CHAPTER 1.0 SOFTWARE THEORY OF OPERATION

1.1 Functional System(s) Operation.

1.1.1 Architecture

A single Digital Signal Processor handles all signal processing functions. An H8 microcontroller is used to control the user interface and implement other radio control functions. Functionality partitioning is shown at Figure 1-1.

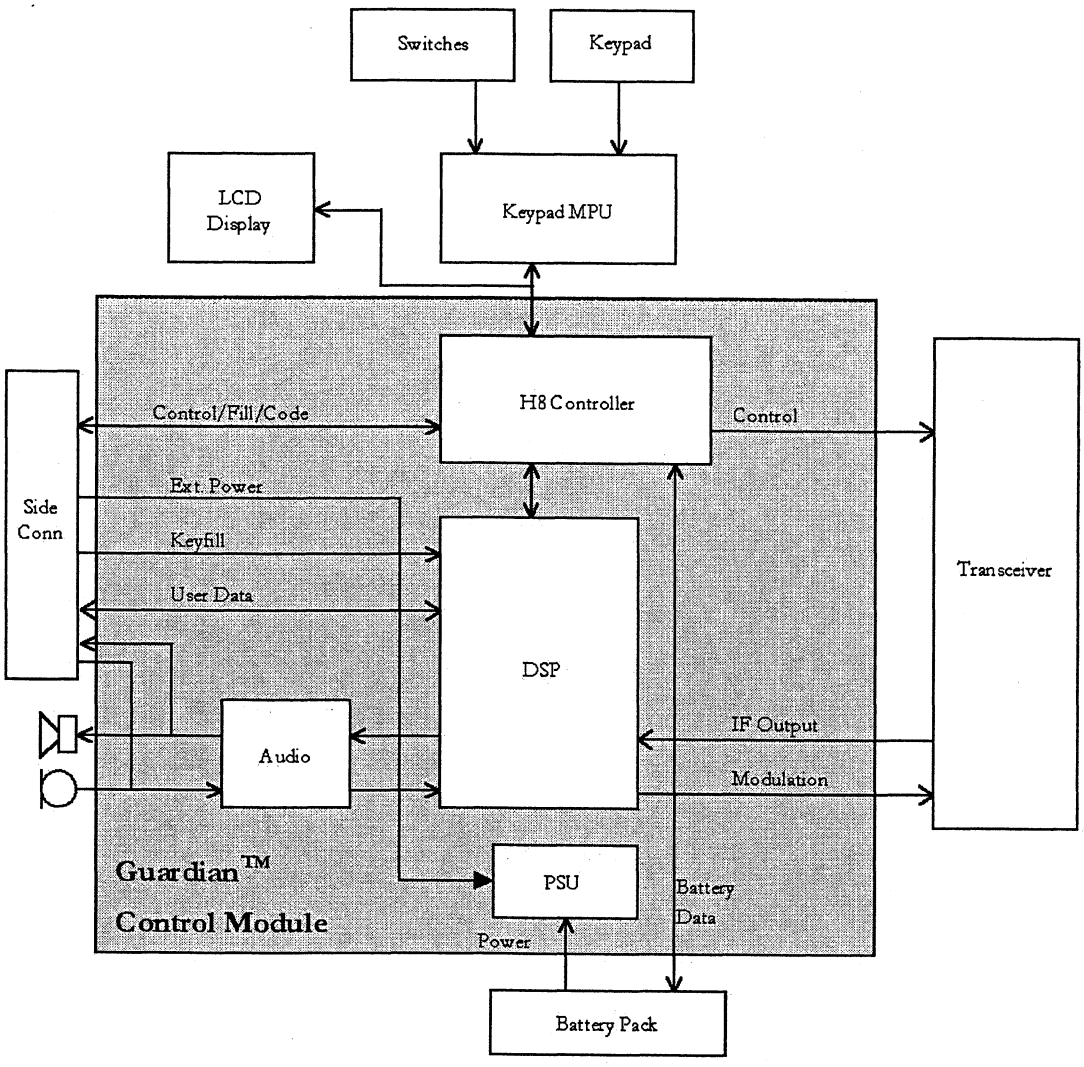

Figure 1-1 Guardian Block Diagram

1.1.2 Module Identification

The control module stores an electronic serial number and modification status within non-volatile storage on the module.

1.1.3 Self-Test on Power-Up

The software executes self-test automatically when the radio is switched on. This test is capable of detecting and identifying faults that prevent the radio from properly operating.

1.1.4 Flash Software Upgrades

The radio software can be updated if required using a PC and the Guardian G25AXG004 PC Programming /Cloning Cable.

1.1.5 Voice Coder/Decoder (VOCODER)

The VOCODER uses an Improved Multi-Band Excitation (IMBE) voice-coding algorithm as specified in Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA)-102.BABA. The IMBE VOCODER compresses a high-bit-rate waveform into a low-bit-rate data stream suitable for transmission over the channel. The VOCODER operates at a net bit rate of 4.4 kilobits per second (kbps) for voice information and a gross bit rate of 7.2 kbps after error control coding.

1.2 Radio Control Software

This software controls the transceiver and baseband signal processing functions.

1.2.1 Audio Control

The H8 controls the analog audio signal processing. Audio for transmission comes via either the internal microphone or an external microphone attached to the side connector. Both are wired in parallel to the microphone amplifier which is permanently powered.

Audio output is required when a voice message is received or a tone is generated by the user interface. To allow audio output, the H8 sets either SPKRON or EXTSPKRON to the internal speaker or the side connector. If an external audio accessory is detected by Who Are You (WRU) < 0.5 VDC, the audio is routed to the side connector. Otherwise audio is routed to the internal speaker. The sixteen-position volume control knob is decoded and sent to the DSP through the controller software to control the output audio volume.

1.2.2 DSP Control Software

The DSP implements most of the baseband signal processing in the radio. Its function is controlled by the H8 controller through its host port. The DSP operates in a number of basic modes, controlled by the H8 through the host port, these are:

- Idle — Current shut-down mode released through the host port.
- Searching — Actively looking for a signal on the IF input signal.
- Searching Paused — Search algorithm paused for an economize cycle or frequency change.
- Active Receive — Actively receiving a message, initiated by detecting a signal or H8 command
- Transmit — Actively transmitting voice or data.
- Key Fill/ — Keyfill operations and key
- Management — management tasks.

The DSP pages-in different program images from the Flash for different modes of operation. Typically one image is used for receive and standby modes, but a new image is needed for transmit and for key management operations. The DSP can interrupt the H8 controller, and then pass data over the host port back to H8. Interrupts from the DSP include the following events:

- Signal detected, with type data.
- Signal lost
- DSP BIT errors
- Paging request

In all active modes the H8 software must be able to write a number of parameters to the DSP and also read back a number of parameters from the DSP. This is implemented through the host port. The parameters used include:

- Searching Reference oscillator temperature, used

by DSP to correct frequency offsets. AGC reset control used at start of search period.

Search modes:
Analog: bandwidth, squelch tones, squelch code, and squelch level.
Digital: data rate, key, and algorithm
Project 25: NAC and TGID
CVSD: data rate

- Receive Reference oscillator temperature, used

by DSP to correct frequency offsets. Audio Volume.
Analog parameters: squelch controls, de-emphasis, and companding.
Digital parameters: data rate and key algorithm.
Project 25 parameters: NAC, TGID, BER, and Test mode.
CVSD: data rate and key
Project 25 parameters read by H8: SS bits, low rate data (future), sender ID

- Transmit Reference oscillator temperature, used

by DSP to correct frequency offsets.
Audio volume, sidetone on/off.
analog parameters: squelch controls and de-emphasis.
CVSD digital parameters: data rate and key
Project 25 parameters: NAC, TGID, key and low-rate data (future).

1.2.3 Transceiver Module

The transceiver module is controlled through a synchronous serial bus from the H8 to the transceiver that allows the H8 to control: the synthesizer; two 4-channel 8-bit DACs; and a control shift register in the transceiver module. Some of the DAC channels are set according to data in the transceiver Electronically Erasable Read-Only Memory (EEPROM) calibration tables.

1.2.3.1 Transceiver Module Mode Control

The transceiver module mode of operation: transmit, receive or standby is controlled by the transceiver shift register and the CTX output of the FPGA. The outputs are controlled as below:

- Spare (SR bit 1)
- 3.3VRXSynth (SR bit 2) Set in active receive mode RXVCO enable.
- 3.3VTXSynth (SR bit 3) Set in active transmit mode, TXVCO enable.
- 3.3VRXEnable(SR bit 4) Set in active receive mode receiver enable
- Spare (SR bit 5)
- Spare (SR bit 6)
- TX/RX (SR bit 7) Set in active transmit mode, front end Tx/Rx control
- STD/SIDE (SR bit 8) Set to use radio antenna, reset to use side connector RF port
- CTX (FPGA output) Set in active transmit mode to enable the RF power amplifier.

1.2.3.2 Transceiver Frequency Control

The frequency of operation in both transmit and receive is controlled by the H8 setting the synthesizer through the serial bus. To set the desired frequency: the appropriate Tx or Rx synthesizer enable S-R bit must be set; the serial data must be loaded into the synthesizer chip; and the DAC2 output A, synthesizer coarse tune, must be set to the appropriate value for the frequency according to the EEPROM calibration table. Synthesizer lock can be monitored by the OOL input. Once synthesizer lock is achieved the transmitter or receiver can be enabled with the appropriate control bits, 3.3VRX enable, CTX and TX/RX. Economizing the synthesizer function is implemented by controlling the 3.3VTXS/RXS bits and by controlling the EM main divider enable bit in the synthesizer control word. The synthesizer serial data need not be reloaded when coming out of economize if the frequency is unchanged.

1.2.3.3 12-Bit DAC

DACLDA, DACADCCLK, and DACDOUT are used to control the 12-bit DAC for IFAGC, TXVCOMOD, REFOSCMOD, and VATT.

1.2.3.4 Transceiver Reference Oscillator Temperature Compensation

The H8 software constantly monitors the reference oscillator crystal temperature using the XTALMON line. The temperature data is then used to lookup a compensation factor in the transceiver EEPROM calibration table. This compensation factor is then written into the DSP when it is added as a DC offset the reference oscillator modulation signal, and used as a DC offset to the same in receive modes.

1.2.3.5 Transceiver Receiver Control

The linear receiver chain is enabled by setting 3.3VRXE. The DSP implements a software AGC system to control the gain of the linear receiver chain. The H8 controller can monitor the actual received signal level by reading RSSI. At all times during receive the RXVTF DAC2 output C must be set to the value in the EEPROM calibration table corresponding to the receive frequency being used. This sets the receiver front end tunable filter to be centered on the desired frequency. At all times in receive modes the 2nd LO DAC2 line output B must be controlled using data from the EEPROM calibration table indexed with the reference oscillator temperature data XTALMON. Temperature compensates the second LO in the receiver chain.

1.2.3.6 Transceiver Transmitter Control

The radio uses a complex H8 software-based algorithm to control the transmit power of the radio dynamically. The inputs to the power control algorithm are:

- The requested power level: 0.1, 0.5, 1, 2 or 5W
- PA calibration data in the EEPROM
- Supply voltage, BATMON - used for monitoring
- The transmit frequency
- PA current - used for monitoring
- PA temperature - used for monitoring
  The power control algorithm takes these inputs and uses them to control the following outputs to provide a steady RF power output with a clean rise and fall at switch on/off.

• PWRSET	Sets the power level in the
• (DAC1 output A)	power amplifier ALC loop.
• PABIAS1	Adjusts the bias in the final
• (DAC1 output B)	driver stage.
• PABIAS2	Adjusts the bias in the final
• (DAC1 output C)	driver stage.

1.2.3.7 Transceiver Tx/Rx Switching

The basic principle of events needed to quickly switch the transceiver module from receive to transmit and back again is to shut down the current mode, lock the synthesizer in the new mode on the new frequency, then enable the transmitter or receiver, as required.

1.2.3.8 Receiver Scanning

In some scanning modes it is necessary for the radio to scan a number of channels looking for traffic, controlled by the H8 software. The basic requirement is to change the synthesizer frequency, and RXVTF and Synthesizer Tune DACs, and resume searching on the new frequency. The DSP may have to be informed of new traffic parameters to search for on each new frequency. Scanning is interrupted when the DSP detects a signal of interest.

1.2.4 DC Power Control

The H8 controller software controls the power supply switching in the radio. The control software algorithm uses the following inputs:

- /PWROFF This input indicates the current position of the radio on/off switch and the side connector off line.
- WRU Indicates if the radio is fitted into a harness providing external power
- /LBOUT Indicates that the supply voltage at the minimum that is required for correct operation.
- BATBUS Battery serial bus indicates whether a Smart battery is connected, and if so its charge state.
- BATMON Indicates the voltage on the main radio supply from battery or external power source.

These inputs are used to control the following FPGA outputs:

- PWRHOLD Set during normal operation, used to hold the radio on regardless of the on/off switch. When PWROFF indicates that a switch off is required, a clean software shut down is executed followed by release of the PWRHOLD output.
- BATOFF This output can be reset to prevent current flowing out into the battery from an external power source. This line is set when the battery indicates it is fully charged and an external power source is being used as the primary radio power.

Additionally the /LBOUT interrupt is used to execute a fast shutdown of the software when the supply voltage drops below that needed for normal operation or when the power source is removed without switching the radio off.

1.2.4.1 Power Supply Frequency Control

The power supply control software controls the switch mode power supply frequency output according the RF frequency being used. The frequency is checked and changed if necessary at every transceiver synthesizer frequency change.

1.2.4.2 Battery Interface

The battery interface software implements a single-wire bi-directional serial interface to the Benchmarq ® power gauge device in the smart battery pack. The battery interface software provides an interface to read the battery voltage register and the compensated available capacity registers in the power gauge. Data is read out of the battery at power up, then at least every minute, and within five seconds of every transmit exit. The battery interface software includes timeouts to start again in case of errors, to cope with the situation where a charger may be accessing the battery at the same time as the radio, and a clash on the serial bus occurs.

1.2.5 Monitoring

The H8 software monitors the following signals:

- Out-of-Lock In all active modes, every 100 ms.
- EPTT/RTS In all modes, every 20 ms.
- RSSI In receive modes, every 100 ms.
- WRU In all modes, every 1 second.
- Battery Volts In all modes, every 5 seconds.
- PA Temp In transmit modes, every 1 second.
- REF Temp In all modes, every 5 seconds.
- PA Current In transmit modes, every 1 second.

1.2.6 Radio Control Drivers

A number of low level software drivers are used by the H8 to interface to the transceiver hardware.

1.2.6.1 Audio/Power Supply Unit (PSU) Driver

A serial interface driver controls the output bits of a serial to parallel output shift register in the FPGA. Clock and data source for this shift register is the same serial port used for the user interface serial bus, but data is directed to the shift register using high-order H8 address lines.

1.2.6.2 Transceiver Serial Bus Driver

A serial interface driver is used to control the transceiver shift register, DAC, and synthesizer. This interface uses a common clock and data line, and three separate strobe lines for each device.

1.2.6.3 Digital Signal Processing (DSP) Host Driver

The H8 software includes a DSP host driver for controlling the DSP mode of operation, and initial start-up code download.

1.2.6.4 BATBUS Driver

The H8 software includes a driver to implement the smart battery serial bus.

1.2.6.5 IIC Bus Driver

The H8 software includes a driver to allow the controller software to read and write to the transceiver EEPROM using IIC protocols. The two lines are general purpose I/O lines controlled on a bit-by-bit basis by the software

1.3 Digital Signal Processing

The DSP software implements all baseband signal processing in the radio. It processes signals between the user audio and data interface, and the transceiver modulation and Intermediate Frequency (IF) interfaces. The signal processing provides compatible analog FM modes, Common Air Interface (CAI) compatible modes, and 12 kbps secure CVSD modes.

1.3.1 DSP Transmit Chain

Signal processing while the radio is transmitting depends on the radio's operational mode. The possible modes are Clear Analog Voice FM, CVSD DES Voice, Project 25 Clear Digital Voice, and Project 25 DES Digital Voice. The DSP Transmit Chain Block Diagram is shown at Figure 1-2. The major signal processing functions of the DSP transmit chain are described in the following paragraphs.

1.3.1.1 Audio Coder/Decoder (CODEC)

The Guardian uses a Texas Instruments ® TLV320-AC36 Audio CODEC. Data is transferred to and from the CODEC using the DSP Enhanced Synchronous Serial Interface (ESSI) 0 port. The data word is sixteen (16) bits long. The first thirteen bits are the two's compliment audio sample, the last three are the volume control word in receive direction (DIN) and are zero padded in the transmit direction (DOUT). The DSP currently sets volume control bits for no attenuation and the volume is controlled by scaling the signal prior to sending it to the CODEC. The sample rate from the CODEC is 8 kilo-samples per second (ksps).

1.3.1.2 Audio Processing Module

The Audio Processing Module receives audio input from the Audio CODEC, applies filtering and Automatic Gain Control (AGC), then transmits it to the mode-specific formatting module. The audio filter has a passband from 300 Hz to 3 kHz. This module also transmits DTMF tones to the Audio CODEC. DTMF over-dial is supported to allow redirection through the phone network via a base station. Data is transferred to and from the CODEC under Interrupt Service Routine (ISR) control.

1.3.1.3 Project 25 Voice Module

The Project 25 Voice Module performs framing and conversion tasks. The framing Function uses it's own task table to build a CAI TDMA frame. This includes compression of the voice signal using the IMBE VOCODER, forward error correction, and encryption. The physical layer task converts a 4.8 ksps dibit data stream into a 48 ksps real sampled waveform, which is then fed to the Modulation Module. The physical layer scales each dibit symbol so that the proper frequency deviation is attained. It also applies raised cosine filtering for control of inter-symbol interference.

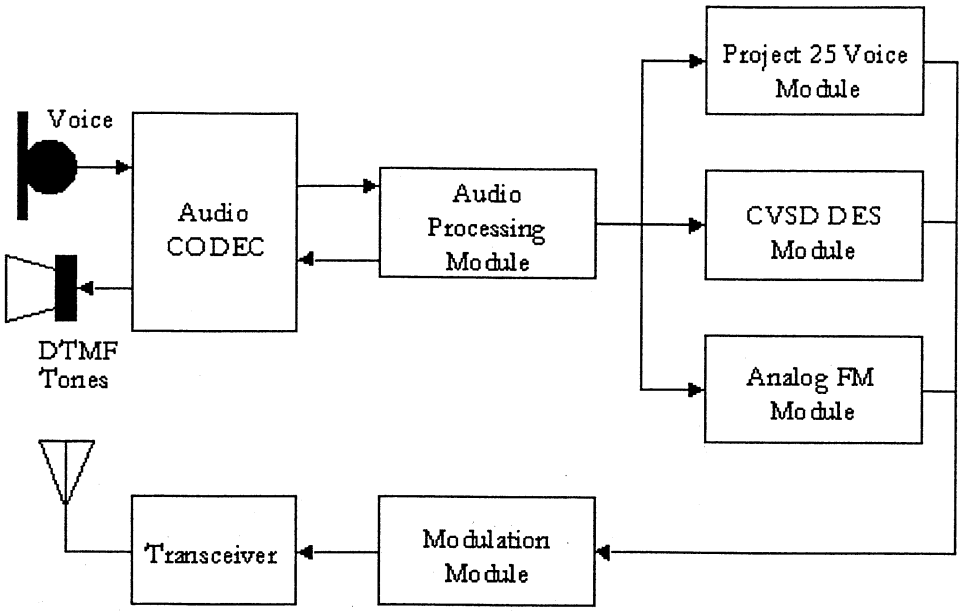

Figure 1-2 Transmit DSP Chain

1.3.1.4 CVSD DES Module

Audio data from the Audio Processing Module is sent to the audio circular buffer. The sample rate is then increased from 8 ksps to 12 ksps. The CVSD encoder encodes the data and sends it to the transmit CVSD audio circular buffer. The data is then DES-encrypted and differentially encoded before being sent to the physical interface buffer. The CVSD physical layer converts the CVSD encoded, DES encrypted 12 ksps data stream into a 48 ksps waveform suitable for processing by the Modulation Module. The module contains a Finite Impulse Response (FIR) raised cosine filter that acts as an interpolation filter. The end of a transmission is signaled by transmitting an End of Message (EOM) indicator, which consists of 160 ms of alternating ones and zeros. This allows the receiving radio to squelch the audio output before the radio stops transmitting.

1.3.1.5 Analog FM Module

Audio data entering the Analog FM Module is sent through a linear-phase, FIR, audio-shaping filter. Interpolation from 8 ksps to 48 ksps is accomplished using a linear-phase, FIR filter. A single-quadrant sine Look-Up Table (LUT), using fractional addressing and quadrant folding, is used to generate CTCSS tones. If the DCS audio turn-off code is to be transmitted, the tone is fixed at 134.4 Hz and the codes are transmitted at a rate of 134.4 bits per second (bps), which is derived using the CTCSS tone generator. The DCS data stream is passed through a raised cosine filter before being added to the speech. The 8 ksps audio stream, with CTCSS/DCS controls, is interpolated to 48 ksps before being sent to the Modulation Module.

1.3.1.6 Modulation Module

Modulation Module prepares the signal for transmission. The signal is split into a reference oscillator signal and a Voltage Controlled Oscillator (VCO) signal. This allows independent scale and offset values for each signal. A modulation balance variable scales the reference oscillator voltage, so that the maximum frequency deviation is constant for all RF channels. A transmit modulation variable does the same for the VCO signal.

1.3.1.7 Transceiver Interface

The transceiver Digital to Analog Converter (DAC) has four output ports, two of which are used to modulate the carrier. One of the two channels is used to maintain carrier frequency accuracy. On transmit channel changes, the controller provides the DSP with two fractional values used to scale the two signals output from the DAC. The controller provides the DSP with an additional integer value at one second intervals, that is added to one of the DAC output signals to control carrier frequency accuracy. The modulation interface receives modulation data samples at

48 ksps, independent of transmit mode. When the radio is operating as a transmitter, the transceiver interface controls the operation of the DAC via ESSI 1 on the DSP. Data is written to the DAC at 96 ksps.

1.3.2 DSP Receive Chain

The radio receive chain hardware consists of an RF transceiver board, Analog to Digital Converter (ADC), a Motorola ® DSP 56302 or DSP 56309, and an Audio CODEC. The DSP Receive Chain Block Diagram is shown at Figure 1-3. The major signal receive functions of the DSP receive chain are described in the following paragraphs.

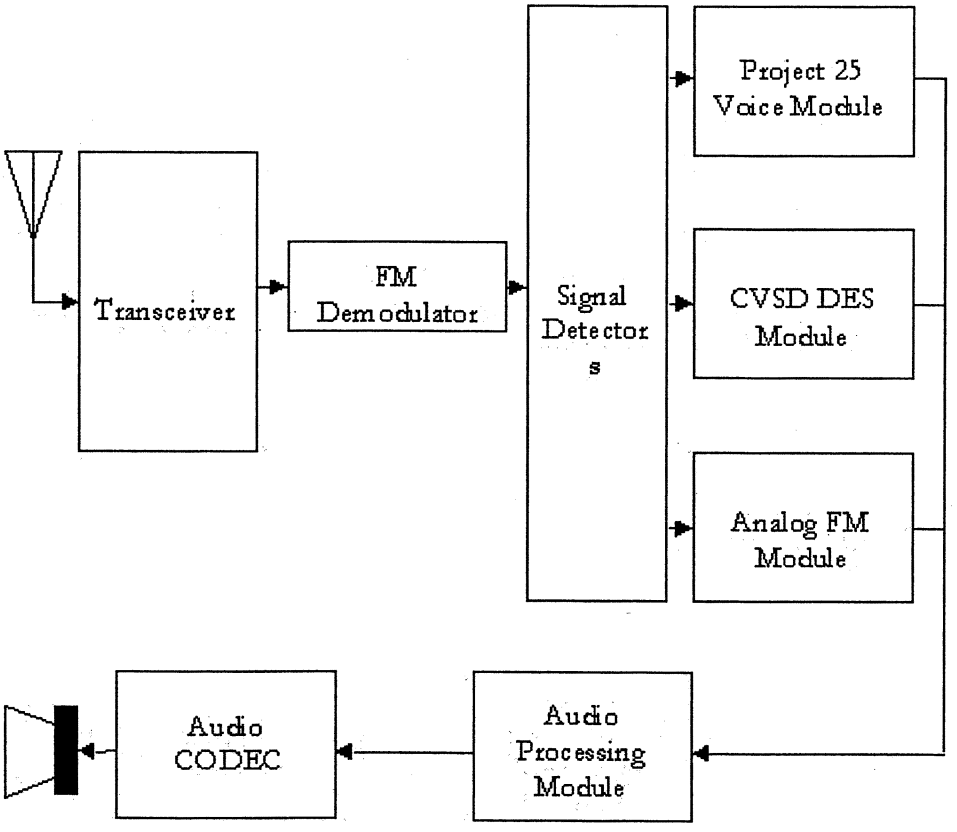

Figure 1-3 Receive DSP Chain

1.3.2.1 Transceiver

The RF transceiver board performs mixing and filtering of the received signal to produce a 455kHz, 25 kHz Bandwidth (BW), IF signal. The output signal from the transceiver is digitized by the ADC and fed to the DSP. The bulk of signal processing is performed by the DSP. An ISR that implements the Transceiver/ ADC/DAC interface is called at a rate of 96 kHz in receive modes. The ISR reads ADC output data and stores the values in a circular buffer and controls data transmission to the DAC.

1.3.2.2 FM Demodulator

The FM Demodulator converts the FM output of the transceiver to a real-valued, baseband signal. The FM demodulation is implemented by a discriminator task. Sub-sampling the 455 kHz IF at 96 kHz folds down the signal to 25 kHz. A mixing function mixes the sampled IF data in the input buffer before filtering, For 12.5 kHz channels, a second filter is applied to the IQ data stream. Calculating the angular difference between consecutive IQ pairs demodulates the received signal.

1.3.2.2.1 Analog to Digital Converter

The ADC sub-samples the 455 kHz first IF producing a frequency translation as part of the sampling process, since the signal BW is much less than the 455kHz carrier frequency. The ADC sampling rate is 96 ksps.

1.3.2.2.2 25 kHz Frequency Translation

The 25 kHz frequency translation converts the signal image into a baseband signal, centered at 0 Hz. DSP implements the digital equivalent of a mixer to perform frequency translation.

1.3.2.2.3 IF Filtering

The complex baseband signal is sent through two linear phase, FIR filters. The first IF filter is implemented as a decimate by two, polyphase, FIR filter and is applied to the 96 ksps, complex, baseband output of the 25 kHz mixer. This filter removes some of the out-of-band noise produced by the nonlinear analog components of the transceiver. CVSD DES and Analog Wide modes have a 25 kHz BW and the first IF filter is the only filtering performed for these modes. Project 25 and Analog Narrow modes have a 12.5 kHz BW, and the second IF filter provides the filtering required for these modes. The second filter is applied to the 48 ksps output of the first IF filter.

1.3.2.3 Signal Detectors

The radio uses three signal detectors to detect the presence or absence of a modulated signal in the tuned channel. These signal detectors search for Project 25, Analog FM (including noise, CTCSS, and DCS), and CVSD DES signals.

1.3.2.3.1 Project 25 Detector

The Project 25 frame detector detects a Project 25 signal by searching for the Frame Synchronization (FS) signal and Network Identifier (NID)that are embedded in the preamble of every project 25 data unit. The detector uses this information to perform bit recovery and packet identification. It processes and buffers the binary data for use by the Project 25 Voice Module. Once a target signal is detected, the radio disables squelch using an enable transmit function, so the signal can be monitored by the user. If the detected signal is lost, squelch is enabled by the shutdown active receive function.

1.3.2.3.2 Analog FM Detector

The Analog FM Detector uses a function to decimate the incoming data stream by six, and run the noise detector, CTCSS single-tone detector, CTCSS multi-tone detector, and DCS multi-code detector. A noise squelch detect function detects the appearance of a carrier by searching for a drop in power in a frequency band just above the audio band. In the analog noise detector, the input data is scaled and high-pass filtered, then rectified and scaled again. Then the data is low-pass filtered. The output of the low-pass filter is used to determine whether or not a signal is present.

The detector has two states: SEARCHING and LOCKED. If the detector state is SEARCHING and the detected power drops below the lower squelch threshold, the detector state transitions to LOCKED. Conversely, if the detector state is LOCKED and the detected power rises above the upper squelch threshold, the detector state transitions to SEARCHING. Upper and lower threshold values are BW dependant and can be adjusted at run time.

The multiple-value DCS detector searches for a 134.4 bps bit stream in the sub-audible frequency band used for DCS codes. If found, the code is extracted and appropriate state variables are updated. Code extraction is performed in two steps: first the input data is converted to a binary bit stream and second, data extraction, and code comparisons are performed.

The conversion of the input data to a binary bit stream starts with the 8 ksps input data being sent through a decimate by six, FIR filter to produce a 1.33 ksps, real valued data stream. This filter removes any signal energy outside of the sub-audible frequency band. The data is then split into two paths. The lower path estimates the Direct Current (DC) content of the signal with a very narrow low pass Infinite Impulse Response (IIR) filter. Subtracting the lower path signal from the upper path signal removes the DC component from the upper path signal. Following this, the resulting signal passes through a single-bit quantizer and the output is buffered for use by the code removal step. Data extraction, and DCS code comparisons are then accomplished.

1.3.2.3.3 CVSD DES Detection

Detection of CVSD DES waveforms is performed by a secure detection function. This function also recovers the 12 kbps bit stream from the 48 ksps input signal. The detector looks for a 12 kbps data stream to determine if a CVSD signal is being received.

1.3.2.4 Project 25 Voice Module

The physical layer task extracts FS, NID, SS symbols, and data. All other dibits are passed to the receive framing task. The module performs recovery and symbol extraction based on frame synchronization using a correlation detector. Carrier frequency offset compensation is followed by symbol extraction and error-correction decoding. VOCODER data and Project 25 framing data is removed and secure mode decryption is performed. The VOCODER converts the compressed voice data stream to a 8 ksps audio data stream that is sent to the Modulation Module.

1.3.2.5 Analog FM Module

The analog FM module performs two tasks. The Detection Task uses a FIR filter to down-sample the FM demodulated bit stream from 48 ksps to 8 ksps. It then uses four detectors (noise, single-tone CTCSS, multi-tone CTCSS, and multi-code DCS) to determine signal squelch. The Post-Detection Audio Shaping Task applies de-emphasis on/off filtering to a received clear analog signal.

1.3.2.6 CVSD DES Module

The CVSD DES Module consists of a 12 kbps clock detection/recovery task, a 12 kbps symbol resolver, a differential decoder, a DES decoder, a 12 kbps CVSD decoder, and a 12 ksps to 8 ksps sample rate converter. The input to the clock detection algorithm is a 48 ksps data stream, representing the sampled FM demodulated carrier. To allow for variation in carrier frequency, the DC component of the demodulated carrier is removed before zero-crossing detection. From a zero-crossing phase profile, a decision can be made whether a 12 ksps data stream is present on the demodulated carrier and a 12 kHz clock can be recovered for usage within the 12 kbps symbol resolver. Differential encoding of the binary FSK modulation is used to ensure compatibility between manufacturers, in that either a positive or negative frequency shift can be used to represent a "1" symbol. In the CVSD receive chain, differential decoding precedes one-bit cipher feedback DES decoding. To conserve memory and aid processing efficiency, all symbols (encoded and decoded) are packed in memory. The 12 kbps CVSD decoder is modeled after FED-STD-1023.

The decoder consists of a Modulation Level Analyzer (MLA), a Syllabic Filter, a Pulse Modulator, a Principal Integrator and a Comparator. The output of the CVSD decoder is at 12 kbps that must be changed to 8 ksps for output by the CODEC.

1.3.2.7 Audio Processing Module

A audio receive task function and a audio filter is used to output Project 25, clear analog, or secure analog speech samples to the CODEC. When in active receive modes, the ISR is enabled and the task outputs data to the CODEC circular buffer as data is being written to it's audio input circular buffer.

1.3.2.8 Audio CODEC

The Audio CODEC and the DSP interface using the DSP ESSI 0 port. The serial clock to the CODEC operates at 2.048 MHz, and is derived from the DSP internal clock. ESSI 0 is configured to operate using a frame rate divider of sixteen (16) and a word length of sixteen (16) bits, transmitting packets of encoded audio to the CODEC at 8 kHz. The CODEC is used in a linear decode mode, where thirteen (13) bits are used to represent the full audio range. The post-processed DSP signal is fed to the Audio CODEC, which converts the signal to an analog waveform, applies gain, and routes it to the appropriate output device.

1.3.3 DSP Software

The program data for the DSP is stored in 64K Flash program blocks. The data is stored as unpacked bytes. The blocks used for the DSP software are dedicated so that selective upgrades of this code only are possible.

1.4 Keypad MPU Software

1.4.1 Overview

The keypad Micro-Processor Unit (MPU) provides the direct interfaces to the radio keypad and switches. It communicates with the main controller via a synchronous bi-directional serial link.

1.4.2 General

The software is designed so that processor activity and hence current consumption is minimized. The only continuous operation required is the keypad scanning and switch reading. The keypad MPU is clocked by an external clock at 1.5 MHz, and the hardware reset supplied from the main controller.

1.4.3 Keypad Scanning

The keypad scan software continuously scans the keypad at a rate of a row every 10ms. A debounce period of 40ms is used on key presses and key releases. The key scan software deals with simultaneous key presses and key rollovers, such that only single key presses are validated. Debounced and validated key presses are passed to the serial data output buffer.

1.4.4 PTT Input

The inputs from the momentary input switches, PTT and the Auxiliary keys are read every 10ms. and are debounced for 40ms. The validation software filters out simultaneous presses of the auxiliary keys and key rollover between them. Simultaneous presses of the PTT switch and one auxiliary key are allowed. Debounced and validated auxiliary key presses and PTT press and releases are passed to the serial data output buffer.

1.4.5 Switch Input

The inputs from the rotary switches and toggle switch are read at least every 40ms. Changes in state are debounced for 100ms. Debounced new switch positions are then passed to the serial output buffer.

1.4.6 LED Output

The outputs to the LED are controlled under instruction from the serial port. It is possible to set both outputs off, set the red LED on, set the green LED on, set both LEDs on (orange), and to flash either or both on a 50% duty cycle at a controlled rate of approximately 1 Hz.

1.4.7 Backlight Control

The two LCD backlight controls to set bright and dim operation are controlled under instruction from the serial port. The keypad uses a fixed level backlight operation. A timeout facility, to switch off the backlight after 30 seconds if not requested by the main controller, is provided.

1.4.8 Serial Interface

The keypad controller implements a synchronous bi-directional serial interface using its serial port that allows it to interface to the main controller. The serial data clock is always sourced by the main controller. To allow autonomous transfers from the keypad controller a separate Keypad interrupt line is provided with the interface. The interrupt line is used to request 8 clocks from the main controller to transfer data from the keypad. The LCD Chip Select (CS) input line is used to distinguish between serial data for the keypad controller and LCD driver. The serial interface supports the following transfers:

- Keypad to Controller
  - Keypad power up OK
  - Keypad error 1-n
  - Key press 1-16
  - Key release 1-16

  - PTT press
  - PTT release
  - Volume Switch 1-16
  - Channel Switch 1-16
  - Toggle switch 1-3
  - Auxiliary key press 1-3
  - Emergency key press
- Controller to Keypad
- Request current switch status
- Reset, execute BIT test
- Backlight off/bright/dim
- LED off/red/green/yellow/flash/flash rate
- Keypress request, interrupt acknowledge

LCD data transfers are in blocks of 80 bytes maximum, to allow a pause on the serial interface at least every 100ms for the keypad MPU to assert the interrupt and transfer keypress or switch change data. During the LCD data transfers, the key data are buffered in the keypad MPU.

1.5 Data Interface

The DSP incorporates a user data interface through its SCI port

1.5.1 CAI Data Interface

The DSP supports an asynchronous data interface for CAI modes using its SCI port. This interface conforms to the CAI Data Peripheral Interface. It uses standard V24, and RS232 baud rates up to 9600 baud. The software also controls the associated flow control signals Data Terminal Ready (DTR) input to DSP and Clear to Send (CTS) output from DSP. The Request To Send (RTS) input to the radio for this interface is processed by the H8.

1.5.2 Synchronous Serial Data Interface

The DSP supports a 12 kbps synchronous serial port using its SCI port. The interface is half duplex, uses a DSP generated clock, and includes minimum data buffering within the DSP and RTS/CTS flow control on the transmit function.

1.5.2.1 Receiver Synchronous Serial Data Buffering

In receive synchronous serial data modes the DSP software uses a variable length First In First Out (FIFO) buffer to cope with differences in clock rates between the transmitter and receiver.

1.5.3 CAI Data Link Layer

This software provides the link between the raw voice or data bit streams and the data formats required to implement a 9.6 kbps CAI compatible interface.

1.5.3.1 CAI Transmit Voice Mode

The DSP software takes the 144 bit voice code words (encrypted or not) and a number of link control fields set by the host H8 or from the DES system, and formats CAI-compatible logic link data units.

1.5.3.2 CAI Transmit Voice Test Modes

The DSP software is capable of transmitting the CAI voice silence test pattern, the CAI 1 kHz test pattern, and a 9x144 bit (1296) PRBS test pattern used for error rate tests. These test modes are controlled by the H8 controller.

1.5.3.3 CAI Receive Voice Mode

The DSP takes the 9.6 kbps CAI-compatible data stream and framing, split out the voice data for passing to the VOCODER. The DSP decodes the link control words so that the link control fields can be read by the host H8, and the encryption synchronization information is available to the encryption process. The CAI receive processing is initiated by the frame synchronization correlator trigger. When this is asserted the next 64 bits of Network Identifier (NID) data are decoded and checked. If the NAC code matches the one selected for the channel, voice or data processing proceeds, otherwise the physical layer will be forced back into search mode.

1.5.3.4 CAI Receive Voice Test Mode

The DSP software is capable of testing the 9 voice code words received in a CAI frame against a known 144 x 9 PRBS segment. The total number of errors in that frame is then output to the H8 controller. This test mode is controlled by the H8 controller.

1.5.3.5 CAI Transmit Data Mode

The DSP selects the user data (encrypted or clear) and a number of link control fields set by the host H8 or from the DES system, and formats logic link data units, compatible with the CAI at 9600 bits/second.

1.5.3.6 CAI Receive Data Mode

The DSP selects the 9.6 kbps CAI-compatible data stream and framing, splits out and decodes the data for passing to the user data port. The DSP decodes the link control words so that the link control fields can be read by the host H8, and encryption synchronization information is available to the encryption process.

1.5.4 Transmit Physical Link Layer

This software uses common modulator interface software and a number of mode dependent physical link layer software modules.

1.5.4.1 Transmit Modulation Interface

The software provides a common interface to the dual modulation Digital to Analog Converters (DACs) in the transceiver through its SSI serial port 1 for all transmit modes. In transmit modes, the SSI uses an externally sourced clock at 3072 kHz. This interface takes frequency deviation samples at 48 kHz, and writes each value scaled by a fixed number set by the host to both the reference oscillator DAC and the VCO DAC. Additionally a host-controlled DC offset is added to the reference oscillator DAC value.

1.5.4.2 Transmit CAI Physical Link Layer

This software takes the 9.6 kbps CAI-compatible data stream and converts it to 48 k samples of frequency deviation data. To achieve this the software implements the dibit to symbol mapping and Nyquist and shaping filters as described in the CAI.

1.5.4.3 Transmit Analog FM Physical Link Layer

This software takes the 8 ksps filtered audio and converts it to 48 ksps of frequency deviation data compatible with TIA/EIA-603 in 12.5kHz and 25kHz modes. The signal processing used is additional high pass filtering to reduce the energy in the DCS tone band, audio band pre-emphasis if required, DCS tone addition, deviation limiting and smoothing. Software is capable of operation in 12.5 kHz, and 25 kHz channel spacing with appropriate deviation scaling. The software is capable of: appending a phase reversed tone burst of 180 ms as defined in EIA-603, generating DCS and audio turn-off codes, and companding the voice signal in 12.5kHz mode.

1.5.4.4 Transmit CVSD Physical Link Layer

The transmit CVSD physical link layer converts the 12/16 kbps CVSD data stream and converts it to 48ksps of frequency deviation data. The software implements a pre-modulation filter with raised cosine time response and 100% eye height.

1.5.5 Receive Physical Link Layer

This software uses common FM demodulation software, and mode dependent receiver physical layer software modules.

1.5.5.1 Receive ADC and DAC Interface

In receive modes the SSI port 1 is used in a duplex manner to allow the ADC to be read continuously at 96 kHz and the DAC to be written to at up to 48 ksps for AGC and reference oscillator adjustment. In receive modes the SSI port is clocked at 1536 kHz from an external clock source, using a sixteen bit cycle. Every cycle a value is read out of the ADC. Every other cycle a value may be written to one of the DAC channels to control the AGC and reference oscillator.

1.5.5.2 FM Demodulator

This software provides a common interface to the 96 ksps IF signal at the SSI port 1 and produce 48 ksps of frequency deviation data for use in all modes. The SSI port uses an external clock at 1536 kHz. The software implements an FM demodulator function using a quadrature mix with a 24 kHz (Fs/4) local oscillator, dual I and Q channel filters and a frequency estimator. The channel filtering function is programmable dependent on the channel spacing being used. The channel filtering provides the adjacent channel filtering additional to that provided by the hardware needed to achieve the radio adjacent channel rejection performance.

1.5.5.3 Receive CAI Physical Link Layer

This software takes the 48 ksps of frequency deviation data and outputs a 9.6 kbps data stream. The software implements an integrate and dump filter and data slicer as described in the CAI. The integrate and dump filter is controlled by a clock recovery function which selects one of ten possible phases for output to the slicer. The slicer incorporates an averager with a time constant of at least 100 bits to correct for DC offsets in the received signal.

In parallel with the above, a FIR correlator searching for the CAI fixed framing sequence of 24 symbols operates on the filtered 48 ksps of frequency deviation data. The correlator therefore operates at 10 samples per symbol. The correlator phase that has the highest correlation peak is used to select the clock phase for use in the integrate and dump filter, and slicer. This correlator operates continuously when searching for CAI traffic and occasionally when tracking an CAI signal when subsequent frame syncs are expected. The correlator trigger is used to provide a framing signal for the subsequent CAI data link layer processing.

1.5.5.4 Receive Analog FM Physical Link Layer

This software takes the 48 ksps frequency deviation data and outputs 8 ksps of audio to the receive audio processing. The software signal processing implements a high pass filter to remove CTCSS tones and de-emphasis if required. The gain of the signal path is adjusted to cope with the different deviations used on different channel bandwidths. The signal processing signal path is controlled by squelch signals. The software includes audio expanding to reverse the transmit companding.

1.5.5.5 Receive CVSD Physical Link Layer

This software takes the 48 ksps frequency deviation data and output 12/16 kbps serial data. The software implements a data filter, a slicer and a clock recovery function.

1.5.6 DES Encryption

The DSP software implements DES encryption of traffic in CAI modes and CVSD modes.

1.5.6.1 DES Kernel

The DSP software implements the DES encryption kernel as described in FIPS 46-2, encrypting 64 data bits using a 56 bit key using output feedback operation or single bit cipher feedback operation.

1.5.6.2 CAI Encryption

The DSP software uses the DES kernel software to implement the CAI encryption of voice traffic as described in TIA/EIA/IS-102.AAAA. The encryption key is supplied by the key manager. In transmit, the Message Indicator (MI) vector is passed to the data link processing for encoding and transmission. In receive, the MI vector is decoded by the data link layer, and flywheeled if decoding fails for up to n frames.

1.5.6.3 DES Data Link Layer

This software encrypts and decrypts the 12 kilobits of CVSD data using the DES kernel. In transmit, framing synchronization data and the MI vector are inserted into the data stream. In receive, the software searches for and extracts the framing data and MI data. The bit definitions and formats used are defined in the DES protocol.

1.5.6.4 Key Interface

This software provides an interface for inputting DES encryption keys from the DSP SCI port using synchronous data transfers with an external clock, conforming to the Motorola KVL data transfer mechanism and the CAI DES keyfill protocol.

1.5.6.5 Key Bank

The radio maintains a bank of up to 16 encryption keys stored in the flash memory. Associated with each key are a Key ID, Key Data, and an eight character alpha-numeric tag. Each encrypted channel is assigned one of the 16 keys for both secure transmit and secure receive modes. Channel key assignment is accomplished via selecting the corresponding key tag. Upon entering secure transmit or secure receive mode, the H8 transfers the appropriate encryption key to the DSP through the SCI port.

1.5.7 Host Interface

The DSP is controlled through its host interface by the H8. It initially boots up through this interface. The host interface is used for DSP mode control, encryption key transfer, link control data transfer, low rate data transfer, frequency variable data transfer, CTCSS mode control, and initial software download.

1.5.8 Flash Interface

The DSP also has direct access to the main radio Flash memory through the H8 bus arbitration logic. This interface is used for software downloads using byte-wide Direct Memory Access (DMA) transfers under host control for mode changes. The DSP software does not write to the Flash memory.

1.5.9 Paging

The DSP software is designed such that normal operation does not involve off-chip bus accesses. This means that the program code size must be limited to 24k words and the data memory to 10k words. A number of program images corresponding to different modes are allowed, with paging of images out of the Flash by DMA at mode changes allowed. The minimum subdivision of images used corresponds to the following modes plus a continuously resident core host interface function.

- Initialization/POST
- Receive 12.5 kHz
- Receive 25 kHz
- Transmit 12.5 kHz
- Transmit 25 kHz
- Keyfill

The paging DMA mechanism is controlled by the host H8 and allows the transfer of a program image within 50ms.

1.5.10 Hardware Control

The DSP software controls the DSP clock rate through the Phased Locked Loop (PLL) output divider such that the DSP clock rate is dynamically matched to the mode of operation, in coarse steps for example, between searching and tracking receive modes. The DSP software is designed to use low current wait modes in pauses between processing to minimize current consumption. The host is also able to request a very low current idle mode in the DSP, this mode is released by the Host.

1.6 Controller Software

1.6.1 Overview

The controller software has overall control of the radio, including user interface operations, and control of the DSP and transceiver. Figure 1-4 shows a block diagram of the controller software.

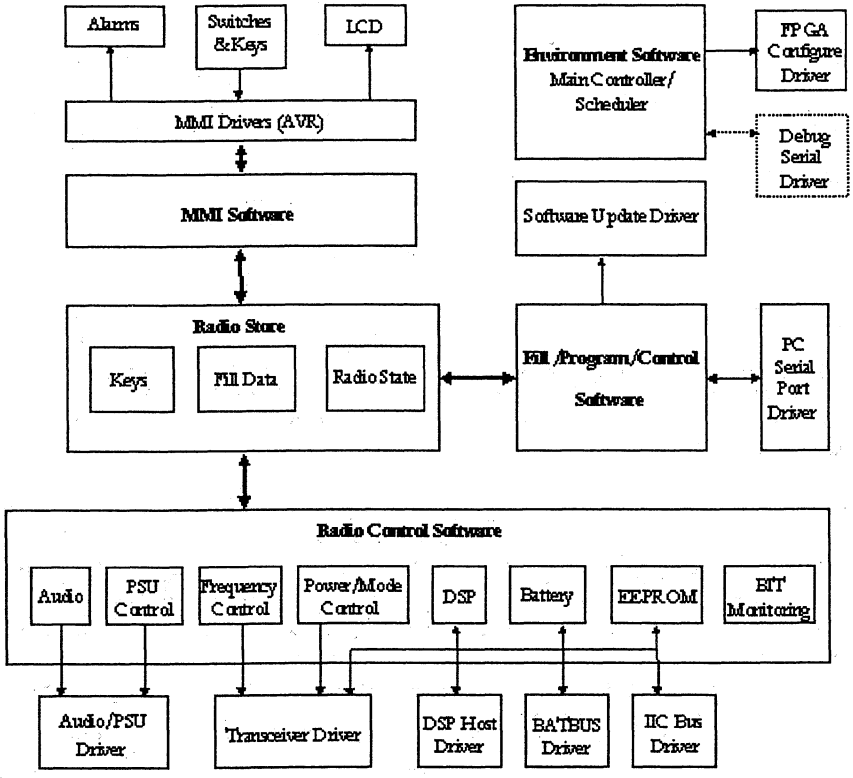

Figure 1-4 Controller Software

1.6.2 Environment

1.6.2.1 General

The H8 controller system is designed for minimum external bus activity and minimum current consumption. These features are provided by the maximum use of low current standby modes in the H8, and an interrupt driven architecture, with the minimum of input polling. In radio standby and receive modes the only H8 tasks are the control of the transceiver frequency and DSP mode as the radio scans, and economizes. The most H8 intensive activities are associated with USER INTERFACE interactions with the user, and operations on the fill/program/control port.

1.6.2.2 Scheduler

The H8 operates with a simple scheduler that launches tasks after interrupt events. A timebase interrupt of 10ms is used to keep track of time and poll inputs at regular intervals.

1.6.2.2.1 Interrupt Sources

The following interrupt sources are used in the H8:

- User Int. Inter. External interrupt from keypad
- DSP Interrupt External interrupt from the DSP, signal detected etc.
- Low Battery External NMI from power supply indicates power supply fail
- Timer Interrupt Internal timebase tick interrupt every 10ms
- PC Serial Port Internal interrupt from PC Interrupt serial port
- U.I. serial port Internal interrupt from USER INTERFACE Interrupt serial port, keypress data and LCD data
- Debug serial port Internal interrupt from DMA/ Timer
- Alarm generator Internal interrupt from DMA/ Timer

1.6.2.2.2 Polled Inputs

The following inputs are polled by the H8 software at regular intervals.

- EXTPTT/RTS External PTT and data RTS
- OOL Synthesizer Out of Lock
- PWROFF The on/off switch position
- SENSE External keyfill device detect

ADC as regularly as appropriate to the radio mode of The following analog inputs are measured with the operation.

- RSSI Receiver signal strength
- WRU External Device Detect
- BATT Main radio 10V supply monitor
- PA TEMP Transmitter temperature
- XTAL TEMP Reference crystal temperature
- PA CURRENT Transmitter Current

1.6.2.2.3 Watchdog

A regular watchdog service task is scheduled to prevent the H8 watchdog controller overrunning and a hardware reset occurring. The target watchdog timeout is 100/ 200ms.

1.6.2.3 Start-Up Software

1.6.2.3.1 Boot Block Start-Up Software

The minimum simplest start-up software is provided in the boot block of the Flash. This software holds the keypad, DSP, USER INTERFACE and Field Programmable Gate Array (FPGA) in reset, then establishes whether a valid H8 program image exists in the program blocks of the Flash. If no valid program exists a simple alarm is sounded. The boot block software includes a minimum basic BIT facility to check the code itself and internal and external Random Access Memory (RAM). The boot block code also includes the software to allow programming of the program blocks of the Flash through the PC serial port.

1.6.2.3.2 Full Start-Up Software

If a valid H8 program image exists the full start-up code is executed. This involves: initializing RAM, DSP, keypad, USER INTERFACE, FPGA, transceiver etc.; executing the start-up BIT; and then transferring control to the main scheduler.

1.6.2.3.3 FPGA Configure Software

At start-up the H8 configures the FPGA using data from the main Flash memory and transferring it via a synchronous serial bus to the FPGA.

1.6.2.4 Shut Down Software

At normal shut down when the on/off switch is switched off the H8 software executes a clean shut down to shut down the transceiver, DSP and user interface (UI), save any usage data to the Flash, then release the main power supply. In cases where the battery is removed the Low battery interrupt is used to execute a minimum fast shut down, just saving RAM data as required, with no Flash update.

1.6.2.5 Debug Driver Software

The H8 controller includes software to implement an asynchronous serial port on two Input/Output (I/O) pins of the H8. Facilities provided include the ability to monitor particular radio variables, and to control specific variables. This port is used to allow PC serial access to the board at board level factory test, through the test connector.

1.6.3 Radio Store

The radio data store is accessed by all functional areas of the controller software, including the user interface, fill control and radio software.

1.6.3.1 Physical Data Storage

The radio data is physically stored in 4 devices all accessible by the controller software.

1.6.3.1.1 H8 Internal RAM

The H8 controller has 2k x 8 of internal RAM. This data is not retained when the radio is switched off or the battery is removed. It is used for short term storage of frequently accessed variables, stack workspace etc. to minimize the bus activity when the H8 controller is running. The internal RAM is used as program space to execute from during some Flash update operations.

1.6.3.1.2 External RAM

The H8 is provided with an external 128k x 8 bit RAM that is backed up for at least 30 sec when the radio battery is removed, and also at all times when a battery is fitted even when the radio is switched off. This device is used as a variable data expansion area, and to store specific user-entered data which must be retained over battery changes (the unlock password etc.)

1.6.3.1.3 Flash ROM

The H8 is provided with 512k x 16 bit Flash Read-Only Memory (ROM) that is primarily used for program storage. The data in the Flash is retained permanently.

Different areas of the Flash have different characteristics: The boot sector is a 16k block that is used for the reprogramming software and the radio serial number etc. The data in this sector is designed to be programmed or block erased only in the factory.

The Flash has fifteen 64k and six 8k program blocks that can be block erased and programmed by the boot block code during normal reprogramming operations without special equipment and without opening the radio. These blocks are use for H8 and DSP operating software, radio fill data, and FPGA programming data. The Flash has two small 8k parameter blocks that can be used for changing data that must be stored indefinitely, examples are user specific settings and usage data.

1.6.3.1.4 Transceiver EEPROM

The radio transceiver has an 8k x 8 serial EEPROM that is used to store transceiver calibration data. This data is set during production test for the specific transceiver. The data in this device is essentially constant and it is never

written to by the main controller. At switch-on the contents of the EEPROM are copied into the external RAM, and the EEPROM is not accessed during normal operation.

1.6.3.2 Data Types

A number of different data types as below are used by the controller software.

1.6.3.2.1 Volatile Variables

Variable data used by the H8 controller that is not retained when the radio is switched off is stored in the H8 internal RAM and the external RAM.

1.6.3.2.2 Short Term Stored Variables

Variable data that is retained while the radio is switched off or the battery is removed is stored in the external RAM.

1.6.3.2.3 Permanent Stored Variables

Variable data that is retained indefinitely is stored in the parameter blocks of the Flash. Every time this data changes a parameter block must be erased and the new data written into the now blank parameter block.

1.6.3.2.4 Radio Fill Data

The frequencies, modes, power levels, etc. associated with different channels programmed into the radio. This data is programmed into the radio through the fill port

1.6.4 Program/Fill/Control Interface

The controller provides a serial port for PC access to allow the following functions:

- Programming – updating radio software.
- Filling – Modifying the radio data store of modes and frequencies etc.
- Control – Controlling the radio operating mode.

1.6.4.1 Radio Programming

The controller software allows reprogramming of the Flash memory program blocks, on a block by block basis. During these operations, the controller executes from the boot sector of the Flash and no radio or user interface operations are possible. After a programming operation, the radio must be restarted by cycling the power. Programming operations are initiated on receipt of a specific serial message on the PC serial port.

1.6.4.2 Radio Fill

The controller provides the facilities to modify the system, group, bank, and radio global data through the PC serial port. This interface provides the following facilities:

- Radio erase - delete all fill data in the radio
- Selective erase - delete (mark as deleted) specific systems, groups , banks (future)
- Radio Fill - add specific systems, groups, banks and global data to the radio store.
- Radio read - export the fill data contents of the radio store to the PC.

All transfers and operations on the fill port are CRC checked and acknowledged.

1.6.4.2.1 Cloning

The radio can export channel data to other radios. The data export is initiated by a user interface operation at the exporting radio. The exporting radio emulates a PC programmer during the data transfer. **Cloning of keyfill data is not allowed.**

1.6.4.2.2 Radio Keyfill

The radio keyfill protocols are managed by the DSP software.

1.6.4.3 Radio Control Port

It is possible for an external PC to control the functioning of the radio. This provides the following facilities:

- Radio status read - export the radio serial number, revision status, history, usage etc.
- Set external control mode.
- Set radio transmit frequency, power level, and mode.
- Set radio receive frequency and mode.

The transceiver mode control also allows transmission of 1kHz test tones in analog modes, and BER test patterns in digital modes. The receiver mode control allows the continuous (every 0.5 second) output of the bit error count per frame in digital modes.

1.6.4.4 PC Serial Port Driver

The controller software controls the H8 serial port to implement the asynchronous data formats and baud rates (9,600; 19,200; and 38,400) for the PC serial port. The serial port driver software also controls the 232OFF signal to maintain the RS232 in its low current standby state, except when data is being driven out and while RTS is asserted.

1.7 User Interface

The radio user interface is described in the following paragraphs.

1.7.1 Display Description

The radio has a 80 x 32 dot matrix LCD radio display. Some of the features of the display are:

- Phone mode is indicated by a icon in the top right. (future)
- Scan occurring is indicated by 'SCAN****', 'SRCH****', or 'ZONE****' flashing on and off in the top row of the display.
- Encryption is indicated by a key icon.
- Power level is indicated by 'HI/LO/2W' in the bottom row of the display.
- Priority scan is indicated by 'SCANP1(P2), 'SRCHP1(P2)', or 'ZONEP1(P2)' flashing on and off in the top row of the display.
- Receive Only Channel is indicated by an 'RX' in the bottom left corner of the display.
- Talkaround is indicated by an 'TA' in the bottom left corner of the display.
- Repeater Mode is indicated by a receiver icon in the bottom left corner of the display.
- An 'EMG' appears in the bottom left corner when the radio is transmitting an emergency message.
- A battery level bargraph display is permanently displayed on the far right of the display.

1.7.2 Keypad

The radio can be programmed using the keypad and display. Pressing the ENTER key from an operational screen will allow the user to enter the programming menu screens. These screens are shown at Appendix A. For detailed instructions on programming the radio through the display and keypad see the Guardian User's Guide (p/n 84326).