THE
HOME COMPUTER SECURITY SYSTEM
(HCSS)

A study defining the hardware and algorithmic requirements of a home-computer-based home security system.

by

ART RODRIGUEZ

Lubbock, Texas
July 21, 1978

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

LIST OF FIGURES

1.0 INTRODUCTION

This report documents the results of a study on security systems for the home, performed by the Personal Communications Department for the Home Computer Department at the TI Lubbock site. The objectives of the study were to define, within the framework of the Home Computer (HC) environment, the characteristics of a home security system and to identify as much of the hardware requirements as possible. The most extensive part of the study was establishing both the protocol for communications with the security sensors and the format required.

From the outset, the primary emphasis has been on fully utilizing the capabilities of the HC to offer a system with the features necessary to answer the security concerns of home dwellers as adequately and cost-effectively as possible. Although it is intended that the Home Computer Security System (HCSS) as proposed here be implemented utilizing a radio-frequency (RF) communications link between the sensory devices and the Security Peripherals Controller (SPC), the consequences of utilizing a power-line (PL) link were explored in the course of the study and are considered throughout this report.

One main drawback of a home-computer-based security system for the home is its relatively high price tag. In fact, it is possible to design a system that is non-computer based but which incorporates the more essential security features and would retail for approximately one-half the price of the HCSS. We believe TI's approach to this should be to offer a Home Computer Security System that would appeal to both the more affluent consumer and the consumer that would like to justify a home computer (either at the time of the purchase or later on when he decides to expand his hardware), as well as to offer a stand-alone ("TICOM") security system that would appeal to a much more massive market. (See Appendix B for a description of the TICOM security system vis-a-vis the HCSS.)

We will begin by considering the general characteristics of the system. Then, the system architecture will be examined in detail, particularly with regard to the communications protocols involved. After that, the interface of the system with the user at the console will be delineated. Finally, the system components will be individually described.

2.0 GENERAL DESCRIPTION

As is characteristic of any security system, the HCSS operates by having security sensors (smoke detectors, magnetic switches, motion detectors, etc.) strategically placed throughout the home. The physical layout of these sensors is referred to as the topology of the system.

Each sensory device contains a transmitter and receiver as well as a plug-in ID code module. To provide greatest installation flexibility, it is recommended that an RF link be employed (see section 3.0).

When a sensor is triggered, a digital FM transmission burst is initiated by the triggered sensory device. The transmission contains the system ID and the sensor ID. (See Appendix A.) The Security Peripherals Controller (SPC) detects the transmission, decodes the system ID and the sensor ID and verifies the latter, locates in its memory the phone number associated with that sensor's alarm category (fire, intrusion, personal injury, personal danger, or general emergency) and automatically dials the number, detects the status of the phone lines (busy, ringing, connected, or limbo) and, upon detection of completed status (after re-dial if necessary), delivers a sythetic voice message on the phone line continuously until a disconnect is detected. The synthetic voice message will identify the alarm category and give the street address of the home. Up to three phone numbers can be specified for each alarm type and the SPC will cycle through them, in the order (priority) indicated by the user when the numbers were stored, until a connected status is detected.

The status of the sensory devices is maintained by the SPC. Approximately once every 24 hours, the SPC polls the sensory peripherals by broadcasting an unaddressed polling signal which is in the form of an RF carrier frequency-modulated by a 1-KHz tone. Each sensory device responds with a digital transmission burst that indicates the device is in working order. Failure to obtain a poll response from any device indicates a "dead" status for that device. After a poll, if any sensory device is deemed dead that was not dead before the poll, the SPC will sound its buzzer and continue to sound it in an intermittent fashion until a status inquiry is made at the HC console or until it is time for the next poll, whichever comes first.

If a PL link were employed, the frequency of the polls may be increased as desired, but it is not clear that this would be advantageous. If an RF link were employed, the frequency of the poll cannot be increased without sacrificing battery life.

The HCSS proposed here will support 106 sensory devices; 4 alarm categories, expandable up to 8, 3 phone numbers for each; 12 emergency phone numbers, expandable up to 24; a 30-character street address; and 10 phone answer phrases.

The SPC is backed-up by a secondary battery and will operate for 48 hours in the event of a power outage, independent of the state of the HC mainframe. If an RF link is used, the sensory devices will operate for <u>two</u> years on a set of primary cells (see Appendix C). If a PL link is used, the sensory devices will be backed-up in the same manner as the SPC.

3.0 UNIQUE FEATURES OF THE HCSS

The home security environment is primarily characterized by the security concerns of home dwellers. Through at least two market surveys and three marketing focus groups, the following concerns have been established:

1. Fear of confronting an intruder when returning home or aroused from sleep.
2. Concern for the loss of family mementoes in a fire.
3. Concern for the ability of the alarm to reach someone who can do something about it.
4. Fear of not being able to reach the telephone when in danger or injured around the house.
5. Considerable concern for the ability of an alarm system to operate reliably when needed (e.g., during power outages).
6. Concern for the installation effort required, even of such simple items as window (magnetic) switches.

The following features of the HCSS, as proposed here, answer these concerns:

1. Remote interrogation of the system status with the PST from bed, from outside the home (up to 150 feet away with an RF link), or from a telephone at virtually any distance, answers concern number 1 above quite adequately.
2. Smoke detectors of improved reliability are a standard sensory device that answers concern number 2.
3. Alarm conditions are forwarded to user-specified telephone stations via a synthetic voice message, thereby answering concern number 3.
4. A pocket-size Personal Security Transceiver (PST) can be carried in a shirt pocket by an individual and manually triggered by depressing one of its buttons. Such a

panic-button feature has a highly perceived value to the aged and/or physically impaired and answers concern number 4.

5. 100% battery operation in the RF system and battery back-up in the PL system and the SPC allows for operation during power outages. Also, the ability of the system to test automatically the sensory devices at least once a day increases the reliability that can be achieved manually. This answers concern number 5.

6. Low-cost infrared (IR) motion detectors are a standard sensory device which offers an extremely cost-effective installation-free alternative to magnetic switches.

Note that it is virtually impossible to answer concerns 1 and 4 with a PL-link system. Yet, our market research to date indicates that features which answer these concerns contribute significantly to the consumer perceived value of a home security system.

4.0 SYSTEM CONFIGURATION

The HCSS is configured as a multitude of sensory devices which communicate their status to the Security Peripherals Controller (SPC) through either an RF link or a PL link. The status of each sensory device at any one time can be any one of the following:

1. Triggered - the sensor has detected an alarm condition.
2. Armed - the sensor will initiate a transmission to the SPC if triggered.
3. Disarmed - the sensor will not transmit to the SPC if triggered.
4. Dead - the sensor appears not to be working.

In the case of traffic counters (these are sensors which detect people moving through entry points — doors, hallways — and the direction of motion), armed means that the device is being used as a motion detector and disarmed means that it is keeping track of the traffic. Armed and disarmed are in general referred to as the sensor operating states since they are dictated by the user.

The SPC is linked to the HC via a cable that connects to the HC through the HC cassette port. That cable will be of the same approximate length as the standard cable used to link the HC to the cassette recorder. The standard cassette cable connects the SPC to the cassette recorder (see Figure 1). Two 9-pin "D"-type connectors are provided on the SPC for connection to these two cables. A selection switch on the SPC determines whether the signals coming from the HC cassette port will be received and processed by the SPC ("SEC" position) or will be passed along to the cassette recorder ("CAS" position). A "Y" connector can

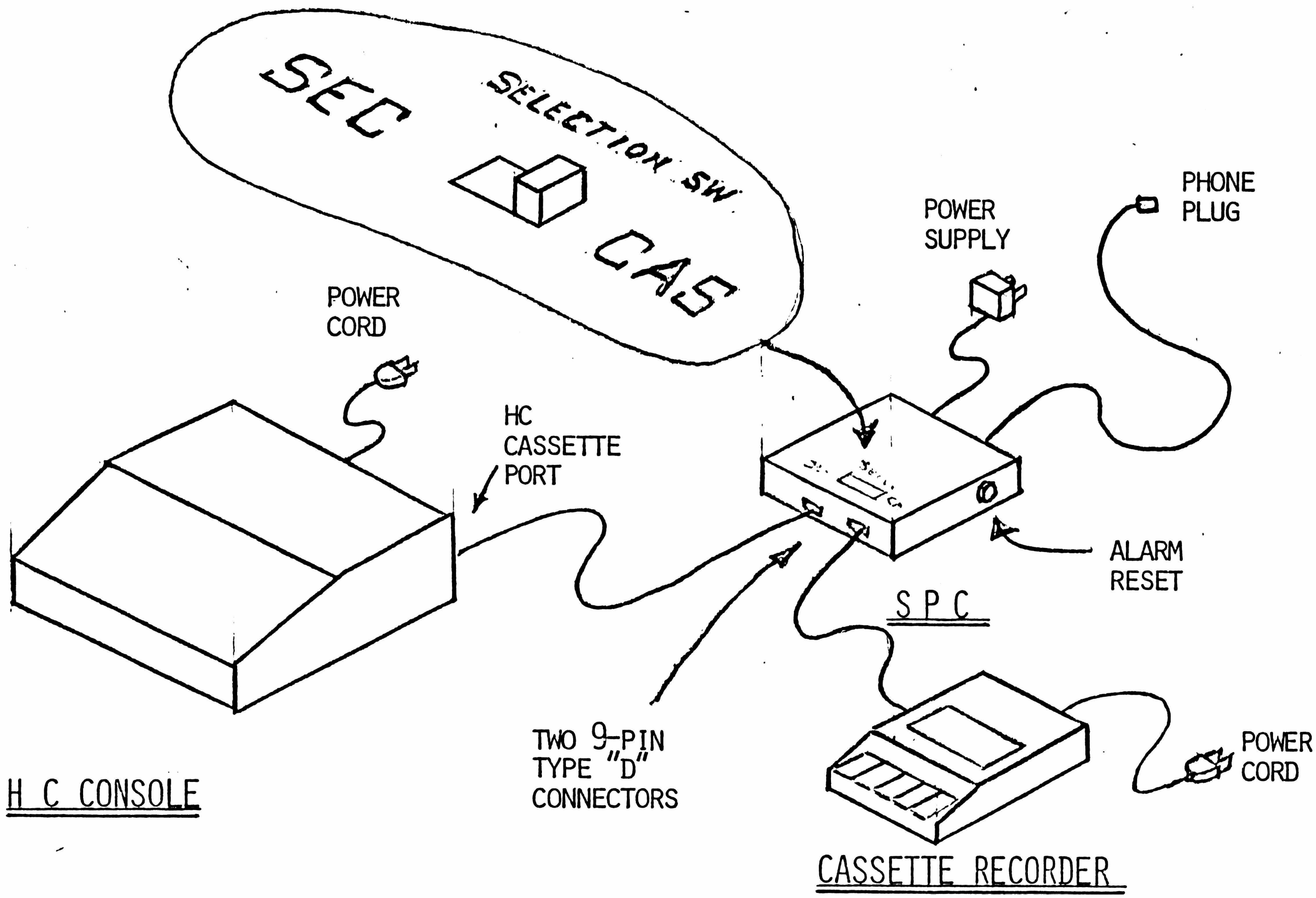


FIGURE 1 - SPC HOOK-UP

be used at the HC cassette port to allow both the SPC and a cassette recorder to connect to the HC directly.

The SPC is also connected to the telephone lines through a cable of arbitrary length and to the house AC lines through a low-power cord and a wall-mounted power supply.

Basically the SPC communicates status information, emergency telephone numbers, and synthetic-voice-message program information to the HC on request of the HC and accepts the same kind of information from the HC. The SPC sounds a buzzer when a sensory device status change is detected. In addition to handling the complete communications protocol with the sensory devices, the SPC interfaces with the telephone network by performing automatic touch-tone telephone number dialing and by delivering synthesized voice messages on the phone lines in response to an alarm from a sensor. It also detects ringing and performs automatic answering of incoming calls by delivering phone answer messages to the caller in synthesized voice. The SPC contains a phone-guard circuit that will sound the buzzer if the phone lines are cut.

Optionally, the SPC can features a key-top to allow speed-dialing by depressing a user-defined button key on the SPC. It can also feature the ability of the user to interrogate the system for status by calling-in from an outside touch-tone phone. This is accomplished by overdialing on a standard touch-tone phone. The user first enters a system ID of 5 digits followed by a one digit command. The procedure is guided by synthetic-voice prompts from the SPC. Note that up to ten commands are possible.

The phone-interrogate feature is available on the standard product, but the user must use the Voice-Actuated Phone Command Scheme (VAPCOS) also being proposed in the TICOM products. Although VAPCOS is somewhat cumbersome for the user (each digit is entered by counting: e.g., 5= one, two, three, four, five), it does have the advantage of not requiring a touch-tone instrument, or the overdialing capability.

The HC, under control of the GROM security module program, handles the communications protocol with the SPC and provides the human interface to the user through its keyboard and its display capabilities (see Section 7.0 below).

5.0 PROTOCOL FOR COMMUNICATIONS BETWEEN SPC AND SENSORS

Once every 512 seconds, the SPC broadcasts a timing pulse consisting of an RF carrier frequency-modulated by a 1-KHz tone. The duration of this pulse is ¼-second.* The sensory devices contain a timekeeping circuit which operates continuously at a mere 6 μA circuit drain. The timekeeping circuit turns on the sensory receiver 512 seconds after the end of the last timing pulse, in anticipation of the next timing pulse. Thus, the trailing edge of the timing pulse initializes the sensor timer. This allows simplification of the timing circuitry in the sensory device. Furthermore, the receiver turn-on time in the sensory device is allowed to slip up to 82 mS with respect to the leading edge of the SPC pulse, which means 160 ppm — the stability spec, over temperature, of a watch crystal. This non-continuous receive-mode technique permits the use of a low-cost, medium-current RF receiver in the sensory device without unduly degrading battery life in a battery-operated-sensor system. (See Appendix C for battery-life calculations.) Note that since a single unaddressed pulse is broadcast, all sensory receivers must turn on at approximately the same time in order not to miss the pulse.

Upon detecting the end of a broadcast transmission, the sensory devices first re-initialize their timers. Then, if the transmission (1-KHz tone) was less than ¼-second long, it is deemed a timing pulse and nothing more is done at the sensory device. If the transmission was longer than ¼-second but shorter than ¾-second,

---

*No RF transmissions, whether from the SPC or the sensors, may exceed one second in duration and a single transmitter must not transmit more often than once every 30 seconds in order for the HCSS to operate under part 15 of the Rules and Regulations of the FCC. These restrictions do not apply to PL links.

it is deemed a system update command which causes all intrusion sensors in the system to change state. If the transmission was longer than ¾-second, it is deemed an individual sensor update command. This command means that a state change has been requested for only certain devices in the system. The sensory devices are required to wait a certain amount of time before responding by initiating a 1-second transmission (see Figure 2). That is, each device is assigned a time slot in which to respond, as shown in Figure 3(a). Note that all serial 1 devices respond first, serial 2 second, etc.

Upon receiving each device response, the SPC decodes the transmission which consists of the System ID, sensor type ID, and sensor serial ID. As shown in Figure 2, the format is an expanded version of the TICOM format (see Appendix A), the composite ID being 20 bits long instead of 16 and the bit rate being 128 bps instead of the original 110 bps in TICOM (currently TICOM is slated for 128 bps also.) The SPC verifies the sensor ID (type and serial) by determining the time slot in which the response occurred. For the case of traffic counters which are operating in the "disarmed" state, the leading 13-bit block will not constitute the system ID but will constitute the plus and minus counts accumulated since the last individual update command. The SPC will decode these 13 bits as two 6-bit counts and one count parity bit, as shown in Figure 2. A traffic counter transmission will also be initiated whenever one of the event counters at a sensor reaches the full count of 64. Note that, effectively, an individual update transmission polls the sensory devices for status (ref. Section 2.0).

As shown in Figure 3 (a), following the response time slot of one

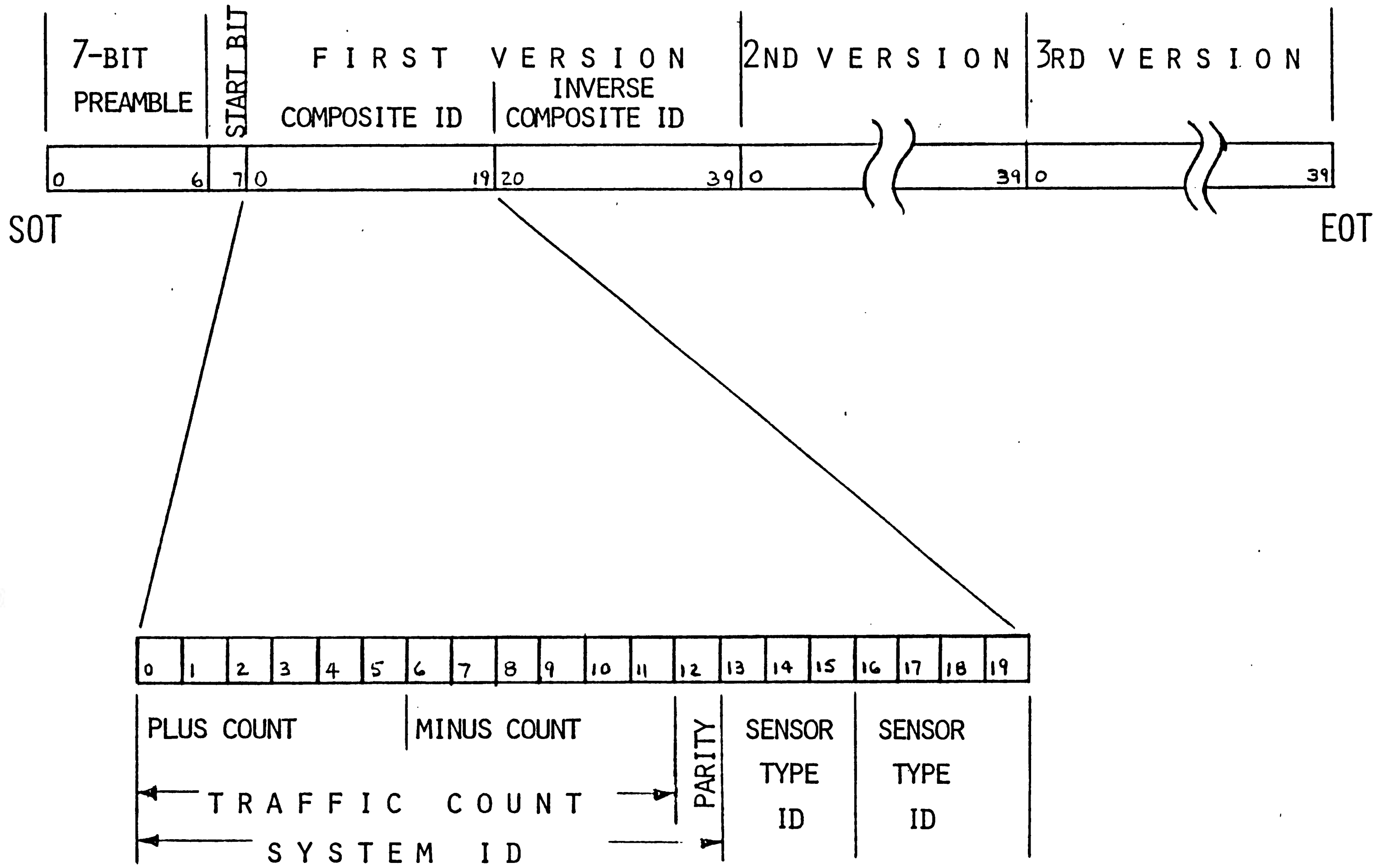
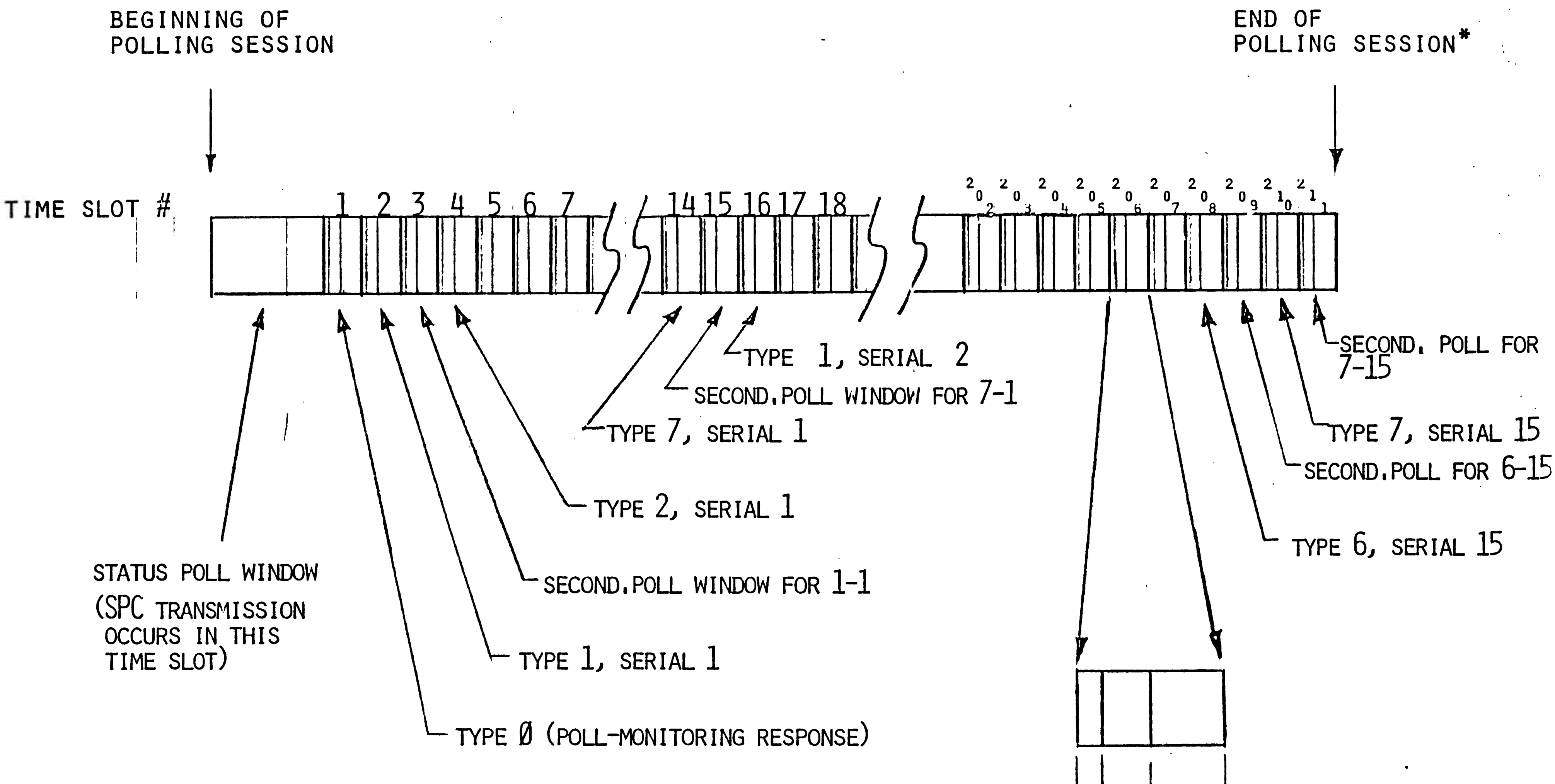
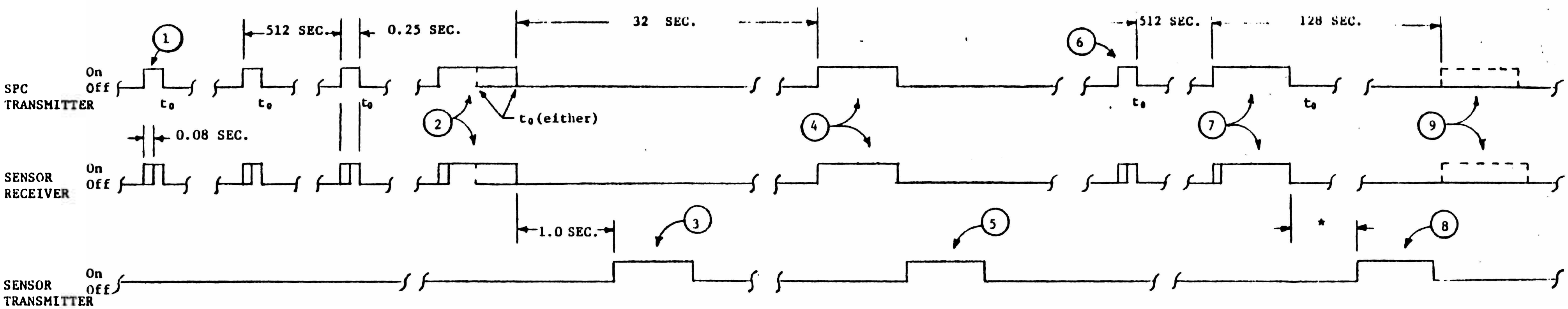


FIGURE 2 - SENSOR TRANSMISSION FORMAT



*CAN OCCUR AT THE END OF ANY ODD-NUMBERED TIME SLOT — NAMELY, THE ONE ASSOCIATED WITH THE HIGHEST SERIAL NUMBER OF THE HIGHEST TYPE NUMBER IN THE SYSTEM.

FIGURE 3a - TIME SLOT DIAGRAM FOR POLLING



(1) - SPC is continuously sending RF timing pulses of 1/4-second at 512-second intervals.

(2) - A timing pulse that is longer than 1/4-second is an update poll and constitutes a signal from the SPC that a state change has been requested. If the duration of the pulse is 1/2-second, then all intrusion devices change state (this is a system update). If the duration of the pulse is greater than 3/4-second, then the timing pulse constitutes a status poll and the devices are required to respond in their assigned time slots, one at a time, for individual device update.

(3) - This is the poll response of Device 1-1. The 1-second window proceeding it is for the poll response of the poll-monitoring device.

(4) - This is the answer from the SPC to Device 1-1. If this transmission is 1/2-second long, the state of the device is unchanged. If it is greater than 3/4-second long, the state of the device is changed.

(5) - This is the poll response of Device 2-1. The interchange between the SPC and Device 1-1 described above is thus repeated for up to 15 devices (1-1 through 7-1, 1-2 through 7-2, and 1-3). Then, another timing pulse is sent by the SPC (512 seconds after the end of the update pulse), after which another group of 15 devices (2-3 through 7-3, 1-4 through 7-4, 1-5, and 1-6) communicate with the SPC. This procedure continues for another 5 groups, of 15 devices each, or a total of 7 groups.

(6) - This is the 168th timing pulse since the last update or status poll.

(7) - This is the status poll. It is really a mandatory 1-second update poll that occurs if 24 hours (168 timing pulses) have elapsed since the last individual device update or status poll.

(8) - This is the sensory device response (like (3) and (5)) to (7) .

(9) - When either an individual update poll or a status poll is initiated, and no response from the poll-monitoring device is detected by the SPC in the corresponding time slot, the SPC will re-initiate the poll 128 seconds later. The sensor receiver will turn on in anticipation of this second try only if no transmission was detected in (7) .

* This time is between Ø and 448 seconds, depending on which device in each group is responding.

t_0 indicate the times at which the sensor timers are initialized.

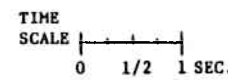


FIGURE 3 b- ACTIVITY SEQUENCE ON SENSORY CHANNEL sensor and preceding the response time slot of the next, there is a time slot for the SPC to initiate a secondary poll transmission. However, this SPC transmission is only received by the device that just transmitted a response. The duration of this secondary transmission indicates if a change in the operating state of that sensor has been requested since the last timing pulse (duration is greater than ¾-second) or not (duration is less than ¾-second). The secondary poll constitutes an acknowledge signal from the SPC that the device response was received.

Note that the SPC must wait 32 seconds after reception of the device response before it initiates the acknowledge signal in order to comply with part 15 of the FCC Rules. This results in a total of 55 minutes elapsing from the response of the first device to that of the last device in a fully-loaded system. The timers in the sensory devices cannot keep time longer than 512 seconds without accumulating a possible time error that would destroy the time-slot structure of the system. Therefore, a standard (¼-second) timing pulse must be inserted every 15 device responses in order to re-initialize the sensor timers. The sensory devices must therefore keep track of the number of timing pulses that have occurred since the individual update command in order to determine when it is time for their response transmission.

If 24 hours (168 timing pulses) have elapsed since the last individual update pulse, the SPC will automatically initiate a 1-second individual update transmission. This is the actual status poll. The entire sequence of activity in the sensory channel is illustrated in Figure 3 (b). Note that the SPC will attempt to poll for status twice before generating an alert. Also note that the protocol described so far does not apply to the PST devices. These devices are effectively manual system control devices which contain their own battery indicator. Their status is strictly user-selected at the time one of their buttons is depressed.

When a sensor is actuated and its operating state has been set (by the user) to "armed," it initiates a digital 1-second transmission to the SPC. The transmission format is shown in Figure 2. A total of 128 bits are transmitted at 128 bits per second. 32 seconds after the transmission is over, the sensory device turns on its receiver (it is normally off to conserve battery) for one second, during which time the SPC will transmit a broadcast transmission. Reception of this transmission by the sensory device constitutes an acknowledgement from the SPC that the sensory device's transmission was received and instructs the sensory device to turn off its receiver. If the acknowledge transmission is longer than ¾-second, the device is disarmed. If the acknowledge transmission is shorter than ¾-second, the sensor is re-armed but will not be susceptible to activation until 128 seconds have elapsed from the time the acknowledge signal was received. If an acknowledge signal is not received in the prescribed one-second window, the sensory device will continue to send 1-second transmissions at 32-second intervals until an acknowledge signal is received from the SPC or a maximum of five 1-second transmissions are sent, whichever comes first.

In addition to the sensory devices mentioned thus far, a poll-monitoring transceiver device will also be offered, which plugs into a power outlet and is battery-backed. This device has a timer that will turn on its receiver for the SPC timing pulse and checks the tone duration just as the sensory devices do. The first response time slot following the status poll is assigned to this device. If the SPC does not receive a poll response from this device in that time slot, it will re-initiate the status poll after a delay of 128 seconds. If the SPC still does not receive a poll response from the poll-monitoring device, a buzzer is sounded continuously at the SPC. If the poll-monitoring device fails to detect a status poll from the SPC within the prescribed 130-second window, it will sound its own buzzer alert.

A test button is provided on each sensory transceiver. Depressing this button results in sensor activation, which can be used to manually test the system. Depressing the test button on a sensory devices arms that devices and after 32 seconds also causes that receiver to be turned on for 2 seconds, off for 25.6 minutes, and on again for 2 seconds following the transmission. The sensory receiver thus looks for the acknowledge signal from the SPC within 34 seconds after the transmission. If it does not find it, it looks again 25.6 minutes later. Note that depressing the test button will cause an alarm condition at the SPC. If the user does not wish the SPC to autodial, he must disconnect the SPC from the phone lines prior to depressing the test button. After using this test feature, the user must depress the "alarm reset" button on the SPC. Depressing the test button on the poll-monitoring device causes a special type-number ID (binary ØØØ) to be transmitted to the SPC which results in the SPC's delaying the corresponding acknowledge transmission for 25.6 minutes. When that acknowledge transmission is finally broadcast, it constitutes the first timing pulse, which will repeat once every 512 seconds from then on. Thus, by first depressing the test button on the poll-monitoring device and then proceeding to depress the test button on all the sensory devices one at a time, the user can initiate the system timing cycle. Note that the user has approximately half an hour (25 minutes) from the time the poll-monitoring test button is depressed in which to depress the test buttons on all sensory devices that are desired in the system. This identical initialization must be performed whenever a device is added to the system or a battery change is made on any existing device.

The protocol with the PST is the same as with a sensor that has been triggered. There are six fuctions that can be associated with a PST transmission:

1. System interrogation.
2. System activation.
3. System deactivation.
4. Personal injury.
5. Personal danger.
6. Test.

The above functions are identified by type 7, serial numbers 6 through 11, respectively, with serial numbers 12 through 15 treated as spares for future expandability. The first function will receive an acknowledge transmission in response to a PST signal, which will indicate by its duration whether an intrusion alarm has occurred (duration less than ¾-second) or not (duration greater than ¾-second). All other functions receive an acknowledge signal less than ¾-second long. Thus, when one of the six buttons on the PST is pressed, the device initiates a 1-second transmission, after which it turns on its receiver for a maximum of two seconds.

Note that this entire communications protocol will support a maximum system of seven sensor types, fifteen devices of each type, for a total of 105 sensory devices plus the poll-monitoring device.

Shown in Figure 4 is a frequency plan which supports the above protocol. Figure 4 (a) is for an RF system and Figure 4 (b) is for a PL system. Note that the RF system can accomodate 100 system channels, while the PL system can only accomodate 10 system channels. Also, each RF system channel consists of a pair of simplex frequency channels, each 100 KHz wide and separated from each other by 455 KHz, with one frequency ("A") assigned to SPC transmissions and the other ("B") to sensory transmissions. By contrast, each PL system channel consists of a single frequency channel on which both the SPC and the sensory devices must transmit in half-duplex mode. This lack of channel capacity is a marked disadvantage of PL systems. In the face of this capacity limitation, the fact that it is desired to use a PL link in the Home Computer Control System (for automatic computer controls around the house), being currently defined, renders PL quite unsuitable for security system implementation.

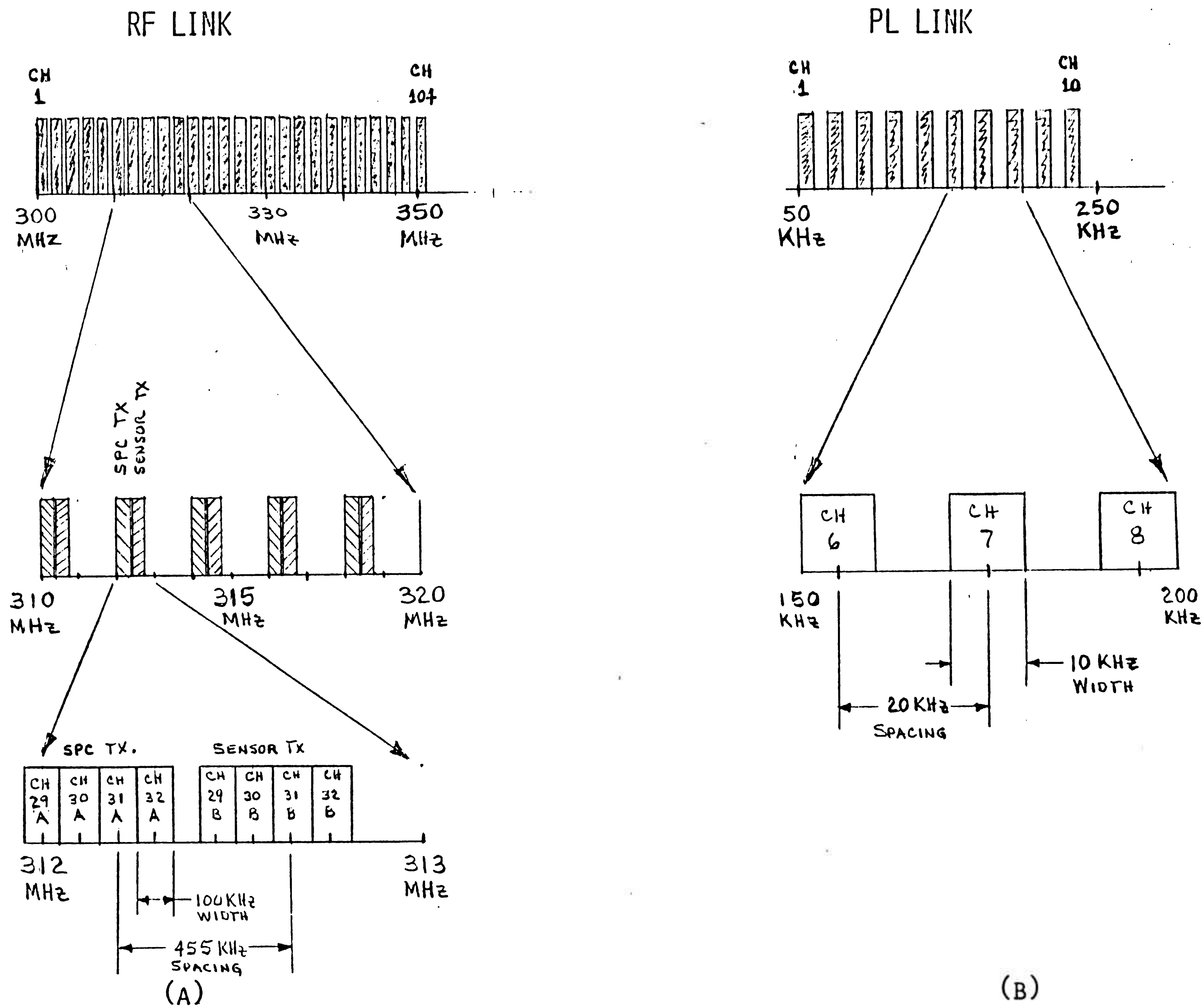


FIGURE 4 - FREQUENCY PLAN

6.0 PROTOCOL FOR COMMUNICATIONS BETWEEN HC AND SPC

All communications between the HC and the SPC must be initiated by the HC. Furthermore, the HC does not initiate any SPC communications automatically. It will only initiate communication with the SPC in response to a user command under GROM-security-module program control. This relieves the HC of having to perform any background tasks for security.

As mentioned previously (see Section 4.0), there are six reasons for the HC to communicate with the SPC:

1. A status inquiry is being made at the console,
2. An emergency-phone-number update is being made at the console,
3. A street-address update is being made at the console,
4. A phone-answer-message update is being made at the console,
5. A traffic counter update is being made at the console, or
6. A system timer update is being made at the console.

Note that these correspond to options 1 through 6, respectively, of the security option prompt (see Section 7.0 below and Figure 8).

The SPC accepts the same block-oriented transmission format used by the HC to communicate with the cassette, as shown in Figure 5. Note that the HC outputs the data in the 1024-bit block as 128 8-bit words. The SPC looks only at the least-significant (i.e., leading) 4-bits in each of these words. Therefore, to the SPC, the 1024-bit block looks like 128 4-bit words. This is done to allow the 4-bit microprocessor in the SPC to communicate with the same HC Device Service Routine (DSR) that is used to talk to the cassette recorder. Note that the same bi-phase mark coding of

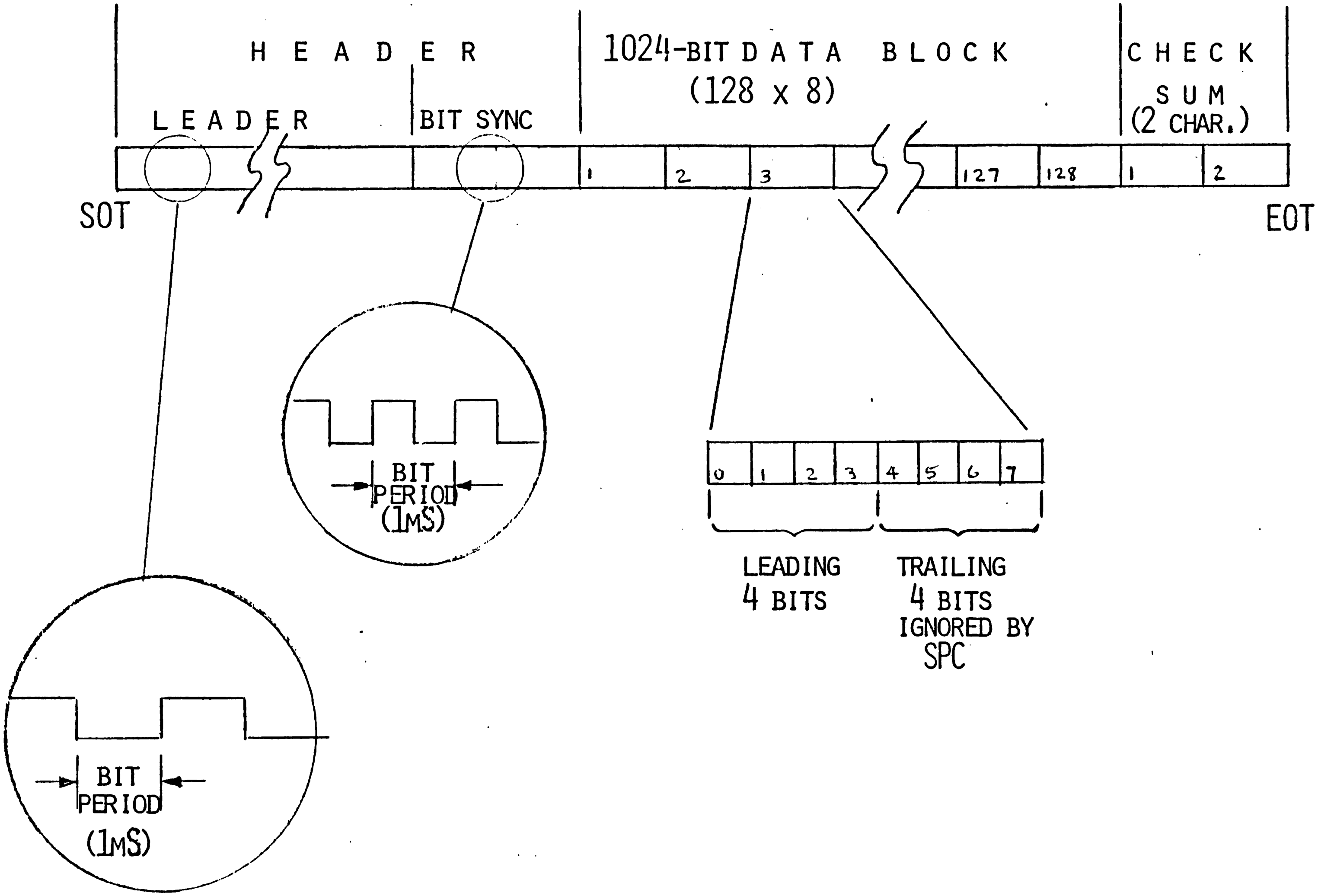


FIGURE 5 - HC- SPC TRANSMISSION BLOCK FORMAT

each bit is used for SPC communications as for cassette communications.

When the user selects any one of the options 1 through 6 in response to the security option prompt (see Figure 8), a command is issued by the HC to the SPC asking for data that is stored in the SPC memory. This command is implemented by transmitting the option (command) number (1-6) as the four leading bits of the 1024-bit data block, with the remaining bits set to zero. The data block coming back from the SPC will have different meanings, depending on the command. Figure 6 shows the six commands and their associated SPC response formats.

All responses can be accommodated in a single block transmission, except that for future expandability it is desirable to signal the SPC for a second block transmission in response to command 2 by deactivating and activating the cassette motor control lines after the first command-2 response transmission has been received by the HC. For the initial system, that second block will be all zeroes.

Once the SPC has responded to a command, it awaits the update transmission from the HC which contains any new information. Since the SPC knows what command is being serviced, the update transmission from the HC need not identify the option number. The formats of the data blocks in the update transmissions are shown in Figure 7. If the leading 4 bits of the first 8-bit character in an update transmission are all Ø, then the SPC will assume that the whole data block is all Ø's which implies that no new information has

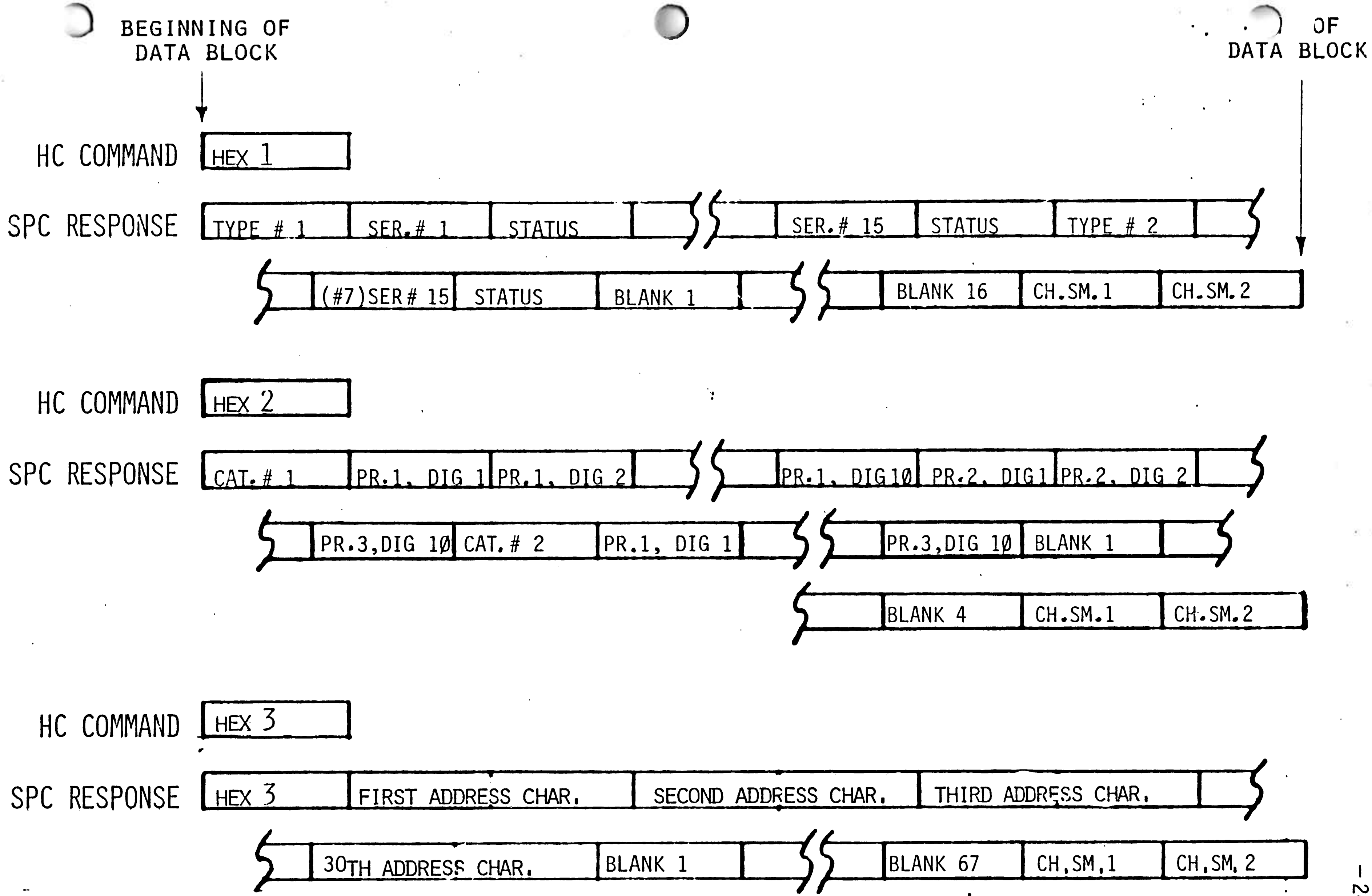


FIGURE 6 - HC-SPC RESPONSE DATA BLOCK FORMAT

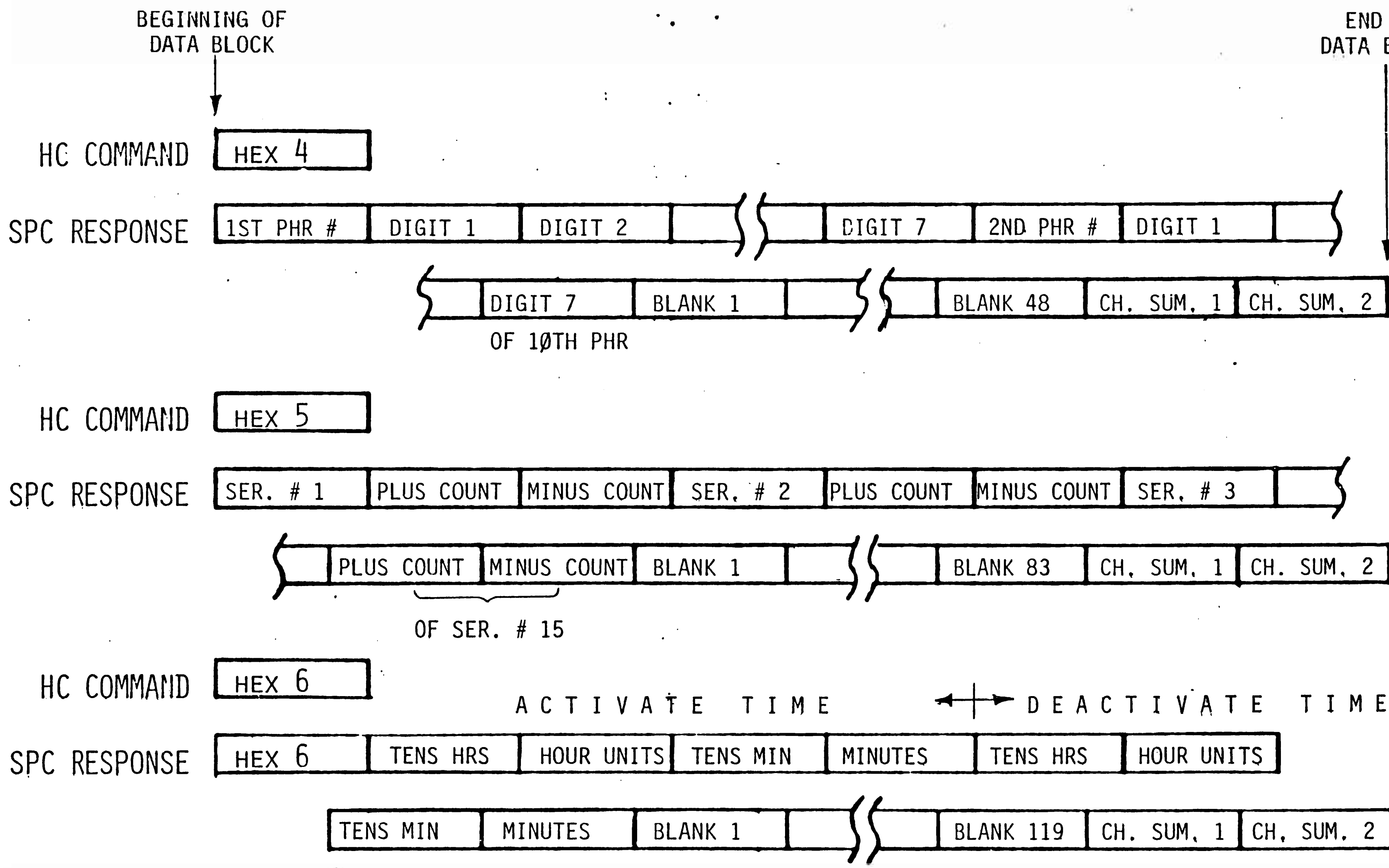


FIGURE 6 - CONTINUED

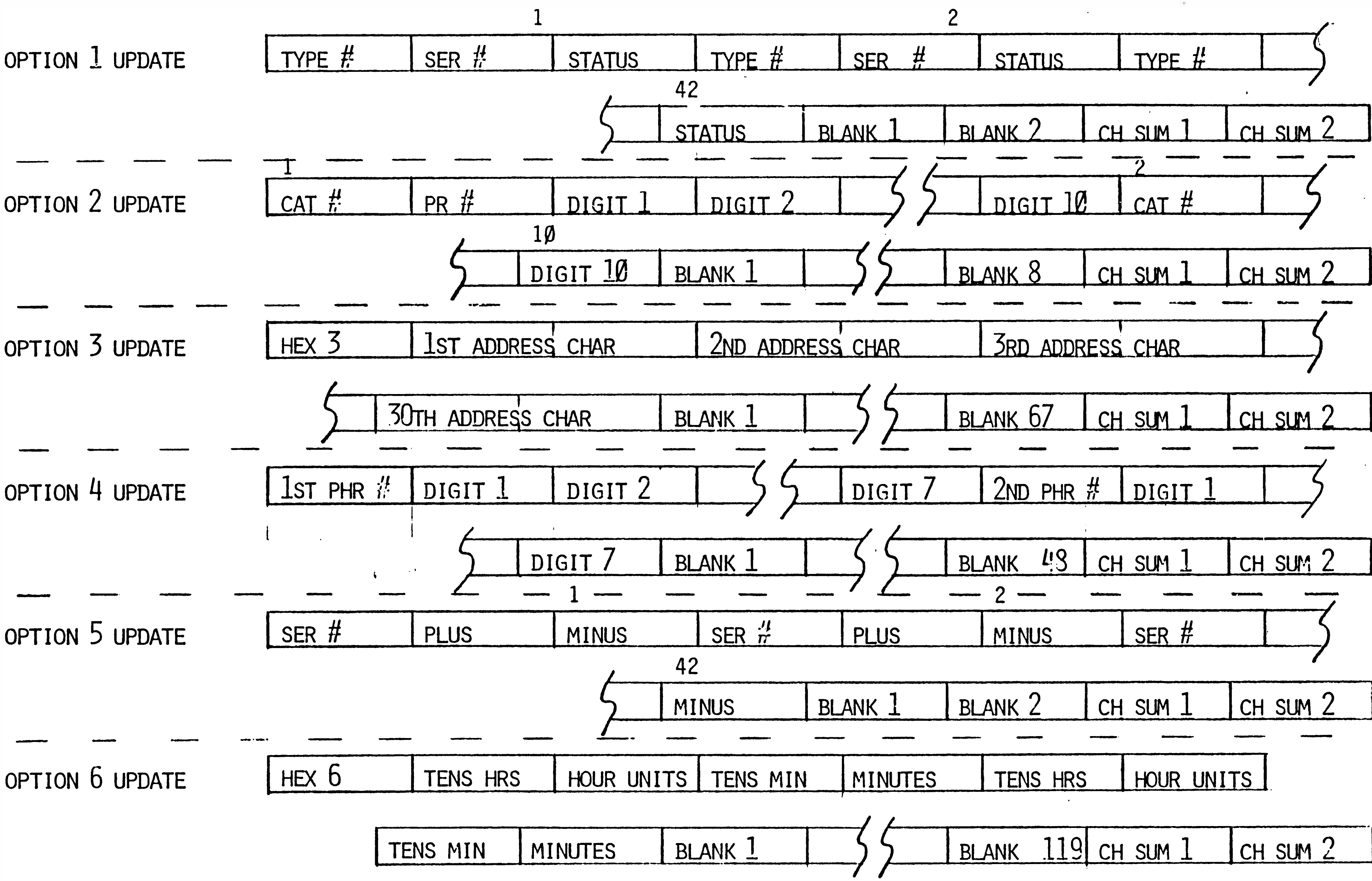


FIGURE 7 - HC-SPC UPDATE TRANSMISSION DATA BLOCK FORMAT

been entered at the console. Only for this reason is the option number identified in the update transmissions for options 3 and 6.

Note that this communications protocol will support a system with a maximum of eight sensor types, fifteen devices of each type, for a total of 120 sensory devices; eight alarm categories, three phone numbers for each, for a total of 24 telephone numbers; 64 characters in a street address; 128 phone answer phrases; 40 traffic counters; and 15 activate-deactivate time pairs.

7.0 USER SCENARIO AT THE CONSOLE

To set-up, update, or review the information that the computer stores for him (either in the SPC or in cassette tape) regarding his security system, the user inserts the GROM security module in the console and flips the selection switch on the SPC to the "SEC" position (see Figure 1). After the user follows the standard HC procedure for reading and executing a GROM module program, the security option prompt appears on the display screen asking which option he wants and giving him a menu of alternatives to choose from (see Figure 8).

If the user selects option 1, the computer will display the status of each sensory device on last poll as either triggered, armed, disarmed, or dead, and list these by device type (smoke detectors, magnetic switches, motion detectors, traffic counters, PSTs, etc.) and serial number (see Figure 9). At the bottom of the display, a prompt will appear asking for the type and serial number of the device to be updated as well as its new operating state (armed or disarmed). Upon entry of the requested information, the same prompt will continue to re-appear so that any number of devices (up to 42) can have their operating states updated. Upon entry of "Ø" for the type number, the security option prompt appears on the display again as shown in Figure 8 and the new information will have been communicated to the SPC.

If the user selects option 2, the computer displays the phone numbers perviously stored by alarm category (fire, intrusion, personal emergency, general emergency) with Ø's appearing if no number had been entered. Within each category, the numbers are

TEXAS INSTRUMENTS INCORPORATED

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
THE FOLLOWING OPTIONS ARE
AVAILABLE:

Φ-NONE, END OF SESSION

1-STATUS UPDATE

2-PHONE NO. UPDATE

3-STREET ADDRESS UPDATE

4-PHONE ANSWER MESSAGE UPDATE

5-TRAFFIC COUNTER UPDATE

6-SYSTEM TIMER UPDATE

7-TOPOLOGY UPDATE

8-FLOOR-PLAN GRAPHICS


ENTER OPTION DESIRED (Φ-8): _
```

VIDEO/COPY:

AUDIO/TONES:

TI Strictly Private

FIGURE 8 - SECURITY OPTION PROMPT

TEXAS INSTRUMENTS

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
SYSTEM INTRUSION STATUS: ARMED

     ***SENSOR STATUS***

 TYPE 1- SMOKE DETECTORS
         1-ARMED     2-ARMED
         3-DEAD!!!   4-ARMED

 TYPE 2- MOTION DETECTORS
         1-ARMED     2-DEAD!!!
         3-DISARMED  4-ARMED
         5-ARMED

 TYPE 4- MAGNETIC SWITCHES
         1-DISARMED  2-DISARMED
         3-DISARMED  4-ARMED

 TYPE 7- S/N 6-15, MAG.SW.
         6-ARMED     7-ARMED


ENTER TYPE AND S/N TO BE UPDA-
TED (ARM=2, DISARM=3):_
```

VIDEO/COPY: ENTERING "NEXT" AS THE TYPE NO. WILL CAUSE THE DISPLAY ABOVE THE PROMPT TO SCROLL UPWARDS ONE LINE. IN THIS WAY, OTHER DEVICES CAN BE VIEWED.

AUDIO/TONES:

FIGURE 9 - STATUS UPDATE PROMPT

listed in order of priority, which simply means that this is the order in which the SPC will cycle dial until it gets an answer. A prompt will appear at the bottom of the display asking for the category and priority number to be updated (see Figure 10). After the user enters the category and priority numbers, a phone number is requested through another prompt, which appears in place of the previous one. After the phone number is entered, the category prompt is again displayed, and so on until a Ø is entered for the category number, after which the security option prompt appears on the display again as shown in Figure 8.

If the user selects option 3, the computer will display a list of abbreviations to be used in entering the street address (see Figure 11) and will prompt for the address at the bottom of the display (a maximum of 30 characters is allowed). Upon entry of the address, the security option prompt appears on the display again as shown in Figure 8.

If the user selects option 4, the computer will display a list of phone-answer messages available, each along side its numeric code, and ask through a prompt for the code number(s) in the order in which they should be spoken (see Figure 12) to the phone caller. A "Ø" code causes the security option prompt to appear on the display once more.

If the user selects option 5, the computer will list the traffic count devices by serial number and give plus counts and minus counts of each (see Figure 13). A prompt will appear at the bottom of the display asking for the device serial number to be updated and its

```
EMERGENCY-PHONE-NUMBER UPDATE
     *  *  *  *  *  *  *  *  *  *

CATEGORY 1- FIRE
             1-  747-3731
             2-  1-797-6ØØ5
             3-  312-591-4267

CATEGORY 2- INTRUSION
             1-  579-6111
             2-  747-3731
             3-  1-324-41ØØ

CATEGORY 3- PERSONAL EMERGENCY
             1-  374-3131
             2-  ØØØ-ØØØØ
             3-  ØØØ-ØØØØ

CATEGORY 4- GENERAL (USER-DEF)
             1-  ØØØ-ØØØØ
             2-  ØØØ-ØØØØ
             3-  ØØØ-ØØØØ
ENTER CAT. &
PIRORITY NO. TO BE UPDTED: _
```

VIDEO/COPY: ENTERING "NEXT" AS THE CATEGORY NO. WILL CAUSE THE DISPLAY ABOVE THE PROMPT TO SCROLL UPWARDS ONE LINE. IN THIS WAY, OTHER CATEGORIES AND THEIR NUMBERS MAY BE LISTED.

AUDIO/TONES:

FIGURE 10 - PHONE NUMBER UPDATE PROMPT

TEXAS INSTRUMENTS

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
*** STREET ADDRESS UPDATE ***

ABBREVIATIONS:
AV - AVENUE          PL - PLACE
AP - APARTMENT       RD - ROAD
BO - BOULEVARD       RT - ROUTE
CR - CIRCLE          S -  SOUTH
DR - DRIVE           SE - SOUTHEAST
E -  EAST            ST - STREET
LN - LANE            SW - SOUTHWEST
MN - MANOR           TR - TERRACE
N -  NORTH           W -  WEST
NE - NORTHEAST
NW - NORTHWEST



CURRENT ADDRESS IN MEMORY:
11630-N-MOCKINGBIRD-LN--AP-234

ENTER NEW ADDRESS:
_
```

VIDEO/COPY:

AUDIO/TONES:

TI Strictly Private

FIGURE 11 - STREET ADDRESS UPDATE PROMPT

TEXAS INSTRUMENTS INCORPORATED

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
*PHONE ANSWER MESSAGE UPDATE*

CODE #-          MESSAGE
1-WE ARE OUT MOMENTARILY
2-WE MAY BE REACHED @ XXX-XXXX
3-PLEASE CALL BACK IN XX MIN.
4-PLEASE CALL BACK AT XX:XX
5-PLEASE CALL BACK AFTER XX:XX

6-WE ARE NOT TAKING ANY CALLS,
  PLEASE DO NOT DISTURB.
7-AT THE SOUND OF THE TONE
  PLEASE LEAVE YOUR MESSAGE
8-PLEASE CALL BACK LATER BUT
  NOT AFTER XX:XX.
9-WARNING! PREMISES HEAVILY
  GUARDED!
10-WARNING! THESE PREMISES ARE
  UNDER COMPUTER SURVEILLANCE!
ENTER 1ST PHRASE CODE # DATA:_
```

VIDEO/COPY: HOURS MUST BE 1 THRU 12; MINUTES MUST BE 15, 30, OR 45. WHEN THE [ENTER] KEY IS DEPRESSED AFTER ABOVE IS DISPLAYED, DISPLAY WILL SCROLL UPWARDS ONE LINE BUMPING THE TOP TITLE LINE OFF THE SCREEN. AFTER ENTERING CODE NO. AND NUMERIC DATA, IF ANY, THE COMPUTER WILL PROMPT FOR THE SECOND PHRASE AND SO ON.

AUDIO/TONES:

TI Strictly Private

FIGURE 12 - ANSWER MESSAGE UPDATE PROMPT

TEXAS INSTRUMENTS
INCORPORATED

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
*** TRAFFIC COUNTER UPDATE ***

 1- +100,-99     2- +97,-98

 3- +Ø,-Ø        4- +Ø,-Ø

 5- +Ø,-Ø        6- +Ø,-Ø

 7- +Ø,-Ø        8- +Ø,-Ø

 9- +Ø,-Ø       1Ø- +Ø,-Ø

11- +Ø,-Ø       12- +Ø,-Ø

13- +Ø,-Ø       14- +Ø,-Ø

15- +Ø,-Ø


ENTER S/N & + & - COUNTS:

_
```

VIDEO/COPY:

AUDIO/TONES:

TI Strictly Private

FIGURE 13 - TRAFFIC COUNTER UPDATE PROMPT

new plus count and minus count. This gives the user the ability to indicate the number of people in a room, for example, by indicating a certain "plus" count on the device(s) that is(are) located at the entrance(s) of the room. This prompt will continue to appear so that any number of traffic devices can be updated. A "Ø" entry for the device serial number will cause the security option prompt to appear on the display again.

If the user selects option 6, the computer will display the stored activate and deactivate times of day and will ask if an update is desired, as shown in Figure 14. If the answer is "yes," the computer will prompt for the new activate time and then prompt for the new deactivate time (both in 24-hour, military-type format). Upon entry of the latter, or if the user answers by entering "no" to the time update question, the computer will display the security option prompt again.

Option 6 thus allows the user to specify the time of day (to within 512 seconds) at which the intrusion sensors will be automatically armed as well as the time of day at which they will automatically be disarmed each day. If the user wishes to arm these devices because he is going out, he simply enters the current time of day plus whatever delay he wishes to insure himself before the sensors are activated. A "Ø" deactivate time suppresses any automatic deactivation. He can also use his PST to activate or deactivate at random without disturbing the automatic time settings and without getting the HC involved. Option 6 also sets the time on the SPC 24-hour clock.

If the user selects option 7, the computer will ask if there is

TEXAS INSTRUMENTS

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
   *** SYSTEM TIMER UPDATE ***
      ACTIVATE TIME IS 23:ØØ
    DEACTIVATE TIME IS Ø6:ØØ

DO YOU WISH TO CHANGE TIME?YES
ENTER ACTIVATE TIME: 23,ØØ
ENTER DEACTIVATE TIME: _
```

VIDEO/COPY:

AUDIO/TONES:

TI Strictly Private

FIGURE 14 - SYSTEM TIMER UPDATE PROMPT

topology data on the security topology cassette tape. The user must flip the selection switch on the SPC to the "CAS" position (see Figure 1) at this point. If system topology data has been previously stored on tape, the computer will proceed to read the tape (which must be in place in the recorder) and the user should follow the standard HC procedure for loading data from the cassette tape prior to giving a "yes" answer to the prompt. If no such data has been stored, the user will simply enter "no." The computer will then display a list of the sensory devices by type and serial number, giving the location of each as previously stored (see Figure 15). If the answer entered above was "no," only the title headings will be displayed. At the bottom of the display, the computer will prompt for the type and serial numbers of the device to be updated. Upon entry of the type and serial numbers, another prompt will appear asking for a description of the new location as a 25-character string. After the location is entered, the type and serial number prompt re-appears, and so on until a "Ø" is entered for the type number, prior to which the user must follow the HC procedure for writing data on tape and the topology data will be written on tape. The security option prompt will then appear on the display again.

If the user selects option 8, the computer will ask if there is floor-plan data on the security floor-plan cassette tape. The user must flip the selection switch on the SPC to the "CAS" position (see Figure 1) at this time. If floor-plan data has been previously stored on tape, the computer will proceed to read the tape (which must be in place in the recorder) and the user should follow the

TEXAS INSTRUMENTS INCORPORATED

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS

```
   *** TOPOLOGY UPDATE ***

SENSOR:LOCATION
1-Ø1:KITCHEN
1-Ø2:MASTER BEDROOM
1-Ø3:FIREPLACE

2-Ø1:GARAGE
2-Ø2:FOYER
2-Ø3:PATIO DOOR
2-Ø4:HALLWAY TO BEDROOMS

3-Ø1:FRONT DOOR
3-Ø2:MASTER BEDROOM
3-Ø3:UTILITY HALLWAY
3-Ø4:INTERIOR GARAGE DOOR


ENTER TYPE & S/N TO BE UPDATED
2,5
ENTER LOCATION (26 CHAR.):

_
```

VIDEO/COPY: ENTERING "NEXT" AS THE TYPE NO. WILL CAUSE THE DISPLAY ABOVE THE PROMPTS TO SCROLL UPWARDS ONE LINE.

AUDIO/TONES:

TI Strictly Private

FIGURE 15 - TOPOLOGY UPDATE PROMPT

standard HC procedure for loading data from cassette tape prior to giving a "yes" answer. If a "yes" is entered, the computer will read the tape and display a floor-plan of the protected premises, showing the physical location of the sensory devices identified by type and serial number. A prompt will appear at the bottom of the display screen requesting type and serial number of the device to be updated, along with its new location in (x,y) coordinates (see Figure 16). A "Ø" in response to the type number will cause the new floor-plan data to be written on tape and the security option prompt will appear on the display again.

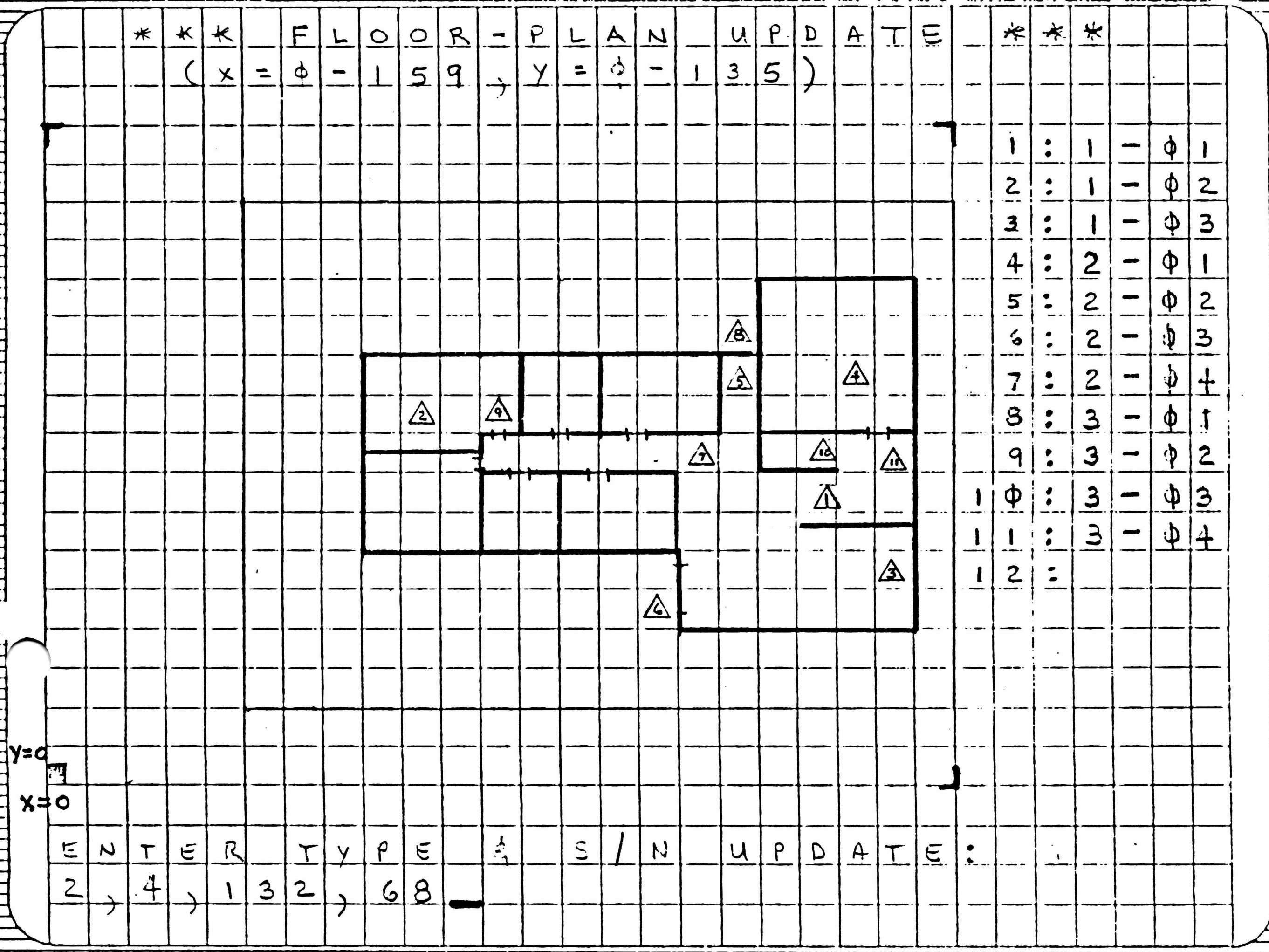
If the answer to the option-8 prompt is a "no," then the floor-plan itself must be generated. This is done by superimposing a graduated grid transparency, supplied with the HCSS owner's manual, over an actual floor-plan of the home (see Figure 17). The floor-plan is entered into the computer by inputting, through the keyboard, the (x,y)-coordinates of each line point of the floor-plan in ascending horizontal (x) and then vertical (y) order. Once the floor-plan has been entered for the first time, it need not be entered again (unless the home changes). After the floor-plan has been entered, the computer will display its graphic version of the floor-plan on the screen. At the bottom of the display, a prompt will appear asking for the sensory device type and serial number to be updated and for its location in x and y. A "Ø" in response to the type number writes the floor-plan data (this includes the device placement) on tape and returns the security option prompt to the display.

Finally, if the user selects option Ø, the session with the GROM

TEXAS INSTRUMENTS

HOME COMPUTER "GROM" DEVELOPMENT

PROJECT: HCSS



VIDEO/COPY:

UDIO/TONES:

TI Strictly Private

FIGURE 16 - FLOOR -PLAN UPDATE PROMPT

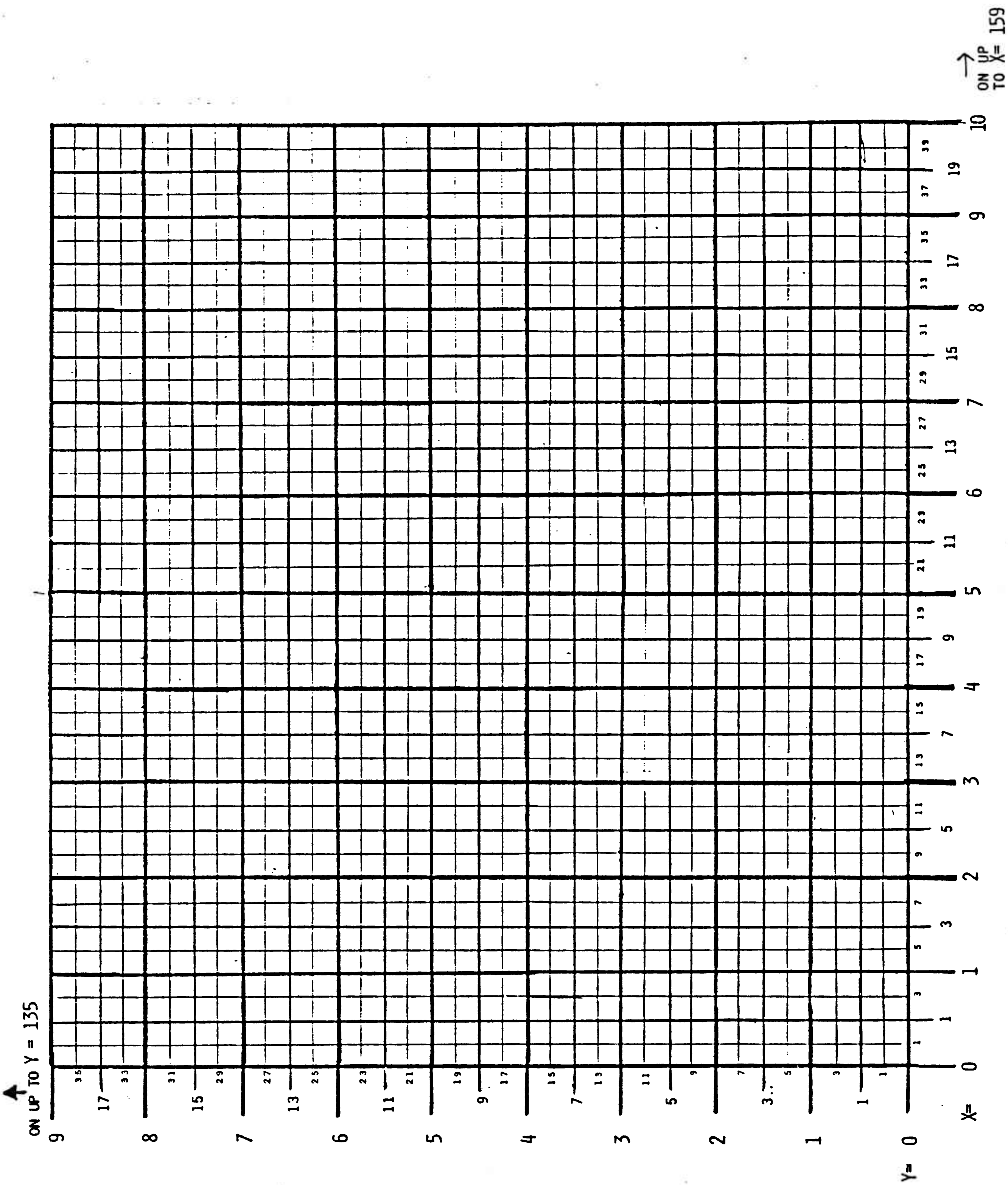


FIGURE 17 - FLOOR-PLAN GRID

security module is ended.

It should be noted that the floor-plan graphics feature is non-essential to the operations and convenience offered by the HCSS.

8.0 SYSTEM COMPONENTS

The Security Peripherals Controller (SPC):

This device interfaces the security channel (RF or PL) to the HC. It also interfaces to the telephone network. A block diagram of the SPC is given in Figure 18. The dual µP (TMS-1100 NLL) approach is recommended because it isolates the security channel from any HC command activity. The security µP (μP_1) contains the same software as the TICOM security controller µP. The other µP (μP_2) is used as a communications controller for the HC-SPC link. Note that by using the off-board RAM, both processors can share access to the same memory. A watch chip and crystal are also included to provide the necessary timing functions. See Sections 2.0 and 4.0 for further descriptions of the SPC functions. Price : $300.00.

The Sensory Transceivers:

These devices consist of an FM transmitter, FM receiver, and timekeeping circuit. A block diagram of a sensory transceiver is given in Figure 19. Both the transmitter and the receiver operate at very low duty cycles which permits battery operation. The timekeeping circuit is implemented by a 32.768 KHz watch-crystal oscillator driving a digital divider chain. A maximum current drain of 6 µA can be tolerated on the timekeeping circuit. Also, part of the transceiver is an encoder circuit and an ID code module that can be plugged in and out. The encoder circuit can be implemented with a TMS-1000C or with a custom IC, the choice being primarily one of economics; in either case, it will be the same as that used in TICOM.

The battery used to power the transceiver will be 3 primary Alkaline

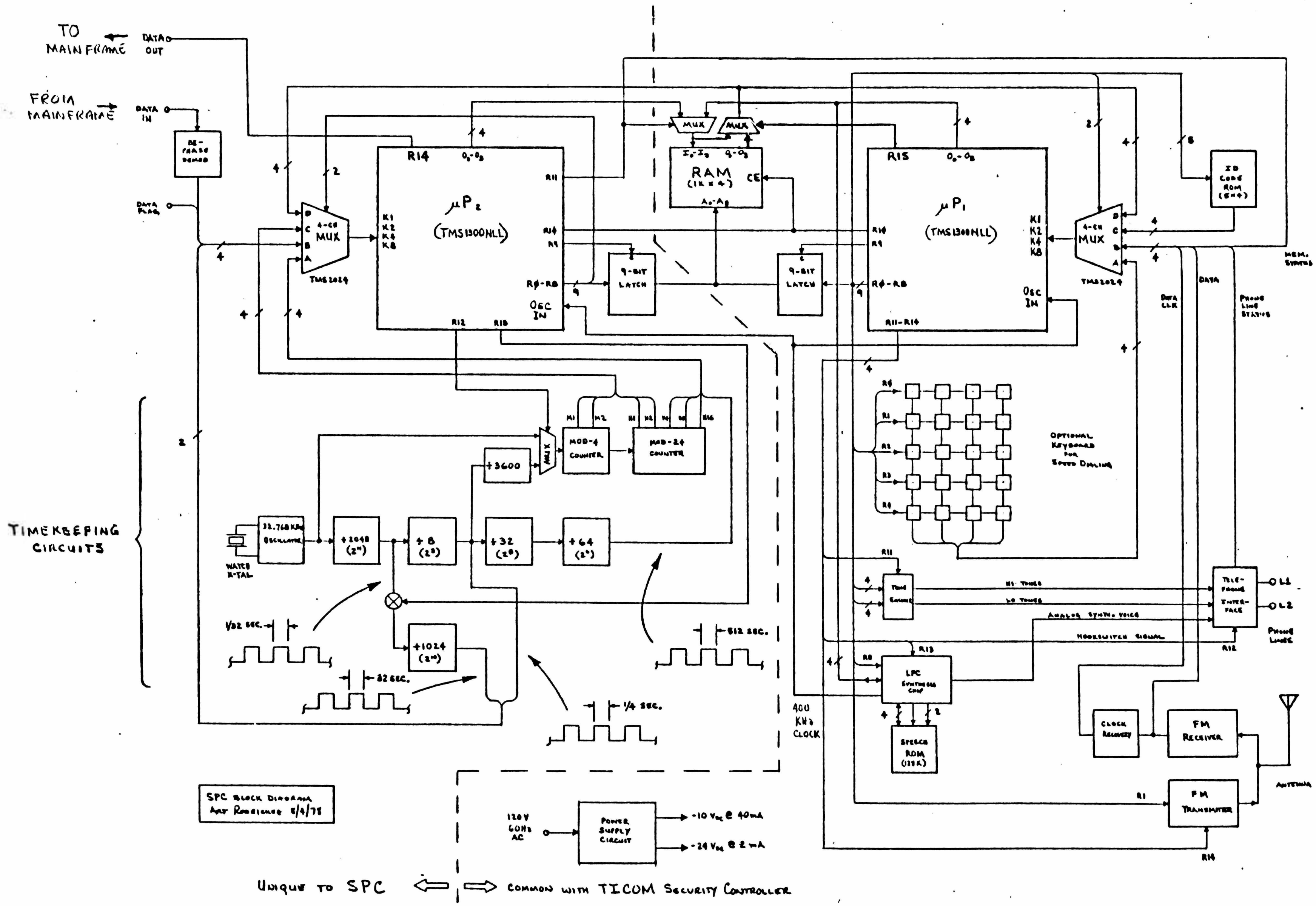


FIGURE 18 - SPC BLOCK DIAGRAM

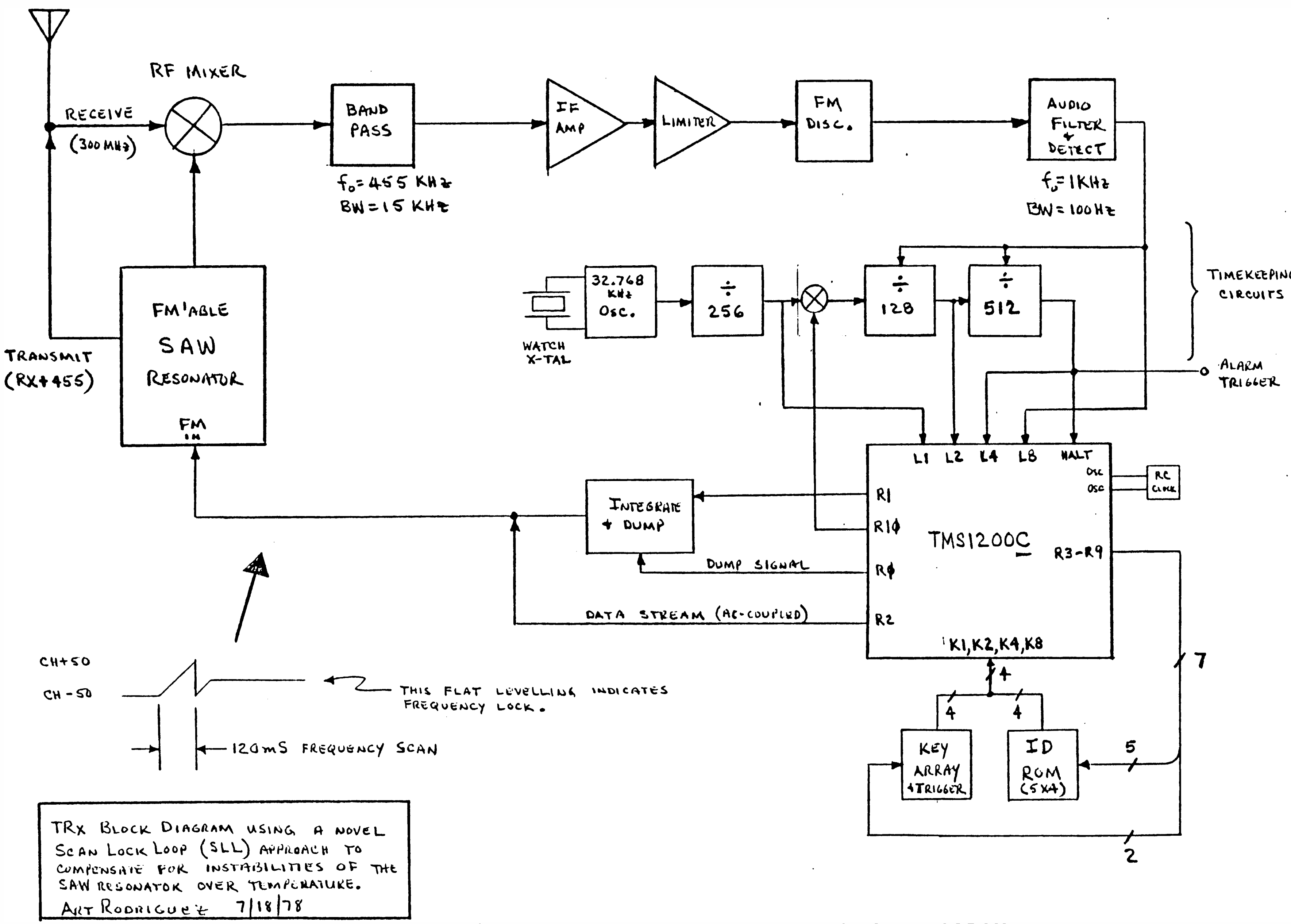


FIGURE 19 - SENSORY TRANSCEIVER BLOCK DIAGRAM

cells for a nominal operating voltage of 4.5v at 400 mAh.

The Smoke Detector: Type Number =1, S/N=1-15
This will be a custom TI design which combines the ionization-chamber principle with the photoelectric scheme to yield the highest reliability detector possible. This device is being designed for the TICOM security system and will also be used with the HCSS. Price : $75.00 with transceiver.

The Motion Detector: Type Number =2, S/N =1-15
This device will operate by sensing changes (of a minimum rate) in the ambient infrared (IR) energy level, the priciple being that human beings (and animals) constitute a source of (thermal) infrared radiation. One big advantage of these detectors is their low power consumption (0.25 mA). The radiation is optically concentrated onto an IR detector which converts it to a minute electrical current which is then amplified and compared with previous levels (see Figure 20). The optical concentration is accomplished through lense. By providing three adjustable lens, the coverage area can be made to accomodate different requirements, as shown in Figure 21. How far away the motion can occur from the detector and still be detected is determined by the sensitivity setting of the device.

Since pets are a smaller IR source than adult human beings, some resistance to pet falsing can be achieved at the expense of coverage distance by lowering the sensitivity setting on the detector. Pet falsing can also be minimized by aiming the lense so that no Ir body shorter than, say, 3 feet off the ground will set off the

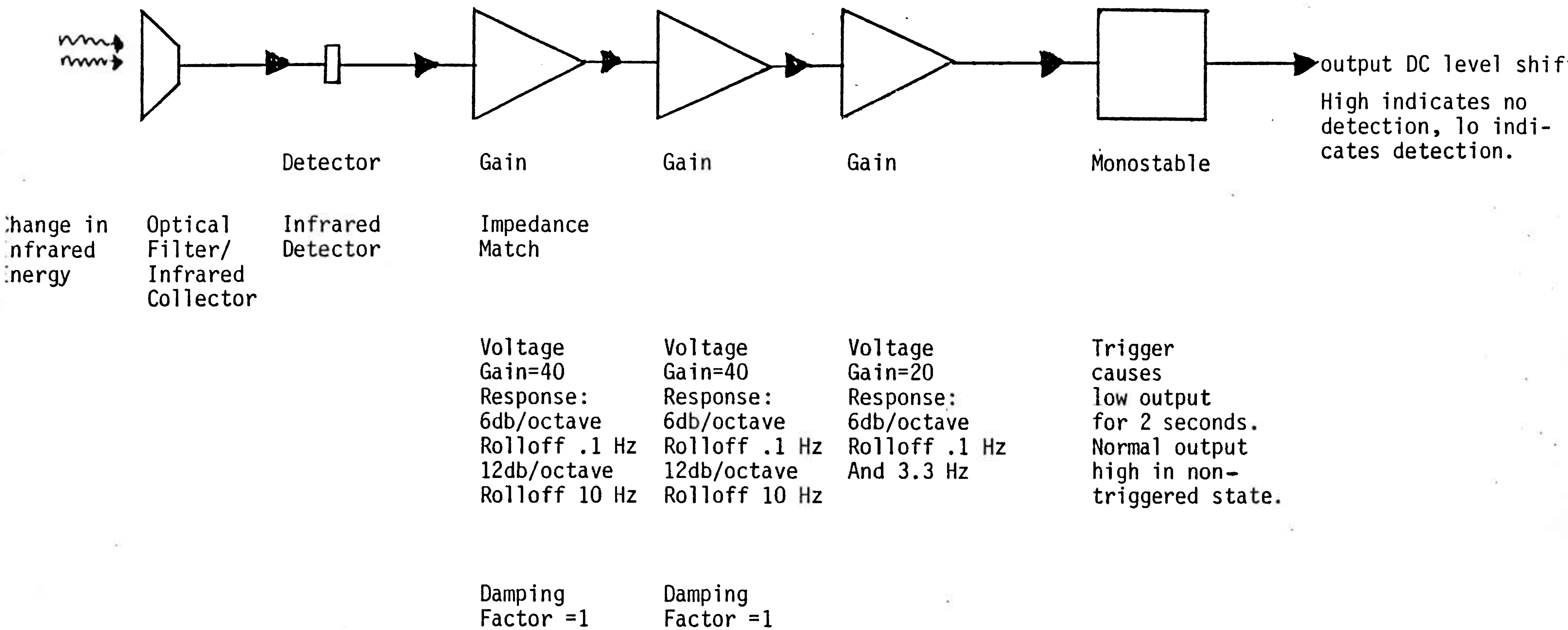


FIGURE 20 - IR MOTION DETECTOR BLOCK DIAGRAM

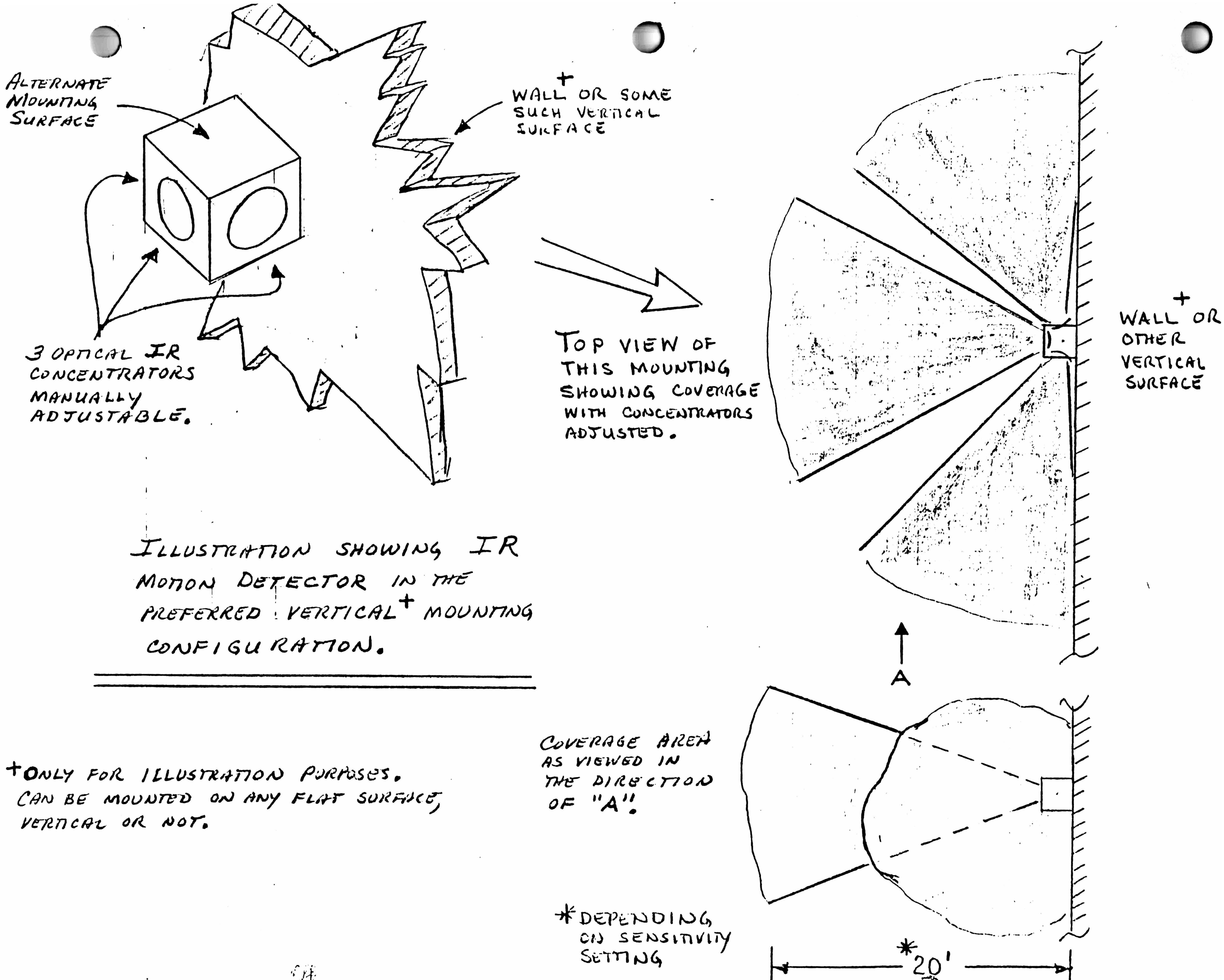


FIGURE 21 - IR MOTION DETECTOR COVERAGE AREAS

detector.

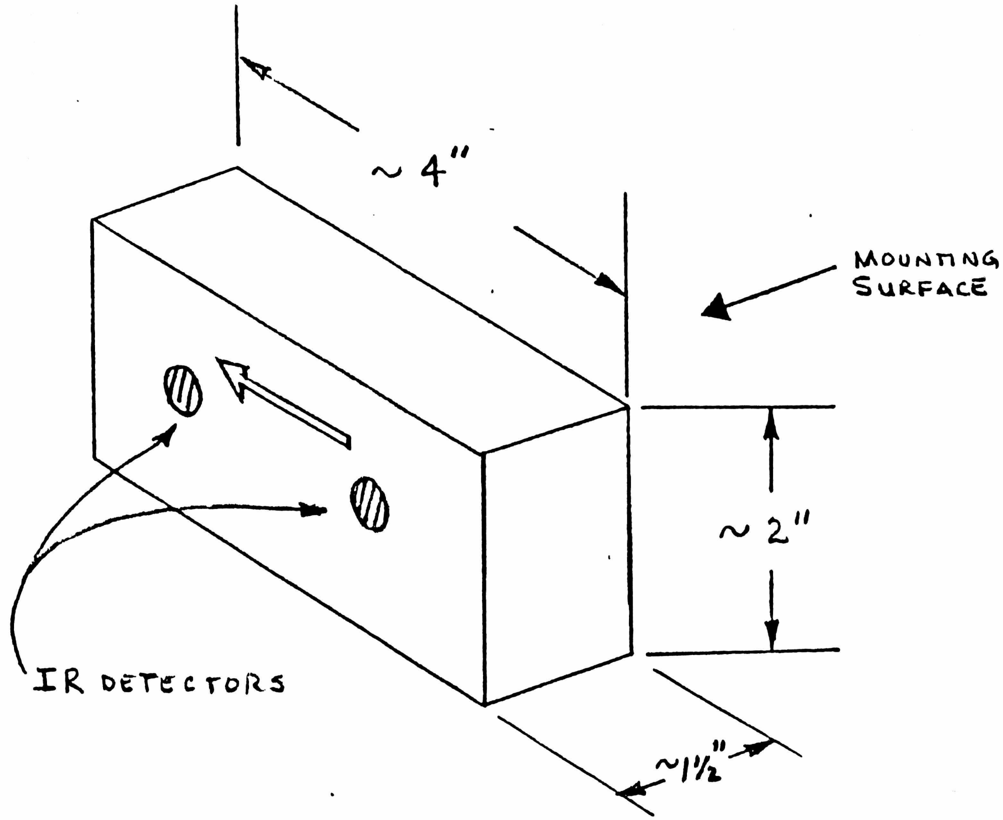
These types of detectors are known for their good falsing rates and TI can make them very cheaply. They will be offered in the TICOM security system. Price : $75.00 with transceiver.

The Traffic Counters: Type Number =3, S/N =1-15

These are devices which are nothing more than our IR motion detectors without the optical equipment. They consist of a pair of IR detectors in one package that, when mounted in place (in a doorway or hallway), will be colinear in the direction of motion, as shown in Figure 22. When an IR source moves across the field of view of one of the "eyes," that detector is triggered. As the source continues to move, the other detector is triggered. By noting which detector went off first, the direction of motion is established. If the traffic counter is in the disarmed state, it uses the information just gathered to increment either a "plus" (for one direction) or a "minus" (for the other direction) count, up to a maximum count of 64. The "plus" direction is indicated by a small arrow between the two "eyes." If the traffic counter is in the armed state, the information gathered simply constitutes a sensor actuation and an intrusion alarm condition is generated. Price : $65.00 with transceiver.

The Magnetic Switches: Type Number =4, S/N =1-15
Type Number =7, S/N =6-15

These are devices that are used to detect the proximity of two surfaces. When the surfaces are close, a magnetic field bridges the air gap between the surfaces and maintains a closed circuit. When the surfaces are far apart, the circuit is broken and this is easily detected. There are also switches that operate in the



ARROW INDICATES DIRECTION OF "PLUS" COUNT

FIGURE 22 - TRAFFIC COUNTER ILLUSTRATION

opposite sense and these will also be offered. Price : $55.00 with transceiver.

The Gas Detectors: Type Number =5, S/N =1-5
These devices can sense natural gas in the air. Price : $70.00 with transceiver.

The Heat Detectors: Type Number =5, S/N =6-15
These are solid-state heat sensing devices that would also attach to transceivers. Price : $65.00 with transceivers.

The Personal Security Transceiver (PST): Type Number =7, S/N =6-15
This device is essentially a manually-triggered multi-fuction panic button. It allows the user to remotely (150 feet) interrogate the system intrusion status (triggered or untriggered) and receive a "red" or "green" indication accordingly; to generate a personal emergency alarm condition; and to activate or deactivate the system at a 150-foot distance. Several keys are provided on the device, which is about the same size as a hand-held calculator, for these functions. Figure 23 illustrates this device. This device has its own "yellow" battery indicator and is therefore not subject to automatic status inquiries or updates from the SPC. Price : $60.00.

The Poll-Monitoring Device: Type Number =Ø, S/N =1-15
This device is identical to a sensory transceiver, except that it is AC-powered (irrespective of whether the security link is RF or PL), battery-backed, and contains its own buzzer. Its function is described in Section 5.0 in detail. Price : $65.00.

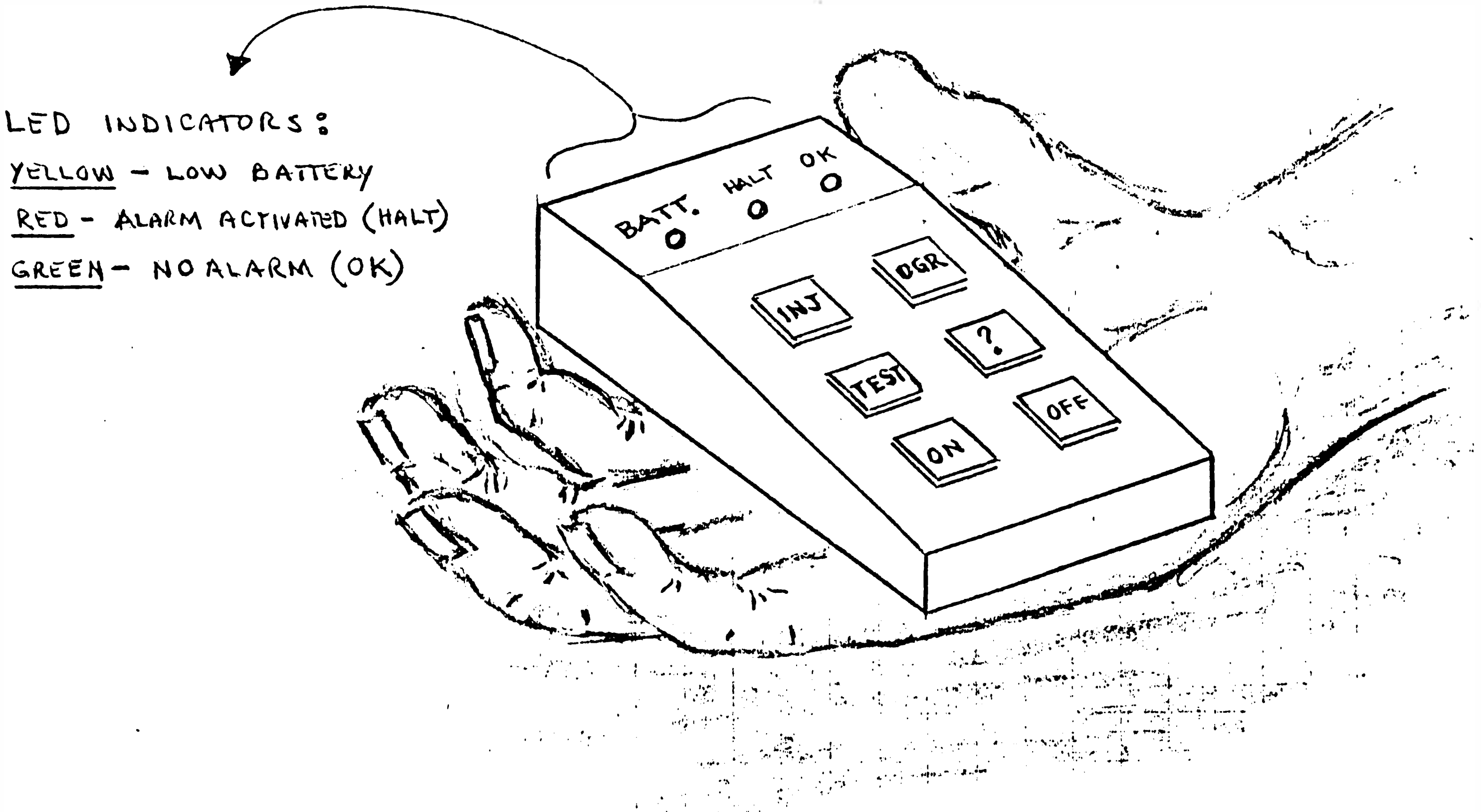


FIGURE 23 - PERSONAL SECURITY TRANSCEIVER (PST) ILLUSTRATION

9.0 CONCLUSION

An HCSS has been proposed which is believed to offer unprecedented capabilities and effectiveness to semi-affluent consumer at an affordable price. In summary, its features are as follows:

- Remote interrogation
- Remote activation and deactivation
- Autodialing of selectable emergency phone numbers with a repertoire of up to 24 numbers
- Programmable synthetic voice alarm messages
- Programmable automatic daily activation and deactivation
- Automatic self-testing and diagnosis
- Up to 106 sensory devices can be supported
- Redundantly reliable smoke detectors
- Low-cost, low-falsing IR motion detectors
- Battery operation with 2-year sensor battery life
- Capability for speed-dialing from the SPC

Furthermore, the above features can only be adequately provided if the system is implemented using an RF link between the SPC and the sensors.

An important feature that has not been mentioned consists of the ability of the system to cause doors and/or windows to be locked. What is needed is a "sensor" that can respond to a state change command by locking a door-lock mechanism. This could easily be designed if only one-way "arm" automatic operation is desired. For example, a device could be designed that could only be unlocked manually. The manual unlock could cause a spring to wind-up, thus storing mechanical energy that could be released in response to a state change command, causing the device to lock. The system as proposed here can easily accommodate this feature by assigning type number 6 to such devices. This would allow the user to cause doors and windows around the house to be locked automatically at the prescribed system activate time.

It is important to realize that much market research must be conducted before the architecture of this system, because of its effect on the design of features, can be finalized. What is needed is focused consumer surveys conducted in several major metropolitan areas. Also, a survey of local public safety agencies across the country is needed on their views on automatic home security systems, particularly with autodialers. The same market data is needed for the finalization of the TICOM home security system and, unfortunately, as of this writing, no real definition exists as to when the required funds will be made available. Any program to design and develop the HCSS proposed here must take this into account when committing to schedule dates.

Another question associated with these types of systems is that of the extent of the manufacturer's liability. The inputs that we have received from the TI legal Department (see Appendix D) seem to indicate that no unuasually high risks are involved.

Finally, it is appropriate to point out that from an architectural standpoint, much of the needed system design groundwork has been laid, as documented herein, towards the structuring of an industrial-grade security system for small businesses.

It is interesting to hear that the Lubbock Police Department reports a total false-alarm rate of over 96%, of which 87% are originated by business rather than residential systems. This is a serious problem that distracts the diligence and dilutes the effectiveness of the local police force. We understand that some city legislation is pending regarding this situation. There is little doubt that a small-business security system of superior performance that was, say, SR-70-based, could have a dramatic impact on the commercial security market if properly planned and properly marketed.

APPENDIX A

CODING AND SIGNALLING ANALYSIS

This Appendix consists of a copy of the report on the signalling scheme formulated for the TICOM security system.

TELEPHONE

INTERCONNECT

COMMUNICATION

(TICOM)

A REPORT SUMMARIZING THE SIGNALLING AND CODING WORK DONE TO DATE.

BY

ART RODRIGUEZ

LUBBOCK, TEXAS

MARCH 14, 1978

TABLE OF CONTENTS

SIGNALLING FOR PHONALERT
A SUMMARY

Art Rodriguez
3/14/78

INTRODUCTION

Phonalert is a family of products designed for radio-controlled home security systems. These systems consist of small pocket-size transmitters which when activated emit a radio-frequency burst of one second duration, as limited by the FCC. This burst is sensed at the "base" which is connected to the telephone lines in the home. Upon sensing the burst transmission, a telephone number previously stored by the user at the base is dialed automatically and an audible tone is impressed on the phone lines which will alert the person answering the phone call. Since the initial product will be aimed primarily at applications where an alarm condition is indicated by the call, we call this function alarm autodialing. More generally, it is a form of remote autodialing.

Because the number of R.F. channels available for phonalert systems is limited by law (FCC), when the base senses a transmission it must be capable of deciding if it came from its own system or from some near-by adjacent system (call it the "neighbor" system) on the same channel. This establishes the need for some kind of system ID. In addition, several distinct alarms are envisioned -- e.g., intrusion, fire, etc. -- which would necessitate some kind of alarm ID or, more generally, function ID. It is easy to conceive of an expanded system wherein these transmissions (RF bursts) can serve as control functions, with some of the function ID's being assigned to alarms and others to control commands of some sort.

Since low-cost is paramount in the marketing philosophy of these consumer products, we are faced with the task of coding the transmissions for system and function ID in the simplest form possible consistent with the performance requirements of low probability that the base would not recognize a transmission from its own system -- Pr(missed) less than 10^{-4}--, low probability that the base would mistake a transmission from a neighor system for one from its own system -- Pr(false) less than 10^{-5}--, and low current drain to allow long battery life, all at minimum cost.

SIGNALLING SCHEME SELECTION

The simplest and most widely used codes are those generated by shift-register sequences. They can be generated very economically and are thus desired for our application. This means that the system ID should consist of a sequence of binary digits (bits). The longer the sequence (in number of bits), the larger the number of distinct ID's available. For a K-bit sequence, for example, 2^K ID's are available.

Because of the short-burst nature of the transmissions in phonalert systems, linear block codes are ideally suited for coding the ID's for error and falsing protection. However, these codes are formed by adding L redundant "parity" bits to the "block" of K minimum number of "information" bits necessary to obtain the desired number of distinct ID's ("codewords"). That is, even though only a K-bit sequence is needed to transmit 2^K possible ID's, a longer N-bit (N=K+L) sequence is actually transmitted with the result that in a given codeword several bits could be changed by channel noise during transmission without causing the received sequence to look like another "valid" codeword. A one-to-one mapping is thus effected from a K-dimensional space into an N-dimensional space. Since linearity under modulo-2 addition is preserved by the coding transformation, the two spaces are isomorphic and the minimum distance of the code (i.e., the minimum number of bits in one codeword that must be changed in order to obtain another codeword), d, is given by the minimum number of "1's" in any one codeword -- called the minimum Hamming weight of the code. This concept of minimum distance is very important because this is what gives the transmission added noise immunity since more than d/2 bit errors must occur during transmission (instead of just one if no redundancy were used) before the codeword is mistaken for another codeword -- the code is said to "correct" (d/2)-1 bit errors.

Another way to accomplish additional noise immunity is by retransmission of the information bits. Retransmission and block coding both lead to redundant transmission time, but retransmission can be accomplished with considerable less hardware at the transmitter and is therefore preferred for our application. See Figure 1.

Since it is desired to be able to assign system ID's at random, thus eliminating the need to keep track of what customer gets what ID, the size of the ID set (2^K) should be as large as possible in order to minimize the probability of assigning the same ID to near neighbors. (Note that if the neighbors are 9 houses or more apart, the same ID can be assigned to them without fear of interference between them due to the weakness of the interfering RF link required.) It is deemed that a set of 2,047 ID's would minimize such probability sufficiently for practical purposes. This means an 11-bit system ID sequence. In addition, a set of 32 function ID's is deemed adequate to accommodate future expansion into control, in addition to alarm, functions. This means a 5-bit function ID sequence. Thus a composite 16-bit sequence is needed to convey system and function ID information without redundancy. This 16-bit sequence will be referred-to as the composite ID.

RETRANSMISSION TECHNIQUE

Figure 1a shows how simply the ID encoder can be built. The circuit shown transmits the 16-bit sequence associated with the 11-bit system ID programmed by the code plug and the 5-bit function ID programmed with jumpers on the PC board of the transmitter at F1 through F5. When the 16-bit composite ID is transmitted, it is immediately followed by its one's complement (we will call it its inverse), which in effect constitutes a retransmission and gives us a 32-bit sequence with equal number of "1's" and "0's" in it. This insures the optimality of a V/2-threshold bit decision rule at the receiver, where V is the difference between a logical "1" voltage and a logical "0" voltage. (See figure 3.)

In order to use the low-cost inverter RC oscillator shown in Fugure 1a, bit timing must be recovered at the base. This is most easily accomplished by encoding each bit with a two-bit barker sequence: "0" $\rightarrow$ (0,1); "1" $\rightarrow$ (1,0) (This is also known as split-phase, bl-phase level, Manchester coding, or differential phase shift keying, and is simply accomplished by exclusive-or'ing the data stream with the clock). The effect of this encoding is that logic transitions occur more often in time allowing timing information as to when a bit should be present to be extracted more accurately from the received bit stream. This extraction is accomplished with the clock recovery circuit of

Figure 1b at the base. The "lock indicator" allows us to ignore the presence of noise when no signal (or a signal too weak to recover timing) is present.

The split-phase technique also has the effect of doubling the information bandwidth of the binary waveform which means 3dB more noise power at the receiver. As we shall see, we can afford this in our systems since plenty of signal-to-noise margin is available due to the low bit rate chosen.

As shown in Figure 2, the circuit of Figure 1a transmits ten bit times of clock to lock the clock recovery circuitry, followed by a 32-bit pattern consisting of the composite ID and its inverse. This is followed by the 32-bit pattern twice so that the 32-bit pattern is transmitted a total of three times for additional noise immunity.

The bit rate has been selected to be 110bps which is standard low-speed teletype (10 characters per second). With the standard assumption that the energy in the secondary spectral lobes is negligible, this means that our information bandwidth is 220Hz.

BIT ERROR RATE

In order to establish what kind of Pr(missed) and

Pr(False) the above retransmission technique will yield, we first need to determine the probability that a bit is in error, Pr(e). Under the white Gaussian noise assumption, if we plot the probability density function (pdf) of a received voltage after filtering, it is recognized as a Gaussian pdf centered about the voltage (signal) transmitted. This represents the corruption of the signal voltage by additive Gaussian noise. The larger the noise power present (σ^2), the more spread-out the Gaussian pdf becomes. Since two logical voltages are possible at the transmitter, two such pdf's are possible depending on which signal was transmitted. Thus in Figure 3 we see one pdf which applies on the hypothesis that a "1" was transmitted (H1), and one which applies on the hypothesis that a "0" was transmitted (HO). If the two signals are equilikely at the source (i.e., the probability that a "1" was transmitted equals the probability that a "0" was transmitted equals 1/2) such as is guaranteed by our code inversion technique, then the optimum decision threshold is where the two pdf's cross. For the case of unipolar baseband (which is our case: "0"=0 volts, "1"=V volts), this threshold is V/2. That is, if the recovered voltage is greater than V/2, we decide that a "1" was transmitted; if it is less than V/2, we decide that a "0" was transmitted. Since this threshold could be selected from any value in the horizontal axis of the plot in Figure 3, it is referred to as the decision variable, r Decision theory deals with the various ways of utilizing the decision variable in formulating an optimum "decision rule." In our application above we used the simple threshold decision rule: $r \underset{H_0}{\overset{H_1}{\gtrless}} V/2$.

Note that one way that a decision error can occur is that the detected voltage is larger than V/2 but the signal transmitted was a "0". In order to obtain the total probability that a decision error will be made when a "0" is transmitted - i.e., the probability of a bit error given that a "0" was transmitted, Pr(e/o) - we need to integrate the area under the Gaussian tail in the region $r > V/2$ and then multiply this by the probability that a "0" was transmitted, Pr(0). The other way that a decision error can occur is when the detected voltage is less than V/2 but the transmitted signal was a "1". The situation is completely analogous to the one just discussed and results in a decision error with probability Pr(e/1) multiplied by the probability that a "1" was transmitted, Pr(1). The total probability of making a decision (bit) error is thus given by

$$P_R(e) = P_R(e|0)\,P_R(0) + P_R(e|1)\,P_R(1) \,. \tag{1}$$

From the symmetry in Figure 3, we see that $P_R(e|0) = P_R(e|1)$

$\equiv \Phi(V/2\sigma)$. Therefore,

$$P_R(e) = \Phi(V/2\sigma)\left[P_R(0)+P_R(1)\right] = \Phi(V/2\sigma), \qquad (2)$$

Where $\Phi(V/2\sigma)$ is the area under the Gaussian pdf of standard deviation σ from V/2 to infinity. Although the integral of the Gaussian pdf is not expressible in closed form, many numerical evaluations of this integral have been made and it is normally tabulated as the normalized error function. The normalized error function erf(x) is the integral of the Gaussian from 0 to X with σ =1, therefore $\Phi(x)$ is given by

$$\Phi(x) = \frac{1}{2} - \mathrm{ERF}(x) \, . \qquad (3)$$

PROBABILITY OF MISSING A TRASMISSION

We will now assume that we can count on the probability of a bit error $P_R(e) = \Phi(x) = .001$ or better.

Let us begin by recognizing that the probability of a composite ID being in error is given by the probability that one or more of its 16 bits are in error. Under the assumption that each (bit) error is independent of all other errors, the probability that one specific bit out of 16 is in error is given by

$$P_{16}(\text{A SPECIFIC BIT IN ERROR}) = p^1 q^{16-1}, \qquad (4)$$

where p is Pr(e) of equation (2) and $q=1-p$. Since there are several combinations - given by the binomial coefficient $\binom{16}{1}$ — of one-bit errors in 16 bits, the probability that <u>any</u> one bit out of 16 is in error is given by

$$\begin{aligned} P_{16}(\text{1 BIT ERROR}) &= \binom{16}{1} p^1 q^{16-1} \\ &= \frac{16!}{1!\,(16-1)!} p^1 q^{16-1} \\ &= 16\, p^1 q^{15} \,. \end{aligned} \tag{5}$$

In general, we can write

$$P_{16}(k \text{ BITS IN ERROR}) = \frac{16!}{k!\,(16-k)!} p^k q^{16-k} . \tag{6}$$

So, the probability that one or more bits are in error is given by

$$\begin{aligned} P_{16}(k \geq 1 \text{ BITS IN ERROR}) &= \sum_{k=1}^{16} \frac{16!}{k!\,(16-k)!} p^k q^{16-k} \\ &= 1 - P_{16}(k=0 \text{ BITS IN ERROR}) \\ &= 1 - q^{16} , \end{aligned} \tag{7}$$

and for our assumed Pr(e)=.001, we have

$$P_{16}(k \geq 1) = .0158 \,. \tag{8}$$

However, at the base we require that no error be made in the 32-bit sequence comprising the composite ID and its <u>inverse</u>. This essentially means that the base is looking for two composite ID transmissions to occur without error. The probability of one or more errors in 32 bits is given by

$$P_{32}(K \geq 1) = 1 - q^{32} = .0315, \qquad (9)$$

for p=Pr(e)=.001.

As mentioned previously, our transmitter will transmit the composite ID followed by its inverse a total of three times. This means that if any one of the three versions of the 32-bit pattern is error-free, the transmission will be detected. Conversely, if one or more errors occur in all three versions, the transmission will be missed. Under the assumption that the errors in one version are statistically independent of those in the other versions, the probability that a transmission will be missed is given by

$$\begin{aligned} P_R(\text{MISSED}) &= P_3(\text{3 VERSIONS ARE IN ERROR}) \\ &= \binom{3}{3} p^3 q^0 \\ &= p^3, \end{aligned} \qquad (10)$$

Where p now represents the probability that a version is in error, $P_{32}(K \geq 1)$, given by equation (9). Thus,

$$P_R(\text{MISSED}) = .0315^3 = 3.13 \times 10^{-5} \qquad (11)$$

For Pr(e)=.001. This is well within the one-in-ten-thousand (10^{-4}) performance sought.

PROBABILITY OF A FALSE TRANSMISSION

To obtain the probability of a false, Pr(False), we need to first determine the probability of the 11-bit system ID portion of the composite 16-bit ID sequence of a near neighbor's being corrupted by channel noise into the reference system's own 11-bit ID. Since this probability, call it P(F), is essentially the probability that the right 11-bit error pattern occur with the right near neighbor 11-bit ID, in order for the reference system to be falsed this <u>same</u> error pattern must occur again when the inverse of the neighbor's ID is subsequently transmitted. The probability of this double occurrence is thus the probability of a false and is given by $Pr(\text{false}) = [P(F)]^2$.

Now, to obtain P(F) we can write

$$P(F) = \sum_{k=1}^{11} P_{11}(F/k)\, P_{11}(k), \tag{12}$$

Where

$P_{11}(F/k)$ is the probability of one ID falsing given that k errors have occurred in 11 bits,

and

$P_{11}(k)$ is the probability that k bit errors will occur in the first 11 bits of ID.

The conditional probability $P_{11}(F/k)$ is simply the probability that the 11-bit neighbor ID transmitted differs from the reference system's own ID by k bits (i.e., that the bit distance between the falsing ID and the falsed ID is k). Since no redundant bits are used in the ID sequence, $\binom{11}{k}$ neighbor ID's can cause a false given that any error pattern of weight k has occurred. Assuming that all possible ID's are equalikely, this means that

$$P_{11}(F|K) = \binom{11}{K} P_R(\text{ONE OF THE } 2^{11} \text{ ID'S WAS TRANSMITTED})$$

$$= \binom{11}{K} \times \frac{1}{2^{11}}$$

$$= \binom{11}{K} 4.88 \times 10^{-4}. \qquad (13)$$

Substituting equation (13) into (12) then gives

$$P(F) = \sum_{k=1}^{11} 4.88 \times 10^{-4} \binom{11}{K} P_{11}(k)$$

$$= 4.88 \times 10^{-4} \sum_{K=1}^{11} \binom{11}{K} P_{11}(K), \qquad (14)$$

But the summation factor is nothing more than

$$\sum_{K=1}^{11} \binom{11}{K} P_{11}(K) = \sum_{K=1}^{11} \frac{11!}{K!(11-K)!} p^K q^{11-K}$$

$$= P_R(\text{1 OR MORE BITS OUT OF 11 IN ERROR})$$

$$= 1 - q^{11}, \qquad (15)$$

As previously given in equiation (7) for a 16-bit sequence.

So, we have

$$P(F) = 4.88 \times 10^{-4}\,(1 - q^{11}), \tag{16}$$

and for a neighbor signal of the same strength as the system's own transmitters would produce (i.e., $p = P_R(e) = .001$, $q = .999$), this yields

$$P(F) = 4.88 \times 10^{-4} \times .011 = 5.34 \times 10^{-6}. \tag{17}$$

However, neighbor signals should be weaker by design making the likelihood of a false greater because the noise now has more corruptive power over the signal. In the limit, the worst-case falsing is that due to pure Gaussian noise. (This is only true in general for the case in which no redundant bits are used to code the information.)

In this case, $q = .5$ and

$$1 - q^{11} = .9995 \sim 1.0, \tag{18}$$

So that P(F) is bounded by (i.e., could never be worse than)

$$P(F) = 4.88 \times 10^{-4} \tag{19}$$

Which is the protection afforded us by the length (11-bits) of the ID (notice that $.5^{11} = 4.88 \times 10^{-4}$).

The actual probability of a system false is thus given by

$$P_R(\text{FALSE}) = [P(F)]^2 = 2.38 \times 10^{-7}.$$

(20)

This is well within the one-in-one-hundred-thousand performance sought.

SIGNAL-TO-NOISE REQUIREMENTS

In order to allow inexpensive low-stability crystals to be used for RF carrier generation at the transmitter, we wish to make the transmission bandwidth smaller than the assigned channel (and therefore IF) bandwidth of 15KHz. A peak deviation of 220Hz accomplishes this and results in a modulation index of one and a transmission bandwidth of 440 Hz. (A small peak deviation also allows inexpensive FM oscillator design.) This means that the carrier frequency can have an error of

$$\Delta f_c = \pm \frac{1}{2}\left(BW_{CHAN.} - BW_{TX}\right) = \pm(7.5 - .22) = \pm 7.28 \text{ KHz}$$

at $f_c = 49.9$ MHz, for example, this translates to a frequency stability of $\Delta f_c / f_c = 146$ ppm. If the same crystal oscillator is used in the receiver at the base, then each must be ± 73 ppm or better.

The sacrifice involved in using a wider channel (IF) bandwidth than the signal requires is that the carrier power at the receiver input required to capture the limiter (10dB rise in the IF) must be larger than with a smaller IF bandwidth. However, RF coverage calculations show that a 10-dB rise in the receiver IF input to the limiter can be guaranteed economically in our systems. Once we have limiter capture, we can use post-detection filtering of the discriminator output to improve the audio signal-to-noise RATIO (SNR) AND FACILITATE BIT RECOVERY. AT THIS POINT, WE could filter as much as our information bandwidth (220Hz) will allow.

Before proceeding to calculate the SNR available in the recovered baseband, let us first determine what the required SNR is for a Pr(e) of .001 as assumed in our probability calculations earlier. From a tabulation of the complement of $\Phi(x)$ in reference [1], we find that in order for $\Phi(x) \leq .001$, x must be ≥ 3.08.

Thus,

$$x = \frac{V}{2\sigma} = \sqrt{\frac{V^2}{4\sigma^2}} = \sqrt{\frac{V^2/2}{2\sigma^2}} = \sqrt{\frac{1}{2}\frac{S}{N}} \geq 3.08, \quad (21)$$

From which we obtain the required SNR to be

$$SNR = \frac{S}{N} \geq 10 \log[2 \times (3.08)^2] = 10 \log 18.97 = 12.8 \text{ dB}. \quad (22)$$

Now, our RF coverage guarantees a 10dB rise in the IF.

This translates into a carrier-to-noise ratio (CNR=C/N) at the limiter-discriminator input of

$$RISE \equiv \frac{C+N}{N} = \frac{C}{N} + 1 = 10 \tag{23}$$

$$\Rightarrow \left(\frac{C}{N}\right)_i = 10 \operatorname{Log} 9 = 9.5\ dB . \tag{24}$$

From page 434 and page 435 in reference [2], the output noise power, N_0, and the output signal power, S_0, at the discriminator output are respectively given by

$$N_0 = \left(\frac{K_d}{A_c}\right)^2 (2\pi)^2 \frac{2\eta_0}{3} f_m^3 \tag{25a}$$

and

$$S_0 = K_d^2 (\Delta F)^2 \overline{x^2(t)} , \tag{25b}$$

Where

- Kd is a discriminator constant,
- Ac is carrier amplitude at the limiter input
- ΔF is the peak frequency deviation,
- η_0 is the noise spectral density,
- f_m is the maximum modulating frequency, and

$\overline{x^2(t)}$ is the variance of the modulating signal normalized in amplitude.

Therefore, the audio SNR at the discriminator output is given by

$$\left(\frac{S}{N}\right)_o = \frac{K_d^2 (\Delta F)^2 \overline{x^2(t)}}{K_d^2 \frac{1}{A_c^2} \frac{2}{3} \eta_o f_m^3} = \frac{3 A_c^2 (\Delta F)^2 \overline{x^2(t)}}{2 \eta_o f_m^3} ; \tag{26}$$

but the input CNR at the limiter is, by definition, given by

$$\left(\frac{C}{N}\right)_i \equiv \frac{\text{CARRIER POWER}}{\text{NOISE POWER}} = \frac{A_c^2/2}{\eta_o B_{IF}} . \tag{27}$$

equating equations (24) and (27), we have

$$\frac{A_c^2/2}{\eta_o B_{IF}} = 9 , \tag{28}$$

$$\Rightarrow \frac{A_c^2}{2} = 9 \eta_o B_{IF} . \tag{29}$$

Substitution of (29) into (26) yields

$$\left(\frac{S}{N}\right)_0 = 3\left(\frac{\Delta F}{f_m}\right)^2 \frac{9\eta_0 B_{IF}}{\eta_0 f_m} \overline{x^2(t)} \,.$$

(30)

For our system, as described previously, a modulation index $\Delta F/f_m$ of <u>one</u> is desired. Also, $\overline{x^2(t)} = 1/4$ for a normalized unipolar baseband signal. Therefore,

$$\left(\frac{S}{N}\right)_0 = 3 \times 9 \times \frac{1}{4}\left(\frac{B_{IF}}{f_m}\right)$$

$$= 6.75\left(\frac{B_{IF}}{f_m}\right),$$

(31)

Where fm represents the cutoff frequency (i.e., bandwidth) of the post detection low-pass filter mentioned previously. Thus, the best $(S/N)_0$ will be for a cut-off frequency equal to the maximum baseband frequency desired (220Hz). For future flexibility at higher data rates , and in order to provide margin against our secondary lobe assumption, we will use 500Hz in our computations:

$$\left(\frac{S}{N}\right)_0 = 6.75\left(\frac{15\,\text{KHz}}{.5\,\text{KHz}}\right) = 202.5 \cong 23\,\text{dB} \,.$$

(32)

This is almost twice what we needed -- see equation (22) --

in dB's in order to insure the bit error rate of 10^{-3} on which our probability calculations were based.

CONCLUSION

It is concluded that with a 10dB rise in the IF and the signalling scheme described above, the probability of missing a transmission assuming ten transmissions per day is less than once in 8.7 years. Similarly, the probability of detecting a false transmission assuming 100 neighbor transmissions a day, is less than once in 11.5 years. This renders the proposed scheme acceptable.

The decoding algorithm at the base simply looks for the

composite ID and its inverse in succession, then matches the system ID, and finally decodes the function BEFORE taking any action.

References

[1] - Cooper, G.R., and McGillem, C.D., Probabilistic Methods of Signal and System Analysis, Holt, Rinehart, and Winston,Inc, N.Y., 1971.

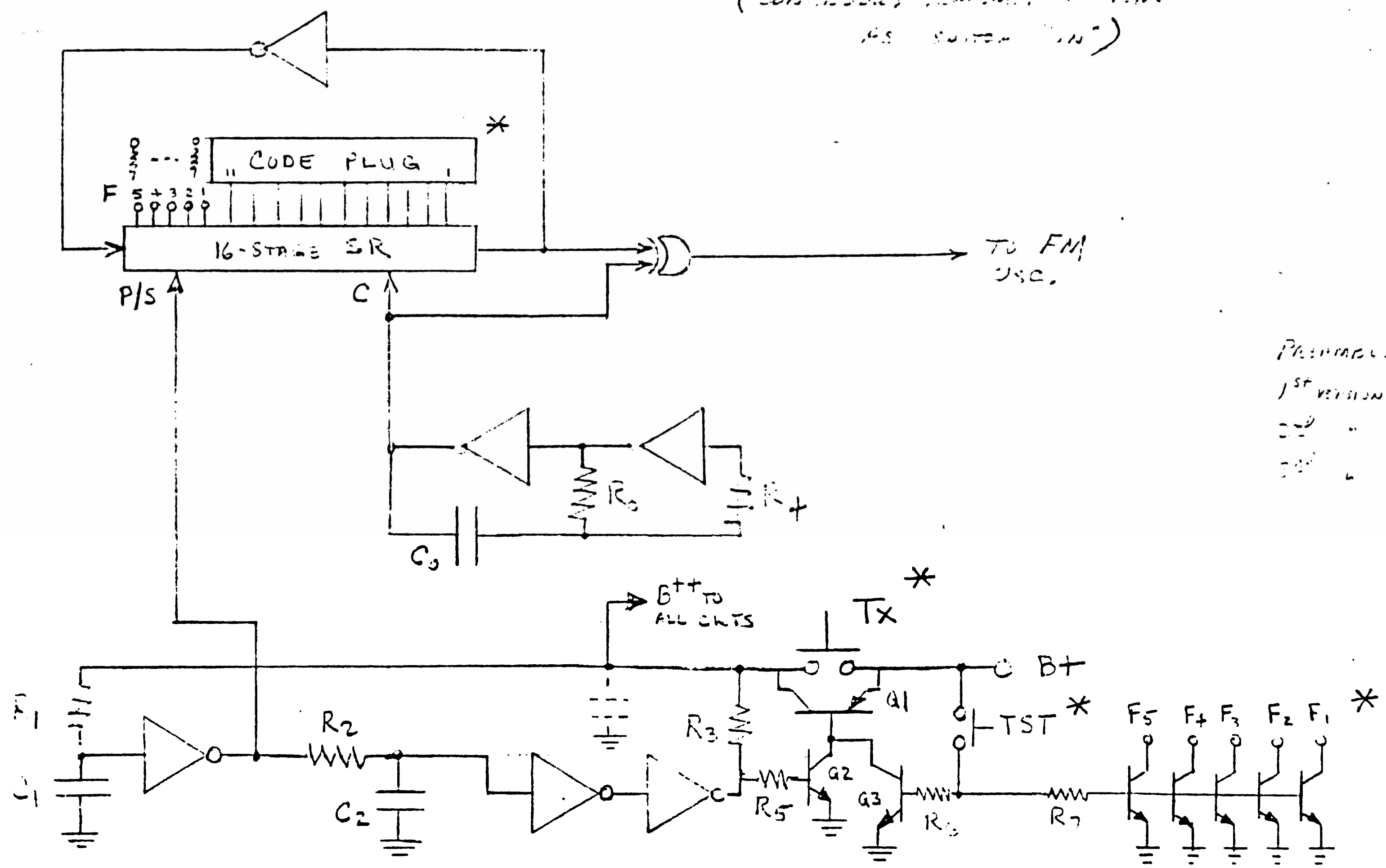
[2] - Panter, P.F., Modulation, Noise, and Spectral Analysis, McGraw-Hill Book Co., N.Y., 1965.

Panic Button Transmitter Logic

(Continuous transmit as long as button "in")

12/22/—

Revised 3/3/78



Preamble 10 T
1st version 32 T
32 T
32 T
166 T = .333 sec.

$R_6 C_3 = \frac{9.1}{1.4} = \ldots$ => $C_3 = .0\ldots$ uF

$R_1 C_1 = 0.5 \times R_6 C_3 = \ldots$ => $R_1 = 155 \ldots$, $C_1 = .005 \ldots$ uF

$R_2 C_2 = 70 \times R_1 C_1 = \ldots$ => $R_2 = 10K$, $C_2 = 6.5$ uF

$R_3 = 470 K\Omega$, $R_4 = 100 K\Omega$

FIGURE 1a

3/17/78 LLW 039-367

TI STRICTLY PRIVATE

Clock Recovery Circuitry

Revised 3/13/78

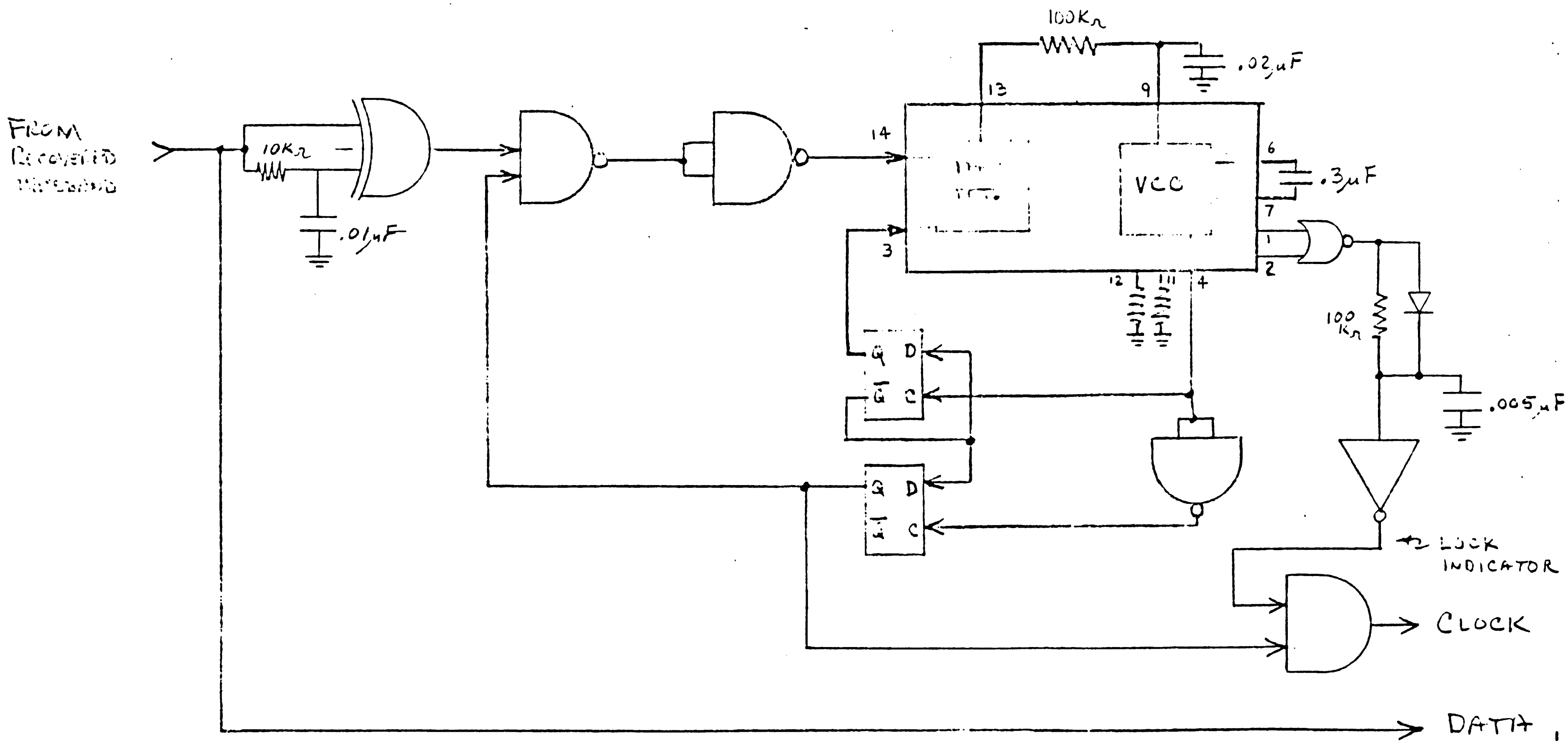


Figure 1b

Art Koor. [illegible]
2/25/78

TRANSMISSION FORMAT FOR TICOM

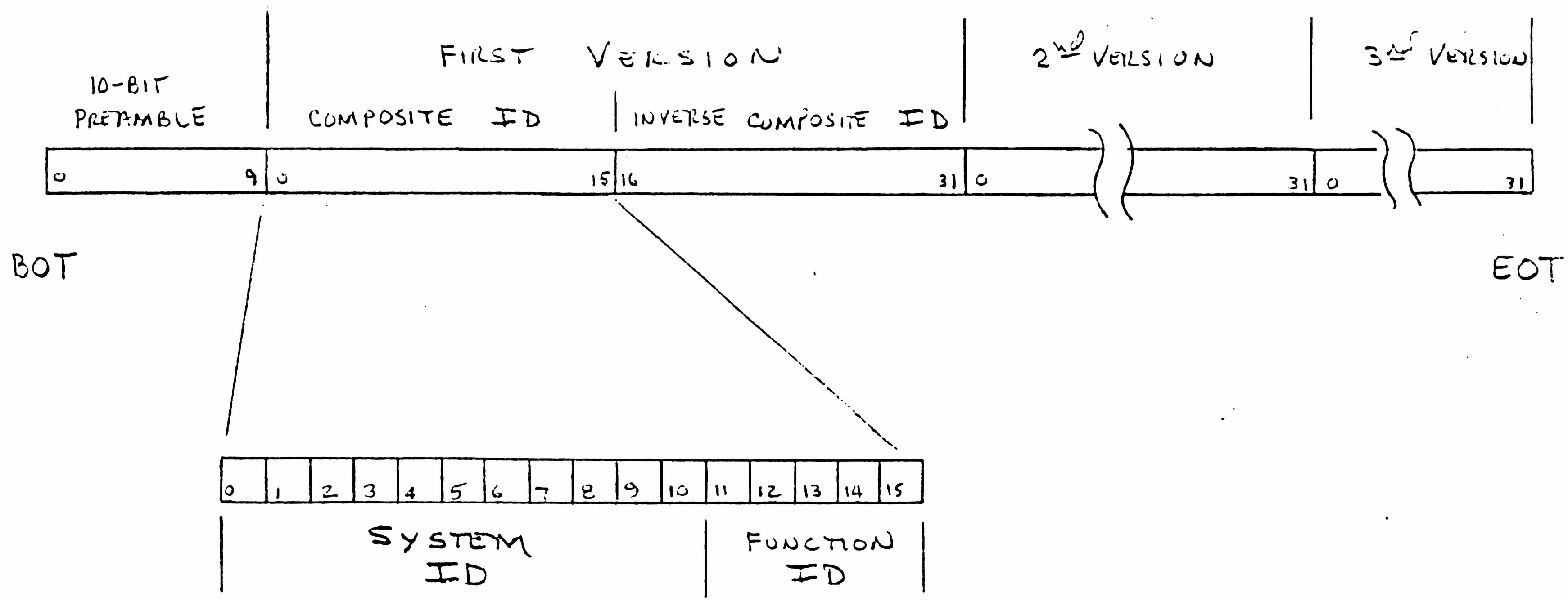


FIGURE 2

Art Rodriguez
3/4/78

PLOT OF PROBABILITY DENSITY FUNCTION OF
RECOVERED VOLTAGE

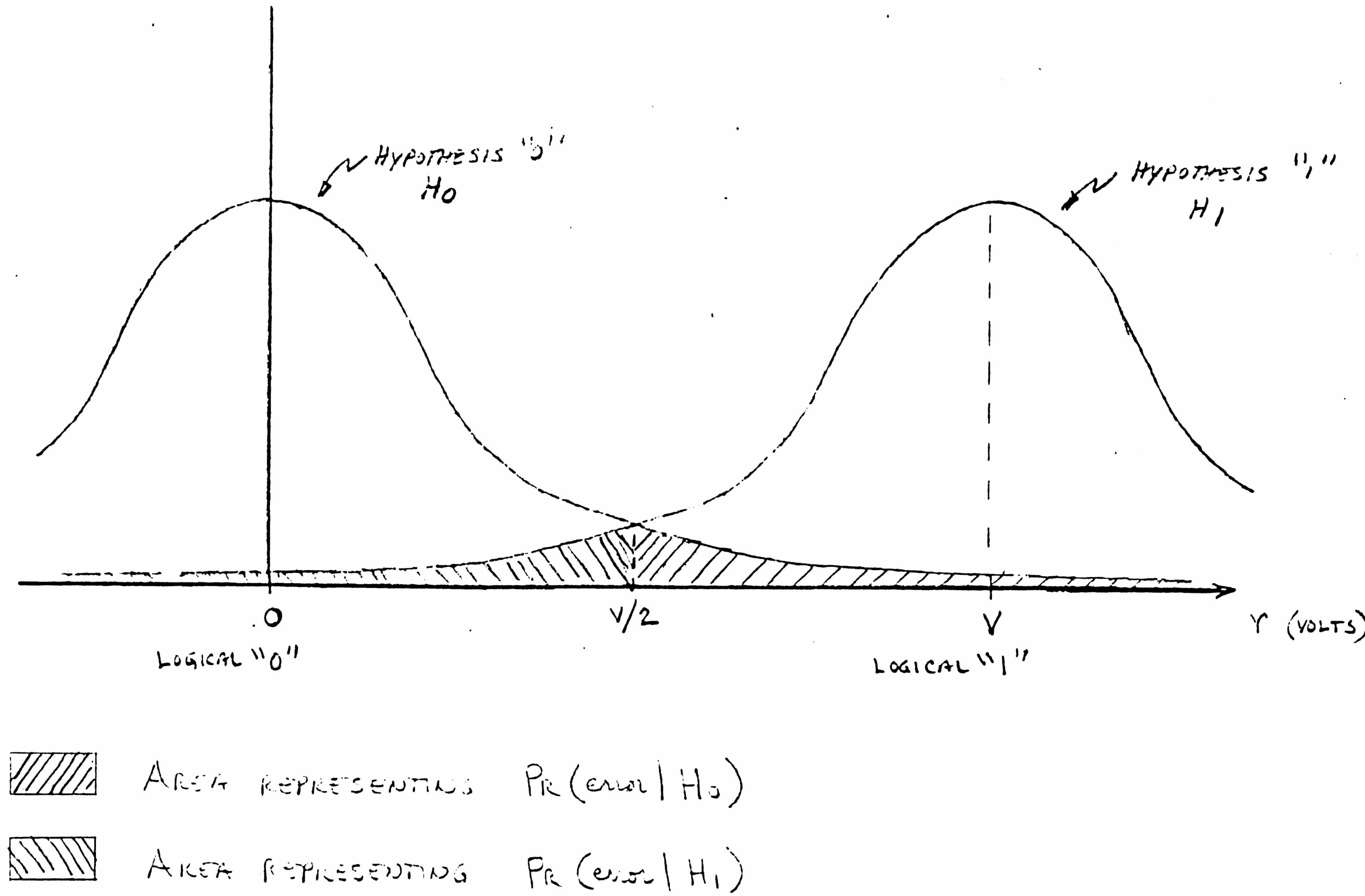
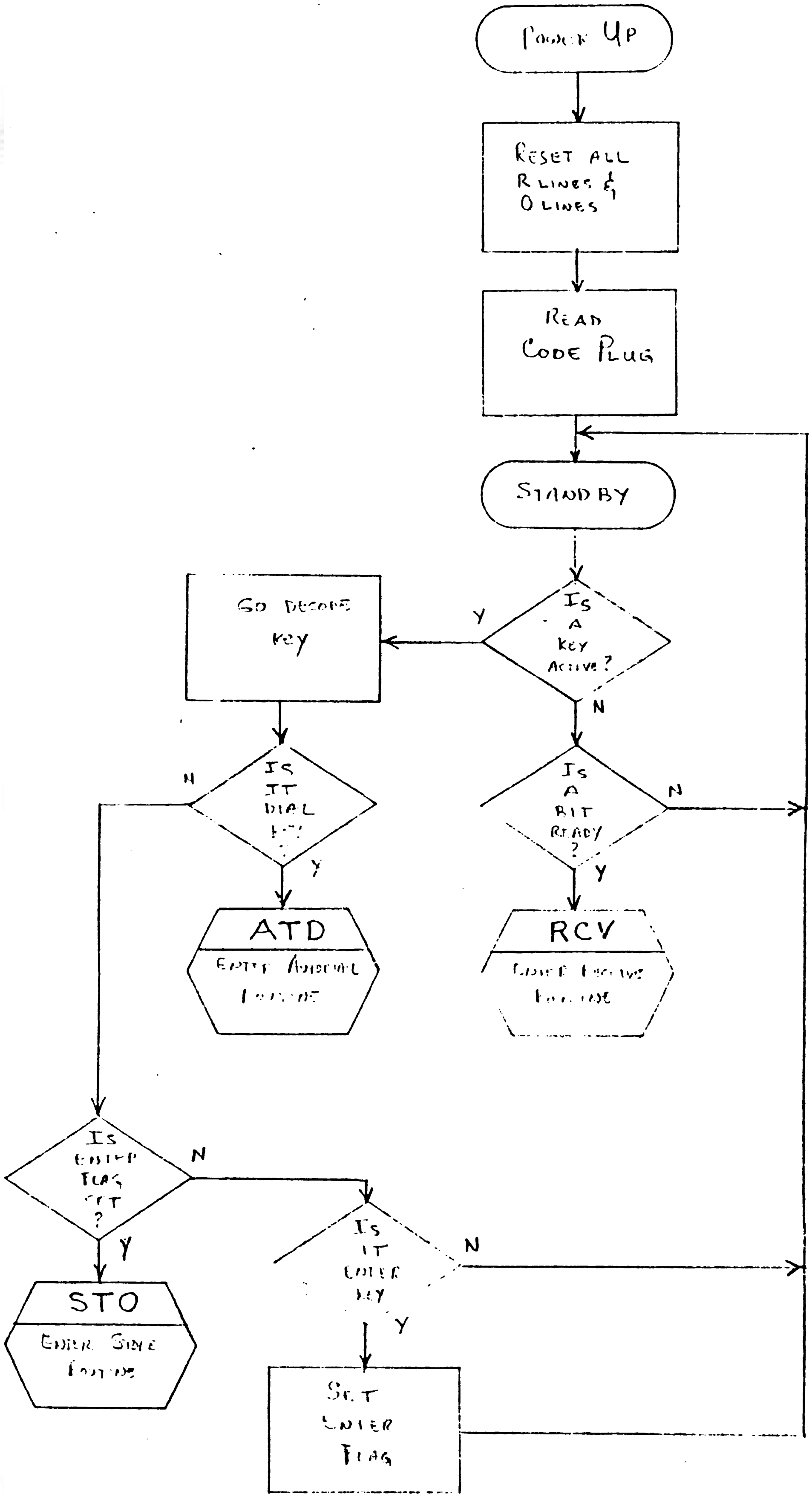


FIGURE 3


Power Up
Reset All R Lines & O Lines
Read Code Plug
Stand By
Is A Key Active?
Y
N
Go Decode Key
Is A Bit Ready?
N
Y
ATD
RCV
N
Y
Is Enter Flag Set?
N
Y
STO
Is It Enter Key
N
Y
Set Enter Flag

APPENDIX B

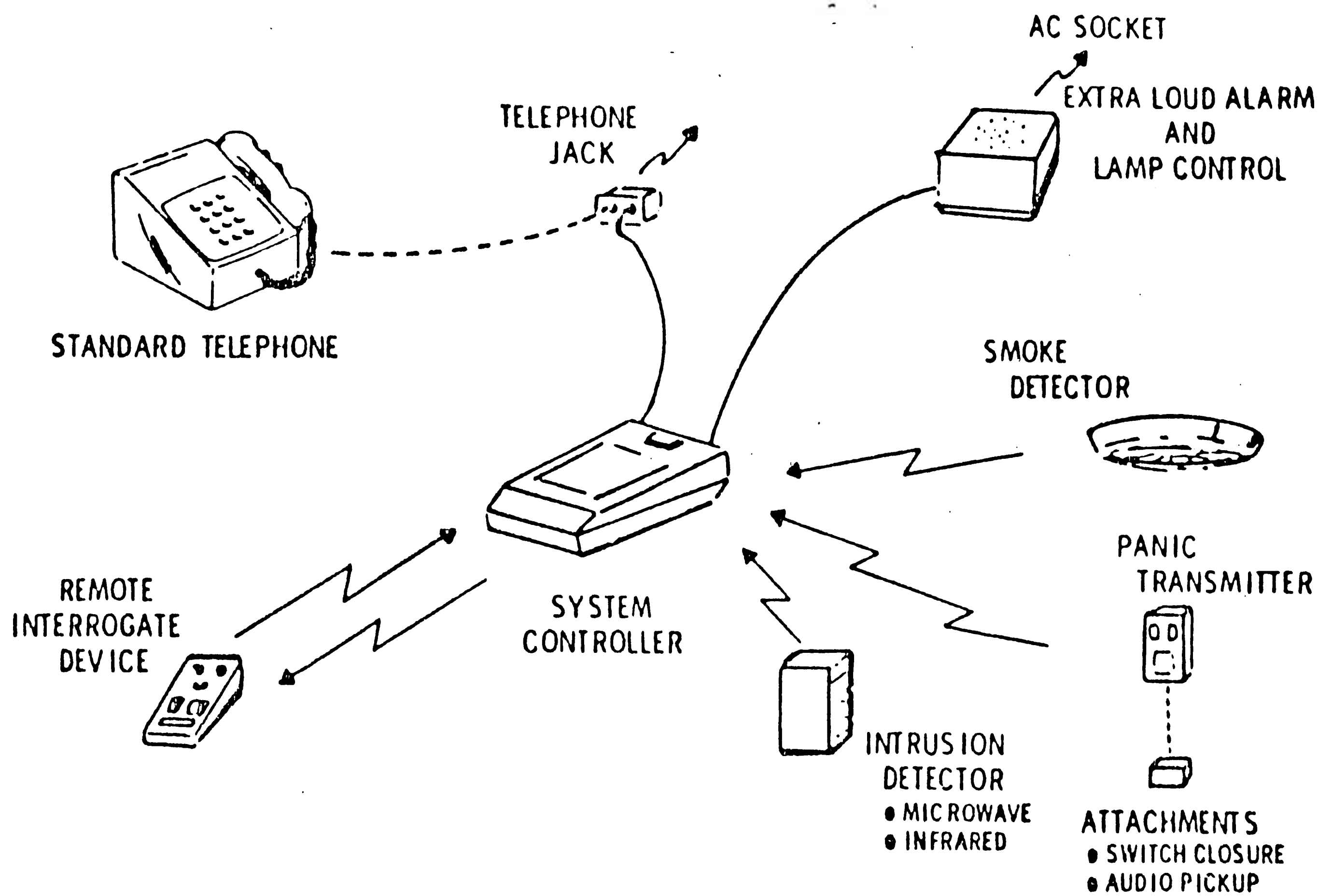
COMPARISONS WITH THE TICOM SECURITY SYSTEM

This Appendix compares the features and hardware of the HCSS and the stand-alone TICOM security system.

Our market research to date has shown that there is a large mass market for an inexpensive, brand-name home security system. Central to the success of such a product is its ability to meet the security concerns of home dwellers as enumerated in Section 3.0 of the HCSS report. The price resistance lies in the $500.00 range for a full system. This rules out using anything like the home computer. It also rules out the two-way communications between the Security Controller (SC) and the sensory devices because of the cost of the sensory receivers required. In order to meet some of the dweller concerns mentioned, a PST must be offered. This device is almost identical to the one offered with the HCSS.

As part of the Telephone Interconnect Communications (TICOM) stategy, the Personal Communications Department has proposed a stand-alone home security system. (The other TICOM products are telephone accessories and a cordless telephone.) This system, illustrated in Figure B-1, consists of fire and intrusion sensors that contain RF transmitters. Upon activation, either by the sensor itself or manually by depressing the test button, these devices initiate a 1-second digital FM transmission identical to that of the HCSS sensory devices. The devices re-transmit twice at 32-second intervals for added reliability. The only way to determine the condition of the battery is to depress the test button.

Upon reception of a sensor transmission, the SC decodes its ID, waits 30 seconds and confirms it by decoding that sensor's next transmission. The device then forwards the alarm condition by autodialing the appropriate telephone number and delivering a synthesized voice



- FREQUENCY: 300 MHz
- RANGE: 150FT

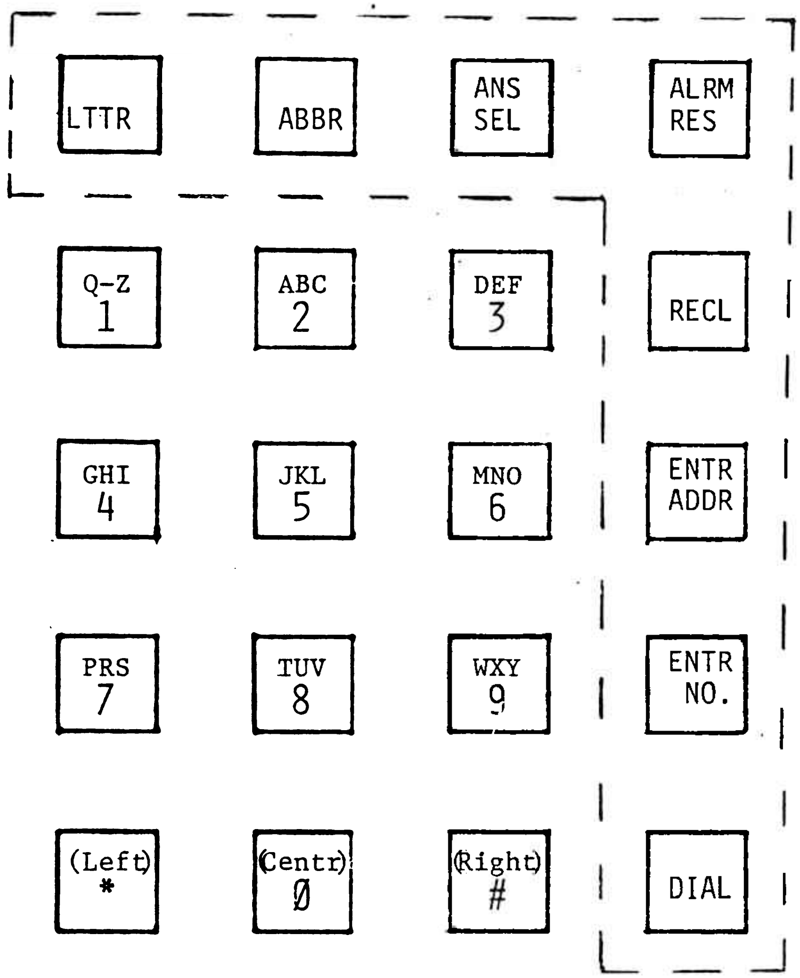
FIGURE B.1 - TICOM SECURITY SYSTEM

message. Cycle dialing of three numbers is provided as in the HCSS. The SC will also answer the phone automatically and deliver phone-answer messages in sythetic voice.

To allow the user to enter the street address, his emergency phone numbers, and the phone-answer messages which he desires, the SC has a 20-key entry keyboard and an eight-digit LED numeric display. The layout of the keyboard is shown in Figure B-2, along with phone number storage assignment. Entry of the street address is accomplished using the same abbreviations as in the HCSS (see Figure 11). Letters are entered using the two-stroke key sequences of Figure B-3.

Of the features listed in Section 9.0 for the HCSS, all except the programmable daily activation and deactivation and the automatic self-testing and diagnosis, both very outstanding features of the HCSS, are provided by the TICOM security system. Retail of a typical TICOM system is estimated at $600.00, while that of a typical HCSS is estimated at $1200.00. See Figure B-4 for the respective breakdowns of these estimates.

As can be seen, the HCSS and the TICOM security system target different segments of the buying public. In fact, they relate to each other in the marketplace in just the same manner as the current TI Professional calculators and TI low-cost four-function calculators do. Yet, the significant amount of synergism produced by both these security lines shall yield good manufacturing economies, however difficult the quantitative prediction of these may be.



These are the command keys and are of a different color (yellow) than the rest (gray).

LTTR	-	(Letter)
ABBR	-	Abbreviations for street address
ANS SEL	-	Answer Select
ALRM RES	-	Alarm Reset
RECL	-	Recall
ENTR ADDR	-	Enter Address
ENTR NO.	-	Enter Number

FIGURE B.2 - TICOM SECURITY CONTROLLER KEY LAYOUT

Twenty phone numbers can be stored in locations 1 through 2Ø.

Emergency phone numbers are assigned to locations 1 through 9:

> Fire alarm numbers are in locations 1, 2, and 3: intrusion alarms numbers are in 4, 5, and 6; and personal emergency numbers are in 7, 8, and 9.

Sample key-stroke sequence for storing "747-3731" as the second phone number that the controller would dial in case of a personal emergency alarm :

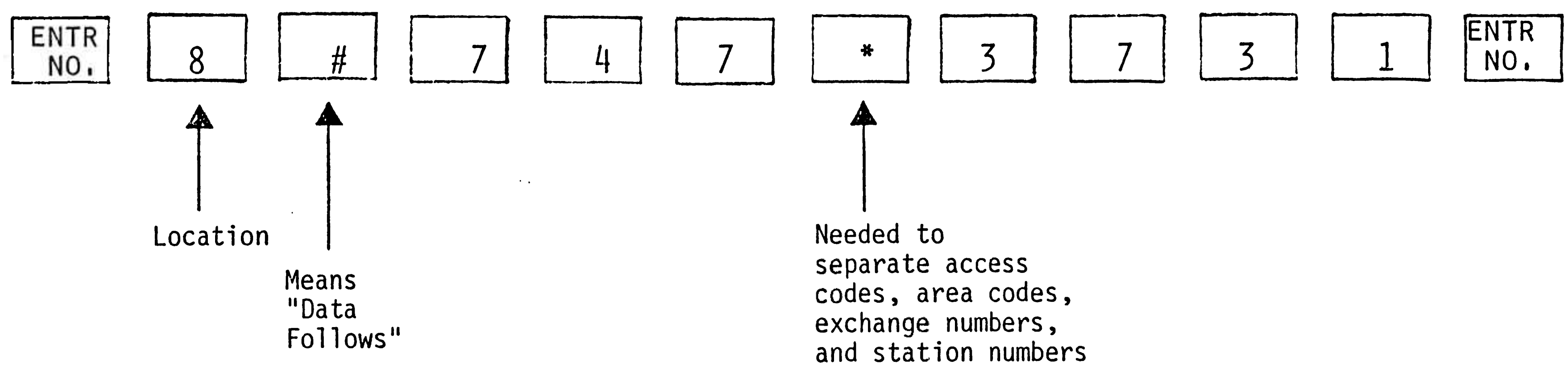
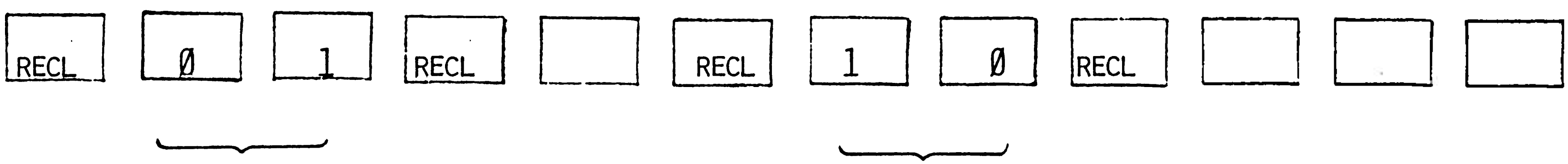


FIGURE B.2 - CONTINUED

Sample key-stroke sequence to recall a phone number:



Recalls phone number in location 1.

Recalls phone number in location 1Ø.

Speed dialing is accomplished using the dial key in place of the recall key in above sequence.

FIGURE B.2 - CONTINUED

Sample key-stroke sequence for selecting the following phone answer message:

"We may be reached at 747-3731; Please call back at 10:30."

Phrase #2 ("We may be reached at 747-3731;") — Phrase #4 ("Please call back at 10:30.")

ENTR NO.	ANS SEL	2	#	7	4	7	*	3	7	3	1

ANS SEL	4	#	1	Ø	*	3	Ø	ENTR NO.

FIGURE B.2 - CONTINUED

Sample key-stroke sequence for entering "235 East Lovers Lane, Apt. 25" as the street address:

ENTR ADDR	2	3	5	ABBR	Ø	3	ALPHA	#	5	#	6
#	8	Ø	3	Ø	7	#	7	ABBR	#	5	Ø
6	ABBR	*	2	*	7	ENTR NO.	2	5	ENTR ADDR		

FIGURE B.2 - CONTINUED

TWO-STROKE LETTER ENTRY USING TOUCH TONE NUMERIC KEY PAD.

A	-	*2
B	-	Ø2
C	-	#2
D	-	*3
E	-	Ø3
F	-	#3
G	-	*4
H	-	Ø4
I	-	#4
J	-	*5
K	-	Ø5
L	-	#5
M	-	*6
N	-	Ø6
O	-	#6
P	-	*7
Q	-	*1
R	-	Ø7
S	-	#7
T	-	*8
U	-	Ø8
V	-	#8
W	-	*9
X	-	Ø9
Y	-	#9
Z	-	#1
SPACE	-	Ø1

FIGURE B.3 - TWO STROKE ALPHABET SEQUENCES

TYPICAL TICOM SYSTEM			TYPICAL HCSS*		
1	SECURITY CONTROLLER	$185.00	1	SPC	$300.00
1	SMOKE DETECTOR	50.00	1	SMOKE DETECTOR	75.00
1	MOTION DETECTOR	50.00	1	MOTION DETECTOR	75.00
1	PST	60.00	1	PST	60.00
7	INTRUSION TRANSMITTERS	210.00	7	MAGNETIC SWITCHES WITH TRANSCEIVERS	350.00
7	MAGNETIC SWITCHES	25.00	1	POLL-MONITORING DEVICE	60.00
		$ 580.00			$920.00
				HOME COMPUTER & GROM	330.00
					$1250.00

*THIS HCSS IS INTENDED ONLY TO PROVIDE THE SAME SENSOR CAPABILITY AS THE TICOM SYSTEM LISTED HERE AND THUS INDICATES THE PRICE DIFFERENTIAL TO OBTAIN THE ADDED RELIABILITY AND CONVENIENCE OF AN HCSS OVER TICOM. IN ACTUALITY, A TYPICAL HCSS IS LIKELY TO INCLUDE TRAFFIC COUNTERS AS WELL AS OTHER SENSORS AND WOULD END UP RETAILING AT ABOUT $1500 - $2000.

FIGURE B.4 - RETAIL PRICE COMPARISON OF TICOM AND HCSS

APPENDIX C

SENSOR BATTERY LIFE CALCULATIONS

There are three battery-drain modes in each sensory device: time-keeping, receive, and transmit. The current drains associated with each of these is specified at 10 μA, 10 mA, and 100 mA, respectively.

From the timing diagrams of Figure 3 in the main body of this report, the following duty cycles are established:

Timekeeping -	1 sec./1 sec.	= 1.00000
Receive -		
Timing pulses:	0.25 sec./512 sec.	= 0.00049
Updates (4/day):	4 sec./24 hrs x 1 hr/3600 sec.	= 0.00005
		0.00054
Transmit -	4 sec./24 hrs x 1 hr/3600 sec.	= 0.00005

Therefore, the total battery drain per day is found by multipling each duty cycle by 24 hours/day and its corrsponding current drain and adding these:

Timekeeping -	1.00000 x 24 hrs/day x .010 mA	= 0.240 mAh/day
Receive -	0.00054 x 24 hrs/day x 10 mA	= 0.130 mAh/day
Transmit -	0.00005 x 24 hrs/day x 100 mA	= 0.120 mAh/day
Total Battery Consumption		= 0.490 mAh/day

Using primary Alkaline cells with 400 mAh capacity, this translates into a battery life of two years and 2.8 months. Initializing system timing will degrade this by 0.039 mAh (∿ 4 days) each time. Depressing the test button or triggering the sensor degrades the battery life each time by between 0.03 and 0.15 mAh, depending on the number of re-transmissions required. Thus initialization of the system, triggering of a sensor, or testing of a sensor can occur as often as once every four days while maintaining the battery life at no less than two years.

The preceding calculations do not apply to PSTs. As mentioned in the report (see Section 5.0), these devices do not keep time. Therefore, their operation is strictly transmit and receive as described in Section 5.0. Thus for the PST drain calculations, we have:

Receive duty -	2 sec./2 hrs x 1 hr/3600 sec.	= 0.00028
Transmit duty -	1 sec./2 hrs x 1 hr/3600 sec.	= 0.00014

So,

Receive drain -	0.00028 x 24 hrs/day x 10 mA	= 0.0672 mAh/day
Transmit drain -	0.00014 x 24 hrs/day x 100 mA	= 0.3360 mAh/day
Total Battery Consumption		= 0.4032 mAh/day

This translates into a battery life of two years and 8.6 months. Thus, the PST can be activated as often as once every two hours while maintaining the battery life at well over two years. In fact, a battery life of two years can be maintained if the PST is not activated more often than once every 1.5 hours.

All the above figures confirm that adequate frequency of operation can be allowed on the sensory devices while still guaranteeing a two-year minimum sensor battery life. (Note that a separate battery pack is required to power the motion detector.)

APPENDIX D

LEGAL QUESTIONS ON PRODUCT LIABILITY

This Appendix consists of a copy of a memo from the TI legal department in response to our questions to them on the manufacturer liability issues, if any, associated with fire and burglar alarm products.

M E M O R A N D U M
July 17, 1978

TO: Hugh Barnes

FROM: Robin Green

SUBJECT: Potential Liability for Smoke/Burglar Alarm

Bill Fargo asked that I research the legal issue of TI's potential liability for the new smoke/burglar alarm, should the alarm fail to work during an emergency and the consumer suffer economic loss from a burglary or fire.

Regarding the burglar alarm, case law indicates that TI would probably not be held liable for the economic loss of a burglary in the event the alarm was defective and failed to work.

As for the smoke alarm, however, the case law is less clear. Should a TI smoke alarm fail to work, TI would have fairly good arguments that it should not be liable for any resulting fire damage because (1) the defective alarm did not cause the fire, and (2) our warranty disclaims liability for consequential damages. However, the effectiveness of these arguments is difficult to predict in view of the fact that courts tend to favor consumers in product liability cases.

In short, our disclaimer of consequential damages in our warranty affords us about the best protection against liability as is possible, next to a totally bug-free product.

Robin Green

Robin Green

kw