1/83

DOC CONTRACT REPORT

PROBLEMS OF SYNCHRONIZATION OF DBS SCRAMBLING SYSTEMS

DSS Contract No. OST81-00251
DSS File No. 21ST.36001-1-3741

DOC Scientific Authority: Mr. Brian Bryden, P.Eng.

Contractor: **Philip A. Lapp Limited**
CONSULTANTS TO INDUSTRY AND GOVERNMENTS

January, 1983

HEAD OFFICE: SUITE 302, 14A HAZELTON AVENUE, TORONTO, ONTARIO, CANADA M5R 2E2
Phone (416) 920-1994

OTTAWA OFFICE: SUITE 904, 280 ALBERT STREET, OTTAWA, ONTARIO, CANADA K1P 5G8
Phone (613) 238-2452, Telex 053-3314

CONTENTS

GLOSSARY

A/D - Analog to Digital
APL - Average Picture Level
BER - Bit Error Rate
BS - Broadcast Specification
CANCOM - Canadian Satellite Communications
CC - Closed Captioning
CCIR - International Radio Consultative Committee
C/I - Carrier-to-Interference ratio
D/A - Digital to Analog
DBS - Direct Broadcast Satellite
DES - Data Encryption Standard
LCET - Low Cost Earth Terminal
FFSK - Fast Frequency Shift Keying
MAAST - Multiple Audio Addressable Secure Television
M/NTSC - M-format/National Television System Committee
NRZ - Non Return to Zero
NTSC - National Television System Committee
PAM - Pulse Amplitude Modulation
RARC - Regional Administrative Radio Conference
RF - Radio Frequency
RFI - Radio Frequency Interference
RGB - Red Green Blue
RSP - Radio Standards Procedures
SCPC - Single Channel Per Carrier
TC & OC - Technical Construction & Operating Certificate
SNR - Signal-to-Noise Ratio
TDMA - Time Division Multiple Access
TES - Time Element Scrambling
TRC - Telecommunications Regulation Circular
TRS/DOC - Telecommunications Regulatory Service/Department of Communications
TVRO - Television Receive-Only terminals
VBI - Vertical Blanking Interval
VCR - Video Cassette Recorder
VIRS - Vertical Interval Reference Signal
VSB - Vestigial Sideband (amplitude modulation)
Z-TAC - Zenith - Tiered Addressable Converter

PROBLEMS OF SYNCHRONIZATION OF DBS SCRAMBLING SYSTEMS

1. INTRODUCTION

1.1 Background

It is widely assumed (and increasingly practised) that television signals transmitted via satellites will be scrambled so that reception of the signals by unauthorized ground stations will be to no avail. This will be essential for the economic viability of direct (to subscriber) satellite broadcast when low-cost TVRO's are readily available and installed in very large numbers.

The technology exists to deny access to intelligible television to eavesdroppers of almost any level of sophistication, and several scrambling schemes are in operation on cable-TV and off-air broadcast systems. Scrambling is also used for the secure delivery of television from a "packager" to a cable head-end for redistribution. In the latter case, the supplier and the distributor can co-operate to exclude others from obtaining useable material. They can use relatively expensive equipment that can be physically protected, and can communicate about the scrambling technique over secure channels that are not easily available to even determined and malicious eavesdroppers. As well, the cable-TV distributor already has the cable which can provide two-way communications with subscribers' premises.

The satellite broadcaster, whose signal may cover a large part of the country, cannot assume successful cooperation on the part of hundreds of thousands of subscribers; cannot count on non-broadcast, two-way communication to their premises; and, in fact, seems constrained to count only upon the one-way satellite channel into the subscriber's location. This channel must carry all of the information required to control access to particular channels and to descramble them. The only other contact the DBS operator has with subscribers is when the descrambler is installed or commissioned, and when a bill is paid.

The DBS environment, then, may be viewed from the subscriber location point-of-view as a TVRO receiving several channels of scrambled television, each of which contains the information required to descramble it (over and above any that might be stored in the descrambler), and a descrambler, which is supplied and controlled by the broadcaster.

An implication of one-way control and lack of timely physical access to the subscriber, is that every unauthorized receiver must be de-authorized as quickly as possible. One way to achieve this is to authorize all bona fide subscribers on a regular and periodic basis, by broadcasting specific authorization to each and every one of them. Those descramblers not positively re-authorized within a reasonable number of authorization cycles would automatically time-out and require special action to be reactivated. The time-out period should be long enough not to inconvenience legitimate subscribers who may have missed re-authorization while channel switching or due to momentary power loss, or transmission errors. On the other hand, the period must be short enough to deny useful viewing times to users of stolen or counterfeit descramblers. Of course, direct de-authorization may be carried out on a pre-emptive, priority basis as well.

> CONSIDERATION OF THE ADDRESSING AND AUTHORIZATION REQUIREMENTS INDICATES THAT DIGITAL INFORMATION MUST BE CARRIED AND IT (PROBABLY) MUST BE CARRIED ON ALL CHANNELS - A SEPARATE CHANNEL WOULD MEAN A SEPARATE RECEIVER WHICH WOULD MEAN EXTRA COST. SINCE THE INFORMATION CONTROLS THE DESCRAMBLER IT MUST BE RECOVERABLE WITHOUT DESCRAMBLING THE TELEVISION SIGNAL (EVEN THOUGH IT COULD BE ENCRYPTED).

The components of the received signal on a DBS channel may be assumed to be scrambled video and/or audio; addressing and authorization data; and descrambling information. The descrambling information contains the critical elements to re-construct and synchronize chroma demodulation, raster display, data demodulation, luminance descrambling, and audio decryption as required.

In an earlier report on the economic, policy, and technical aspects of DBS systems (Ref. 1) attention was drawn to the problem of synchronizing the various signal formats likely to be used in DBS Scrambling Systems. At the time it was noted that synchronization is a critical element in any communications system carrying encoded information. In this context even a normal television signal carries encoded information because it contains the synchronization signals; however scrambled television signals, because they are further manipulated, usually by a sequence of operations, require another layer of reliable sychronization. In addition, if the manipulation is carried out upon digitized signals the precision with which synchronization must be established is increased, and the reliability of successful performance will decrease unless compensating improvements are made to the transmission system.

It was noted in Ref. 1 that the state of the art in television scrambling was advancing rapidly as more companies entered the field in anticipation of lucrative markets for secure, low cost, scrambling systems. This state of affairs is still very much in existence a year later. To add to the problem it is apparent that some scrambling systems being considered for satellite use will create problems in a DBS system because they are being developed and tested for other communications channels, for example, cable television service. Attempts to operate through a satellite network into low cost television receive-only terminals (TVRO's) have already presented unanticipated problems. The purpose of the current study therefore is to re-examine scrambling technology in a number of DBS network configurations emphasizing the merits or deficiencies of particular synchronization requirements in a DBS environment.

1.2 Study Methodology

The Statement of Work calls for an investigation of synchronization problems in a number of uplink situations. Specific potential problems to be addressed were sync update rate, sync susceptiblity in a multiple channel environment, multi-point and transportable encoding. The limiting parameters for reliable synchronization in a one way broadcast with varying pathlengths and in systems with subscriber addressing and tiering were to be examined. A preferred synchronization scheme was to be identified.

The methodology employed in the study was conventional - assemble a set of findings, analyse them, draw conclusions and make recommendations. The findings were accomplished through a review of the earlier study reports, reviews of literature provided by current and future scrambler suppliers, visits to local suppliers of video processing equipment, in particular equipment used to resynchronize television signals from diverse sources for broadcast, a literature search into synchronizing techniques for digital signals, especially burst signals, and discussions with Telesat Canada and with the Department of Communications regarding interference levels anticipated for DBS or DBS type systems.

In addition to the foregoing, several visits were made to Canadian Satellite Communications, "CANCOM", to review the performance of the OAK ORION Scrambling System which CANCOM has purchased for its satellite distribution network. The latter visits were particularly helpful in elucidating some of the real-life synchronising problems being encountered in an operating system.

1.3 Form of Final Report

This final report is divided into several principal sections beginning with this introduction.

Section 2 is a general discussion of synchronization as it applies to DBS systems. Section 3 is a review of the problems in a variety of network configurations. It also describes and analyses the communications channel through which scrambled signals will be sent. Section 4 is a review and an update of the candidate scrambling systems identified in earlier reports. Section 5 provides a discussion of the unique synchronizing requirements for a number of candidate systems. The second purpose of this section is to identify the critical transmission features of the DBS channel. Section 6 contains the conclusions regarding synchronization schemes. Section 7 is the final section of the report and contains the recommendations.

1.4 Study Limitations

It is characteristic of scrambling systems that internal features of the system remain secret to all except a small number of individuals who develop and service the systems. Accordingly, the statements in this report regarding the detailed format of scrambled systems are sometimes hypothetical, representing best engineering judgement of a reasonable method of implementing a particular scrambling concept. This proviso is noted for completeness, but it is not seen as a limitation on the validity of the results. The variety of synchronization schemes examined includes most known practical methods of synchronizing signals for transmission through communications systems. Internal subtleties therefore rank as second-order in terms of the synchronization problems.

2. SYNCHRONIZATION

2.1 Definition

Synchronization is the process which determines the time of occurrence (or phase) of various, or all, of the parts of the signals in a communications system. Synchronization is required at many different levels that span a wide range of time scales; each with different requirements for precision. Synchronization may be achieved by the use of local time references at the receive end of a system; by observation of the received information signal; or by reception of specifically transmitted synchronization information.

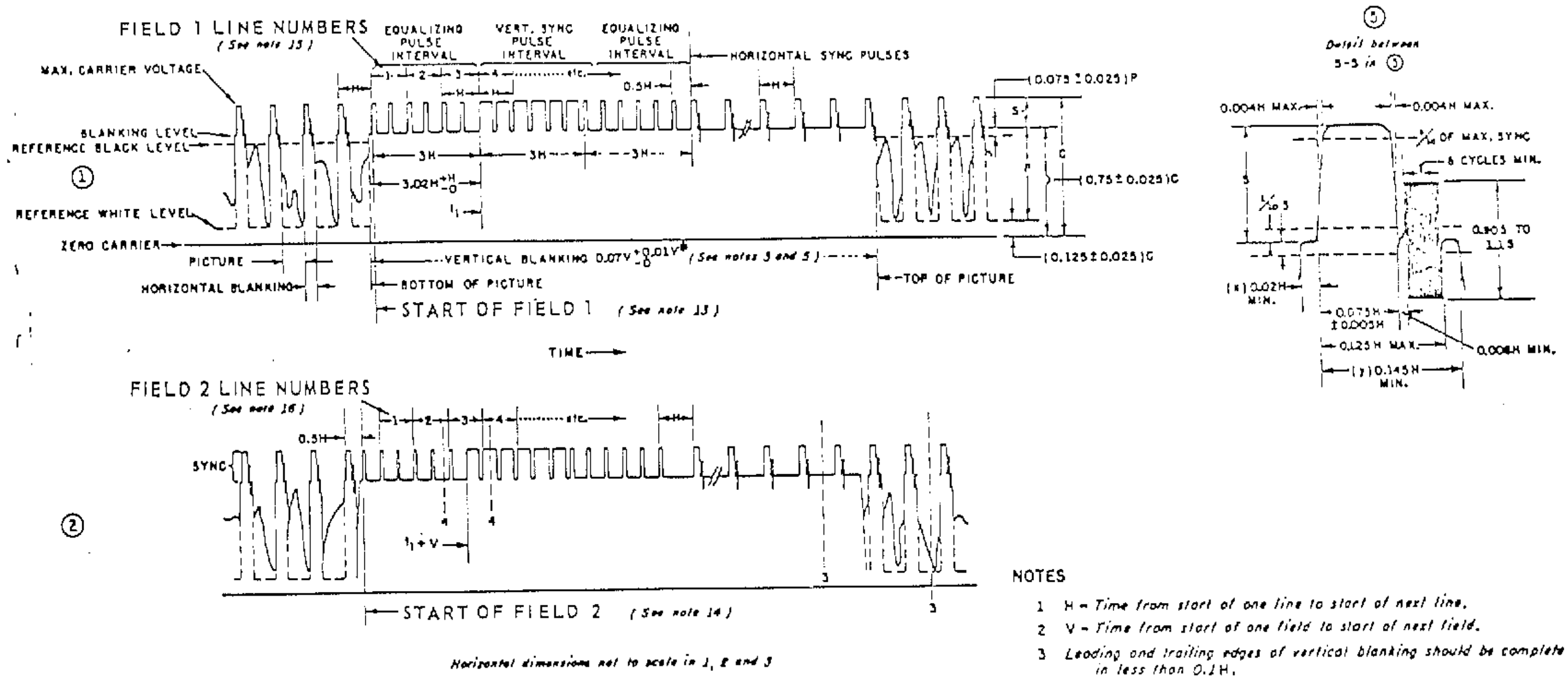
Synchronization may be required before demodulation - to either implement or improve the extraction of information from a modulated carrier, or after demodulation - to extract information from the demodulated signal.

A colour television signal is highly synchronized, with a large fraction of its transmitted energy devoted to raster synchronization, and with information transmitted on each and every line to provide a phase reference for coherent chrominance demodulation. In this section we review synchronizing schemes in conventional and scrambled TV underlining the fact that if the conventional television signal is severely modified during scrambling, and the fraction of transmitted energy devoted to sync is reduced, received signals will have to be of higher quality and sophisticated signal processing electronics will have to be used to faithfully restore high fidelity images and sound.

2.2 Conventional NTSC Colour Television

Conventional NTSC colour television signals consist of three separate frequency-multiplexed signals: chrominance, luminance and sound; and three time-multiplexed synchronization signals: vertical and horizontal start-of-sweep pulses and the colour subcarrier phase-locking burst. In a colour television receiver these six signals, as they appear at the output of the demodulator in the receiver, are combined to re-create the scene originally viewed by the colour television camera. All three time - multiplexed sync signals have exact, well-defined waveforms; and the definitions are standardized, and readily available. Details of shape, amplitude and timing are illustrated in Figure 1.

The luminance, or brightness information, is carried as Vestigal Sideband Amplitude Modulation (VSB) on the picture carrier.



NOTES

1. H = Time from start of one line to start of next line.
2. V = Time from start of one field to start of next field.
3. Leading and trailing edges of vertical blanking should be complete in less than 0.1H.
4. Leading and trailing slopes of horizontal blanking must be steep enough to preserve minimum and maximum values of (x + y) and (z) under all conditions of picture content.
5. *Dimensions marked with asterisk indicate that tolerances given are permitted only for long time variations and not for successive cycles.
6. Equalizing pulse area shall be between 0.45 and 0.5 of area of a horizontal sync pulse.
7. Color burst follows each horizontal pulse, but is omitted following the equalizing pulses and during the broad vertical pulses.
8. Color bursts to be omitted during monochrome transmission.
9. The burst frequency shall be 3.579545 mc. The tolerance on the frequency shall be ±10 cycles with a maximum rate of change of frequency not to exceed 1/10 cycle per second per second.
10. The horizontal scanning frequency shall be $\frac{2}{455}$ times the burst frequency.
11. The dimensions specified for the burst determine the times of starting and stopping the burst, but not its phase. The color burst consists of amplitude modulation of a continuous sine wave.
12. Dimension "P" represents the peak excursion of the luminance signal from blanking level, but does not include the chrominance signal. Dimension "S" is the sync amplitude above blanking level. Dimension "C" is the peak carrier amplitude.
13. Start of Field 1 is defined by a whole line between first equalizing pulse and preceding H sync pulses.
14. Start of Field 2 is defined by a half line between first equalizing pulse and preceding H sync pulses.
15. Field 1 line numbers start with first equalizing pulse in Field 1.
16. Field 2 line numbers start with second equalizing pulse in Field 2.
17. Refer to text for further explanations and tolerances.

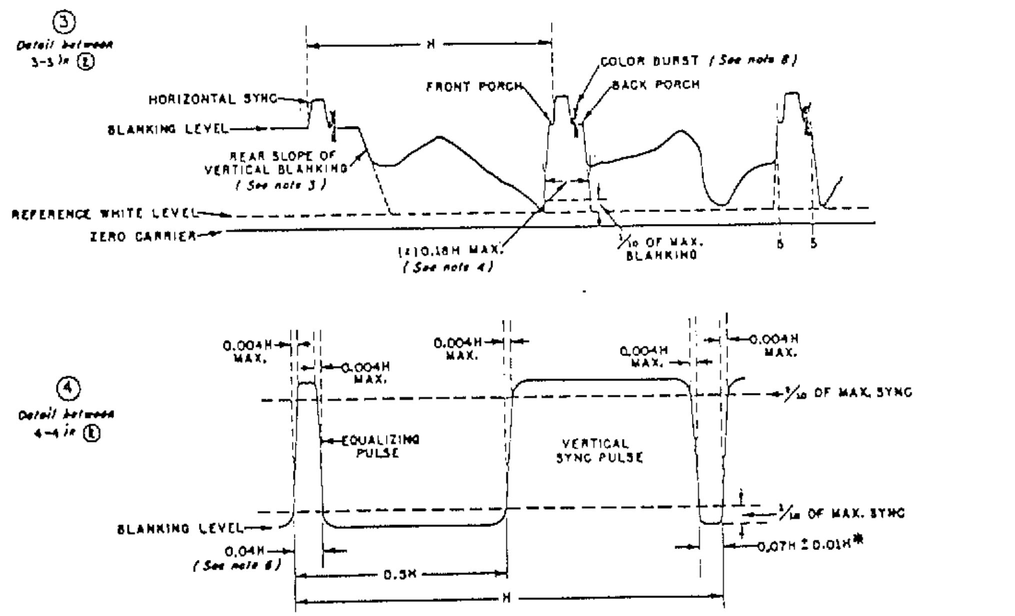


FIGURE 1 - STANDARD COLOUR TELEVISION BROADCAST SIGNAL FORMAT (REFERENCE: FCC 73.699)

The chrominance, or colour, information is represented by two colour difference signals transmitted in quadrature on a colour subcarrier, whose frequency is 3.58 MHz above the picture carrier. One of the colour components, the Q, has symmetrical sidebands whereas VSB is used to restrict the other, or I, component.

The audio signal is carried as frequency modulation (FM) on an audio carrier whose frequency is 4.50 MHz above the picture carrier.

Horizontal sync pulses, as shown in Figure 1, may be extracted directly from the composite colour video signal by clipping. Note that these pulses occupy about 16% of each line and are transmitted at from two to three times the average picture level. Note also that in the NTSC modulation standard - vestigial sideband amplitude modulation - maximum RF carrier occurs during the horizontal and vertical sync pulses.

Horizontal sync pulses must be detected simply, and reliably, hence they contain a substantial fraction of the transmitted energy. The reason is fairly obvious: the signals were designed to ensure the reliable operation of receivers in the 1940's (the NTSC "compatible" colour standard was not adopted until 1953). Modern receivers could synchronize with a much smaller fraction of the energy, given the input signal-to-noise ratios most TV sets are expected to operate with. Horizontal sync is very accurate because it is established from the leading edge of a steep pulse. This leading edge is specified to take no longer than 250 nsec to change from the 10% to the 90% level and vice-versa. Typically the rise and fall time is in the order of 50% of the maximum time allowed.

Vertical synchronization is derived from a pattern of wide pulses at the horizontal rate at the beginning of each field. Usually a capacitor charging above a threshold establishes the exact timing. Vertical synchronization is much less precise than horizontal, and it is a rare TV receiver that has accurate interleaving of the alternate fields. This compromise is intentional in the NTSC standard because slight vertical displacement of horizontal lines is not as perceptible to the viewer as lateral displacement caused by offsets or jitter on the horizontal sync.

The vertical sync is less robust than that of the horizontal, it is more vulnerable to noise, and there is a relatively long time between vertical sync pulses. Hence the viewer is aware of missed vertical synchronization. Momentary or transient problems during a horizontal line can be corrected on the next line since each carries both horizontal sync and colour burst.

Some television systems depend upon extraction of frame synchronization. Those with specific information in one field and not another, such as field multiplex systems for instance, require the identification of field 1 and field 2. Frame synchronization requires a detailed examination of the equalizing and vertical sync pulses. Better signal quality is required to extract it reliably, compared to horizontal and vertical sync.

The third sync signal in an NTSC colour signal relates to the colour subcarrier. Since quadrature multiplexing is used in the colour signal, it must be demodulated synchronously. It is essential that the local oscillator in the synchronous detector in the receiver be exactly in phase and frequency with the transmitter. This is accomplished by sending eight cycles - the 'colour burst' - of the colour carrier during the blanking interval following the horizontal sync pulse, i.e. on the 'back porch'.

In the receiver the colour burst time-of-arrival is anticipated by the horizontal sync pulse which opens a gate to the colour oscillator circuits. The gated colour-burst corrects the phase of the local oscillator, or excites a narrow band high-Q filter, to produce a local reference carrier for the synchronous demodulator. The exact phase relationship must be maintained between transmitter and receiver for successful operation of the quadrature multiplexing. If the receiver oscillator is not in correct phase, or if differential phase errors occur in transmission (or in video recording) a distortion in the hue results.

The stability of the colour carrier frequency is very carefully controlled, particularly over one line. Broadcast station tolerances for the 3.579545 MHz frequency are ±0.0003% or about 1/1000th of a cycle over a horizontal line.

Conventional television usually works very well, as far as raster synchronization is concerned. As noted earlier, there is so much energy in the raster synchronization signals that receivers will lock when there is almost no discernible image. Colour reproduction on the other hand requires relatively good signals; degradation in colour fidelity often being the first indication of impairment.

2.3 Scrambled Television Via Direct Broadcast Satellite

2.3.1 Control Signals

As a general principle the added complexity of scrambling in a DBS environment means that control information must be delivered faithfully to each decoder to authorize (or de-authorize) reception of specific scrambled program material and, once authorized, to unscramble the program. This requirement is common of course to all scrambling systems but the method of delivery of the control signals can vary. For the purposes of this study, delivery of authorization is assumed to be by electronic means, using the television program channel itself. Delivery of authorization and tier control messages by, for example, manual switching in a subscribers' decoder, though perfectly acceptable in many cases, is not feasible in a DBS system. Delivery of the actual unscrambling control signal must be done in real-time, electronically, because in some scrambling systems each line and frame of a TV scene constitutes a differently-coded signal. Controlling decoders thus comprises two sequential operations: (i) transmission of digital address and control signals from time to time, to open or close total, or tier, authorization gates, (ii) continuous transmission of digital signals to control the decoding of the scrambled voice and picture signals and, if needed, re-create the sync for the sweep circuits in the television receiver. Depending on the system concept, the first part of this 2-part sequence may occur several times a minute, or it may be repeated only when a change is required. The same can hold true for the second, the actual scrambling part.

2.3.2 Categorization of Scrambling Sequence and Associated Synchronization

There is a wide variety of scrambling techniques, and they may be classified in a number of ways. Scrambling may be classified in terms of the order in which the various techniques are applied (to the signal), at what rate, and how the receiver is informed of the order and rate; in other words, in terms of the scrambling sequence used.

With reference to Figure 2, it can be seen that the time scales involved vary from virtually forever with a fixed method (e.g. video inversion) down to the duration of a single pixel with full digital encryption. In the figure, video scrambling is further divided into two categories: these which involve delaying the signals during scrambling/descrambling, and those which do not.

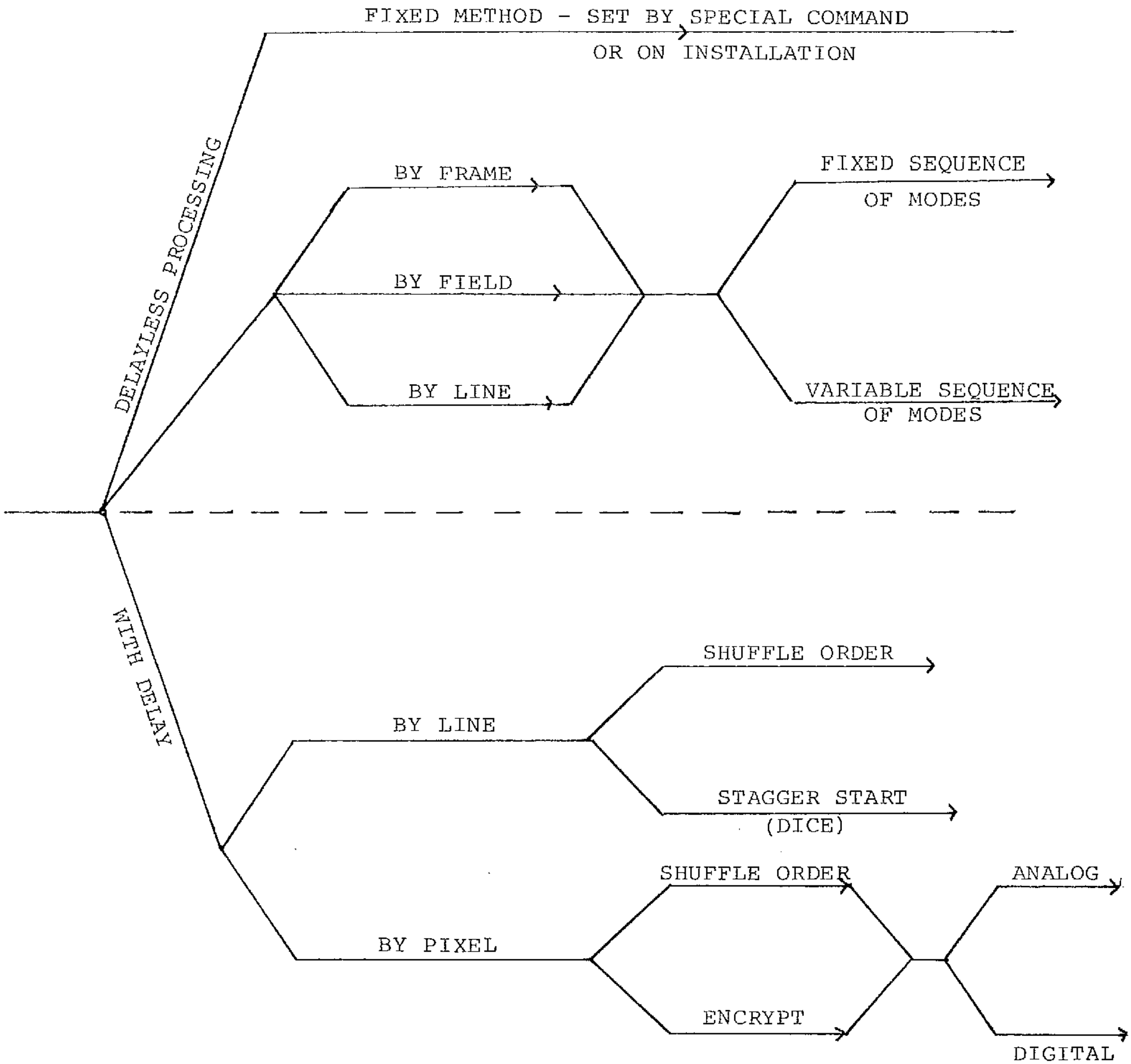


FIGURE 2

SCRAMBLING SEQUENCES

The delayless processing methods include:

a) a fixed method (which could be changed on special command);

b) a fixed, pre-arranged sequence of scrambling methods, processing the signal on a frame-by-frame, field-by-field, or line-by-line basis;

c) a variable sequence, operating on the signal as in b), but not prearranged.

Methods requiring signal buffers and delay include:

d) line manipulation techniques in which
   i) entire lines are shuffled; or
   ii) the starting point of each line is varied (dicing); and

e) pixel manipulation techniques.

Method d) can include field and frame manipulation techniques. The scrambler output signal is assumed to be analog, even though digital signal processing may have been used.

Method e) includes pixel shuffling and encryption, and either (re-constituted) analog output or digital bit stream output.

Synchronization may be achieved as follows.

a) With a fixed method, the method being used can be broadcast frequently and a simple switch set at each receiver.

b) With a pre-arranged sequence, the starting time or the state of the sequence generator may be transmitted.

c) With a variable sequence it may:

   i) be generated at the subscriber location if, in fact, it is a pseudo-random sequence, by transmitting generator state data; or

   ii) be transmitted with the scrambled signal if it is a "one-time pad" type of sequence.

d) With line manipulation either of b) or c) might apply.

e) with pixel manipulation, shuffling order would probably be pre-determined or controlled by a simple algorithm; pixel-by-pixel encryption, on the other hand, would require a keystream generator at the receiver and the transmission of state information to it.

Note that any information transmitted may be encrypted, whether it is addressing/control, digital audio, or key stream generator data. It is assumed that a self-synchronizing data-stream encryption process would be used. As described in Refs. 12 and 21, it is relatively simple to construct such a system from Data Encryption Standard (DES) devices, as shown in Figure 3. Transmission errors in the encrypted data can cause a string of errors in the decrypted data, but systems in which errors do not propagate require keystream synchronization to the exact bit.

In certain uplink/downlink configurations there may be a supplementary requirement to control and synchronize slave encoders at remote uplink sites, because scrambled signals arriving at a remote re-broadcast site may have to be re-synchronized to local signals or vice versa. Typical requirements might be local insertion of programming, added tier-ing, local scrambling, local insertion of data into the Vertical Blanking Interval (VBI), or local insertion or substitution of another audio channel.

2.3.3 Addressing and Tiering Control

A DBS system is eventually seen as serving in the order of 10^6 or more subscribers. Reliable, individual, addressing and tier control in a dynamic operating environment, with subscribers in these numbers, becomes a formidable problem. Indeed, should the actual scrambling technique eventually chosen for DBS be relatively simple, the address/tier control subsystem may well turn out to be the dominant problem. The basis of the problem is simply the high bit rates needed to address sequentially such a large population of DBS subscribers in a short cycle time. In a later section it is noted that long delays between authorization or tier change will probably be unacceptable in a mature DBS system. It follows that the bit rate must be high. In Section 3.6, the calculations indicate a requirement for megabit rates for operationally effective address and tier control.

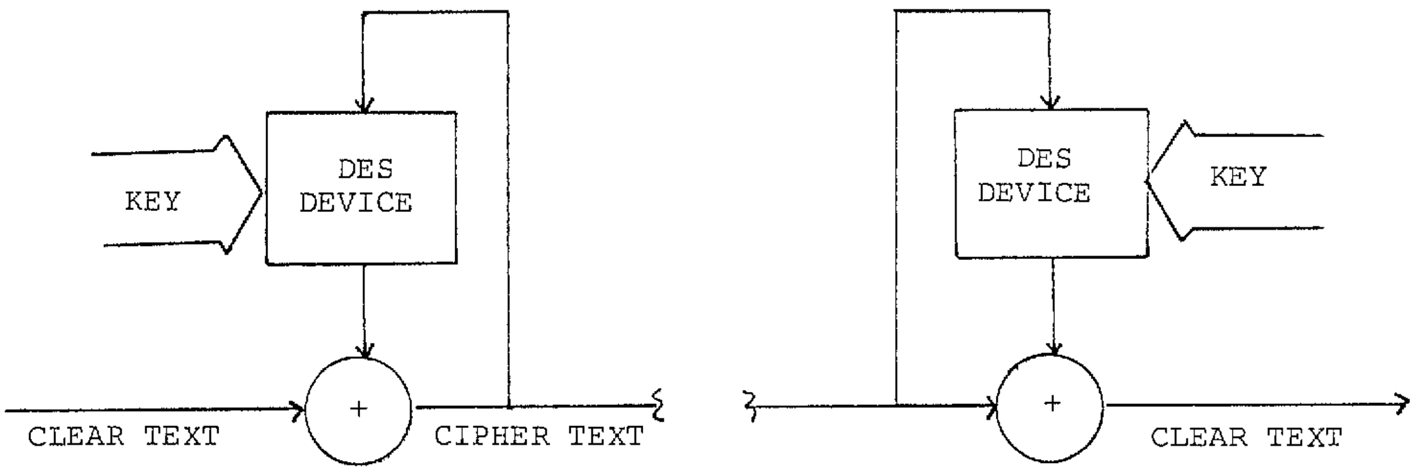


FIGURE 3

SELF-SYNCHRONIZING ENCRYPTION

2.4 Synchronization Factors In Scrambled Television

In this study the following assumptions were made in relation to the DBS system:

(i) Authorization/control information is transmitted on all channels at all times. Therefore there must either be:

- a single uplink; or
- communications from a central (subscriber registry) to every uplink:
    - to relay information, or
    - maintain local data bases.

(ii) Operational and subscriber reaction/tolerance times dictate the time scales for authorization and descrambling. Channel-hopping at a subscriber location requires clear, synchronized signals (or "access-denied" indication) within a very few seconds or even within a few frames.

Questions that relate to synchronization of TV descramblers may be summarized as follows:

1) what signals, or portions thereof, are scrambled and/or encrypted;

2) what information is being carried on each channel;

3) how can such information be transmitted;

4) what synchronization is required, and what are the time scales; and

5) where can synchronization problems arise?

2.4.1 What Signals, or Portions Thereof, are Scrambled and/or Encrypted

As discussed above, the normal television signal has two parts: video and audio. The video part has two sub-parts: picture information and synchronization. The picture information has two parts: brightness (luminance) and colour (chrominance). The colour information has two components: the I (in-phase) and Q (quadrature) components.

Any one, or more, of these parts and sub-parts may be scrambled or encrypted.

The scrambling may be introduced in a fixed manner, as for example by inverting the luminance signal and leaving it that way; or dynamically, by inverting the luminance on any given line in a pseudo-random fashion. Scrambling may merely inconvenience the technically sophisticated viewer. At the other extreme, scrambling may hide the information from even the most versatile eavesdropper since the scrambling pattern may be derived from a keystream generated by a crytographically secure device. Thus, scrambling can be considered as an encryption/decryption process.

Let us consider the various ways in which the television signal can be scrambled. Scramblers embodying most of these were described in previous reports.

Audio

Analog encryption techniques have been used in speech scramblers for telephone calls for fifty years or more. These devices have tended to be analog devices which typically distort the audio signal by such operations as inverting its spectrum (replacing low frequencies with high, and vice-versa). Digital techniques are also used to implement what is sometimes called "analog encryption". The clear signal is sampled and digitized; the digital samples may be simply re-ordered, or may be combined with a pseudo-random keystream; and the samples are converted back to an analog signal, ostensibly occupying the same bandwidth.

Analog encryption is fraught with problems caused by the redundancies of speech, the difficulties of precisely reconstructing a bandlimited analog signal from its samples; the distortions and noise encountered in transmission; and, in the case of sample-by-sample encryption, the necessity for synchronization of the sampling clocks at the transmitter and receiver. These problems are discussed in more detail in Appendix A; but, in general, the performance of analog scramblers as a function of signal-to-noise and channel distortion (intersymbol interference) is very difficult to assess, and usually requires subjective testing in any actual situation.

Digital encryption of audio can be achieved very successfully if enough bandwidth is available to transmit the encoded digital samples as a digital stream without reconversion to analog (except in the modems, of course). For the 15 kHz audio signals in television approximately 300 kilobits/second would have to be transmitted, and many would argue that for high fidelity as many as 500 kilobits/second should be used. However, in this all-digital environment, the problems are the classic encryption problems of choosing codes, distributing keys, and synchronizing the keystream generators at each end of the link. These problems are normally well-understood and the performance of data communications systems may be calculated fairly accurately. However, data transmission in television channels depends on the characteristics of the complete video channel. These characteristics are often not well known, and thus the channel is difficult to analyze.

Judging by the number of commercial scrambling systems in which the audio is transmitted as an encrypted digital bit-stream it appears reasonable to assume that the audio portion of the television signal will be transmitted as a data signal. Just how and where it is transmitted is still a variable however.

Video

The video portion of the television signal can be scrambled in a number of ways as described in previous reports. These techniques include:

1) masking the true video with corruption by a removable jamming signal;

2) manipulation of the analog signal on a line-by-line basis through video inversion, removal of the sync signals, or line dicing;

3) scrambling the order in which various lines or fields are transmitted;

4) scrambling the order in which the pixels of a sampled television signal are transmitted;

5) encrypting the samples of a digitized video signal, and transmitting them as reconstituted analog or as data.

It is possible to scramble the entire video signal or any of its components; and to do this over the entire raster, or only over the visible portion of each line leaving the vertical retrace interval and/or the horizontal sync pulses clear.

2.4.2 What Information is Carried

The information carried with the television signal, scrambled or not, must include luminance and colour information; audio; raster synchronization; addressing, control and descrambling information.

The scrambling information that is carried along with the transmitted signal depends, of course, to a large extent on the scrambling method that is being used. If the normal raster synchronization has been removed, it must be derivable from some other part of the signal. In addition to the many signals such as Vertical Interval Test Signals (VITS), Vertical Interval Reference Signals (VIRS), Closed Captioning (CC), and teletext (Telidon) that might be found in the Vertical Blanking Interval of a standard television broadcast, one can expect to find a digital data packet containing the following information associated with each line or field of the television signal:

1) subscriber addressing, in the form of three or more bytes in which the addresses of all legitimate subscribers are transmitted in regular rotation.

2) subscriber authorization, in the form of one or two bytes which describe the specific selection of channels and programs that the addressed subscriber is authorized to view. In most systems the authorization can be diminished at the subscriber location by anyone such as a parent who wishes to temporarily restrict the range of programming being viewed at that location.

3) control information, which might be used to communicate information to subscribers; to specify the current program material for matching against authorization codes; to positively deactivate or commission subscriber descramblers.

4) scrambling information, which could consist of the descrambling sequence (the keystream) which might or might not be encrypted itself; the key for and/or the state of the keystream generator; or new keys; or scrambling mode definition.

This digital information can always be encrypted.

2.4.3 Where Can the Information be Carried

The information described above may be transmitted in a number of ways, and in a number of "places". It is assumed that each scrambled television signal and all of its associated signals shall be transmitted in a standard television channel. Regulation of the TRS/DOC may in fact prevent anything else, as discussed in Section 4.6.

If the information to be transmitted is assumed to consist of scrambled, composite analog video with sync intact, digital audio, and digital information, then the following is likely to be true.

The analog video signal will be carried with wideband frequency modulation, although, an alternative possibility exists and should not be overlooked. Since the signal broadcast through the satellite will be direct frequency modulation of the transmitter, component (RGB) rather than composite television might be used, particularly if component television sets (tuner, plus RGB monitor) make any sort of impact in the market.

If the audio is not scrambled it can be carried in the conventional way as frequency modulation of a separate sound carrier or sub-carrier. The presence of a frequency modulated sound carrier is used in current scrambling systems as a vehicle to carry auxiliary information by amplitude modulating the FM sound signal.

If the audio is in digital form, it can be transmitted on a data sub-carrier in any number of modulation formats, even including spread spectrum (Ref. 27); during blank lines in the Vertical Blanking Interval either as an autonomous data packet or as Pulse Amplitude Modulation of the normally black video signal (i.e. "line inserted" data, as in teletext); or on a shortened back-porch on the horizontal sync pulse or instead of the horizontal sync pulses ("in-sync" data).

In a similar manner, the digital auxiliary signals may be carried on the audio, on a separate sub-carrier, on the back porches, or on blank lines in the VBI, or instead of the normal sync pulses.

2.4.4 What Synchronization is Required

Synchronization is required for the following:

1) Demodulation of the television signal at three levels:

   i) at the carrier level, which is unlikely to be a problem for satellite delivered television as it will be transmitted as direct frequency modulation the microwave carrier;

   ii) at the composite video signal level, if required to synchronously demodulate the quadrature colour components; and

   iii) at the raster level, to provide interlaced raster scan lines in synchronism with the transmitter.

2) Detection of digitally encoded information at three levels:

   i) extraction of bit timing;

   ii) recognition of byte, or word timing; and

   iii) recognition of framing.

3) The scrambling or encryption process. Whatever scrambling method is used, the descrambler must be able to invert the scrambling process as it occurs, and therefore must be continuously aware of the method. If the scrambling is controlled by a sequence of binary, or other, numbers then the descrambler must:

   a) know the sequence;

   b) be sent either it or an encrypted version of it; or,

   c) must be able to generate an exact replica of it at the receiver. In the latter case, the sequence generator at the receiver must be provided with both the key in use and the state of the generator at specific times. This information is usually transmitted digitally in encrypted form requiring demodulation, detection and self-synchronizing decryption before it can be used. If the error rate is very low, it might be reasonable to assume that all decrypters will be self-synchronizing, as shown in Figure 3; even though single errors can cause the loss of a block of data.

4) The addressing and control of subscribers. In addition to synchronization required for the demodulation, detection and decryption of addresses and authorization information it is necessary in an operational system to have frequent 're-synchronization' between changes in subscriber status and the control information.

2.4.5 Where Synchronization Problems can Arise

Synchronization problems arise at two levels:

1) at the network level in switching, editing, taping, inserting, and rebroadcasting; most of which must be done with NTSC standard signals.

2) at the subscriber level upon

    a) installation and commissioning: the new descrambler must be included in the authorization cycle, presumably during the time when the installer is present;

    b) a "cold start" after a lengthy dormant period, total loss of power, moved location, reinstatement as an authorized subscriber, or similiar situation;

    c) a "warm start": caused by channel switching or momentary loss of signal or of power.

2.5 Summary

There are three levels at which synchronization is required, and they have distinctly different time scales.

The first level is the operational level in which the authorization cycle must be tuned to the subscriber's requirements for tuning in, on-demand viewing, simultaneous recording, multiple channel viewing, channel switching, bill payments, and so on.

The second level is related to network operations such as switching, time-base correction, frame synchronization, insertion, recording, and so on.

The third level relates to signal recovery and descrambling and requires synchronization for raster, colour, and code.

In both conventional television and data communications an appreciable amount of the transmitted energy is devoted to the synchronization components of the signal. In many practical systems, distortionless and virtually noise-free channels are required for reliable communications. As discussed in more detail in Appendix C, it is difficult to analytically predict the performance of scrambled DBS systems due to errors in synchronization, however it does appear that, because of the requirement for the extraction of synchronization from a scrambled signal which is more complicated than normal TV, very good channels are going to be required; loss of synchronization will cause abrupt loss of intelligible signals (Appendix B); and any particular system would require careful evaluation before universal adoption.

3. DBS NETWORKS AND DBS CHANNEL CHARACTERISTICS

3.1 General Considerations

A Direct Broadcast Satellite will receive uplink signals from a number of sources that change with time. Uplink change-over may occur infrequently, say every 30 minutes, or it may happen as often as several times a minute, as during an election coverage. In some cases, it will be advantageous to cue uplinks in and out of the same DBS transponder to avoid the cost of providing a supplementary satellite channel to bring a distant signal to a production centre for subsequent uplinking to the DBS channel.

Program continuity of the type modern consumers are conditioned to expect will place extra demands on the cue-ing in and out of all- scrambled signals or mixed scrambled/clear signals.

In subsequent paragraphs we will review engineering problems to be solved in designing satisfactory sync circuits for discreet module blocks in a scrambled DBS system. Before doing that, however, we wish to note for the record a number of operational constraints and imperatives that will in all probability compromise the optimum design of sync signals and sync detectors in the system.

3.2 Operational Constraints and Imperatives Affecting Synchronization Techniques for DBS Scrambling Systems

Though not in themselves a problem for synchronization, operational constraints and imperatives in a DBS system may force the system concept towards non-optimal designs as far as synchronization is concerned. These constraints are in two classes: those imposed from outside to meet the requirements of standards and control for the public good, and those imposed internally by the need to offer subscribers a service with sufficient quality, variety and adaptability to attract and hold their subscriptions.

The most important outside constraints are the DOC documents pertaining to scrambled TV systems and decoders. Copies of the current issue of the documents - TRC59, Issue 1 and TRC 60 Issue 1 - are attached at Appendix D.

TRC 60 sets out electrical characteristics of decoders, hence it refers to a particular module in a DBS system.

TRC 59 on the other hand sets out constraints and imperatives that are system - wide. The basic points in TRC 59 are as follows:

TRC 59 ISSUE 1, MAY, 1981

- Implicit that DOC intends to certify scrambled systems for "broadcasting transmitting undertakings for which a Technical Construction and Operating Certificate (TC & OC) is required".
- Coding and decoding method is not standardized.
- There is to be no perceptible degradation of the quality of the signal provided at the output of the decoding device.
- Transmission and reception must be compatible with M/NTSC system specifications set out in DOC BS #12, Issue 2.
- There is to be no interference to the radio environment.
- Scrambler shall not increase the spectral energy beyond limits of RSP 151, 154 and 157.
- Visual or aural carrier frequencies cannot be altered.
- No specific taboos on synchronization.
- No specific reference to DBS.

A set of "interval" constraints and imperatives has been developed for this study as a necessary input to the eventual recommendation of preferred synchronization schemes. Though not necessarily complete, the constraints are typical and apply to all scrambling systems. Their importance lies in the fact that modern television viewers are conditioned to expect smooth transitions in the continuity of a program and (virtually) instantaneous synchronization of the television picture tube raster when a channel is switched on. These constraints are:

(i) At a subscriber's terminal "immediate" descrambling of authorized programs must occur during a 'dial search'. A consumer will invariably utilize such a dial search to determine which programs he wishes to view. Excessive time required to 'clear' an authorized picture during such a dial search will frequently mislead the viewer to believe that a particular program is not authorized, when in fact it is authorized but synchronization time is excessive. In other words sync delay will be mistaken for program denial. Therefore, descrambling synchronization must be delivered several times a second.

(ii) 'Instant' re-synchronization following a transient loss of signal is required. To meet this requirement the synchronization update rate should be once per frame. Alternatively, the descrambler can have a memory mode which will allow re-synchronization to occur immediately upon recovery of the scrambled signal. In any event instant de-authorization during a transient demands instant re-authorization and unscrambling.

(iii) By virtue of (i) and (ii) above long synchronization sequences are deemed unacceptable. Here 'long' is taken to mean sequences requiring several full picture frames in time to execute.

(iv) Decoder addressing subsystem design must be capable or restoring authorization within a few seconds of power failure or DBS transmitter failure. As an alternative, authorization must be remembered for, say, several days in a decoder because a subscriber may turn off the main power switch to his home during a prolonged absence.

(v) The compromises to be made in selecting an optimum addressing and scrambling technology for DBS must favour simple, reliable decoders that will perform with TVRO's that show moderate, i.e. normal, aging and misalignment characteristics.

(vi) The scrambling system design must include at least the potential for home video recording of a scrambled signal.

(vii) Production centres and remote re-broadcast studios must be able to use existing video processing equipment such as time-base correctors and digital frame stores for inserting or substituting program material or even VBI signals.

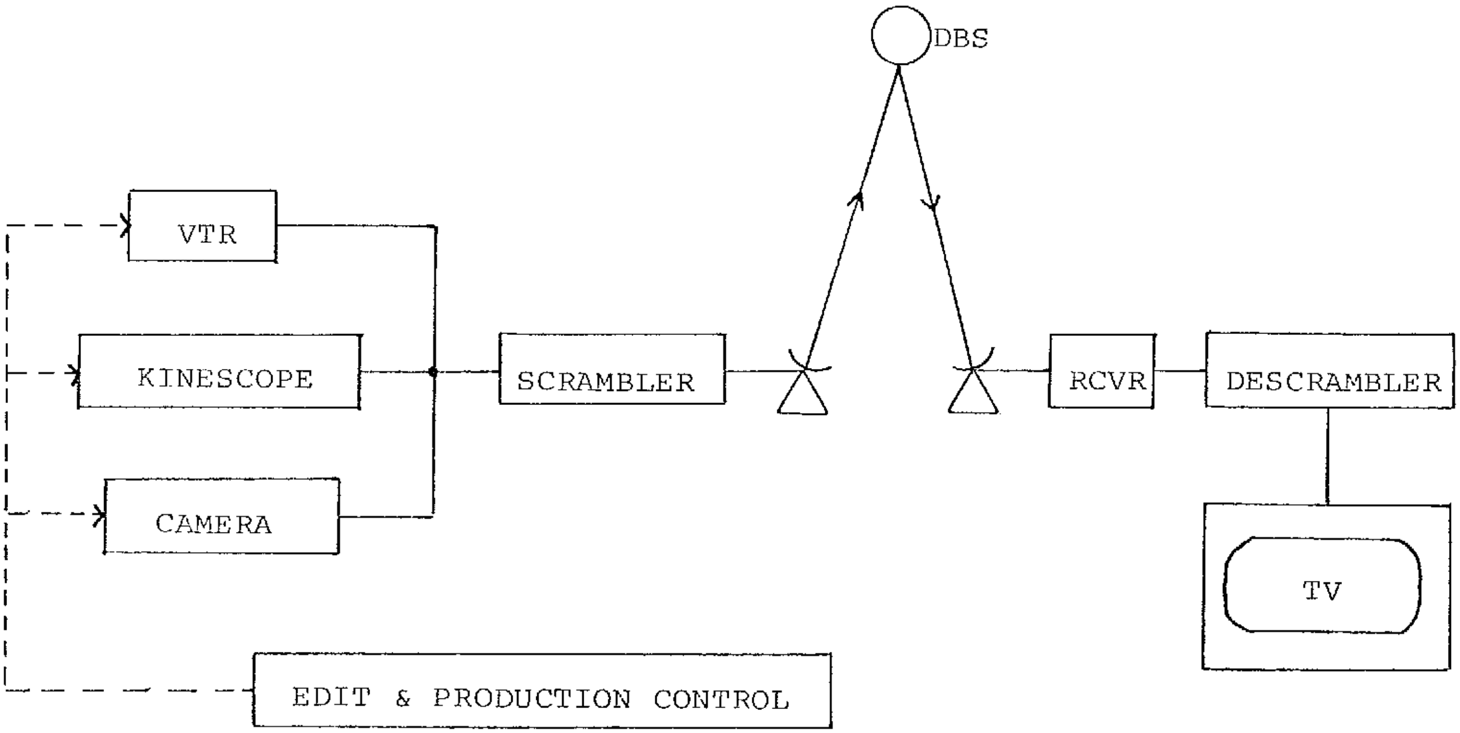
The seven foregoing points can be summarized by stating that "the scrambling system should be transparent to subscribers and intermediate nodes in the DBS network".

3.3 DBS Network Configurations

In the following paragraphs ten specific network configurations and situations are described. Some do not present any new synchronizing problems, some may cause momentary loss of picture or loss of synchronization if certain types of scrambling are used.

3.2.1 DBS Network Configuration #1

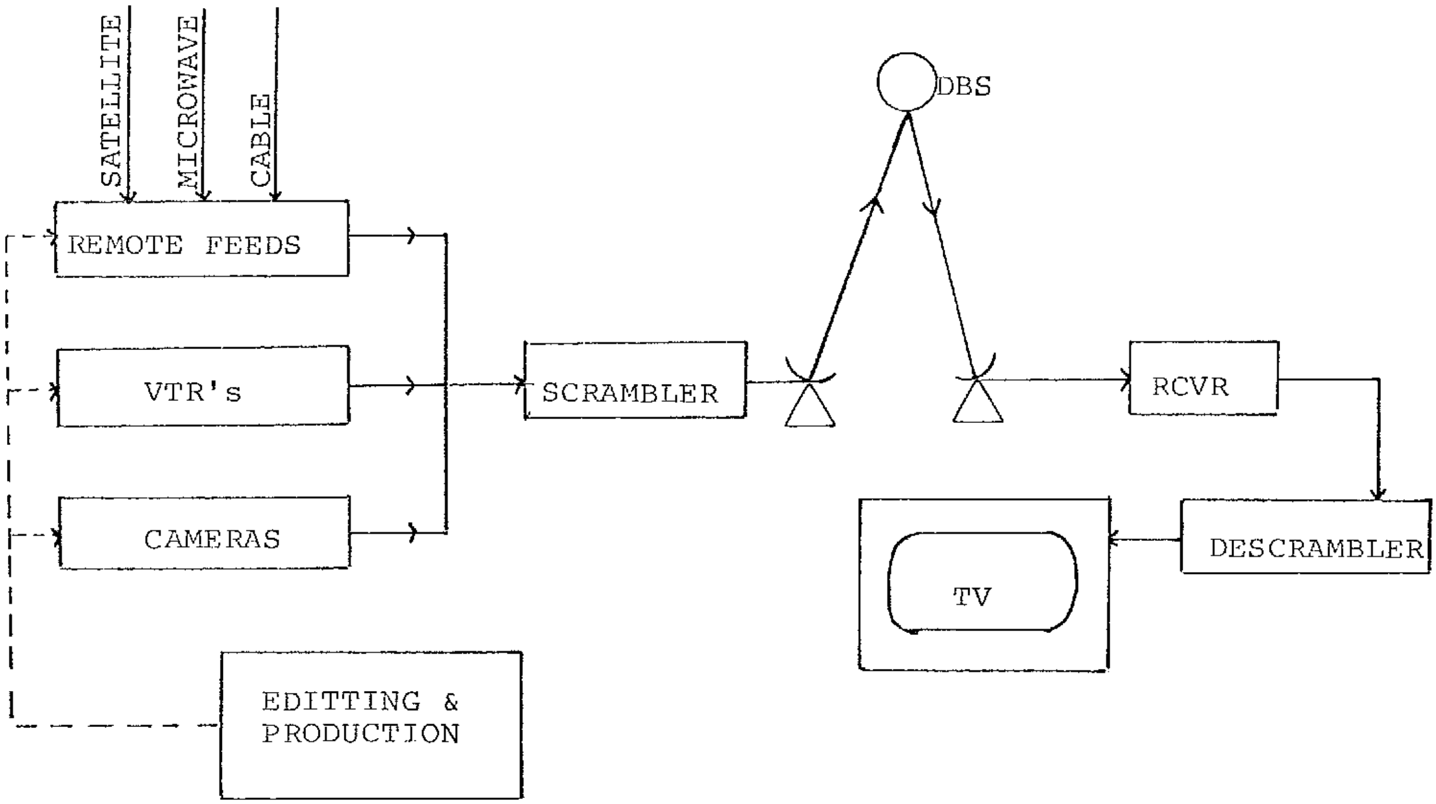
- Entire program originates at a single source. Insertions, fades, and special effects are introduced before scrambling, using a local time base to give a continuous composite video signal. Scrambling is continuous and uninterrupted.
- Example: full-length movie.



Special Synchronization Problems - None.

3.2.2 DBS Network Configuration #2

- Program material assembled in time sequence into a coherent, continuous program. All video inputs are locked or re-synchronized to a common timing reference. Scrambling is introduced into the final continous video stream.
- This a subset of configuration #1.
- Example, news broadcast, major sports event.



Special Synchronization Problems - None.

3.2.3 DBS Network Configuration #3

SEE FIGURE 4

- Program material supplied by more than one source at more than one location. DBS channel is 'shared' to avoid cost of transmitting material to a central site for retransmission on DBS.

- Remote uplinks under central scrambling control (slave mode).

- Example: News, election, international incident.

<u>Synchronization Problems</u>

- Cue-ing timing problem exists.

- 250 msec loss of signal at cut-over. Resynchronization of descrambler will be necessary.

- Slave must have 'memory' mode.

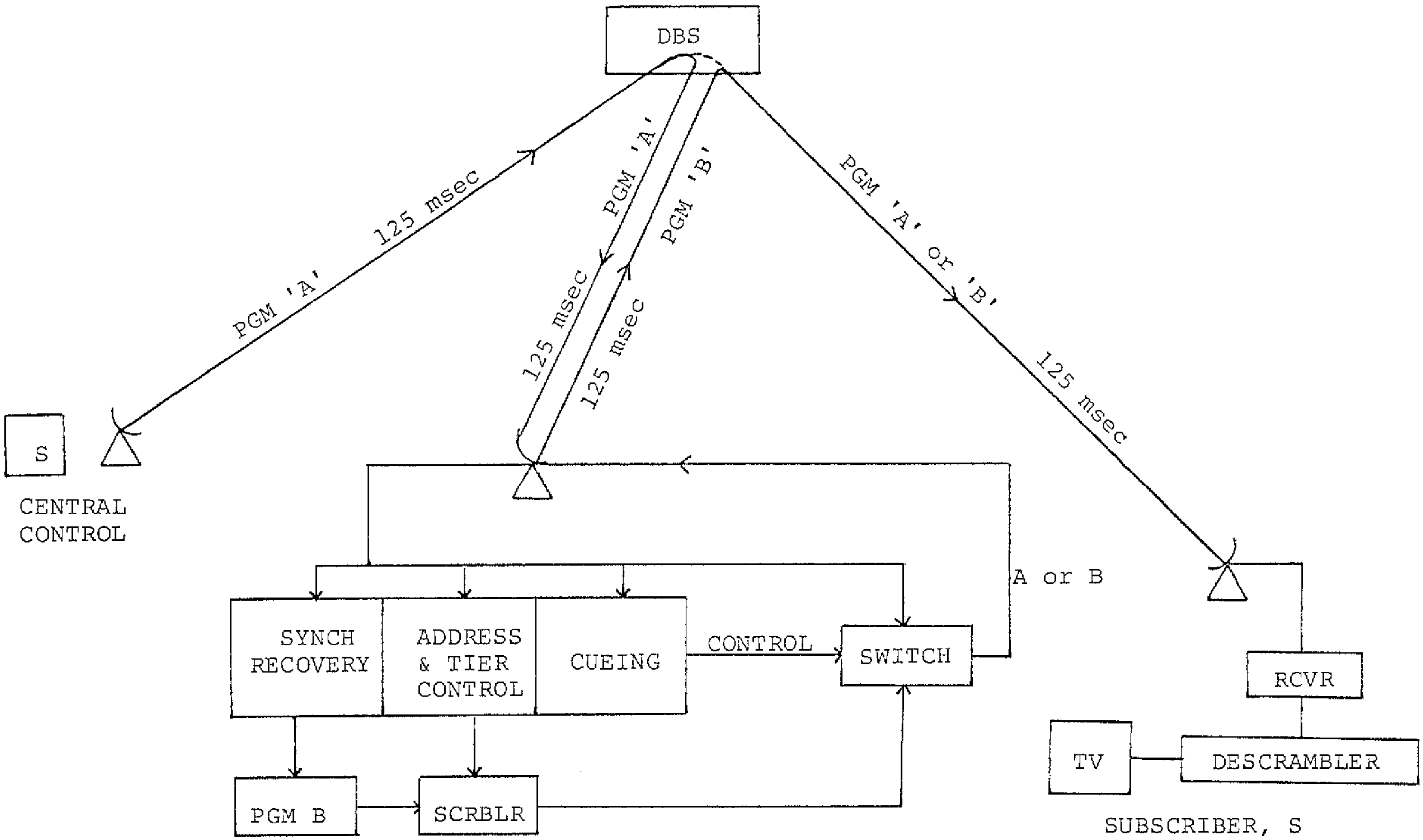
Referring to Figure 4, note that the A signal leads the B by 250 msec at Subscriber S. Central control can cue substitution of B and A in the common satellite channel, but when B starts to uplink A must cease. When A ceases, slave loses address and control information and defaults to 'last-in' memory mode. The default condition can be avoided if the address and control information can continue to be sent on a narrow-band audio-type channel, emulating an order-wire. Without an order-wire, B transmission must be pre-programmed to stop after a certain interval because wide-band control signals cannot be sent from central control to B through the same channel. Satellite channels normally have enough spare bandwidth for a small number of Single-Channel-Per-Carrier (SCPC) audio channels. Such a channel could serve as a common order wire.

Reversion to program A must result in momentary loss of signal at S to avoid two simultaneous uplink signals in the satellite channel.

Serious synchronization problems exist in this uplink situation if temporary loss of signal causes, or permits, random default settings to occur in the

FIGURE 4

NETWORK CONFIGURATION #3, COMMON SATELLITE CHANNEL, CENTRAL CONTROL (DUMB SLAVE)



addressing, tiering and descrambling logic circuits in the descrambler. Such an occurence would require re-addressing, etc., which could conceivably take several seconds. This event would be a severe impairment in the DBS service. A solution would be a 'memory' mode in the descrambler which would delay closure of gates, etc. for several seconds.

3.2.4 DBS Network Configuration #4

SEE FIGURE 5

- Program material supplied by more than one source at more than one location.
- DBS channel is 'shared' to avoid cost of transmitting material to a central site for retransmission on DBS.
- Remote uplink is cued by central control but has independent scrambling, tiering and addressing capability.
- both signals are "authorized".

<u>Synchronization Problem</u>

- Similar to situation #3 except for scrambling mode. If the remote uplink has independent scrambling-mode control descramblers will have to be re-synchronized to the new scrambling mode. Resynchronization within one frame or less would be essential.

  Note that address and tiering control information would now originate at the remote site although it would be unchanged because this information is supplied from central control. It would have been previously stored in the remote's control system because all parts of the 'program' are authorized to the same subscribers.

3.2.5 DBS Network Configuration #5

SEE FIGURE 6

- Satellite performs onboard program switching between beams or channels. All program material is scrambled.
- Switching occurs at relatively infrequent times - for example once in 30 minutes.

FIGURE 5

DBS NETWORK CONFIGURATION #4

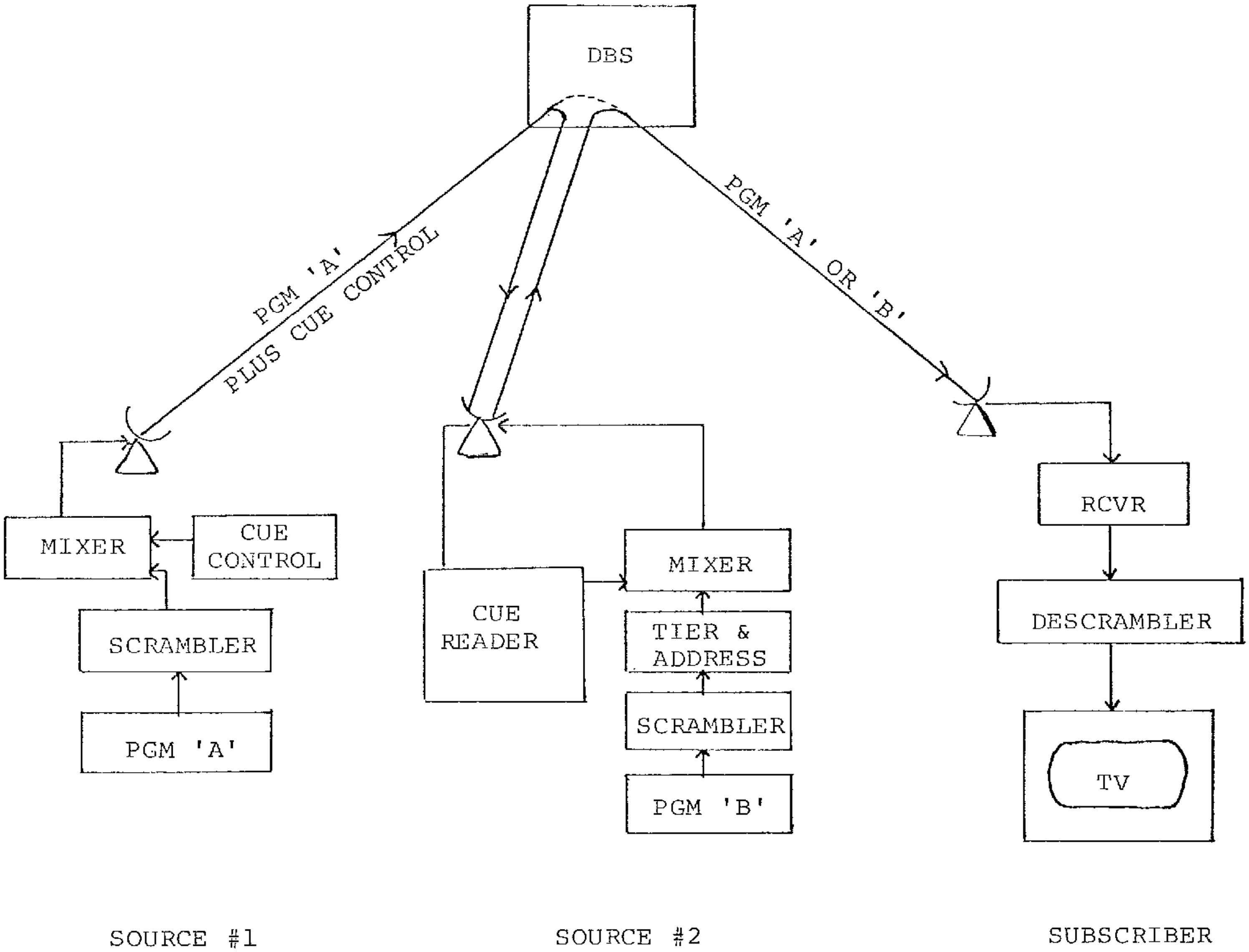
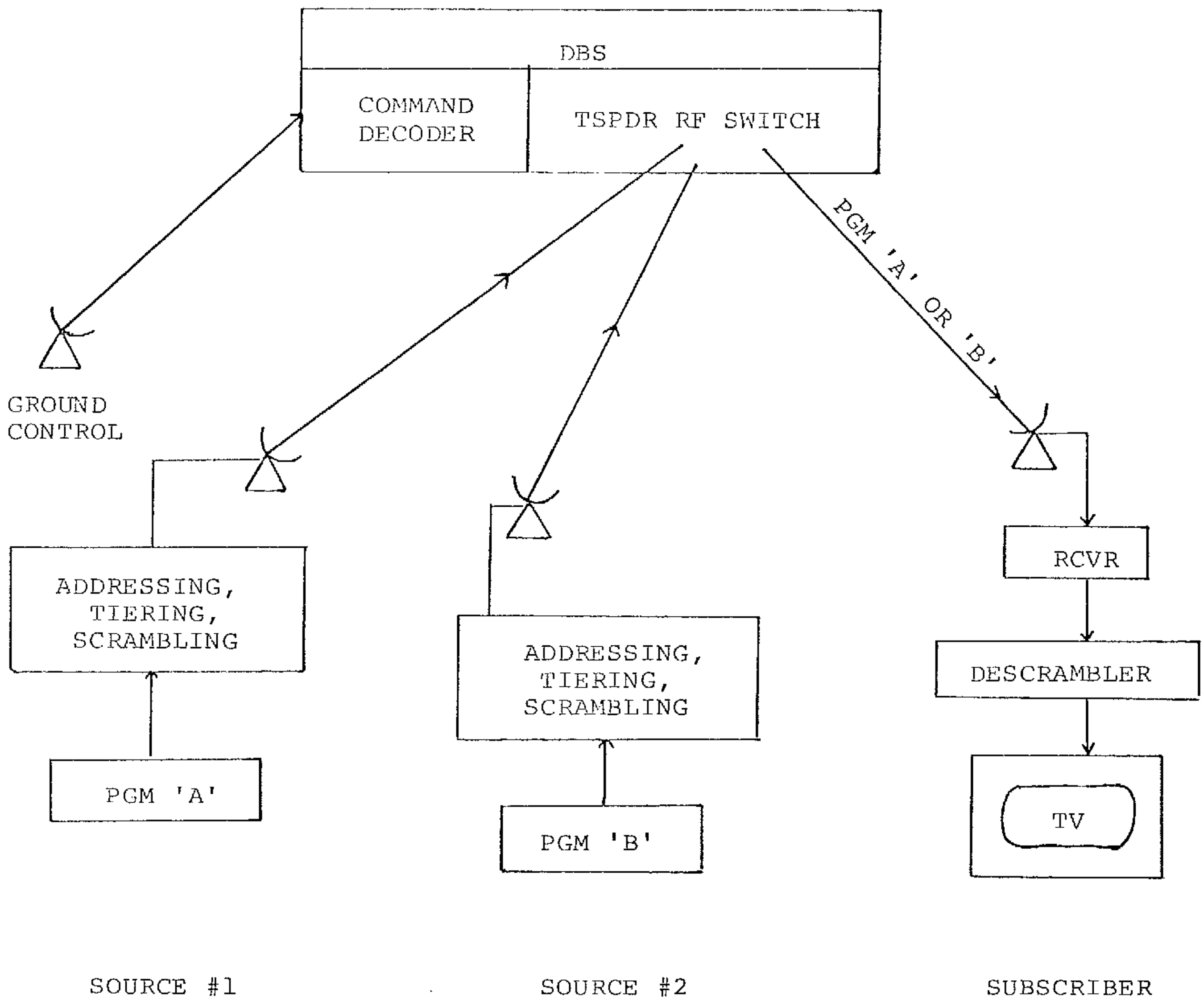


FIGURE #6

DBS NETWORK CONFIGURATION #5



This is similar, in the context of synchronization, to uplink situation #4, assuming each program is independently scrambled. There will be momentary loss of signal at the instant of cut-over. The authorize/de-authorize and scrambling mode trigger gates must be enabled within the first full frame period to avoid subscriber confusion.

3.2.6 DBS Network Configuration #6

Digital TV Transmission

If baseband is simply sampled, encrypted and transmitted in digital words there is no scrambling - unique problem, because an encrypted digital signal is no more sophisticated or complex than an unencrypted one. Both require similar synchronizing sequences.

Digital TV in a TDMA mode is a special case of digital TV. Here the requirements to capture synchronizing information can impose severe requirements if "burst" TDMA is used.

3.2.7 DBS Network Configuration #7

SEE FIGURE 7

- Two DBS scrambled programs share a single transponder channel.
- Crosstalk and cross modulation result in interference 50 db below the desired signal.

Potential Viewer Problem

- Faint background noise from unwanted program.

Potential Synchronization Problem

- Practically speaking, the amplitude difference of the two signals is such that the interfering signal cannot achieve the threshold levels of the synchronization-detection circuits in the descrambler. No synchronization problem is foreseen.

3.2.8 DBS Network Configuration #8

SEE FIGURE 8

- Co-channel interference.
- Desired program is scrambled, interfering program is clear or scrambled.

FIGURE 7

DBS NETWORK CONFIGURATION #7

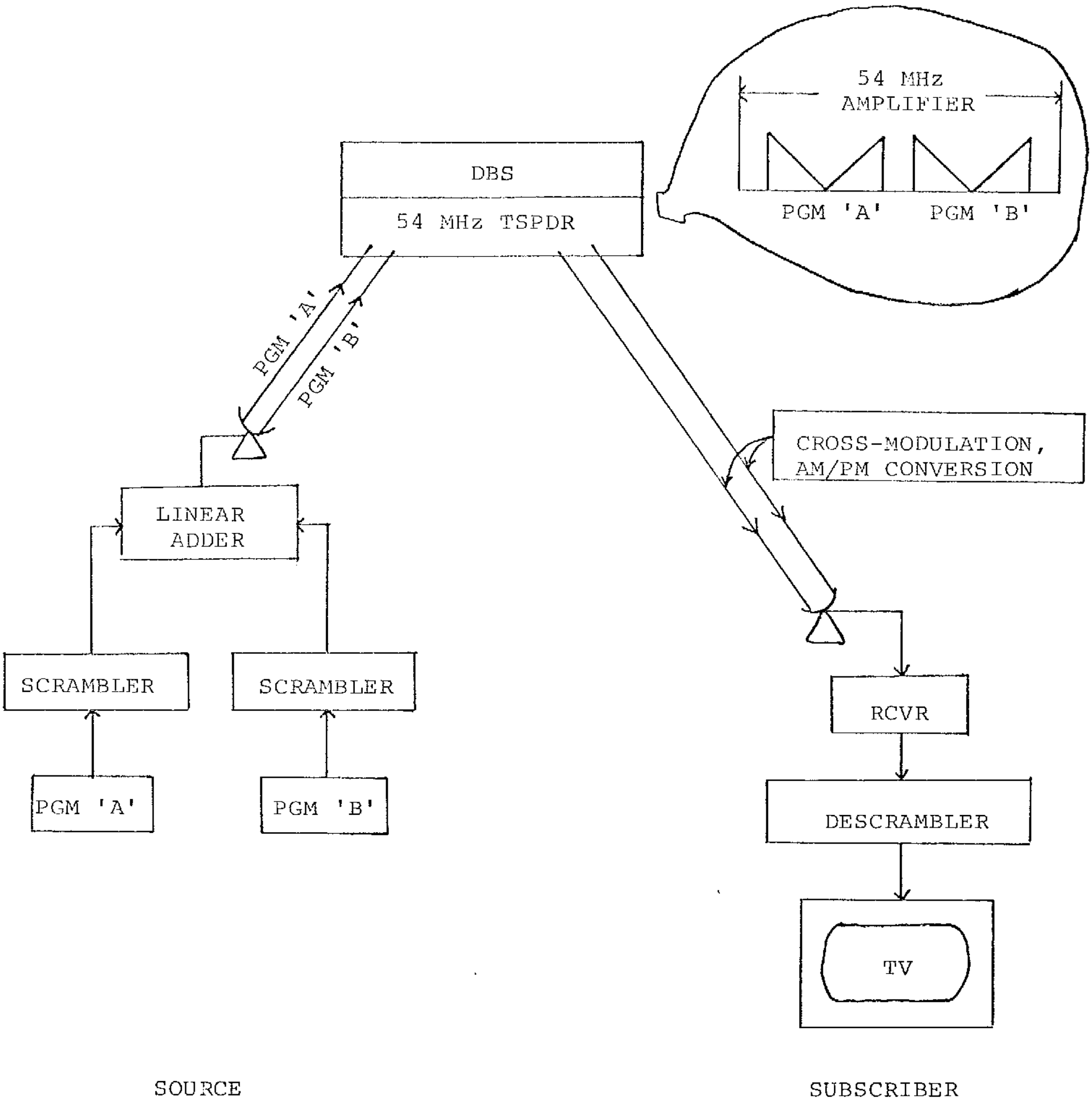
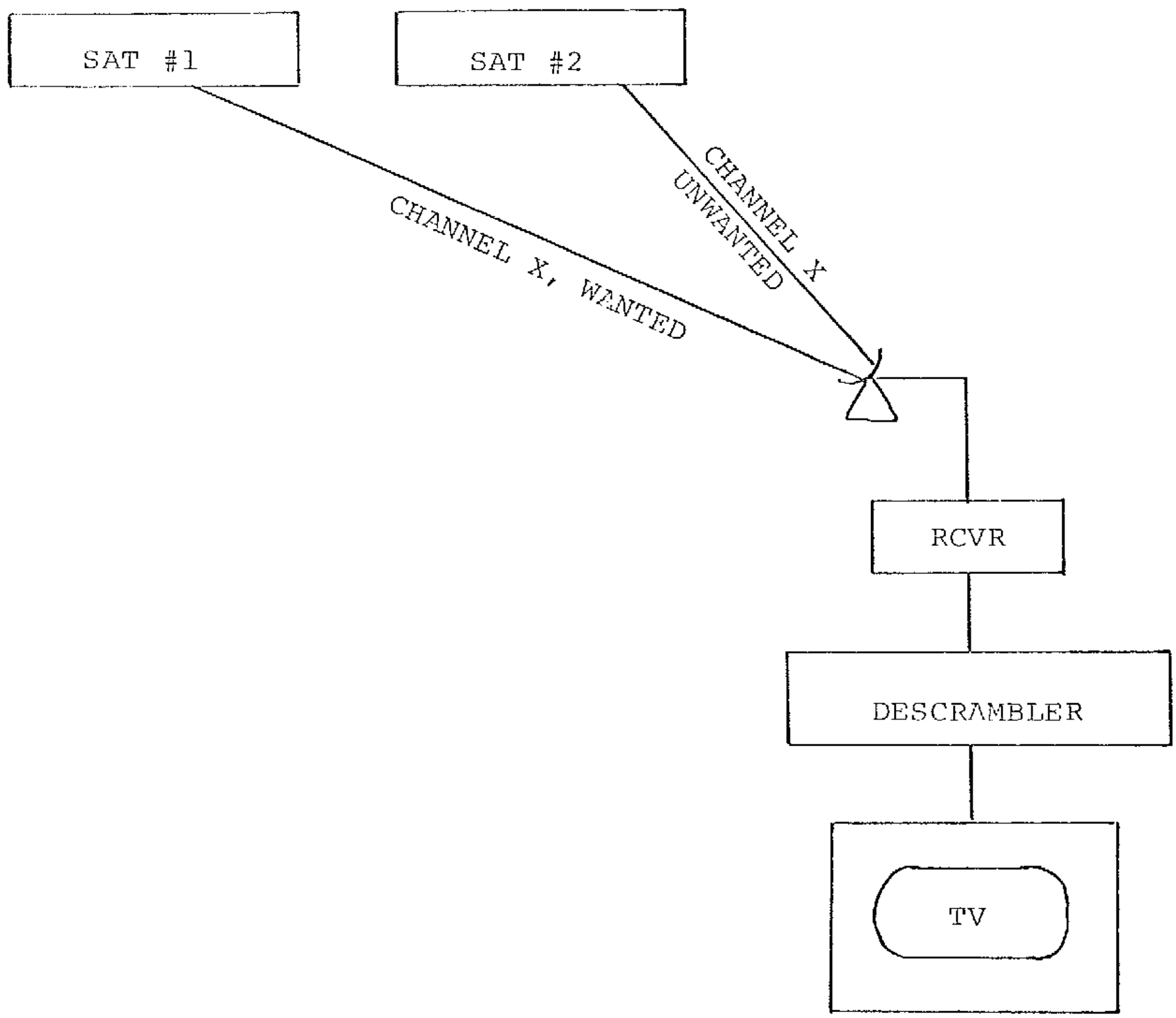


FIGURE 8

DBS NETWORK CONFIGURATION #8

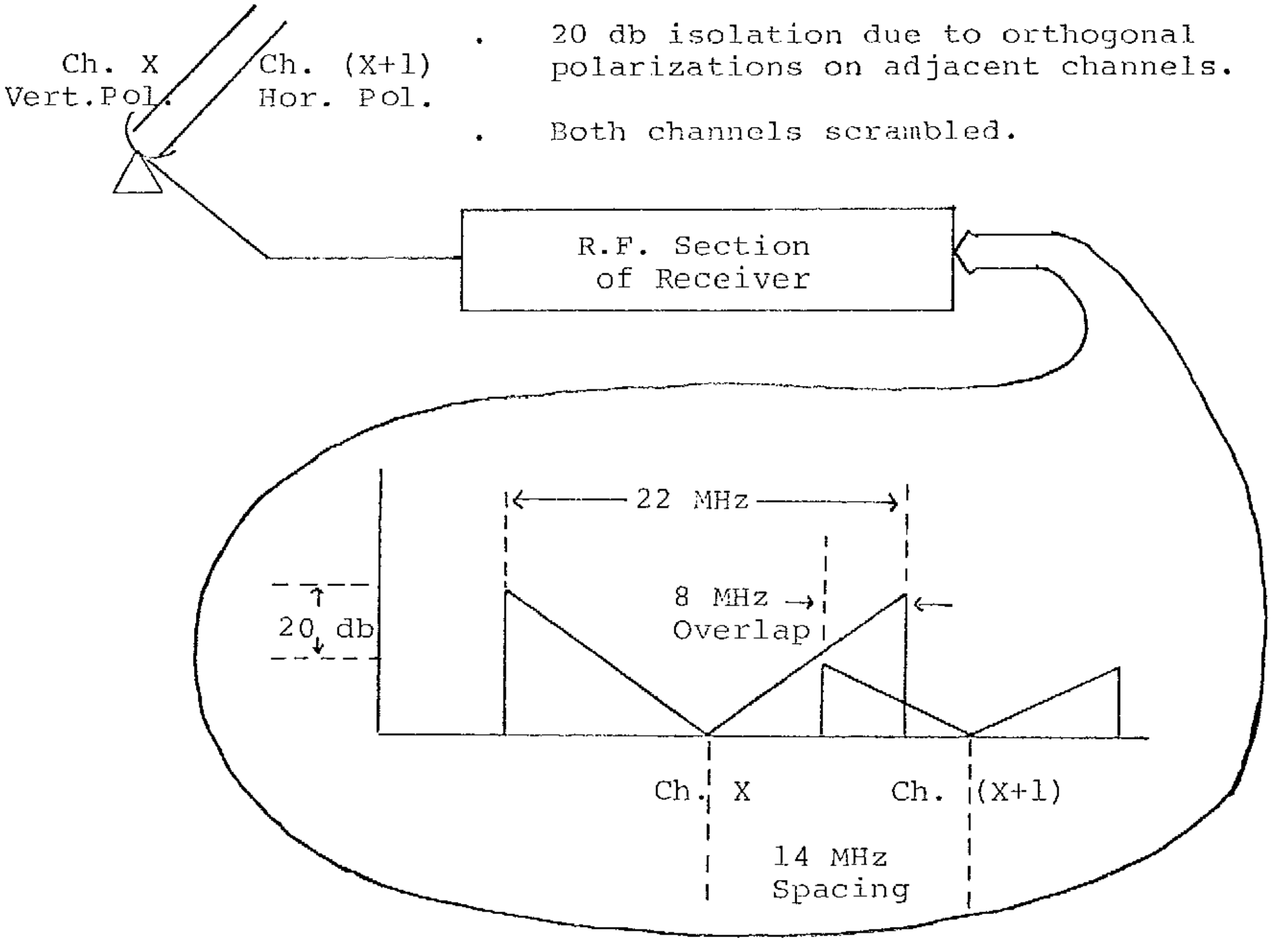


Synchronization Problem

Discussed in detail in paragraph 3.3.

3.2.9 DBS Network Configuration #9

- Adjacent-channel sideband overlap.
- Channel carriers are spaced 14 MHz.
- Individual Carson's Rule* bandwidth is 22MHz.
- 20 db isolation due to orthogonal polarizations on adjacent channels.
- Both channels scrambled.



Synchronization Problems

20 db pre-detection C/I ratio should yield adequate S/I ratio to assure no aliasing in synchronization. See analysis in Section 3.3

---

* Carson's rule states that the RF channel bandwidth required for full FM threshold effect is:

2 X (highest modulating frequency maximum frequency deviation)

3.2.10 DBS Network Configuration #10

- Simultaneous broadcast of two scrambled programs.
- Subscriber wishes to view one scrambled signal and record another.

Potential Problem

- No network problem.
- VTR will not record random analogue or digital signals without normal TV frame and line synchronization pulses.

Solution #1

Descrambled signal must include normally recognizable frame and line synchronization pulses.

(Trivial) Solution #2

Use separate decoder.

Special Synchronization Problems - None.

If the scrambled signal can be recorded and played back without compromising bandwidth or dynamic range, the descrambler will not differentiate between a previously-recorded and 'live' signal.

3.3 Multiple Channel Environment

3.3.1 Sources of Coherent Interference

Widespread acceptance of DBS service by the public implies that subscribers will be offered a number of simultaneous program choices. For the purposes of this study it may be assumed that all programs are scrambled. Given the finite attenuation properties of system elements such as bandpass filters, antenna sidelobes, polarization selectors, etc., and the compromises that must be made in system design because of cost and technical trade-offs, cross-talk and interference between DBS channels must be expected and allowed for in a multi-channel system. This crosstalk interference can occur at several points in the DBS system.

(i) Crosstalk at Baseband

Cross talk in a baseband channel before it is scrambled will simply be carried with, presumably, high fidelity to the output of the descrambler. Crosstalk at baseband can occur as a result of reduced isolation in digital electronic switches.

(ii) Crosstalk Between Two Channels in the Same Satellite Transponders

Telesat predicts maximum crosstalk to be -50db.

(iii) Co-Channel Interference from Another Earth Terminal at a Satellite

Co-channel interference can occur at a satellite when a satellite antenna main lobe aligns with the sidelobes of an earth terminal uplinking to another satellite at the same normal frequency. In Ref.3, Telesat calculates a typical worst case to be 29.9 db (Table 2.5.6, carrier-to-interference ratio).

(iv) Co-Channel Interference from Another Satellite In a DBS TVRO

Co-channel interference can occur at a DBS earth terminal when a sidelobe of the earth terminal antenna aligns with the main lobe of an adjacent satellite downlinking on the same nominal frequency.

In Ref.3 Telesat calculates worst case C/I to be 20.9 db (Table 2.5.6) at a 1.8 meter earth terminal.

Combining the effect of the uplink and downlink co-channel interference gives a worst-case C/I of 20.5db.

Based on interviews with cognizant DOC staff, the expected minimum level of C/I for co-channel interference, to be set at the forthcoming Regional Administrative Radio Conference, 1983 (RARC'83) will be in the range 30 to 35db. This is some 10db more conservative than the Telesat estimate. The Telesat estimate is therefore considered to be a safe planning number.

(v) Adjacent Channel Interference

Close spacing of carriers in the DBS frequency bands will be necessary to make best use of the limited 500 MHz bandwidth. Projected carrier spacings are in the order of 14 MHz. With FM channel bandwidths in the order of 22 MHz, there is a potential 8 MHz overlap of sidebands from adjacent carriers in any channel. This situation is illustrated in network configuration #9. The expected isolation of the wanted signal from the aggregate of all unwanted signals is 20 db. Subjectively, the isolation between these signals is some 17 db better than the 20 db, because of the incoherent nature of the interfering signals. This subjective improvement has little meaning however as far as digital synchronizing circuits are concerned.

3.3.2 Effects of Coherent Interference

(i) Crosstalk at Baseband

The likelihood of any serious cases of crosstalk at baseband is extremely remote. As a potential source of interference in synchronizing scrambled television signals, its' contribution is negligible.

(ii) Crosstalk Between Two Channels in the Same Satellite Transponder

With this type of crosstalk limited to -50db, the likelihood of its desynchronizing scrambled signals is negligible.

(iii) Co-Channel Interference at a Satellite from Another Earth Terminal

This phenomenon is discussed in more detail later but it can be stated here that a worst case interference level of 29 db below the wanted signal will not be significant desynchronizing factor.

(iv) Co-Channel Interference from Another Satellite at a DBS TVRO

The effect is discussed with (v) below.

(v) Adjacent Channel Interference

For this analysis it is convenient to discuss adjacent channel and co-channel interference together. Aggregating the two effects results in a carrier-to-interference ratio in the order of 19 to 20 db.

In considering the degradation of a digital message by in-channel coherent interference it must be borne in mind that the amplitude statistics of aggregated coherent interference differ significantly from those of noise. More specifically the peak amplitude of aggregated coherent interference can be expected to exceed the rms value by a factor between 1 and 3, say, whereas in the case of noise the instantaneous peak amplitude will occasionally exceed the rms value by an order of magnitude or more.

In other respects though coherent interference will appear as noise background in a picture, assuming none of the interfering FM carriers is at the exact same frequency as the wanted carrier. (An interfering channel may have the same nominal carrier frequency as the desired channel but the two frequencies will never coincide exactly for more than an instant because they do not have a common reference.)

Panter (Ref.4) has analysed quantitatively the effect of coherent FM interference in an FM channel in which the receiver is operating in a full-limiting region. In his analysis Panter considers the interference due to two frequency-modulated signals, the desired signal, $e_1(t)$, and an interfering signal, $e_2(t)$ where

$$e_1(t) = \cos(\omega_1 t + \beta_1 \sin pt)$$

$$e_2(t) = \rho \cos(\omega_2 t + \beta_2 \sin qt + \psi_0), \ \rho < 1,$$

ω_1 and ω_2 are the carrier frequencies, p and q the modulating frequencies, and $\beta_1 = \Delta\omega_1/p$, $\beta_2 = \Delta\omega_2/q$, the modulation indices. Combining the two signals yields an instantaneous amplitude term and an instantaneous RF frequency term. We assume the amplitude term is removed by limiting. The instantaneous frequency ω_1 is shown to be

$$\omega_1(t) = \frac{d\phi}{dt} = \omega_1 + \Delta\omega_1 \cos pt - \sum_{s=1}^{\infty} \frac{(-1)^s \rho^s}{s} \sum_{m=-\infty}^{\infty} J_m(s\beta_1)$$

$$\times \sum_{n=-\infty}^{\infty} J_n(s\beta_2)(s\omega_2 - s\omega_1 - mp + nq)$$

$$\times \cos\{(s\omega_2 - s\omega_1 - mp + nq)t + s\psi_0\}$$

Inspection of the components making up the instantaneous frequency $\omega_1(t)$ reveals five significant features.

(i) If $\omega_2 \neq \omega_1$, the detected signal does not in general contain the interfering modulation q.

(ii) For $S \ll 1$ as is the case for interference being considered for DBS, the infinite series in s can be truncated after s=1 because the next term in the series contains S^2.

(iii) All sum and difference combinations of $(\omega_1 - \omega_2)$, p, and q and their harmonics appear as sidebands.

(iv) The frequency deviation, and hence the post-discriminator amplitude of the wanted modulation p is proportional to the original frequency deviation β_1, whereas the post-discriminator amplitude of any interfering frequency is proportional to the frequency itself.

(v) The amplitude of the interfering signals is characterized by the same triangular effect as is noise output of FM discriminators. Normal FM de-emphasis will therefore reduce the triangular effect significantly.

The net effect is to raise the post-discriminator signal-to-interference significantly above the original carrier-to-interference ratio. If, as expected, the carrier-to-integrated- interference ratio is 20db or greater in DBS receiver, the further suppression of the interference during demodulation should ensure an adequate margin for error-free recognition of digital signals.

As a further comment on the effects of coherent interference in an FM receiver Terman, Ref.5, in discussing interference in audio FM channels, notes that suppression of signals at the exact-same carrier frequency - i.e., true co-channel - is almost perfect as long as the wanted signal is 6 db higher than the unwanted one. The "sizzling" due to beat-notes from a closely-spaced carrier are rendered inaudible by the demodulator if the interfering carrier is 10 to 20 db down.

Finally, in C. Loo's work in Ref.6, subjective tests indicate that, with C/I ratios of 20 db, background distortion is essentially imperceptible.

3.4 System Noise

In colour television reception an unweighted signal-to-noise ratio of approximately 37 db is necessary to maintain picture impairment at or below the threshold of perceptible impairment.* It is also generally agreed that a picture with an unweighted signal to noise less than 25 db is badly impaired and viewers in the 1980's would not accept it. From the point of view of reliable detection of digital signals in a conventional digital system a signal to noise ratio of 20 db would be an acceptable design figure, assuming the signal is not otherwise compromised by mismatch between the digital pulse shape and the system's effective filter response. However, extrapolation of this figure to digital bursts time-multiplexed with analogue television signals cannot be justified until some particular examples are examined in the laboratory and in the field and until the channel is characterized. The analysis in Section 3.7 illustrates a theoretical approach to the noise problem for a specific type of digital signal sent in the burst mode, but the caveats noted above still apply for, while theory can point the way, measurements in the real situation are vital.

3.5 Channel Response

It was noted above that post-demodulation signal-to-noise and signal-to-interference ratios in the order of 20db were acceptable for reliable transmission of digital signals as long as the bandpass characteristics of the communications channel were properly matched to the digital waveform. The ideal channel for optimizing noise performance and undistorted transmission of digital signals cannot be realized in practice because the required attenuation is uniform to a certain upper frequency limit at which point it must be "rolled-off" very precisely at higher frequencies. The upper band edge characteristics of a practical channel must therefore be designed for a compromise between noise and spectral requirements. There is ample theoretical and experimental evidence that significant reductions of RF bandwidth below the Carson's rule figure in an FM

---

*DOC Broadcast Procedure 23 calls for 40 db carrier-to-noise, reference to 4 Mhz, for Canadian cable systems. This predetection C/N figure produces 37.2 db Signal-to-Noise ratio after envelope detection.

satellite channel has a pronounced negative effect on BER. The same holds for too-low baseband frequency cut-off. The latter is well illustrated in the work of Taylor and Haykin in Ref.7 on high-speed digital signalling through the HERMES satellite. Taylor and Haykin observed that simulated transmission of a 60 MHz FFSK signal through the satellite channel with a 36 MHz low-pass filter interposed between the FFSK modulator and the input to the transponder caused an order of magnitude increase in the BER. Similarly, the work of C. Loo in Ref.8 shows that increasing the carrier deviation from 6 MHz to 8.5 MHz, in an otherwise constant FM channel carring binary signals at 4.5786 Mbs, improves the post-detection signal-to-noise by approximately 4 db but the improved noise performance is more than offset by the degregation in pulse identification, as determined by conventional eye-openings. The cause of the increase in BER is intersymbol interference due in turn to the fact that a peak deviation of 8.5 MHz was too high for a signal to be received with an IF filter of 19 MHz. Pulse distortion resulted. Loo concluded that an unweighted, peak-to-peak,* less sync, signal-to-noise ratio of 27 db in a channel that is designed for low sideband distortion at RF and full high frequency response at baseband will provide reliable transmission of teletext signals in the Telidon format.

3.6 Effects of Bit Error Rate on Addressing and Control Addressing

The analysis contained in this Section, and the results thereof, are highly speculative but they do show the magnitude of the problem of addressing a large subscriber population. The bit rates necessary to address various population sizes are derived for both line-inserted and in-sync data packets.

If addressing and authorization data is transmitted continuously there are a number of possible ways to do it. For example:

a) The data could be amplitude-modulated on the FM audio signal,
b) the data could be transmitted on a separate sub-carrier, perhaps in combination with digital audio and descrambling keys; or
c) the data could be inserted, à la teletext, in blank lines in the video; or

---

*The peak to peak level is used by Loo because the digital transmission occurred during the normal luminance and chrominance period of a horizontal line. Modulation was from reference black to reference white.

d) the data could be inserted as a burst in place of the horizontal sync pulse.

Cases a) and b) are fairly straightforward and no synchronization problems would be expected for SNR's of 15 db or better in the data bandwidth.

In case c) a broadcast Telidon format might be assumed, where the horizontal sync pulses are undisturbed, at least during the Vertical Blanking Interval.

In the Telidon mode the bit rate is 5.72 Mbits/second. A packet consisting of a 16-bit (8 cycles of 2.86 MHz) bit-sync sequence at the start, followed by an 8-bit byte sync character, and 32 bytes of information is sent on each horizontal line used. Two lines are used normally per field. At 2 lines per field and 60 fields per second, 3840 bytes of information may be transmitted each second in this mode.

(At the slower rate of 2.4 mega symbols/per second that the Leitch 8-level PAM system uses, 96 data symbols could be transmitted, each with 3 bits of information, for a total of 36 bytes per line).

If the addressing/control/descrambling information for each subscriber takes as few as 4 bytes, then a (Telidon-like) system could service:

960 subscribers per second;
57,600 subscribers per minute; or
576,000 subscribers per 10 minutes.

If as another possibility, only one subscriber message were transmitted per line; at 2 lines per field 7200 subscribers could be serviced per minute; and it would take 35 minutes to service half-a-million. The rate at which subscribers can be addressed with this scheme is shown in Table 1.

In case d) we might assume a data packet that replaces the entire horizontal sync period of 0.165H (where H duration of one horizontal sweep). The packet might contain a 16-bit bit-sync sequence of alternating 1's and 0's, an 8-bit byte sync sequence, and a number of 3-bit, 8-level symbols, as shown in Figures 9 and 10. This scheme, using the data as described below, could address 15,734 subscriber per second, or almost a million per minute.

Two bits in the data can be used to indicate whether the sync pulse on this line is to be a regular, a vertical retrace, or an equalization pulse as described in Refs. 22 and 24.

BINARY DATA RATE $\times 10^6$	BITS/LINE	DATA BITS / LINE	SUBS/LINE	SUBS/SEC	SUBS/MIN	SUBS/HOUR $\times 10^6$
5.72	280	256	8	960	57,200	3.456
4.60	225	200	6	720	43,200	2.592
2.40	120	96	3	360	21,600	1.296

TABLE 1

SUBSCRIBER ADDRESSING RATES VIA LINE-INSERTED MESSAGES

(4 bytes per subscriber
2 lines per field)

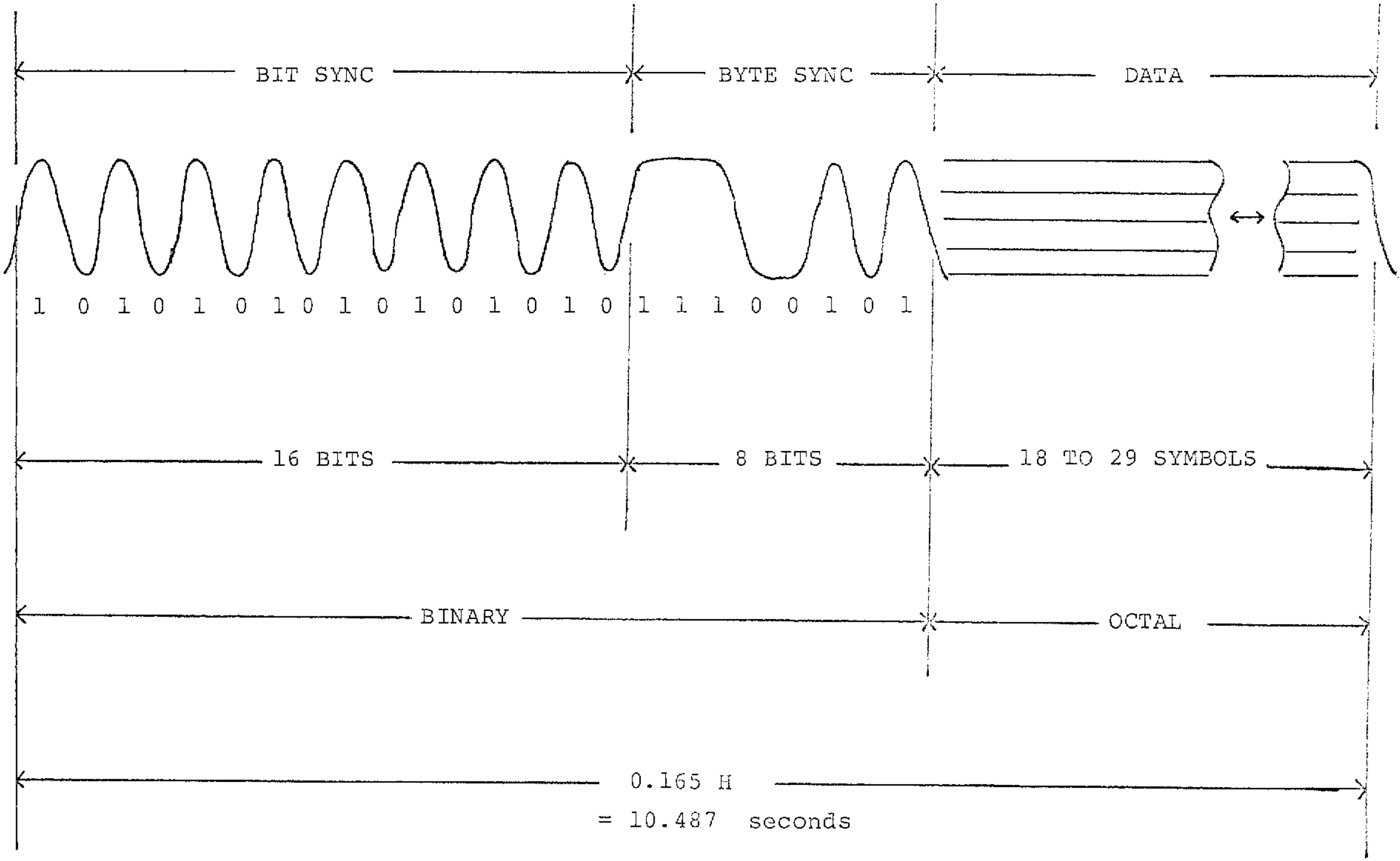


FIGURE 9

SIGNAL FORMAT

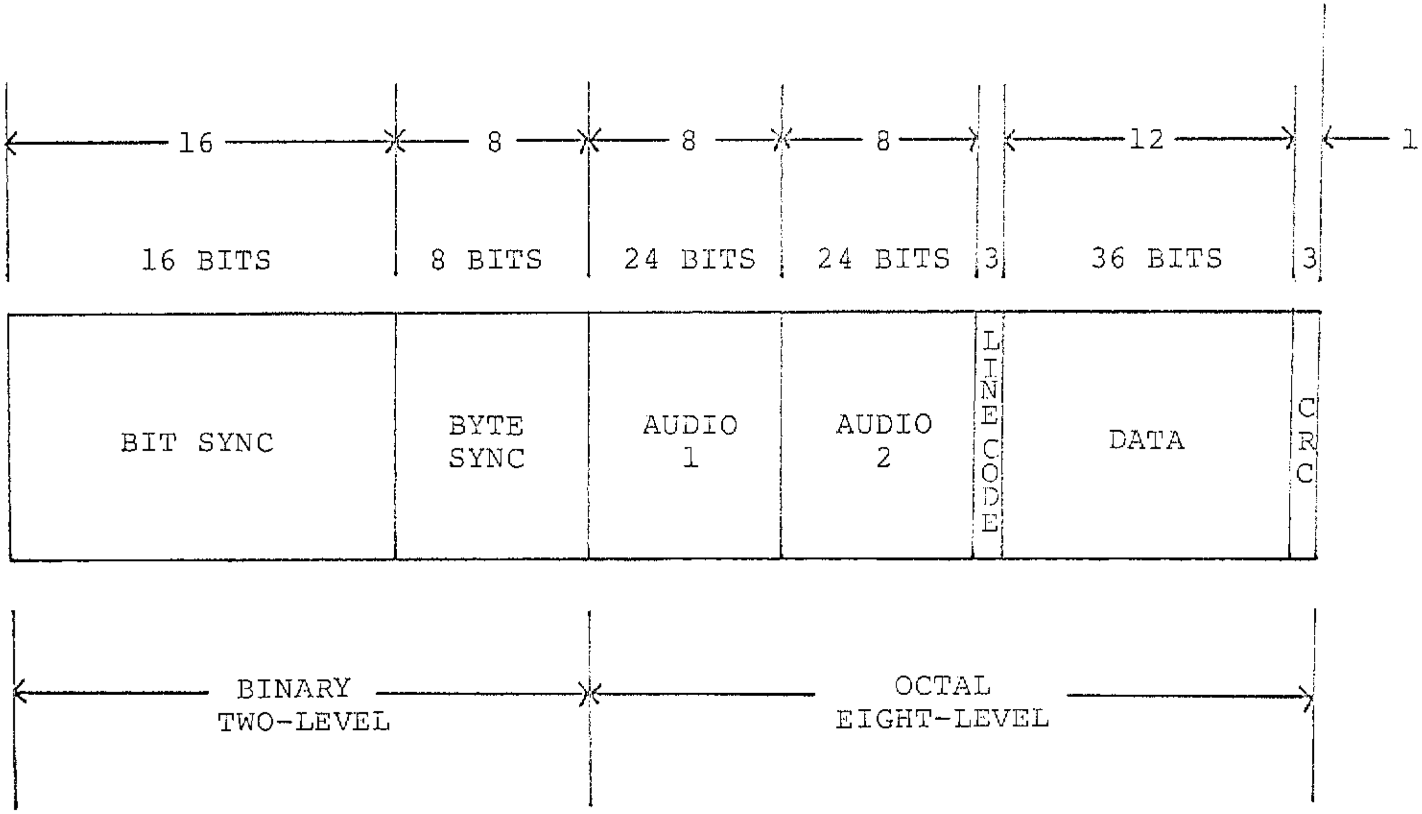


FIGURE 10

PACKET LAYOUT

Others can be used for audio. For example, if we assume that there are two audio signals sampled at twice the line rate, with twelve bits per sample then the audio could take 48 bits per packet. If subscriber addressing requires 36 bits, data could be transmitted at about 5.5 megasymbols per second.

Removal of one audio channel (or reduction of the accuracy to a single 12-bit sample per line) and reduction of the addressing requirements to 27 bits, could reduce the symbol rate to $4x10^6$ per second. The data rate (in mega-symbols per second) versus packet length in given in Table 2.

If 25 db SNR is attained, the 8-level error rate will be about $1x10^{-4}$ and the binary about $1x10^{-8}$, if synchronous demodulation is used.

With an error rate of Pe, it might be expected that a packet would be lost due to sync problems if any of the 8 byte-sync bits were wrong with probability 8Pe.

Thus, if 15,734 subscribers were being addressed per second, with an "in-sync" data burst, (944,000 per minute), one would expect an address to be missed once every thirteen minutes or so, (due to byte-sync loss) which would not be any problem.

The probability of error for 8-level symbols is about 12db's worth of SNR worse than for binary. This is about four orders of magnitude worse in probability. Thus, if the probability of binary error were $1x10^{-8}$, an address or authorization might be missed with probability $1.2x10^{-3}$, i.e. once in 800 times. The implication being that 1200 subscribers out of a million might not be successfully addressed in any one-minute authorization cycle; and one might be missed twice.

In the case of line-inserted data packets (case c) above, where 360 to 960 subscribers were addressed per field (instead of 15,734) with binary signals, the error rate of $1x10^{-8}$ would translate to a probability of a missed subscriber of $3.6x10^{-7}$, which would mean that virtually all addresses would almost always be correctly received.

The numbers generated in this Section are pure conjecture and very sensitive to the actual performance of real systems. They are affected by modulator/ demodulator design, the modulation method, data rates, ground station transmitters and receivers, transponder resonse, the impulsive noise environment, interference, and so on; and should be treated as very tentative.

SERVICE	NUMBER OF SYMBOLS	NUMBER OF DATA BITS	FREQUENCY X 10^6
EMPTY	26	0	2.48
32 BITS	37	32	3.53
1 AUDIO PLUS 27 BITS	43	51	4.10
2 AUDIO PLUS 36 BITS	54	84	5.15

INCLUDES: 16-bit bit sync block,
8-bit byte sync character,
1 symbol line code,
1 sumbol cyclic redundancy check.

TABLE 2

TRANSMISSION RATE FOR IN-SYNC DATA PACKETS

Assessment of synchronization performance is critically dependent on whether or not the sync detection circuitry has been designed in an optimal fashion - that is, with linear matched filters and phase - and delay - locked loops; or for a noise-free environment - that is, dependent on the detection of undistorted, sharp edges. There is some hope of analyzing the former; the latter is amenable only to simulation (if a good enough model of the channel is present) or actual experimentation. The effects of noise on one type of bit-timing recovery from one type of asynchronous burst is described in some detail in the next section.

3.7 The Effect of Additive Noise on Edge Sensitive Bit Timing Recovery from 'Start' Pulses

An approximate idea of the effect of noise on NRZ binary PAM when the bit timing is recovered by the detection of the leading edge of a start-pulse may be obtained by considering the reception of a train of raised-cosine pulse of width 2T seconds as shown in Figure 11.

Each pulse, and the start-pulse can be represented by the expression:

$$g(t) = \frac{A}{2}\left(1 + \cos\frac{\pi t}{T}\right); -T < t < T$$

We are assuming that bit timing is determined when the leading edge of the start-pulse crosses the A/2 amplitude level. We can approximate the effect of additive noise on the time of the level crossing by considering the situation shown in Figure 12. Here, we assume noise of amplitude n is added to the pulse at time $t = -T/2$. This shifts the time of the level crossing τ seconds, where

$$\frac{n}{\tau} = -\frac{dg}{dt} \Big/ t = -T/2$$

or

$$\tau = \frac{-2T}{A\pi} n$$

Actually, the level crossing at $t = -\tau$ is caused by noise, n_1, added at time t_1; but, as can be seen from the diagram the approximation made is reasonable, expecially for small n.

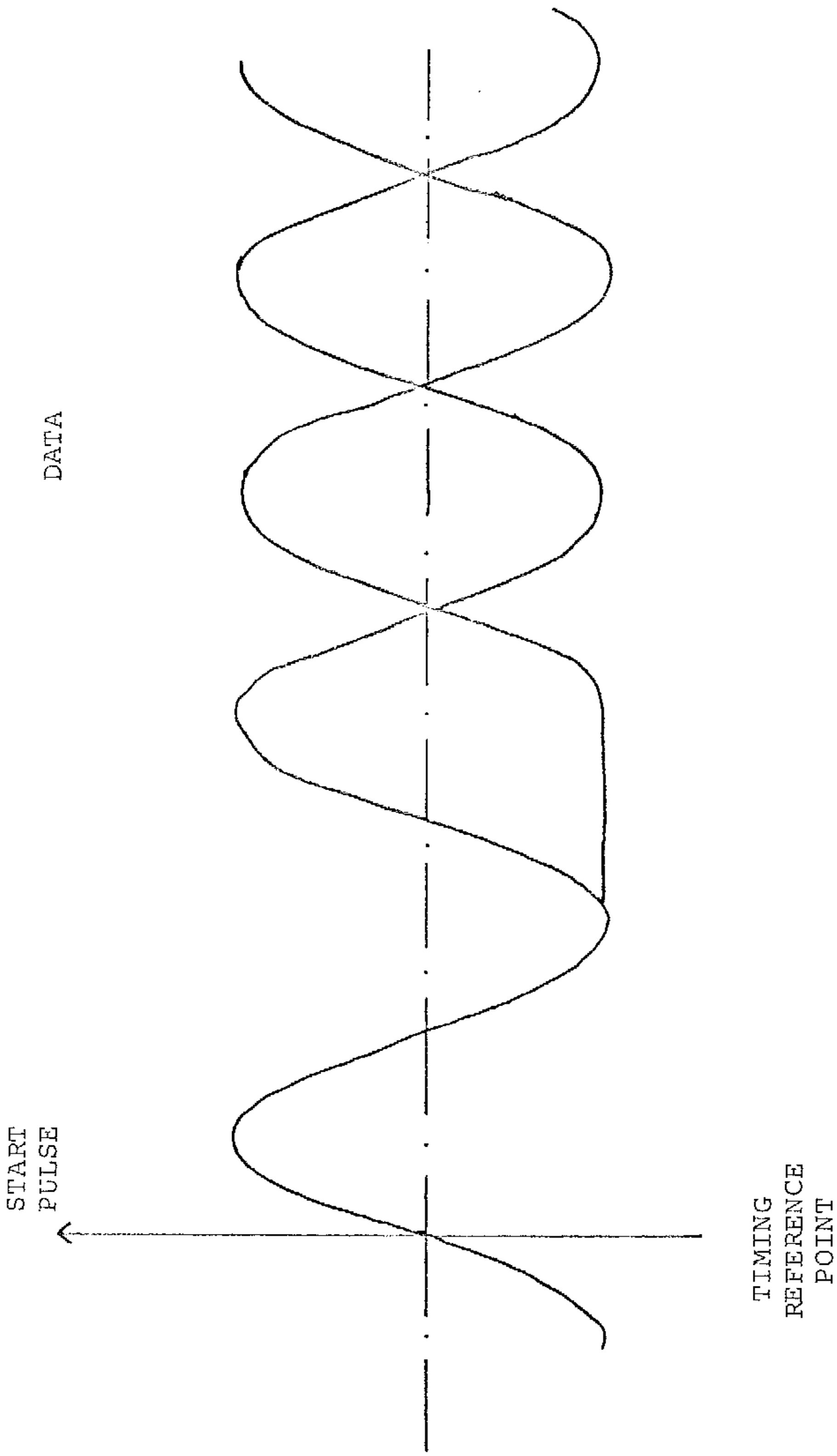


FIGURE 11

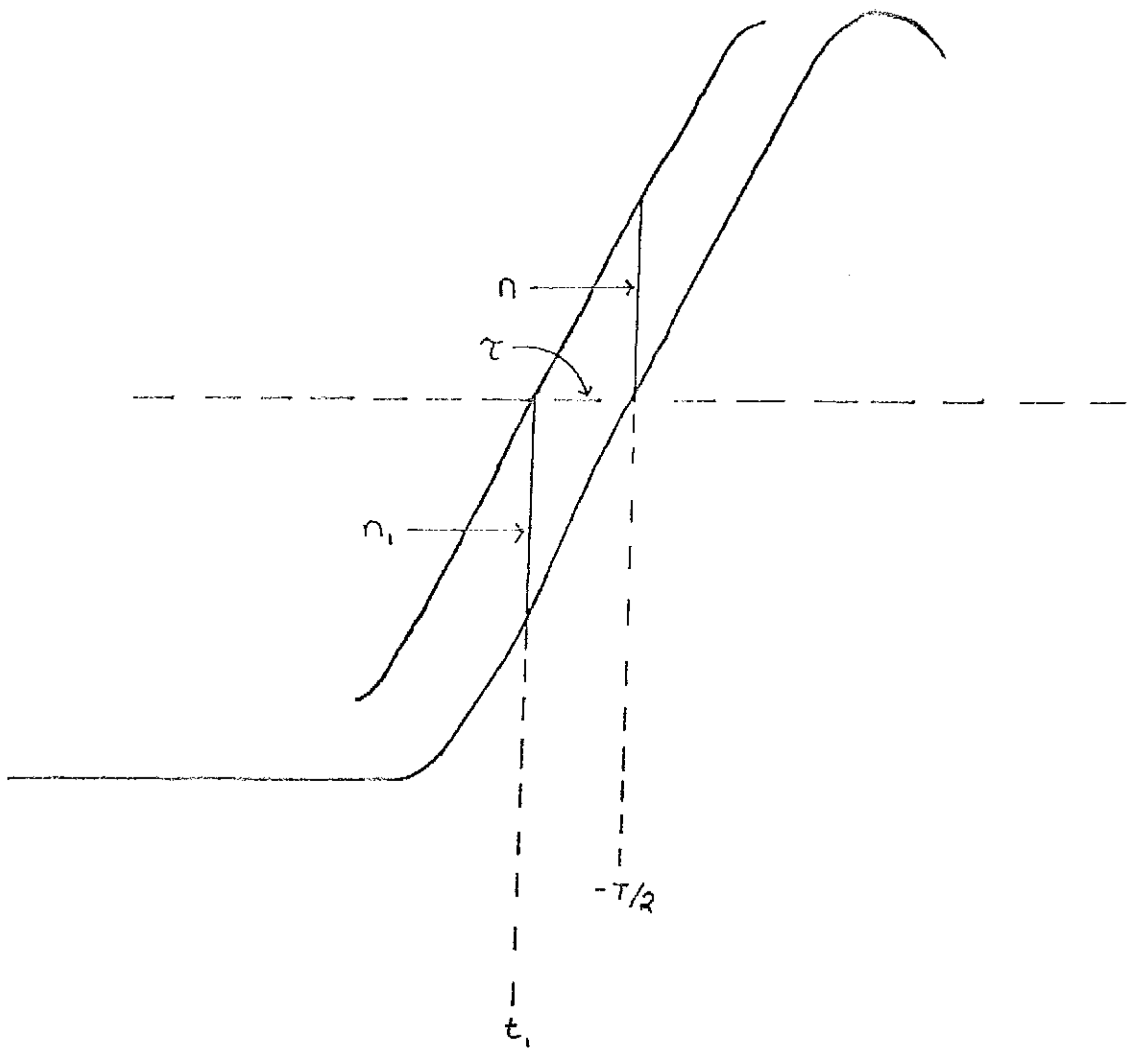


FIGURE 12

The effect of mis-timing of the probability of error can be seen in Figure 13. The eye opening as a function of the timing error, τ , is

$$e(\tau) = A \cos \frac{\pi t}{T} \; ; \; -T/2 < t < T/2$$

The conditional probabilities are shown in Figure 14. If we assume that the additive noise is gaussianly distributed with zero mean, the probability of error is

$$P_e(\tau) = 1/2 \; \text{erfc} \left(\frac{A}{2\sqrt{2}\sigma} \cos \pi t/T \right) ; \; -T/2 < t < T/2$$

where σ is the rms value of the noise;

and

$$\text{erfc}(u) = 1 - \text{erf}(u), \text{ where}$$

$$\text{erf}(u) = \frac{2}{\sqrt{\pi}} \int_0^u e^{-y^2} dy$$

Under the assumptions that have been made, the distribution of τ is also gaussian with zero mean and standard deviation.

$$\sigma_\tau = \frac{2T}{A\pi} \sigma$$

Thus $$\rho(\tau) = \frac{A}{2\sigma T} \sqrt{\frac{\pi}{2}} \; e^{-\frac{\pi^2 A^2 \tau^2}{8\sigma^2 T^2}}$$

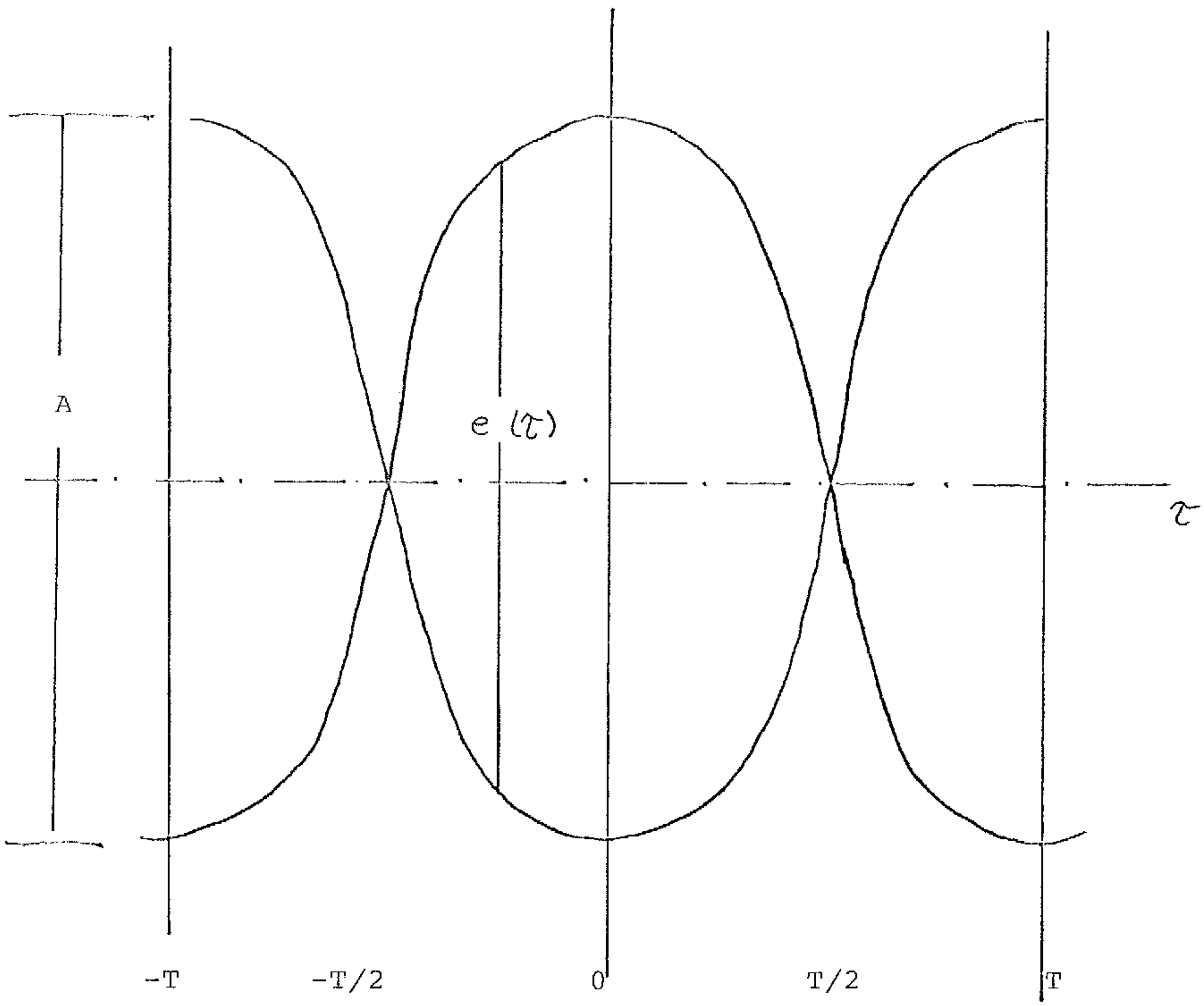


FIGURE 13

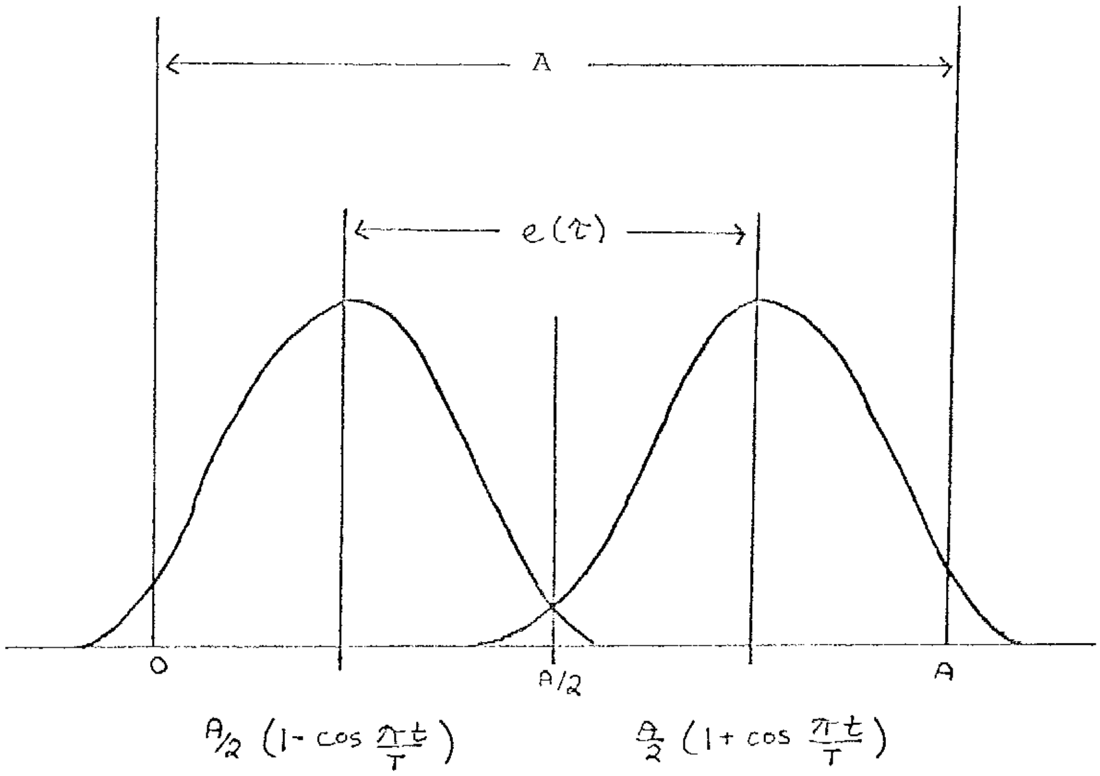


FIGURE 14

The average probability of error may be expressed as:

$$P_e = \int_{-T/2}^{T/2} p(\tau)\, P_e(\tau)\, d\tau$$

or

$$P_e = \frac{A}{4\sigma T}\sqrt{\frac{\pi}{2}} \int_{-T/2}^{T/2} e^{-\frac{\pi^2 A^2 \tau^2}{8\sigma^2 T^2}} \operatorname{erfc}\left(\frac{A}{2\sqrt{2}\sigma} \cos \frac{\pi\tau}{T}\right) d\tau$$

For large SNR, i.e. $A^2/\sigma^2 >> 1$, and small τ, the complementary error function may be approximated by:

$$\operatorname{erfc}(u) = \frac{e^{-u^2}}{u\sqrt{\pi}}$$

Thus, the average probability of error becomes:

$$P_e \approx \frac{1}{2T} \int_{-T/2}^{T/2} e^{\frac{-A^2}{8\sigma^2}\left(\frac{\pi\tau}{T} + \cos^2 \pi\tau/T\right)} dt$$

We might also consider the timing error to be uniformly distributed over some interval $[-\Delta, \Delta]$. In this case the average probability of error would be

$$P_e = \frac{1}{4\Delta} \int_{-\Delta}^{\Delta} \operatorname{erfc}\left(\frac{A}{2\sqrt{2}\sigma} \cos \pi\tau/T\right) d\tau$$

$$= \frac{1}{2\pi\alpha} \int_{0}^{\pi\alpha} \operatorname{erfc}\left(\tfrac{1}{2}\sqrt{\frac{\rho}{2}} \cos x\right) dx$$

which for large SNR can be approximated by

$$P_e \approx \frac{\sigma}{\sqrt{2}\,\Delta A} \int_{-\Delta}^{\Delta} \frac{e^{-\frac{A^2 \cos^2 \pi\tau/T}{8\sigma^2}}}{\cos \pi\tau/T}\, d\tau$$

or, if we let $\chi = \pi\tau/T$,

$$P_e \approx \frac{1}{\alpha\pi}\sqrt{\frac{2}{\rho}} \int_{0}^{\pi\alpha} \frac{e^{-\rho\frac{\cos^2 x}{8}}}{\cos x}\, dx$$

where $\rho = (A/\sigma)^2$ is the signal-to-noise ratio; and

$\alpha = \Delta/T$ is the range of the timing uncertainty.

4. REVIEW AND UPDATE OF CURRENT CANDIDATE SCRAMBLING SYSTEMS

The earlier report (Reference 1) identified twelve generic types of scrambling systems. In a subsequent analysis and presentation of these systems (Ref. 2) the twelve types were broken down into three categories viz: unsuitable for DBS scrambling; suitable for DBS scrambling and currently feasible; acceptable for DBS scrambling at a future date. The data from Ref. 2 are reproduced in Table 3. A literature search including the monitoring of current journals revealed no new system concepts that would be revelant to the current study. However, attendance at the 1982 NCTA and CCTA Conferences indicated that definite progress towards implementation of certain of the candidate systems was being made. A system being developed by Leitch Video Limited of Toronto is a case in point.

The Leitch system is a hybrid derived from the concept of candidate system No. 11 of Table 1. The differences lie in the fact that the Leitch approach is to sample on a frame by frame basis the picture information only, disregarding sychronization and colour burst signals. Each frame is subsequently broken down into blocks, these blocks being interchanged in a random manner to scramble the picture information. Furthermore, information within the blocks can also be reordered randomly so that there is in essence a double scrambling of the picture information. The digital information is subsequently converted back to analogue form, combined with the appropriate synchronizing and reference signals and transmitted in an ordinary analog bandwith TV channel. This process of digitizing, encrypting or disordering and re-formatting to analog is commonly called analog encryption, and is subject to the problems described in Appendix A.

Four other noteworthy systems are MAAST (Multiple Audio Addressable Secure Television) by Telease Inc.; a Digital Baseband Encryption System under development at Digital Video Systems; the Zenith Z-TAC; and the OAK Orion System.

MAAST utilizes denial of synchronizing pulses, audio encryption and video inversion as a scrambling technique. Subscriber authorization and audio decryption messages are transmitted as an encrypted code word on one of the unused lines in the vertical retrace interval. MASST combines features of candidates 5, 7, and 10 of Table 3. MAAST can accomodate five audio channels with a high level of encryption.

TABLE 3: SCRAMBLING CANDIDATES vs TECHNICAL CONSIDERATIONS

Note: . It is assumed that the decoder will be a separate, self-powered unit from the TV
. *see paragraph indicated
. norms given in relevant sub paragraphs of section 3

CANDIDATE	Decoder Results (norm) / Scrambling Method and Current Status	Decoder Cost ($100) (3.2*)	Reliability (3.3*)	Robustness (3.4*)	Size (3.5*)	Degree of Security . trivial . easy . hard . secure (3.6*)	Residual Intelligibility (3.7*)	Degree of Restoration (3.8*)	Degree of Interference with Other Signals (3.9*)	Bandwidth Requirements (3.10*)	Encoder Costs (3.11*)	Conformity to Current Standards, Regulations and Policies (3.12*)	Ease of Multi-Channel Scrambling or "Tiering" (3.13*)	Effects of Redistribution (3.14*)	Availability (3.15*)
1	Non-Standard Transmission Frequency	very low	high	high	small	trivial but acceptable for data and audio	N/A	N/A	none	N/A	low	low	N/A	N/A	Yes
2	Interfering Carrier	very low ($12 to $25)	N/A	high	small	easy	norm	below norm	medium to high	norm	low ($1K to $2K)	low	poor	difficult	[illegible]
3	Continuous Video Insertion	low (approx. $50)	high	high	small	easy	norm +	norm +	norm +	norm	low (approx. $1000)	good	poor	good	[illegible]
4	Sine Wave Sync Suppression	high ($170)	high	high	small	easy	norm	below norm	norm	norm	low	good	up to four	good	Oak
5	Gated Sync Suppression	low ($50)	high	high	small	easy	below norm	norm +	norm	norm	approx. norm	good	good	good	Jerrold Blonder/ Tongue Dynacom
6	Continuous Carrier Suppression	unknown	unknown	likely to be above norm	likely to be small	unknown	unknown	probably above norm	meets norm	meets norm	unknown	poor	good	good	Experimental (Scientific Atlanta)
7	Line Inversion	currently slightly high ($150)	high	high	small	hard	meets norm	meets norm	meets norm	meets norm	unknown	good	good	good	Oak Pay-TV Corp. American TV & Comms Corp. Zenith Satcom
8	Line Swapping	currently very high	high	high	norm	hard	meets norm	meets norm	meets norm	meets norm	low	good	good	may need some filtering	Microtime (in development)
9	Line Dicing	currently very high	high	high	currently large	hard	better than norm	approx. norm	meets norm	meets norm	meets norm	good	good	good	Westinghouse (pre-production)
10	Audio only Encryption	likely to meet norm	high	high	small	secure (audio only)	better than norm	meets norm	meets norm	meets norm	estimated to meet norm	good	good	good	pre-production Satcom Inc.
11	Complete Digital Frame Encryption	estimated norm	high	high	small	secure	better than norm	meets norm	meets norm	meets norm	estimated low	unknown	good	good	not available
12	Complete Digital Bit Stream	estimated norm	high	high	small	secure	better than norm	meets norm	meets norm	does not meet norm	estimated low	unknown	good	good	not available

The Digital Video Systems concept is based on "in-band multiplexing of digital audio, data and analogue video in a single standard video channel". It is a derivative of candidates #10 and #11 of Table 3. The usual features of multi-channel tiering, subscriber addressing and control systems are claimed in a one-way mode as is hard encryption of audio, video and data. Dual audio capability or single audio plus a 300 Kbits/s data channel are built-in standard. The system, it is claimed, can handle up to 4 billion users or terminal addresses, with up to 65,000 tiers or control conditions per address, which requires 48 bits per address.

The Zenith Z-TAC (for Zenith Tiered Addressable Converter) System also combines sync suppression and video inversion. Although horizontal sync is not removed completely it is suppressed to the point where a normal television receiver would not be able to separate the sync pulses from the luminance signal. For additional security the Zenith System can be pre-programmed to operate in independent, random, sync suppression and video inversion modes or to select video inversion according to average picture level (APL). (CCIR defines APL as the mean value of the picture d.c. component averaged over a complete frame period, excluding blanking periods, expressed as a percentage of the maximum (nominal) value of the luminance component, measurements being taken with blanking level as the zero reference.)

Discussions with the users of the OAK ORION system revealed that the OAK ORION System is essentially a combination of Candidates No. 5, 7 and 10 of Table 3, using line inversion, gated sync suppression, and encrypted audio. The OAK ORION System has seven modes of operation all of them based on single or 'double' line inversion, but structured on a continuous basis, or a field by field basis, or a line by line basis, or a random basis. No details are available on the format used in the OAK System to convey authorization of decoders, program tier labels, or changes in scrambling mode. Furthermore, no information is available on the flexibility of the central control system to change the key that controls the disordering and reordering of the line inversion sequence.

A known characteristic of the OAK system is that momentary loss of signal can cause complete loss of picture and sound until the descrambler is turned off and turned on again. This phenomenon may be due to a very fast-acting and robust default mode. Re-authorization seems to require mandatory, pre-set, initializing conditions in the decoder which are only be established at 'turn-on'.

The OAK ORION system exhibits one of the general characteristics of scrambled systems that was mentioned in an earlier chapter namely, that successful decoding of a signal stream with the added complexity of scrambling and digital control signals requires an average, or better, end-to-end channel. Experience with this particular system has shown, for example, that very low cost TVRO's, designed with reduced IF bandwidth to improve carrier-to-noise ratios, while providing an impaired but acceptable picture from a standard satellite FM transmission, are marginal components in a channel carrying complex scrambled colour television signals. Other scrambling system can be expected to behave similarly in such a channel if, as seems likely, undistorted transmission of high bit-rate address signals is require. It is characteristic of these systems that they will exhibit a steep threshold effort in the decoded and synchronized picture (and sound) at which point the reconstituted program will go from, perhaps an impaired but acceptable picture, to an annoying intermittently descrambled/unscrambled and hence unintelligible one. The point at which this threshold effect will occur will be dictated by the demands of the control signals in combination with the noise and bandpass characteristics of the channel but, unless these demands are less stringent than, for example, normal raster synchronization in a television picture tube, or synchronization of the syncronous colour demodulator, the decoding will fail while the 'picture' being received at the moment of failure is relatively good. This is in contrast to the unscrambled-channel situation where simple, robust, raster sync will hold a noisy picture until it is completely unviewable, the colour having already been lost.

At the time of writing (December, 1982) Direct Broadcast Systems Inc. of Surrey B.C. claim to have a system concept ready for demonstration in early 1983. The security of the DBS Inc. System, it is claimed is essentially unbreakable. Other features of the system are:

(i) several million individual subscribers addressed at a rate of 720,000 per minute,

(ii) occupies a standard TV baseband channel,

(iii) horizontal and vertical sync is not altered,

(iv) the active video is not altered,

(v) the decryptor is low-cost with 12 IC's on one board,

(vi) the decryptor could readily be built into a TVRO or a standard TV set and switched in and out - like Dolby noise suppression,

(vii) add-on addressing at slave uplinks or cable headends is simple.

The system, it is claimed is an optimal response to a requirement for a universally acceptable, simple, reliable, undefeatable scrambling technology. No specific details of the scrambling and addressing methodology are available at present but disclosure is planned for early 1983 after suitable patent protection is obtained.

5. SYNCHRONIZATIONS REQUIREMENTS FOR SPECIFIC SCRAMBLING TECHNIQUES

The results of the analysis of synchronization, networks, and candidate systems are summarized in Table 4. In this table, each of the candidates identified in Chapter 4 is examined qualitatively for its performance in a DBS environment. The necessity to be qualitative in this assessment has been pointed out in earlier chapters but it is apparent even from a qualitative assessment that certain classes of scrambling cannot fail softly - i.e. the picture would not disappear gradually into noise. The onset of synch-damaging interference will cause tearing and blanking-out similar to the picture breakup observed from a defective video tape recorder playback. Complete loss of signal may occur for several frames while digital data synchronization is being re-established.

In addition to the summation by candidate, general conclusions have been drawn from the study. There conclusions are set out in the next chapter.

TABLE 4: [illegible] SYNCHRONIZATION REQUIREMENTS OF TWELVE CANDIDATE SCRAMBLING SYSTEMS

	CANDIDATE \ SYNC FEATURE	1. SEPARATE [illegible] TIER CONTROL REQUIRED	2. SPECIAL DESCRAMBLE SIGNAL REQUIRED	3. DESCRAMBLE CONTROL RATE	4. PREDICTED DBS SYNCHRONIZING DESCRAMBLER PERFORMANCE	5. RESULT OF POOR SYNC	6. REMARKS
1	NON-STANDARD FREQUENCY (FIXED)	YES	NO	NONE	N/A	N/A	EXTRA TUNING RANGE REQUIRED.
2	INTERFERING CARRIER (FIXED)	YES	NO	RF PHASE-LOCKED LOOP OR BASEBAND PLL	N/A	N/A	SHARP RF FILTER REQUIRED.
3	CONTINUOUS VIDEO INVERSION	YES	NO	PLL TO OBTAIN 2X CARRIER + 180° + COHERENT DETECTION	.MEDIUM .PLL MUST FOLLOW CARRIER FILTER DUE TO NOISE	POOR PICTURE QUALITY	
4	SINE WAVE SYNC SUPPRESSION AT RF	YES	YES	.CONTINUOUS .PLL AT HF FOLLOWING AUDIO DEMOD	.RELIABLE	POOR PICTURE QUALITY	RESTORATION OF UN-SCRAMBLED RF ENVELOPE MUST BE EXACT. RESIDUAL H-RATE AM -50 DB OR LESS. BP-23 ALLOWS -48 DB H-RATE X-MOD ON RF CARRIER.
5	GATED SYNC SUPPRESSION AT RF	YES	YES	.CONTINUOUS .SAME AS #4 PLUS SQUARING CIRCUITS	RELIABLE	IMPAIRED PICTURE	
6	CONTINUOUS CARRIER SUPPRESSION	YES	YES	.CONTINUOUS .CARRIER MUST BE DERIVED IN PLL OR FROM AN OFFSET PILOT	.MEDIUM .PLL MUST FOLLOW CARRIER JITTER TO RE-CREATE ENVELOPE	IMPAIRED PICTURE	
7	RANDOM, DYNAMIC LINE INVERSION	YES	YES	H-RATE BEFORE BEFORE START OF LINE	.MEDIUM .MISSED CODE CAUSES COMPLETE LOSS OF LINES	LOSS OF PICTURE	
8	DYNAMIC LINE SWAPPING	YES	YES	.CONTINUOUS .H-RATE	SAME AS # 7	LOSS OF PICTURE	REQUIRES MEMORY FOR MAX INTERCHANGED, DELAYED LINES.
9	LINE DICING	YES	YES	H-RATE	.VARIABLE .HIGH SAMPLING RATES DEMAND EXACTING CHANNEL CHARAC'S	LOSS OF PICTURE	REQUIRES LINE STORE.
10	AUDIO ONLY ENCRYPTION	COULD BE MULTIPLEXED INTO AUDIO BITSTREAM	YES	KEYSTREAM CONTINUOUS OR INITIAL CONDITIONS OF KEYSTREAM GENERATOR		LOSS OF SOUND	
11	VIDEO AND AUDIO ANALOGUE ENCRYPTION	YES	YES	H-RATE	HIGH SPEED SAMPLING AS IN #9	LOSS OF PICTURE AND SOUND	
12	COMPLETE DIGITAL BITSTREAM	AS IN # 10	YES			LOSS OF PICTURE AND SOUND	

6. CONCLUSIONS

The foregoing analysis of scrambling systems in a DBS environment reveals a number of potential problems that will emerge immediately or later, as the subscriber base increases. These problems are summarized in the following twelve conclusions.

1. Authorization/de-authorization, tier control, descrambling mode control must be conveyed 'in-band'.

2. Digital techniques are the most efficient practical method for implementing authorization and tier control and controlling descramblers. Time-division multiplexing with other elements of the video signal is the most compact.

3. Any scrambled TV system is dependent on the delivery of a quality replica of the scrambler output to the descrambler input for reliable re-construction of the original signal. The channel requires low noise and low distortion over the entire bandwidth.

4. The more the signal is scrambled, the better the channel has to be to allow accurate restoration of the original signal. Scrambled signals containing high speed digital data bursts will fail more abruptly than will a conventional analogue signal because modest degradation in the descrambling digital control bursts will have catastrophic effects on the picture.

5. Scrambling systems dependent on broadband pulse transmission will be particularly susceptible to TV channel distortions - similar to the broadcast teletext channel. Lessons learned from Telidon trails should be heeded in any scrambling system employing high-speed data in the TV signal. The IF and baseband channel characteristics of low cost earth terminals (LCETs), if poorly designed can be a dominant source of synchronizing problems because of intersymbol interference.

6. The end-to-end systems implications of using sophisticated scrambling technology for broadcasting to a wide range of high-and low-cost TVROs is not well understood. In particular the basic requirements for reliably synchronizing digital data bursts has not been considered in current combinations of TVROs and descramblers. Furthermore, scrambling systems are so varied, basic analysis of specific systems is so lacking, and realistic total channel models are so poor that the performance of scrambling systems can only be judged by measurements, tests and field trials (or by accurate simulation).

To be measured are such parameters as:

a) cold start "lock-up" times
b) warm start response times
   - channel switching
   - power drop-outs/surges
   - loss of signal
c) SNR effects - low signal, interference
d) distortion effects - bandlimiting, distorting discriminators.

7. In the OAK Orion satellite system continuous broadcast cycles of subscriber address/authorization to keep descramblers "alive" typically allow 7200 subscribers to be addressed per minute. The time to reauthorize N subscribers is:

N	T(minutes)
7200	1
14400	2
21600	3
36000	5
72000	10
108000	15
216000	30
432000	60
864000	120 (2 hours)

Global addressing of all DBS subscribers numbering in the hundred of thousands or even millions must be accomplished and repeated within a few minutes at most and, more desirably, within a few seconds. This addressing problem is unique since it must be done sequentially on an individual-subscriber basis. The time required to repeat the sequence is directly proportional to the number of subscribers. Megabit data rates may be necessary because of limited time-multiplex space in the signal stream.

Alternatively the address and tiering information must be kept in "hard copy" form in the descrambler, but this involves an entirely different time scale of operational control, and could require a visit to the subscriber premises to de-authorize a subscriber.

Program tier authorization requires sequential messages also but it need not be repeated often, as is the case with on/off authorization. In practice tier control can be sequenced several times per day. Should a rapid "churn" of tiering commands be required, the necessity to re-tier many subscribers instantaneously can be avoided by pre-loading new tiers into decoders and tagging program material accordingly. A well structured computer program could sort out the optimum arrangement for such an event.

8. Some scrambling systems being produced currently have a short authorization memory mode in the decoder. Accidental de-authorization of such a decoder may mean delays of several minutes or more before a re-authorizing code is received. Operationaly, this would seriously reduce the perceived value of DBS service.

9. Scrambling techniques that remove or suppress horizontal and vertical sync pulses will dictate the use of either descrambling devices or very sophisticated signal processing techniques to manipulate the scrambled signals in, for example, time base correctors or frame stores. This would be a significant operational burden in efficient production of continuous programming, for example, local program or VBI insertion. Furthermore, each descramble-rescramble sequence degrades the signal.

10. A video signal without normal NTSC synchronization cannot be recorded for future playback through a subscriber's descrambler, even though it is an authorized program. With the increasing spread of home VCRs, program limitation could have serious consequences on the sale of simultaneous channels to a subscriber. A subscriber who has the basic VCR but who cannot record and view at the same time will be inclined to select and pay for one channel at a time, like the subscriber who only has a basic TV receiver and no VCR. The loss of potential sales to the sophisticated user could be significant.

11. The introduction of High Definition TV or enhanced TV (which is a high-quality coherently demodulated NTSC signal) will stretch the scrambler's fidelity - especially for complex methods.

12. The predicted levels of interference in TVROs from other satellites, either co- or adjacent-channel, will be so low as to have no effect on capturing digital bit-streams.

The final task of the study is to transform the conclusions into recommendations. This is done in the next and final chapter.

7. RECOMMENDATIONS

The twelve conclusions of Chapter 6 have been transformed into nine recommendations. If implemented, these recommendations would ease the technical and operational difficulties likely to occur with the introduction of a Direct-Broadcast-Satellite Service.

Recommendation #1

From conclusion #1, it is recommended that priority consideration be given to scrambling systems whose control systems are time or frequency multiplexed in-band with the associated video and sound signals. While the utilization of a separate channel for control of scrambling is not ruled out technically, such a configuration imposes the penalty of a separate receiver on subscribers, with the attendant risks due to malfunction and unreliability in addition to extra cost.

Recommendation #2

Digital technology should be given preference in developing the program and tier control and scrambling control systems for scrambled DBS programming.

Recommendation #3

From conclusions #3, 4, 5, 6, and 8, it is recommended that comprehensive field trials of an actual scrambling system or a number of systems be carried out. Such trials would include, but not be restricted to, measurements on the back-to-back performance of the system at least to the IF portion of the uplink and the receiver and must include the appropriate modulation techniques and the actual demodulator to be used in a TVRO.

Measurements would be conducted with certain parameters varied. Typical of these would be carrier-to-noise variations typical of fading, coherent interference, and simulation of aging, drift and temperature cycling in low cost TVROs.

Observations and measurements would be made on the loss of synchronization leading to a no-decode default mode, time to synchronize and re-synchronize after an inadvertant loss of signal and synchronization, time to synchronize following channel switching and time to acquire or re-acquire address information, tier information and descrambling information, each of them treated separately.

Recommendation #4

When some of measurement data referred to in Recommedation #3 have been gathered, a study should be undertaken to build up a computer simulation of the transmission channel including the hardware at both ends, and the traffic that is to be passed through it. This channel would be characterized from the measurements made. The next task in the study would be an investigation of optimal data bursts when multiplexed with analogue video. This study would examine the trade-offs that must be made in a realistic DBS system if scrambling technology acceptable to unsophisticated subscribers is to be used. In the work described under Task 2 which was the investigation of optimal data burst, it is assumed that this investigation would be based on use of further computer simulation to study a transmission of a number of candidate multiplex configurations through the channel which had been previously characterized and simulated.

Recommendation #5

Given the problem of efficiently and effectively addressing subscribers numbering in the 100,000's, it is recommended that the final choice of a scrambling system favour a system with minimum complexity at the receiving end. A complex microcircuit chip is acceptable provided that it is reliable and that it is embedded in an otherwise simple circuit. It is assumed that all the information required to descramble the signal will be transmitted, even the key.

Recommendation #6

Any decryption keys used in a descrambler must be protected appropriately, probably by coding. However, the use of public key crypto systems is not suggested because of their possible vulnerability to decryption.

Recommendation #7

If it is assumed that a universal DBS scrambling for a national scrambling system will eventually be used in Canada, it is recommeded that consideration be given to studying the vulnerability of scrambling systems to "attack". The purpose here is not to decide which system or systems can be defeated; in time, all of them can likely be defeated. What is more relevant is to to gauge the complexity and sophistication of the analysis facility needed to successfully defeat the address, tier and scrambling subsystems. Any system requiring sophisticated technology plus ingenuity and dedication to break it should be deemed robust enough to be commercially viable.

Recommendation #8

In the light of conclusions 9 and 10, which deal with the added difficulty of handling signals without normal horizontal synchronization, it is recommended that horizontal and vertical synchronization pulses not be removed or altered. In other words, the basic information needed to generate a raster display on a subscriber television receiver should always be present.

Recommendation #9

It is recommended that the federal government consider establishing standards for scrambling, that is for addressing and tiering and for the scrambling itself. Certain basic standards, were they to be established, would control characteristics of TVROs as far as band-pass characteristics and signal-to-noise ratios were concerned. The Department of Communications might consider whether or not meeting a standard would be a prerequisite to DOC acceptance of a particular scrambling technique for DBS. Such a procedure would be consistent with current DOC practice in connection with the technical evaluation and approval of cable systems. Establishing standards to be met by licencees operating scrambled systems in a direct broadcast system might be a preferred alternative to establishing a standard uniform scrambling system which would eventually be imposed on all users. Although the latter cannot be ruled out in the long term, the pursuit of it would entail protract negotiations among parties having a vital interest in its outcome.

REFERENCES

1. Philip A. Lapp Ltd., "The Final Report of a Study of the Technical and Economic Consequences of Scrambled TV Services Offered by Direct Broadcast Satellites," DOC Contract Report, February, 1982.

2. K.E. Hancock, D.C. Coll, "An Analysis of the Delivery of Scrambled TV Signals via Direct Broadcast Satellite," Annual CCTA Convention, May 31 - June 3, 1982.

3. Telesat Canada, "Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services," DOC Contract Report, September, 1981.

4. Philip F. Panter, "Modulation, Noise, and Spectral Analysis," McGraw-Hill, 1965.

5. F.E. Terman, "Radio Engineers Handbook," McGraw-Hill, 2943.

6. Chun Loo, "Subjective Evaluation of FM/FM Protection Ratio For Television Broadcasting by Satellite," CRC Report No. 1340, December, 1980.

7. D.P. Taylor and S.S. Haykim, "The CRL 60 Mb/s FFSK Modem: Its Development and Its Performance on the Hermes System," Royal Society of Canada Twentieth Symposium 29-30 November, 1 December, 1979.

8. C. Loo and A. Vincent, "Measurements of ANIK-B Broadcast Telidon Signals Received by a Low-Cost TVRO Earth Terminal," 1982. IEEE Canadian Communications and Energy Conference.

9. L.M. Adleman and R.L. Rivest, "The Use of Public Key Cryptography in Communication System Design," IEEE Communications Society Magazine, 16(6), 20-23, November, 1978.

10. B. Arazi, "Self-Synchronizing Digital Scramblers", IEEE Transactions on Communications COM-25 (12), 1505-1507, December, 1977.

11. H.J. Beker, "Cryptographic Requirements for Digital Secure Speech Systems", Electronic Engineering (GB) 52(634) 37-46, February, 1980.

12. C.M. Campbell, "Design and Specification of Cryptographic Capabilities," IEEE Communications Society Magazine, 16(6), 15-19, November, 1978.

13. D.C. Coll, "An Evaluation of the Transmission of Multi-Level Digital Symbols on Television Channels with Particular Application to Broadcast Telidon," A Report to CRC/DOC, DSS Contract No. OST81-00201, March 31, 1982.

14. C.O. Eissler, "Addressable Control," Official Technical Record, CCTA 24th Annual Convention, May, 1981.

15. D.D. Falconer and R.D. Gitlin, "Optimum Reception of Digital Data Signals in the Presence of Timing-Phase Hits," BSTJ, Vol. 57, No. 9, 3181-3208, November, 1978.

16. J.M.K. Friend and E.W. Beddoes, "Advances in Communications Security for Speech and Data," Conference on Comm. Equipment and Systems pp.411-414, 4-7 April, 1979. Birmingham, U.K.

17. M.E. Hellman, "An Overview of Public Key Cryptography," IEEE Communications Society Magazine, 16(6), 24-31, November, 1978.

18. H.J. Hindin, "LSI-Based Data Encryption Descourages the Data Thief," Electronics S2(13), 107-120, July 21, 1979.

19. N.R.F. MacKinnon, "The Development of Speech Encipherment," The Radio and Electronic Engineer, 50(4), 147-155, April, 1980.

20. R. Morris, "The Data Encryption Standard-Retrospective and Prospects," IEEE Communications Society Magazine 16(6), 11-14, November, 1978.

21. M.J. Orceyre and R.M. Heller, "An Approach to Secure Voice Communication Bases on the Data Encryption Standard," IEEE Communications Society Magazine, 16(6), 41-50, November, 1978.

22. M.T. Sun and K.R. Rao, "An ADPCM Receiver for NTSC Composite Video Signals," IEEE Trans on Broadcasting, vol. BC-28, No. 3, pp. 85-93, September, 1982.

23. D.P. Taylor and S.S. Haykin, "The CRL 60 Mb/s FFSK Modem: Its Development and Its Performance on the Hermes System. Hermes (The Communications Technology Satellite) Its Performance and Applications Volume 2," I. Paghis (Ed), pp. 179-205, 1977, The Royal Society of Canada.

24. T.B. Wu and K.R. Rao, "Digital TV Receiver for NTSC Color TV Signals with Dual Word-Length DPCM Coding," IEEE Transactions on Broadcasting, vol. BC-28, No. 1, pp. 20-24, March, 1982.

25. M. Kavehrad, "Phase Noise Effects on QPSK Carriers in Burst Transmission," IEEE Proc., Vol. 129, pt.F, no. 5, pp. 366-372, October, 1982.

26. R.E. Ziemen and W.H. Tranter, "Principles of Communications: Systems, Modulation, and Noise," Houghton Mifflin Company, 1976.

27. D.C. Coll and N. Zervos, "The Use of Spread Spectrum Modulation for the Co-Channel Transmission of Data and Television," NTC 79. IEEE No. 79 CH1514-9, Vol. 1. November, 1979.

Restrictions on "Analog" Encryption

"Analog encryption" refers to schemes for the scrambling of analog signals in such a way that the scrambled signal is in an analog form with the same bandwidth as the unscrambled signal; is unintelligible to an eavesdropper or unauthorized receiver; and such that the inverse descrambling operation may not be derived easily from the scrambled signal. These are properties that are also associated with more commonplace digital character or bit stream encryption, but the efficacy of analog encryption is severly limited by inescapable relationships between intelligibility and fidelity introduced by the filtering/reconstruction of the scrambled signal so that it has the same bandwidth as the clear signal.

The effect may be understood by considering time element scrambling (TES). With reference to Figure A1, the analog signal to be scrambled is sampled at, or above, its Nyquist rate, and the samples quantized in an analog-to-digital converter. The digital samples are stored (sequentially) in a buffer. While current samples are being stored in the buffer, samples previously stored are read out in random order, and converted to analog values in the digital-to-analog converter. The filtered output of the D/A converter is constructed by the superposition of interpolation functions, each of which has the amplitude of its corresponding digital value. Unless each interpolation function has zeros located at the times at which other samples occur, there will be intersymbol interference between samples of the scrambled waveform. If this is the case, the original amplitude values cannot be recovered at the receiver and the reconstructed (unscrambled) waveform will be distorted; that is, it will be corrupted by time-scrambled intersymbol interference. To avoid this distortion, either very wideband analog transmission must be used to preserve the output of a zero-order hold D/A; a 'Nyquist' reconstruction filter, whose impulse response has periodically spaced zeros, must be used; or the time elements must be many samples long (i.e., the analog waveform be highly over sampled); or segments of the waveforms may be shuffled.

TES has the effect of converting a waveform with a given spectrum into "white" noise with the same bandwidth; because, theoretically a sample of any amplitude can follow any other without correlation between successive samples. This has the effect of widening the bandwidth requirements of any channel, since it must be flat over the entire signal bandwidth to avoid distortion because all parts of the spectrum of the scrambled signal are equally important.

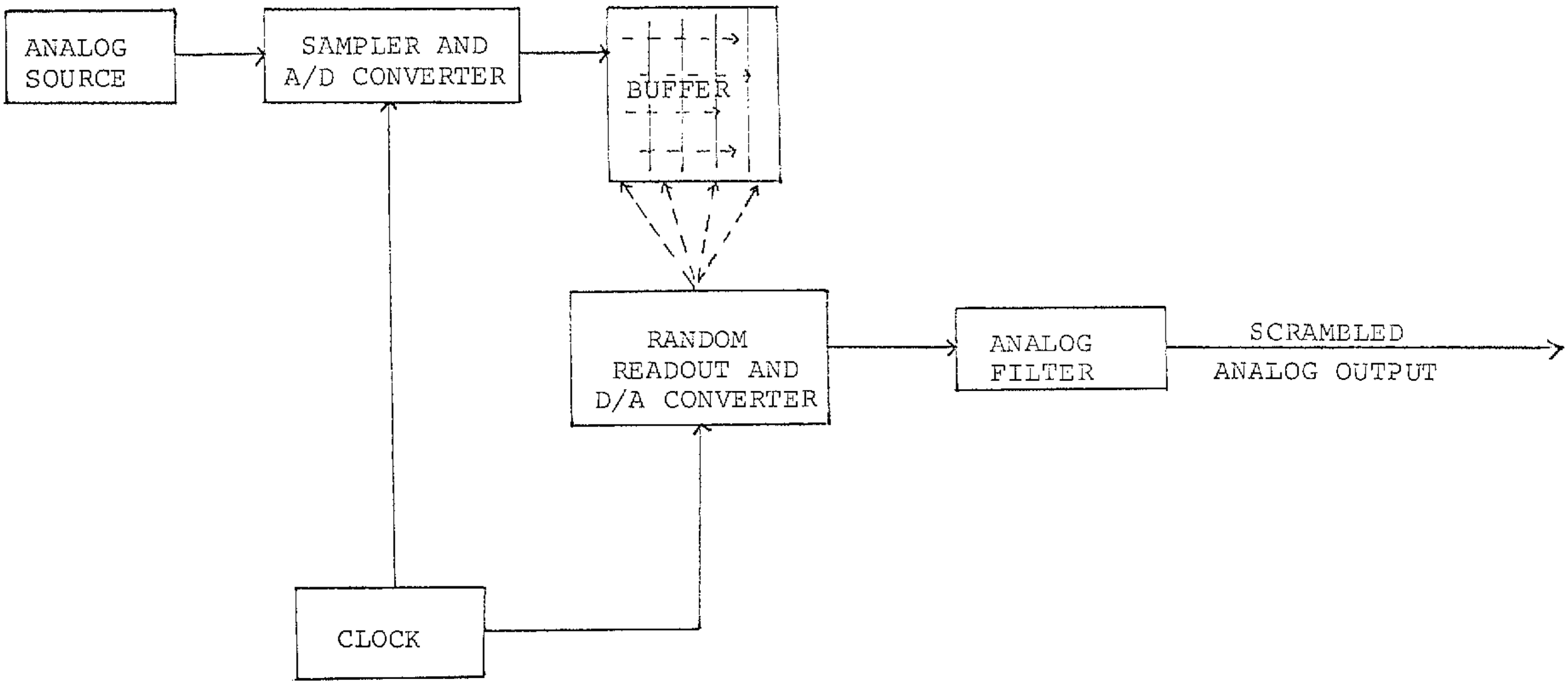


FIGURE A-1: TIME ELEMENT SCRAMBLING IN 'ANALOG' ENCRYPTION

Threshold Effects in Scrambled TV

The television signal system we use in North America was designed in the 30's and 40's; with the NTSC colour standard adopted in 1953. The signal was designed to be received with the electronic circuits of the time; and consequently a large portion of the time and energy in the baseband video signal was allocated to synchronization. Television receivers, especially modern ones, with very sophisticated gated AGC amplifiers, sync separators, and coherent phase-sensitive detectors (phase-locked loops) can extract synchronization reliably at low signal-to-noise ratios. It is a common experience to be able to synchronize the raster when the picture is totally non-recognizable 'snow'. It is clear that raster synchronization is the most robust portion of the conventional video signal.

Sync-denial scrambling techniques rely on the fact that much of the sync energy in the video signal can be removed. Television receivers designed to expect normal levels will not synchronize, but phase-locked loop synchronizers can; and many modern receivers will lock on suppressed-sync signals without being modified.

The picture quality in standard video normally degrades gracefully as the signal level drops, or as interference, echoes and noise increase. Synchronization is relatively immune to both linear and non-linear distortion of the video signal; effects which are very hard on picture quality and colour fidelity. In fact, modern TV receivers have such an array of circuits that automatically compensate for distortions, that good quality pictures can be displayed even though the received signal is of low quality. Many broadcasts include test and reference signals in the VBI for the automatic circuits to "work on". Significant advances are being to de-ghost signals with multipath interference, using automatic equalizer techniques, as a result of the requirement for echo-free channels for reliable data transmission (teletext) in TV broadcasts.

It is a well-known fact (observable by dropping into any neighbour's home) that most consumers watch badly mis-adjusted television receivers, particulary in terms of colour saturation and hue (as well as contrast and brightness) - in spite of the automatic tuning circuits in modern sets. It is also true that consumers will watch badly impaired channels if nothing else is available or if the subject matter is of sufficient interest.

It is, therefore, a fact of life in normal television veiwing that the viewer is seldom presented with a picture that will not synchronize (if it is intelligible); and is, in fact, often able to view severely distorted, impaired and noisy pictures because his receiver will synchronize.

The situation with scrambled television is radically different. Most scrambling systems of any complexity will not degrade gracefully - they will either work reasonably, or not at all. This threshold effect will come about because in most scrambling systems the fraction of transmitted energy devoted to synchronization has been substantially reduced (either by gated sync suppression or by transferrance of the synchronization mechanism to data streams imbedded in, or added to, the video) and successful descrambling requires successful extraction of basic raster synchronization.

Sync extraction from standard horizontal sync pulses is very different from the establishment of sync from detection of a specific bit pattern in embedded data.

The Assessment of Sync Performance

It is difficult to make analytical statements about the performance of scrambled television satellite systems in general, and statements made about particular systems most likely have no generality. If a particular system were postulated and analyzed merely to provide some concrete results, the generality of those results would be doubtful; and their validity, in view of the lack of good channel and noise models, highly questionable.

Thus, to understand how a scrambling system will behave, it is necessary to test it under real conditions. Even so, some observations on the subject can be made.

An analytical assessment of the performance of the synchronization components of scrambled television channels, and subsequent effects on the overall performance of the subscriber link is highly dependent on the particular system being used, especially on the characteristics of the modulator, demodulator and channel.

Two factors contribute to the difficulty of making general statements about sync performance. The first factor is that little is known about the details of any particular system, due to the very nature of scrambling systems and the secrecy surrounding them. The second factor is that there are few basic analytical results that relate to regular television sync performance in the presence of noise, interference, or distortion.

Optimal signal processing receivers that are used in modems and other modern data receivers, and which have been analysed extensively, are not used in TV receivers because the television channel is usually so good. For example, the horizontal sync detection circuit may be a narrowband phased locked loop or a wideband, edge-sensitive, trigger circuit; in most video signal circuits it is the latter. In a phase locked loop, variance of the phase jitter of a carrier in noise is inversely proportional to the signal-to-noise ratio in the loop bandwidth; but it is difficult to obtain results about the jitter on the horizontal sync pulse derived by a non-linear sync separator circuit. To extrapolate the results to the jitter on a gated suppressed-sync scrambler is difficult and the generality or usefulness of the results (even if obtainable analytically) is questionable.

Reference can be made to two classes of communication systems to give some indication of the problems that could befall synchronization components in a scrambled TV delivery system.

The first class includes conventional television and practical data communications systems. In both, a considerable fraction of the transmitted bandwidth and /or energy is devoted to synchronization. Most data communication systems use special line codes and data shuffling techniques to insure that energy at the bit rate is available at the receiver. Others, such as FFSK, allow bit timing to be derived from the received waveform. The energy, and transmission time, devoted to sync in standard television signals has already been emphasized.

One should note that a system designed to operate in an ideal environment is usually very susceptible to unexpected noise and distortion, both in classical systems as described by Taylor and Haykin; and those of the second class, discussed later.

The properties of the channel over which scrambled television signals are to be delivered that are going to affect the synchroniztion are not likely to be revealed by standard television measurements. They are liable to be transient effects: data dependent intersymbol interference, echoes, picture level fluctuations, demodulator response, impulse noise, cycle slips in timing extractors, and so on.

Falconer and Gitlin have demonstrated in their paper (Ref.15) the difficulty of analysing the performance of a data communications system under specified distortions that can cause synchronization problems. Their work also indicates the complexity of the receivers required for the reliable extraction of bit sync; some abrupt shifts in their time bases of one-half a bit period required 15,000 bits to recover from.

Two facts emerge from a consideration of this class of systems:

a) synchronization requires significant energy or bandwidth; and
b) the extraction of synchronization information can require complex processing unless the channel is virtually error and distrotion free.

The second class of system to be considered is teletext, or broadcast Telidon. This system provides an interesting example of the performance results that might be expected when data is transmitted as part of the video signal at high rates through television systems. Consideration of the results obtained in the recent trials of this class of system indicates clearly that:

a) performance of the system as judged by one set of criteria, namely the acceptability of received television images and the standard measurements devised to relate to this requirement, does not necessarily ensure adequate performance of different signals using the same system;

b) errors are being caused by transient effects, channel characteristics, and other sources of disturbance that are not clearly understood; and

c) the design of the teletext modems has not been well matched to the channel.

The implications for delivery of scrambled TV signals in which most of the normal sync information could be replaced by inserted data packets, and which will carry control information in inserted data packets, is fairly obvious. It will not perform well, or as expected, unless and until the complete delivery system is well understood.

For reliable DBS system design, original work is still required:

a) to undertake analytical or simulation studies of the performance of complete scrambling schemes (or even data schemes) under specified noise, interference, and distortion conditions for specified receivers; and

b) to test various scramblers under conditions of controlled impairment.

Given that scrambling and its associated in-band data signalling will operate satisfactorally under normal TV situations (40 db or more of signal-to-noise-ratio), this work would determine the effects of

a) the use of receivers that one might normally expect to find in operation in remote subscriber location (TVRO, descramblers and television sets);

b) fringe area reception; and

c) subscriber reaction to operational control; view on demand; billing; synchronization delays; and degradation of the scrambled system.

In other words, some basic work is required to determine the overall performance of scrambling systems under realistic conditions.

Government of Canada
Department of Communications

Gouvernement du Canada
Ministère des Communications

TRC 59
ISSUE I

TELECOMMUNICATIONS REGULATION CIRCULAR

TECHNICAL REQUIREMENTS FOR THE CERTIFICATION OF SCRAMBLED TV SYSTEMS

RELEASE DATE: MAY 1, 1981

TELECOMMUNICATION REGULATORY SERVICE

CRT 59
1ère ÉDITION

CIRCULAIRE DE LA RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS

EXIGENCES TECHNIQUES POUR LA CERTIFICATION DES SYSTÈMES DE RADIODIFFUSION TÉLÉVISUELLE À TRANSMISSION CODÉE

DATE DE PUBLICATION: 1er MAI 1981

SERVICE DE LA RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS

Telecommunications Regulation Circular No. 59

Technical Requirements for the Certification of Scrambled TV Systems

Introduction

Under Section 5(d) of the Radio Act, the Department intends to introduce minimum technical requirements for scrambled TV systems for use by broadcasting transmitting undertakings for which a Technical Construction and Operating Certificate (TC & OC) is required. This TRC is intended to inform manufacturers and broadcasters, as well as the general public, of the technical requirements and procedures required for the certification of scrambled TV systems. The purpose is to ensure that the transmission and reception of the scrambled TV signal is compatible with the M/NTSC system specifications and to prevent interference to the radio environment. Additional technical requirements for the descrambler devices are contained in TRC No. 60: "Technical Requirements for Radio Apparatus Capable of Receiving Television Broadcasting".

Technical Requirements

Systems capable of transmitting scrambled television signals shall conform to the following technical requirements:

Coding Methods - The method of encoding and decoding is not standardized. However, the encoding and decoding process shall not perceptibly degrade the quality of the signal provided at the output of the decoding device and must be compatible with the M/NTSC system specifications as defined in the Department's Broadcast Specification No. 12, Issue 2 on "Basic Television Transmission Standards".

Radiated Spectral Energy - The use of the scrambler shall not increase the spectral energy of the transmitted signal beyond the limits established in the Department's Radio Standards Specificatons 151, 154 and 157.

TV Channel Frequencies - The use of the TV transmission, when operating in either the scrambled or non scrambled mode, shall not alter the frequency of either the visual or aural carriers as defined in the the M/NTSC system specifications.

Technical Acceptance Procedure

Applicants proposing the use of scrambled transmissions for TV broadcasting stations for use in Canada shall, in conjunction with manufacturers or suppliers of such systems, satisfy the Department at their own expense that the apparatus actually meets the requirements contained in this TRC, as a condition of the issue of a TC & OC. The Department reserves the right to request additional information, or a production model of the apparatus, to perform measurements in its own laboratory. All information furnished in support of a submission will be retained by the Department and will be treated as company confidential.

Notwithstanding the fact that a particular apparatus meets these requirements, the Department reserves the right to require that adjustments be made to that apparatus whenever it causes interference within the meaning of the Radio Act.

Applications for the use of scrambled TV broadcasting systems may be sent to the Director, Broadcasting Regulation Branch, Telecommunication Regulatory Service, Department of Communications, 300 Slater Street, Ottawa, Ontario K1A 0C8.

Comments on these technical requirements would be welcomed by the Department.

Dr. John deMercado
Director General
Telecommunication Regulatory
Service

Government of Canada
Department of Communications

Gouvernement du Canada
Ministère des Communications

TRC 60
ISSUE I

TELECOMMUNICATIONS REGULATION CIRCULAR

TECHNICAL REQUIREMENTS FOR RADIO APPARATUS CAPABLE OF RECEIVING BROADCASTING (DECODERS, CLOSED-CAPTIONING DEVICES, ETC.)

RELEASE DATE: MAY 1, 1981

TELECOMMUNICATION REGULATORY SERVICE

CRT 60
1re ÉDITION

CIRCULAIRE DE LA RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS

EXIGENCES TECHNIQUES RELATIVES AUX APPAREILS DE RADIOCOMMUNICATIONS POUVANT CAPTER DES ÉMISSIONS DE RADIODIFFUSION (DÉCODEURS, APPAREILS DE SOUS-TITRAGE CACHÉ ETC.)

DATE DE PUBLICATION: 1er MAI 1981

SERVICE DE LA RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS

TELECOMMUNICATIONS REGULATION CIRCULAR

TECHNICAL REQUIREMENTS FOR RADIO APPARATUS CAPABLE OF RECEIVING BROADCASTING

Introduction

Under Sections 6(1)(b)(ii) and 7(1)(h) of the Radio Act, the Department of Communications intends to introduce regulations concerning the sale of a certain class of radio apparatus capable of receiving television broadcasting. This class of radio apparatus which is currently not regulated under the General Radio Regulations includes descramblers (decoders), closed captioning adapters and other similar apparatus which are capable of receiving television broadcasting and which feed, by conduction, a modulated radio frequency carrier to the antenna terminals of a television receiver. This Telecommunications Regulation Circular (TRC) is intended to inform manufacturers, distributors, retailers, as well as the general public of the technical requirements and technical acceptance procedure which the Department intends to introduce for this class of radio apparatus.

Radio apparatus of the class described in this TRC shall conform to the following technical requirements:

Gain Characteristics

(A) For apparatus having automatic gain control circuitry, the output signal level shall be not less than 1 millivolt (0 dBmV) and not more than 5 millivolts (14 dBmV) when measured across an impedance of 75 ohms, or

(B) For apparatus not having automatic gain control circuitry, the conversion gain shall be not less than 0 dB nor more than 7 dB.

Carrier Frequency Stability

The frequency stability obtained with any line voltage in the range from 104 to 127 volts and measured, after twelve hours of warm-up operation, over a period of three hours shall be such that the visual carrier frequency of signals of an output channel shall,

(A) if the apparatus is equipped with a fine tuning control, be maintained within 450 kHz of the nominal carrier frequency for the output channel, or

(B) if the apparatus is not equipped with a fine tuning control, be maintained within 250 kHz of the nominal carrier frequency for the output channel.

Radiated Field Strength

The field strength of any emission emanating from the apparatus, when measured at a distance of 3 metres shall not exceed:

(A) 70 μV/m in the frequency range above 5 MHz and below 30 MHz,

(B) 100 μV/m in the frequency range from 30 MHz and below 88 MHz,

(C) 150 μV/m in the frequency range from 88 MHz and below 216 MHz,

(D) 200 μV/m in the frequency range from 216 MHz and below 1000 MHz.

Spurious Signals at the VHF Input Terminals

The level of any local oscillator signal and any signal of an undesired or spurious nature generated within the apparatus and arriving at the VHF input terminals, measured across 75 ohms,

(A) in the frequency range above 5 MHz and below 30 MHz, shall not exceed -50 dBmV,

(B) in the frequency range from 30 MHz to below 54 MHz, shall not exceed -35 dBmV,

(C) in the frequency range from 54 MHz to 300 MHz, shall not exceed -26 dBmV, and

(D) in the frequency range above 300 MHz and below 1000 MHz, shall not exceed -10 dBmV.

Technical Acceptance Procedure

Those seeking to establish the technical acceptability of radio apparatus of the class described in this TRC, shall ensure that the apparatus or a production sample or other representative unit of that type of apparatus is tested in accordance with accepted engineering practices to determine whether or not it conforms to the applicable technical requirements described herein.

For apparatus which are established to be technically acceptable for use in Canada, manufacturers or importers should ensure that each unit of a type offered for sale by him bears, in a location convenient for inspection, a permanent label or marking containing, in both official languages, the statement, "DOC TRC 60" and "MDC CRT 60".

Comments on these proposed requirements would be welcomed by the Department.

JOHN deMERCADO
Director General
Telecommunication Regulatory
Service