Continuity Monitoring of Audio, Video and Data in a Multi-Channel Facility
David Strachan
Evertz Microsystems, Ltd.

Much has been written on the subject of maintaining video quality in a modern television facility. But with often as many as a hundred or more television channels to monitor, we must be concerned not only with signal quality, but also with the continuity of the video, multiple audio channels, closed captioning, V-Chip parental guidance and other VBI data associated with each channel. The task of monitoring so many channels, often involves employing a plethora of gadgets specifically designed to check each function. But even with the best equipment, it is difficult to watch up to a hundred picture monitors and impossible to monitor the levels and phases of hundreds of audio channels. And then what do we do about the closed captions, XDS and other data on every channel?

This paper describes a system using in-line video and audio converters, to automatically monitor signal continuity, at the same time as reporting video errors (including EDH, frozen video and black), audio levels and phases, closed captions, V-Chip parental guidance, source identification and time information. Any errors discovered, are automatically flagged over a TCI/IP network and may be logged in a database. A remote monitoring and control system, based on the common SNMP protocol, is described.

The Challenge
There seems to be no limitation to the number of specialty channels being offered to television viewers around the globe. Along with these ever expanding services, comes an ever increasing load on the broadcast engineer to ensure that no information is missing on any of the services within his demarcation area of responsibility. The engineer must be always cognoscence of management’s desire to increase the number of viewing choices without increasing engineering resources.

If we take a step back and look at the radical changes taking place in our industry, we can appreciate that only a radical solution will satisfy these needs. It is no longer practical for any single person to simultaneously monitor video, audio and all of the metadata on each channels. What is required is a completely automatic system, which activates an alarm if one of the services is missing or has developed a fault requiring attention. We need precise knowledge of the error condition, before dispatching a service engineer with the appropriate skills and tools, to rectify the problem. When all channels are functioning normally, there should be little need for human involvement.

Let’s take a closer look at the parameters we need to examine in each television signal:

**Video continuity**
- Video present
- Video not black
- Video not frozen
- No EDH Errors
Audio Continuity
- Volume too low condition
- Volume too high condition
- Phase reversal condition
- Good audio balance

Data Continuity
- Closed Captions present
- V-Chip Parental Guidance information present
- Time stamp present
- Source ID present
- Special service VBI data present

In each case we need to be able to predetermine an acceptable threshold and time duration, which may be tolerated, before initiating an alarm. (We don’t need an alarm to sound every time the star of a show stops talking, but if there is no audio for 30 seconds, we really want to know about it).

Multiple Channels and Multiple Locations
In today’s broadcasting networks, the chief engineer is often charged with the responsibility for monitoring program continuity at multiple venues and for ensuring that all signals which may be handed over to another carrying company, are complete and free from errors. Demarcation points, separating areas of responsibilities, must be clearly defined, and monitoring systems must be in place at these boundaries, to ensure that no disputes can arise over who’s equipment is responsible for generating errors. A remote monitoring system must be capable of producing a continuous log of errors found on all channels at all locations.

An effective solution to these problems may be realized by employing SNMP methods, as described in the following paragraphs. With a suitable system in place, the engineer will have the tools he needs to identify a problem, note the time that it occurred and the corrective measures taken. If so desired, switching gear can be automatically actuated, to by-pass faulty circuits.

SNMP
For the reasons described above, the computerized Simple Network, Management Protocol (SNMP) has been employed in the telecommunications industry for many years. The increasing complexity of the television industry, makes the adoption of SNMP techniques a truly worthwhile pursuit in broadcasting too.

SNMP is a standard computer network protocol, which enables different devices sharing the network, to communicate with each other. For monitoring video, audio and data, we need to have some sort of detecting device, which automatically reports all errors detected to a central alarm and error logging station. We also need to be able to interrogate the detector from the central station to determine the status of any signal we wish to monitor. Finally, we need to be able to control devices in the network and to receive feedback that our instructions have been carried out. Monitoring and control tasks should be possible using TCP/IP browsing techniques from a computer terminal anywhere in the world. These tasks can all be accomplished using SNMP.
Figure 1 shows a simple network comprising a computer and three devices. Each of these devices has a unique address known as an Object Identification (OID). Each enterprise (company) subscribing to the SNMP system, will have been provided with a unique ID and the company in turn will have allocated unique IDs to each of its products. The SNMP Management Information Base (MIB), a software package resident in the main computer, knows the OID of every company participating in the system and of every device connected, either directly or indirectly, to the network.

Fig 2. - OID Mapping
Figure 2 shows the communication route between the computer and the device being interrogated. 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. For example the following string for characters, will steer computer commands to an Evertz product - 1.3.1.4.1.6827. Subsequent OID characters will locate the required device. All protocols, have their own vernacular and so with SNMP, there are some new words to learn. Figure 3 will help in the understanding of these functions.

![Manager and Agents Diagram]

The Manager software resides on the main computer, together with all the system MIB information. Between the main computer and each monitoring device, there will be a Transaction Handler controlled by an Agent. These latter terms refer to firmware residing in some controller hardware, which is located with the monitoring device. The Agent and local Transaction Handler may well have the job of handling transactions to and from one or many devices, each having its own unique OID.
GET, SET and TRAP
A variety of instructions are used in the SNMP system, to facilitate communication between the main computer and the monitoring devices. Fortunately there are only a few essential ones to learn. They are; GET, SET and TRAP. A GET command, as the name implies, is used when the computer wants to get the status of some variable at the monitoring end. The monitoring device will respond with the requested value. The SET command is used when the computer wishes to set something at the monitoring end. For example there may be a need to set a silence detector to -50dBm instead of -55dBm. The TRAP message is autonomously sent by the monitoring device when an alarm condition is detected, to trap some piece of error information.

There are many rules governing which signals have priority over others, but the principals of the three primary instructions always apply.

It can be seen that by employing the standard SNMP protocol, products may be monitored and controlled either locally, or at the main computer, or via TCP/IP from anywhere in the world.

Local Monitoring
Although the primary objective should be to offer automatic logging with remote alarms, a complete system should also offer local monitoring. Significant cost savings can be realized if on-screen monitoring is provided, instead of having to install separate audio level meters. Not only can we save space and cost, but the new system will immediately identify the fault, without the operator having to scan through an array of audio level and phase meters to identify the source of a problem. As with many software tools, it should be possible to display or hide audio bar graphs and status screens as required. This avoids the risk of burning the screen.

Monitoring Hardware
To detect and report errors in video, audio and VBI data, we need some hardware, which analyses the digital signals in these areas. The hardware can comprise one or more monitoring detectors and, as described earlier, a firmware Agent talks to the main computer, while a Transaction Handler passes messages to and from the individual detector units.

The following describes a typical system designed by Evertz specifically for this purpose. The system is based on an enclosure with up to 15 plug-in cards. One card is the frame controller card which houses the Agent and Transaction Handler while the other cards (the AVMs), detect any errors in the audio, video or data streams. In addition to their monitoring duties, the AVM cards can also serve as NTSC/PAL decoders, encoders, audio A to Ds and D to As, embedders and de-embedders.

These cards flag errors to the screen, initiate GPI closures and report any errors detected to the SNMP system. Additionally, the devices can key audio level bar graphs, audio phase meters and a host of other status information onto the screen, by activating GPI contacts.

Video and Audio Error Detection
The system checks to ensure that the video is present, but also looks for persistent black pictures and for frozen frames. The status display, as can be seen in Figure 4, provides metadata information identifying the video standard, EDH errors, presence of VITC, SID, V-Chip (PR), Closed Captioning and which audio groups are occupied.

The AVM Encoders have outputs of NTSC or PAL, and 2 stereo pairs of analog audio outputs, derived either from embedded audio or from AES/EBU inputs. On-screen bar graph types may be
selected from a menu (described later). Variations include all the common scales, such as PPM or VU, and various standards of PPM such as BBC, DIN, Nordic N9 and AES/EBU. The colors and opacity of the display may be optimized for appearance and to avoid damage to the CRT phosphors.

![Fig 4 - On-Screen Display](image)

**Metadata Detection**

Many TV stations employ separate Under Monitor Displays (UMDs) to identify sources. These work fine, as long as you can be sure that nobody up-stream switches your signal to a different source. The AVM decodes SIDs, which has been encoded at the source by a Pesa or Evertz source ID encoder and keys it onto the video. If the input signal contains Vertical Interval Time Code (VITC) the card may be programmed to display it on the screen.

AVM cards may also be programmed to decode the line 21 parental guidance rating (V-Chip rating) used in North America and to decode closed captions and display them on the screen. The card can also be programmed to pop a RED message flag onto the screen to notify the operator that closed captions are missing. As with other programmable alarm features, the card may be programmed to close a GPI contact if captions are lost.

Programming the AVMs can be carried out either from card edge controls using a comprehensive on-screen display system, or from a computer over the network or directly to each card using RS232 communications.
Conclusions
The system described, combines NTSC/PAL encoders and decoders and audio digital/analog converters, with a monitoring system designed to automatically alert the engineer only when problems are detected on any of the numerous channels active in today’s multi-channel television facility. The system handles video, audio and metadata. When a fault is detected, a GPI closes and an alarm flag pops onto the screen associated with the impaired channel. The operator may then enable status reports and audio level bar graphs to appear on the screen, for further investigation. SNMP extends control and monitoring, to any location with a TCP/IP connected computer.