DISTRIBUTED REAL TIME SIGNAL PROCESSING FOR CELLULAR AND PAGING TRAFFIC ANALYSIS, FRAUD DETECTION, AND INTELLIGENT WIRELESS NETWORK CONTROL

Scott L. McCulley
Research and Development
TSR Technologies, Inc.
P.O. Box 10727
Blacksburg, VA 24062

Theodore S. Rappaport
Mobile and Portable Radio Research Group
Bradley Department of Electrical Engineering
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061

ABSTRACT
This paper describes the control language and common data interface for a real-time digital signal processing (DSP) receiver. This receiver decodes TDMA, AMPS or ETACS cellular digital control channels and blank and burst data in real time, and also decodes POCSAG, GOLAY, and NEC digital paging traffic, including POCSAG 2400 bits per second. The receiver also serves as a digital signal strength measurement system over the frequency range of 25 MHz to 2000 MHz. We describe a low level serial interface standard for the DSP receiver, and discuss techniques which allow multiple DSP receivers to be remotely controlled by a single controller. This arrangement of remote receivers can be configured to measure and respond to real-time multiple-channel traffic on cellular and paging channels for market studies, adaptive RF coverage and control, fraud detection and abatement, and law enforcement applications. With a standardized control language, the receiver system described in this paper can be used for a wide range of custom applications for cellular, paging, and personal communication network (PCN) measurement and control, as well. Extensions of this receiver system allow real-time measurements of cellular control traffic or ERMES paging data to timing accuracies of a millisecond.

I. INTRODUCTION
In expanding cellular radio markets, it is becoming necessary to measure traffic activity so that systems can be adjusted to provide coverage where subscribers are most in need of service. In urban cellular markets, changing traffic patterns, volatile shifts in user demands, and migration from mobile to hand-held portable cellular phones require that near real-time control of the cellular telephone system be provided in order to exploit potential local increases in demand with fixed resources. Also, wireless system providers are requiring flexible, portable measurement systems that allow engineers to rapidly determine cellular or paging coverage needs, system faults, areas of traffic congestion, and customer usage profiles. Fraud is also a concern to cellular carriers and is becoming a major problem in the cellular radio community. In the U.S. alone, the Cellular Telephone Industry Association estimates that over $1 million in revenue is lost to fraudulent cellular users every day [1]. Wireless communications has also been increasingly involved in criminal activities, and sophisticated tools are needed to combat criminal use of cellular telephones and pagers.

Furthermore, the ability to scan banks of radio spectrum rapidly is becoming important for cellular systems which employ new dynamic channel allocation algorithms, and for personal communication systems which will share spectrum with fixed microwave users. An inexpensive measurement system with flexible bandwidths and rapid scan rates could be used within a real-time dynamic allocation strategy for wireless services in shared-spectrum applications.

A new DSP receiving system [2,11] which provides all of the capabilities listed above is available in a single, portable receiver. CELSCOPE is a real-time cellular system monitor that provides real time cellular radio demodulation, decoding, and data transmission. PAGETRACKER is a real-time digital paging and spectrum scanning receiver that provides real time paging demodulation, decoding, and data transmission, and also provides autonomous spectrum scanning and power measurement features. POWERTRACKER is a high resolution measurement receiver that provides a scan rate of 20 frequencies per second with radio signal strength indication (RSSI) accuracies within +/-1 dB over a 1 GHz bandwidth. The receiver bandwidth and demodulation is selectable through the serial interface, and may be specified to be AM, SSB, and FM using bandwidths of 3 kHz, 15 kHz, 25 kHz, 30 kHz, or 150 kHz. In addition, a 3 MHz wide IF port is provided. All three receiving systems may be incorporated into a single receiver (an Icom R7000) through use of a custom DSP system which is installed within the receiver. The resulting receiver provides a serial data stream of 19.2 kilobits per second which conforms to the RS-232 standard. It is well suited to portable applications, and may be controlled by a standard personal computer, or remotely controlled using a dedicated microwave link or standard telephone modems capable of supporting a 19.2 kilobits per second RS-232 link.

In this paper, we present an open data format for communication between the CELSCOPE/PAGETRACKER/POWERTRACKER receiver and a controller. For brevity, this paper considers the basic low level interface between the CELSCOPE/PAGETRACKER/POWERTRACKER DSP receiver and a single controller, and extensions to multiple units can be made easily using standard Universal Asynchronous Receiver-Transmitter technology (as described in Section II).

1. CELSCOPE, PAGETRACKER, and POWERTRACKER are registered trademarks of TSR Technologies, Inc.
II. SERIAL DATA SPECIFICATIONS

Serial data is transmitted at 19.2 kilobytes per second both to and from the DSP receiver. The serial data is transmitted without hardware handshaking. The CELLSCOPE/PAGETRACKER/POWERTRACKER system receives and simultaneously demodulates 10 kilobits per second cellular AMPS or TDMA (or 8 kbps cellular ETACS data), 2400 bps POCSAG, 1200 bps POCSAG, 512 bps POCSAG, 256 bps POCSAG, GOLAY 300/600 bps and 200 bps NEC digital paging data. All blank-and-burst data is received on any cellular channel, as well. With all cellular data transmissions, the receiver performs majority vote decoding for each complete word of every cellular transmission. If a cellular data transmission does not pass the majority vote test, the receiver does not pass the corrupted data to the serial interface [3]. For digital paging data, the receiver performs parity error checking and passes the decoded page and an error bit over the serial interface for each decoded paging word. The host computer or controller is responsible for receiving and buffering all serial interface data from the DSP receiver. Since standard personal computers have UARTs connected to their serial ports (COM ports), this is a simple task, and is readily accomplished by commercial PC software packages [4,5,6].

Duplex serial data transmission between the DSP receiver and the host controller is configured with 1 start bit, 8 data bits, 1 stick parity bit, and 1 stop bit at 19.2 kbps. Some early personal computers do not support stick parity serial transmissions. The CELLSCOPE/PAGETRACKER/POWERTRACKER receiver sends over the RS-232 two types of information: cellular/paging/diagnostic data and radio signal strength indicator (RSSI) data. These two types of information are distinguished by the stick parity bit.

Cellular, paging, and diagnostic data are sent from the receiver with no serial parity error bit, and RSSI data is sent from the receiver with a serial parity error bit. By testing the stick parity bit, the host can differentiate between on-the-air data and signal strength information. The DSP receiver accepts control data from the host with stick parity low. Cellular, paging, and diagnostic data require more than eight bits of data in order to synchronize on the start of the data word with the most significant bit (see the F bit in Figure 1). To synchronize, the receiver searches the first bit of all off-the-air data transmissions to find the first byte of the data word. The F bit is a logic one to indicate the start of a data word and logic zero otherwise. The CELLSCOPE and PAGETRACKER receivers are configured such that in any receiver decoding mode (e.g. forward control channel for cellular), there is a specific number of data bytes sent over the RS-232 interface which make up a single off-the-air data word. Off-the-air data words have different lengths, depending on the standards defined by the cellular and paging industries [3, 7, 8, 9, 10]. By using the F bit, and knowing the receiver mode, the host can use a simple counter to determine when a complete data word can be constructed from several serial data transmissions. The number of serial data bytes required in each receiver mode is described in Sections IV-VI.

When the receiver decodes cellular data or provides diagnostics to the host, the host is responsible for knowing what mode the DSP receiver is in. During digital paging reception, several different paging standards are decoded simultaneously, so a descriptive lead byte is sent from the receiver to indicate which type of paging standard is being decoded. Section V provides more detail about the descriptive byte.

III. RECEIVER CONTROL DATA

The radio receiver control data is the information sent serially from the host computer to the DSP receiver interface. The control data must be sent to the radio in the following order: the decode byte, five frequency bytes, the two receiver mode bytes, and the end byte. The decode byte, five frequency bytes, and two receiver bytes are described below. The end byte is simply the byte value FF and indicates the end of the serial control data stream from the host. The control data may also be sent in two abbreviated forms. These two abbreviated control streams may either be a) the decode byte, the five frequency bytes, and the end byte, or b) the decode byte and the end byte. As a precaution, it is often useful to insert small delays, on the order of 1 millisecond, between every byte in the control data stream, to allow the DSP receiver to interpret control commands from the host.

III. A. DECODE BYTE

The decode byte informs the DSP receiver whether to decode cellular, paging, or DSP receiver diagnostic data. Table 1 show all possible decode bytes (in hexadecimal).

<table>
<thead>
<tr>
<th>Decode byte</th>
<th>Receiver mode</th>
<th>Mode type</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>FCC decode</td>
<td>Cellular</td>
</tr>
<tr>
<td>01</td>
<td>FVC decode</td>
<td>Cellular</td>
</tr>
<tr>
<td>02</td>
<td>RCC decode</td>
<td>Cellular</td>
</tr>
<tr>
<td>03</td>
<td>RVC decode</td>
<td>Cellular</td>
</tr>
<tr>
<td>40</td>
<td>Auto detect decode</td>
<td>Paging</td>
</tr>
<tr>
<td>41</td>
<td>POCSAG decode</td>
<td>Paging</td>
</tr>
<tr>
<td>42</td>
<td>GOLAY decode</td>
<td>Paging</td>
</tr>
<tr>
<td>43</td>
<td>NEC decode</td>
<td>Paging</td>
</tr>
<tr>
<td>7E</td>
<td>Diagnostics</td>
<td>Diagnostic</td>
</tr>
</tbody>
</table>
A decode byte of 00 through 03 instructs the receiver to decode cellular data. A decode byte of 40 instructs the receiver to decode paging in an auto detect mode, which allows the receiver to intelligently decode the proper paging standard in real time. A decode byte of 41, 42, or 43 forces the receiver to only recognize the particular paging format. A decode byte of 7E instructs the receiver to send a serial diagnostic word. The cellular, paging, and diagnostic formats are described in Sections IV - VI.

The CELLSCOPE/PAGETRACKER/POWERTRACKER receiver allows the host to control the status of the audio speaker. The most significant bit of the decode byte controls whether the speaker is active (high) or muted (low). Using Table 1, it is clear that to decode the forward voice channel of a cellular transmission with the speaker on, the host should send the decode byte value of 81. To turn the speaker off the decode byte would be 01.

### III. B. Five Frequency Bytes

The five frequency bytes contain 10 binary coded decimal digits (BCD) representing the desired frequency in Hz. A BCD value requires 4 bits, thus each byte contains two BCD digits. The host must send the five frequency bytes in the following manner: first the two least significant digits of the frequency are sent, and then the more significant BCD digits are sent, and so on. In each byte, the most significant BCD digit of the two is placed in the upper four bits of the byte. This is best described with the following example. The five frequency bytes required to set the receiver to 931.827500 MHz are, in sequential order, 00 75 82 31 09. The CELLSCOPE/PAGETRACKER/POWERTRACKER receiver has two continuous frequency ranges, one from 25 MHz to 999.9999 MHz and another from 1025 MHz to 1999.9999 MHz, controlled by a front panel switch. The receiver has 100 Hz resolution and accepts frequencies ranging between 25 MHz and 999.9999 MHz.

### III. C. Two Receiver Bytes

The two receiver bytes control the demodulator used by the DSP receiver. The possible demodulation types and bandwidths are FM (selectable between 25 kHz, 30 kHz, or 150 kHz), FMN (selectable between 6 kHz, 15 kHz, 25 kHz, or 30 kHz), SSB (3 kHz), and AM (6 kHz). In addition, there is a 3 MHz passband output at an IF of 10.7 MHz, for future DSP applications. To decode the frequency-shift keyed cellular or paging transmissions, the CELLSCOPE/PAGETRACKER/POWERTRACKER receiver demodulates the frequency shift keying (FSK) using FM or FMn demodulators, although any demodulation format provides digitized signal strength (RSSI) data to the host computer (see Section VII). The two receiver bytes consist of a high byte and low byte. The low byte must be sent first. Table 2 below shows the required high/low receiver byte pair to set a desired demodulation type.

**Table 2: Two Receiver bytes for desired demodulation**

<table>
<thead>
<tr>
<th>Low byte</th>
<th>High byte</th>
<th>Demodulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>00</td>
<td>FM</td>
</tr>
<tr>
<td>05</td>
<td>02</td>
<td>FMn</td>
</tr>
<tr>
<td>02</td>
<td>00</td>
<td>AM</td>
</tr>
<tr>
<td>05</td>
<td>01</td>
<td>SSB</td>
</tr>
</tbody>
</table>

### IV. Cellular Decoding

The decoded cellular data is sent by the DSP receiver to the host using the most significant bit first, so that the 28 bit data block (for AMPS, TDMA, and ETACS forward channels) or 36 bit (AMPS, TDMA, and ETACS reverse channels) block can be constructed easily by the host. The AMPS and ETACS cellular standards include additional parity error bits which are transmitted on the air along with the data, but the DSP receiver uses these parity error bits to correct errors which occur on the RF propagation path. If the data has errors which cannot be corrected, then the corrupted data block is not sent to the host by the DSP receiver. Figure 1 shows all the bits that are transmitted to make up one complete data block. Note that the first bit of every byte is the F bit described in Section I.

**FCC-Forward Control Channel**

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Bytes 2 - 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 W 1</td>
<td>Reserved 01</td>
</tr>
<tr>
<td># of bits</td>
<td>1 1 6 1 7</td>
</tr>
</tbody>
</table>

**FVC-Forward Voice Channel**

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Bytes 2 - 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 01</td>
<td>Reserved 01</td>
</tr>
<tr>
<td># of bits</td>
<td>1 1 6 1 7</td>
</tr>
</tbody>
</table>

**RCC-Reverse Control Channel or RVC-Reverse Voice Channel**

<table>
<thead>
<tr>
<th>Byte 1</th>
<th>Bytes 2 - 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 01</td>
<td>data 01 01</td>
</tr>
<tr>
<td># of bits</td>
<td>1 1 6 1 6</td>
</tr>
</tbody>
</table>

Figure 1. Cellular Data Transmission from DSP receiver to the host. Note that the first byte of every cellular data block contains a logical 1, denoting the F bit.

In Figure 1 for the FCC, W indicates which of the two interleaved data streams the FCC byte is from. Cellular standards dictate that the FCC is interleaved so that subscriber phones only need to listen to half of the FCC data.
message. Phones with even mobile identification numbers (MINs) listen to the A stream, and phones with odd MINs listen to the B stream. Bit W is 0 if the data came from the A stream and is 1 if the data came from the B stream. When CELLSCOPE/PAGETRACKER/POWERTRACKER is in the FVC mode, the W bit has no meaning in AMPS and ETACS because only one mobile is listening to that channel, thus the W bit is zero.

For example, suppose the receiver is in the FCC mode and receives a string of data bytes, in order: 7A, C0, 4F, 3D, 49, 0E, 80. This is decoded to a 28 bit data block from the B stream as 10011110111010010001110 in base 2 or 9EF648E in base 16. Note that the first byte, 7A, does not have the F bit set but byte C0 does, so C0 is the first byte of the five FCC data bytes. Also note that 80 is beginning of the next FCC data word on the A stream. The translation of the 28 bit or 36 bit data word is a simple matter of comparing, masking, and matching the data words received on the known channel type (FCC, FVC, RCC, and RVC) to the fully described standards [3, 7] for AMPS, TDMA, and ETACS.

V. Paging

Paging data is sent in eight byte data blocks. The first byte is a descriptive byte which has the F bit set to one. The following seven bytes in each block are data bytes, each byte containing 7 bits of data, with the F bit set to zero in each of the seven bytes. See Figure 2 below for byte order and bit placement of a paging data block.

Table 3: Descriptive format byte meaning

<table>
<thead>
<tr>
<th>Descriptive format byte</th>
<th>Type of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>POCSAG 256 baud</td>
</tr>
<tr>
<td>81</td>
<td>POCSAG 512 baud</td>
</tr>
<tr>
<td>82</td>
<td>POCSAG 1200 baud</td>
</tr>
<tr>
<td>83</td>
<td>POCSAG 2400 baud</td>
</tr>
<tr>
<td>A0</td>
<td>GOLAY Preamble</td>
</tr>
<tr>
<td>A1</td>
<td>GOLAY Pager Address or Activation</td>
</tr>
<tr>
<td>A2</td>
<td>GOLAY Message Block</td>
</tr>
<tr>
<td>A3</td>
<td>GOLAY Comma Block</td>
</tr>
<tr>
<td>E3</td>
<td>End of GOLAY block</td>
</tr>
<tr>
<td>90</td>
<td>NEC page</td>
</tr>
</tbody>
</table>

Byte 1. Descriptive format byte

1 | format

# of bits 1 7

Bytes 2 - 8. Seven bytes

01 data

# of bits 1 7

Figure 2. Paging data blocks generated by the CELLSCOPE/PAGETRACKER/POWERTRACKER receiver for the host computer.

The descriptive format byte is the first byte in each eight byte paging data block. It describes the type of data that follows in the remaining seven data bytes. Table 3 below lists all possible descriptive format bytes that can be transmitted. Note the byte value in Table 3 includes the F bit being set.

Each paging standard is extensively documented in [8],[9], and [10] and the reader should consult these references to translate the digital data into capcodes and messages (alpha-numeric or numeric). A guideline to assist the decoding of the paging data follows.

For POCSAG pages, the CELLSCOPE/PAGETRACKER/POWERTRACKER receiver sends the framing number [8] in the least three bits of the first data byte (byte 2 of the paging data block). The next three data bytes (paging data block bytes 3 through 5) contain 21 data bits. The most significant bit in byte 3 indicates an address codeword (logic 0) or a message codeword (logic 1). The other 20 data bits are sent with the most significant bit first. The last three data bytes should be ignored. The 20 data bits of POCSAG data sent make-up a capcode or message data [8]. By using the most significant bit in byte 2 of the paging block, a capcode and its complete message can be constructed. Each alpha-numeric character requires seven bits and numeric characters require four bits. The POCSAG standard sends characters in reverse bit order, e.g. a numeric character 2 (0010) would be sent as 4 (0100). Refer to [8] for more detail.

For GOLAY pages, the CELLSCOPE/PAGETRACKER/POWERTRACKER receiver sends numerous housekeeping information bytes to the host that provide easy GOLAY paging interpretation. The preamble descriptive format byte indicates that a GOLAY paging burst will follow (begin GOLAY page interpretation). The first data byte contains the preamble which is contained in the least five bits of byte 2 of the paging block. Bytes 3 through 8 of the paging data block for GOLAY preamble should be ignored by the host and have no meaning. Following the preamble data block, the page address or activation data block follows. The address or activation indicators are described and calculated using the GSC coding system [9]. The GSC system requires the preamble (known from the preamble data block) and two GSC words (sent in the data bytes of the paging data block) in order to properly decode a page or a group of pages. Each GSC word is 12 bits long and is contained in two consecutive.
data bytes (6 bits per byte) of the GOLAY address or activation data block. Word 1 is constructed by combining the least six bits in the paging block byte 2 (high six bits) and the least six bits in the paging block byte 3 (low six bits). Word 2 is constructed in the same manner using paging block bytes 4 and 5. Bytes 6 through 8 have no meaning and may be ignored. If a message is sent to a GOLAY pager address, then the next descriptive data block will be a GOLAY message block. The GOLAY message block uses all 7 bytes of the paging data block (bytes 2 through 8), resulting in 49 bits of message data within the paging block. The last byte in the paging block contains the first character of the message. Numeric messages use 4 bits per character and alpha-numeric message use 6 bits per character [9]. The most significant bit in paging packet word 2 indicates if an additional data block will follow (logic 1) or if this data block is the end of the message (logic 0). Additional messages blocks are sent with another descriptive format byte GOLAY message and the message is contained in the 49 data bits that are in the paging block. The GOLAY comma block and GOLAY end byte are described in the standard [9] and are provided to the host by the receiver.

For NEC pages, the first data byte of the paging data block contains the value 90 (hex), indicating a NEC page will follow (see Table 3). The data (address or message) is contained in the paging block bytes 2 through 4 (21 bits of data per NEC data block). Bytes 5 through 8 have no meaning for NEC decoding and may be ignored by the host. The most significant bit in byte 2 indicates if the page is an address used to compute a capcode (logic zero), or a digital message (logic 1) for the most recently sent NEC address. The 20 bit NEC address is decoded into a capcode using an equation described in [10]. The digital message is sent in BCD with the least significant digit in the most significant byte. Each paging data block which is an NEC digital message can only contain 5 digits, so page messages that have more than 5 numeric characters are sent using multiple paging blocks from the receiver to the host. Each block containing the descriptive byte 90 and the most significant bit in paging block byte 2 as logic 1.

All of the decoded paging standards support a tone-only page to any address. This occurs when a pager address is sent with no message. For all paging standards, the pager address is sent before any message data for that particular address.

The DSP receiver is able to accommodate multiple paging standards simultaneously by incorporating idle codewords in the data transmission from the receiver to the host computer. CELLSCOPE/PAGETRACKER/POWERTRACKER sends a unique idle codeword during idle time between pages. Such idle time occurs when a paging transmitter goes off the air, or a particular standard (POCSAG or NEC) transmits known idle words which are interpreted as such by the receiver. For POCSAG, the idle codewords are sent to the host having values ranging between 1EA270 and 1EA277, GOLAY has no idle codewords, and NEC uses the idle codeword 0F5138.

VI. Diagnostics

When the host computer instructs the DSP receiver into the diagnostic mode (see Section III.A), eight serial diagnostic bytes are sent by the CELLSCOPE/PAGETRACKER/POWERTRACKER receiver to the host. The first byte is always A5 (note that the F bit is a logical 1), and the next seven bytes describe various characteristics of the DSP receiver, as described in Figure 3.

Byte 1. First Diagnostic byte
110100101
# of bits 1 7

01A
# of bits 1 7

01b
# of bits 1 7

01c
# of bits 1 7

Byte 5. Authorization Byte
01RRRRRRC
# of bits 1 7

Bytes 6 - 8. Reserved
01XXXXXXXX
# of bits 1 7

Figure 3. Diagnostic bytes sent by the DSP receiver.

The manufacturing version of the DSP receiver is transmitted using three bytes: the major version byte, minor version 1, and minor version 2. When the C bit is set, cellular operation is supported. When the P bit is set, paging operation is supported. The R bits are reserved bits for increased capabilities in new wireless systems which are under development. The X bits indicate any bit value may be sent to the host.

VII. RSSI

Radio signal strength indication (RSSI) data are automatically sent to the host in real time by a single 8-bit byte at a rate of 112 times a second. See Section II for how to differentiate between decode data bytes and RSSI data bytes. The RSSI byte value has either 6 or 7 bits of precision (depending on the CELLSCOPE/PAGETRACKER/POWERTRACKER model number and version number) which is sent in the most
significant bits of the RSSI byte. Thus, bits 8 through 2 of the RSSI byte contain the binary signal strength data, and bit 1 of the RSSI data byte has a value of 0. A byte value of 254 corresponds to the strongest received signal and a value of 0 corresponds to the weakest received signal. The DSP receiver signal strength is linear in dB over a 70 dB dynamic range from -40 dBm to -110 dBm, so a straight line interpolation of the RSSI byte value can be used. Equation 1 shows how the received RSSI byte is converted to a dBm value over a dynamic range of -20 dBm to -130 dBm.

\[
RSSI \text{ (dBm)} = \frac{110 \text{dBm}}{254} \times \text{byteValueReceived} - 130\text{dBm} \tag{1}
\]

The CELLSCOPE/PAGETRACKER/POWERTRACKER receiver provides calibration adjustments so the user can establish accurate RSSI readings over any range.

VIII. Applications

While the DSP receiver described above has an extremely easy-to-use computer interface, and is currently being used in over 100 worldwide markets as a flexible, all-in-one cellular, paging, and PCS system measurement tool [11], there are numerous applications, including distributed processing and fraud abatement, that the above open interface standard will support. Multiple DSP receivers can be connected together at a common base, using landline, microwave radio, or existing T1 channels to support real time RS-232 data transmission. A distributed network of DSP receivers described in this paper, each with their own local controller, could provide real time traffic monitoring, system control and intelligent network support in a wide range of wireless systems.

At each remote receiver, a simple UART and buffer with storage and polling capability is required. Alternatively, distributed processors could be dedicated to one or more DSP receivers. Polling the remote receivers can be performed by a main terminal with a data base manager. The data base could search and give listing of activities on any cellular phone number or capcode. Cellular cloning and illegal ESN/MIN pairs could be determined in real-time by simple radio reception. Paging messages can be detected in real-time for specific messages or parts of messages, and can be used to trigger remote alarms or update displays. Absolutely no hardwire connections to switching equipment or the PSTN is required. Thus, a completely reconfigurable and rapidly deplorable wireless monitor and control system can be installed.

IX. Conclusion

This paper has described the complete serial interface for the CELLSCOPE/PAGETRACKER/POWERTRACKER digital signal processing receiver. The serial interface provides all data necessary to construct a wide range of real-time traffic and signal measurement equipments using a sophisticated, yet inexpensive, DSP receiver as a building block. The paper has laid the technical foundation for system integrators to combine the CELLSCOPE/PAGETRACKER/POWERTRACKER receivers, local and distributed controllers, and data base software to provide true real-time cellular and paging traffic analysis, RF measurements and control, dynamic channel allocation schemes, real-time fraud detection, and law enforcement. The low-level data interface and data formats described here allow any system to communicate with the receiver.

X. Reference


