Considerations for Multichannel Signal-Integrity Monitoring

By David Strachan and Orest Holyk

Since the publication of SMPTE's S22.02 Advanced System Control Architecture Working Group's Summary Report in May 2000, much has been written and discussed on the subject of monitoring and maintaining video and audio quality in both digital and transitioning-to-digital television facilities. In addition, a number of articles on employing various architectures and networking tools within the traditional facility to ensure signal integrity have also been published. This paper examines some of the facility monitoring issues identified by Roger Crooks in the June 2001 SMPTE Journal and reviews some specific issues pertaining to the implementation of SNMP as a multi-channel signal integrity monitoring solution.

There seems to be no limit to the number of specialty channels offered to television viewers worldwide. Along with the expanding number of digital television channels and services, comes an increasing demand on the broadcast engineer to ensure that no information is missing. At the same time, in an effort to reduce operating costs, we are seeing a trend: large television networks are adopting a policy of "centralcasting." This is the process of originating numerous "local" services from a central network operation center (NOC), thereby reducing the number of fully staffed and equipped facilities required at each remote location, but increasing the facility monitoring needs at the central location. This trend parallels SMPTE's S22.02 Working Group finding that "many different organizations within the broadcast industry have already recognized the need for a comprehensive control and monitoring environment for studio equipment."[1]

By reviewing the radical changes taking place in our industry, we can appreciate that only a radical solution will satisfy broadcasters' facility monitoring needs. As a result of these changes, it is no longer practical for any single person to simultaneously monitor video, audio, and metadata on every channel. What is required is an automatic system that activates an alarm if one of the services, or a component thereof, is missing or has developed a fault. We need to know precise details of where the error has occurred and what exactly is wrong, so that corrective action can be taken while maintaining high-quality levels of service.

Roger Crooks[2] identifies a facility monitoring strategy as a key strategic factor in the transition to a networked operation. With the transition-to-digital era upon us, we must be concerned not only with signal quality, but also with the continuity of the video and multiple audio channels, as well as VBI data associated with each channel, regardless of the number of television channels. Traditionally, the task of monitoring channels has required a plethora of gadgets specifically designed to check each function. But even with the best equipment, it is difficult to watch up to 100 picture monitors and impossible to monitor the levels and phases of hundreds of audio channels. Crooks states that "…in the past there were racks of equipment, such as waveform monitors, checking the actual signal [while] today with digital signals, signal monitoring is of limited use. However, tracking the health of the equipment that stores and moves these signals is critical." Not surprisingly, during recent facility visits a number of questions from end-users regarding possible facility monitoring strategies arose; most decision-makers are addressing their monitoring needs and are also looking at implementing networked monitoring solutions.

Local and Remote Facility Monitoring

Although a remote monitoring solution centralizes operations, offering remote configuration, automatic alarming, and data logging, it is the localized equipment that monitors signal integrity and reports information to the central facility through a network. Considerations for local signal monitoring should therefore include the following parameters (Fig. 1):

- Video continuity (video presence, video not black, video not frozen, and EDH errors if the complete chain is EDH-enabled).
- Audio continuity (audio volume too high or too low, phase reversed, and balance).
- Data continuity (closed captioning presence, V-chip parental guidance presence, time stamps, and source ID presence).
- Signal path integrity or signal strength especially when using fiber for long-haul transport.

In addition, audio monitoring itself presents further considerations in handling capabilities, especially with various "flavors" of audio including stereo analog, AES/EBU, embedded, Dolby E, Dolby-D or AC-3/5.1 within the facility. In transitioning facilities, a number of audio formats may be in use at a particular time requiring monitoring equipment to be versatile. An interesting dilemma arises for the equipment monitoring surround sound: if audio becomes silent on the two rear channels while still present in general, should this trigger an audio

A contribution (2001-10) received on Sept. 5, 2001.
David Strachan and Orest Holyk are with Evertz Microsystems Ltd., Burlington, Ont., Canada, L7L, 5Z9.
Copyright © 2001 by SMPTE.

alarm? Perhaps!

Crooks offers an effective facility monitoring strategy of first addressing the big picture to understand a facility's workflow. Subsequently, local and remote signal monitoring follows with the identification of key operation or demarcation points within the facility's broadcast chain. Analyses of the "smaller picture" by identifying these demarcation points are critical to the implementation of a monitoring solution, especially to maintain signal integrity and service quality.

Remote Monitoring Market Trends

If recent observations hold true, then it appears that the unofficial trend toward a networking communication protocol standard, for remote signal health-status monitoring and reporting between equipment and a central location, is the use of simple network management protocol (SNMP). From a facility monitoring, signal-integrity perspective, this appears to be the preferred route because it is a proven solution, offering simple network strategies, and is a widely available, open standard.

Again according to Crooks on SNMP, "by consolidating all monitoring at a central location, it is easy to determine the condition of all the equipment in a facility. Being a network-based protocol, this can also be used to monitor systems at remote locations and other facilities." For similar reasons, SNMP has been employed in the telecommunications industry for many years, and the increasing complexity of the television industry along with the need for a networked reporting tool also makes the adoption of SNMP techniques a truly worthwhile pursuit in broadcasting.

Simple Network Management Protocol (SNMP)

SNMP is an open standard computer network protocol developed by the Internet Engineering Task Force (IETF) that enables different devices sharing the network to communicate with each other. For monitoring video, audio and data, we need a local detecting device that automatically reports all errors detected to a central alarm and error logging station; the ability to interrogate the detector from the central station to determine the status of any signal to be monitored; and to configure devices in the network and receive feedback that our instructions have been carried out. Finally, we need to enable our monitor and control tasks from a networked computer terminal anywhere in the world. All of these requirements can be accomplished by using SNMP as shown in Fig. 2.

There are three basic components to SNMP:

- Managed objects, each with unique addresses (OID), which communicate with the network management system (NMS) through an "agent."
- A virtual database that lists all the unique variables (managed objects with unique addresses) being monitored and which both the agent and manager understand—referred to as the management information base (MIB).
- A network manager referred to as the network management system (NMS).

Each managed object (a product or device with device features/variables) has a unique address. These unique addresses are known as object identifiers (OID). Each enterprise (company) subscribing to the SNMP system, is provided first with a unique OID for the company, then allocated a unique OID to each of its SNMP-enabled managed objects. The SNMP Management Information Base (MIB) is a virtual blueprint of the assigned OIDs and serves as the common dictionary between SNMP components. A unique string of characters, preceding the instruction, steers the command to the intended device. This string includes a numerical representation of everything from the standards organization, which issued the numbers, to the target device in the system. Subsequent managed object OID characters for enterprise equipment will locate the required device and specific parameters within that device.

Get, Set, and Trap

A simple set of instructions is used in the SNMP system to facilitate communication between the manager and the managed devices. These are Get, Set, and Trap. In the case of a facility monitoring system, a Get command, as the name implies, is used when the computer wants to get the status of some variable at the monitored end, usually at a specific demarcation point. The SNMP-enabled monitoring device will respond with the requested value. A simple Get process is shown in Fig. 3.

Similarly, the Set command is used when the computer wishes to set a parameter value at the monitored end. For example, there may be a need to set a silence detector to -50 dBm instead of -55 dBm. Finally, the monitoring device autonomously sends a Trap message when a condition has changed. In most cases, Traps are associated with fault condition alarms, which are detected by the localized monitoring equipment.

As Crooks writes, "if a fan dies, a message will be sent over the network to the monitoring workstation." True, but in order for an SNMP network to report on a monitored parameter, that parameter must first be coded into the MIB or virtual blueprint of parameters. For example, if the chassis fan dies, a chassis MIB must exist so that the event can be reported to the NMS and eventually the end-user. Subsequently, when looking at an SNMP monitored system solution, a strategic list of key parameters to monitor and control should be identified by the end-user prior to implementation.

SNMP Simplicity and Security

With increasing demands on facility transition, one of the greatest limitations facing facility managers is time—time to plan, design, and imple-

ment equipment into a modern facility. With many factors, (mandates, budgets, legacy assets, and personnel) to consider, implementation delays due to complicated monitoring and control solutions are likely the least desirable. Therefore, decision-makers search for simple, cost-effective solutions to meet their needs. An effective, networked monitoring solution is possible with SNMP, but is still far from simply being "plug-and-play."

In addition, as should already be obvious, the "S" in SNMP is not an acronym for "secure." Apart from community strings present with SNMP data packets, there are no additional security measures in place, such as encryption, to protect information travelling over the SNMP network. This may not be a particular problem for a facility employing a private, local network where security concerns are limited to login passwords.

However, the lack of security could pose a problem if the SNMP packet is sent over IP from a remote location to a central facility. Furthermore, beyond the LAN, consideration for the use and configuration of firewalls is necessary in order to accept SNMP packets from remote locations. Efforts by standardizing bodies are under way to implement a more secure version of SNMP without increasing the complexity of this protocol.

Equipment Interoperability

Another key consideration for a remote facility monitoring strategy is equipment interoperability. This issue is not only economically important when considering the re-employment of legacy equipment assets, but also operationally important when attempting to consolidate operations under one control system. It is also important to realize that neither may be possible. As identified by the S22 Working Group, "due to differing product lines and market direction, each of these systems will have likely been derived from a different set of requirements." Product differentiation has always been used by competitors to gain the upper hand with end-users, but when considering a facility monitoring system, ideally one manager should be interoperable with third-party equipment as it is definitely not feasible or practical to use additional managers.

A common issue with today's SNMP network management and control system offerings can be summarized by the "too many chiefs" analogy. Most third-party equipment manufacturers offer some form of SNMP manager (NMS) with minimal differentiation, creating considerable confusion for the end-decision maker about which is the best to implement. For manager developers, selling a manager is very attractive as it not only serves as the "brain" for facility monitoring but also is a lucrative revenue generator. However, end-users are in a quandary for several understandable reasons. They are unsure which managers offer the most robust solution, which interfaces the best with all third-party equipment—either legacy and/or new—who is responsible for fixing interface and/or equipment problems when they arise, and which manager developer will continue to support the product for the long term.

To ease the burden of making a hasty decision, a common solution employed by many facilities has been HP OpenView (Network Node Manager). For those facilities with some IT experience, this offers all SNMP networking tools and the convenience of experimentation without the cost of installing customized SNMP application software or the hassle of complicated equipment set-up. This "diagnostic" tool also allows facilities to test potential user interfaces not only for problem-solving engineers and technicians who require in-depth information and statistics about monitored signals, but also for frontline operators who need simple user-friendly GUIs for immediate problem identification and solution implementation.

Furthermore, equipment interoperability efforts among third-party equipment manufacturers are under way. As reported by Ken Kerschbaumer in *Broadcasting & Cable*,[3] Harris has initiated a connectivity partnership of at least 18 third-party equipment manufacturers, including GVG, Sea Change, Snell & Wilcox and Evertz. Harris's central-casting focus unites a number of third-party equipment manufacturers with specialties throughout the broadcast chain, ensuring that connectivity works through their Brain approach.[4] Similarly, other partnership efforts have been initiated with third-party SNMP manager developers to proactively develop SNMP communication interfaces, thereby offering end-users a proven solution for local and remote facility monitoring.

The Threat of Too Many Alarms

As with the boy who cried wolf too many times, over-alarming, especially for noncritical events, will render a newly-implemented, networked facility monitoring solution useless as operators begin to ignore subsequent alarms. Receiving too many frivolous alarms should be avoided through good NMS control, with the ability to identify which alarms are critical while filtering noncritical "noise." It is important to be able to predetermine and set an acceptable threshold and time duration, which may be tolerated, before initiating an alarm. There is no need for an alarm every time the star of a show stops talking, but if there is no audio for 30 sec, one should sound.

There are several forms of an alarm. Crooks identifies the possibility of SNMP alarming technicians or repair people via e-mail, pager, or cell phone notification; however, the primary alarm is still destined to a manned, centralized facility in the form of a trap. Frontline operators can acknowledge the alarm, switch to a backup signal and take the problem off-line without any downtime. The faulty signal is then addressed and repaired by a technician, without the customer ever noticing or complaining. Off-line notification for repair and maintenance through e-mail or pagers becomes a

user-definable, secondary function, and is only effective if it fits the facility's workflow.

Conclusion

SNMP is an effective tool for monitoring both incoming and departing signals from local signal monitoring equipment located at strategic locations throughout the video enterprise network. If there are no problems, no alarms are raised. However, when a problem exists, an alert is sent through the SNMP network notifying the operator and in effect acting as your "eyes and ears" in our ever-expanding digital television universe!

References

1. SMPTE Engineering Committee Report, S22.02 Advanced System Control Architectures Working Group, "System Overview," *SMPTE J., 109*:363, May 2000.
2. Roger Crooks, "Considerations for Moving to a Video Server Based Facility," *SMPTE J., 110*: 377, June 2001.
3. David Strachan, "Continuity Monitoring of Audio, Video and Data in a Multi-Channel Facility," Evertz Catalog 2001, p. 211.
4. Ken Kerschbaumer, "Harris-Putting the BRAIN Behind Centralcasting," *Broadcasting & Cable, 56,* July 23, 2001.

Figure Captions

Figure 1. Signal integrity monitoring through local on-screen display.

Figure 2. Simple SNMP network setup with local monitoring and demarcation points.

Figure 3: Simple Get.