WHITE PAPER

SNMP I/O Devices Make Monitoring Environmental Conditions Easy

Austin Lin

Product Manager

Wayne Chen

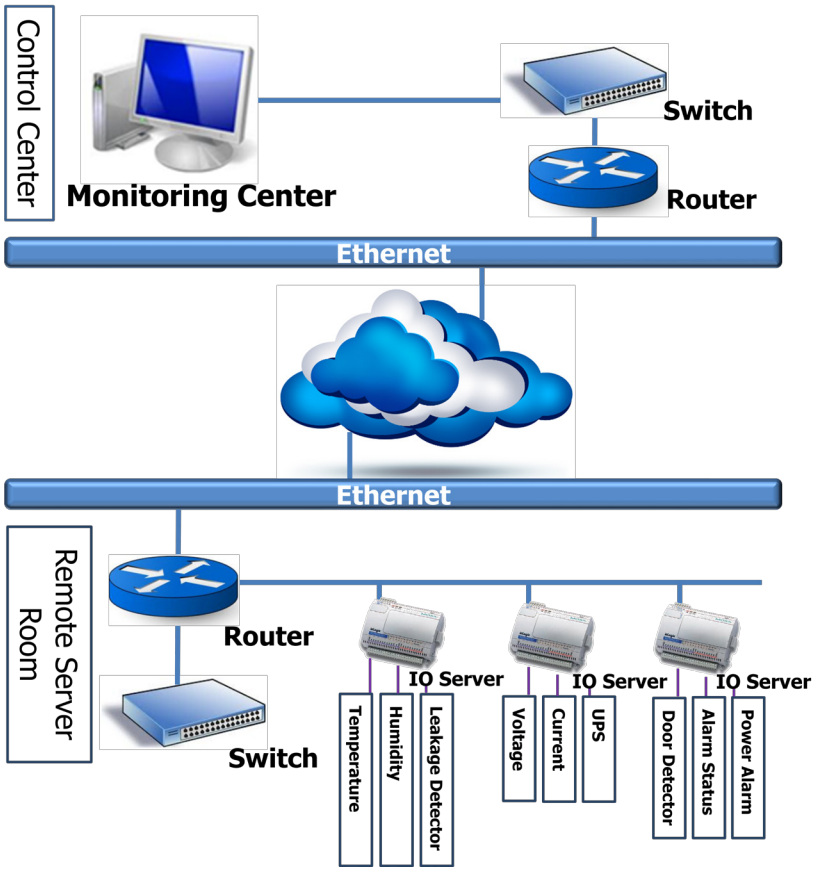
Technical Service

Moxa Inc.

Overview

According to the US Census Bureau's 2012 Statistical Abstract there were more than TWO MILLION cases of burglary and vandalism at unmanned remote sites from 2009 to 2012, with damage averaging at about US$2100 per incident.

Some methods currently used to monitor unmanned remote sites are not very practical, and could result in potential threats being ignored. As the equipment used in sites have evolved and become more complex, it is not enough to simply monitor the equipment; we should also pay attention to aspects of the surrounding environment such as temperature, humidity, airflow, power, and smoke.



To enhance onsite security and monitor equipment status at remote infrastructures, some IT administrators have used an alternative way for environmental monitoring that incorporates network management software (NMS) with a proprietary SCADA system. However, due to lack of functionality and interoperability with other systems, these solutions were costly and generated complex management implementations. Using a multitude of management systems and network-related commands made managing and maintaining these systems extremely difficult. In addition, IT administrators also needed to take the time to learn a totally different protocol such as Modbus.

Released on October 1, 2012

Moxa manufactures one of the world's leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial boards, embedded device servers, and remote I/O solutions. Our products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact Moxa

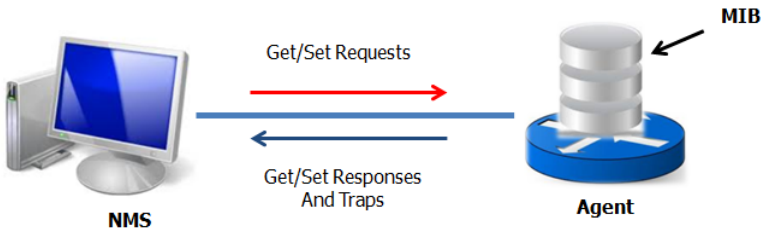
Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

What is SNMP and why use SNMP for environmental monitoring?

This paper will first explain what SNMP is, why you should use SNMP for environmental monitoring, and then discuss how an SNMP environmental monitoring device will help ease the management and implementation process. Lastly, we will give a real life application and then address how Moxa's SNMP supported I/O devices will help you easily set up your environmental monitoring system.

SNMP is a standard application protocol used for collecting information or configuring network devices such as routers, switches, servers, and environmental sensors (for temperature, humidity, etc.). Today, the third generation of SNMP is the standard for network management.

An SNMP-enabled network consists of a Network Management Station (NMS), agent, and Management Information Base (MIB). For the NMS to communicate with its agents, each SNMP agent will include its own MIB file, which is a text file that includes a collection of all the managed objects. The MIB file defines a set of hierarchically organized characteristics associated with the managed objects, such as the object identifier (OID), access right, and data type of the objects. After the MIB compiler converts these text-based MIB modules into a format usable by the NMS, the NMS can start to read or write the managed device using different commands to obtain device-specific information.



The NMS uses three basic delivery mechanisms to exchange information with an SNMP agent: First is the "GET" command, which allows the manager to request information for a specific list of objects. Second is the "SET" command, which allows the manager to request a change in the value of a specific variable. Lastly, the SNMP "TRAP" allows the agent to inform the manager of significant events. Most of the messages are issued only by the NMS. Only trap messages are initiated by the agent, and are typically used to notify the NMS of an alarm condition—before the NMS queries that object.

Since SNMP was first developed, three versions have been introduced by the Internet Engineering Task Force (IETF). SNMPv1 provides the bare minimum of network management functions and processes required to define network management information; however, it has security defects. SNMPv2 is compatible with SNMPv1, has extended features such as the ability to retrieve data in bulk rather than individually, allows the NMS to acknowledge trap message, supports other data types such as Counter 32, and provides various error codes, allowing it to distinguish errors in greater detail. SNMPv3 goes even further by encrypting the communication strings used to access agents and the SNMP data transmitted between devices.

Why use SNMP for environmental monitoring? Over the last decade, SNMP environmental monitoring has become critical for any company with a large network. As any IT company can tell you, it is hard for network administrators to remotely manage a large network that is not confined to a single area. Most of the time, these sites are isolated and not conveniently accessed or reached by foot, making it impractical to station a person onsite to monitor everything that happens. SNMP environmental monitoring employs the Master-Agent concept to transmit messages between the central alarm master and its agents at each network site. Furthermore, SNMP protocol is a familiar IT protocol for network management. By enabling SNMP for environmental monitoring, the IT administrator won't need to take the time to learn another protocol and can easily monitor not only the network but the environment of the system.

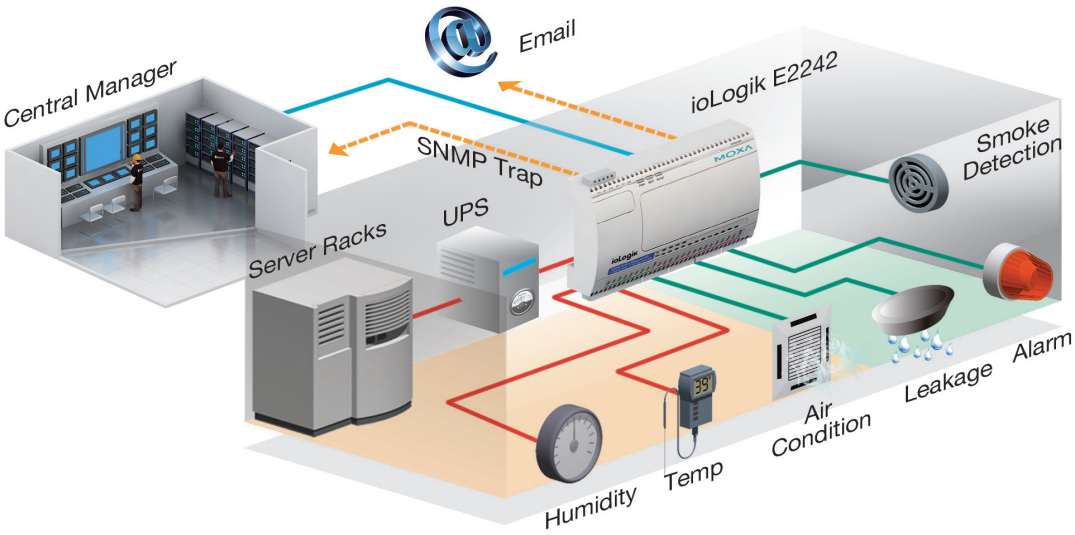
What are the benefits of SNMP environmental monitoring devices?

As the world continues to advance and business efficiency becomes more and more dependent on connected computer systems, ensuring the reliability, performance, and security of the monitoring devices has become absolutely necessary. What are the benefits of using SNMP environmental monitoring devices?

- **Cost savings and easy integration with an existing NMS**
  Normally, integrating a non-IT system into an IT system will increase the overhead on processing and network elements, but by using an SNMP-supported environmental monitoring device, IT administrators can quickly and painlessly integrate these SNMP-supported devices into their existing NMS. And because it uses the same protocol, IT administrators would not need to spend much time to familiarize themselves with network monitoring extensions after integration, and the process will not increase the amount of overhead.

  Integrating the environmental monitoring system under a single SNMP platform will not only enable growth and platform independence, but will also allow the entire system to be controlled by a single, centralized NMS. While larger IP networks may require SNMP proxies to minimize WAN-based SNMP traffic, the reduction in the number of NMSs compared to other alternatives will enable IT to focus on other issues and to simplify the management network.

- **Fast response with event-driven monitoring system for your assets**
  Implementing an effective environmental monitoring system to protect these remote sites will drastically reduce the workload of the administrator to manually monitor the condition at individual remote site. SNMP trap is event driven, allowing the administrator to custom define alarm traps, which the administrators can respond to immediately in response to abnormal or critical events. The ability of the system to inform an NMS, and ultimately the administrator, of the safety conditions, will result in an increase in remote site safety and reduction in system failure.



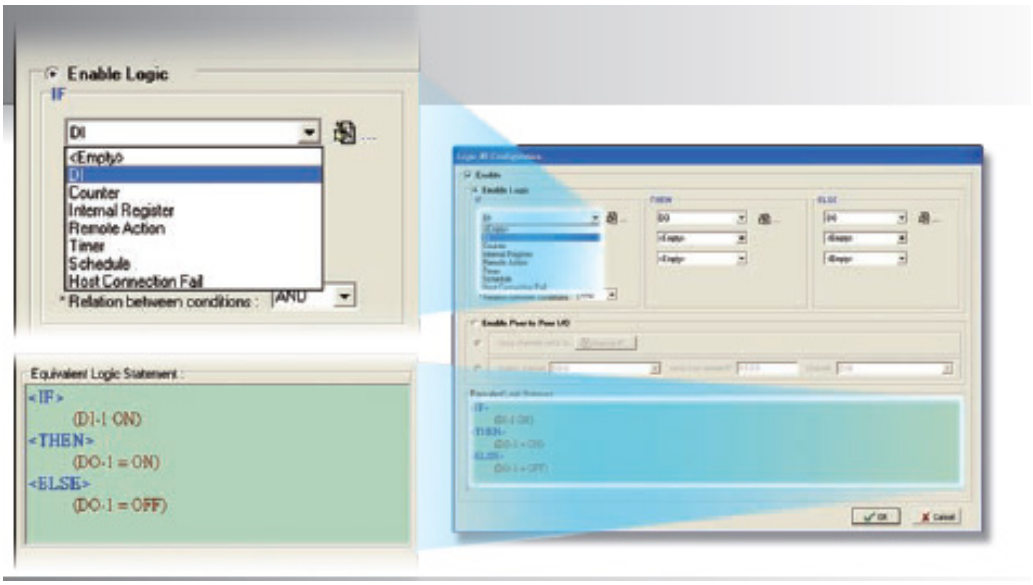
- **Privacy/security issues resolved with SNMPv3 encryption**
  By and large, administrators need a functioning network management protocol even when major portions of the network and its services are impaired. With SNMPv3's incorporated security and administration mechanisms, SNMPv3 is able to work independently of any other network services for the secure transmission of SNMP messages.

  With SNMPv3, administrators are protected from the following threats:
  - Masquerade (data origin authentication): interloper assumes the identity of a sender to gain its privileges.
  - Modification of information (data integrity): alteration of in-transit messages.
  - Modification of message stream: messages are re-ordered, delayed, or replayed
  - Disclosure (data confidentiality): privileged information is obtained via eavesdropping on messages.

Data from SNMP devices can be collected securely without fear of tampering or corruption. Confidential information such as SNMP Set command packets that change a router's configuration can be encrypted to prevent the information from being exposed on the network.

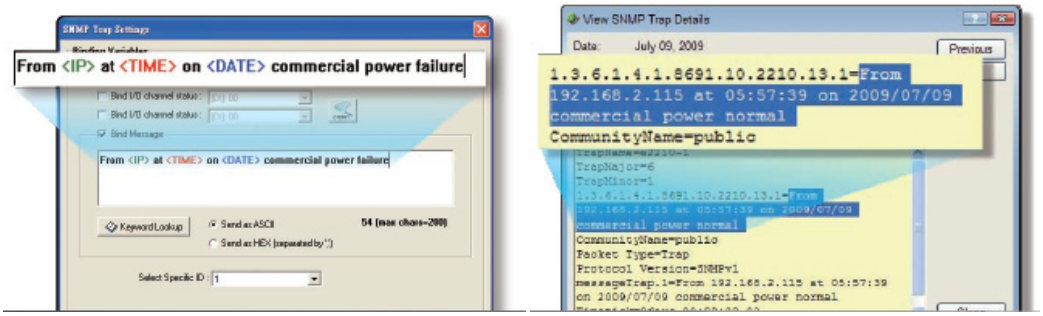
Moxa's Click&Go™ offers value-added user-control capability

In addition to these benefits, Moxa also offers its patented programming tool—Click&Go™. Moxa's Click&Go™ control logic grants administrators unparalleled control over the behavior of their I/O devices, without involving third-party development tools or complex code. With Moxa's Click&Go™, various user-defined events can be configured through the intuitive IF-THEN-ELSE logic for local control to send various types of alarms, including TCP/UDP messages, emails, SMS messages, and SNMP traps. For example, to configure a fire alarm, just select *"IF" DI fire alarm is ON "THEN" DO buzzer ON "ELSE" DO buzzer OFF*. And then click, click, click, you're done.



Programming-free Click&Go I/O Control Logic

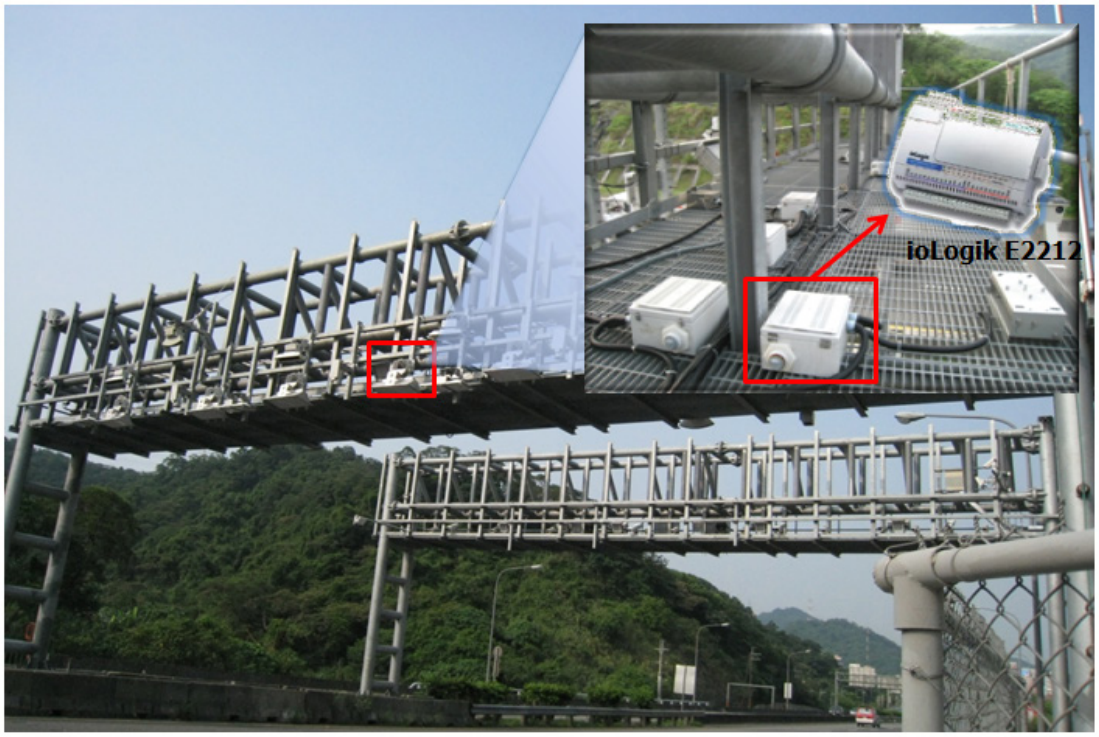
The traditional disadvantage of using SNMP traps is the limitation of the information conveyed. With only seven standard trap numbers available in SNMP, it can be difficult to tell what is happening just by looking at the traps. Moxa's Click&Go™ gives the users the flexibility of defining SNMP trap formats, which allows variable binding, and adds more information to each SNMP trap. For example, an SNMP trap that is triggered when a door sensor is tripped can include the message ""Intrusion Alert," plus date, time, and server name."



User Definable SNMP Trap Content

Real life application: ETC system on a highway

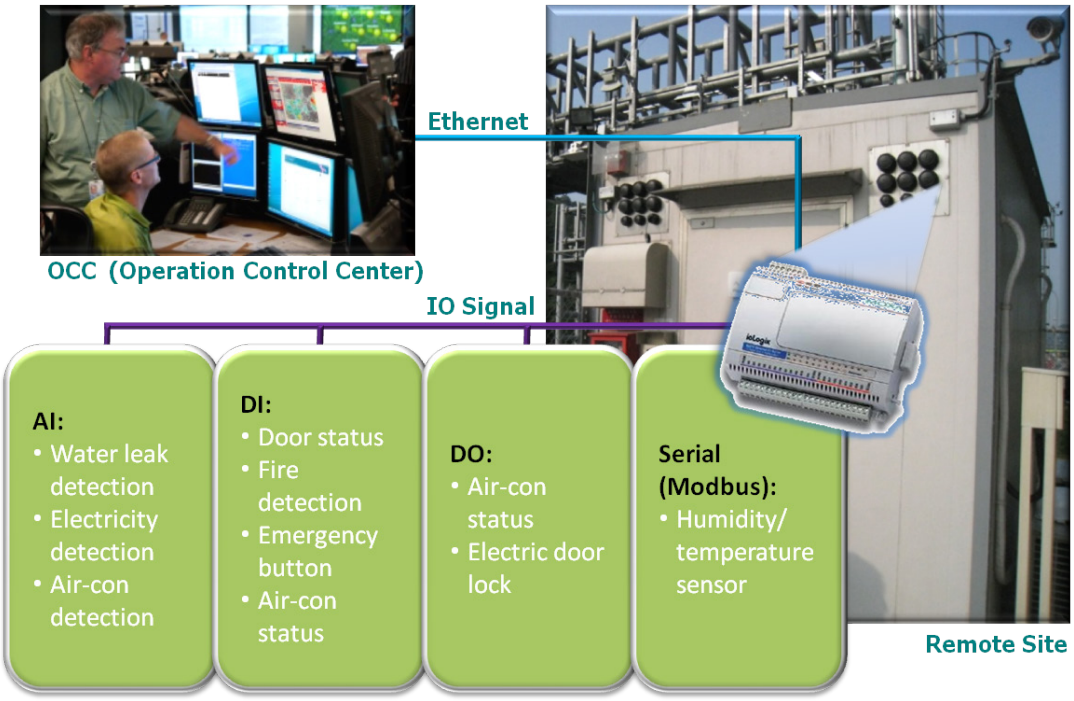
Both for environmental reasons and to control traffic jams, countries all over the world are implementing unmanned ETC systems throughout the major highways in their cities. These tollgates are equipped with laser detectors to monitor vehicles by identifying the size of the vehicle, and generating a pulse output to trigger different cameras to take snapshots. The ETC tollgates help regulate highway traffic by smoothing out the traffic flow and reducing gas emissions.



ETC Tollgate System

Thousands of ETC tollgates are being installed on highways around the globe, and to help with monitoring and maintaining the tollgates, some system integrators are choosing Moxa's products.

The ioLogik E2242, for example, is an environmental monitoring device that can monitor ETC tollgates via the Ethernet. In addition, the ioLogik E2242 provides local control capability, an AI channel to detect water leaks, electrical conditions, and monitor the status of air conditioners, and uses an RS-485 interface for temperature/sensor monitoring. Furthermore, Moxa's Click&Go™ logic offers a straightforward "if-then-else" local control capability, giving users the flexibility to define different traps to customize their front-end control capability.



Moxa's Intelligent SNMP Solutions

Moxa's ioLogik E1200 (non-programmable), E2200, E4200, and W5300 series of intelligent SNMP environmental monitoring devices allow you to easily monitor your telecommunication infrastructure environment and remote sites. These devices are specifically designed for information field applications that use the SNMP protocol for monitoring environmental conditions (temperature, humidity, airflow, door, and intrusion) with programming capability and multiple alarm notifications that include email, SMS text messaging, and SNMP traps.