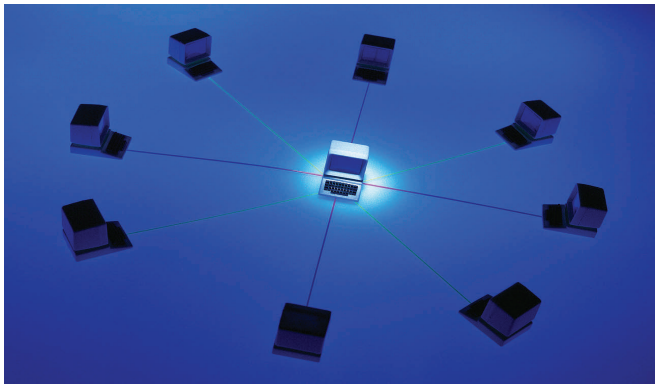
Volume 1 Issue 3 February 2008

SEMAPHORE
a CSE-Global Group Company

Good Fortune for 2008

Asia & Oceania

SNMP—Advantage to RTU's



Definition

The acronym SNMP stands for **S**imple **N**etwork **M**anagement **P**rotocol.

SNMP is an application layer protocol which has been widely accepted by the IT community as a platform for the monitoring and management of a wide range of network attached devices.

From a high-level perspective, SNMP as a management model consists of:

- At least one, but generally many, devices or nodes that contain an SNMP application component that exposes elements of it's configuration or operation for management through the SNMP protocol – These nodes are traditionally referred to as **agents** and comprise those elements of the network subject to monitoring and management using SNMP. From a more traditional SCADA perspective, these agents could be referred to as SNMP slave devices.

- At least one, but potentially more, SNMP agent that is capable of initiating management commands and or receiving monitoring notifications from other devices – A node of this manner is traditionally referred to as a **manager**. From a more traditional SCADA perspective, these agents could be referred to as SNMP master devices.

This architectural model in turns permits the management and monitoring of network attached devices by the direct polling and query of an SNMP agent by a manager, or the asynchronous receipt of a monitoring notification, referred to as a **trap** (or as an exception report in more traditional SCADA terms) by an SNMP manager from an agent.

The configuration or operational elements that are exposed to monitoring or management through the SNMP protocol are typically referred to as objects – The list of these objects, typically referred to as a **mib** (or **management information base**), available within a given SNMP device is highly variable and while there are some "standard" recommendations with respect to configuration items that should be made available for any given device, there is absolutely no mandate for this to be the case. As such, when interfacing to a new device using SNMB, the first level of information that is generally sought is the device mib file that lists and describes the SNMP objects of the device.

Features

The implementation of SNMP on Semaphore RTUs consists of:

- **SNMP trap** – This implementation permits the RTU to receive and generate SNMP trap messages from and for dispatch to other devices respectively.

- **SNMP daemon protocol** (SNMP slave) – This implementations permits the RTU to be interrogated and queried by other SNMP devices to discover configuration and operational information about the RTU including network address, installed hardware, event logs and network interface and traffic information.

- **SNMP client** (SNMP master) – This implementation permits the RTU to query, retrieve and set object information in another device using SNMP. The object can be defined as a variable of any type in a device.

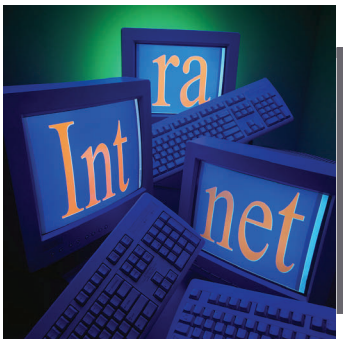
Benefits

The primary benefit that SNMP offers end-users of Semaphore RTU technology is that it opens new opportunities to extend the reach of monitoring and control – Through the use of SNMP, the Semaphore RTU can query, monitor and manage the status and operation of SNMP devices, removing the requirement for multiple monitoring systems within IP networks, where deterministic control is required for business processes. Moreover, Semaphore RTUs using SNMP can extend the reach of existing SNMP managed networks providing access to physical contacts and I/O states in a manner which is a natural extension to the existing operation of the network.

In short the inclusion of SNMP in Semaphore RTUs provides a strong value proposition for the extension and addition of existing telemetry and IP networks, simplifying and removing the duplication that can exist in device monitoring and management between these realms.

Rob Casey

Research and Development (R&D) Director



Inside this issue:

Cyber Security for SCADA

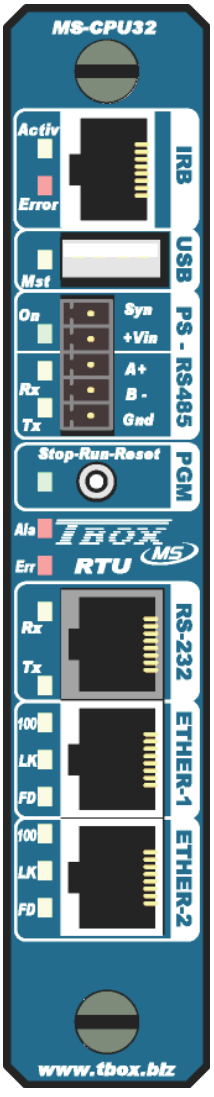
Semaphore on Display
TBox
Lite & MS products.
Kingfisher
Series II and KF Plus
CP30, G30 & Wireless
I/O G3

CSE-Semaphore has joined the Industrial Defender Enabled Partner Program. As an Industrial Defender Enabled partner, Semaphore offers the industry's first RTU product lines, T-BOXand Kingfisher, to fully support cyber security protection for SCADA networks.

T-BOX is the first, IP-based telemetry solution that enables the complete integration of SCADA, control, and communications functionality in one rugged package. It leverages easy-to-use Web technologies and inexpensive public networks for decentralized, monitoring and control systems. T-BOX products offer up to 50% less total installed cost per point versus traditional SCADA/ PLC systems and permit greater organizational access to data through automated reporting and browser software.

The Kingfisher RTU line provides many advanced features for SCADA system solutions, including redundant configurations, intelligent I/O, and open programming that is compliant with IEC 61131-3. Kingfisher is also the first RTU product line that is compliant with IEC 61499, the distributed processing and interoperability extension to IEC 61131-3. Kingfisher systems are well suited to large, demanding measurement and control applications that employ central stations.

Semaphore is collaborating with the only company in the industry dedicated and uniquely focused on providing end-to-end Defense in Depth™ cyber security solutions for the real-time process control / SCADA market. Users benefit by leveraging Industrial Defender's 2 comprehensive Defense in Depth™ approach to cyber security, which includes network security professional services, cyber security technology, and managed security services.



NEW 32 Bit TBOX CPU

Semaphore has added a 32-bit CPU SCADA software module to T-BOX line of RTU SCADA system products. The new MS-CPU32 is compatible with the T-BOX MS Modular System and offers up to 100 times the performance of current T-BOX processors.

Based on a 505 MIPS PowerPC processor, the MS-CPU32 uses a Linux core, includes two Ethernet ports and supports up to 16 serial ports in a T-BOX MS installation. The MS-CPU32 additionally supports processor redundancy. Two MS-CPU32 CPU modules can be installed in a T-BOX MS rack and operate in a Primary/ Backup configuration. T-BOX MS also allows redundancy in power supplies and communications ports.

The significantly higher performance of the MS-CPU32 brings advantages to a broad range of automation applications. In a test run by a U.S.-based systems integrator, the MS-CPU32 executed a filter backwash application program on a loop time of 8 milliseconds vs. a one-second loop time using the 16-bit CPU, representing an improvement of more than 100 times.

The MS-CPU32 also supports sequence-of-events (SOE) recording with a resolution of one millisecond. Information stored with millisecond resolution can be displayed in tabular and trend chart reports as well as in SCADA screens generated by Semaphore WebForms software. Millisecond resolution is also supported in alarm reports, which a T-BOX MS can send to multiple recipients via e-mail. 2 Applications programs, which were developed for use with the T-BOX 16-bit processor, can be converted for use with the MS-CPU32 by simply clicking on a "Tools – Conversion" dialog box in Semaphore's TWinSoft SCADA software programming environment. The MS-CPU32 is compatible with TWinSoft version 10.00 or higher.

The robust packaging for this module is designed for industrial applications in harsh environments. The MS-CPU32 operates over a wide temperature range as well as in areas, which experience high vibration and radio frequency interference.