A PROGRESS REPORT ON THE WORK OF THE ATSC SPECIALIST GROUP ON INTEROPERABILITY AND CONSUMER PRODUCT INTERFACE

by

Bernard J. Lechner
Consultant
Princeton, New Jersey

Abstract

Since August of 1989, a group of dedicated television engineers has been meeting approximately every six weeks to help ensure that the Advanced Television standard chosen by the FCC for terrestrial broadcast will be friendly to Cable TV and other alternate media as well as the American consumer. The work of this group and the results it has achieved in the last 2 1/2 years is described. It is concluded that a single baseband ATV format should be adopted by all television delivery media. It is also concluded that a single standard for encryption of conditional-access programming is technically feasible.

INTRODUCTION

In August of 1989 the Advanced Television Systems Committee (ATSC) created a Specialist Group on Interoperability and Consumer Product Interface to study issues relating to interoperability among the various media that will be employed to deliver Advanced Television (ATV) service to U.S. consumers and to study the resulting impact on the interface between consumer products and the various media. An objective of the Specialist Group (known as T3/S2) is to develop a body of technical information relating to the requirements of the alternate media that the ATSC can provide to the FCC Advisory Committee on Advanced Television Service (ACATS) to assist in the choice of an ATV standard for terrestrial broadcast. A further objective is to encourage the alternate media to adopt voluntary standards for transmission of ATV signals that will maximize the interoperability among media and especially between the alternate media and terrestrial broadcast. A final objective is to encourage the adoption of a voluntary interface standard by television receiver manufacturers that will accommodate the needs of the alternate media. The goal is to achieve a set of harmonized standards that are friendly to the various delivery media and the consumer.

The membership of T3/S2 totals approximately 30 and includes a broad cross-section of the television industry with representation from broadcasters, receiver manufacturers, programmers, the telephone industry, Cable TV operators and equipment manufacturers, ATV system proponents, satellite operators and equipment manufacturers, etc. The Group has met over 20 times with a typical attendance of 12 to 15 members at each meeting.

In carrying out its work, T3/S2 has concentrated on issues relating to the deliv-

ery of ATV by Cable TV and DBS. A major part of our effort has been focussed on conditional-access systems for ATV. The Group has sought to identify which, if any, aspects of conditional-access systems are suitable for voluntary industry standardization. Working with our sister Group, the ATSC Specialist Group on Digital Services (T3/S3), we developed a list of attributes for scrambling (The term "scrambling" is used here and throughout this paper in the broad contest of rendering the signal unintelligble.) and conditional access to be applied to the proposed ATV systems.

To assist T3/S2 in its work, written inputs were obtained from the various ATV system proponents and other interested parties. We have also had presentations at our meetings by system proponents and others. The Group is now in the process of distilling these many inputs to organize them into a final report by mid-1992. Toward this end we recently developed a strawman list of nearly 30 possible points of agreement relating to interoperability and consumer product interface as a basis to achieve a consensus.

BACKGROUND

As the U. S. moves towards the adoption of standards for a terrestrial broadcast ATV service, it is important to recognize that ATV services will also be provided by Cable TV and the other alternate media. Since Cable TV and the other media have differing needs as well as differing technical and regulatory constraints, it is important to insure coordination and cooperation among all media in the development of standards so that program material delivered by any one medium can also be easily delivered by all other media and so that consumer receivers can be easily interfaced to all possible media. If this is not done, expensive conversion equipment might be required to exchange programming between media and, worse yet, consumer television receivers might require complex, and potentially user-unfriendly, interface boxes to receive programs from the various alternate media.

This need has been recognized by the FCC and has been addressed in part by the Advisory Committee through the Planning Subcommittee Working Party 4 (PSWP4) on Alternate Media and the Systems Subcommittee Working Party 4 (SSWP4) on System Standards. Specifically, SSWP4 recognized the importance of Cable TV in delivering terrestrial broadcast signals to consumers and has explicitly stated that any standard(s) adopted for terrestrial broadcast must be capable of being transmitted over Cable TV systems. The HDTV Subcommittee of the NCTA Engineering Committee, PSWP4 and Cable Television Laboratories (Cable Labs) developed a basic test plan to evaluate the performance of proposed ATV systems when transmitted through Cable TV systems and over fiber optic links. Cable Labs converted this basic test plan into a specific series of tests and installed the necessary Cable TV and fiber optic equipment at the Advanced Television Test Center (ATTC) where Cable Labs is now conducting tests of the proposed ATV systems.

In late 1988, PSWP4 developed a strawman proposal for an ATV Multiport receiver interface that would make it possible for ATV receivers to interface to alternate media sources. Subsequently the Electronics Industries Association (EIA) ATV Committee created an ATV Multiport Receiver Subcommittee. This Sub-

committee, which is now a part of the EIA R-4 Engineering Committee (designated as the EIA Receiver Interface Subcommittee - R4.1), developed a detailed generic model of an ATV receiver multiport interface.

It is in the context of these various related activities that T3/S2 undertook its work in August of 1989. To insure that there would be neither competition nor unnecessary duplication of effort, T3/S2 established and has maintained liaison with EIA, PSWP4, SSWP4 and the NCTA.

ACTIVITIES OF T3/S2

Early in its work, T3/S2 realized that the alternate media were free to choose ATV standards totally unrelated to those developed for terrestrial broadcast. We concluded that such a scenario was both unwise and unlikely, and in any event, unless and until some medium chose such a standard, there was little if anything we could do to deal with its interoperability with other media. Recognizing that the various media will employ different modulation methods and may format and condition the signals for transmission differently, we concluded that the requirements for interoperability and consumer product interface would be most easily met if all media were to adopt substantially the same baseband video signal format. We made this statement intentionally vague to allow for the possibility that variations among media will allow exploitation of extra capability by a given medium or fitting within a constraint by another medium without unduly compromising interoperability or complicating the consumer product interface. As an example, VHS tape has less luminance bandwidth than NTSC and S-VHS has more luminance bandwidth.

Therefore T3/S2 has focussed on examining the standards proposed for terrestrial broadcast of ATV, assuming that the terrestrial standard chosen by the FCC will form the basis for the standards employed by the alternate media. We have attempted to evaluate how well each of the proposed terrestrial standards meet the unique needs of Cable TV and the other alternate media with regard to interoperability and consumer friendliness.

Cable Television

T3/S2 decided initially to concentrate on Cable TV and to characterize the needs of Cable TV in an ATV environment. We agreed that most of the issues of concern to the Cable TV industry would be covered by the test program now being conducted by Cable Labs at the ATTC. The major issue that is not covered by the Cable TV test plan is scrambling and the need for data transmission to control conditional access to scrambled programming. Since the data transmission for controlling access falls within the charter of the ATSC Specialist Group on Digital Services (T3/-S3), starting with our January 18, 1990 meeting, T3/S2 has met jointly with T3/S3. At that meeting we agreed to develop an attributes list for scrambling and conditional access to be applied to the proposed ATV systems.

At our March 7, 1990 meeting, we reviewed the criteria for scrambling and conditional access used by the Direct Broadcast Satellite Association (DBSA) in 1986 as well as a list of attributes generated by Graham S. Stubbs, the Chairman of T3/S3. We reached a consensus on four basic desireable attributes for a scrambling and conditional-access system.

- The images displayed on receivers not authorized to receive the scrambled programming must be unrecognizable.

- It must not be possible to recover the image by inspecting the transmitted signal and performing any reasonable real-time processing on the information contained therein.

- The details of how the system operates must be general public knowledge.

- The security of the system is entirely contained in the delivery and processing of the key.

During subsequent joint meetings of T3/S2 and T3/S3, this list was modified and expanded and it was augmented by a second list of desireable features and other considerations. A first draft was mailed by T3/S3 to the ATV proponents and other interested parties in August of 1990. The comments received were incorporated into a second draft which was mailed by T3/S3 to a wide cross-section of the television industry in December of 1990. The final result is ATSC document T3/180 "ATV Encryption System Characteristics" dated 16 May 1991 (see Appendix), which has been widely distributed to the ATV proponents and others for use as a guideline in developing and evaluating ATV systems.

During 1990 T3/S2 solicited and received information from the ATV system proponents concerning how they planned to meet the original four basic desireable attributes for a scrambling and conditional-access system. This was at a point in time when most of the proposed systems were based on analog transmission. By the end of 1990, that had all changed. Four of the five full high-definition ATV simulcast systems are now based on digital transmission, and it is clear that they can all meet the six general requirements for System Security listed under Desireable Attributes in the Appendix by encrypting the transmitted digital signal bit-by-bit and providing an appropriate replaceable security module.

The attention of T3/S2 then turned to the question of which, if any, aspects of such a conditional-access system might be subject to voluntary industry standardization. To address this issue, during 1991 we invited ATV system proponents and others to present their views at our meetings. Those presentations and the ensuing discussion have led us to the following tentative conclusions, assuming an all-digital simulcast ATV system:

- For conditional-access programming, the source-coded digital video, audio and data will be scrambled by encrypting the transmitted digital data stream using a DES-like algorithm.

- The process of scrambling and descrambling the transmitted digital data stream will be implemented by performing a mathematical operation on the source-coded digital signal and a pseudo-random number generated from a seed provided by the encryption algorithm.

- With respect to the equipment in the consumer's home, the security of the system shall reside entirely in the hardware/firmware used to implement the encryption algorithm, i.e., process the delivered keys to

produce the seed for the pseudo-random number generator.

- In order to provide for recovery in the event that the security module, i.e., the hardware/firmware used to implement the encryption algorithm, is cloned by a pirate, this portion of the in-home system must be easily replaceable.

- It is highly desireable that the security module be replaceable by the consumer himself, not requiring a service call.

Given the above five tentative conclusions, all of the system security attributes listed in the Appendix can be met, and if ATV receivers have a multiport interface which passes the source-coded digital signal, a decoder box can be connected to the interface to perform the descrambling operation. Different service providers can use different encryption algorithms if desired. However, this may lead to multiple boxes connected to the multiport interface with each box having its own replaceable security module.

T3/S2 also concluded that it is possible to design and standardize a conditional-access system that meets all of the requirements for the desireable attributes listed in the Appendix. The hardware for such a standardized conditional-access system could be contained in a back-of-the-set box connected to the ATV receiver multiport interface, or alternatively, except for the replaceable security module, it could be built into the ATV receiver. If the conditional-access hardware is built into the ATV receiver, a separate interface (not the multiport interface) will be required to accommodate the replaceable security module and still another interface will be needed to provide signals to an upstream data link to order pay-per-view programs. The EIA R4.1 Receiver Interface Subcommittee is studying both of these interfaces as well as the multiport interface.

Although a standardized conditional-access system built into the ATV receiver, rather than external, is technically feasible and would provide the most cost-effective and user-friendly system for both service providers and their customers, the design of such a system will require a major cooperative effort by all segments of the television industry. However, since the various U.S. television industry segments traditionally compete with one another and each has vested short-term business interests that argue against a single conditional-access standard, T3/S2 has concluded that agreement on a single voluntary standard for conditional access is not likely, despite its technical feasibility and obvious long-range advantages of cost and convenience for both service providers and the American public.

DBS

Beginning at our March 7, 1990 meeting, T3/S2 began to study satellite (DBS) delivery of ATV programming to consumers. We understood that the Satellite Broadcasting and Communications Association (SBCA) was planning to distribute a questionnaire to present and prospective satellite programmers concerning ATV-related issues. We established a liaison with SBCA to initiate a cooperative effort and avoid duplication of work. It quickly became clear that the conditional-access issues for DBS and Cable TV were substantially the same, except possibly for

data capacity requirements to address a larger universe of subscribers from a single transmission point in the case of DBS.

The major difference between DBS and Cable TV is the different modulation method likely to be used by DBS. T3/S2 concluded that the proponents of ATV systems should be asked how they proposed to deliver ATV signals over satellites, and that it would be desireable to conduct comparative satellite delivery tests of the proposed ATV systems. PSWP4 had developed a skeleton test plan for satellite transmission and T3/S2 volunteered to convert this into a specific test plan, if the SBCA could put a test program in place. During the period from December, 1990 to July, 1991, there was an ongoing dialog between T3/S2, SBCA and ATTC. In July, 1991 SBCA created a Working Group on Satellite Testing of ATV Systems, which first met on July 17, 1991. By early December of 1991, the Working Group developed a Conceptual Test Plan for Satellite Delivery of ATV. This plan differed significantly from the earlier PSWP4 plan because of the change from analog systems to all-digital systems.

Later in December of 1991, the SBCA Working Group initiated discussions with PSWP4 and in January, 1992, the Working Group became a sub-group of PSWP4. The present plan is to conduct a theoretical evaluation of the proposed ATV systems based on information supplied by the proponents about how they propose to deliver ATV by satellite.

Consumer Product Interface

With respect to the television receiver interface issues, T3/S2 believed from the outset that the EIA Multiport Subcommittee (now R4.1) had this well in hand. During 1989 and 1990, we reviewed drafts of their reports at various stages and provided our comments. We held a joint meeting with them in April of 1990 and the Chairman of T3/S2 has been attending their meetings as an active participant since early 1991. Initially, R4.1 developed a generic model of an ATV receiver multiport interface. Recently the Committee has focussed on being more specific. Although precise details of the interface must await the choice of a terrestrial broadcast standard by the FCC, R4.1 has identified four possible interfaces: An analog interface which probably will be luminance and two color difference signals; a digital interface which will most likely be source-coded compressed digital video, audio and data; a conditional-access interface to accommodate a replaceable security module; and a control interface to pass receiver status to other devices, receive status from other devices and to allow user inputs (either directly to the TV or via remote control) to be passed to other devices, e.g., to order pay-per-view programs via a modem or other up-stream communications link.

In early February of 1992 the EIA R4.1 Committee distributed a questionnaire concerning these four possible interfaces to a wide cross-section of the television industry. The responses to the questionnaire will be analyzed this spring and, along with inputs from T3/S2, T3/S3, PSWP4 and other industry groups, will help to define appropriate interface ports that can lead to EIA recommendations for voluntary standards for television receiver manufacturers.

CONCLUSIONS

Since its inception in August of 1989, T3/S2 has been working to achieve harmonization of standards among the various media that will deliver ATV to the American consumer. We have focussed on Cable TV and DBS and it appears at this point that both Cable TV and DBS will adopt standards that embody substantially the same baseband format chosen for terrestrial broadcast. It also appears that other media (telephone companies, pre-recorded video, etc.) will do likewise. Working with our sister group T3/S3 we have, with the help of many in the television industry, developed a list of ATV Encryption System Characteristics to serve as guidelines for the industry. We have also, through SBCA and PSWP4, initiated an evaluation of the proposed ATV systems for DBS transmission. With the EIA R4.1 Committee, the definition of TV receiver interfaces that will provide user-friendliness in an alternate media environment is proceeding apace. Finally, T3/S2 has achieved agreement that a single standard for conditional-access programming is technically feasible and can, with an interface for a replaceable security module, be implemented within the TV receiver. The challenge to achieve a single conditional-access standard is not technical; it is a business challenge that will require cooperative efforts within the industry to achieve win-win rather than win-lose scenarios.

* * * * * * * * * * * * * * * *

APPENDIX
ATSC DOCUMENT T3/180
Dated 16 May 1991

ATV Encryption System Characteristics

I. DESIRABLE ATTRIBUTES

1. System Security

- General -- The system security design should provide:
  - System security entirely contained in the delivery and processing of encryption keys; it should permit recovery from any security compromise.
  - Secure operation even when threatened by a party with total system information; i.e., the system must be secure even if all details of how the system operates should become public.
  - To the extent that withstanding piracy threats over a long period of time may require the periodic exchanging of at least some key components of consumer decoders, this capability for changes should be provided in a way so as to minimize the costs of such exchanges.

- Images and audio of transmitted signals should be unrecognizable when received and displayed by receivers not authorized to receive the scrambled programming.
- Non-feasibility of decryption by inspection of the encoded signal and performance of any reasonable processing on the encoded information.
- Secure transmission of ancillary services.

- Physical -- Physical security measures should:
  - Preclude a typical homeowner with household tools from defeating any security function.
  - Preclude a commercial enterprise from making cloned units or modifying legitimate units such that security measures are defeated. The cost of cloned devices should be much greater than the value of the deferred service cost.

2. Signal Quality

- Under perfect signal conditions:
  - There should be no perceptible decoding artifacts in video.
  - There should be no perceptible decoding artifacts in audio.

3. Signal Robustness

- The effect of noise or signal degradation on reception and decoding of encrypted signals should be no greater than the effect of such signal-path imperfections on non-encrypted signals.

4. Universality

- Applicability, where possible, to alternate media intended for program delivery to the consumer.
  - Terrestrial broadcast.
  - Wired networks (cable, fiber, etc.)
  - Satellite broadcast.
  - Pre-recorded.
- It is desirable that an encrypted format be useable in all of the alternate media without completely decoding and re-encoding as the signal passes from one medium to another.

II. DESIRABLE FEATURES AND OTHER CONSIDERATIONS

1. Addressability and Tiering

- Pre-authorized tiers.
  - Number available.

    - Independent control of audio, data, and text.
  - Addressability
    - Size of the universe (per operator/system).
    - Data space required per addressable consumer terminal.
    - Universal key and fail-safe modes.
    - Interface to automatic ordering systems.

2. Subscriber and Pay-Per-View

   - Lock-out functions.
     - By rating (parental control).
     - By channel or time of day.
     - By pay-per-view.
   - Program tracking.
   - Transactions per month.
   - Impulse pay-per view: increment/decrement function.
   - Return loop provision.
   - Multiple operator pay-per-view.
   - Consumer-friendly operation.

3. Multiple Operator Use and Control

   - Feasibility of simultaneous multiple operator use.
   - When encrypted signals are delivered to cable headends, provision for local cable system intervention to manage conditional-access control and key distribution within the cable system.
   - Separate billing systems for multiple operator use.
   - System capacity: how many simultaneous billing systems.

4. Ancillary Services

   - Multiple sound channels.
   - Teletext/captioning capability.
   - Allocation flexibility for ancillary services.