interoperability testing. Without such a comprehensive licensing program, interoperability could not be achieved or sustained over time.

3. Technical Advantages of the GI DigiCipher II System

The following technical attributes of GI's DigiCipher II digital television system provide substantial performance improvements relative to competing MPEG-2 systems:

- Access Control and Security
- Trellis Coded QAM Modulation
- MPEG-2 Video Encoding
- Dolby Digital AC-3 Audio
- System Information (SI)
- Data Services
- Vertical Blanking Interval (VBI) service coding

(a) Access Control and Security

Perhaps the most important aspect of GI's DigiCipher® II system is the conditional access and security system. An alarming phenomenon in GI's extensive experience with pay TV systems is the length to which pirates will go to break a security system which is protecting a valuable array of programming and services. The greater the value of the protected content, the more massive and relentless will be the pirates' attacks. GI's DigiCipher II conditional access/security system is the most advanced system of its kind; it received an Emmy Award from the Academy of Television Arts and Sciences in 1996.

Offering maximum protection to content providers and distributors, GI's security philosophy begins with a highly secure and cost-effective initial system with an embedded, single-chip decoder implementation, providing multiple levels of technical and economic barriers to pirates. Complementing this foundation, GI's system includes a path to renewable security, by distributing TvPass™ Card renewable elements in the event of a breach. If and when TvPass Cards are issued and installed, they are "mated" to the embedded secure processor through a secure communications protocol.

The fundamental elements of GI's approach include: (i) a secure, non-reusable, single die VLSI custom decoder chip; (ii) a cryptographically secure mating verification scheme between the buried secure processor and the renewable element (if and when renewable elements are

installed); (iii) battery backed-up volatile memory for secure storage in both the fixed and renewable security elements; (iv) working key (control word) which changes several times per second; (v) use of proven and strong cryptographic algorithms (e.g., DES and DES variants); and (vi) renewable security.

In addition to its emphasis on security integrity, GI's access control system incorporates many advanced features such as:

- Multi-tier key hierarchy, with the lowest level key changing several times per second
- Extensive decoder tier bit space, providing program packagers with complete flexibility for service offerings
- Flexible support of subscription, call-ahead Pay Per View (PPV), and Impulse Pay Per View (IPPV) services
- Regional and circular blackouts, enabling sports blackouts and segmentation of programming rights by geographic region
- Program ratings and parental lockout capability
- Macrovision copy-protection to inhibit taping of designated PPV events

(b) Trellis Coded QAM Modulation

GI's digital system complies with the ITU J.83 Annex B Trellis Coded QAM Forward Error Correction (FEC) standard, the most powerful and advanced modulation/FEC standard for bandwidth-limited channels such as those in cable television systems. The same standard has been adopted by the SCTE in the U.S. GI's initial system employs 64 QAM modulation, allowing a 27 Mbps information rate and a 30 Mbps total data rate (including FEC coding bits) in a 6 MHz channel. Other 64 QAM systems only use Reed-Solomon block coding. GI will soon introduce a 256 QAM option, allowing a 38.8 Mbps information rate per 6 MHz channel.

Trellis coded modulation, concatenated with a Reed-Solomon block code, provides system operators with a 2 dB performance advantage in carrier to noise, with no increase in complexity (cost), versus a Reed-Solomon only (t=8) approach.

The ITU Trellis Coded QAM standard has major performance advantages for both wired (cable/telco) and wireless (MMDS) applications. For wired networks, relative to the older Reed-Solomon only FEC systems, trellis coding permits system operators to transmit their digital signals either with greatly enhanced robustness (i.e., lower bit error rates) or at lower power levels to reduce interference into analog or other digital signals. Also, since cable systems can experience third-order intermodulation distortions such as composite triple beat, each 1 dB reduction in input power results in a 3 dB reduction in third-order intermodulation products.

Trellis coding has dramatic implications for digital MMDS system. The 2 dB signal to noise advantage enables a much larger broadcast coverage area, theoretically an increase of 58%.

A further technical advantage of the ITU Trellis Coded QAM standard is the use of rotationally invariant coding. Rotational invariance arranges the QAM symbols in such a way as to make decoders insensitive to phase offset (rotation) of the QAM constellation. This innovative technique facilitates the initial acquisition of the digital signal, and also minimizes the need for re-acquisition in the event of carrier phase slips.

GI has worked with other leading companies to define extensions to the ITU Trellis Coded QAM standard for operation at 256 QAM, enabling information data rates of 38.8 Mbps through a 6 MHz channel. The 256 QAM/FEC trellis code extensions have now been adopted by both the ITU and the SCTE, and will allow equivalent (i.e., 2 dB) performance advantages over Reed-Solomon only (t=8) 256 QAM systems. The ITU J.83B standard also now includes a programmable interleaver depth capability, allowing system operators to make a tradeoff between robustness and latency. The programmable interleaver depth capability equates to a burst protection range of approximately 4 uS to 528 uS. Operators desiring very low latency for applications such as two-way data (i.e., cable modems) may select a low burst protection rate, while operators more concerned with robustness (e.g., 256 QAM video) may select a greater interleaver depth.

(c) MPEG-2 Video Encoding

The primary determinant of video quality in an MPEG-2 video system is the encoder implementation, i.e., the methods and efficiency of compressing source material into an MPEG-2 bitstream. Since the MPEG-2 video standard does not specify encoding techniques, but rather only specifies the resulting compliant bitstream, there will be major differences in quality and performance between the various MPEG-2 video systems now coming to market.

GI's MPEG-2 video encoder teams have unparalleled experience in designing and developing digital video encoders. Since 1989, GI has developed several high-performance digital video

encoder systems: (i) the DigiCipher I encoder, which won an Emmy Award as the world's first digital television system; (ii) the FCC "test slot 3" interlace scan HDTV Encoder, the world's first all-digital HDTV encoder; (iii) the FCC "test slot 6" progressive scan HDTV encoder; (iv) the Grand Alliance HDTV MPEG-2 video encoder (with AT&T), the world's first MPEG-2 compliant (Main Profile, High Level) HDTV encoder; (v) GI's MPEG-2 compliant (Main Profile, Main Level) standard resolution (NTSC/PAL) DigiCipher II encoder; (vi) the DirecTv DSS MPEG-2 encoder; and (vii) the Magnitude DVB/MPEG-2 encoder.

There are at least three noteworthy technical features of GI's DigiCipher II/MPEG-2 encoders that allow enhanced video performance.

First, GI's video encoders use exhaustive, full search motion estimation techniques, providing a major performance advantage over the less efficient method of hierarchical motion estimation. Second, GI's encoders employ an advanced implementation of "film mode," enabling a major boost in quality and/or channel capacity for film material. Film mode automatically detects program material originally derived from film (24 frames/second), and takes advantage of the inherent redundancy in film which has been converted to NTSC video (59.94 fields/second) via "3:2 pulldown." GI's current film mode implementation is less sensitive to false edits typically found in film material which has been converted to video. Third, GI's encoder utilizes an innovative method of "statistical multiplexing," allowing much better and more consistent video quality by dynamically reassigning bandwidth between the programs sharing a common bitstream multiplex, depending on the content of each individual program at any given moment in time.

The benefit of these advanced encoding techniques to programmers and network operators is the ability to carry up to 40% more channels of the same video quality, or to carry the same number of programs at higher quality, relative to competing MPEG-2 encoding systems.

(d) Dolby Digital AC-3 Audio

The excellence of the Dolby Digital AC-3 audio system is widely known throughout the international technical and creative communities, as a result of side-by-side tests with other digital audio systems in visible standards arenas such as the Grand Alliance/ATSC and MPEG. More recently, Dolby AC-3 has been adopted by the consumer electronics industry for important emerging products such as the Digital Video Disk (DVD) format and the Pioneer Laser Disk Format. Hollywood studios generally favor Dolby's AC-3 technology, and consumers around the world perceive the Dolby name as being synonymous with a high standard of sound.

Stereo AC-3 signals can be coded at a rate of 192 kbps with equivalent quality to other two-channel digital audio systems operating at 256 kbps. High quality 5.1 channel Dolby AC-3 digital surround sound signals can be coded at 384 kbps, with good quality at 320 kbps. Importantly, stereo Dolby AC-3 decoders can extract two high quality channels from future 5.1 channel AC-3 surround signals. Finally, Dolby AC-3 is designed to be fully compatible with Dolby Pro Logic Surround decoders, which have become integral components of home entertainment systems with several million consumers throughout the world.

The Dolby Digital AC-3 audio system has been adopted as a standard by the ATSC and the SCTE.

(e) System Information (SI)

The System Information (SI) used in GI's DigiCipher II system is compliant with the SI standard adopted by the ATSC and the SCTE.

The SI Standard defines the transmission parameters needed by digital decoders to acquire and process both digital and analog transmissions. The SI incorporates the system-wide network information needed to define frequency plans, modulation modes, and associated information for terrestrial, cable and satellite network environments. It also provides for the definition of virtual channels, a powerful technique for permitting flexibility in network management and supporting convenient user navigation through the multi-channel program universe. Importantly, the SI's compact virtual channel tables provide the necessary linkage to any independent electronic program guide database. The SI also provides for the association of program source information with packetized program stream elements.

The SI's multilingual text format supports any language via the Universal Multiple-Octet Coded Character Set standard (ISO/IEC 10646-1) for enhanced functionality in worldwide applications.

The SI's Modulation Mode Tables encompass a broad scope of currently used or planned modulation techniques, including QPSK, OQPSK, BPSK, QAM and VSB.

The SI serves as a general purpose platform to enable broadcast television, audio and data services, as well as extensions to support the implementation of interactive services. For cable and satellite applications, the SI provides clarifications and extensions to the MPEG Program Specific Information (PSI).

The SCTE has not only adopted the ATSC SI standard, but has also adopted a supplemental standard involving cable and satellite extensions. The SI Extensions standard includes additions

to the MPEG Program Map Table, certain information about video parameters, and messages containing detailed program information. The SI Extensions standard also provides a flexible and extensible program rating and parental control mechanism, an increasingly important capability highlighted by the V-Chip portion of the Telecommunications Act of 1996.

(f) Data Services

GI's digital system uses a flexible syntax for carriage of isochronous and asynchronous data services. The system supports a continuous range of isochronous data rates from 19.2 kbps to 9 Mbps.

The syntax also supports a wide but non-continuous range of asynchronous data rates, ranging from 300 bps to 288 kbps. The supported asynchronous rates must be multiples of 300, 2400 or 19200, with the integer multiple ranging from 1 to 15. For example, a base rate of 19.2 kbps and an integer multiplier of 15 provides the maximum asynchronous data rate of 288 kbps.

(g) Vertical Blanking Interval (VBI) Service Coding

GI has defined a generic syntax for carriage of specific types of VBI data in the MPEG-2 user data section of the video coded bitstream. The user data is carried at the MPEG-2 video picture level, in the style of the remainder of the MPEG video data. This user data is coded flexibly to carry closed caption format information, Vertical Interval Test Signals (VITS) and any non real-time information formats, Subscriber Identification/Automated Measurement of Lineups (SID/AMOL) formats for Nielsen ratings and commercial insertion verification, and full bandwidth real-time formatted lines. The syntax is extensible in the future for newly defined formats such as emergency information or program ratings.

4. Conclusion

GI's DigiCipher II/MPEG-2 digital television system is based on the MPEG-2 video and transport standards, as well as on other open standards such as the ITU/SCTE Trellis Coded QAM standard, the ATSC/SCTE Dolby AC-3 audio standard, and the ATSC/SCTE System Information (SI) standard. Open standards, however, are not sufficient for achieving interoperability. GI has therefore supplemented its selection of open standards with a broad licensing program. By providing documentation, engineering support, and interoperability testing, GI and its licensees offer multiple sources of interoperable equipment to the emerging digital television market.

Various other MPEG-based digital television systems have also now emerged. As these systems are examined, customers will observe significant performance differences between the various

systems, particularly with respect to video quality (due to differences in MPEG-2 encoders), transmission performance (due to advanced forward error correction techniques such as trellis coding), and access control (with respect to both security and features). In developing its DigiCipher II/MPEG-2 digital television system, GI has strived to achieve the difficult task of simultaneously embracing open standards and achieving uncompromised technical performance.

APPENDIX D

Smart Card Technology & Broadcast Systems White Paper

Eric J. Sprunk

Director, Access Control & Security Technology

General Instrument Corporation

1 April 1997

Introduction

General Instrument continually encounters certain over-simplified viewpoints regarding the applicability of smart cards to broadcast-oriented security systems. These viewpoints are primarily the result of efforts by smart card suppliers to present their product as the solution to all problems, for obvious marketing reasons. This white paper outlines some of the reasons General Instrument does not employ certain types of "standard" smart cards for security purposes, as well as some of the history behind these decisions.

Smart Card Companies and Marketing

Smart card supplier organizations divide into two basic groups, with different motivations. First among these are the manufacturers of the smart cards or the chips that go within them. These companies are involved in a commodity-oriented business, and have years of sale efforts in numerous industries behind them. I discuss below why this is not necessarily a good thing for the broadcast application.

The second group of companies pushing smart cards as a "universal solution to all problems" are companies without the history or resources to provide a product on any other platform. This is because smart cards are a low-entry-cost product, basically consisting of no more than some simple software development, and involving no hardware or circuit expertise whatsoever, and little system perspective. The smallest of companies is able to produce a smart card for many applications, which allows them to appear as competent and experienced as more long term, committed industry participants, yet not actually have a large commitment in resources or substantial relevant background.

In essence, then, there are three forces behind the prevalence of smart cards today, with only the first of these being relevant to market need:

- Smart cards, along with similar technologies, are consumer-oriented and thus an appropriate form for a portable or removable technical device in many applications. There are no mysterious reasons for this, and other technologies are prevalent in applications such as the game industry. Smart cards make technical sense in some applications.

- Large corporations such as Motorola or SGS-Thomson naturally take steps to sell their product into all conceivable or even remotely plausible applications. Unfortunately, this sometimes entails the manufacturer having to purport their product as appropriate for an application they really know nothing about. But, this is not surprising. It is left to the (perhaps unfortunate) customer, or to the competitors familiar with the application, to counter their argument.

- Smaller corporations which are either not sufficiently funded or unwilling to propose anything but an off-shelf device. These companies must point to the technical "benefits" of the technologies as the reasons for their use of it, since they can hardly admit a lack of financial commitment to their product line. Smart cards are an excellent mask to make a very small player look much larger.

Inappropriateness For Broadcast Application

First, let us examine the basic technical appropriateness of smart cards to a modern digital broadcast Access Control System (ACS). The use of any security technology in such an application should be limited to technologies that were designed for or have experience in similar or identical environments; otherwise the reality of the new environment could prove disastrous as a proving ground.

Smart cards were developed for banking and telephony applications, which are certainly consumer, portability-oriented environments. These areas are where the popularity of smart cards began. But consider what was being protected in that environment of "one use, one smart card" and point-to-point, low-value transactions. These would include transactions from a remote ATM to a central bank for a consumer to extract a few dollars for lunch, or perhaps for a consumer to make a two dollar phone call on a public phone.

Almost all financial transactions are of two basic types: inter-company and consumer-company. Note that the amount of money differs by a huge factor between these, with million or billion dollar transactions in the former case and perhaps a few tens of dollars in the latter (on average, or course). Smart cards are used for the consumer-company transactions ONLY, and NEVER for the inter-company. This is not for any technical reason, since it is clearly possible for billions of dollars to be protected using the same technology, yet it is never the case that one bank mails a smart card to another, or buys stock for a pension fund, or makes a business loan using a smart card. Though there are applications where this could be convenient, it is conspicuously never done! Why?

This is simply because smart cards are not designed to protect more than the small amounts of money in the consumer-company transaction, and banks or phone companies or other large organizations are not so foolish as to risk larger amounts. Any intelligent company seeks to optimize the level of protection placed on any transaction, and will not spend money on exorbitant protection for small transactions. The technology should fit the need.

But in a broadcast environment, the amount of money is vastly larger due to the simple fact that so many potential customers of the pirate all want exactly the same thing - the entertainment service. In the US, pirates have been known to make several hundred thousand dollars per month because of this effect, so there is no question that

a market exists. This means that the value of the material protected in a broadcast environment is more similar to the inter-company transactions in the banking industry, as described above. A broadcast environment transaction is not the same as a customer-company transaction, which is why smart cards are inappropriate. Smart cards actually have NO track record of successfully protecting the amount of value present in a broadcast environment. Smart cards protect a few hundred dollars, and the broadcast environment routinely transmits information worth millions of dollars. It is the self-serving "smart cards are the panacea" claims of companies that either make them or must use them (due to resource limitations) that attempt to blur this important distinction.

As an aside, this is how some vendors claim "top quality security". If a product has not protected material of enough value, there is no market drive for someone to test its security! (If everyone knows there is nothing in a safe, no one will break into it!)

Difficulties with Generic Solutions for Specific Problems

As mentioned above, smart cards were developed as a generic mass-consumer vehicle for simplistic technical functions, primarily telephony and banking. These and other similar (but not-identical) application needs were responded to by the makers of smart cards. Their response was to commit resources to the development of smart card chips, card bodies, etc. But, since chip development is not an inexpensive thing, the smart card vendors necessarily created generic components to meet the widest variety of applications. Smart card devices are necessarily very general things.

As with any specific application, there will be functions or aspects of a generic device which are inappropriate or simply not needed. In most cases with smart cards, this is not problematic since no significant cost burden is associated with the unused functionality. A more troublesome case is when an important aspect of a specific application is not correctly supported in smart card devices, so that using a smart card in that application means accepting a sub-optimal solution. In the case of high-security applications such as a broadcast environment, this is the case.

General Instrument has had hard experience with exactly this situation. An initial GI product issued in the mid 1980's used an off-the-shelf part that was developed by a major chip vendor as a generic security component. This part was thought adequate for the broadcast environment, and the security of the GI product completely depended upon it. Unfortunately, that part had never been subjected to the attacks broadcast environment security devices must realistically resist, and the component failed miserably. General Instrument had to invest multiple millions of dollars to develop a truly effective security device.

Smart cards today are quite similar. They were optimized for an environment different from the broadcast one, and are inappropriate in several ways, some involving

security, and some involving performance that affects security. The basic desire for a *perceived* cost saving by using a smart card (due to *assumed* economy of scale with other applications) is severely threatened (or outright invalidated) by the lack of security measures that are mandatory for survival in the broadcast environment.

Examples of this are easy to come by once one considers the issue. For example, the exact encryption algorithms, data formats, message protocols, and secure memory arrangements will necessarily vary from application to application, yet a single smart card design is often proposed for all applications. This would necessitate general data load or extraction capabilities (or lack of specific defense), as well as a lack of custom hardware to protect against protocol violations or manipulations. At the very least, any fundamental problem with a chip would exist in all applications for that device, which had occurred in more than one case with a standard off-the-shelf component.

Fundamental Security Problems

In the broadcast environment, the use of a smart card presumes a partitioning of system security functions *out of* the Decoder (or IRD) and *into* the smart card. Since a smart card cannot perform high-speed data decryption, there is a need for a standardized data decryption device within the Decoder, and the smart card would necessarily supply keys to that decryption device as needed. This architecture follows purely from the assumption of standardized smart card use, and there are fundamental problems with it.

The first of these is the easy ability to move a smart card from one Decoder to another. This may be trivially limited by some component within the Decoder, but the smart card architecture itself, with its endemic architectural assumptions, mandates the separation of security function between Decoder and smart card. The smart card is therefore fundamentally mobile. The DirecTV System has this characteristic.

Mobility means that it is difficult to enforce where a particular smart card is located. This means that a consumer can often take his (subscribed and legal) smart card with him to a friend's house to view services there, even though this may not be the intent or conditions of his subscription for those services. This also means that it is very difficult to tell if a single smart card is in *more than one Decoder at the same time*.

What does "*more than one Decoder at the same time*" mean? It means that a copy, or clone, of the smart card can proliferate without limit, since a single smart card that is copied 10,000 times will happily work in 10,000 different Decoders, without restriction. In this regard, the architecture resultant from the use of a smart card is inherently susceptible to this and certain other forms of piracy. The presumed savings in initial Decoder cost is more than offset by this vulnerability, since tremendous lost revenues can result!

Another basic problem with smart cards in the described architecture is the transfer of keys from the smart card to the (necessarily standardized) encryption algorithm within the Decoder. Recall that this is necessary because smart cards cannot encrypt or decrypt high-speed information; thus another component must do so.

In most systems, including those in Europe, the smart card sends a key to the Decoder about once each 10 seconds. This is usually a key of about 64 bits, so the data rate is about 6.4 bits per second. This amount of information is trivial to transmit to other units that do not even have a smart card in them. This key information is usable by the Decoder decryption device in all Decoders, no matter which one it came from, so this is fundamentally possible. This attack is called a "McCormack Hack", and is named after an Irishman who invented it years ago. The attack is now used actively in Europe, since smart cards are prevalent there.

Fundamental Security Technology Limitations

There are other numerous limitations of smart cards for security applications in general, with the broadcast application the most acutely suffering example:

- Smart cards are limited in the size and power dissipation of the chip they contain, which limits the memory and processing power they can contain. This limits not only the application complexity within the card, but also the complexity of security algorithm possible. Though this may not be a problem in many applications, it remains a ceiling on smart card capabilities.

- Smart cards adherent to the ISO-7816 standard are 0.75 mm thick, which restricts the use of a battery in the card. This limits the technology used in the smart card chip to less dense EEPROM, and is typically less secure.

- The ISO-7816 interface runs from 9600 to about 100K bits per second, which might be sufficient for key transfer every 10 seconds, but is woefully inadequate for faster key rates or notable data traffic. General Instrument prefers to change its system keys several times per second, not once in 10 seconds, and the slow interface prevents this most basic security measure. In addition, the card cannot support the key transfer for multiple services at such low rates, as well as limiting other system message traffic. Fewer total services can thus be supported by this interface rate. The equivalent GI product interface rate is several megabits per second to avoid these problems.

- As mentioned, a smart card architecture presumes a standardized high-speed encryption algorithm located in the Decoder. This is problematic if that algorithm is untested or erroneously specified. Unless a very-high-confidence algorithm is used for this purpose, then the smart card architecture results in added risk in this algorithm as well. The DVB Common Scrambling Algorithm is an example

of this, since it is a new method without history or confidence. Use of DES, for example, avoids this particular problem.

For these and other reasons, several organizations have rejected standard smart cards as proper solutions for portable modern security technology. General Instrument is in philosophical agreement with organizations such as the National Renewable Security Standard (NRSS) 50 megabit device, or the Digital Video Broadcast (DVB) Common Interface high-speed PCMCIA solution. Both of these organizations are aware of many of the problems associated with standard smart cards, and have chosen another route for their future.

The GI Solution

All of the problems and issues mentioned above explain why GI does not use smart cards in the normal sense of the word. General Instrument stands behinds its products with a security warranty, and our hard-won experience tells us that problems will be substantial with a generic smart card approach. In fact, all of the smart card systems we are aware of are known to be broken as of this writing, with one possible exception that recently entered the marketplace. Our products have been unbroken in actual use (to the best of my knowledge as the person responsible for tracking it) for more than 7 years, since we began on our post-piracy technical path. But what is the approach that we have found to be so secure? It has the following characteristics:

1. All security components are 100% custom chips developed and optimized for the broadcast environment. The cost of this is borne by GI as a necessity for providing an effective security product to our customers.

2. All Decoders are initially shipped with a security component embedded within the unit, not in any smart card or other removable package. Should this component be the victim of a security breach, it is designed to relinquish control of the Decoder to a renewable security device when that occurs (and NOT before).

3. All GI security components, whether they are the initial, embedded type or a renewable type, are designed for advanced security algorithms including battery-backed RAM, very-high-density chip geometry, and several potent defense mechanisms for resisting tamper efforts even by advanced laboratories. The embedded security device contains buried packet decryption circuits, so that no McCormack Hack is possible.

4. The GI renewable security component, called the TvPass Card, is a similarly advanced custom GI chip. It is connected to the embedded security device (when needed, only) by a several megabit path, which allows support of multiple simultaneous services and other system message traffic without the limitations of slow smart cards. This device is not packaged in a smart card package, but is

instead housed in another form well known for consumer practicality and widespread use. This form is actually very similar to game cartridges used by Nintendo, or Amiga, and is an established approach to high-speed, consumer oriented portable technology.

Conclusion

This memo has covered some of the basic problems associated with smart cards in high-security, broadcast applications, and why General Instrument does not adhere to their simplistic, standard-component philosophy of ubiquitous use. It is hoped that the reader will find this material thought-provoking, and apply his own judgment to the issues.

APPENDIX E

SYSTEM INFORMATION FOR DIGITAL TELEVISION ON CABLE

Mark Eyer and Robert Rast
General Instrument

Abstract

The Advanced Television Systems Committee (ATSC) has adopted, to this date, five standards documents defining digital broadcast television in the United States. ATSC's job continues this year, as its work extends to coordination with standards in non-broadcast media including satellite and cable. One new ATSC standard, System Information for Digital Television *(A/56), defines the transmission parameters broadcast digital decoders need to acquire and process both digital and analog transmissions, together with features that facilitate interoperability among non-broadcast media. The SI database includes frequencies, modulation methods, virtual channel descriptions and other useful data for the Decoder to facilitate user-friendly navigation among the profusion of digital services available. This paper will describe how A/56 can be extended to the cable application, how (with extensions) it is used to define or re-define the environment in which digital cable decoders navigate among available analog and digital services, and how it supports Interactive Program Guide (IPG) and Near Video On Demand (NVOD), as well as downloaded or ROM-resident applications.*

INTRODUCTION

As cable television service makes the transition from analog to digital, the need for standards increases in importance. Standards permit interoperability, which has many dimensions. Words evoked by the concept of interoperability include *interchangeable*, *exchangeable* and *consistent*.

Interoperability can mean that cable operators are able to buy interchangeable hardware from a number of vendors, with the resulting competition providing better performance at lower prices. Interoperability can mean that TV signals can be exchanged between media readily, e.g., signals received off satellite can be passed into the cable plant with a minimum of processing. Interoperability can also mean that consumer electronics equipment performs equally well when interconnected with cable, satellite or telco equipment. Interoperability is desirable, and is achieved through standards.

In 1995, the Advanced Television Systems Committee (ATSC) documented the standards for the broadcast digital television transmission system recommended to the FCC by its Advisory Committee on Advanced Television Service (ACATS). While most of the standards focused solely on over-the-air broadcasting, *System Information for Digital Television* (A/56) was written more broadly as a reference standard, with "hooks" to facilitate interoperability with cable and satellite. This paper describes the standard as it can be extended to apply to cable.

Digital Standards for the Cable Industry

Looking forward, the ATSC will broaden its role to coordinate standards across media for North America. It will depend on those industries to set their own standards, and to bring them to the ATSC for coordination. While companies in the cable industry are already broadly involved in digital standards setting activities, including ACATS, ATSC, EIA/NCTA Joint Engineering Committee, and MPEG, there is a need for increased standards setting activity within the cable industry itself.

Now sanctioned as an official ANSI standards setting body, the SCTE is an ideal

body to sponsor digital cable standards work. The SCTE is launching a digital standards committee, the work products of which will be brought to the ATSC for coordination with other media. We urge you to participate in and support this important SCTE activity.

THE MOVE TO DIGITAL

For a cable decoder box on a cable carrying analog-only carriers, life is simple. One need only know the overall frequency plan in use to access the single audio/video service in each 6 MHz band. Channel numbering is hard-wired — each channel number the user sees is associated with a known fixed frequency.

With the introduction of the first digital multiplex comes a new distribution method for programming. Thanks to video compression, each 6 MHz channel can carry several video services, and each of those can include one or many audio tracks, as well as associated data such as subtitles, text, or game-related data.

The operator may want to provide on one "channel" a movie service that offers a given movie starting every 15 minutes (NVOD). In this case it is clear the old paradigm, in which the channel number simply maps to a frequency, must be left behind.

Other digital channels can provide access to special program guides, news services, or a weather information service. The data for such channels will be carried along with many other services on one of the digital multiplexes available to the cable box.

THE NEED FOR DYNAMIC NETWORK RECONFIGURATION

In the analog cable plant, changes to the channel line-up are infrequent because subscribers must be notified by mail of changes well in advance and supplied with updated channel reference cards—an expensive procedure, both in money and in time.

By contrast, in the digital world, the system operator will be required to reconfigure the network often, not only because the total number of programming sources is now so much larger, but also because of the way digital services are transported.

In the digital multiplex pipeline, each digital service occupies a different portion of the total bandwidth available in the pipe. It is possible to carry in one multiplex four high-quality digital NTSC signals carrying video frame-rate material. But for programming originating at film frame-rates, six can be carried at roughly the same quality level. As an example, and with this in mind, it is possible the operator may want to change the multiplex configuration on Sundays in order to carry NFL games. Shifts in bandwidth allocation for video services will be commonplace.

Especially in the beginning, new digital video services will be popping up every day. The subscriber needs to be able to conveniently access the new services, and have them seamlessly integrated into the channel line-up. If the system operator needs to move a service from one multiplex to another he needs to be able to do so freely, without having to worry that customers will be confused by such changes.

How does the cable box adapt to the digital environment and guide the user to select among the new digital offerings? How can it manage a mixture of analog and digital services, and seamlessly accommodate the dynamic changes in network definition as they occur? How are NVOD, data services, and access to broadcast downloaded applications handled?

The answers to all these questions can be found in ATSC A/56, *System Information for Digital Television*. Although A/56 effects constraints on possible SI tables to reflect the needs of broadcast, it defines the data structures and tables necessary to facilitate interoperation with media needing broader functionality.

STANDARDIZATION FOR NON-BROADCAST MEDIA

ATSC A/56 fully specifies SI for the broadcast application. It states that constraints for other media are "under study." Work is underway to complete the system specification of SI for non-broadcast media, building on the message syntax provided in A/56. It is expected that other media will standardize on their practice in a way that effectively builds around the broadcast kernel. A proposed standard based upon A/56 is called *Cable and Satellite Extensions to the ATSC System Information Standard*, available for review. The document be downloaded from the Internet through http://www.gi.com.

WHAT IS THE FUNCTION OF SYSTEM INFORMATION?

The primary function of SI is to facilitate acquisition and navigation among analog and digital services available to a particular Decoder. SI also serves as a support platform for applications such as Interactive Program Guides (IPGs) and Near Video On Demand (NVOD). This paper discusses the *System Information for Digital Television* specification and its applicability and expected use in the cable environment.

System Information comprises a database of various tables pertinent to the cable application, including the Carrier Definition Table (CDT), Modulation Mode Table (MMT), the Virtual Channel Table (VCT), and the Source Name Table (SNT). The function of these tables is described below, and their relationship to one another is outlined.

SI also includes tables which support consumer features like parental ratings control and Impulse Pay-Per-View (IPPV). Tables in this category include the Rating Text Table (RTT), the Ratings System Table (RST), the Currency System Table (CST), and the Map Name Table (MNT). Each of these tables is also briefly described.

The functionality of the Virtual Channel Table is discussed in detail because its fu[illegible] in the cable application is seen as [illegible] The VCT is critical to the [illegible] management of distribution and end-user navigation of digital services, as well as to the migration from an all-analog to an eventual all-digital network.

WHAT IS SYSTEM INFORMATION?

System Information comprises a database whose tables describe various aspects of the network. The tables include:

- Carrier Definition Table (CDT) — defines each of the frequencies in use in the cable plant.
- Modulation Mode Table (MMT) — defines the method used to modulate digital carriers in the network.
- Virtual Channel Table (VCT) — defines the collection of analog and digital services available to the cable box and assigns a user channel number to each. The VCT also acts to support downloaded and resident applications such as IPG and NVOD.

In addition to these three primary tables, Network data includes a System Time message, used to time-synchronize all components in the system, from equipment at

the satellite uplink all the way down to the cable Decoder. Using a reference to System Time, changes to entries in the Virtual Channel Table may be specified in advance of the time they are to become effective.

HOW IS SI DELIVERED?

In a typical cable plant, an out-of-band (OOB) channel is made available to each Decoder. The transmission format for the OOB channel is compatible with the standard MPEG-2 multiplex defined in *ISO/IEC 13818-1 (MPEG-2 Systems)*. ATSC A/56 says that SI data is carried on the "Network PID" in the MPEG-2 multiplex. A review of the structure of an MPEG-2 multiplex may be helpful.

THE MPEG-2 TRANSPORT STREAM

Figure 1 shows the composition of an MPEG-2 Transport Stream (TS) as it is output from an MPEG-2 encoder. A TS may be thought of as a pipe that carries a number of smaller pipes, each of which comprises a digital service. Each service is in turn composed of a number of Elementary Streams. In a typical case, the service might be composed of one MPEG-2 video stream, two stereo audio streams (compressed using Dolby AC-3), and two subtitle streams. In addition, one stream carries data the Decoder uses for access control, and another carries the definition of the service itself, a structure called the Program Map Table (PMT).

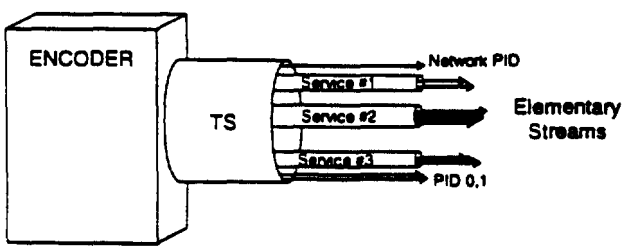

Figure 1. MPEG-2 Transport Stream

Each MPEG-2 TS also must include three special streams: a stream that carries a directory structure for all services on the TS (the Program Association Table [PAT]); the Network PID; and a stream that allows the cable box to find Entitlement Management Messages (EMMs) for conditional access.

The PAT is always carried in PID 0, so the place a Decoder starts when processing a TS is to acquire PID 0 and record it. The PAT provides a list of pointers to Program Map Tables on the TS. It also provides a pointer to the Network PID, the stream that carries System Information.

CARRIER DEFINITION TABLE

The CDT is a simple table that lists the center frequency of each 6 MHz channel in use. Frequencies in excess of 2 GHz can be represented at 125 kHz resolution.

MODULATION MODE TABLE

The function of the MMT is to provide a list of all the digital modulation methods and symbol rates in use in the network. For QAM modulated carriers, the size of the constellation is given.

VIRTUAL CHANNEL TABLE

The Virtual Channel Table provides the cable Decoder with a numbered list of all available analog and digital services, as well as the path and demodulation method required for their access. Each record in the table provides:

- The Virtual Channel Number (VCN), a number in the range 1 to 4095. Typical systems may limit definitions to the three-digit range, 1-999.
- The channel type, including NVOD, "hidden," or regular (described below).

- The physical cable (A or B) which carries the service (for cable plants in which two cables are available).

- A digital/analog flag to indicate whether the channel is carried in an MPEG-2 Transport Stream, or is a clear or scrambled analog NTSC waveform.

- A reference to the CDT, to indicate the center frequency of the 6 MHz band carrying the analog or digital carrier comprising the service.

- For digital services, the modulation format and symbol rate, by means of a reference to the Modulation Mode Table.

- Again for digital services, the MPEG-2 program_number, used to select one service from the many that may be carried on the Transport Stream.

- The Source ID, a number uniquely identifying the programming source. Optionally, an application ID may be specified to tie the channel to a ROM-resident or downloaded application.

Virtual Channel Numbers

An important aspect of the VCT is that it provides a channel mapping function, allowing the system operator to assign a familiar and consistent one- to three-digit number to each service offering.

Channel line-ups will change from time to time. When they do, changes will be reflected in the composition of the Virtual Channel Table. The VCT, as well as all the other tables and messages in the Network PID, are transmitted continuously at a low, background, rate in the Network PID in the OOB channel.

At one point in the future, each analog channel is likely to convert to digital transmission format. At that time, the VCT reflects the change in access path. The channel number, however, can remain the same, allowing customers to continue to access the programming via the same familiar channel number.

Flexibility in channel numbering also allows the cable operator the chance to group channels by theme or category, if desired. For example, premium movies could start at channel 100, the sports channels at 200 and Spanish-language programming at 300.

Hidden Channels

Channels may be defined in the VCT to be regular, "hidden," or NVOD.

A channel may be marked hidden in the VCT to prevent its access by direct ehannel number entry or by channel "surfing." A hidden channel may be used as an access point to an application such as a program guide. A button marked GUIDE on the remote control, for example, could be wired to a hidden channel that provides the access point to the IPG function. The VCT also uses hidden channels to define the components of an NVOD group.

Near Video On Demand

The Virtual Channel Table supports NVOD in the following way. A channel may be marked as an NVOD access channel. If that is the case, the VCT record for that channel points to a group of hidden channels in the table that form what is called the "NVOD group."

Each channel in the NVOD group will typically be offering the same program title, but with start times that are offset by some number of minutes from the previous channel in the group.

The services which comprise the NVOD group need not be carried on a common MPEG-2 transport multiplex. In fact, they do not even need to be digital services (although in all likelihood they will be).

Tuning to an NVOD channel is analogous to walking up to a theater multiplex in which the same movie is playing in several theaters, each with different starting times. Taking a look at the schedule, it will be clear which theater to enter for the shortest wait for the next showing.

In the case of acquisition of an NVOD channel, the Decoder handles this selection process transparently to the user. The "schedule" is found when the Decoder tunes to the first channel in the NVOD group. Then based on start times, it tunes to the appropriate channel in the group.

To continue with the theater analogy, let's say a showing of the movie starts every 15 minutes. It is possible to leave one theater, go out to the lobby for 15 minutes, and then go into the adjacent theater without missing any of the film. This "pause" feature can be offered in NVOD as well. Alternatively, a person could "jump" backwards or forwards in the movie simply by moving from one theater to another. NVOD can work similarly.

SOURCE NAME TABLE

Program sources in the SI standard are uniquely identified in the system by a 16-bit number called the Source ID. For example, Showtime's East coast feed will have a different Source ID than the West coast feed. Every broadcast channel, cable channel, and satellite super-station channel will have a unique Source ID.

Uniqueness is necessary because Source ID is used as a pointer into program guide databases and acts as the linkage between the VCT and an IPG.

The Source Name Table simply provides a textual name for each Source ID currently used in the system.

VIRTUAL CHANNELS AND AN IPG DATABASE

Like any database, a program guide database is a collection of records indexed by a *primary key*. All records, for example, pertaining to schedules, program titles, and program descriptions for WNBC must be associated with one another. The primary key for an IPG database is the Source ID.

The Source ID links an IPG database to the Virtual Channel Tables in the following way. If a user is browsing through the interactive guide looking for current programs, he may stop, highlight a certain program, and select it for viewing. The selection process results in the need to find a virtual channel associated with the selected Source ID. To resolve the reference, the Decoder searches through the VCT to find a match on Source ID. Once a match is found, the service is acquired by following the access path defined in the virtual channel record.

The Source ID may also be used by the IPG application in the Decoder to avoid displaying on the grid any channels that are not accessible (i.e., currently have no access path defined).

An IPG database could be designed that did not use Source ID as an indirect pointer. Consider what would happen if the IPG database had the access path information inside it. Commonly, one program source is available in many hundreds (or even thousands) of physical locations, as when for example HBO is carried on many cable systems. If the IPG carried the access path data for HBO, each

cable system would need to have a custom version of HBO's program guide database. If, instead, indirection through Source ID and the VCT were used, just one version of HBO's program guide data would be usable throughout the country. Use of Source ID eliminates the need to edit the IPG database at the cable headend.

INTEROPERABILITY AMONG MEDIA

One of the primary distribution paths for programming made available on cable is via satellite. The System Information transmission format described in ATSC A/56 supports the satellite delivery medium as well as cable and over the air broadcast. Furthermore, the SI design accommodates the need for a single Transport Stream to cross media boundaries without the necessity to reconstruct or edit the accompanying SI data.

Transport across a media boundary, for example from satellite or off-air broadcast to cable, is simplified by nature of the fact that SI data for several media can be present in the same Network data stream. A particular Decoder box ignores any SI data that pertains to a transmission media it does not support.

A small cable operator, for example, may wish to receive a digital Transport Stream via satellite feed, perform QPSK demodulation, remodulate it using QAM and then place it on a carrier for transmission down the cable. SI data present in the satellite signal can include the VCTs, MMTs, CDTs, and SNTs necessary for proper functioning of the cable boxes.

SUPPORT FOR APPLICATIONS

Each Virtual Channel can be associated with a programming source by the Source ID parameter. Alternatively, in order to tie the service components targeted by the channel record to an application program running in the set-top box, the channel can be tagged with an "application ID."

One example of such an application would be an interactive service that offers detailed critiques by well-known reviewers of various movies. A designated "channel" number could be defined to bring up this service. When the subscriber selects this channel, the application is downloaded (if - already resident) and executed.

SUMMARY OF SI FOR CABLE APPLICATION

Figure 2 diagrams an example Virtual Channel Table and shows its relationship to the Carrier Definition Table, Modulation Mode Table, and Source Name Table.

The example shows that channel 2 is defined as a standard MPEG-2 digital channel. Programming for the channel can be accessed by tuning to the frequency at index 4 in the CDT (79 MHz), using modulation parameters from index 3 of the MMT, and that accessing program number 0x2EA9 within the MPEG-2 TS.

Channel 2 is associated with Source ID 0x0030 which, by reference to the Source Name Table, is found to be "WNBC."

The example also shows that channel 4 is an NVOD channel and that NVOD group is four hidden channels starting at channel 1000.

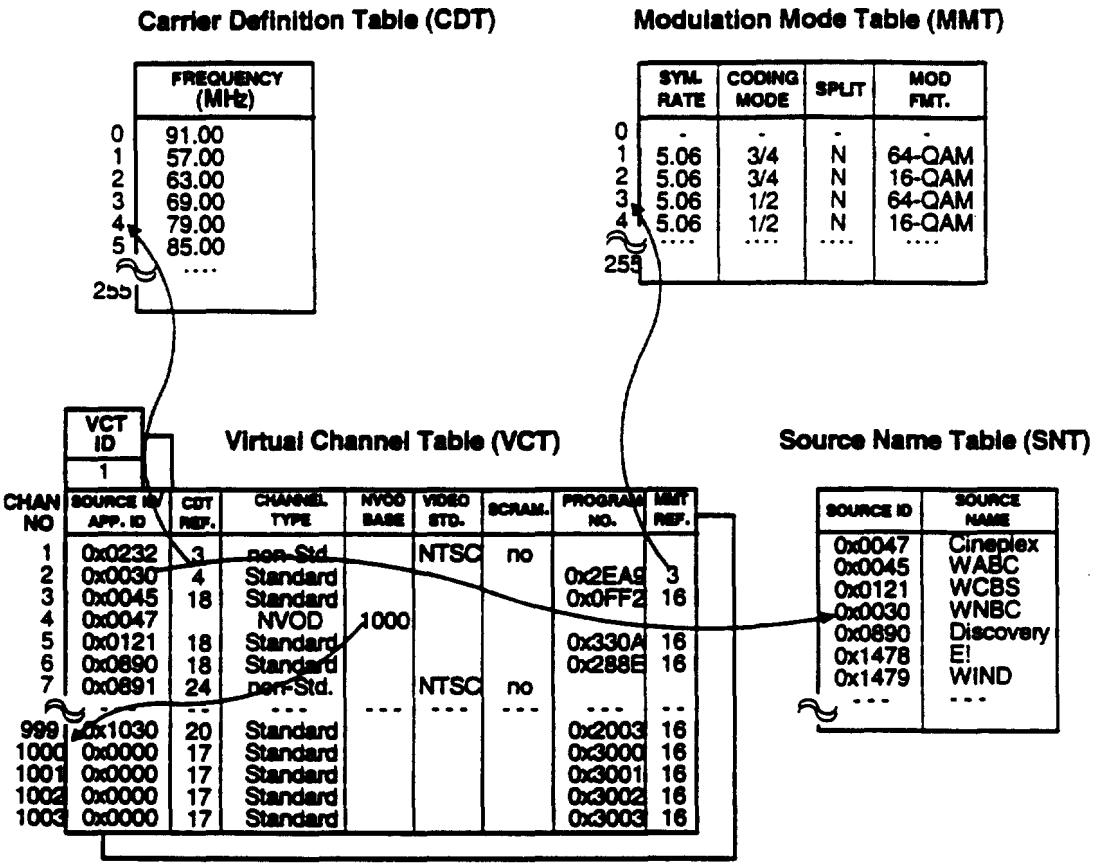

Figure 2. Relationship Between Network Tables for Cable

OTHER SYSTEM INFORMATION TABLES

The most important SI tables have been described, but several others applicable to cable are defined in ATSC A/56. These include the Rating Text Table, the Rating System Table, the Currency System Table, and the Map Name Table.

Rating Text Table

SI includes tables which define a flexible parental rating system. The recently passed Telecommunications Reform Act includes mandatory adoption of support for a "V-chip" device in television sets. The SI tables provide the basis for tagging digitally-transported programming with multi-dimensional, and even multi-regional, ratings.

The Motion Picture Association of America (MPAA) rates movies, and the MPAA rating is an example of one rating dimension. Six levels are currently defined: G, PG, PG-13, R, and NC-17. Violence level can be another dimension. Programmers such as HBO have defined and labeled violence levels in their movies, such as "mild violence," "violence," "graphic violence," etc.

The Rating Text Table defines names for up to six dimensions. Typical names might be "MPAA," "Sex," "Violence," and "Language." Within each dimension, up to fifteen levels can be defined. For the MPAA dimension, the levels would be defined with the familiar G, PG, PG-13, etc. tags.

Decoders can be built to automatically adapt to the rating dimensions and levels,