# A Modular Testbed for Hardware Reconfigurable Radio at the 2.4 GHz ISM Band

Gerard Baldwin[a] and Ronan Farrell[b]

[a] Department of Electronic Engineering, NUIM, Maynooth, Co. Kildare, Ireland
[b] Department of Electronic Engineering, NUIM, Maynooth, Co. Kildare, Ireland

## ABSTRACT

A modular testbed for use in developing software defined radio is documented in this paper. The testbed is focused on the 2.4 GHz ISM band but may be used at other frequencies. An RF transceiver with variable transmit/receive frequencies and bandwidths is provided.

It provides the capability to support many modulation schemes and standards such as GSM, UMTS, IEEE 802.11b and parts of the IEEE802.16 standards. It performs the RF functions of the radio, with the other PHY and MAC layer functions such as equalisation and error-coding being performed by a host computer. It communicates with the host computer system through a USB2 interface allowing data rates of up-to 60Mbytes a second. An API is used for communication with the host computer system allowing for modulation/demodulation and coding/decoding in software on the host system and reconfiguration of the radio system.

**Keywords:** Software radio, reconfigurable

## 1. INTRODUCTION

The testbed described here is in development at the Department of Electronic Engineering, National University of Ireland Maynooth, as a tool for developing software defined radio. As such it provides the hardware required to develop a range of software radio applications. This paper is primarily concerned with the requirements placed on this hardware in order to meet many of the air-interface specifications that exist today and that are planned for the near future. It is envisioned that this platform, once it is verified, will be used to develop experimental 2G/3G mobile and wireless LAN implementations, providing the capability to operate across a range of licensed and un-licensed standards.

## 2. STANDARDS

In order to develop the radio, the specification of the radio must be determined. In order to do this we have selected a group of standards that the radio must be capable of implementing. At first glance it would be tempting to implement all of the wireless standards from GSM, CDMA2000, UMTS, IEEE802.11x, IEEE802.16x, IEEE802.15x and IEEE802.20x together with bluetooth and the emerging UWB standards. However these require radically different air interfaces which are in general not compatible. Instead these standards can be broken down into groups that share similar requirements for the air interface. To that end three groups can be identified.

The first group is the low rate, short range personal communications protocols. This group is made up of the bluetooth and IEEE802.15.4a standards. This group is characterised by having transmit powers of less that $1mW$, ranges of approximately 10 meters and data rates of less that 1Mbit/s.

The second group is high rate, short range personal communications protocols. This group is made up of the emerging UWB standards and the remaining IEEE802.15x standards. These are characterised by low transmitted powers, high bandwidths and high data rates of up-to 500 Mbit/s over short ranges in the region of 10 meters.

The third group is made up the 2G/3G mobile standards, and the IEEE802.11x, IEEE802.16x and IEEE802.20x standards. These all operate at higher powers over longer ranges at range of different bit rates. They share a

Further author information:
Gerard Baldwin: E-mail: gbaldwin@eeng.nuim.ie, Telephone: +353 (0)1 708 6329
Ronan Farrell: E-mail: rfarrell@eeng.nuim.ie, Telephone: +353 (0)1 708 6197

common thread in that they deliver connections to the end user over longer distances, using similar frequencies at a range of bit rates.

This work is focused on the third group of standards. This group is more demanding than the other two as a higher specification radio is needed to meet these standards as will be shown here.

Several metrics are used to define the performance requirements of the transceiver. These are, for the receiver, reference sensitivity, channel bandwidth, IP3, and blocker performance. Briefly, reference sensitivity is the minimum power level at the receiver input for which it can meet the required BER (Bit Error Rate) for a particular standard. The channel bandwidth is the frequency band occupied by one example signal from any of the standards of interest. IP3 is the third inter-modulation product. It is a function of any third order non-linearity in the system. It is important as these produce inband distortion. Blocker performance is more difficult to quantify. It is the ability of the receiver to meet any of the earlier requirements in the presence of a large blocking signal either in the band of interest or out-of-band. The transmitter is characterised by phase noise performance and distortion. The phase noise is a measure of how accurately the phase of the transmitted signal can be controlled. This determines the types of modulations the transmitter is capable of generating. Distortion is measured by IP3 as in the receiver.

## 2.1. UMTS

The UMTS standard is the European 3G standard. It implements the IMT-2000 3G standard. It has two specified air interfaces UMTS-FDD[1] and UMTS-TDD.[2] The UMTS-FDD band is allocated from 2110MHz to 2170MHz, which is coincident with the PCS-1900 allocation. As the name suggests Frequency Division Duplexing (FDD) is used in this band. With-in the individual channels spread spectrum modulation is used. The UMTS-TDD band is allocated from 1900MHz to 1920MHz and 2010MHz to 2025MHz. Time Devision Duplexing (TDD) is used in these bands. Again spread spectrum modulation is used. The blocking specification for both standards are given in figure (1). The reference sensitivities for UMTS are:

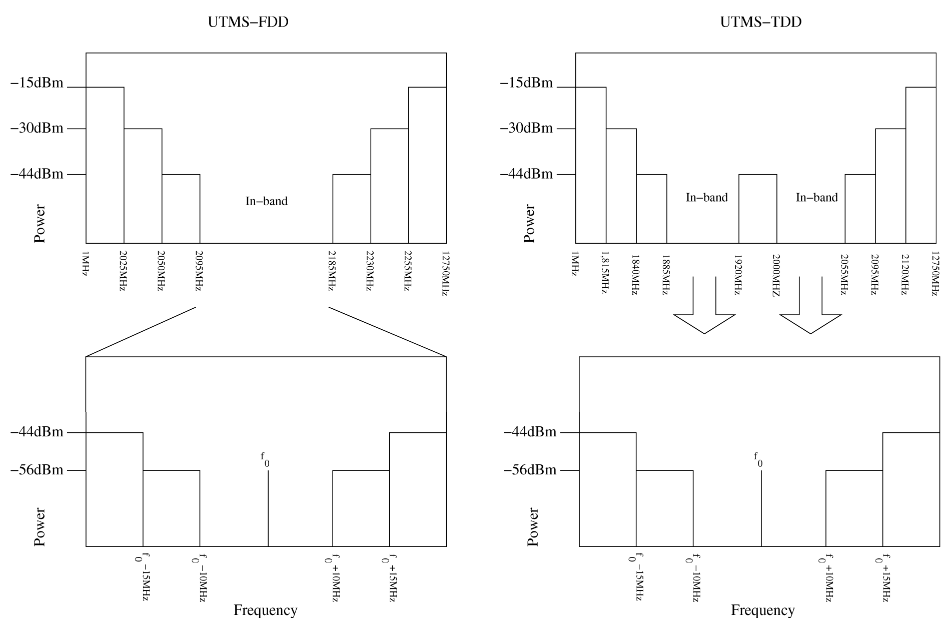


**Figure 1.** UMTS receive mask

$$\text{BER} \leq 10^{-3} = \begin{cases} \text{UMTS-FDD} & -117dBm \\ \text{UMTS-TDD} & -117dBm \end{cases}$$

## 2.2. GSM

The GSM standard[3] utilises GSMK (Gaussian Minimum Shift Keying) in a range of frequency bands depending on worldwide location. The bands of principle interest are given in table (1). With-in these bands we are

| | | | | |
|---|---|---|---|---|
| GSM 900 | uplink | 890-915MHz. | downlink | 935-960MHz |
| DCS 1800 | uplink | 1710-1785MHz. | downlink | 1805-1880MHz |
| PCS 1900 | uplink | 1830-1930MHz | downlink | 1910-2010MHz |

**Table 1.** GSM bands

primarily interested in the PCS and DCS bands as these are shared with the European 3G standards. For these reason we restrict ourselves to these bands in our support for the GSM standard. The receiver blocker specification for these bands is given in figure (2) and table (3). The basestation performance (BTS), and

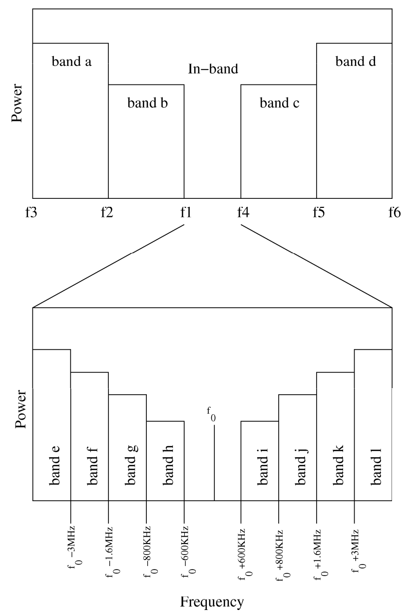


**Figure 2.** GSM receive mask

| frequency | f3 | f2 | f1 | f4 | f5 | f6 |
|---|---|---|---|---|---|---|
| DCS 1800 MS | 0.1MHz | 1705MHz | 1785MHz | 1920MHz | 1980MHz | 12750MHz |
| DCS 1800 BTS | 0.1MHz | - | 1690MHz | 1805MHz | - | 12750MHz |
| PCS 1900 MS | 0.1MHz | 1830MHz | 1910MHz | 2010MHz | 2070MHz | 12750MHz |
| PCS 1900 BTS | 0.1MHz | - | 1830MHz | 1930MHz | - | 12750MHz |

**Table 2.** Out of band GSM blocker frequency band edges in the DCS and PCS bands

mobile station performance (MS) are slightly different. The BTS performance requirements are more stringent the the MS requirements. The reference sensitivity levels are:

$$\text{BER} \leq 10^{-3} = \begin{cases} \text{DCS} & 1800 & \text{MS} & -102dBm \\ \text{DCS} & 1800 & \text{BTS} & -104dBm \\ \text{PCS} & 1900 & \text{MS} & -104dBm \\ \text{PCS} & 1900 & \text{BTS} & -104dBm \end{cases}$$

| band | a | b | c | d |
|---|---|---|---|---|
| DCS 1800 MS | 0dBm | -12dBm | -12dBm | 0dBm |
| DCS 1800 BTS | 0dBm | 0dBm | 0dBm | 0dBm |
| PCS 1900 MS | 0dBm | -12dBm | -12dBm | 0dBm |
| PCS 1900 BTS | 0dBm | 0dBm | 0dBm | 0dBm |

| band | e | f | g | h | i | j | k | l |
|---|---|---|---|---|---|---|---|---|
| DCS 1800 MS | -26dBm | -33dBm | -43dBm | -43dBm | -43dBm | -43dBm | -33dBm | -26dBm |
| DCS 1800 BTS | -25dBm | -25dBm | -25dBm | -35dBm | -35dBm | -25dBm | -25dBm | -25dBm |
| PCS 1900 MS | -26dBm | -33dBm | -43dBm | -43dBm | -43dBm | -43dBm | -33dBm | -26dBm |
| PCS 1900 BTS | -25dBm | -25dBm | -25dBm | -35dBm | -35dBm | -25dBm | -25dBm | -25dBm |

**Table 3.** GSM blocker specifications for the DCS and PCS bands

## 2.3. IEEE 802.11b

The IEEE 802.11b standard[4] is the most common wireless LAN standard in use. It uses a variety of modulation schemes, varying the bit rate depending on the quality of the channel. The most common one in use is Complementary Code Keying (CCK) providing a 11Mbit/s transfer rate. It operates in the ISM band at 2.4GHz with a channel bandwidth of 22MHz. The reference sensitivity is given as -76dBm. The standard requires an adjacent channel interference specification of -35dBm, but unusually does not specify the out-of-band interference specifications.

## 2.4. Summery

To summarise the receiver requires the ability to operate across a band from 1.6GHz to 2.5GHz, with a maximum reference sensitivity of -104dBm in the presence of a 0dBm interferer, and a maximum bandwidth of 22MHz. Similarly the transmitter must operate over the same band with a maximum peak-power output of 30dBm.

| | Duplex | Freq. downlink | Freq. uplink | Multiple access | Modulation | Channel BW(MHz) | Data rate |
|---|---|---|---|---|---|---|---|
| DCS 1800 | FDD-45MHz | 1805-1880MHz | 1705-1785MHz | TDMA | GMSK | 0.2 | 12.2kbps |
| PCS 1900 | FDD-45MHz | 1930-1990MHz | 1850-1910MHz | TDMA | GMSK | 0.2 | 12.2kbps |
| UMTS-FDD | FDD-190MHz | 2110-2170MHz | 1920-1980MHz | CDMA | QPSK,16QAM | 1.6,3.84,5 | 2Mbps |
| UMTS-TDD | TDD | 1900-1920MHz 2010-2025MHz | 1900-1920MHz 2010-2025MHz | CDMA | QPSK,16QAM | 1.6,3.84,5 | 2Mbps |
| 802.11b | TDD | 2400-2497MHz | 2400-2497MHz | CSMA | DBPSK, DQPSK, CCK | 22 | 11Mbps |

**Table 4.** Summery of standards of interest here

| | Reference Sensitivity | BER | Required SNR |
|---|---|---|---|
| DCS 1800 | -102dBm | $10^{-3}$ | 10dB |
| PCS 1900 | -102dBm | $10^{-3}$ | 10dB |
| UMTS-FDD | -117dBm | $10^{-3}$ | QPSK: 7dB |
| UMTS-TDD | -117dBm | $10^{-3}$ | QPSK: 7dB |
| 802.11b | -76dBm | $8 \times 10^{-2}$ | CCK: 10dB |

**Table 5.** Summery of standards of interest here

# 3. RECEIVER ARCHITECTURE

The receiver supports the standards outlined. To do this it has to be able to cover a band from 1.6GHz to 2.5GHz. It has to satisfy the blocker and sensitivity requirements of these standards. All of the standards require simular performance from the receiver in this regard. The GSM blocker specification is the tightest. It requires a sensitivity of -102dBm in the presence of an out-of-band blocker of 0dBm which amounts to 102dB of dynamic range.

| | NF (dB) | $IIP_2^{(1)}$ dBm | $IIP_3$ dBm |
|---|---|---|---|
| DCS 1800 | 9dB | 43 | -18 |
| PCS 1900 | 9dB | 43 | -18 |
| UMTS-FDD | $9.6^{(2)}$ | 8 | -21 |
| UMTS-TDD | $9.6^{(2)}$ | 8 | -21 |
| 802.11b | $9^{(3)}$ | 10 | -18 |

(1) $IIP_2$ is required when a zero-IF or low-IF architecture is used
(2) Assuming processing gain = 25dB
(3) Assuming processing gain = 10.41dB

**Table 6.** Summery of standards of interest here

A direct conversion architecture is chosen for its ability to tune across the wide selection of channel bandwidths needed. This architecture does not require an intermediate frequency (IF). Selecting an IF for a broad band of signals is difficult. The IF must be high enough to allow the transfer of the full band of interest with out folding (folding occurs when the center frequency is not greater than half the bandwidth) which causes distortion. It is also prone to image rejection problems. Using a direct conversion architecture avoids these problems, simplifying the radio considerably. The radio receiver outputs appear as quadrature signals in the baseband. From an implementation stand point this also avoids the requirement to construct a channel select filter at an IF with an adjustable bandwidth. Instead this is achieved by a pair of filters in the baseband on each of the I and Q channels. Off the shelf components can be used to construct these filters. The direct conversion architecture does have a sensitivity to DC offsets due to local oscillator issues, but this can be addressed by careful design of this component of the system.

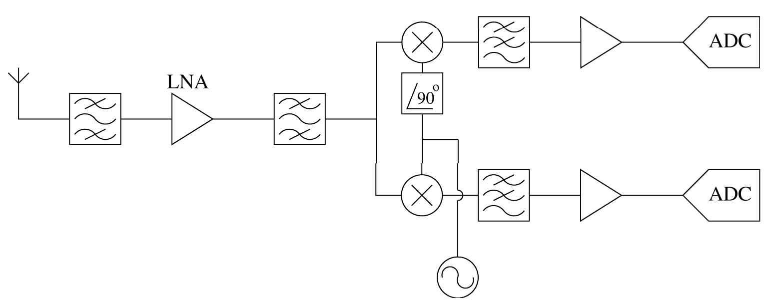


**Figure 3.** Receiver architecture

## 3.1. Transmitter Architecture

Again a direct conversion transmitter architecture is chosen for its ability to tune across the bands of interest avoiding the need for an IF filter with adjustable bandwidth. The transmitter is required to meet the phase noise specification for GSM as this is the tightest phase-noise specification of the standards listed at -152dBc/Hz. At present no mechanism is included for power scaling at the output. Instead this is done in the digital domain. This is far from ideal and will be addressed in a later iteration of the radio.

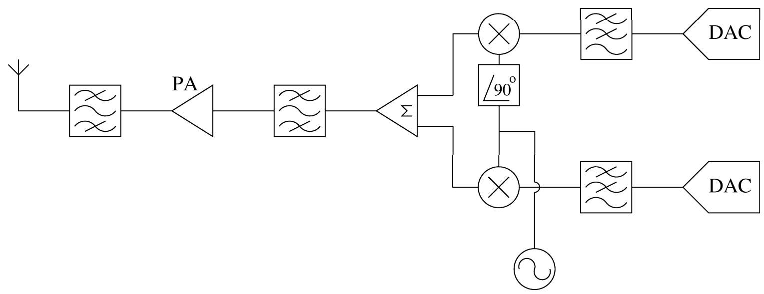


**Figure 4.** Transmitter architecture

## 4. IMPLEMENTATION

The software defined radio is implemented using as many off the shelf parts as possible. While this has some impact on the performance it allows a prototype to be constructed in a short space of time. During the life time of the radio many of these parts will be replaced with be-spoke integrated circuit designs in order to improve performance. The components chosen are shown in figure (5).

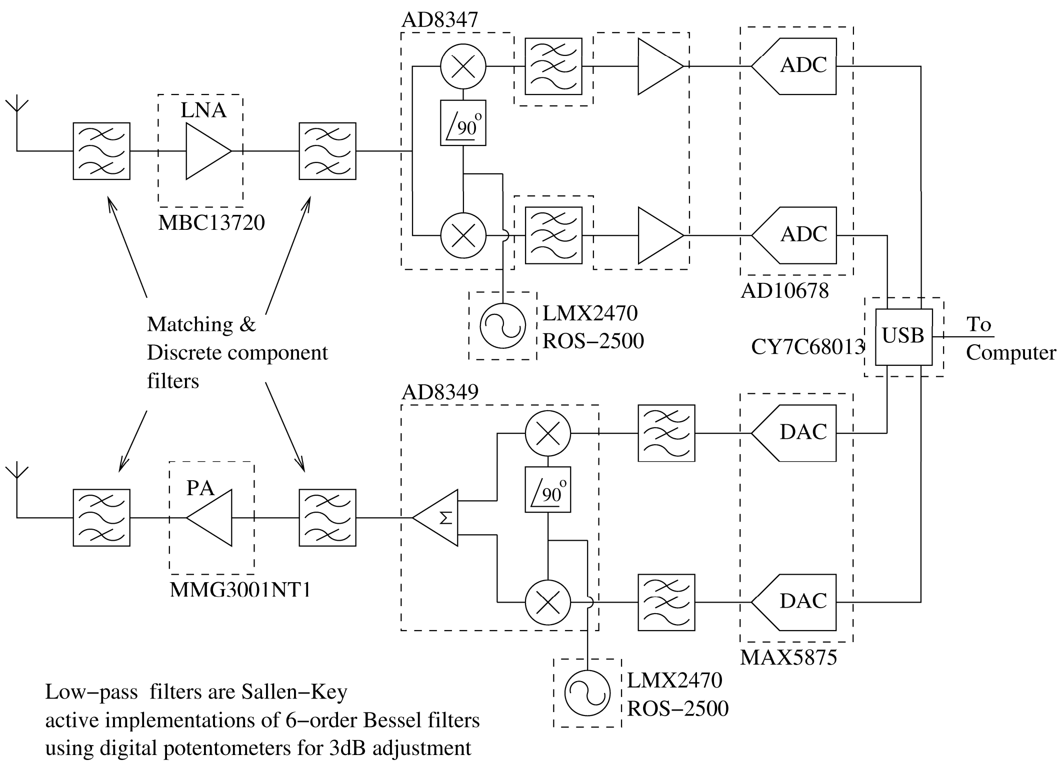


**Figure 5.** Transceiver implementation

### 4.1. Receiver

The LNA chosen is a Freescale semiconductor part: MBC13720, with a gain of 12dB at a noise figure of 1.55dB and an IP3 of 10dBm capable of operating across a frequency range from 400MHz to 2500MHz. Discrete component broadband matching circuits are included to match the LNA to the antenna and the following downconverter.

The downconverter chosen is an Analog Devices part: AD8347. This is a direct conversion part with an I/Q output. It has a conversion gain of up to 69dB by the use of AGC, with a noise figure of 11dB, an IP3 of 11.5dB and an IP2 of 25.5dBm. This meets our specification for IP3 and noise figure but is somewhat poorer than the required IP2 specification. This is one issue that will be addressed in later revisions of the radio with bespoke silicon. The low-pass filters that form the channel-select filters in the analog domain are made-up of active Sallen-Key filter implementations of $6^{th}$ order Bessel filters. Bessel filters are chosen as they have flat group delay responses. This facility is important when looking at broadband signals. The cut-off frequency of these filters is adjustable using digital potentiometers.

The oscillator signal comes from a National Semiconductor PLL :LMX2470 using a Mini-Circuits VCO : ROS-2500. This configuration is capable of producing a frequency in a range from 500MHz to 2.6GHz with a phase noise of -200dBc/Hz.

Next the signal is digitised using two 16-bit Analog Devices ADC's capable of operating up-to 80MSps. The digitised information is then transfered to the host computer for final processing and data extraction over a USB2 interface using a Cypress Semiconductor part: CY7C68013. This part also includes a 8051 micro-controller. This micro-controller is used to provide the digital setup and control signals to the downconverter, the PLL, the channel-select filters and the ADCs.

The two bandpass filters represent the matching networks at the input and output of the LNA. They are constructed from discrete components with an insertion loss of 3dB. Using the equation (1) we calculate the noise figure for the receiver[5]:

$$NF_{total} = NF_1 + \frac{NF_2 - 1}{Gain_1} + .... + \frac{NF_m - 1}{Gain_1...Gain_{m-1}} \tag{1}$$

where $NF$ is the noise figure. We get a $NF_{total} = 7.7dB$ which meets our specification.

The IIP3 is calculated using the approximation[5]:

$$\frac{1}{A^2_{IIP3}} \approx \frac{1}{A^2_{IIP3,1}} + \frac{\alpha_1^2}{A^2_{IIP3,2}} + \frac{\alpha_1^2\beta_1^2}{A^2_{IIP3,3}} + ..... \tag{2}$$

where the input to the first stage is $x(t)$ , the output is $y1(t)$ and the non-linear transfer function of the first two stages are:

$$y_1(t) = \alpha_1 x(t) + \alpha_3 x^3(t) \tag{3}$$

$$y_2(t) = \beta_1 y_1(t) + \beta_3 y_1^3(t) \tag{4}$$

where $A_{IIP3}$ is the third order intercept and is given by:

$$A_{IIP3} = \sqrt{\frac{4}{3}|\frac{\alpha_1}{\alpha_3}|} \tag{5}$$

We get an $A^2_{IIP3} = -0.87dBm$ which meets are specification also.

### 4.2. Transmitter

The transmitter follows a similar specification as the receiver. The encoded data is provided via a USB connection from the host computer using the Cypress Semiconductor USB chip. This part is shared between the transmitter and the receiver.It again also provides a control channel using the 8051 micro-controller for the other components in the transmitter. Next two DACs are used to perform the analogue to digital conversion. These are Maxim MAX5875 capable of 200Msps at 16bits. Following this the signal on each of the I/Q branches enters a low-pass filter. This acts as a reconstruction filter and also to limit the bandwidth at the input to the upconverter. These are again made up of active Sallen-Key implementations of $6^{th}$ order Bessel filters where the filter 3dB bandwidths are again controlled by digital potentiometers which are in-turn controller by the 8051 micro-controller.

The upconverter is an Analog Devices part: AD8349. It has an I/Q bandwidth of 160MHz and an output range of 700-2700MHz. It has a phase error of $0.3^o$ and an amplitude imbalance of 0.1dB at an output power of 3dBm. The transmit oscillator is again provided by the LMX2470 PLL using a Mini-Circuits VCO : ROS-2500.

Finally the power amplifier is a class A device from Freescale Semiconductors. It has a gain of 20dB across a frequency range of 40-3600MHz. Broadband matching circuits consisting of discrete components connect this to the upconverter and antenna. In this iteration of the radio there is no power control around the power amplifier.

### 4.3. Software

An example USB driver has been developed. It allows the various elements of the radio to be controlled through software run under the Linux operating system on a personal computer. Basic functionality is available through this interface. It also allows the transfer of data through the USB interface from and to the DACs and ADCs in the radio. Modules written in the C programming language are under development to support the popular modulation schemes such as BPSK, GMSK QPSK and QAM. These will be used to develop support for the standards outlined earlier.

## 5. CONCLUSION

The design of a software defined radio has been outlined. The relevant specifications from the various standards selected for support have been extracted and documented. These have been used to design a prototype radio which is currently under construction. Several areas where currently available subcomponents do not meet requirements have been identified. These will be addressed in later iterations of the radio. An example USB driver has been developed and further software is under development to take advantage of the radio.

## ACKNOWLEDGMENTS

This work is carried out as part of the CTVR (Centre for Telecommunications Value-Chain-Driven Research) funded by SFI (Science Foundation Ireland).

## REFERENCES

1. "3GPP TS 25.104 V6.8.0 (2004-12)" UMTS-FDD standard
2. "3GPP TS 25.105 V6.2.0 (2004-12)" UMTS-TDD standard
3. "Digital Cellular Telecommunications System (phase 2+); Radio transmission and Reception (GSM 05.05 version 8.5.1 release 1999)" ETSI EN 300 910 v8.5.1 (2000-11)
4. "Information technology - telecommunications and information exchange between systems - Local and metropolitan are networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications" IEEE 802.11 standard.
5. B. Razavi, *RF Microelectronics* Prentice Hall, 1998