DATA INTEGRITY IN ADDRESSABLE CATV SYSTEMS

James P. Ackermann
Director, Field Systems

OAK Communications Inc.
San Diego, California 92127

ABSTRACT

Addressability dictates successful delivery of control data to paying subscribers and to non-paying customers. The ability to supply or withhold programming services is fundamental to economic viability. Yet this unseen control element is often the least monitored. If it does not perform well revenue can be lost. A good fundamental design and diligent application of monitoring and maintenance are required to attain and retain integrity of the control data channel. Many data monitoring techniques are available depending on the distribution system configuration. Persistent testing and designed-in flexibility allow trouble scenarios to be discovered and countered.

INTRODUCTION

The importance of good integrity of the video and audio signals in the CATV operation is quite evident. They form THE PRODUCT for which the subscriber is willing to pay. In a non-addressable pay system another element enters the picture; the scrambling technique. An addressable system adds a fourth element; the control data. For optimum security the data and scrambling subsystems are integrally related to each other. They serve to control the delivery of the product to the customers.

Scrambling and data are not elements paid for by the subscriber for his gratification. They are there only to serve the operator. Functioning satisfactorily, the customer is at best unaware of their existence. Malfunctions can only be a detriment to his satisfaction by interrupting his paid services. When a malfunction of the data system fails to withhold services from a nonpaying viewer, lost revenue occurs. Customer complaint monitoring serves only as a gross check of performance to paying customer. However viewers receiving free services are unlikely to complain, so additional monitoring measures are required.

TECHNICAL DISCUSSION

The Control Data System

The ability to supply or withhold "the product" upon command is a fundamental requirement of an addressable system. Thus control over the descrambling decoder is the control data system's primary purpose. Interface to a business system for billing purposes and control of pay features and other services are ancillary functions.

In its broadest sense the data system (Fig. 1) consists of the business system controlling a data channel which controls the scrambling system which in turn controls the video and audio to the paying customer. The capability to monitor performance at all points in the system is essential. The ultimate function is the maximization of revenues from satisfied subscribers while minimizing lost revenue through security failures or service interruptions.

Data Distribution

In general an addressable scrambling system has two data channels. The out-of-band channel carries the addressing and control data to configure the decoder to its authorized mode. The in-band data carries channel specific information including tier level and any time-varying scrambling commands. Some systems operate with only one data channel but most likely sacrifice security or data integrity or both in the process.

Figures 2 through 5 show typical data distribution systems where remote operation is required. It is assumed that the out-of-band data is transmitted remotely while the in-band data originates from the specific channel scrambler at the headend site. The "special purpose data" terminology reflects the fact that the data from the controller to the decoder is not typically a standardized format (such as RS-232) but a special format for one-way, asynchronous message transmission over a "noisy" communication path. A Data Repeater is shown which is used as the last line of defense, transmitting "pseudo data" to keep the decoders operating in the event of complete loss of data.

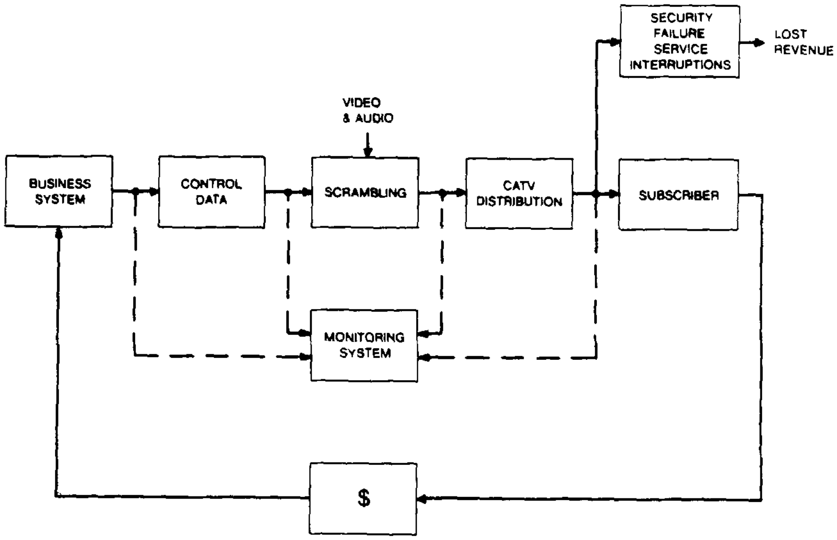


Fig. 1. THE CONTROL DATA SYSTEM

FML. In an FML link system (Fig. 2) baseband video (0-4.2 MHz) is combined with FM subcarrier audio channels (5.6, 6.2, 6.8 ... MHz) and transmitted over a single FML carrier. A reliable interface with this equipment utilizes one audio subcarrier slot (e.g. 5.6 MHz) for data modulated and downconverted to the subcarrier frequency for direct addition to a FML transmitter. At the receive site the subcarrier is then upconverted back to the data carrier frequency (usually in or near the FM band; 88 to 108 MHz). No additional modulation/demodulation is required to utilize the FML and little opportunity exists for developing data errors.

AML. In an AML system (Fig. 3) all channel carriers, FM carriers, and data carriers are transmitted in the exact frequency spectral relationship which they will be carried on the CATV system. The data modulation is done at the Master Headend site so the data carrier is transmitted intact. If the carriers are configured as on the CATV system, no significant degradation should occur over the AML. There is a slight reliability benefit to locating the data repeater at the receive site to guard against failed AML hardware carrying the data. The repeater hardware must then be duplicated at each hub and additional filtering is required.

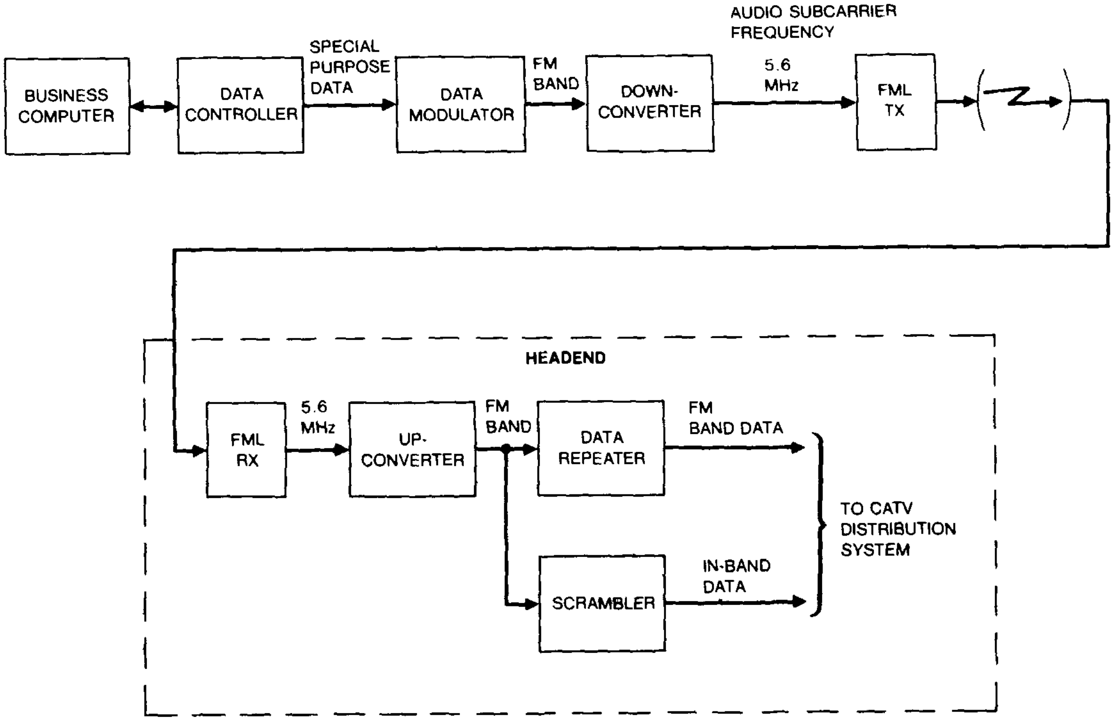


FIG. 2. FML DATA DISTRIBUTION

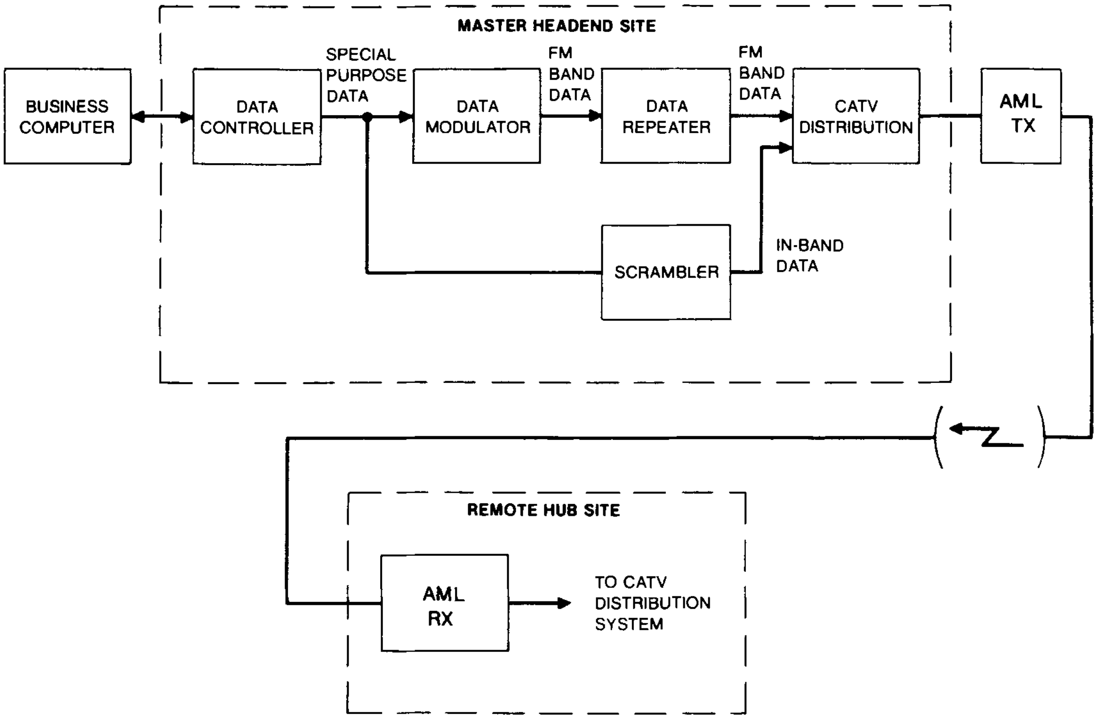


FIG. 3. AML DATA DISTRIBUTION

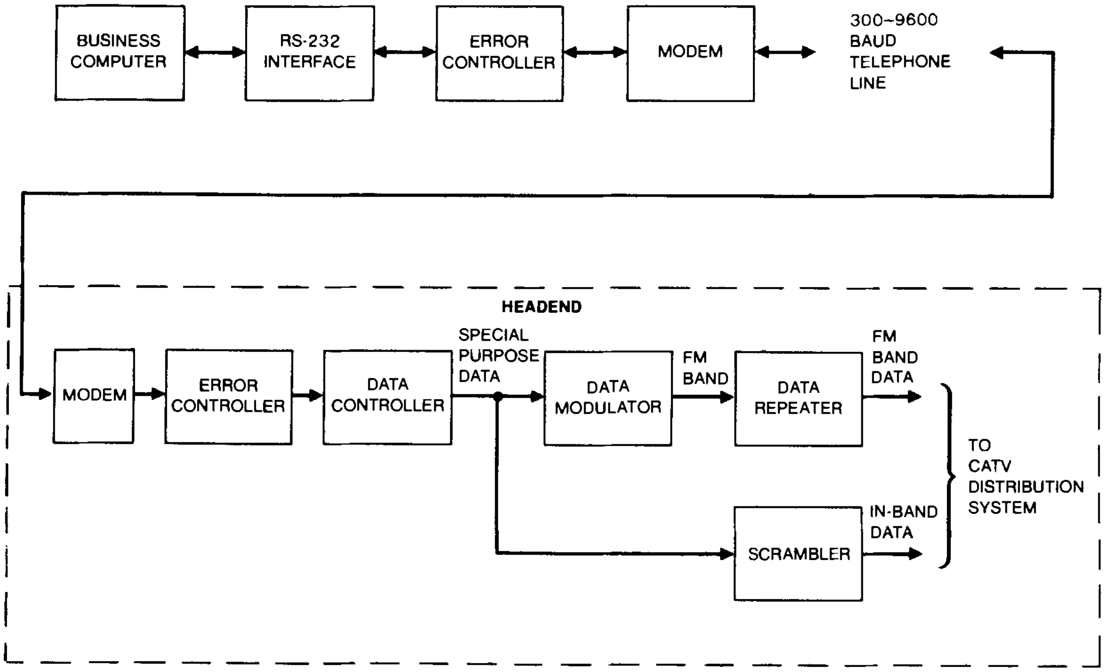


FIG. 4. TELEPHONE DATA DISTRIBUTION

Telephone. The special purpose data for transmission over the cable system is not RS-232 modem compatible as required for distribution via telephone. It is necessary to have a system configuration in which an RS-232 data link can be split. In Figure 4. an additional RS-232 interface is shown and it is assumed that the Data Controller is RS-232 compatible. The main shortcoming of this configuration is the high likelihood of injecting noise via the telephone line. The error controllers are intended to protect the data from noise. The subject of noise will be discussed in more detail below.

Upstream Cable. When the CATV system passes the business office after leaving the headend, it may be possible to use upstream processing (also referred to as subtrunk processing) to accommodate the data carrier (Fig. 6). This approach is similar to the FML case except that the frequency conversion is made compatible to the upstream equipment (below VHF TV channels; 5 - 40 MHz).

Other. In other data distribution systems, such as optical fiber, the specifications of the particular equipment must be matched to the data characteristics to determine the best transmission method. An approach similar to the FML case may be feasible. A video channel may be dedicated to the data signal although special precautions must be observed in regard to clamp circuits.

In many systems the implementation may involve a combination of several of these approaches. For example, the subtrunk scheme may be required from the office to a Master Headend followed by FML to supplemental headends. In this case it may be possible to choose a common conversion frequency to minimize hardware.

Sources of Error and Error Avoidance

Most errors may be categorized as occurring from the following causes:

- o Human Error or Tampering
- o Software Error
- o Hardware Failure
- o Noise or Interference

A distinction must be made between "bit errors" and "message errors." A message is the command that causes the decoder to take action. The digital message is composed of a number of binary "bits." Depending on the design of the individual elements of the system, varying susceptibility to errors may occur. If one of the aforementioned causes of errors results in a bit error, a message error may still be avoided through automatic error detection or error correction.

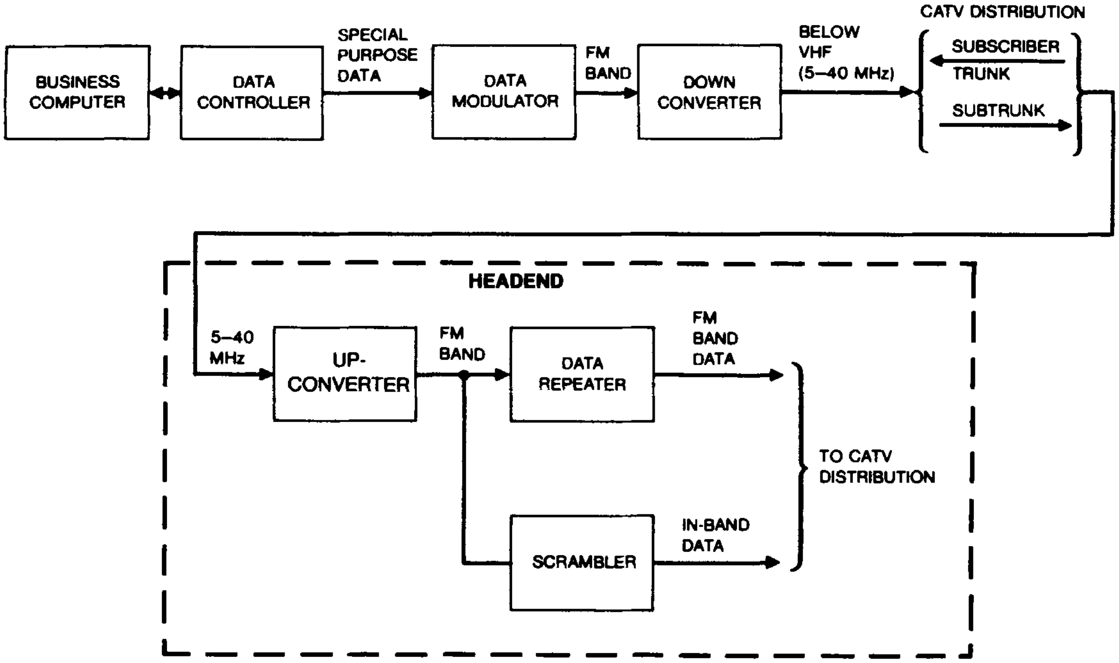


FIG. 5. CATV SUBTRUNK DATA DISTRIBUTION

For example, one of the simplest forms of error processing is to transmit duplicate messages sequentially. With the data receiver designed to respond only if two identical messages recur, most bit error combinations are detected and the bad message is not acted upon. Of course the correct message does not get through either. If the same bit errors occur in each word the process fails to work and a message error would occur.

If three messages are transmitted sequentially and the receiver requires two out of the three to be identical, some bit errors may occur and the correct message could still get through. Modern data communication design techniques allow much more efficient and powerful error detection and correction procedures. However these two examples illustrate the general principle.

The "special purpose data" in Figures 2 - 5 is presumably designed for error detection and/or correction since it must be transmitted over a noisy, interference prone CATV distribution network. It, therefore, is a good candidate for transmission to remote sites. This data however is not formatted for easy interface to standardized equipment and typically has a bandwidth requirement beyond audio circuitry specifications. In the FML, AML, and upstream CATV applications (Figures 2, 3, and 5) the data is sent as a modulated carrier.

In the telephone system case (Figure 4) sending a carrier or the special data format is not possible, so developing standardized RS-232 data is required. From a purely technical point of view, using a telephone line is the least desirable approach for transmission of the addressable control data. Besides slowing the communication speed, a new vulnerability to noise is interjected into the system. But unless a microwave link or alternate communication link exists for other purposes, it is probably not economically justifiable to provide one to handle data only. Thus unless an extremely good communication design has been done within the control data subsystem, external error processing is required. Figure 4 shows the addition of error controllers for error processing of the RS-232 data stream.

In addition to optimizing the system design and configuration, maintenance of all equipment involved in the data system must be diligently performed. The objective must go beyond repair of catastrophic failures to maintain calibration within specification to avoid introduction of errors.

The third area for error avoidance is monitoring, including: hardware functions, software routines, and persistent testing. Monitoring is the means by which data problems become evident and forms the cross-check on inadequacies in design and maintenance.

Monitoring Methodology

Monitor methodology means any effort taken, either hardware, software, or procedural, to detect and isolate problems within the data system.

Software. Monitoring for human errors, tampering, and software errors is a nebulous topic to discuss in a general sense. It entails the integral workings of the business and control software and the scrambling system. The designers must be mindful of these eventualities and build in checks to guard against them. The latter discussion of testing is relevant as a means of detecting loopholes in the system. A printer logging capability of all messages sent to decoders is useful but requires tedious perusal of data. The ability to select a subset of conditions under which the printer logging occurs is an extremely valuable way to trap a suspected occurrence. Running global addressing cycles including a negative global is a means of correcting certain errors that may occur. A global cycle sends the current authorization state to every decoder including those that should be deauthorized. It occurs at random times to thwart efforts to defeat it by disconnecting the decoder at a prescribed time.

Hardware. On the hardware side there are devices and techniques which should be used to isolate and correct errors:

- Monitor Decoder with Oscilloscope;
- RS-232 Data Scope;
- Data Message Analyzer;
- Spectrum Analyzer for Data Carrier;
- Bit and Message Error Rate Testing.

One of the simplest monitor aids is a standard decoder modified to allow the out-of-band and inband data signals to be displayed on an oscilloscope. While not a monitor of message intelligence, it does allow quick and easy perception of gross noise, interference, or carrier degradations and loss of data. This technique should be implemented at the control computer center and each headend site.

An RS-232 data scope is a standard instrument to monitor the messages passing between computers or other hardware devices. It should be online to monitor transactions and made available for troubleshooting other areas of the system as needed. It is particularly important in a system operating remotely via telephone modems.

A Data Message Analyzer is a special purpose device, typically designed by the scrambling system manufacturer, to capture and display the messages in the special purpose data format sent to decoders via the control data channel. if the message structure includes global commands to communicate with all decoders simultaneously, the analyzer should capture them continuously. For other decoder-specific commands the operator selects an address of a decoder that he wishes to investigate. When that decoder is hit with data the analyzer traps and displays it.

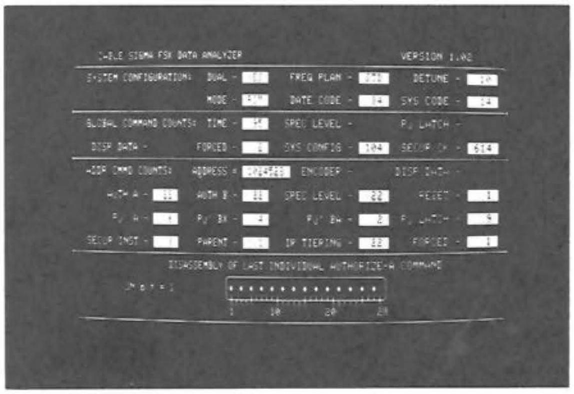
The data analyzer for OAK's SIGMA system is implemented with a data demodulator and special purpose data processor driving a smart terminal. It may be utilized at any point in the system where it can be supplied by the data carrier. Figure 6 shows the terminal display of the counts of global commands on the top two sections and the count of individual decoder information in the third section. The bottom section of the screen allows selection of the message content of any of the above message types. This powerful analytical tool is most useful for verifying complete end-to-end system performance including software functions. Since it processes data with the same error routines as the decoder it is a valid indicator of real message errors.

A data analyzer for in-band data has less value for analyzing system problems. Since the in-band data is channel specific and is generated in the scrambler, an in-band analyzer checks only from the scrambler forward. It is usually sufficient to use an oscilloscope or spectrum analyzer for these types of problems.

A spectrum analyzer is an indispensable tool for calibrating, monitoring, and troubleshooting the RF portions of the system. It is used to set and maintain the data carrier amplitude to specified limits, verify proper data modulation, and identify sources of noise and interference.

Bit error rate (BER) testing is the most precise way to monitor the overall system for data performance in the presence of noise. Message error rates may be measured by the same technique. Figure 7 shows the simplest interpretation of the bit or message error rate detector. Known "clean" data is delayed and compared with actual system data. Any differences on a bit-to-bit or message basis are attributable to noise in the system. All systems will have some bit errors. A particular system bit error counter may show 6 bit errors in a one minute time period or 0.1 errors per second. If the data transmission rate is 10,000 bit per second there is 1 error for every 100,000 bits. The BER is expressed as:

$$1 \times 10^{-5}$$



```
CABLE SIGMA FSK DATA ANALYZER                          VERSION 1.02
SYSTEM CONFIGURATION:  DUAL - [illegible]  FREQ PLAN - [illegible]  DETUNE - [illegible]
                       MODE - [illegible]  DATE CODE - 14   SYS CODE - 14
GLOBAL COMMAND COUNTS: TIME - [illegible]  SPEC LEVEL -     PJ LATCH -
  DISP DATA -        FORCED - 1    SYS CONFIG - 104   SECUR CK - 614
INDIV CMMD COUNTS:  ADDRESS = [illegible]  ENCODER -    DISP DATA -
    AUTH A - 11      AUTH B - 11   SPEC LEVEL - 22    RESET - 1
      PJ A - [illegible]   PJ BX - 4      PJ BA - 2     PJ LATCH - 9
SECUR INST - [illegible]  PARENT - [illegible]  IP TIERING - 22   FORCED - 1
         DISASSEMBLY OF LAST INDIVIDUAL AUTHORIZE-A COMMAND
                    1       10       20       28
```

FIG. 6. OAK SIGMA DATA MESSAGE ANALYZER

The data processor in Figure 7 must be the same as the bit or message processor in the decoder with all of its automatic error detection and correction to allow the most accurate representation of the actual system performance. While message error rate testing gives the best picture of system problems resulting in communication errors, bit error rate testing is the most precise measure of threshold noise problems. As with the data analyzer, error rate test equipment is special purpose equipment supplied by the system manufacturer. BER testing should be done periodically to check for subtle system degradations. Or even more preferable, implement a message error detector as a warning indicator to be on-line and running continuously. If a predetermined number of message errors occur in a specified time period, an alarm occurs to warn of a new source of interference or other degradation.

Monitoring Procedures. There are many monitoring procedures which should be part of the CATV operation's normal routine. Customer service monitoring is an important source of information but, as discussed earlier, not sufficient to catch all trouble scenarios. The additional procedures suggested involve conducting tests on a frequent basis to attempt to seek-out suspected or hypothesized problems. Ideas for trial testing can come from creative thinking, "grapevine" information, or real-time tests with employees in their homes. Information regarding system defeat mechanisms can to be gained through the grapevine. Installation and repair technicians usually know the techniques to defeat the system through personal contacts outside of the company.

A continual real-time field test with employees could uncover failure modes resulting in free services to customers. In order for this to be effective the number of homes involved must be significant without being unwieldy (probably 20 to 30 is the right size). Though motivated to participate and provide information through the incentive of free service, the billing functions must be left as though the employee is a paying customer. The actual bill can be cleared later. As many combinations of services as possible should be covered to simulate the real customer base. Since some installations will get more services than others periodic rotations should occur; also exercising the addressability functions more regularly. Disconnect scenarios should also be checked (the employee may be provided with an additional authorized decoder during this period).

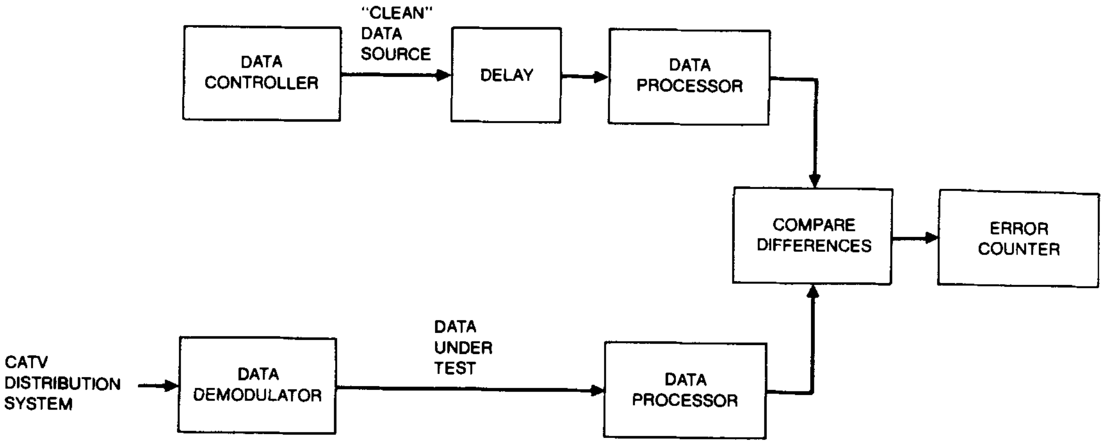


FIG. 7. BIT OR MESSAGE ERROR ANALYZER

CONCLUSION

Equipped with a thorough knowledge of the data system, a motivation to avoid lost revenue, and the resource allocation for requisite monitor systems the CATV operation can do much to avoid loses as the results of data system malfunctions. Even with the best system and software designs it is highly improbable that all prospective trouble scenarios can be anticipated and avoided in the initial design. However the fact that changes in the system are inevitable can be anticipated and flexibility for that change can be designed in.

The addressable system is immensely more complex to design and to operate than a non-addressable one. The factors resulting in maximum profits are more elusive and dictate more applied creativity to optimize; although the potential for profit is higher. It is only through the combined efforts of two partners, the manufacturer and the operator, that full realization can be achieved. The manufacturer must provide a good system design including monitoring capability, good documentation and training, and support of the operation of the system in the field. The operation must apply the system within its design limits, utilize the training and monitoring methodology, be creative and diligent in actively seeking problems and solutions, and commit the resources to accomplish these ends.