutions that have a smaller sales volume, if it's the right solution for the client."

A DPS expert consultant can help your figure out what alarm system will most effectively meet your needs without overloading your budget. Our goal is to help you maximize your return on investment while minimizing your expenditure — without pressuring you to buy a particular system.

There's no hard-sell sales tactics. No harassing sales calls. No pressure to buy. You won't get any equipment recommendations until we've helped you plan the right monitoring strategy for your network.

maintains the facility environment, plus you must be sure to monitor the power supply to the HVAC system. On top of that, you should still monitor temperature and humidity, as another safety check to make sure the HVAC is doing its job.

General Principles for Selecting What to Monitor

In the perfect alarm system of your dreams, you'll have an alarm for every single factor that can affect network operations, but you'll never spend extra money on alarm capacity you don't need. In the real world, time and budget constraints usually mean you have to set priorities and carefully select which alarms you're going to monitor.

When you're choosing network elements to monitor, keep these three principles in mind:

1. Paranoia is your friend. Think about everything that can possibly go wrong, because — guaranteed — someday it will.
2. The more detailed your monitoring, the smaller your windshield time and repair costs. Precise diagnostics help you send the right tech with the right tools on the first site visit.
3. It's OK to start small and scale up. If you get an alarm system that can be upgraded, you can start monitoring your most critical network elements now, and gradually add more monitoring over several budget cycles.
4. Plan for your needs for the next five years. Your network

What RTU Features Do You Need?

How do you find the right RTU? Here's 5 essential features to look for ...

1. **Discrete alarms:** Monitor device failures, intrusion alarms, beacons, and flood and fire detectors.
2. **Analog alarm inputs:** Monitor voltage, temperature, humidity and pressure.
3. **Ping alarms:** Detect IP device failures and offlines .
4. **Control relays:** Operate remote site equipment directly from your NOC.
5. **Terminal server functions:** Control switches and other gear remotely via Telnet over LAN.

DPS Telecom offers RTUs that meet all these requirements — and offer local visibility via Web browser, email and pager notification, and more.

For more information about DPS RTUs, see us on the Web at www.dpstelecom.com/rtus.

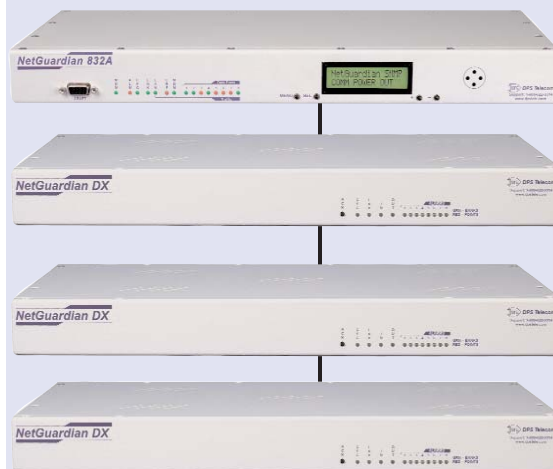
This RTU Grows with Your Network

When you're planning your alarm monitoring, think about the future. You don't want to get locked into an alarm system that's inadequate for your future needs — but you don't want to spend too much for alarm capacity you won't immediately use, either.

The NetGuardian 832A remote telemetry unit expands its capacity as your needs change. Install a NetGuardian at your remote site now, and get exactly the right coverage for your current needs.

Then, as your remote site grows, you can extend your alarm monitoring capabilities by adding NetGuardian DX Expansion units. Each NetGuardian DX adds 48 more alarm points, and you can daisy-chain up to three NetGuardian DXs off each NetGuardian 832A base unit.

Unit	Capacity
Base NG 832	32
1 DX	80
2 DX	128
3 DX	176



and your monitoring needs will grow, and an alarm system that can't grow with them will be obsolete as soon as it's installed.

Section II: How Do You Monitor It?

Now that you have an idea of what you should be monitoring, your next consideration is the nuts and bolts of how you are going to monitor it.

There are three phases to alarm monitoring: acquisition, transport and presentation. Let's look at each phase in order.

Acquisition: Getting Alarms Out of Your Equipment

There are three kinds of alarm inputs: contact closures, analog inputs and protocol inputs.

Contact Closures

Contact closures are also called discrete alarms or digital inputs. A contact closure is a simple on/off switch that produces an electrical impulse when it's activated or deactivated. Contact closures are the simplest kind of alarm input, so they're often used as a kind of lowest-common-denominator means of getting some kind of alarm from any kind of equipment.

Analog Inputs

Analog inputs accept current or voltage level inputs over a continuous range. They're the ideal kind of alarm for monitoring things like temperature and battery charge, where it's important to get an actual, physical measurement of the condition in real time.

Here's where having a quality alarm system really counts. Some alarm systems simulate analog alarms with "threshold" alarms. For example, you might get a low-battery alarm if the battery voltage drops to -48 volts. But that information by itself is meaningless. After the voltage crosses the -48-volt threshold, does it stay there (indicating that the battery is merely low) or does it continue to drop (indicating that the battery is being rapidly drained)? With threshold alarms, you have no way to tell.

DPS Telecom alarm equipment features analog alarms that report live, real-time analog values, giving you true visibility of these kinds of alarm conditions. Additionally, DPS analog alarms support four user-configurable thresholds (Major Under, Minor Under, Minor Over and Major Over), to provide best-quality notification of changing events.

Protocol Inputs

Protocol inputs are electrical signals formatted into a formal code that can represent much more complex information than contact closures or analogs. There's a wide variety of protocols for transmitting telecom alarm data. The most common

3 RTUs to Fit Your Spec and Budget

The NetGuardian RTU family scales to fit your needs ...



Full-featured NetGuardian 832A:

- 32 discretes, 32 pings, 8 analogs and 8 controls
- 8 terminal server serial ports
- NEBS Level 3 certified
- For SNMP, TL1 or T/Mon NOC
- Dial-up backup
- Web browser interface
- Pager and email notification
- Dual -48 VDC, -24 VDC or 110 AC
- 1 RU for 19" or 23" rack

Heavy-duty NetGuardian 480



- 80 discretes, 4 controls
- For SNMP, TL1 or T/Mon NOC
- Dual -48 VDC
- 1 RU for 19" or 23" rack



Economical NetGuardian 216

- 16 discretes, 2 analogs, 2 controls
- 1 terminal server serial port
- For SNMP, TL1 or T/Mon NOC
- Single or dual -48VDC or 110 VAC
- 1 RU for 19" or 23" rack

telemetry protocols are open standards like SNMP, TL1, ASCII and TBOS, but there are also manufacturer-specific proprietary protocols. SNMP, TL1 and ASCII are simply ways of encoding ordinary written text for electronic transmission; these protocols are human-readable, if you know the code's terminology and operators.

Acquiring Alarm Data from Telecom and Transport Equipment

Unfortunately, there's no standard alarm output for switches, routers, SONET equipment and other telecom and transport gear. You'll have to check each type of transport equipment in your network to see what kind of alarms it supports.

The best way to find out what kind of alarming your equipment can do is to check the documentation supplied by the manufacturer. The documentation should have at least a short section describing the equipment's alarm outputs.

Ideally, your equipment will support some kind of protocol interface, giving you detailed visibility of its internal operations. But your equipment may only support contact closure outputs, which — depending on how many contact closures it has — may only give you a handful of summary alarms.

However, if your equipment doesn't have a documented protocol output, check it for a printer port, a report-only printer (ROP) port or a craft port. This port is designed to output a detailed log of equipment activity in the form of an ASCII text stream.

Historically, this ASCII output port was originally intended to connect to a printer for producing activity log printouts. A printout is a great way to keep a detailed record of what has happened in the past, but it's not a good way to monitor what's happening right now.

If It Prints, You Can Monitor It

Why is ASCII alarm processing so great? First, it's a simple way to get useful information from nearly any transport gear. If it prints, you can monitor it. Second ... how many times have you been woken up by an alarm page at 3 A.M.? Wouldn't you like to know if you really have to go to the remote site — or if you can safely go back to bed?

ASCII alarms give you detailed reports on the condition of your equipment, isolating problems right down to the level of what shelf and what card need repairs.

T/Mon NOC Makes ASCII Usable

T/Mon NOC's ASCII Alarm Processor Software Module scans ASCII text for alarm messages and converts them to standard T/Mon alarms.

Once an ASCII alarm is acquired, you can use it with any of T/Mon's advanced features: automatic pager and email notification, automatic alarm correction responses and more.

RTU Choice: NetGuardian 832A



The **NetGuardian 832A** is a full-featured remote telemetry unit. The NetGuardian supports **32 discrete alarms, 32 ping alarms, 8 analog inputs, 8 controls, and 8 serial reach-through ports**. The optional NetGuardian Expansion Unit can expand the NetGuardian's discrete alarm capacity to **80, 128 or 176 discrete alarms**. The NetGuardian reports to T/Mon NOC or to multiple SNMP managers — or you can use the NetGuardian's built-in Web Browser Interface and email alarm notification to monitor your remote site without a master.

For more information, check out the NetGuardian on the Web at www.dpstelecom.com/netguardian.

However, T/Mon provides a way to turn that ASCII stream into actionable, real-time alarm data. T/Mon's optional ASCII Processor Software Module can automatically capture ASCII text, extract important information from the text stream, and convert the text to a standard T/Mon alarm notification.

Acquiring Power, Facility and Environmental Alarms

Power, facility and environmental alarms are collected by groups of individual sensors connected to site equipment like battery plants, generators, doors, temperature sensors and so on.

Outputs from these sensors are in turn connected to a remote telemetry unit (RTU) that converts contact closure and analog inputs into a protocol output, which is forwarded to your alarm presentation master.

Every model of RTU has a defined capacity of how many contact closure and analog inputs it supports. The alarm capacity of your RTU is the limiting factor for how much alarm information you can acquire from your remote site. You don't want an RTU that has too little alarm capacity, because that will give you only vague and incomplete information about the state of the remote site. On the other hand, you don't want to pay for unneeded alarm capacity, either.

Your remote site survey will help you determine the correct alarm capacity for each type of remote site in your network. It's also a good idea to look for an RTU whose alarm capacity can be easily upgraded. An RTU with expansion capability will grow with your remote site without your having to buy entirely new equipment.

Transport: Getting Your Alarms from the Site to Your Screen

Once alarm data collected at your remote sites, it needs to be transmitted over a data network to your alarm presentation master at your NOC. Alarm data can be sent over nearly any kind of data transport: Ethernet LAN/WAN, dial-up modem, dedicated circuit, overhead channel, etc.

There are two things you should keep in mind about alarm data transport:

1. As much as possible, you want to work with transports that are already available in your network. You don't want to create added expenses by committing yourself to installing new network infrastructure. It's best to choose an alarm system that is compatible with the transports you already have.
2. It's a good idea to have a secondary backup path for your alarm data in case your primary path fails. No

The Flexible RTU that Handles all your Transports

With the NetGuardian 832A, multiple transports are no problem. This flexible RTU supports three kinds of transport: LAN, dial-up and optional serial connection for 202 modem, FSK modem, or RS-232. The NetGuardian can work with whatever transport is available at your remote sites.

Networks that are in transition aren't a problem for the NetGuardian either. The NetGuardian supports LAN, dial-up and serial connections simultaneously. So as your network upgrades from legacy transports to LAN, you can use the same NetGuardian units at all your sites.

What can the NetGuardian do for you?

- You can use one RTU at all your remote sites, no matter what transport is available.
- You don't have to install new transport to collect alarms.
- As your network changes, you don't have to buy new remotes for new transports.
- You only have to maintain one set of spare units and spare parts for your entire network, for great cost savings and convenience.
- All your alarms are in one common format. You don't have to use a confusion of multiple consoles and multiple screens to monitor all your remote sites.

Because of its multiple transport capability, the NetGuardian also supports applications for bridging across multiple transports, and even strategies for protocol mediation and replacing legacy monitoring equipment.

transport is 100% reliable, and you don't want to lose alarm visibility of your revenue-generating network under any circumstances.

Presentation: Displaying Your Alarms in an Actionable Format

The final phase in alarm monitoring is presenting the alarm data in a useful way so that a human being can read the information and use it to direct repairs. This is done through a specialized computer called an alarm presentation master. The master collects the alarm reports from RTUs at the remote site and then format, sorts and displays the information for a human operator.

The master is really the most important part of the entire alarm system. For the NOC technicians who monitor alarms and dispatch repairs, the master IS the alarm system — it's the only window they have to see what's going on in the network. The features and capabilities of your alarm master directly control how much useful information your NOC techs can see. A high-quality, full-featured alarm master gives you the tools to substantially lowers your network maintenance costs.

7 Critical Features for Alarm Monitoring Masters

Here's a list of 7 critical features that your alarm master should have:

1. Protocol mediation and multiprotocol support:

You probably have several different types of transport equipment to monitor, and you may have several generations of legacy alarm monitoring equipment as well. All these different types of equipment report alarms using different incompatible protocols.

You definitely want to have one alarm master that can support all the monitoring protocols your equipment uses and display all your alarms on one screen. Trying to monitor by watching two or more screens is hard work that confuses even the best system operators, and sooner or later someone will miss a major alarm.

2. 24/7 unmanned monitoring via pager and email notification:

Some companies can afford to pay staff to watch a monitoring screen 24 hours a day, seven days a week, including weekends and holidays. Your company probably isn't one of them. But you don't need a 24/7 staff if your alarm mas-

ter can automatically send alarm notifications to on-call technicians via pager and email.

3. Detailed alarm descriptions: Some alarm masters display alarms as cryptic numeric codes. You want a system that displays alarms in plain English, with a complete description of what the problem is and what action you should take to correct it.

4. Alarm sorting and categorizing: If your alarm system just shows you one long list of alarms from your entire network, it's easy to lose track of critical information. A quality alarm system can sort and categorize your alarms several different ways, by severity, remote site, equipment type or other criteria you define.

5. Separate Standing Alarm and Change of State (COS) Alarm lists:

A Standing Alarm list displays all alarms that are currently uncorrected. A Change of State (COS) Alarm list displays all new events that happen in your network, including alarm points that go into an alarm state and alarm points that are cleared. If your alarm master supports both kinds of view, you have the quickest and most accurate picture of your network's current status.

6. Nuisance alarm filtering: Your equipment might generate a lot of alarms that are merely status reports that require no corrective action. These are nuisance alarms, and they're more dangerous than you might think. Nuisance alarms desensitize your monitoring staff to alarm reports, and they start to believe that all alarms are nonessential alarms. Eventually they stop responding even to critical alarms. Look for an alarm system with tools to filter out nuisance alarms.

7. Expansion capability: An alarm system is a long-term investment that will last for as long as 10 to 15 years. So you need an alarm system that will support your future growth for up to 15 years. In that time your network is going to grow in size, you're going to add new kinds of equipment, and you're going to need new alarm monitoring capabilities. Make sure your alarm master can grow and change with your network.

Section III: How to Plan Your Alarm Monitoring Upgrade

In the previous sections, you've seen what equipment you should monitor and what features a good alarm

system should have. So you should have some sense of what would be the ideal alarm system that will give you the best possible visibility of your network.

The question is, how do you get from where you are to where you want to be? It's very rare for a company to be able to suddenly leap from their current alarm monitoring to their ideal system. Budget restrictions and the cost of installing equipment mean you can't usually get everything you want in one budget year.

Here are some strategies that will help you find a smooth, gradual upgrade path that will let you transition to a new alarm system over several budget cycles:

- **Define your immediate monitoring needs:** What are the essential alarm monitoring capabilities that you must have today? What critical equipment do you absolutely have to monitor right now?

Keep in mind, your definition of an immediate, essential need might be different than someone else's. For example, if you have the staff to keep an eye on an alarm screen 24/7, you might not need pager notification. But if you need to manage critical network assets during unmanned after-hours and weekend times, paging is an essential capability.

- **Start slow, then expand:** Once you've taken care of your bare minimum needs, you can add more alarm capacity and more monitoring capabilities over several budget cycles. You don't have to spend more than you can afford in one budget year, but you'll gradually move toward your ideal system.
- **Use protocol mediation to incorporate existing equipment:** The first stages of your upgrade can be easier and more cost-effective if you can install a new alarm master first and then gradually replace RTUs at your remote sites. An alarm master with multiprotocol support can support your existing remotes, so you can immediately add new presentation capabilities without replacing all your remote site equipment.
- **Keep your future goals in mind:** While you're planning your expansion, think about what your monitoring needs are likely to be 5, 10, 15 years down the road. It's easier and more cost-effective to add alarm capacity in a controlled way in the immediate future than to rush a new deployment through when you've exceeded your alarm capacity.

How DPS Telecom Can Help You

Building the right alarm system for your network isn't simple. It's easy to spend more than you need ... but there are also opportunities to save money and improve operational efficiency that you don't want to miss. It's hard to learn everything you need to know and still do your everyday job.

DPS Telecom can help you plan your upgrade migration path, with expert consultation, training and information resources. DPS alarm equipment is built with the expansion and migration capabilities you need to make a graceful transition from your existing system. And DPS is committed to helping you get the best alarm system for your specific needs.

DPS Telecom Guarantees Success — or Your Money Back

You're never taking any risk when you work with DPS Telecom. Your DPS alarm system is backed by a **30-day, no-risk, money-back guarantee**. Test your new system at your site for 30 days. If you're dissatisfied for any reason, just send it back for a full refund. We don't want your money unless you're completely satisfied. It's that simple.

What to Do Next

Call or email Rick Dodd at **1-800-622-3314** or rdodd@dpstele.com and ask for a free consultation on your alarm monitoring needs. Rick will be happy to help you define your specific requirements and answer any questions you have.

There's no obligation to buy. You won't be bothered by high-pressure salesmen. You'll just get straightforward information to help you make the best decision about your alarm monitoring.

Alarm Monitoring Solutions from DPS Telecom

Alarm Monitoring Masters



T/Mon NOC: Full-featured alarm master for up to 1 million alarm points. Features support for 25 protocols, protocol mediation, alarm forwarding, pager and e-mail alarm notification, Web Browser access, multi-user access, standing alarm list, alarm history logging.



T/Mon SLIM: Light capacity regional alarm master. Supports up to 64 devices and 7,500 alarm points. Features pager and email alarm notification, Web Browser access, standing alarm list and alarm history logging.

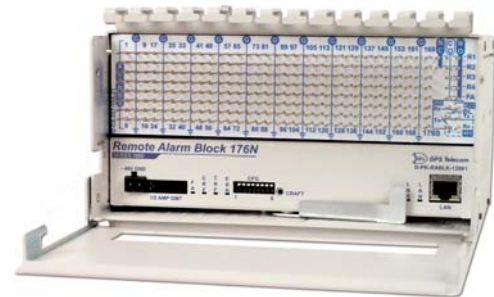
Remote Telemetry Units



NetGuardian 832A: RTU monitors 32 alarm points, 8 analog inputs, 8 control relays, 32 ping targets, 8 terminal server ports; reports to any SNMP manager, T/Mon NOC or T/Mon SLIM



NetGuardian 216: RTU monitors 16 alarm points, 2 analog inputs, 2 control relays, 1 terminal server port; reports to any SNMP manager, T/Mon NOC or T/Mon SLIM



Remote Alarm Block 176N: Wire-wrap alarm block monitors 176 alarm points, 4 controls; reports to any SNMP manager, T/Mon NOC or T/Mon SLIM



NetGuardian 480: RTU monitors 80 alarm points, 4 control relays; reports to any SNMP manager, TL1 master, T/Mon NOC or T/Mon SLIM

www.dpstelecom.com
1-800-622-3314



"We protect your network like your business depends on it"