Integrated Monitoring of a Critical Communication Network

TASC Systems White Paper

Historically, monitoring of critical communication networks have been implemented in a piecemeal manner, with each element monitored by a manufacturer-specific method. Attempts to integrate monitoring to a central location have been hampered by protocol and implementation differences. TASC System's siteVIEW APEX software overcomes these barriers by implementing the networking standard Simple Network Management Protocol (SNMP) for Internet Protocol (IP) capable elements and a multi-protocol approach for other network devices. siteVIEW APEX's holistic and domain-specific integration of nodes in to a singular view, offers network operators an unparalleled method of maintaining and optimizing their infrastructure.

by **Ted Singh**
Software Systems Manager

V1.00 – October 2014

Table of Contents

Introduction

A (mission) critical communication network is used to "*describe the networks specifically designed for public safety teams (e.g. police, fire and rescue, and the ambulance service) to guarantee robust, fail-safe, and secure voice and data communications*"[1]. In public safety applications, these networks are implemented as Land Mobile Radio (LMR) systems, which are "*wireless communications system intended for use by terrestrial users in vehicles (mobiles) or on foot (portables). Such systems are used by emergency first responder organizations, public works organizations, or companies with large vehicle fleets or numerous field staff. Such a system can be independent, but often can be connected to other (…) systems such as public switched telephone network (PSTN), cellular networks*"[2] or other IP networks. **By definition, critical communication networks need to be monitored to ensure maximum uptime and effectiveness.**

These systems are made up of a set of radio transmission sites and, and depending on the end-user's jurisdiction, may cover a wide geographic area, some with very remote access. Within each site is a set of network elements provided by many original equipment manufacturers (OEMs). In addition to the network elements necessary for communication, ancillary equipment (for example, power supplies) and a diverse collection of sensors constitute the complete network location.

Historically, operators have used manufacturer-specific solutions to monitor RF equipment and augment management of other equipment and sensors through remote terminal units (RTUs). This fragmented approach resulted in an inconsistent monitoring and trouble-shooting process, reducing operational effectiveness and network uptime.

Fortunately, the adoption of IP standards has opened a path to an integrated strategy for monitoring of the network. Using the Simple Network Management Protocol (SNMP) and a multi-protocol approach, software solutions like TASC System's siteVIEW APEX provide a holistic solution to critical communication network monitoring.

The purpose of this document is to 1) understand why communication networks need to be monitored, 2) review the history of critical communication network monitoring, 3) explore what can and should be monitored, 4) demonstrate how siteVIEW APEX enables a unified monitoring strategy and finally, 5) highlight siteVIEW APEX's operational and trouble-shooting tools.

[1] Mission Critical Communications definition, http://www.motorolasolutions.com/web/Business/B2B_Internationalization_Patni/_Documents/Brochures/_Static%20Files/Evolution_of_Critical_Communications_Guide.pdf?pLibItem=1, September 2014
[2] Land Mobile Radio system definition, http://en.wikipedia.org/wiki/Land_mobile_radio_system, September 2014

The Rationale for Monitoring Communication Systems

Within the industries that they are deployed, communication systems may be deemed mission critical because of the functionality they provide. Two primary purposes define the essentialness of a critical communication system:

- **Safety Critical** – a significant domain in which LMR communication systems are used is within the public safety sector: Police, Ambulatory, and Fire and Rescue. But even within other sectors – like Mining, Forestry, Transportation – communication is an essential service in dealing with human safety. When dealing with hazardous situations or environments, the communication network is a key tool for avoiding loss of life.
- **Business Critical** – many companies depend on communication systems to connect their remote work force. Better information and timely decisions can play a critical role in the economic health of an organization. Conversely, failure to receive feedback from the field may lead to operational failure.

For these reasons, the communication system must be available at all times; downtime can be catastrophic.

To support the critical nature of the communication system, a monitoring solution provides the following benefits:

- **System Operational Status** – a monitoring solution provides a portal into the operational status of the network. System health and performance can be reviewed in real-time and operators can be notified of any exceptions to these parameters. Correcting network faults before they become service failures is a must – discovering that the network is down when a field worker requests a communication lifeline can lead to disastrous results.
- **System Optimization and Maintenance** – with an integrated view of the system's operation, configuration of the network can be adjusted to tune the system's performance. Additionally, key parameters can be watched – and if required, trended – to plan the preventative maintenance of the network.
- **Network Trouble-Shooting and Recovery** – in the case of network failure, a monitoring solution will have a log of operational history to review. Forensic analysis on this information can assist in tracing the root cause of failures.
- **Enterprise Integration** – information technology (IT) integration continues to be a major driver in improving organizational effectiveness. Often a monitoring solution provides the machine-to-machine (M2M) connectivity between the enterprise and field operations.

History

Before IP Standards

For significant, high-value equipment, Original Equipment Manufacturers (OEMs) provided their own solutions - typically software - to manage their device. Each manufacturer's monitoring solution was implemented differently, some as configurable input/output (I/O) signals, some as command line utilities, and some as graphical-user interfaces. Often these solutions were only available at the equipment's location, and not remotely accessible to a centralized network operations center, which could present a problem if the equipment was located at a hard to reach remote site. Furthermore, many OEMs did not treat these monitoring solutions as a top-end engineering concern – resulting in limited access to key data and poor software implementations.

For smaller, lower-value equipment and sensors, there usually wasn't any OEM monitoring solution. Fortunately, third-party vendors stepped in to provide RTUs with local I/O connections and a radio backhaul for sending collected information back to a monitoring center. For example, the TASC Systems siteRSM platform has digital, analog and temperature inputs and features multiple radio network backhaul options to report critical events to a centralized Network Management Solution (NMS).

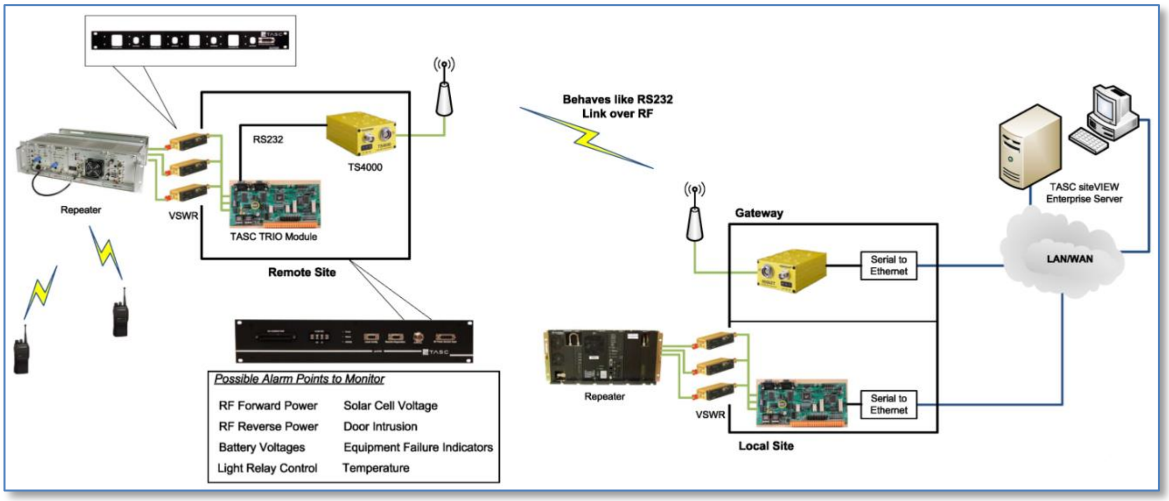


Figure 1 – Pre-IP Solution for Critical Communication System Monitoring

Yet another complexity preventing full network monitoring was the "backhaul" method, or the communication path responsible for "*transporting (communication) traffic between distributed sites (to) more centralized points of presence*"[3]. For many non-urban networks, interconnecting wireline is not a viable option, so alternate backhaul paths are required. Since most of the radio traffic was primarily being used for communications, any permitted data transmission was low-bandwidth and required specialized data serialization software or hardware.

[3] Backhaul definition, http://en.wikipedia.org/wiki/Backhaul, September 2014

This fragmentation, lack of interoperability and a limited backhaul path resulted in an inconsistent and patch-work network management strategy. Operators had the difficult task of switching between different methods of monitoring and, potentially, physically travelling to different locations, to trouble-shoot network issues. Delays in trouble-shooting meant network downtime.

IP Standardization

The wide scale adoption of the IP represents a quantum leap in network management in two respects: first, SNMP has provided a consistent method of reporting events and configuring parameters within equipment, and second, it has provided a standardized method of backhauling this information to a centralized NMS.

SNMP

In the 1980's, to help solve the problems related to the complex task of managing a highly distributed, multi-vendor IP networks, the Internet Engineering Task Force (IETF) worked to define a protocol called Simple Network Management Protocol (SNMP). SNMP consists of a "*set of standards for network management, including an application level protocol, a database schema, and a set of objects*"[4]. Or in plain English: the IETF documented the way equipment should report data, including a way to find out what data was available and how it was organized within the equipment.

The first revision of the standard, SNMP v1, provided definitions for the structure of the information within the equipment (RFC 1065), the dictionary file which defines what information is available (RFC 1066) and the protocol used to transport the information (RFC 1067). So, in SNMP parlance, a *SNMP Manager* communicates with a set of *SNMP Agents* (information providers or, in our case, radio equipment). Both the Manager and Agent use a common database structure, as defined within a *Management Information Base (MIB)* file, which outlines the list of objects that they can exchange.

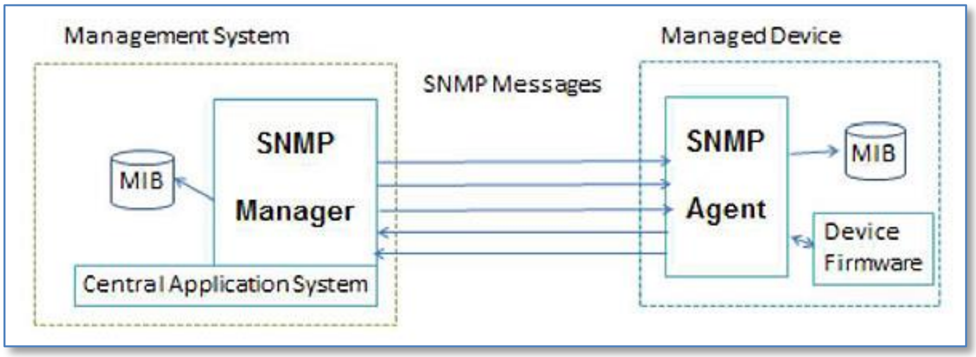


Figure 2 - High-Level SNMP System Diagram [5]

[4] SNMP definition, http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol, September 2014
[5] SNMP system diagram, http://www.pcb.its.dot.gov/standardstraining/mod19/sup/m19sup.htm, September 2014

There have been two subsequent revisions to the SNMP standard. SNMP v2 added several improvements, most notably related to getting bulk data from the equipment, instead of one item at a time. SNMP v3 solved issues related to security and administration.

SNMP has been designed as non-invasive and light weight, ensuring that the equipment's main operation remains unaffected. The NMS is responsible for retrieving, processing and determining what do with the data. Another advantage of the standard is that it gives a way to hierarchically organize all the data parameters within a machine and then reference each parameter via a Unique Identifier (OID). To avoid extraneous network transmission, SNMP can be set up to only report data when a parameter or set of parameters are out of range. These reports, called "traps", are unsolicited events which are reported to the NMS directly.

Because of these benefits, adoption of SNMP in general IP network infrastructure is already ubiquitous. Adoption in the critical communication radio network industry domain has lagged behind until the last few years. OEMs have begun to assign their engineering resources to implement SNMP within their equipment and sensors, driven by the wide acceptance of IP-networks and the business consolidation of radio and IT networking groups at the end-user.

IP Backhaul

Before large scale deployment and integration of IP-based networks, SNMP was not a monitoring option for the critical communication industry. If centralized monitoring was implemented at all, the health data of equipment at remote sites needed to be "backhauled" over the existing radio infrastructure or leased circuits – typically, over Plain Old Telephone Service (POTS) – as concise radio data. To accomplish this, companies, like TASC Systems, developed highly efficient protocols for sending siteRSM (RTU) events via serialized data messages over radio or modem technology to their TASC siteVIEW v2 software, where network data was aggregated for further analysis.

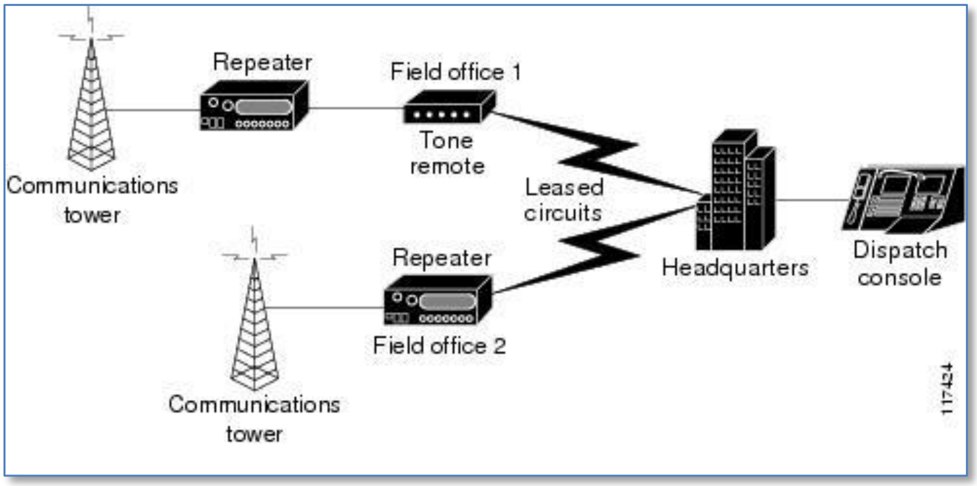


Figure 3 - Monitoring Data over POTS Leased Line[6]

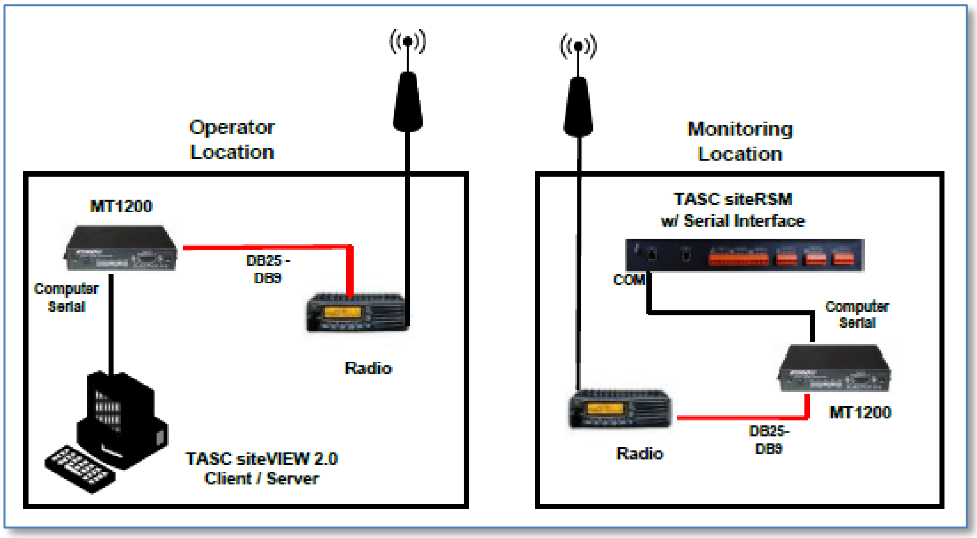


Figure 4 - Monitoring Data over Radio Example using TASC siteRSM and siteVIEW Products

However, with the availability of viable IP-capable terrestrial microwave solutions, and to a lesser extent, data radio, operators were able to augment their communication network to include a high-speed data communication option. If this addition was IP-capable, SNMP equipment data now had a clear path to and from the NMS location. Furthermore, if the IP backhaul was of sufficient bandwidth other higher-end data could now be monitored – for example, image and video streams from IP-based security cameras.

[6] Monitoring over POTS system diagram, http://www.cisco.com/c/en/us/td/docs/wireless/lmr/design/guide/lmrsrnd_1/lmrsvcm.html, September 2014

Consider the diagram shown in Figure 5, which shows an IP backhaul connecting a dispatch console at headquarters to a LMR network. The same backhaul can also be used for integrated monitoring, as will be discussed in the following sections.

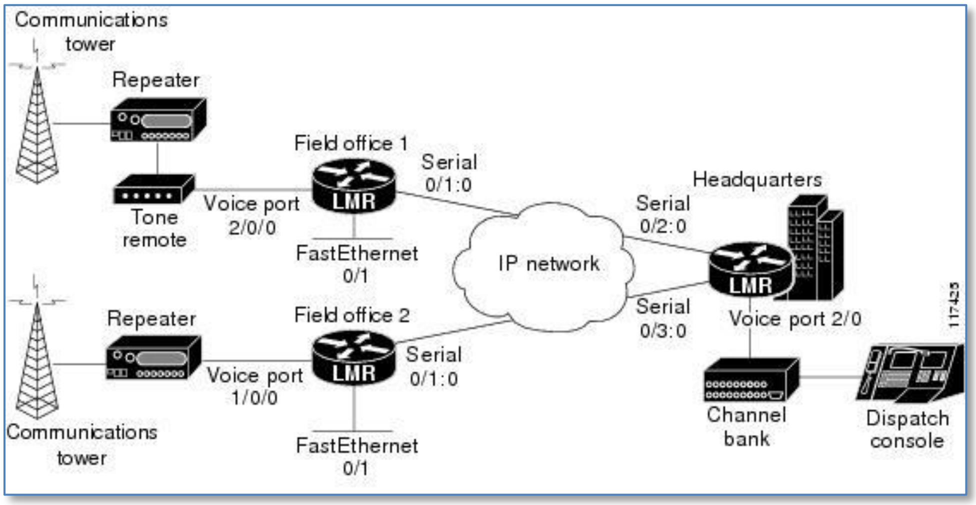


Figure 5 - Critical Communication Network with IP Backhaul[7]

[7] Monitoring over IP Network system diagram, http://www.cisco.com/c/en/us/td/docs/wireless/lmr/design/guide/lmrsrnd_1/lmrsvcm.html, September 2014

Designing a Monitor System

When discussing the monitoring of critical communication networks, it is useful to morphologically review the network components and the methods of monitoring available for each.

We can perform a system survey of the various devices that comprise the Critical Communication System, with a particular focus on:

- Network Elements
- Ancillary Equipment and Sensors

The system survey will not only make a list of devices worthy of monitoring, but also specific data points within each device that define healthy system operation or potential failure points.

Network Elements

The set of "*equipment used in the provision of a (communication) service*"[8] are known as network elements. Typical elements of a critical communication network consist of the LMR base stations and repeaters (elements responsible for voice traffic) and IP backhaul infrastructure (used for system operations and infrastructure). Without proper functioning of these elements, the network's primary function will fail, so an element monitoring mechanism is essential.

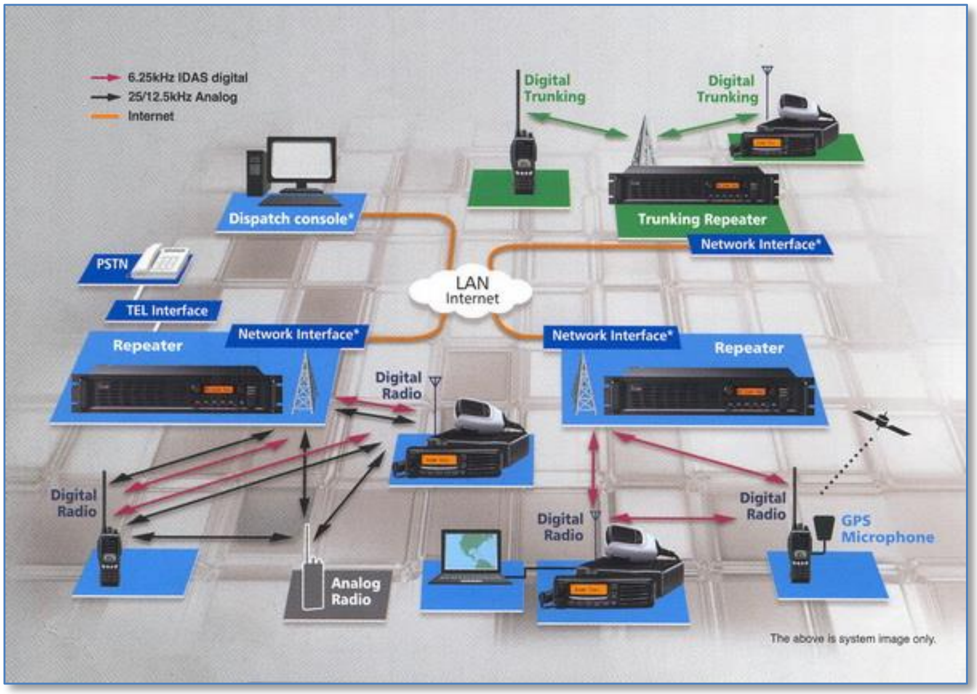


Figure 6 - Diagram of Critical Communication Network Elements (iCOM IDAS Network Topology)[9]

[8] Network Element definition, http://en.wikipedia.org/wiki/Network_element, September 2014
[9] LMR communication network system diagram, http://icomamerica.com/en/products/landmobile/idas/idas/default.aspx, September 2014

Pre-SNMP Monitoring

Precursor monitoring solutions allow operators to extract key data from radio systems via I/O signals. These I/O signals can be connected to a RTU device which is then responsible for transporting the data back to a centralized management system. For example, Kenwood NEXEDGE (NXR) and Icom IDAS elements provide information on the health of the element (temperature, fan state), transmit/receive status and power summary.

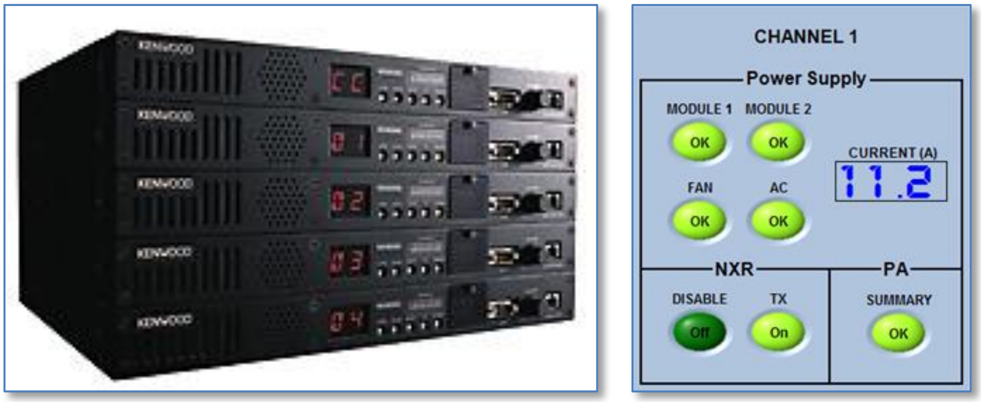


Figure 7 - I/O Information Extracted from Kenwood NEXEDGE Radio[10]

Using SNMP

As IP connectivity becomes enmeshed to what was traditionally a radio only network, OEMs began adding IP capability to their network element equipment, either directly within the device itself or through supplemental interfaces. Because of its role as a beneficial network management component of the IP standard, SNMP implementation has been subsumed in this effort.

In addition to the reporting of key events through SNMP Traps, for example system faults, many manufacturers also use SNMP to allow operators to view key operational parameters and to tweak system configuration. For example, network operators may use SNMP to extract information, in near real-time, to retrieve the status of network links, or the quality of a specific radio channel. Also, by reviewing this information over time, users may be able to view trends, allowing them to take preventative measures to avoid network failures.

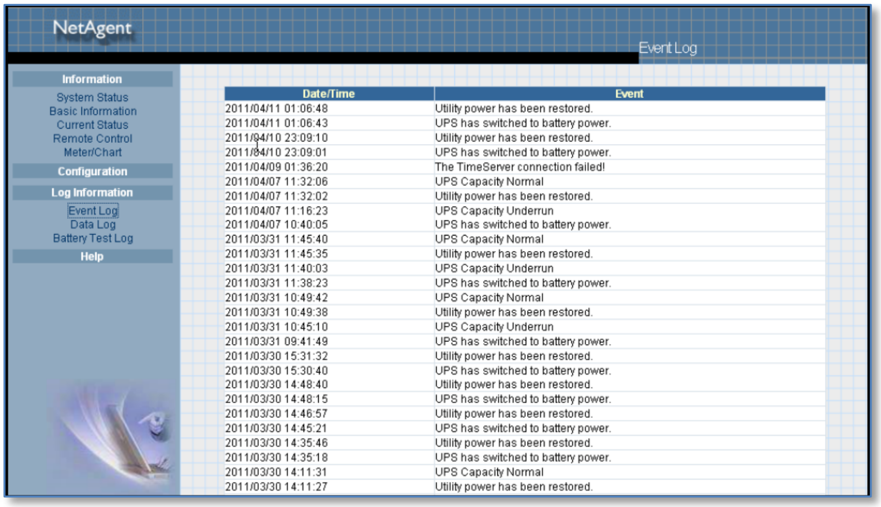
[10] Solutions for monitoring a Kenwood NEXEDGE system, http://www.tascsystems.com/?portfolio=kenwood-nexedge, September 2014

Ancillary Equipment and Sensors

In addition to communication elements, there are ancillary equipment and sensors installed at sites, which provide supporting functionality to the network.

Power Systems

Ancillary equipment of primary importance, for example, power supplies and backup power, without which network elements cannot operate. Power systems have been heavily influenced by the general Internet build out, and as such, have usually implemented SNMP as core functionality.



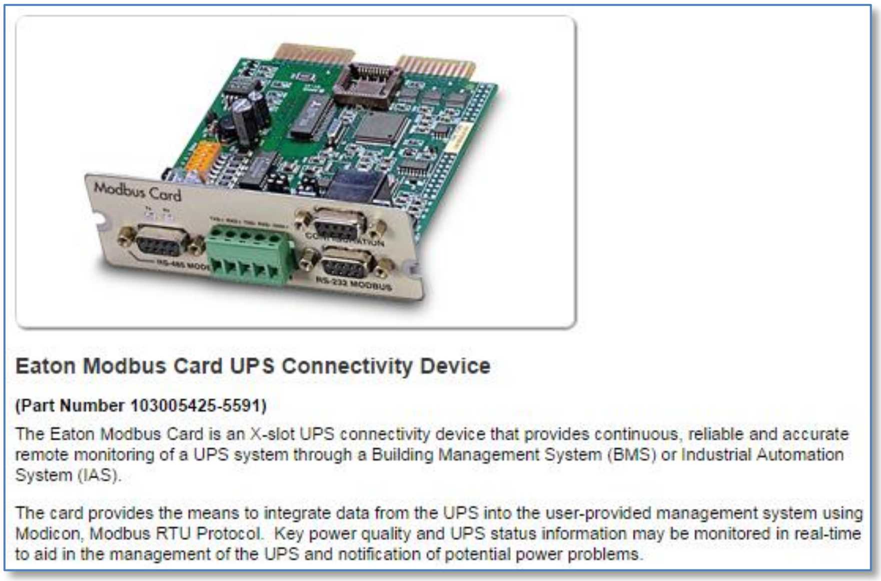
Date/Time	Event
2011/04/11 01:06:48	Utility power has been restored.
2011/04/11 01:06:43	UPS has switched to battery power.
2011/04/10 23:09:10	Utility power has been restored.
2011/04/10 23:09:01	UPS has switched to battery power.
2011/04/09 01:36:20	The TimeServer connection failed!
2011/04/07 11:32:06	UPS Capacity Normal
2011/04/07 11:32:02	Utility power has been restored.
2011/04/07 11:16:23	UPS Capacity Underrun
2011/04/07 10:40:05	UPS has switched to battery power.
2011/03/31 11:45:40	UPS Capacity Normal
2011/03/31 11:45:35	Utility power has been restored.
2011/03/31 11:40:03	UPS Capacity Underrun
2011/03/31 11:38:23	UPS has switched to battery power.
2011/03/31 10:49:42	UPS Capacity Normal
2011/03/31 10:49:38	Utility power has been restored.
2011/03/31 10:45:10	UPS Capacity Underrun
2011/03/31 09:41:49	UPS has switched to battery power.
2011/03/30 15:31:32	Utility power has been restored.
2011/03/30 15:30:40	UPS has switched to battery power.
2011/03/30 14:48:40	Utility power has been restored.
2011/03/30 14:48:15	UPS has switched to battery power.
2011/03/30 14:46:57	Utility power has been restored.
2011/03/30 14:45:21	UPS has switched to battery power.
2011/03/30 14:35:46	Utility power has been restored.
2011/03/30 14:35:18	UPS has switched to battery power.
2011/03/30 14:11:31	UPS Capacity Normal
2011/03/30 14:11:27	Utility power has been restored.

Figure 8 - Avaya Xtreme Power - SNMP Trap Messages[11]

Many remote sites are powered by alternative sources, like solar cells. Sophisticated solutions may offer SNMP or other protocols. Basic solutions may only provide I/O signals – for example, battery level or low-power alerts – which would be connected to an RTU for reporting.

Some industrial power systems may use other domain-specific protocols like Modbus, which has "*become a de facto standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices.*"[12]

[11] Avaya UPS SNMP Messages, http://www.devconnectprogram.com/fileMedia/download/c989310f-4a84-4b24-9628-f63103a7d16f, September 2014
[12] Modbus definition, http://en.wikipedia.org/wiki/Modbus, September 2014



Eaton Modbus Card UPS Connectivity Device

(Part Number 103005425-5591)

The Eaton Modbus Card is an X-slot UPS connectivity device that provides continuous, reliable and accurate remote monitoring of a UPS system through a Building Management System (BMS) or Industrial Automation System (IAS).

The card provides the means to integrate data from the UPS into the user-provided management system using Modicon, Modbus RTU Protocol. Key power quality and UPS status information may be monitored in real-time to aid in the management of the UPS and notification of potential power problems.

Figure 9 - Modbus Interface for Eaton UPS[13]

RF Communication Sensors

Network operations may use additional antenna or transmission sensors to report forward and reflected power, or VSWR readings. These readings are highly beneficial in ensuring optimum transmission and determining any antenna variance or damage.

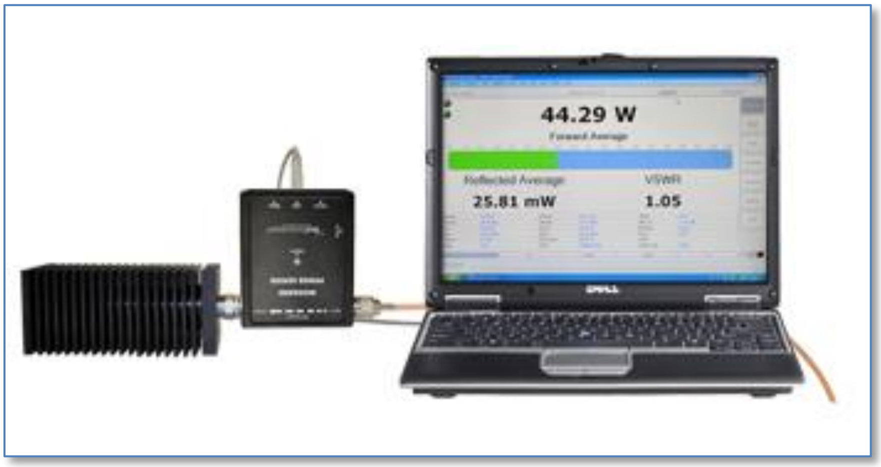


Figure 10 - Example of a Power Sensor (Measuring Forward Power)[14]

[13] Modbus interface, http://powerquality.eaton.com/products-services/power-management/connectivity/modbus.asp, September 2014

[14] Bird RF sensor, http://www.birdrf.com/Products/Power-Measurement.aspx#.VCnirfldWCk, September 2014

While some leading-edge power sensor manufacturers, like Bird Technologies, offer SNMP capability, many RF sensors present this information via analog and digital I/O. These signals can be connected to an RTU which can then report to the monitoring center.

Site Security Sensors

To avoid malevolent intrusion, critical communication network installers will use perimeter and access sensors to alert operation centers. If the remote site is not monitored by an external security service or even if they are, these sensors can be directly attached to the site's RTU to allow network operations an additional layer of security. Safe operation of the site may also depend on a host of other environmental sensors:

- In-shed temperature and external sensors can monitor a safe range for equipment operation.
- Humidity and water leakage sensors can also be used to protect expensive equipment.
- Fire and smoke detectors can signal emergency situations.

With the affordability of IP-based cameras and their ability to send back compressed images or simple SNMP traps, based on detected motion, , a full-featured monitoring solution, like siteVIEW APEX, can provide "eyes" at the site to supplement other security sensors.

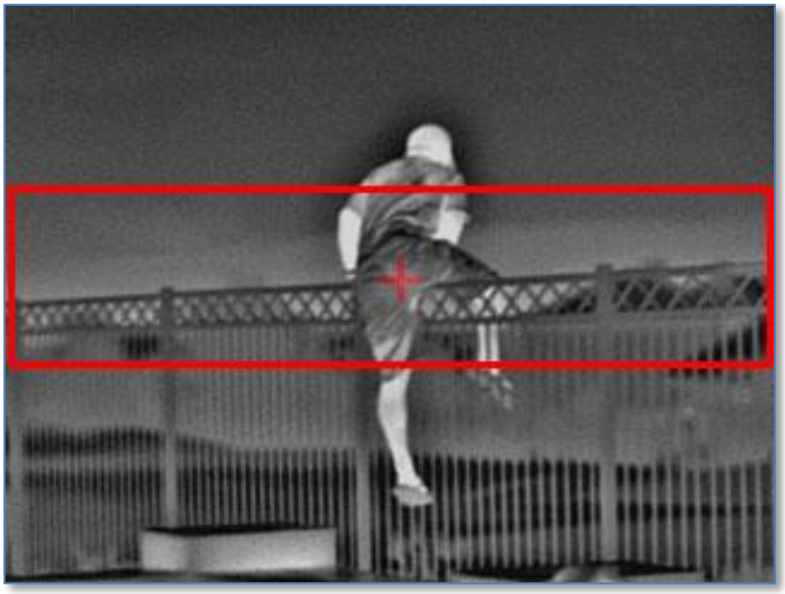


Figure 11 - Intrusion Detection using IP Camera

Application Sensors

Finally, network sites may use application-specific sensors to fulfill monitoring requirements. Here are some parameters that could be brought back to the central monitoring station by an RTU at the site.

- Propane level (using a float or bench scale)
- Gas detection
- GPS Data

Unified Monitoring Approach

To avoid a scattered or fractional approach to monitoring, *a **critical communication management system (CCMS)** must, at first, be capable of integrating all of the network's data sources*.

As we've discovered in the previous section, there is now an abundance of data available as a result of the increasing ubiquity of SNMP, advancements in RTU design, availability of robust inexpensive sensors and broad use of application-specific protocols (like Modbus). This data mandates that a monitoring solution be adept in handling all data providers, not just some, otherwise key analysis data may be excluded.

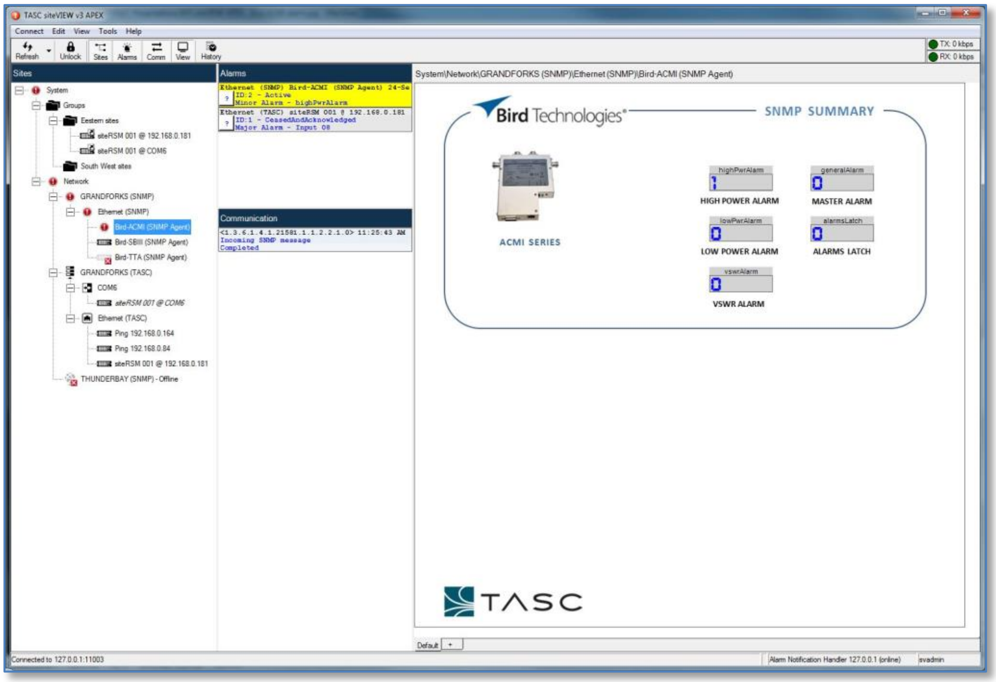
In this section, we'll explore how siteVIEW APEX fits this primary requirement as a CCMS. siteVIEW APEX has been designed, out of the box, to unify the monitoring effort, by bringing together data from all of the sources comprising a critical communication network.

SNMP Monitoring

siteVIEW APEX has integral SNMP protocol support and is designed as both a SNMP Manager and SNMP Agent.

SNMP Manager

As a SNMP Manager, siteVIEW APEX can communicate with the entire network of attached SNMP agent nodes, from simple sensors to higher-order network elements. Just like any other network device, each of these SNMP Agents can be represented as a node within the siteVIEW APEX system.



```
Ethernet (SNMP) Bird-ACMI (SNMP Agent) 24-Se
ID:2 - Active
Minor Alarm - highPwrAlarm
Ethernet (TASC) siteRSM 001 @ 192.168.0.181
ID:1 - CeasedAndAcknowledged
Major Alarm - Input 08
```

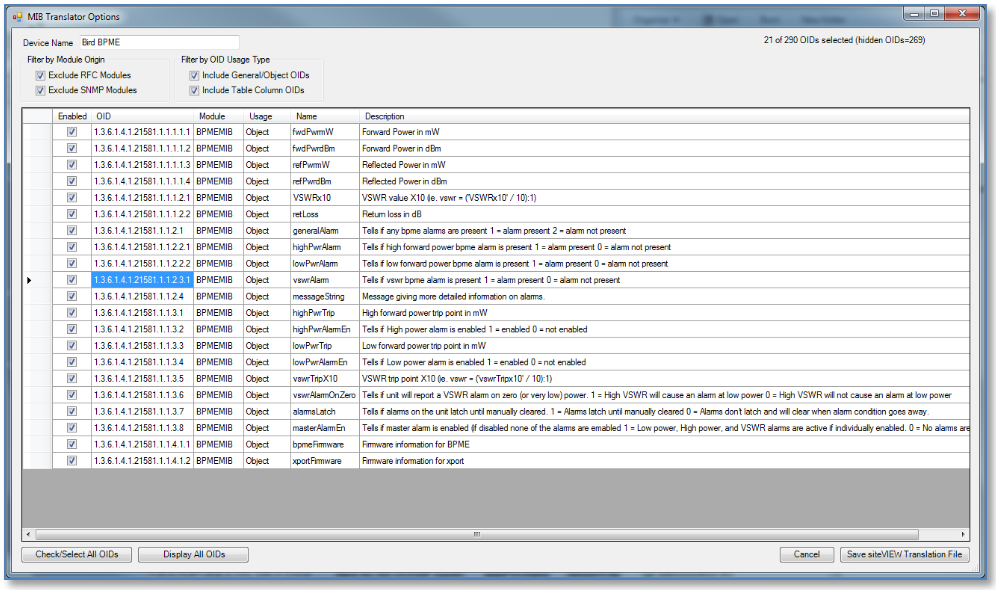
```
<1.3.6.1.4.1.21581.1.1.2.2.1.0> 11:25:43 AM
Incoming SNMP message
Completed
```

System\Network\GRANDFORKS (SNMP)\Ethernet (SNMP)\Bird-ACMI (SNMP Agent)

Connected to 127.0.0.1:11003 | Alarm Notification Handler 127.0.0.1 (online) | svadmin

Figure 12 - siteVIEW APEX Presents SNMP Agents as Network Devices (Bird ACMI)

siteVIEW APEX includes a tool to create and customize how SNMP Agents are defined. The siteVIEW APEX MIB File Translator utility allows users to filter the parameters of interest for the SNMP Agent – users can import the entire set of objects as defined in the MIB files and then export only the necessary OID elements that are of monitoring interest.



Device Name: Bird BPME

21 of 290 OIDs selected (hidden OIDs=269)

Filter by Module Origin
☑ Exclude RFC Modules
☑ Exclude SNMP Modules

Filter by OID Usage Type
☑ Include General/Object OIDs
☑ Include Table Column OIDs

	Enabled	OID	Module	Usage	Name	Description
	☑	1.3.6.1.4.1.21581.1.1.1.1.1	BPMEMIB	Object	fwdPwrmW	Forward Power in mW
	☑	1.3.6.1.4.1.21581.1.1.1.1.2	BPMEMIB	Object	fwdPwrdBm	Forward Power in dBm
	☑	1.3.6.1.4.1.21581.1.1.1.1.3	BPMEMIB	Object	refPwrmW	Reflected Power in mW
	☑	1.3.6.1.4.1.21581.1.1.1.1.4	BPMEMIB	Object	refPwrdBm	Reflected Power in dBm
	☑	1.3.6.1.4.1.21581.1.1.1.2.1	BPMEMIB	Object	VSWRx10	VSWR value X10 (ie. vswr = ('VSWRx10' / 10):1)
	☑	1.3.6.1.4.1.21581.1.1.1.2.2	BPMEMIB	Object	retLoss	Return loss in dB
	☑	1.3.6.1.4.1.21581.1.1.2.1	BPMEMIB	Object	generalAlarm	Tells if any bpme alarms are present 1 = alarm present 2 = alarm not present
	☑	1.3.6.1.4.1.21581.1.1.2.2.1	BPMEMIB	Object	highPwrAlarm	Tells if high forward power bpme alarm is present 1 = alarm present 0 = alarm not present
	☑	1.3.6.1.4.1.21581.1.1.2.2.2	BPMEMIB	Object	lowPwrAlarm	Tells if low forward power bpme alarm is present 1 = alarm present 0 = alarm not present
▸	☑	1.3.6.1.4.1.21581.1.1.2.3.1	BPMEMIB	Object	vswrAlarm	Tells if vswr bpme alarm is present 1 = alarm present 0 = alarm not present
	☑	1.3.6.1.4.1.21581.1.1.2.4	BPMEMIB	Object	messageString	Message giving more detailed information on alarms.
	☑	1.3.6.1.4.1.21581.1.1.3.1	BPMEMIB	Object	highPwrTrip	High forward power trip point in mW
	☑	1.3.6.1.4.1.21581.1.1.3.2	BPMEMIB	Object	highPwrAlarmEn	Tells if High power alarm is enabled 1 = enabled 0 = not enabled
	☑	1.3.6.1.4.1.21581.1.1.3.3	BPMEMIB	Object	lowPwrTrip	Low forward power trip point in mW
	☑	1.3.6.1.4.1.21581.1.1.3.4	BPMEMIB	Object	lowPwrAlarmEn	Tells if Low power alarm is enabled 1 = enabled 0 = not enabled
	☑	1.3.6.1.4.1.21581.1.1.3.5	BPMEMIB	Object	vswrTripX10	VSWR trip point X10 (ie. vswr = ('vswrTripx10' / 10):1)
	☑	1.3.6.1.4.1.21581.1.1.3.6	BPMEMIB	Object	vswrAlarmOnZero	Tells if unit will report a VSWR alarm on zero (or very low) power. 1 = High VSWR will cause an alarm at low power 0 = High VSWR will not cause an alarm at low power
	☑	1.3.6.1.4.1.21581.1.1.3.7	BPMEMIB	Object	alarmsLatch	Tells if alarms on the unit latch until manually cleared. 1 = Alarms latch until manually cleared 0 = Alarms don't latch and will clear when alarm condition goes away.
	☑	1.3.6.1.4.1.21581.1.1.3.8	BPMEMIB	Object	masterAlarmEn	Tells if master alarm is enabled (if disabled none of the alarms are emabled 1 = Low power, High power, and VSWR alarms are active if individually enabled. 0 = No alarms are
	☑	1.3.6.1.4.1.21581.1.1.4.1.1	BPMEMIB	Object	bpmeFirmware	Firmware information for BPME
	☑	1.3.6.1.4.1.21581.1.1.4.1.2	BPMEMIB	Object	xportFirmware	Firmware information for xport

Figure 13 - siteVIEW APEX's MIB Translator Allows Selection of Monitoring Parameters for SNMP Agent

SNMP Agent

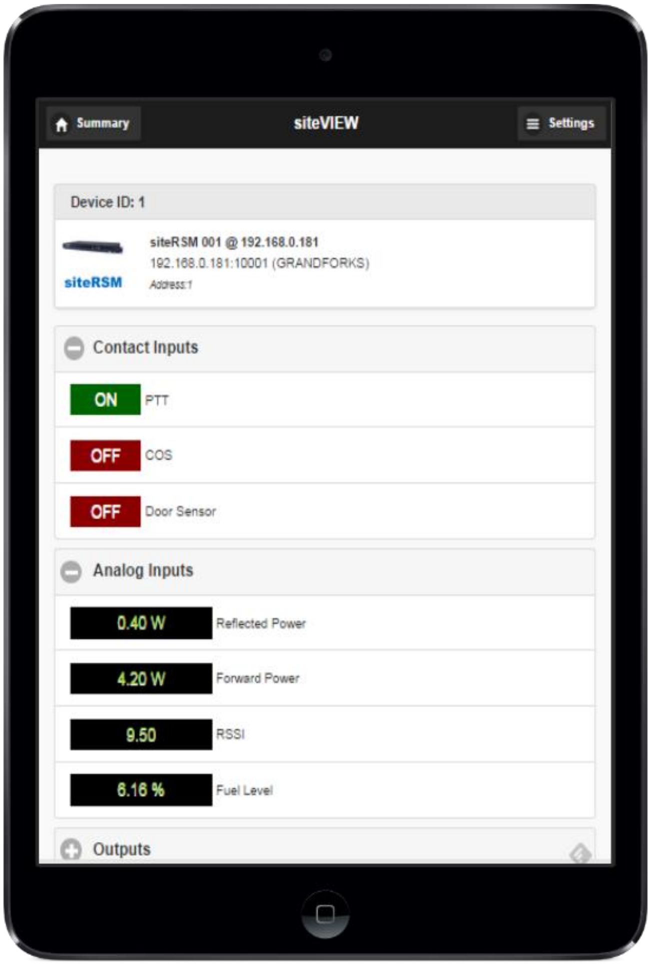
Often a critical communication network is connected to a larger enterprise network for an organization. For example, the radio network used by a law enforcement organization, may be connected with the police's IT network, in this case, the monitoring solution must be able to provide summarized alarm data to the higher-level system.

To fulfill this requirement, siteVIEW APEX can send alarm information to other software systems in many formats. If the higher-level software is itself a SNMP Manager – for example a SNMP-based Network Operations Center (NOC) - then siteVIEW APEX can act as a proxy SNMP Agent for the critical communication network, forwarding any detected variances as SNMP Traps to the NOC.

RTU Monitoring

Since many elements, devices and sensors are not SNMP capable, an RTU must be used to transport monitoring data to the management system. The RTU is responsible for providing I/O inputs, filtering this information and reliably and predictably uploading this information to the centralized monitoring service.

TASC System's siteRSM family of RTUs has been used in thousands of applications to backhaul critical I/O data to siteVIEW software. siteVIEW treats these RTUs as nodes of the monitoring network.



Device ID: 1

siteRSM 001 @ 192.168.0.181
192.168.0.181:10001 (GRANDFORKS)
Address:1

Contact Inputs

ON PTT

OFF COS

OFF Door Sensor

Analog Inputs

0.40 W Reflected Power

4.20 W Forward Power

9.50 RSSI

6.16 % Fuel Level

Outputs

Figure 14 - siteVIEW APEX MOBILE User Interface for a connected siteRSM RTU

In addition to this primary purpose, RTUs typically may also offer the following other benefits:

- **Low-power operation** – this is a key requirement in remote sites where the only power available is via solar or alternative sources.
- **Peripheral connections** – RTUs may also connect to other site-based functional components, for example, in a mobile monitoring applications, the RTU may connect via serial ports to GPS systems or CAN Bus interfaces.

- **Specialized backhaul** – in particularly remote sites or specialized SCADA applications, the RTU may connect to proprietary long-range wireless data radio technologies.
- **Output I/O** – in the case where actuation of a local device may be required on a pre-defined logic sequence. For example, in the case of main AC failure, a switchover to a backup generator maybe initiated via an output signal.
- **Real-time and filtered operation** – the I/O from a site device may change quickly, hence the RTU must be capable of sensing these variations. A robust RTU will constantly check for changes in the sub-second range (e.g., every 100millisecond) and filter out unnecessary noise.
- **Logging** – RTUs may provide local logging of I/O. In the case of a critical problem forensics, this data may be used for detailed historical analysis.

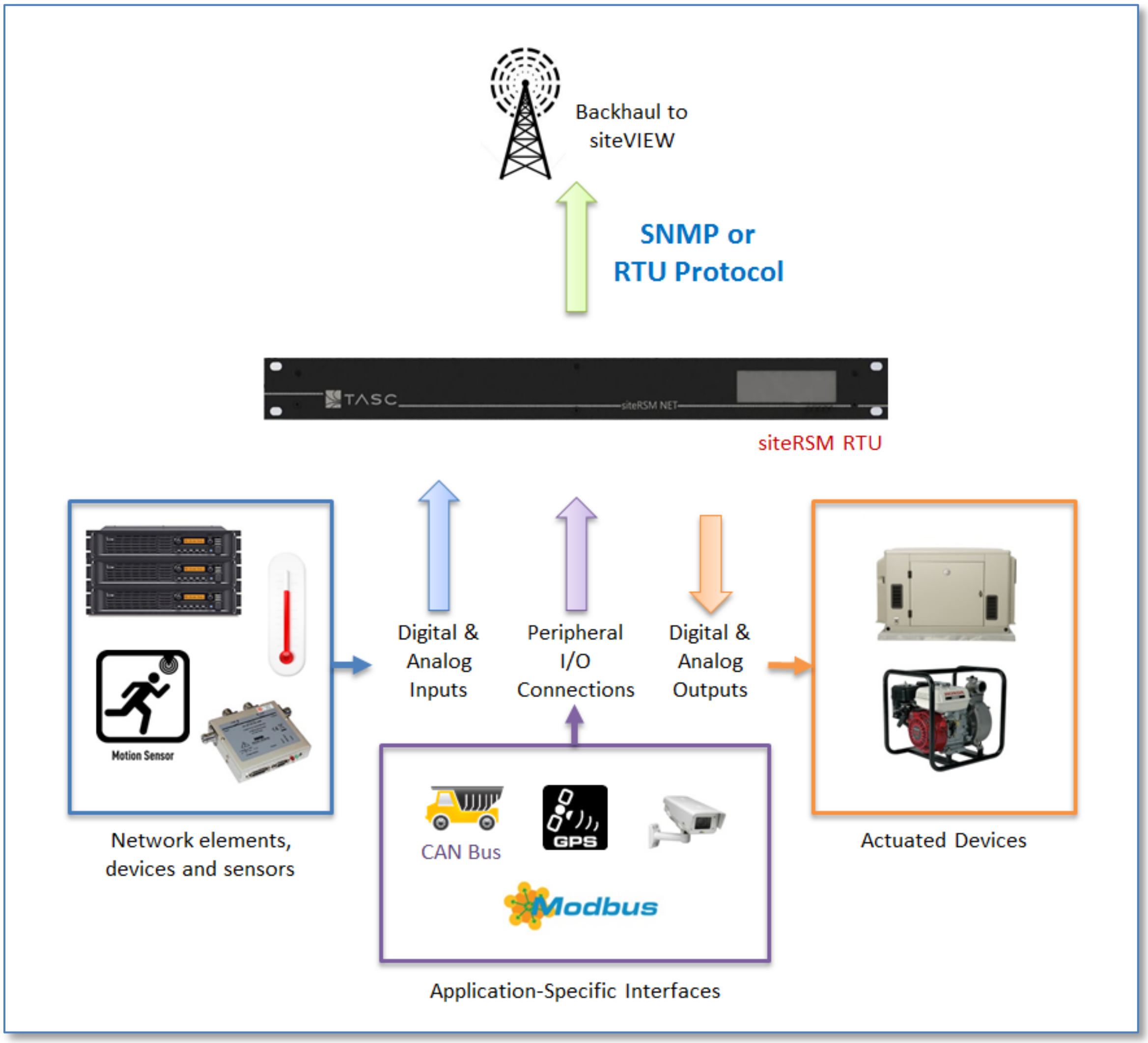


Figure 15 - siteRSM RTU Connects Remote I/O to siteVIEW APEX using SNMP or other RTU Protocol

RTU I/O

At a minimum, a RTU must be able to accept digital and analog inputs from legacy and rudimentary devices. These devices may be network elements, ancillary devices or simple sensors.

The siteRSM family provides a range of input options:

	siteRSM Classic	siteRSM NET
RTU Design		
Digital Inputs	8 to 40	48 to 144
Analog Inputs	8 to 24	32 to 256
Digital Outputs	Up to 8	16 to 32
Analog Outputs	N/A	Up to 4
Serial Ports	N/A	2 to 8 (4 configurable for RS-232, 422, 485)
Wiring Method	Weidmuller 8 channel terminal	DB64 Port (used with cable to terminal block)
Backhaul Method	**RTU protocol via serial or IP**	**SNMP via IP**

The siteRSM family of RTUs features protection circuitry on all I/O to safeguard against electrical spikes or shorts. Filtering options include:

- **Input hold times** – prevent sporadic variations or noise from affecting data validity. This feature is useful in removing false threshold violations.
- **Qualifiers** – data is validated based on another I/O value. A typical use is validating transmission power if PTT is active.
- **Local outputs** – output may be triggered based on a threshold change on an input. An example use of this feature is using a digital output relay to turn on a pump based on a high-water input sensor.

RTU Application-Specific Interfaces

Beyond I/O, RTUs can enable sophisticated application interfaces. Local devices can be connected for enhanced operation, for example:

- For mobile applications, GPS information can be read via a serial interfaces and reported to the monitoring center.
- For vehicle applications, real-time or cumulative vehicle information can be extracted for further as part of a monitoring solution.

- With the emergence of the Internet of Things (IoT), a RTU can act as an interface to Wireless Sensor Networks (WSN), like ZigBee, which may manage a sub-network of local devices.

siteRSM NET offers multiple serial and IP connections, allowing on-board drivers to extract and convey application data to siteVIEW APEX.

Monitoring via Other Protocols

In addition to SNMP and RTU nodes, siteVIEW APEX has been designed to be extensible to other protocols. Domain specific protocols can enable communication with devices specific to the industry. Consider the following examples:

- PLC-centric industries, like Oil and Gas, may provide either direct access to devices or present useful summary data based on protocols such as Modbus or Data Highway Plus.
- Remote SCADA systems may use proprietary backhaul protocols. A driver may be written for siteVIEW APEX that allows access to this data stream.

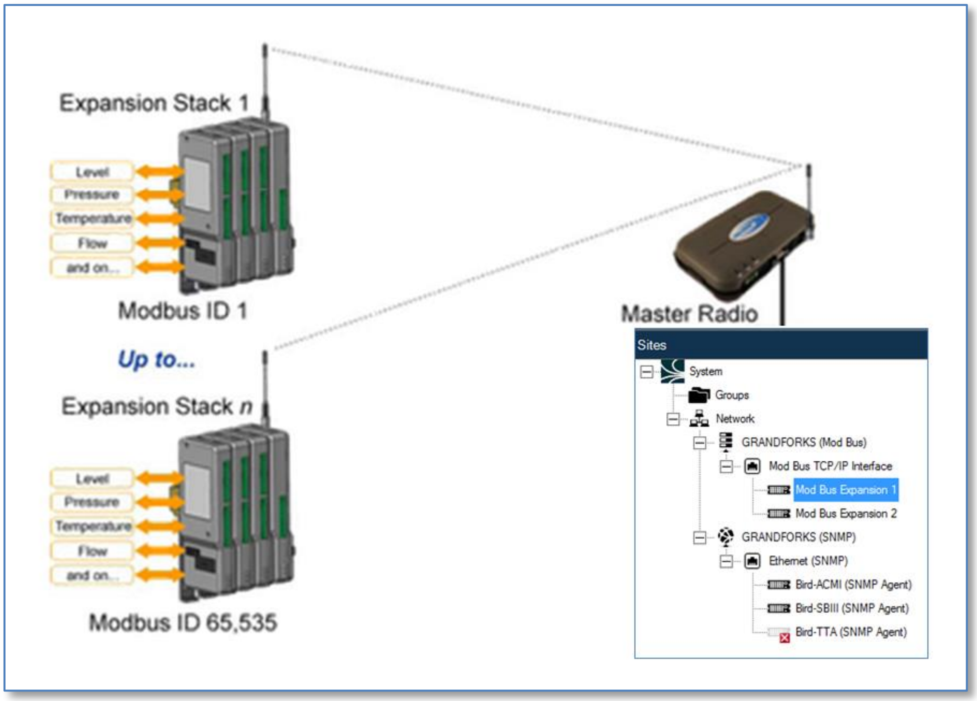


Figure 16 - siteVIEW APEX with Mod Bus TCP/IP Expansions

Essential Functions of a Critical Communication Management Solution

To summarize so far: we've organically established the base for our critical communications management systems (CCMS) by going through the following process steps:

1. **Design through a System Survey** - Identifying the elements, equipment and sensors that would give us the best portal into the healthy operation of our critical communication network.
2. **Defining SNMP Elements** - Where possible, we've recognized the SNMP-capable devices and then determined what specific data points or OIDs are necessary to monitor. We've then established an IP path back to our monitoring solution and entered each of the devices as nodes within the software.
3. **Defining RTU Devices and Sensors** – For devices that don't fit into the SNMP world, but instead rely on physical I/O connections, we've commissioned one or more RTUs at each site and made the requisite I/O wiring connections. We then have determined the optimum backhaul mechanism for each RTU – where IP is available, it will be used, but where there are IP connectivity holes, we've designed a radio, telephonic or custom wireless solution. Finally, we've entered each RTU as a node with our system.
4. **Managing Other Protocols** – For the application-specific interfaces, we've installed the protocol drivers, established the interface with the devices and entered the devices into the software as nodes.

With this infrastructure in place, we're ready to explore how to use siteVIEW APEX to monitor the critical communication network and report any exceptions. Along the way, we'll also review collateral features of a full-featured monitoring solution.

User Interfaces

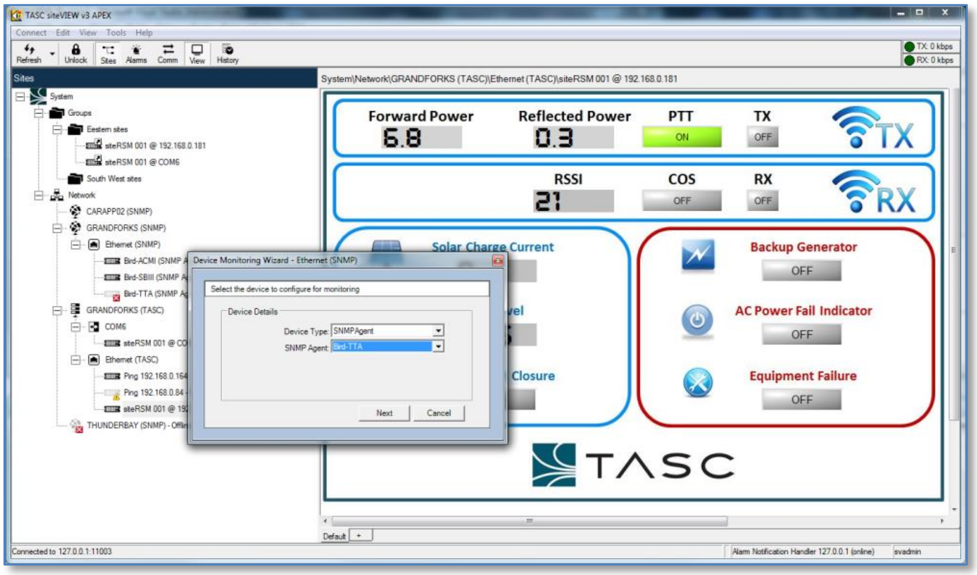
siteVIEW APEX provides multiple user interface options, to satisfy the diverse use models within an organization.

siteVIEW APEX Operator Interface

The siteVIEW APEX Operator Interface is the hub for visual monitoring and configuration of the siteVIEW system and consists of the following sections:

- **Network tree** – shows the various nodes, associated with monitored elements, RTUs and devices in the network. The node is defined within the context of its communication path and load-balancing communication manager.
- **Graphical Panel** – customizable user interface panel, which optimizes the essential data points in a visual framework.
- **Alarm Summary Window** – list of active alarms affecting system operation.
- **Communication Summary Window** – list of active communications to/from the various nodes. Whether the node initiated the communication as some sort of threshold difference or SNMP Trap or if the communication is the result of a scheduled poll, the status will be reported in this window.

- **Menu Strip and Buttons** – a list of system actions are available through this interface or via context sensitive right-clicks.
- **Grouping Infrastructure** – Devices can be further categorized with groups, representing sections or regions. Additional each group may be assigned a user access authentication requirement, allowing only qualified users to view the group.



System\Network\GRANDFORKS (TASC)\Ethernet (TASC)\siteRSM 001 @ 192.168.0.181

Forward Power: 6.8
Reflected Power: 0.3
PTT: ON
TX: OFF
RSSI: 21
COS: OFF
RX: OFF
Backup Generator: OFF
AC Power Fail Indicator: OFF
Equipment Failure: OFF

Select the device to configure for monitoring

Device Type: SNMPAgent
SNMP Agent: Bird-TTA

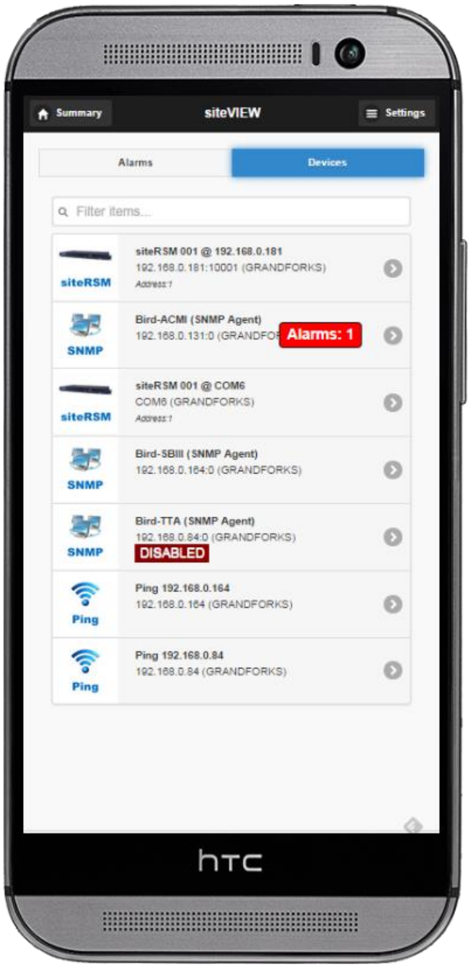
Connected to 127.0.0.1:11003
Alarm Notification Handler 127.0.0.1 (online)
svadmin

Figure 17 - siteVIEW APEX Operator Interface

siteVIEW APEX Mobile Interface

The use model for the siteVIEW APEX Operator Interface may not meet the needs to mobile workers that need to understand network problems, so TASC created the siteVIEW APEX Mobile Interface, which provides a responsive web interface to siteVIEW. Information is distilled to the vitals required to view and then diagnose system issues:

- **Summary Page (Alarms)** – provides a summary of all the alarms active in the system. Alarms are categorized by severity and time, with quick visual indicators to determine alarm states.
- **Summary Page (Devices)** – provides a summary of all the devices on the network. Devices can be easily sorted and filtered. Included with each device is the communication path and address information.
- **Device Detail Page** – one-touch to view the device details for an active alarm, or optionally, navigate from the device summary page. Here the individual data points, SNMP OIDs or RTU I/O, for a device are presented. For siteRSM RTUs, outputs may be activated.



siteRSM — **siteRSM 001 @ 192.168.0.181**
192.168.0.181:10001 (GRANDFORKS)
Address:1

SNMP — **Bird-ACMI (SNMP Agent)**
192.168.0.131:0 (GRANDFO
Alarms: 1

siteRSM — **siteRSM 001 @ COM6**
COM6 (GRANDFORKS)
Address:1

SNMP — **Bird-SBIII (SNMP Agent)**
192.168.0.164:0 (GRANDFORKS)

SNMP — **Bird-TTA (SNMP Agent)**
192.168.0.84:0 (GRANDFORKS)
DISABLED

Ping — **Ping 192.168.0.164**
192.168.0.164 (GRANDFORKS)

Ping — **Ping 192.168.0.84**
192.168.0.84 (GRANDFORKS)

Figure 18 - siteVIEW APEX Mobile Interface

siteVIEW APEX M2M Interface

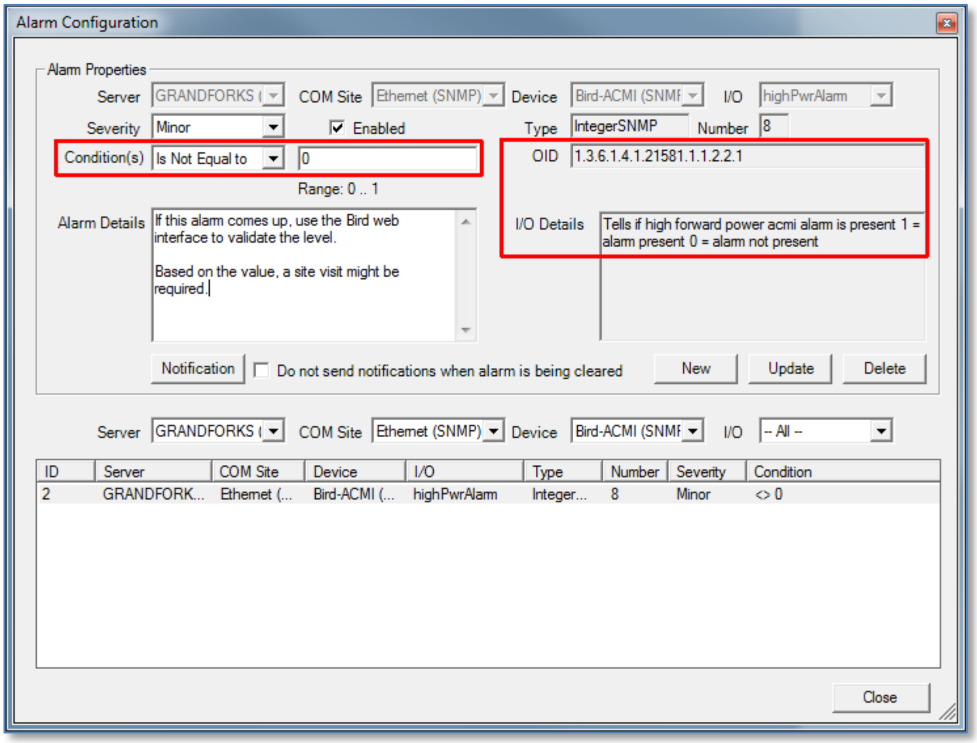
Depending on the IT maturity of an organization, siteVIEW APEX may be directly linked with an enterprise solution, which then takes on a role as meta-manager. In this case, siteVIEW offers the following options:

- **SNMP Agent** – siteVIEW APEX can provide SNMP Trap reports of each alarm incident.
- **siteVIEW APEX API or database connection** – for development teams that want to tie directly into the core of siteVIEW APEX, an API or database connection is available.

Alarm Management

siteVIEW APEX's alarm management is built on over a decade of experience managing mission critical networks and features the following key capabilities:

- **Configurable alarms** – an alarm is raised based on a violation of a configured condition, either as threshold cross, variance from norm or state difference. Alarms can be prescribed a severity and notification model.



Alarm Configuration

Alarm Properties

Server: GRANDFORKS (
COM Site: Ethernet (SNMP)
Device: Bird-ACMI (SNMF
I/O: highPwrAlarm
Severity: Minor
☑ Enabled
Type: IntegerSNMP
Number: 8
Condition(s): Is Not Equal to 0
Range: 0 .. 1
OID: 1.3.6.1.4.1.21581.1.1.2.2.1

Alarm Details: If this alarm comes up, use the Bird web interface to validate the level.

Based on the value, a site visit might be required.

I/O Details: Tells if high forward power acmi alarm is present 1 = alarm present 0 = alarm not present

□ Do not send notifications when alarm is being cleared

Server: GRANDFORKS (
COM Site: Ethernet (SNMP)
Device: Bird-ACMI (SNMF
I/O: -- All --

ID	Server	COM Site	Device	I/O	Type	Number	Severity	Condition
2	GRANDFORK...	Ethernet (...	Bird-ACMI (...	highPwrAlarm	Integer...	8	Minor	<> 0

Figure 19 - siteVIEW APEX Alarm Configuration Dialog

- **Notification mechanisms** – siteVIEW APEX provides multiple notification methods, ranging from local sound, text to speech (TTS), email/SMS or SNMP Traps. Users may also consider using an output on a RTU to trigger an auto-dialer.
- **Alarm State Management** – siteVIEW APEX enforces a stringent system of managing active alarms, to ensure that a standard process is followed in resolving issues.

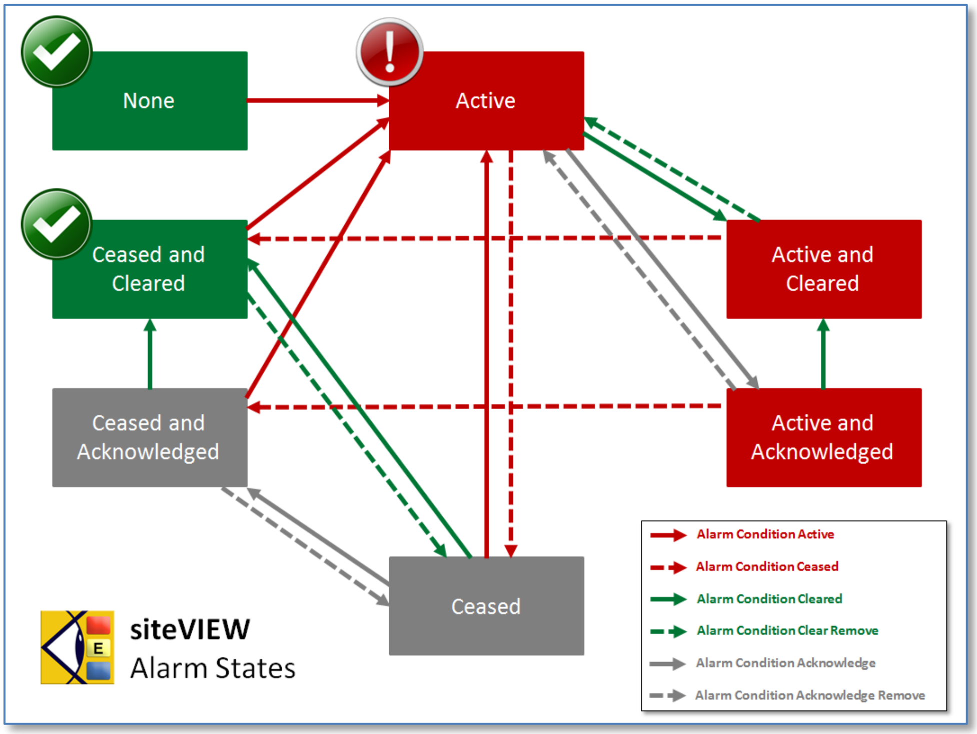
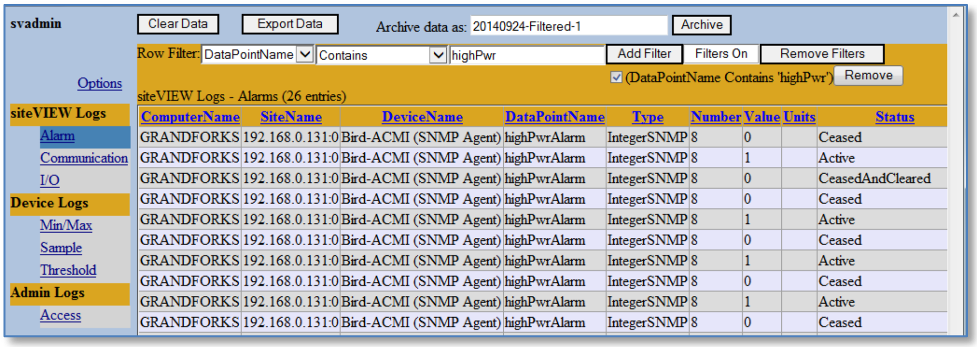


Figure 20 - siteVIEW APEX Alarm State Model

- **Alarm Logging** – siteVIEW features an integral historical logging system, which logs all system activity, including alarm state changes. This information is accessible via web and can be exported for further analysis and reporting.



Archive data as: 20140924-Filtered-1

Row Filter: DataPointName Contains highPwr

☑ (DataPointName Contains 'highPwr')

siteVIEW Logs - Alarms (26 entries)

ComputerName	SiteName	DeviceName	DataPointName	Type	Number	Value	Units	Status
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		Ceased
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	1		Active
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		CeasedAndCleared
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		Ceased
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	1		Active
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		Ceased
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	1		Active
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		Ceased
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	1		Active
GRANDFORKS	192.168.0.131:0	Bird-ACMI (SNMP Agent)	highPwrAlarm	IntegerSNMP	8	0		Ceased

Figure 21 - siteVIEW APEX Alarm Logging Sub-System

System Security

As a critical communication management solution, siteVIEW APEX contains multiple security features to prevent misuse.

User Access

User access is integral to the siteVIEW APEX framework:

- **User Authentication** – by default, siteVIEW APEX includes a user authentication system, but this can be replaced with an LDAP-compatible authentication system, for example, with an Active Directory system in a Windows domain. User must pass through this authentication to access functional components of siteVIEW.
- **User Authorization** – siteVIEW offers multiple levels of authorization from view-only, to normal users and, finally, system administrators. A policy based on the user's authorization defines the functionality presented by all of the siteVIEW APEX interfaces.

General System Security

To ensure robust system operation, siteVIEW APEX's design has multiple safety and security mechanisms.

- **Platform Behavior** – siteVIEW can be deployed on standard platforms, for example Windows Server platforms. Most installations feature a hardened OS configuration, firm security policy guidelines and firewalls. siteVIEW can be configured to work with Virtual Private Networks (VPN) validated connections only.
- **System Architecture** – siteVIEW has highly-scalable and distributed architecture. To ensure a load-balanced system, siteVIEW components can be spread amongst multiple servers.
- **Redundant Operation** – to safeguard against downtime of the primary siteVIEW APEX core system, siteVIEW APEX can optionally operate a redundant core, which is ready at all times for failover. Once the main system is back up, the redundant server will cede authority back to the main core.

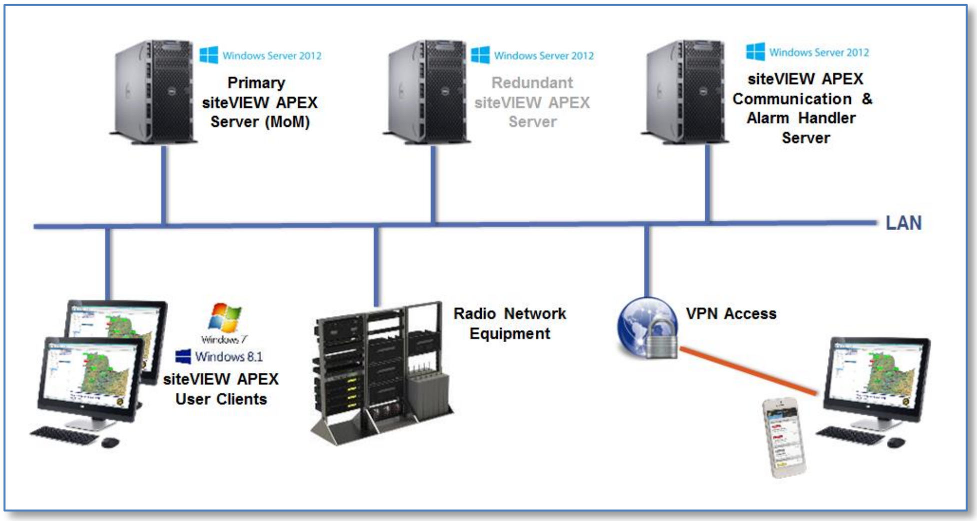
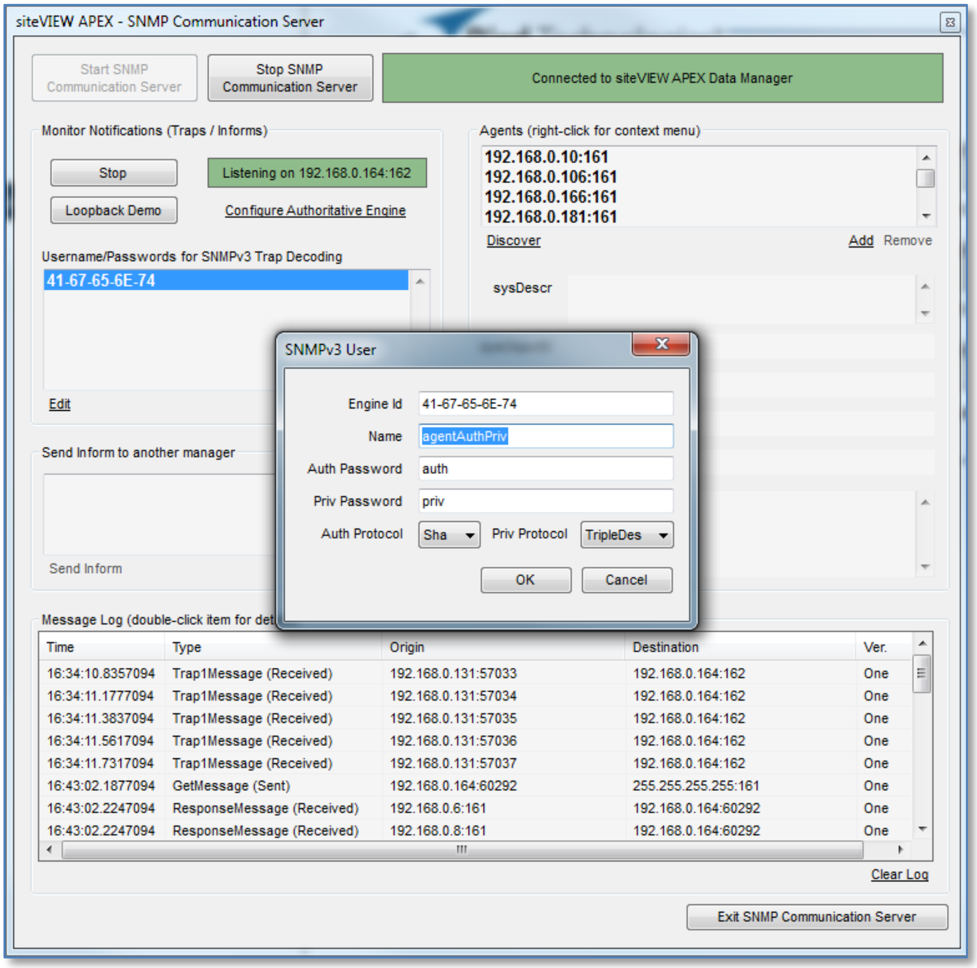

Windows Server 2012
Primary siteVIEW APEX Server (MoM)
Windows Server 2012
Redundant siteVIEW APEX Server
Windows Server 2012
siteVIEW APEX Communication & Alarm Handler Server
LAN
Windows 7
Windows 8.1
siteVIEW APEX User Clients
Radio Network Equipment
VPN Access

Figure 22- siteVIEW APEX is a Scalable, Distributed System and Features Redundancy

- **System Archiving** – siteVIEW has a built-in auto-archiving system to ensure that the core database is copied at scheduled intervals to a safe location. In case of accident, the archived database can be recovered in a matter of minutes.

SNMP Communications

- **SNMP v3** – siteVIEW's SNMP Communication Server offers a security model based on SNMP v3. Configuration allows for authentication and encryption protocols to be used.


siteVIEW APEX - SNMP Communication Server
Start SNMP Communication Server
Stop SNMP Communication Server
Monitor Notifications (Traps / Informs)
Stop
Loopback Demo
Configure Authoritative Engine
Agents (right-click for context menu)
Discover
Add
Remove
sysDescr
Edit
Send Inform to another manager
Send Inform
SNMPv3 User
OK
Cancel
Message Log (double-click item for det
Clear Log
Exit SNMP Communication Server

Connected to siteVIEW APEX Data Manager

Listening on 192.168.0.164:162

Agents:
192.168.0.10:161
192.168.0.106:161
192.168.0.166:161
192.168.0.181:161

Username/Passwords for SNMPv3 Trap Decoding: 41-67-65-6E-74

Engine Id: 41-67-65-6E-74
Name: agentAuthPriv
Auth Password: auth
Priv Password: priv
Auth Protocol: Sha
Priv Protocol: TripleDes

Time	Type	Origin	Destination	Ver.
16:34:10.8357094	Trap1Message (Received)	192.168.0.131:57033	192.168.0.164:162	One
16:34:11.1777094	Trap1Message (Received)	192.168.0.131:57034	192.168.0.164:162	One
16:34:11.3837094	Trap1Message (Received)	192.168.0.131:57035	192.168.0.164:162	One
16:34:11.5617094	Trap1Message (Received)	192.168.0.131:57036	192.168.0.164:162	One
16:34:11.7317094	Trap1Message (Received)	192.168.0.131:57037	192.168.0.164:162	One
16:43:02.1877094	GetMessage (Sent)	192.168.0.164:60292	255.255.255.255:161	One
16:43:02.2247094	ResponseMessage (Received)	192.168.0.6:161	192.168.0.164:60292	One
16:43:02.2247094	ResponseMessage (Received)	192.168.0.8:161	192.168.0.164:60292	One

Figure 23 - siteVIEW SNMP Communication Server Supports SNMP v3

- **siteRSM RTU Protocol** – the protocol used to talk with the siteRSM family checks to ensure RTU availability and data correctness. Any RTU communication failures can trigger siteVIEW alarms, alerting operators of backhaul or site issues.

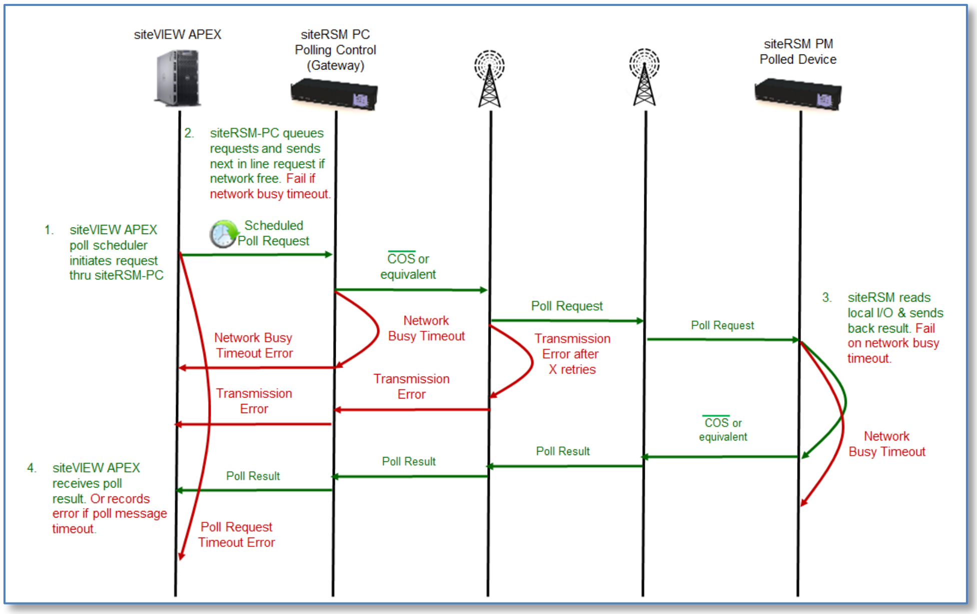
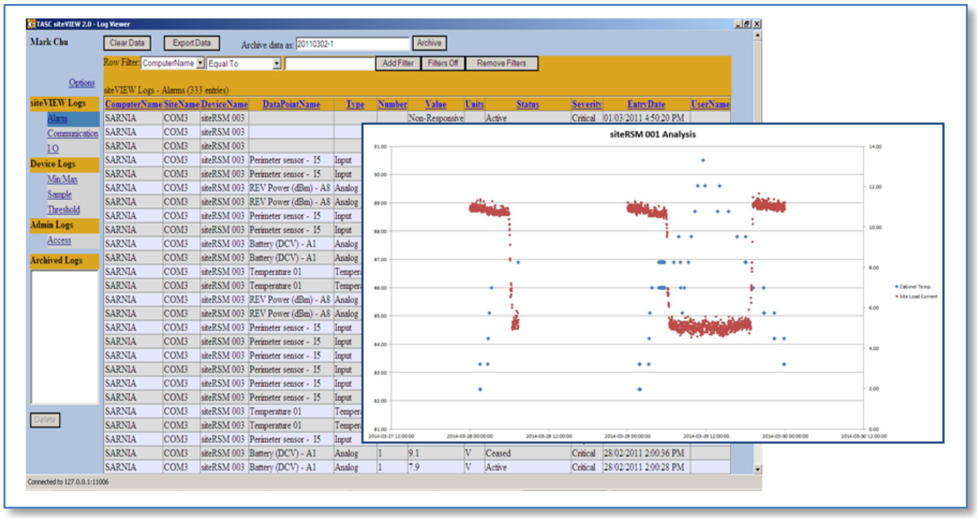

siteVIEW APEX
siteRSM PC
Polling Control
(Gateway)
siteRSM PM
Polled Device
2. siteRSM-PC queues requests and sends next in line request if network free. Fail if network busy timeout.
1. siteVIEW APEX poll scheduler initiates request thru siteRSM-PC
Scheduled Poll Request
COS or equivalent
Poll Request
Poll Request
3. siteRSM reads local I/O & sends back result. Fail on network busy timeout.
Network Busy Timeout Error
Network Busy Timeout
Transmission Error after X retries
Transmission Error
Transmission Error
COS or equivalent
Network Busy Timeout
Poll Result
Poll Result
Poll Result
4. siteVIEW APEX receives poll result. Or records error if poll message timeout.
Poll Request Timeout Error

Figure 24 - siteRSM Protocol is Designed to Report Backhaul Communication Errors

Logging and Diagnostics

Once an issue is detected, system logging and diagnostics can be used to contextualize the problem and forensically determine the cause. siteVIEW APEX offers multiple features to assist the network operator in discerning the root cause:

- **History Tables** – siteVIEW APEX tracks virtually all events sensed by the core within History tables. The following events are tracked: User login, I/O point changes, communication transactions, alarm state changes and, for specialized devices, device status changes. The web-based History view allows filtering of the data and export to CSV files for further analysis. Daily archives of history information are kept in XML format for programmatic analysis, for example for trend analysis.



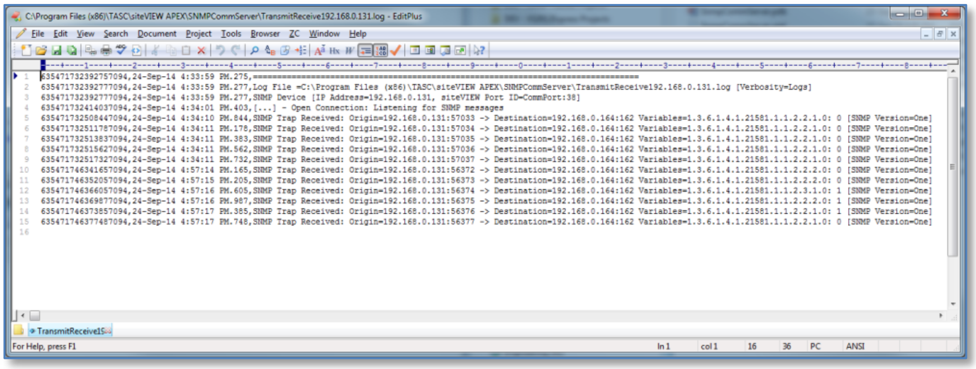
siteVIEW Logs - Alarms (333 entries)

ComputerName	SiteName	DeviceName	DataPointName	Type	Number	Value	Units	Status	Severity	EntryDate	UserName
SARNIA	COM3	siteRSM 003				Non-Responsive		Active	Critical	01/03/2011 4:50:20 PM	
SARNIA	COM3	siteRSM 003									
SARNIA	COM3	siteRSM 003									
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	REV Power (dBm) - A8	Analog							
SARNIA	COM3	siteRSM 003	REV Power (dBm) - A8	Analog							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Battery (DCV) - A1	Analog							
SARNIA	COM3	siteRSM 003	Battery (DCV) - A1	Analog							
SARNIA	COM3	siteRSM 003	Temperature 01	Tempera							
SARNIA	COM3	siteRSM 003	Temperature 01	Tempera							
SARNIA	COM3	siteRSM 003	REV Power (dBm) - A8	Analog							
SARNIA	COM3	siteRSM 003	REV Power (dBm) - A8	Analog							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Temperature 01	Tempera							
SARNIA	COM3	siteRSM 003	Temperature 01	Tempera							
SARNIA	COM3	siteRSM 003	Perimeter sensor - I5	Input							
SARNIA	COM3	siteRSM 003	Battery (DCV) - A1	Analog	1	9.1	V	Ceased	Critical	28/02/2011 2:00:36 PM	
SARNIA	COM3	siteRSM 003	Battery (DCV) - A1	Analog	1	7.9	V	Active	Critical	28/02/2011 2:00:28 PM	

Connected to 127.0.0.1:11006

Figure 25 - siteVIEW Historical View and Exported Analysis on MS Excel

- **System Logging** – In addition to Historical logging, core components can be optionally instructed to log activity within text-based log files. System log files include:
    - **Communication Logs** – there are one or more communication servers for each protocol: SNMP, RTU or other. Each server keeps a running log of the ports and/or devices it is responsible for. If there is a problem with the backhaul detailed information may be gleaned here.
    - **Port or Device Logs** – for each port or device a log file records detailed transactional history. These files contain protocol specific data and may be used to hunt down reporting issues.



```
635471732392757094,24-Sep-14 4:33:59 PM.275,===============================================================================================
635471732392777094,24-Sep-14 4:33:59 PM.277,Log File =C:\Program Files (x86)\TASC\siteVIEW APEX\SNMPCommServer\TransmitReceive192.168.0.131.log [Verbosity=Logs]
635471732392777094,24-Sep-14 4:33:59 PM.277,SNMP Device [IP Address=192.168.0.131, siteVIEW Port ID=CommPort:38]
635471732414037094,24-Sep-14 4:34:01 PM.403,[...] - Open Connection: Listening for SNMP messages
635471732508447094,24-Sep-14 4:34:10 PM.844,SNMP Trap Received: Origin=192.168.0.131:57033 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
635471732511787094,24-Sep-14 4:34:11 PM.178,SNMP Trap Received: Origin=192.168.0.131:57034 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
635471732513837094,24-Sep-14 4:34:11 PM.383,SNMP Trap Received: Origin=192.168.0.131:57035 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
635471732515627094,24-Sep-14 4:34:11 PM.562,SNMP Trap Received: Origin=192.168.0.131:57036 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
635471732517327094,24-Sep-14 4:34:11 PM.732,SNMP Trap Received: Origin=192.168.0.131:57037 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
635471746341657094,24-Sep-14 4:57:14 PM.165,SNMP Trap Received: Origin=192.168.0.131:56372 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.2.0: 0 [SNMP Version=One]
635471746352057094,24-Sep-14 4:57:15 PM.205,SNMP Trap Received: Origin=192.168.0.131:56373 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.2.0: 0 [SNMP Version=One]
635471746366057094,24-Sep-14 4:57:16 PM.605,SNMP Trap Received: Origin=192.168.0.131:56374 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.3.1.0: 1 [SNMP Version=One]
635471746369877094,24-Sep-14 4:57:16 PM.987,SNMP Trap Received: Origin=192.168.0.131:56375 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.2.0: 1 [SNMP Version=One]
635471746373857094,24-Sep-14 4:57:17 PM.385,SNMP Trap Received: Origin=192.168.0.131:56376 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 1 [SNMP Version=One]
635471746377487094,24-Sep-14 4:57:17 PM.748,SNMP Trap Received: Origin=192.168.0.131:56377 -> Destination=192.168.0.164:162 Variables=1.3.6.1.4.1.21581.1.1.2.2.1.0: 0 [SNMP Version=One]
```

Figure 26 - Communication Log file for a SNMP device, showing received Traps

Deployment and Lifecycle

An important part of any mission critical system is the depth of experience in deployed use and the ability to manage the lifecycle of deployed installation.

- **Pre-deployment Engineering** – TASC's Application Department can spearhead or work with the organization's engineering team to develop a plan associated with design and deployment plan for a critical communication management system. TASC Systems has a network of trained dealers and representatives which can aid this process. The typical deliverables are comprehensive system drawings, hardware and software installation plans and on-site installation checklists.
- **Deployment Experience** – TASC Systems has an established history of deployments in mission critical environments. Our installed base includes national level police organizations, state level emergency response authorities and critical transportation infrastructure management. Installations range from ten to hundreds of nodes, from urban environments to the very most remote mountainous regions.
- **Engineering Expertise** – TASC Systems is a domain expert with a 15 year history in the industry. TASC manufactures all siteRSM RTUs and develops software in North America. Manufacturing follows strict Restriction of Hazardous Substances (RoHS) and International Organization for Standards (ISO) processes.

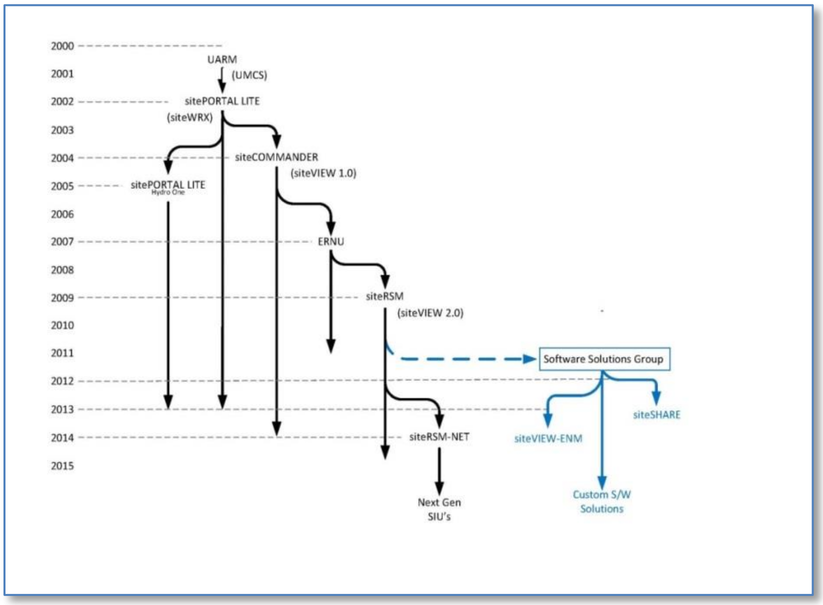


Figure 27 - TASC Systems Legacy of Engineering Experience

- **Support Infrastructure** – TASC offers a complete spectrum of services to ensure that your critical communication monitoring system is always in an optimum state. Service level agreements (SLAs) are available to help manage product repairs and technical support requirements. Technical support, with an experienced team, is available by phone or email. Supplemental engineering services are also available.