THE DESIGN, BUILDING, AND TESTING OF A CONSTANT ON DISCREET JAMMER FOR THE IEEE 802.15.4/ZIGBEE WIRELESS COMMUNICATION PROTOCOL

A Thesis
presented to
the Faculty of California Polytechnic State University,
San Luis Obispo

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in Electrical Engineering

by
Alexandre Jacques Marette
June 2018

COMMITTEE MEMBERSHIP

TITLE:	The Design, Building, and Testing of a Constant On Discreet Jammer for the IEEE 802.15.4/ZigBee Wireless Communication Protocol
AUTHOR:	Alexandre Jacques Marette
DATE SUBMITTED:	June 2018

COMMITTEE CHAIR:	Vladimir Prodanov, Ph.D. Associate Professor of Electrical Engineering
COMMITTEE MEMBER:	Dennis Derickson, Ph.D. Electrical Engineering Department Chair
COMMITTEE MEMBER:	Bruce DeBruhl, Ph.D. Associate Professor of Computer Science

ABSTRACT

The Design, Building, and Testing of a Constant On Discreet Jammer for the IEEE 802.15.4/ZigBee Wireless Communication Protocol

Alexandre Jacques Marette

As wireless protocols become easier to implement, more products come with wireless connectivity. This latest push for wireless connectivity has left a gap in the development of the security and the reliability of some protocols. These wireless protocols can be used in the growing field of IoT where wireless sensors are used to share information throughout a network. IoT is being implemented in homes, agriculture, manufactory, and in the medical field. Disrupting a wireless device from proper communication could potentially result in production loss, security issues, and bodily harm. The 802.15.4/ZigBee protocol is used in low power, low data rate, and low cost wireless applications such as medical devices and home automation devices. This protocol uses CSMA-CA (Carrier Sense Multiple Access w/ Collision Avoidance) which allows for multiple ZigBee devices to transmit simultaneousness and allows for wireless coexistence with the existing protocols at the same frequency band. The CSMA-CA MAC layer seems to introduce an unintentional gap in the reliability of the protocol. By creating a 16-tone signal with center frequencies located in the center of the multiple access channels, all channels will appear to be in use and the ZigBee device will be unable to transmit data. The jamming device will be created using the following hardware implementation. An FPGA connected to a high-speed Digital to Analog Converter will be used to create a digital signal synthesizer device that will create the 16-tone signal. The 16-tone signal will then be mixed up to the 2.4 GHz band, amplified, and radiated using a 2.4 GHz up-converter device. The transmitted jamming signal will cause the ZigBee MAC layer to wait indefinitely for the channel to clear. Since the channel will not clear, the MAC layer will not allow any transmission and the ZigBee devices will not communicate.

Keywords: IEEE 802.15.4, ZigBee, Jammer, Digital Signal Synthesizer, Software Defined Radio

ACKNOWLEDGMENTS

Firstly, I would like to thank my advisor, Dr. Prodanov, for pushing me to pursue a challenging project that covers a broad range of electrical engineering topics. His guidance, knowledge, and motivation in the many topics sampled greatly helped me over my thesis process.

In addition to my advisor, I would like to thank the additional committee members: Dr. Derickson and Dr. DeBruhl. Their comments and incites helped refine my thesis report to ensure an understanding from multiple perspectives.

My sincere thanks go out to the entire Electrical Engineering staff and faculty. Special thanks to Dr. Zhang, Dr. Danowitz, and Dr. Arakaki whose classes in signals and systems, digital design, and RF analysis respectively helped me gain the knowledge necessary to implement many of the special concepts required by this project.

Many thanks go out to my peers and classmates throughout the years. Special thanks to those who spent late nights in the graduate resource lab working before deadlines, those who procrastinated with mindless talks and endless coffee runs, and for those who helped by simply listening to my rants and concerns.

I thank Corey Harris for special contributions to my project in the form of a donated 10 dB coupler and for additional trouble shooting solutions.

Lastly, I would like to thank my family and loved ones: my mom, my sister, my brother, Emily Whitaker, Ted and Jennifer Worden, Morty Lopez, and Pedro for the immense support throughout my many years of my academic life. There is no doubt that I would not be here without these people in my life.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This thesis report describes the design, building, testing, and analysis of a discrete IEEE 802.15.4/ZigBee jamming device that will jam either a selected number of ZigBee channels or all the ZigBee communication channels. This report will discuss the ZigBee protocol and its weakness, the general design to exploit the weakness. and the final system design. This report will explain the complete process for creating the jamming device, from initial plan to final construction. It will describe the challenges faced and how these challenges were overcome. The project is structured into two stages (the Digital Synthesizer design and the Analog Upconverter design) and the report will discuss the building and testing of each design. The report will go over the integration of the two designs and the outcome of the ZigBee jamming attempt along with a full characterization of the integrated device.

1.1 Statement of Problem

Sensors are becoming an integral part of the modern world. There are sensors are in our homes, phones, cars, and soon within human beings [1], [2]. These sensors are part of the ever-growing idea of the Internet of Things (IoT). The idea behind the IoT is that all things (humans, machines, data, etc.) are connected to one another. They share data and computing resources to aid in the operation of advanced everyday actions such as autonomous driving, autonomous farming, or keeping track of stock in a grocery store. IoT is being implemented for safer, more efficient, and more reliable operations in day to day life. The term “smart” is not just for phones anymore. Now with the growing idea of IoT there are smart homes, smart hospitals, smart farms, and of course smart cars.

The use of sensors and communication nodes are required to enable real time, intelligent monitoring and control of IoT network. Although, wired solutions have been used in the past, over the past decade wireless communication sensors have been the focus. This is due to the

accessibility and the ease of implementation of low cost, low power, complete communication devices often integrated on a single chip [2]. Although developed independently from IoT, the Wireless Sensor Network (WSN) has become an essential concept for IoT design [2]. A WSN is a large network of sensor nodes that sense physical quantities such as light, pressure, and temperature within an environment. They also have the ability to control the environment and therefore allow for an interaction between the environment and a controller whether it be a person or a computer. [2]

As with any wireless communication method, extra security precautions must be taken. This is because a signal is much more vulnerable to interception (eavesdropping) or interruption (jamming) when it is propagating through free space rather than when it is propagating through a cable [3]. This additional security risk must not be taken lightly especially when a sensor is linked to the safety or security of the end user. This is a prominent concern as WSNs begin to play large roles in vehicles, medical devices, and home security devices [4]. Additionally, due to the limited unlicensed ISM frequency bandwidth, any new wireless communication protocols must minimally interfere with current protocols already operating in the same frequency range [5]. This concept is called Wireless Coexistence, and the design decisions used to ensure Wireless Coexistence are believed to be a cause of a large security risk in the IEEE 802.15.4/ZigBee protocol.

1.2 IEEE 802.15.4/ZigBee Background

In 2003 IEEE released the 802.15.4 standard [6]. This standard was designed to meet the wireless sensor requirements by enabling low cost, low data rate, low complexity, and low power consumption wireless communication. The IEEE 802.15.4 standard specifies the RF Link Layer and the Data Link Layer. As with most other IEEE 802 standards, this allows for industry to create protocols that integrate with the existing standard by stacking software protocol layers onto the existing link layer defined by 802.15.4. One of the most popular protocols stacked onto the

existing layers of the 802.15.4 standard is the ZigBee Mesh protocol created by the ZigBee Alliance. Figure 1-1 shows how the layers defined by the 802.15.4 standard and the layers added by the ZigBee protocol combine to create a wireless network device [7].

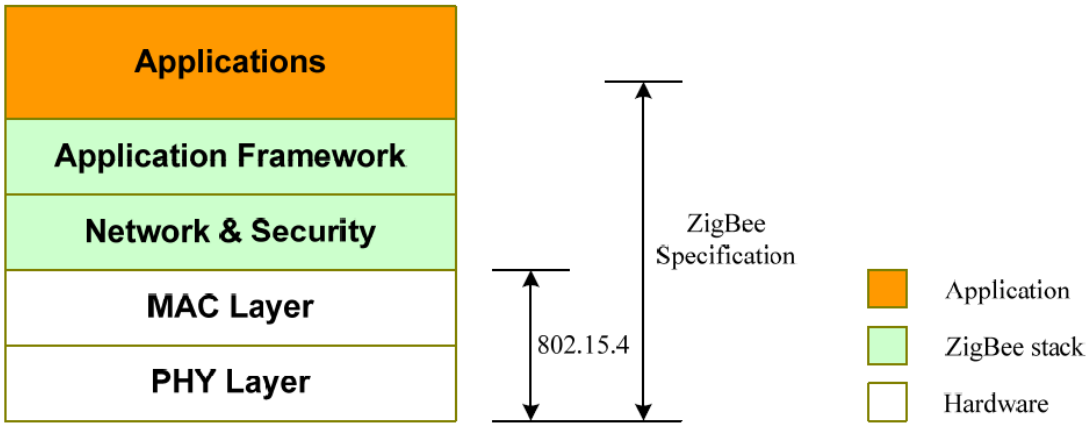


Figure 1-1: The ZigBee/IEEE 802.15.4 protocol stack [7]

ZigBee has begun to dominate the WSN field due to the better applicational performance when compared to WIFI or Classic Bluetooth [8]. For example, in a large wireless sensor network like thermometers throughout a farm, there could be hundreds of sensors throughout the network many of which run of a small battery. The power savings, cost savings, and large device support of the ZigBee protocol make it the top choice for wireless sensor networks [8]. Figure 1-2 compares some of the ZigBee performance specifications with that of other top wireless communication protocols.

Standard	ZigBee/IEEE 802.15.4	Bluetooth	UWB	IEEE 802.11 b/g
Working frequency	868/915 MHz, 2.4GHz	2.4 GHz	3.1 - 10.6 GHz	2.4 GHz
Range (m)	30 – 75+	10 – 30	~10	30 – 100 +
Data rate	20/40/250 kbps	1 Mbps	100+ Mbps	2 – 54 Mbps
Devices	255 – 65k	8		50 – 200
Power consumption	~1 mW	~40 – 100 mW	~80 – 300 mW	~160 mW – 600W
Cost ($US)	~2 – 5	~4 – 5	~5 – 10	~20 – 50

Figure 1-2:Comparison of different wireless technologies [7]

As mentioned above, the ZigBee protocol can be deployed in a mesh network topology. The mesh network topology also allows for the ability to communicate over large distances by hopping the message from one radio to another. To allow this mesh network to work properly, every 802.15.4 standard network has two different types of radio classifications: a full function device (FFD or router) and a reduced function device (RFD or end device). Both routers and end devices can have non-communication roles such a sensors or controllers but typically routers have a constant power source while an end device is typically battery powered and has a low complexity role such as operating a switch. In addition to FFD and RFD radios, one device is assigned as the PAN coordinator which is responsible for managing all the other devices on the mesh network as well as routing the information to the end user or application. An FFD can transmit and receive information from another FFD, PAN, or associated RFD while an RFD can only transmit and receive information with a single FFD (which can include the PAN coordinator). Figure 1-3 shows an example of the ZigBee mesh network topology [6].

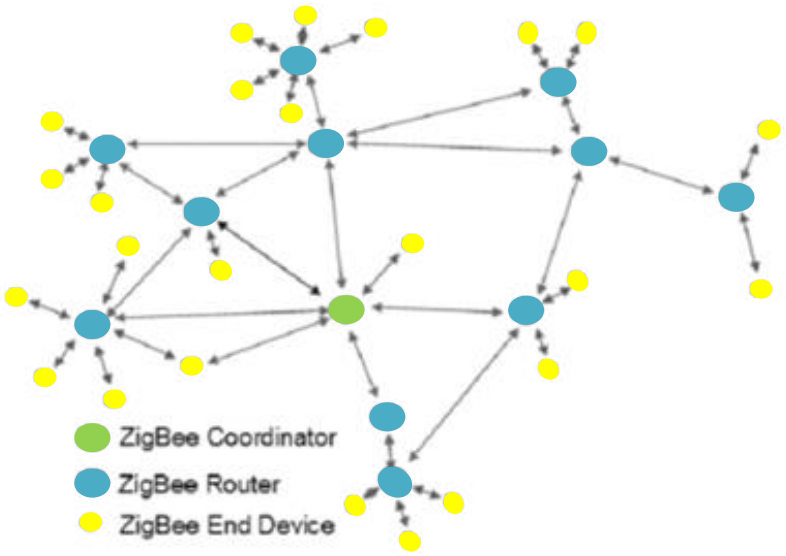


Figure 1-3: ZigBee Mesh Network and Device Types [6]

As with other IEEE 802 standards, the IEEE 802.15.4 standard specifies the RF link layer and the Data Link Layer. The RF Link Layer consists of a RF layer which is the physical medium in

which the information is passed and a PHY or physical layer which controls the RF channels and data transmission. The Data Link Layer consists of the Medium Access Control (MAC) layer and the Link Layer Control. The MAC layer provides an interface between the higher layers and the PHY layer.

The PHY describes the frequency band utilization, data rates, modulation schemes and many other requirements needed to transmit and receive information over a wireless channel. In the PHY of IEEE 802.15.4 there are three bands and 27 total different channels. This thesis project focuses on the 2.4 GHz band which contains 16 channels, channels 11-26. The channel spacing is 5 MHz and the channel bandwidth is 2 MHz. Equation 1-1 gives the channel center frequencies with respect to channel number. Figure 1-4 shows the channel distribution at the 2.4 GHz band.

$$F_C = 2405 + 5(\text{Channel} - 11)\ \text{MHz} \tag{1-1}$$

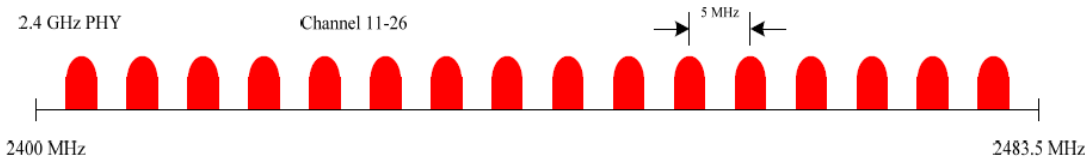


Figure 1-4: Arrangement of Channels in IEEE 802.15.4 2.4 GHz Band [7]

The 2.4 GHz band uses an Offset Quadrature Phase Shift Key (O_QPSK) modulation scheme which allows for a data rate of 250 kbps [9]. For security against random errors and multipath issues, the PHY layer employs a Direct Sequence Spread Spectrum (DSSS) within each channel. Combining QPSK and DSSS means that 4 bits of information are packed into one symbol, and each symbol is then chipped at 32 chips per symbol at the 2.4 GHz band [9]. The PHY layer also is responsible for energy detection. The energy detection command is given by the MAC layer when using Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) to control the channel utilization. The command is called the clear channel assessment (CCA) [10]. This channel control helps reduce interference between devices and helps wireless coexistence by

insuring that the standard does not transmit over any other RF signals within the same band. CSMA-CA works by first checking the channel for any power before the radio can transmit. If the channel is busy, by either another RF signal such as Bluetooth or WIFI or by another IEEE 802.15.4 radio on the same mesh network, the radio waits for a predetermined amount of time before checking the channel again [6]. This is the design decision in the IEEE 802.14.5 standard that this thesis work will exploit.

By placing power within a channel, any device using that channel will be forced to wait for the channel to open. If the channel does not open, the transmission is considered a failure. This CSMA-CA logic flow can be seen in Figure 1-5.

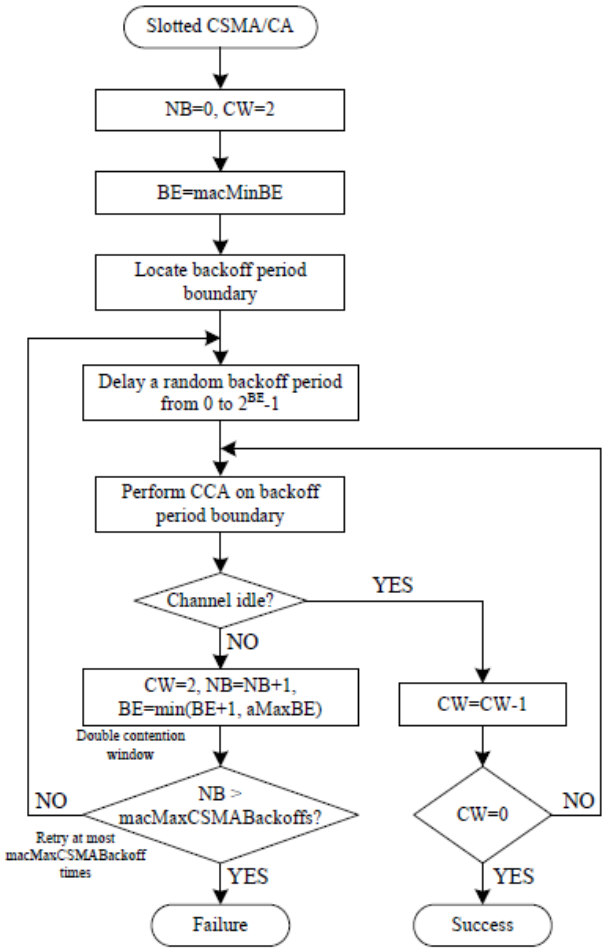


Figure 1-5: The Basis slotted CSMA mechanism in IEEE 802.15.4 [7]

If power is placed in all the 16 channels of the 2.4 GHz band, the IEEE 802.15.4 standard, and subsequently any protocols using the standard such as ZigBee, will fail to transmit.

2 DESIGN OVERVIEW

This project has two objectives. The first and main objective is to produce a device that will create a 16-tone signal to exploit the weakness in the 802.15.4 standard and completely disable a mesh network from any data transmission to or from the PAN coordinator radio. This device will produce a tone in each of the 16 channels (channels 11-26) in the 2.4 GHz band of the IEEE 802.15.4 standard. The secondary objective is to create a device that will be used as a teaching tool by interfering with select IEEE 802.15.4 channels and monitoring the ZigBee mesh network and its response to the interference. To aid in this disturbance, the device must be able to place power in selected channels and leave other channels open to properly monitor the ZigBee dynamics.

Combining the two objective leads to a device that can create a multitone signal with any combination of tones ranging from 2405 MHz to 2480 MHz in 5 MHz increments. Figure 2-1 shows how the spectrum of this device will look both in the full jamming mode and the channel interference mode.

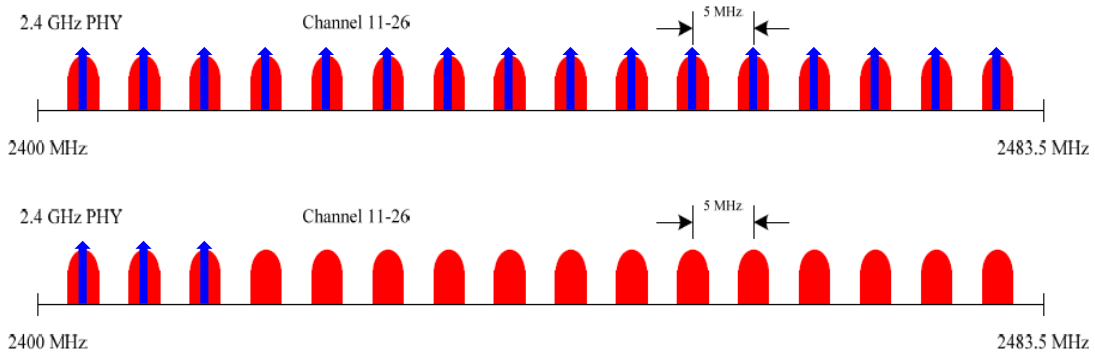


Figure 2-1:16-tone Signal used for complete ZigBee Jamming (top). Multi-tone Signal used for channel interference in Channels 1-3 while the remaining channels are left open (bottom).

2.1 Multi-tone Signal Generation

There are many ways to create a multi-tone signal with 5 MHz spacings but by adding the requirement of selecting any combination of frequencies, the problem becomes more challenging. The first consideration was to use a step recovery diode (also known as a frequency multiplier) to create the 5 MHz harmonics followed by selective filters to choose the desired signals [11]. In theory, the step recovery diode is not difficult to implement and was simulated using Advanced System Design (ADS). Figure 2-2 shows the result of the simulation.

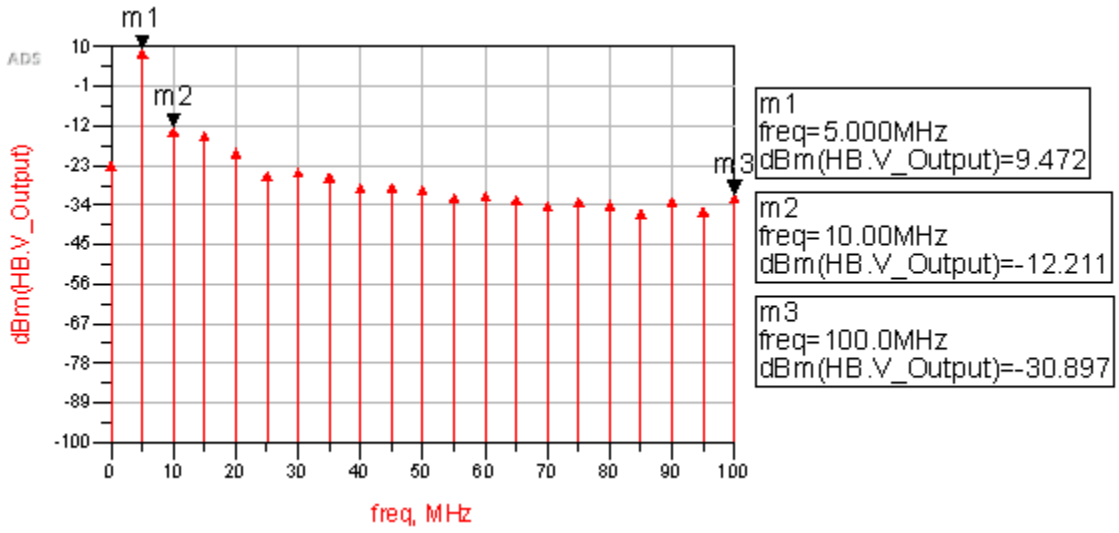


Figure 2-2: ADS Step Recover Diode Simulation

Although the step recovery diode is not difficult to implement, there are many problems that make it a poor approach for this project. The main issue is having a series of filters to condition the signal and to select the different channels. The 5 MHz component is roughly 20 dB larger than the next harmonic. Additionally, the power level after the last required 80 MHz tone does not drop off. Filters would be needed to isolate the 5 MHz to 80 MHz range and to help flatten the response of the tones. A filter of this specific purpose would be hard to find or build.

Additionally, a series of band stop filters would be needed at each harmonic along with a bypass to enable and disable any combination of desired tones. Lastly, a mixing circuit would be required to mix the entire signal up to 2.4 GHz. The series filters would cause the jammer to become very large physically and require repetitive work not beneficial to thesis research.

The next option was to use frequency synthesizers or phase locked loops with integrated voltage-controlled oscillators. This method would require 16 frequency synthesizers and 15 couplers such as a branch line coupler. The biggest benefit of this design is the accuracy of the tones and the simplicity of the design. By using frequency synthesizers every desired tone could be created from 2.405 GHz to 2.480 GHz which removes the need of filters and mixers. Additionally, this method makes turning off any tone very easy by simply disabling the synthesizer. Since most synthesizers have 50 Ohm outputs, disabling it simply acts like a 50 Ohm termination on one of the coupler inputs. This method was also simulated using ADS. Figure 2-3 shows this simulation with the two center frequencies (2.440 and 2.445 GHz) disabled.

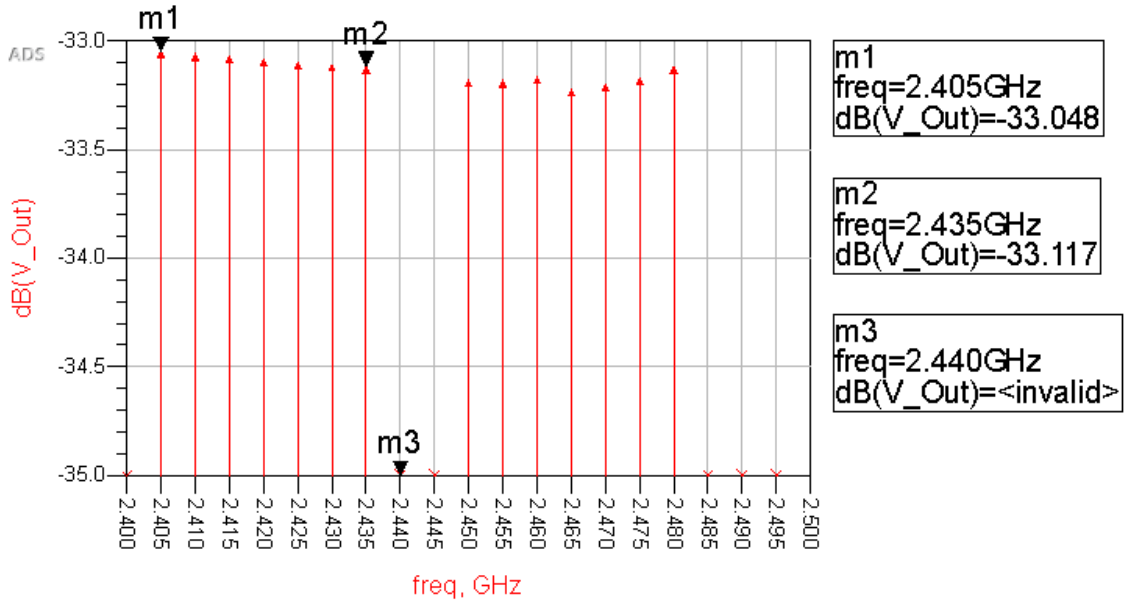


Figure 2-3: ADS Simulation of16 Frequency Synthesizers and 15 Couplers with channels 18 and 19 Disabled

The problems with this approach are cost, layout size, and layout complexity. The MAX2870 dual output PLL with integrated VCO was the best choice for this approach. Since this device is a dual output device, a total of 8 of these PLLs would be needed. At a cost of over $11 each, this would cost more than $90 in just the PLL not including board design and other components needed. This PLL, along with most others, is digitally controlled and requires a micro-controller to operate adding to the cost and complexity. The footprint of the MAX2870 is 32 Thin Quad Flat Pack No-Lead (TQFN) meaning there are 32 connecting pads that can only be soldered using a heat gun or reflow oven [12]. Figure 2-4 shows this footprint.

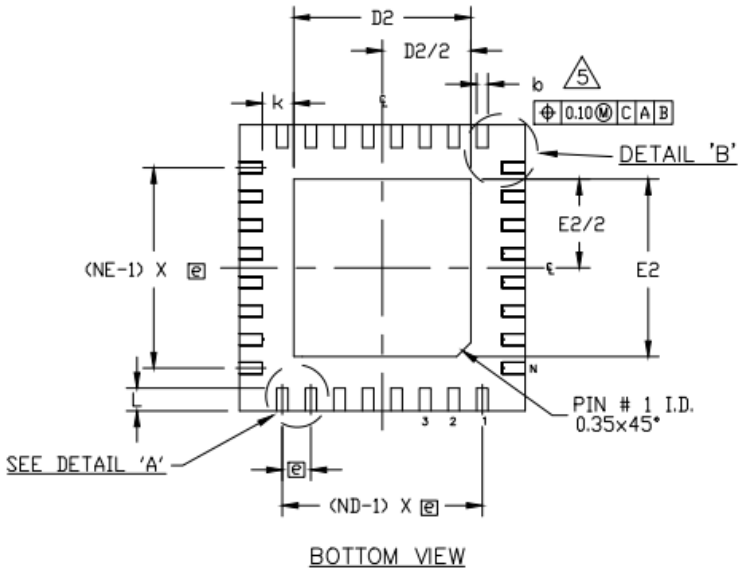


Figure 2-4:MAX2870 32 TQFN Footprint [12]

Trying to create a PCB design with 8 of these synthesizers along with the necessary passive devices, microprocessor, and power supplies would be very complex. This design would also require 15 couplers which would add to the complexity and size of the PCB design. This design was ruled out do the high cost estimate, PCB design complexity, and PCB size estimate.

The next consideration focused on high speed digital to analog converters (DAC). The original plan was to use a microprocessor to load a standalone first in first out (FIFO) with a discrete

version of the multi tone signal. Then the FIFO would feed the highspeed DAC using a single PLL. This design was preferred due to the broad scope of the project along with the ability to change the output signal to any desired signal by simply changing some code in the microprocessor. Further research showed that instead of a separate PLL, microprocessor, and FIFO, all these devices could be combined onto one FPGA (field programmable gate array).

2.2 Top Level Overview

The final design proposition included an FPGA that feed a highspeed DAC. This FPGA sends the DAC the discrete version of the multitone signal from 5 MHz up to 80 MHz. From there the signal would be mixed up to 2.4 GHz and then amplified before being radiated by an antenna. Figure 2-5 shows the early block diagram for the final design proposal.

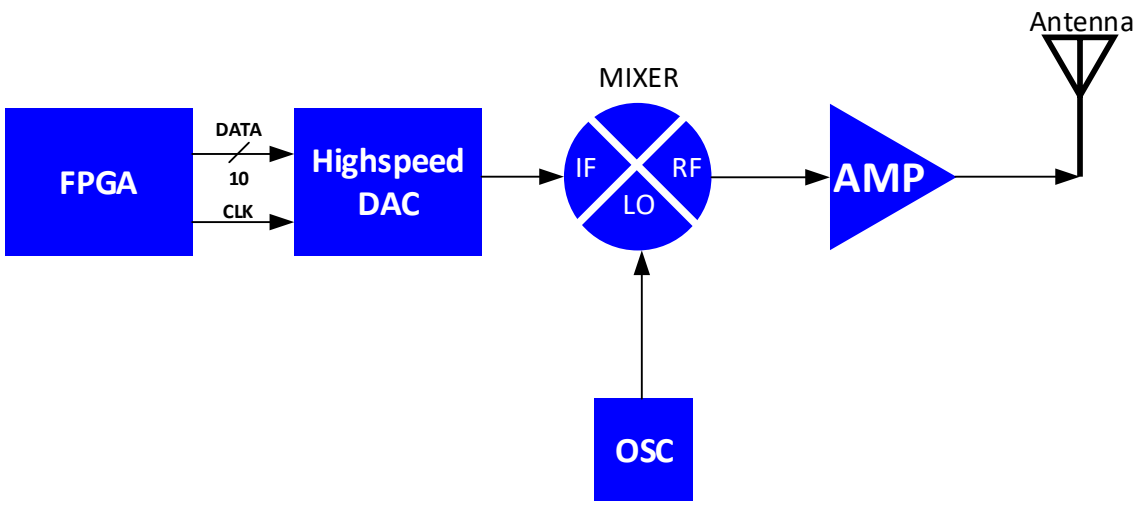


Figure 2-5: Early Top-Level Block Diagram

The FPGA allows for a much simpler block diagram by combining the microprocessor, the PLL, and the FIFO all into one unit. Also, the FPGA is beneficial because it is customizable. If there is a problem with the FPGA design, it can easily be fixed using software. This design also allows for many different applications if desired by future users. By changing the HLD code one could

change this jammer into a broadcast device or a spoofer. Expanding on the idea of future uses, it was decided that this design would be split into two separate boards.

Separating this design into a digital frequency synthesizer board and a 2.4 GHz up converter/amplifier board one could use these devices separately for many other applications. The digital frequency synthesizer could create any desired signal from 1 MHz to 105 MHz including a modulated signal using digital modulation within the FPGA. The analog upconverter would be useful in mixing any input signal up to 2.4 GHz. Separating the analog and digital into two separate boards helps reduce the complexity in mixed signal and highspeed PCB design. The Digital board would deal with issues in mixed signal design, but it would be relatively low frequency. The analog board would have no digital design concerns but at 2.4 GHz, high frequency design would need to be taken into consideration. The separated boards can be seen in the block diagram in Figure 2-6.

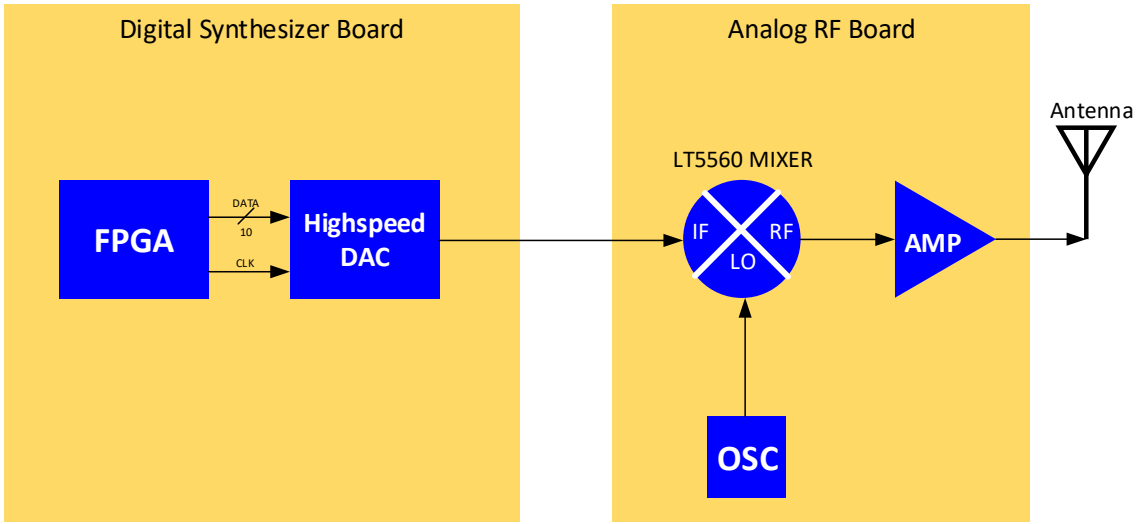


Figure 2-6: Block Diagram with Separate Boards

2.3 Device Requirements

As a jammer, this device is required to produce 16 tones from 2405 MHz to 2480 MHz with enough power for the 802.15.4 PHY layer to consider that the channel is in use. In IEEE 802.15.4

the clear channel assessment (CCA) uses the energy detection (ED) mechanism to decide whether a channel is open or not. If there is any energy above the ED threshold, the channel is considered taken. The ED threshold is 10 dB above the maximum allowed receiver sensitivity [10]. In the ZigBee protocol the maximum receiver sensitivity for channels 11-26 is -85 dBm [7]. This means that if a channel has a power of at least -75 dBm at the receiver, the channel is considered occupied.

The for this project, the jamming device is required to attack a network within the same room. With a jamming distance of roughly 3m, the jamming device could be placed anywhere within a small room and still attack a network. Equation 2-1 is the Friis power equation and it is used to calculate the power budget of a wireless link.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2} \tag{2-1}$$

By knowing the gain of both the receiver and transmitter antennas, wavelength, distance between radios, and the transmit power, one can calculate the received power. This equation can be rearranged to solve for the transmit power required for the receiver to detect a minimum of -75 dBm with the jammer at 3 meters away. The gain of the antenna on the jamming device is 5 dBi and the maximum gain of the Digi XBee PCB antenna is 1.5 dBi [13].

$$P_t = \frac{P_r(4\pi \mathrm{R})^2}{G_t G_r \lambda^2} = \frac{10^{-7.5}(4\pi \times 3)^2}{10^{0.5} \times 10^{0.15}\left(\frac{2.998 \times 10^8}{2.4 \times 10^9}\right)^2} = 644.7 \text{ nW} = -31.9 \text{ dBm} \tag{2-2}$$

Equation 2-2 shows that at least -31.9 dBm transmit power is needed per channel to jam the ZigBee radios at 3 meters from the coordinator. Doubling (adding 3 dB) the power four times results in the combined output power for all 16 tones to be -19.9 dBm.

It is required that the output power of the jamming device be adjustable. The analysis above calculated the minimum power needed. Ideally, the output power of the jamming device should be well over the minimum while also being able to achieve the minimum power and slightly below minimum power. This would allow better analysis of jamming the 802.15.4 standard

including testing at what minimum transmit power the device successfully jams the ZigBee radios. To meet this requirement the Analog Upconverter will rely on a variable gain amplifier (VGA) or a variable attenuator.

This device must easily be able to change what tones are activated without having to reprogram the FPGA. This will allow quick changes to the jamming signal to see how the ZigBee protocol reacts when a transmitting channel becomes occupied. This will require 16 dip switches connected to the FPGA that will act as an on off switch for each channel.

3 DIGITAL SYNTHESIZER DESIGN

3.1 Overview

The digital synthesizer was designed to work by using the on board read only memory (ROM) on the FPGA to store one period of discrete data from each channel center frequency. The on-board switches would then select which ROMs would be routed to a summing and normalization block. The summing and normalization block would sum all the data in the selected ROMS and then divide the results by the total number of signals selected. The output of the summing/normalization block would then feed the FIFO. Once, the entire period is loaded, the output of the FIFO will feed both the DAC and loop back into itself for continued signal output. Figure 3-1 shows the early block diagram for the FPGA design.

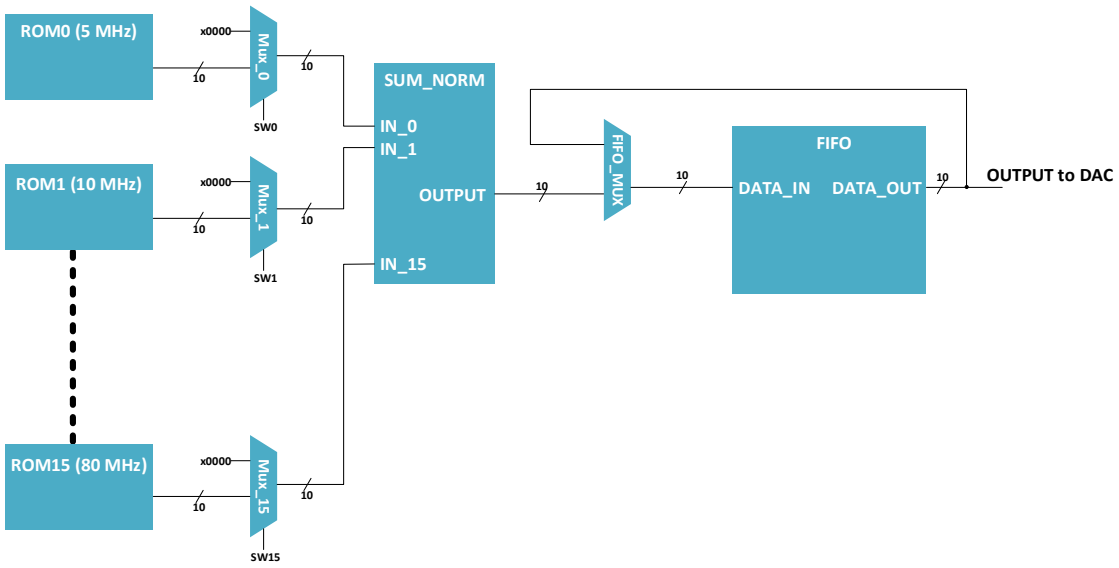


Figure 3-1:Early FPGA Block Diagram

The key of this design is that every ROM block contains one period of digital data and that the period of data is then repeated within the FIFO. After the FIFO, the digital signal is ported out of the FPGA using the IO (in-out) ports and feed into the DAC along with the DAC clock signal.

The DAC will convert the signal into an analog waveform where it can be routed to the analog board for mixing and amplification.

3.2 FPGA Design

Before any FPGA design could begin, a FPGA brand, product family, synthesis software, and simulation software would need to be chosen. The Xilinx Artix 7 with Vivado was an easy choice due to the familiarity with these resources from previous course works. The Bases 3 development boards with Artix 7 FPGAs were readily available for use and the Vivado software pack contained everything needed for synthesis, implementation, and simulation. Using Vivado, a very rudimentary draft of the system was designed to get a rough idea of the hardware and resource utilization required by the design. Figure 3-2 shows the results of the implementation.

Name	Constraints	Status	WNS	TNS	WHS	THS	TPWS	Total Power	Failed Routes	LUT	FF	BRAM	URAM	PCIe %
synth_1 (active)	**constrs_1**	**synth_design Complete!**								**558**	**11**	**0**	**0**	**0.000**
impl_1	constrs_1	route_design Complete!	0.124	0.000	0.121	0.000	0.000	0.230	0	473	32	9	0	0.000

Figure 3-2: First Run FPGA Implementation Results

By referencing the Xilinx Artix 7 family table, one can see that the resource utilization of the hardware is roughly 5% of the smallest FPGA offered by the family [14].

The signal degradation issues when interfacing with highspeed DACs meant that an FPGA development board could not be used. Since a custom board was to be designed, component packages were considered to simplify the manufacturing process and to greatly reduce cost. One of the considerations was to avoid a component with a ball grid array. Ball grid arrays require multiple layers along with blind and buried vias to route all the signals away from the FPGA to other components. All the Artix 7 FPGA come in some sort of ball grid array. This along with the high cost of the Artix 7 caused it to be a bad choice for this project.

The Xilinx Spartan 3A is a modern redesigned version of the older Spartan 3. The Spartan 3A comes in many packages including Quad Flat Pack and Ball Grid Array. The Quad Flat Pack is

only offered in the 50k and 200k gate sizes. The Spartan 3A in quad flat pack is much easier and cheaper to implement and is 4 times cheaper to purchase than the Artix 7.

In addition, I.O pads, PLL Clock speeds, and I.O standards must be considered before committing to an FPGA. At this point, the DAC had not yet been chosen but specifications for interfacing were known. From the Nyquist Criterium, the sampling rate and clock signal into the DAC from the FPGA must be no less than 160 MSPS or MHz (twice the highest frequency of 80 MHz). The DACs in consideration ranged from a sampling rate of 200MSPS to 500 MSPS and ranged from 10 to 16-bit parallel feed. This would require at least 16 200-500 MHz data outputs all on the same side of the FPGA Quad Flat Pack. Lastly the communication standard required from the DACS in consideration were Low Voltage CMOS (LVCMOS) and Low Voltage Differential Signals (LVDS).

By referencing the Spartan-3A FPGA Family Data Sheet [15], one can see that the Spartan-3A meets all of the above requirements. The I.O capabilities section of the data sheet detail the supported interfacing standards which include LVDS and LVCMOS. Under the Features section, the data sheet states that the Digital Clock Mangers can create frequencies ranging from 5 MHz to 320 MHz. This eliminates the DACs in the 500 MSPS range but still allows proper interfacing with the lower 200-300 MSPS DACs. Lastly, within the Pinout Description section of the data sheet, it states that the smallest package (VQ100) contains a total of 68 different I.O ports for single ended interfacing and or 60 different I.O ports for differential interfacing. The package foot print from the data sheet, Figure 3-3, show than any side of the FPGA has enough IO ports to feed the DAC.

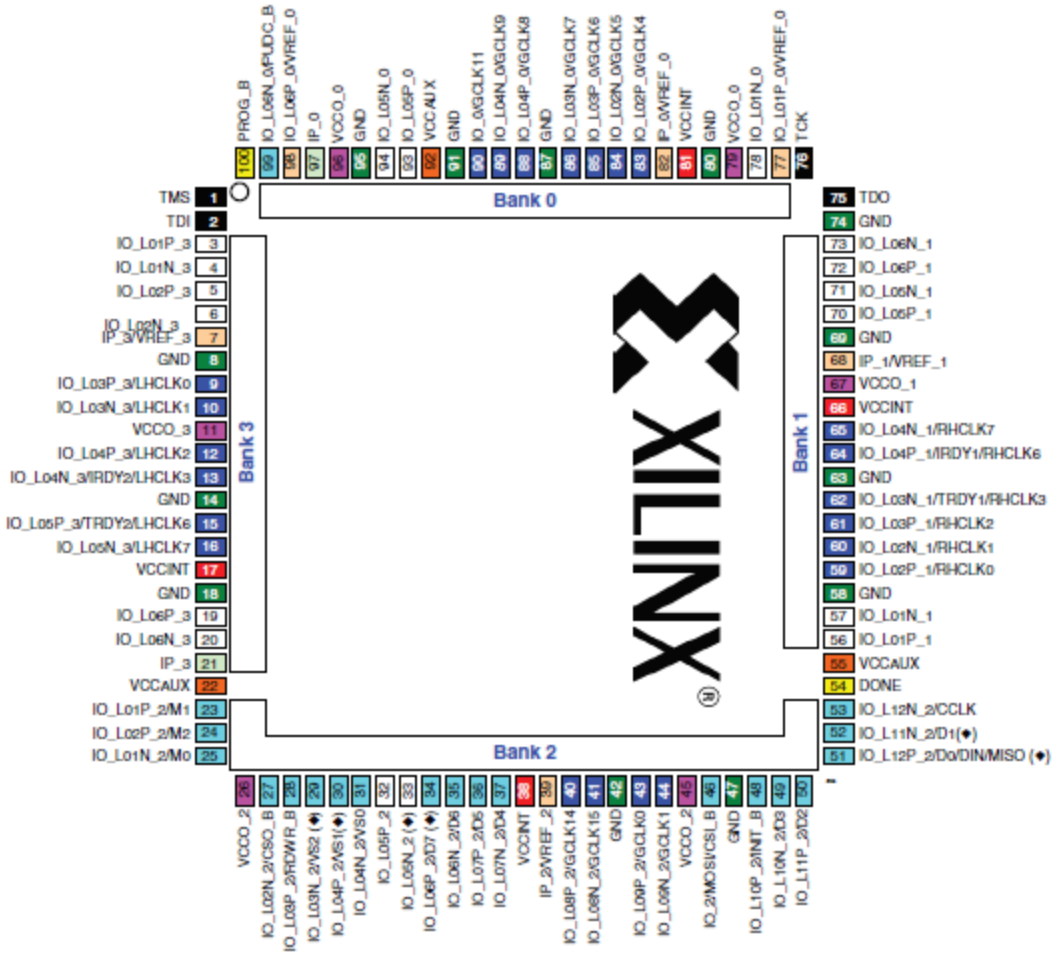


Figure 3-3:VQ100 Package Footprint - XC3S200A (Top View) [15]

At this point the Spartan 3A using the VQ100 package seemed to be a good fit for the project. Unfortunately, the Xilinx Vivado FPGA design software does not support the Spartan 3A and so the old ISE Design Suite had to be used. Figure 3-4 shows the black box diagram for the HDL code written on ISE Design Suite.

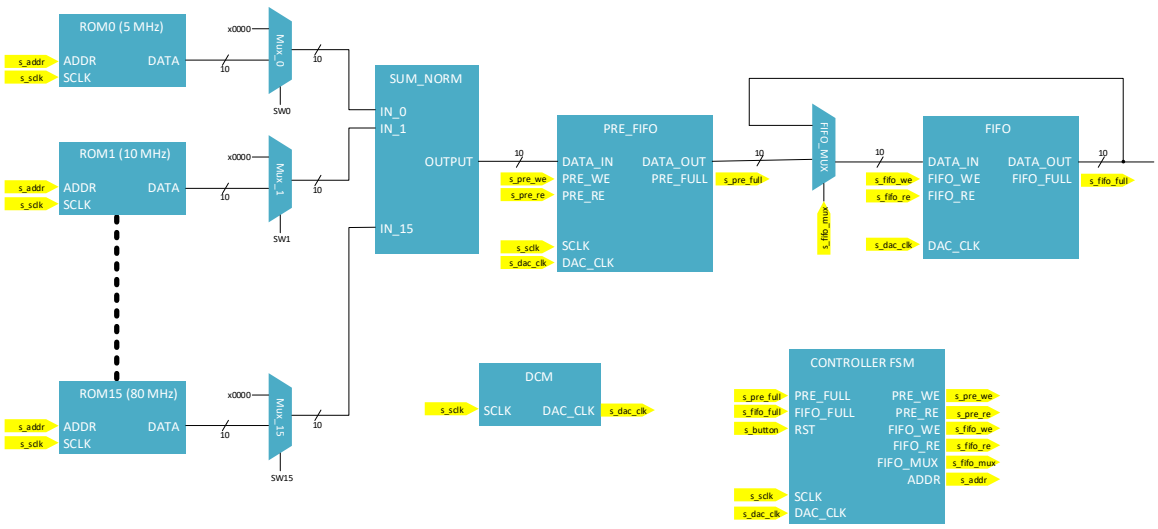


Figure 3-4: Spartan 3A FPGA Black Box Diagram

The FPGA hardware starts with 16 ROMs that contain the digital data for each of the 16 channel tones. The ROMs were created by using the Xilinx IP (intellectual property). The ROMs could be loaded manually in the code or by using a coe file. The coe file was a better choice for ease of modifications in the future. Additionally, at this point, the DAC was not chosen, so the sampling rate and word size were unknown. By using coe files, the data in the ROMs could easily be changed. MATLAB was used to create the coe files. The MATLAB script requires sampling rate, desired frequencies, and word length as inputs and then output a coe file for each desired frequency. Within the coe files are binary numbers that create a digital waveform at the desired channel frequencies. To ensure each coe file had the same number of words, the higher frequencies had multiple periods in them. The MATLAB script can be seen in the **Error! R eference source not found.**. The output of the MATLAB code can be seen in the visual representation in Figure 3-5. Note that at the higher frequencies the low sampling rate degrades the time domain signal but according the Nyquist Criterion, no information is lost.

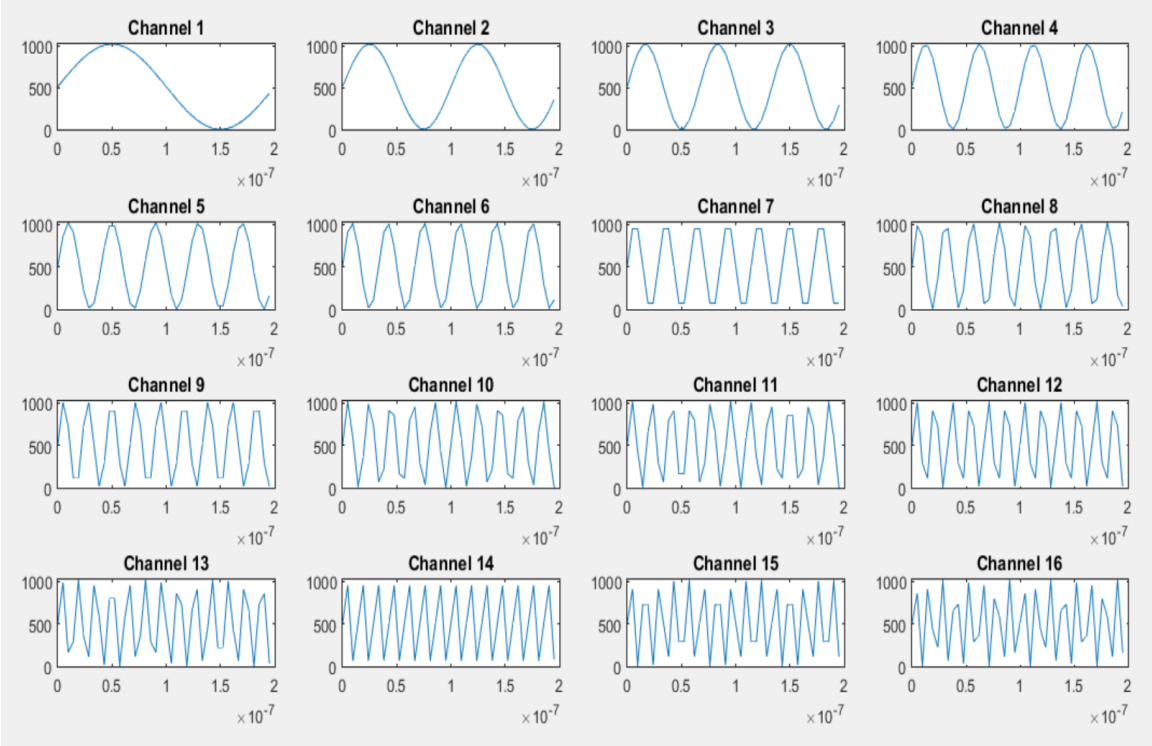


Figure 3-5: MATLAB Waveform Creator Output for ZigBee at 210 MSPS and 10-bit Words

Multiplexers are placed after the ROMs and either pass the ROM data or pass a 10 bit zero. The Multiplexers are controlled by the physical switches that will be placed on the board. The signals from the multiplexers are routed to custom block called SUM and NORM. This block sums all the inputs and then divides the results by the number of switches that are on. This insures that the output of the FPGA will always use the full-scale range of the selected DAC.

Following the SUM and NORM block, two separate FIFOS are needed due to the two different clock speeds. All hardware up to the first FIFO runs at the CLK speed and the hardware following the first FIFO runs at the DAC CLK speed. The CLK is a slower clock signal that will come from an external oscillator. The DAC CLK is a fast clock created by using the slow CLK and a PLL. The DAC CLK runs the second FIFO and will be output to the DAC as well. The original plan was to use just one FIFO and multiplex the CLK and DAC_CLK into the FIFO CLK input. This was not advised due to the speed specific pathlengths used when implementing the FIFOs. Instead, two FIFOs were used. The PRE_FIFO is a two clock FIFO where the write

clock is the slower FPGA clock and the read clock is the faster DAC clock. The second FIFO reads and writes at the DAC clock.

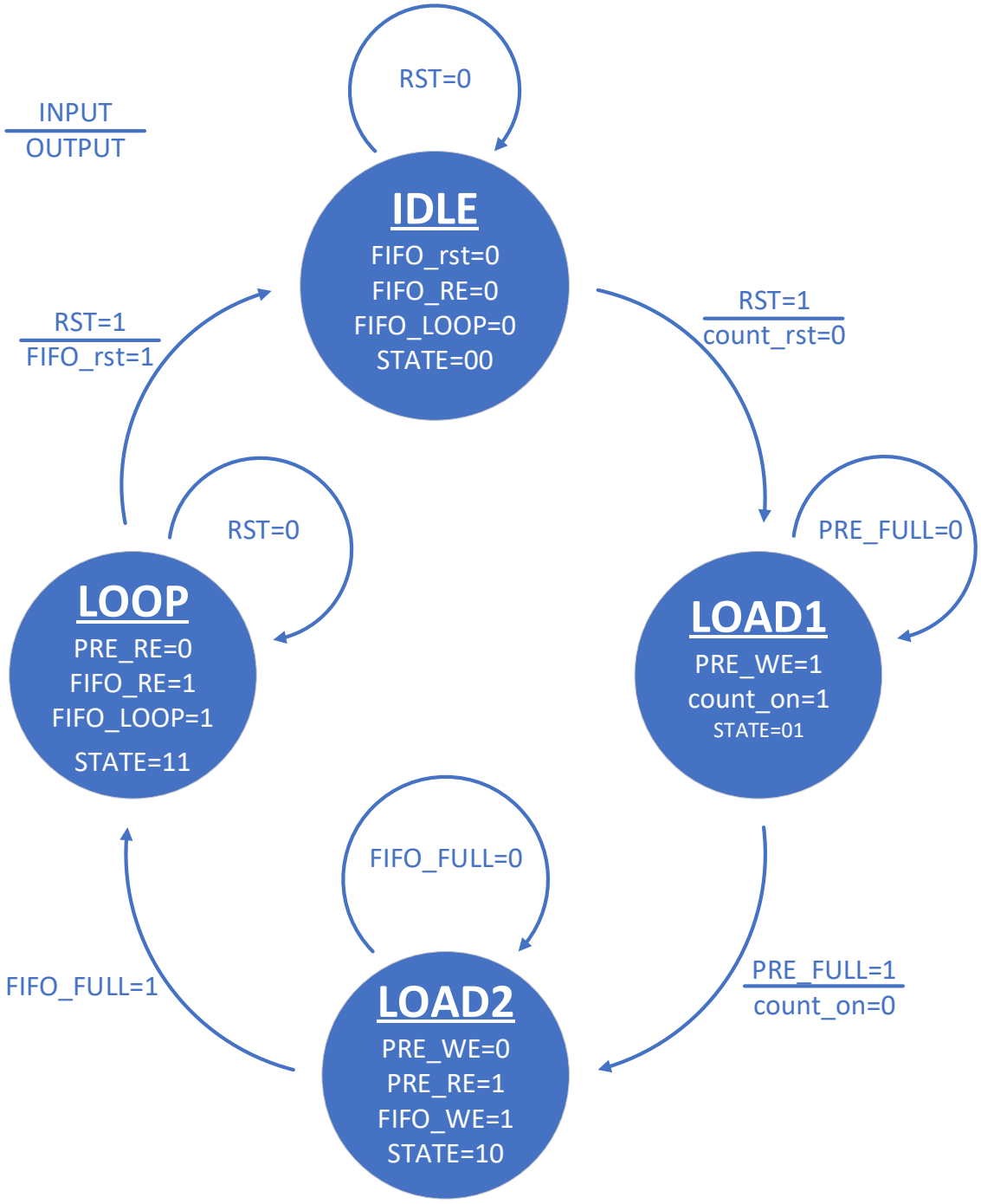


Figure 3-6: FPGA Controller FSM Diagram

A physical button was placed on the board to start the run sequence. When the button is pressed, the data from the ROMs flows through the multiplexers and SUM and NORM block and loads the PRE_FIFO at the slower FPGA clock. When the PRE_FIFO is full with a complete period of data, the data is read from the PRE_FIFO and writes it into the FIFO at the faster DAC clock. Once the FIFO is full, the data is read from the FIFO and is sent to both the DAC and loops back to write into the input of the FIFO. This whole process is controlled by the controller block which consists of two finite state machines (FSM) one running at each of the two clock speeds. Figure 3-6 shows the FSM diagram for the controllers as one single state machine. The second state machine was added during the simulation and testing process due to strict timing constraints. Note that to simplify the diagram only outputs that values' have changed are displayed in the state.

After completing the design, it was synthesized to see what resources the design would use. Before synthesis, the smallest Spartan 3A was chosen, XC3S50A. After synthesis the design utilization summary showed that the number of occupied slices was 880 while the XC3S50A only has 704 slices. The design was then changed to be implemented on the XCS200A which has 1792 total available slices [15]. Figure 3-7 shows the Xilinx ISE Design Suite Device Utilization Summary.

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	344	3,584	9%
Number of 4 input LUTs	1,404	3,584	39%
Number of occupied Slices	880	1,792	49%
Number of Slices containing only related logic	880	880	100%
Number of Slices containing unrelated logic	0	880	0%
Total Number of 4 input LUTs	1,559	3,584	43%
Number used as logic	1,323		
Number used as a route-thru	155		
Number used for Dual Port RAMs	80		
Number used as Shift registers	1		
Number of bonded IOBs	36	68	52%
IOB Flip Flops	1		
Number of BUFGMUXs	4	24	16%
Number of DCMs	2	4	50%
Number of RAMB16BWEs	1	16	6%
Average Fanout of Non-Clock Nets	3.54		

Figure 3-7: ISE Design Suite Synthesis Results with XC3S200A

To test the proper functionality of the code, Xilinx iSim FPGA simulator was used. The simulation set the desired switches to the on position and then activated the run button. Due to the precise timing of the design, much time was spent adjusting signal delays. By using D flip flops and alternating the use of Mealy and Moore FMS design, the timing of the control signals was adjusted until proper operation occurred. This also allowed for a period of the output data to be collected and analyzed. Figure 3-8 shows a screenshot of the iSim simulation with the FPGA data output signal in purple.

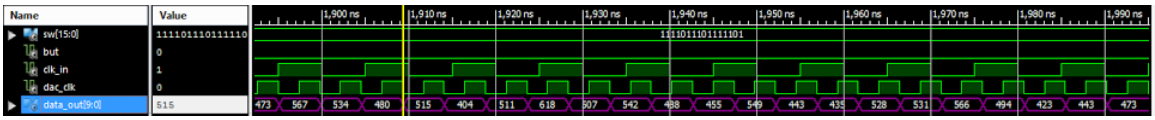


Figure 3-8: Xilinx iSim FPGA Simulation showing the Data Output in Purple

The iSim output data was collected and plotted using MATLAB. Three simulations were conducted: all 16 switches on, switches 1 and 13 off, and switches 5, 9, and 15 off. Three unique

cases showed that the FPGA code worked as designed. The three simulation results can be seen in Figure 3-9.

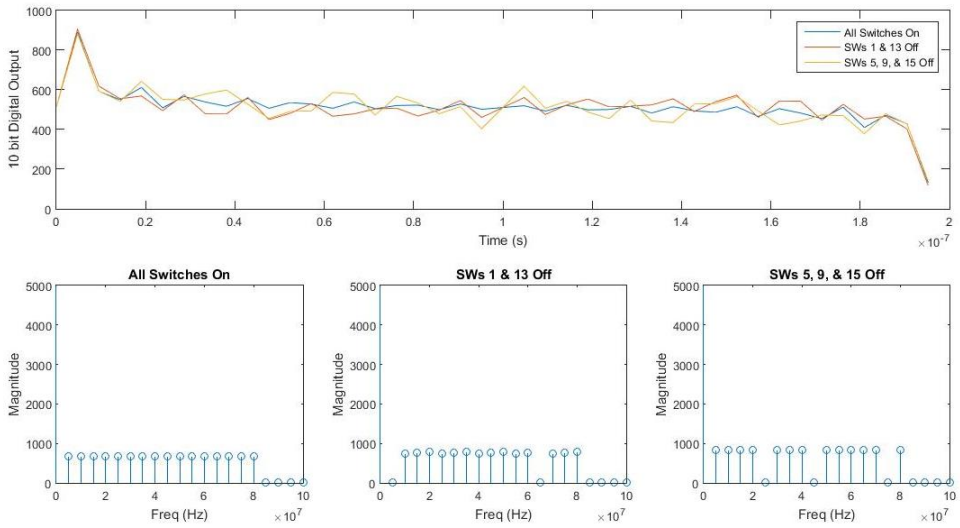


Figure 3-9: FPGA iSim Data plotted using MATLAB showing the Time Domain (top) and the Freq Domain (bottom)

It is important to understand that the DAC has an impact on the quality of the output signal. This will cause the frequency spectrum to have undesired qualities. The operation of the DAC can be estimated using a sample and hold operation. Instead of ramping to each digital data point, the DAC (almost) immediately steps to the data point and holds at the level until the next data point. This impulse contains theoretically infinite frequencies just as a square wave does. This causes the output of the DAC to have a sinc roll off like a square wave. Figure 3-10 demonstrates the sample and hold time domain operation and the sinc roll off frequency domain results.

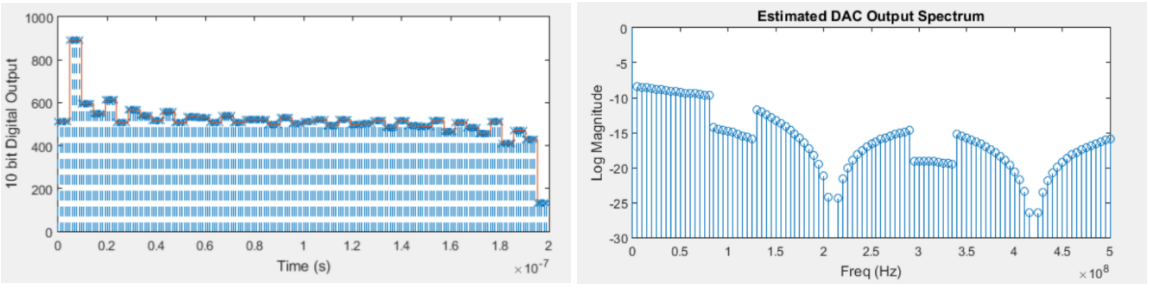


Figure 3-10: MATLAB DAC Sample and Hold Time Domain (left) and Frequency Domain (right)

3.3 Choosing Parts

Before any design could be done, components of the system needed to be chosen. The two main components for this design is the FPGA and the DAC. In addition, an oscillator, an FPGA programmer, switches, connectors, and power supplies are needed. In the last section the Spartan-3A XC3S200A in the TQFP100 package was chosen for the FPGA. Each component has specific requirements but there are a few general requirements for all components. The data sheet indicates that the FPGA requires an internal power supply voltage of 1.2 VDC and an auxiliary power supply voltage of either 2.5 VDC or 3.3 VDC. To simplify the design and reduce the number of power supplies needed, all other components should require the same voltages. As with the FPGA, no ball grid array style packages will be used, and it would be preferred that all components have leads.

The most important specification of the DAC is the sampling rate. This is the speed at which new words (or digital values) are feed into the DAC. Theoretically, the sampling rate must be larger than twice the highest desired frequency. Since the highest frequency for this project is 80 MHz, the sampling rate must be larger than 160 mega samples per second (MSPS). From the previous section, the maximum FPGA PLL output clock is 320 MHz, so the maximum DAC input clock speed is 320 MSPS. The highest speed DAC that is under 320 MSPS is the Analog Devices (AD) 210 MSPS D/A Converter. The next step up is the TI DAC31x1 D/A converter which is capable of 500 MSPS. The TI is advantageous because the clocking speed would be half of the maximum ability of the DAC resulting in better performance when compared to maxing out the abilities of the Analog Devices D/A Converter. Both DACs are available in 10 or 12-bit resolution although 10 bits was selected to aid in the simplicity. The AD DAC communicates with FPGAs using 3.3 V low voltage CMOS (LVCMOS33) while the TI DAC uses low voltage differential signal (LVDS) both of which are compatible with the Spartan-3A FPGA. LDVS is used because of the good signal integrity caused by parallel lines with apposing currents to cancel out magnetic fields

but it requires two traces for each bit, doubling the complexity when designing the PCB. The simpler to implement LVCMOS33 made the AD DAC the better choice along with lower cost, leaded package, and ease of implementation [16], [17].

The next component chosen was the oscillator used as the clock input for the FPGA. The oscillator was chosen to reach the entire frequency range of the FPGA with the PLL. The on-board FPGA PLL can multiple and divide by 32 and the FPGA operating frequency range is 5 to 320 MHz. Equations 3-1 and 3-2 show the minimum and maximum oscillator frequencies.

$$F_{osc\,min} = \frac{320\,MHz}{32} = 10\,MHz \tag{3-1}$$

$$F_{osc\,max} = 32 \times 5\,MHz = 160\,MHz \tag{3-2}$$

By using the frequency range define above, along with the 3.3 V requirement and the LVCMOS standard requirement the SiTime 5001 series Oscillator at 40 MHz was the best fit. Although this device is a QFN (quad flat no lead) package, it has only 4 pads that are over 2 squared millimeters each which should be relatively easy to solder using solder paste and a heat gun [18].

The next important component of the Digital board design was the FPGA configuration method, or in other words, the FPGA programmer. When the synthesis and implementation are complete in the Xilinx ISE Design Suite, the program generates at bit stream. This bit stream is what is used to configure the FPGA. There are many different methods for configuring the FPGA which include many different types of non-volatile memory to enable an auto-configuration when the board is powered on. The non-volatile memory can be loaded into the FPGA via the self-loading master configuration or it can be loaded in the slave mode using a separate microprocessor. Un fortunately some sort of processor is required to load the data onto the non-volatile memory in the first place. The simplest method is to use the JTAG configuration mode which uses an IEEE standard for the configuration and uses a standard style 2x6 pin header that has four interconnections with the FPGA. Figure 3-11 shows the JTAG Configuration Interface. Note that this interface can be used to program a chain of FPGAs but for this project only one FPGA will

be programmed. In addition to ease of implementation, the JTAG protocol can also be used to aid in debugging the FPGA which is very useful when dealing with highspeed signals that cannot be probed [19].

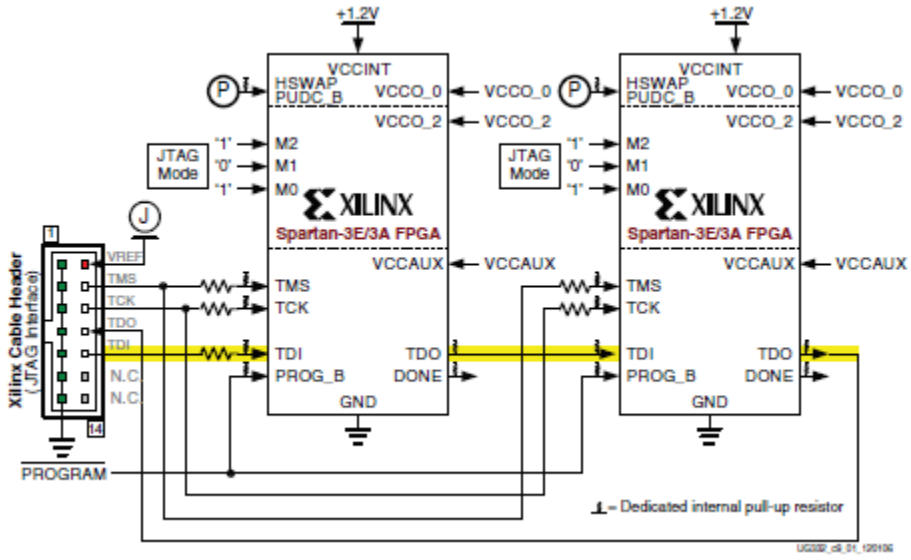


Figure 3-11: JTAG Configuration Interface [19]

Digilent makes a USB to JTAG dongle that connects the Xilinx 2x6 JTAG header to a USB. Additionally, Digilent makes a surface mount JTAG to micro USB board that solders directly onto a PCB board. Both options were considered but for roughly the same price, the JTAG-SMT2 was the better choice in case the JTAG cable was lost or became damaged. Since the JTAG-SMT2 is soldered directly to the board, it cannot be lost, and the generic micro USB cable used is cheap and easy to replace. The JTAG-SMT2 uses the same 4 interconnections with the FPGA as the JTAG dongle.

The last components required are the power supplies. Every component on the board uses 3.3 VDC besides the FPGA internal power which is 1.2 VDC. The DAC requires two separate 3.3 VDC supplies, one for the analog portion of the integrated circuit and one for the digital portion of the integrated circuit. A total of three power supplies will be needed, a digital 1.2 VDC supply for the internal FPGA, a digital 3.3 VDC supply for the FPGA AUX power, the JTAG power, the

digital side of the DAC, and the oscillator power, and lastly an analog 3.3 VDC supply for the analog side of the DAC.

To properly size the power supplies, current draw estimations are required for each supply. This can be done for most of the components by looking at the data sheets for expected current draws. For the FPGA, the clock speeds and aux voltage are set within the constraints file. The constraint file is used to apply constraints on the FPGA implementation such as voltage, clock speed, and IO pin selection. With the proper constrains, the ISE Design Suite can be used to make dynamic and quiescent power estimations. Figure 3-12 shows the total estimated current draw for each of the three power supplies.

Component	ADVCC33 (mA)	DVCC33 (mA)	DVCC12 (mA)
DAC	36	9	N/A
OSC	N/A	33	N/A
FPGA EST Q	N/A	16	8
FPGA ESTDyn	N/A	18	27
LEDs	N/A	10	N/A
Total	36	86	35

Figure 3-12: Digital Design Power Estimations

Since this digital board is very sensitive to noise and has no power efficiency requirements, the best power supply option is a low drop out (LDO) voltage regulator instead of a noisy DC-DC converter. The LDO is a good option because there is no internal switching to change the voltage, instead the voltage is reduced by simply dissipating the extra power in heat. This makes the LDO inefficient but a low noise power supply. The best fit for the previous requirements was the Diode Incorporated AP212x series highspeed, extremely low noise, LDO regulators. Although this project will mostly be used on a bench, in the rare occurrence that it needs to be battery powered, the LDO max input power would need to be greater that 6V or 4 series 1.5 V batteries. 6 V was used instead of 4.5 V because of the knowledge that the analog board would be using 5 V output

LDOs. To insure plenty of current leeway two 300mA VDC AP2125 LDOs were used for the 3.3 VDC supplies and one 150 mA AP2120 LDO was used for the 1.2 VDC supply.

3.4 Schematic Design

Before any design could begin, a schematic symbol and corresponding layout footprint is needed for each component used on the digital board. Since all components were sourced from Digikey, some of them had downloadable part libraries which contained both the layout and symbol for the design. This was the case for both power supplies. For those that did not come with a library, a web service named Symacsys Component Search Engine was used to either find a library for the desired component or it would create the library for free usually in less than 24 hours. For some of the simpler components such as headers, switches, and push buttons, the libraries were created manually using the tools on Autodesk Eagle PCB design software.

Using the symbols in the libraries created and Eagle, the schematic for the entire digital board was created. This was done by first placing the FPGA and the DAC and routing the interconnections. There are total of 11 interconnections between the FPGA and the DAC, one connection for each of the 10 bits and then one connection for the clock. Figure 3-13 shows the interconnection between the FPGA and the DAC along with a 22 ohm series resistor. The resistor is used to aid in the 50 ohm termination. Although the Spartan-3A states that no termination is required for LVCMOS, the AD9740 DAC shows the series 20 ohm resistors on the schematic of the development board. The resistors could easily be replaced with no-load resistors if the 20 ohm termination causes any problems [19], [17].

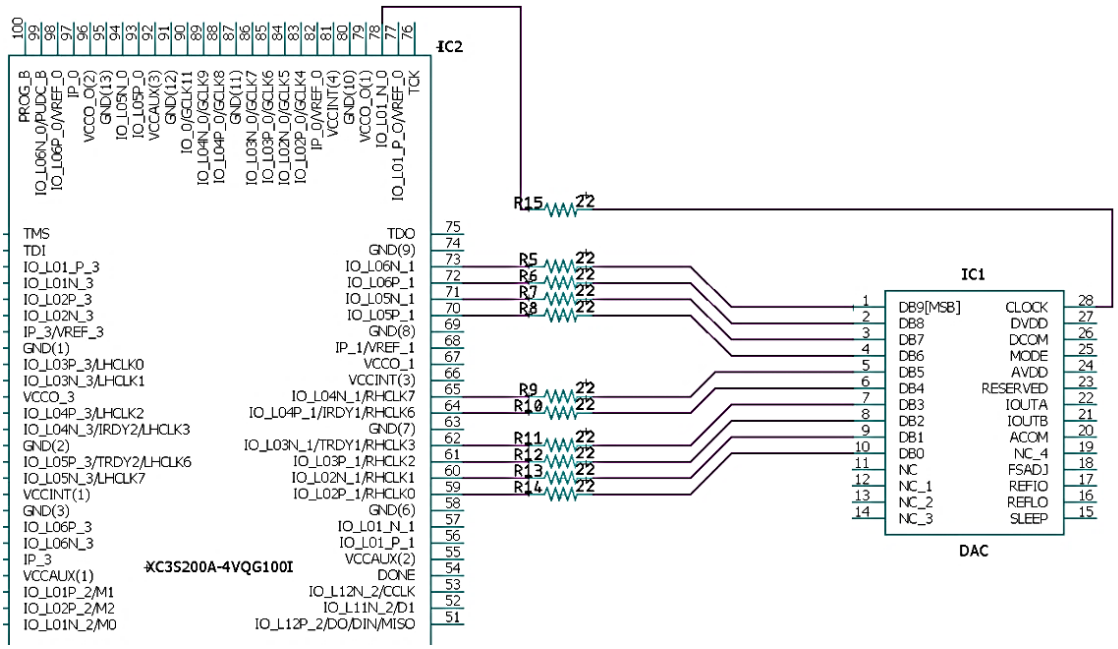


Figure 3-13: FPGA-DAC Interconnection

Next the switches and push buttons were added to the circuit. Generic surface mount push buttons and switches were selected. S1 and S2 are two 8 bank single pole single throw switches that are connected to 16 IO ports on Bank 2 of the FPGA. These 16 switches will control the 16 channels. The FPGA has internal programmable pull up/down resistors but to insure no issue would come up, an external pull up resistor network was added to the switches. S3 is also connected to Bank 2 on the FPGA and it will be used to start the FSM. S4 was connected to the PROG_B terminal on the FPGA and it is used to reset the FPGA if needed. Figure 3-14 shows the schematic of the switches added to the FPGA

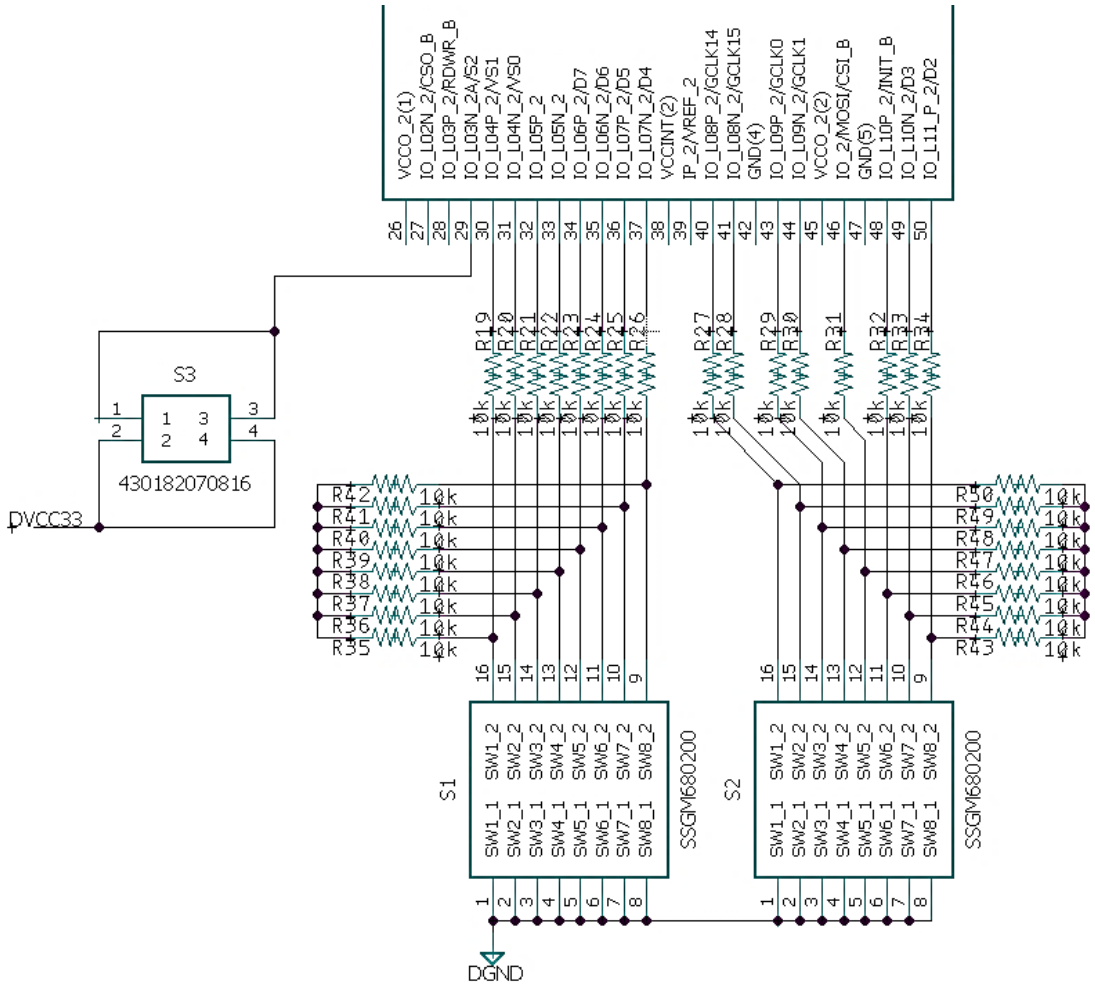


Figure 3-14: Digital Synthesizer Switch Banks

The output of the oscillator was simply connected a global buffered clock input on Bank 0 of the FPGA. No termination was used in the interconnection. This matches the schematic of the Spartan-3A development board. The JTAG-SMT2 was connected using the schematic found on the JTAG SMT2 datasheet which can be seen on Figure 3-15. Typically current limiting resistors are required on all signals but since both the JTAG voltage and the FPGA auxiliary voltage are 3.3 V, this is not needed [19], [20]. Figure 3-16shows a schematic capture of the JTAG and Oscillator interconnections with the FPGA.

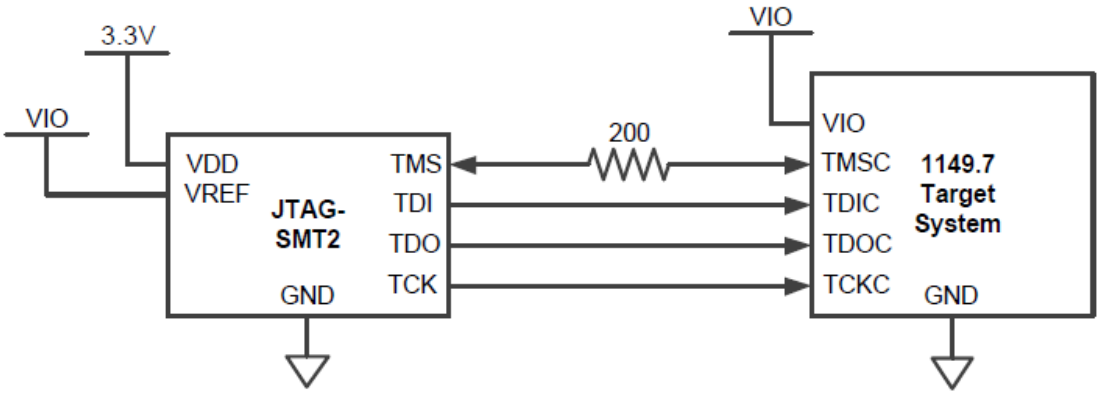


Figure 3-15:JTAG-SMT2 to FPGA connections with Current Limiting Resistor[20]

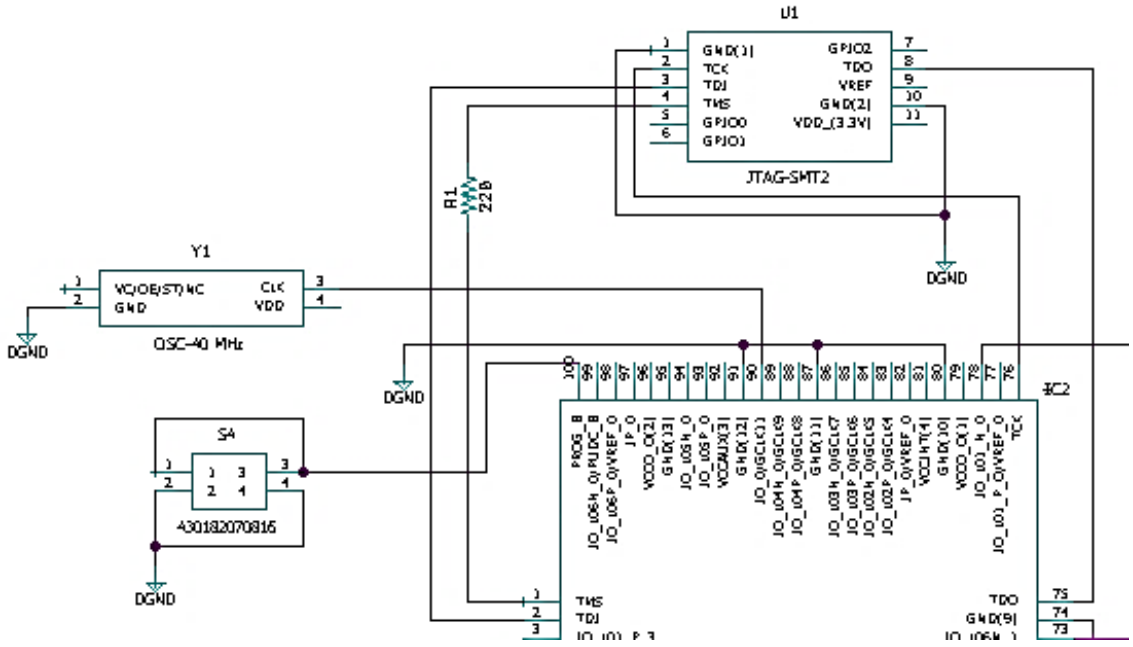


Figure 3-16: Interconnections between the JTAG-SMT2, Reset Switch, Oscillator, and FPGA

Two sets of headers were added to the design. One was used as a set of test points connected directly to 6 IO ports on the Bank 3 of the FPGA. In the future, any desired signal could be routed out of the FPGA onto a pin on the header. The other header was used to control the configuration mode. The JTAG-SMT2 can configure using either JTAG or SPI so this header was added in case there were any issues with the JTAG protocol. The Mode header was connected using pull up

resistors on one terminal and pull down on the other. A jumper across the terminals would bring the mode selector from 1 to 0. There are three total mode selectors.

The power and grounding portion of the schematic required much more though and analysis. Separate grounds are required for the digital and analog portions of the board, decoupling capacitors are required throughout the board, and filtering is required to reduce the amount of digital noise entering the analog circuit. When considering mixed signal (digital and analog) designs, it is very important to separate the components, their power, and their grounds. This is because digital circuits especially those made from MOSFETs have large surges in current when the gate switches. Combine millions of gates together and the switching current can cause noticeable deviation on the power and ground rails. The best way to help combat this is to use a bypass capacitor. A bypass capacitor is a capacitor placed between the power and ground rails of an integrated circuit. The bypass capacitor helps by supply the circuit with extra current when the power rails cannot keep up with the demand. Another way to think of the bypass capacitor is an AC short to ground which helps eliminate the digital noise cause by switching.

Properly sizing bypass capacitors, it crucial to the performance of the circuit. The following are a few rules of thumb when choosing bypass capacitors.

- The higher the frequency, the smaller the capacitor.
- Use parallel capacitors of different sizes with the closest to the device being small and the capacitor closest to the power supply being large.
- Place the coupling capacitors as close to the device as possible.
- Use development board or datasheet recommendations on capacitor sizes.

By referencing the datasheets of all the devices on the board, 0.1 uF capacitors were selected to be placed next to the devices power inputs and 1 uF capacitors were picked for the outputs of the power supplies. A third set of bypass capacitors were added to be placed somewhere in between

the power supplies and the devices in the case where extra bypassing was needed. Lastly the same one 1 uF bypass capacitor was added to the inputs of all three power supplies.

It is important to ensure that this combination of capacitors will have the desired results against the switching noise. The Knee Frequency, F_{knee}, is used with digital circuits as an estimation of significant frequency. In a digital circuit most of the switching power is concentrated below F_{knee} while most frequencies above it have little effect on the digital circuit performance. The circuit response at F_{knee} describes the circuit's ability to process a step. Equation 3.3 shows the calculation of F_{knee} and the results from using the oscillator rise time of 1.5 ns. [21]

$$F_{knee} = \frac{0.5}{T_R} = \frac{0.5}{1.5\ ns} = 333\ MHz \tag{3-3}$$

After finding F_{knee} and the bypass capacitor values, the power delivery circuit can be simulated. For each capacitor an 850 pH inductor and a 50 mohm resistor were added in series to model the parasitics in a 0603 surface mount capacitor. The results of the simulation show that at 333 MHz the impedance to ground is roughly – 9 dB meaning it is a dead short. This simulation indicates that the higher frequencies will indeed short to ground while DC has a high impedance path to ground. The results can be seen in Figure 3-17.

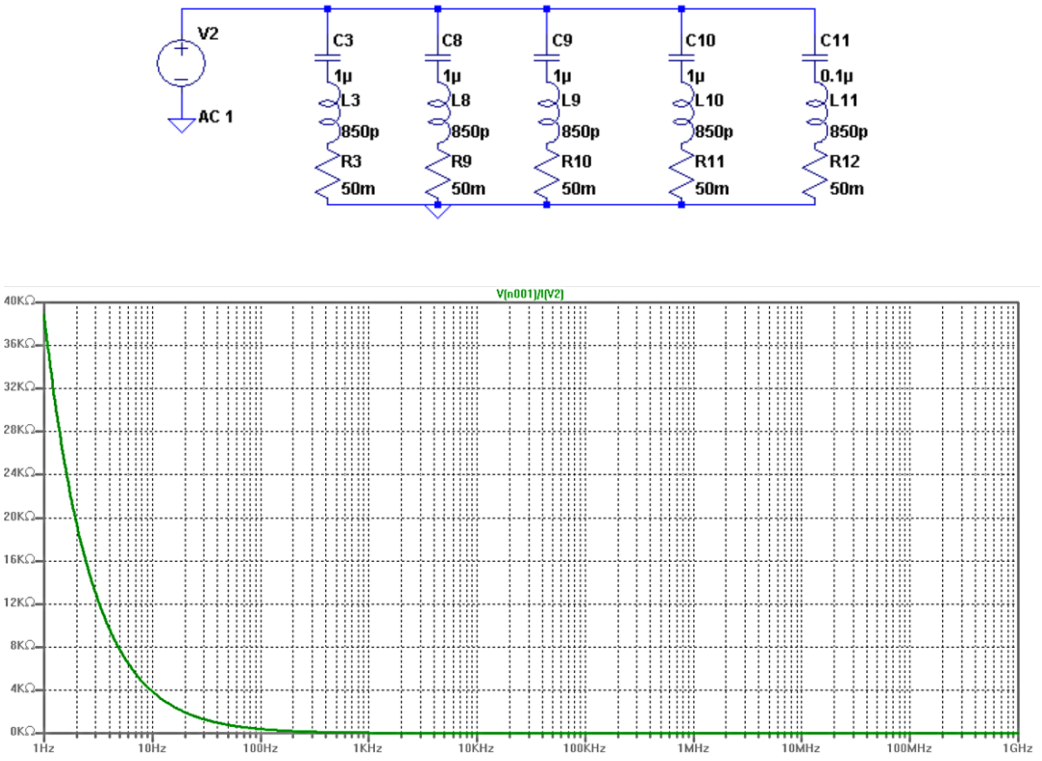


Figure 3-17:Bypass Capacitor Simulation Schematic (top) and Results (bottom)

The AD9740 DAC datasheet recommends using a LC filter with a ferrite bead to aid in the removal of digital noise from the analog circuit. A ferrite bead is used instead of an inductor to help eliminate any resonance by having a lossy core which dissipates energy instead of simply storing it. Figure 3-18 shows an example of the LC filter.

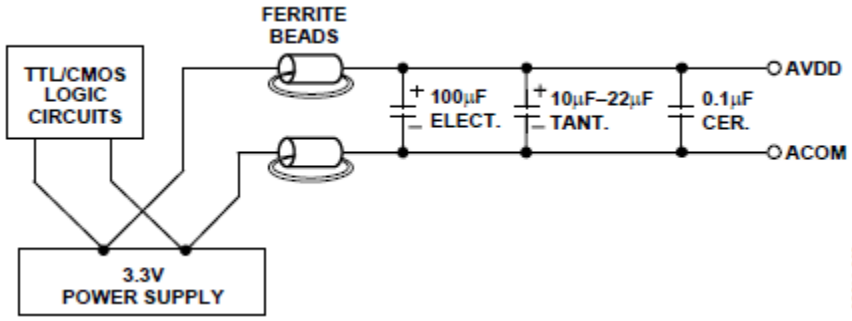


Figure 3-18: AD9740 LC Power Supply Filter [17]

The Taiyo Yuden HS121 ferrite bead was picked for the inductor of the filter. The capacitor was a similar bypass network as in Figure 3-17 but with an added 10 uF capacitor at the beginning of the chain. To ensure this filter did not have any resonance at F_{knee}, it was simulated using LTspice. First a model of the ferrite bead was created using information from the datasheet as well as from the impedance response plot of the ferrite bead. Both the impedance response from the datasheet and from the LTSpice simulations can be seen on Figure 3-19. Figure 3-20 shows the entire LC circuit simulation schematic and results. This results show roughly-45 dB at 333 MHz meaning there should no resonance at the FPGA switching speeds [22].

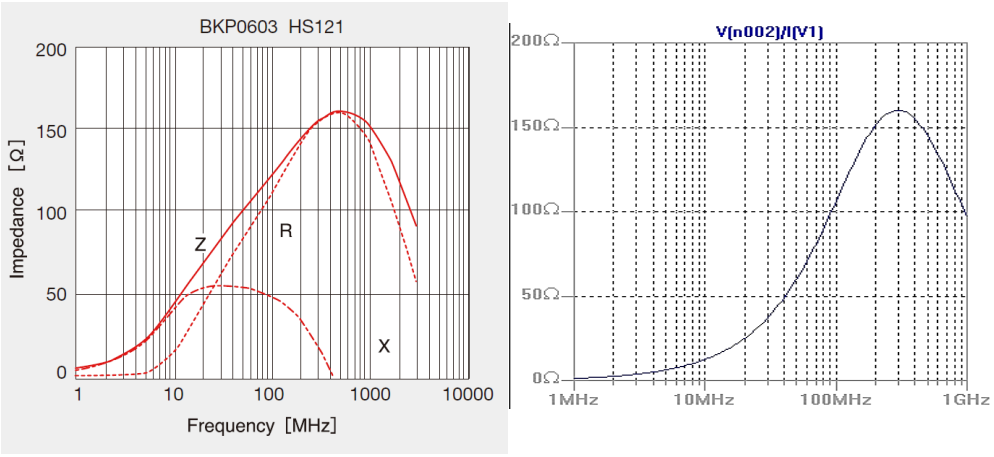


Figure 3-19 Ferrite Bead Expected Impedance Response (left) and the Impedance Response from the Simulated Model (right)[22]

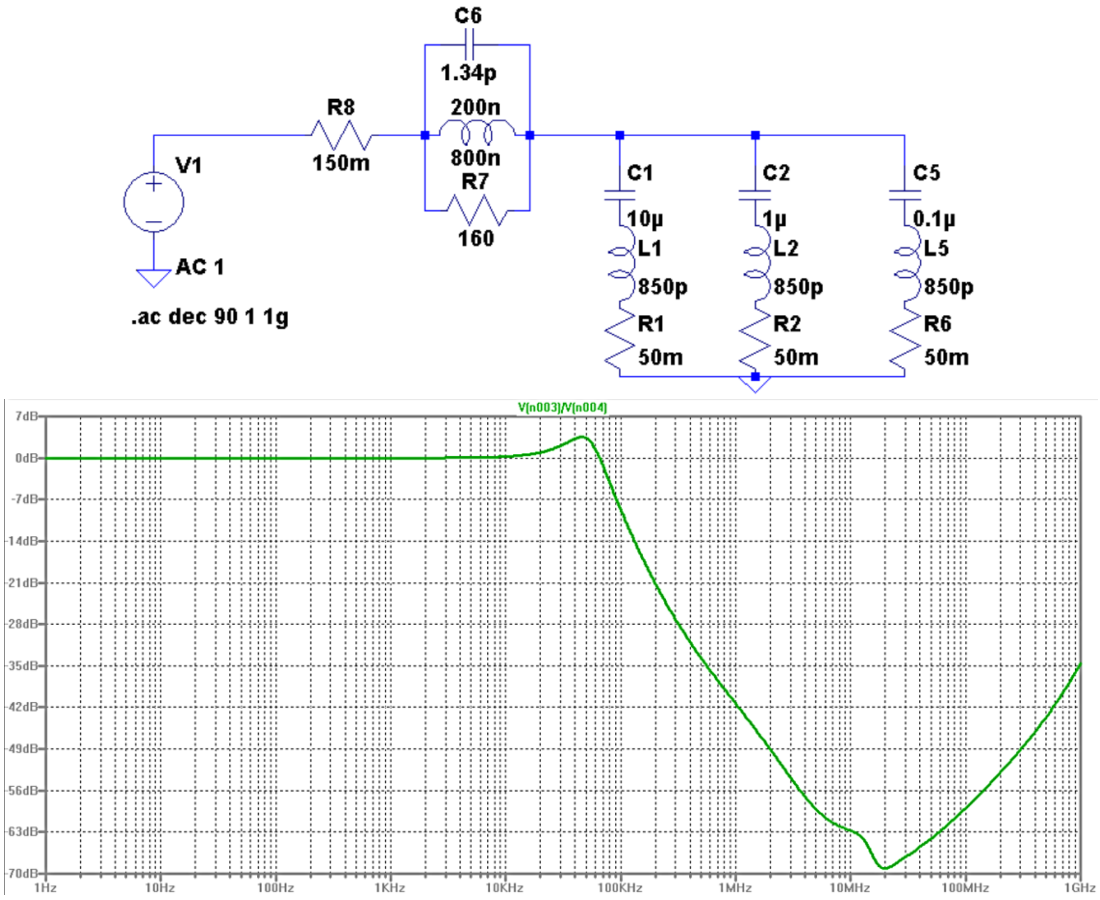


Figure 3-20: LC Filter with Ferrite Bead Simulation Schematic (top) and Results (bottom)

The AD9740 has differential current source outputs. The output could be converted to single end by using just one output or by using a transformer. This was decided against due to most of the RF components in the Upconverter also being differential input and output. The differential outputs had to be converted to voltage outputs. Since two 50 ohm SMA connectors were being used as the output, the current outputs were both shunted with a 50 ohm resistor to ground. With the 50 ohm shunt, the max output voltage must be checked to insure it does not surpass the absolute max output rating listed on the datasheet.

$$V_{max} = R * Imax = 50\Omega \times 20mA = 1V \quad (3\text{-}4)$$

The absolute max rating for Vout on the DAC is 3.6V which is well over 1 V, so the 50 ohm resistors would cause no issues.

A few final details were added to finish the schematic which include:

- Power switch
- Power LED
- Done LED to show programing is complete
- Output On LED
- Mini banana connectors for the 5-6VDC power in
- Test points and current sense resistors to measure current draw

The final schematic for the Digital Synthesizer Board can be seen in APPENDIX B.

3.5 Layout Design

There are numerous concerns regarding the layout of a highspeed mixed signal design. Parasitic affects caused by quick rise times can cause many issues such as cross talk from mutual inductance in traces. It can also cause inductance within vias which degrade the ability for bypass capacitors to shunt to ground. Improper ground paths can cause ground loops which can further increase cross talk or even cause radiation of signals. Path lengths can cause signal delays which can break the tight timing requirements of a digital circuit. To avoid these issues a good layout plan is required before any layout work begins.

Before any layout design was done using Eagle, a rough plan of the layer stack and component placement was devised. A four-layer stack was chosen since there were no BGA components or size restrictions that would require extra signal layers. The standard four-layer stack used consists of a signal layer, a ground layer, a power layer, and another signal layer.

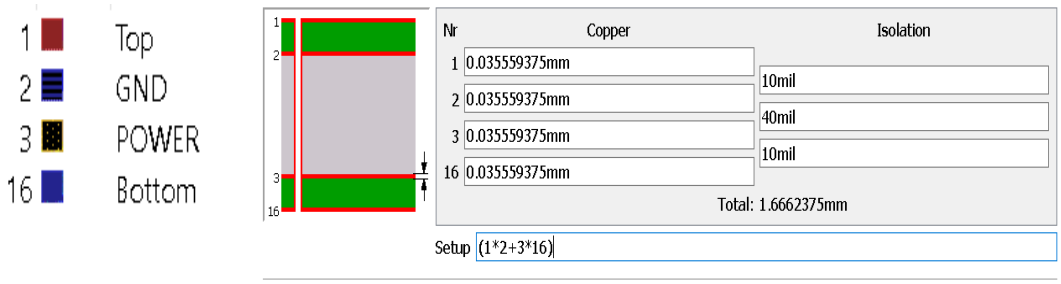


Figure 3-21: Four-Layer PCB Stack

A rough plan was then created of the component placement as well as the power and ground plane designs. Since this is a mixed signal design, two ground planes are required, one for the digital ground and one for the analog ground. This helps keep any digital ground bounce isolated from the analog circuit. The two planes connect near the power supply portion of the board. There are also three different power planes required, one for each of the three power supplies. Figure 3-22 shows the rough layout plan for the design.

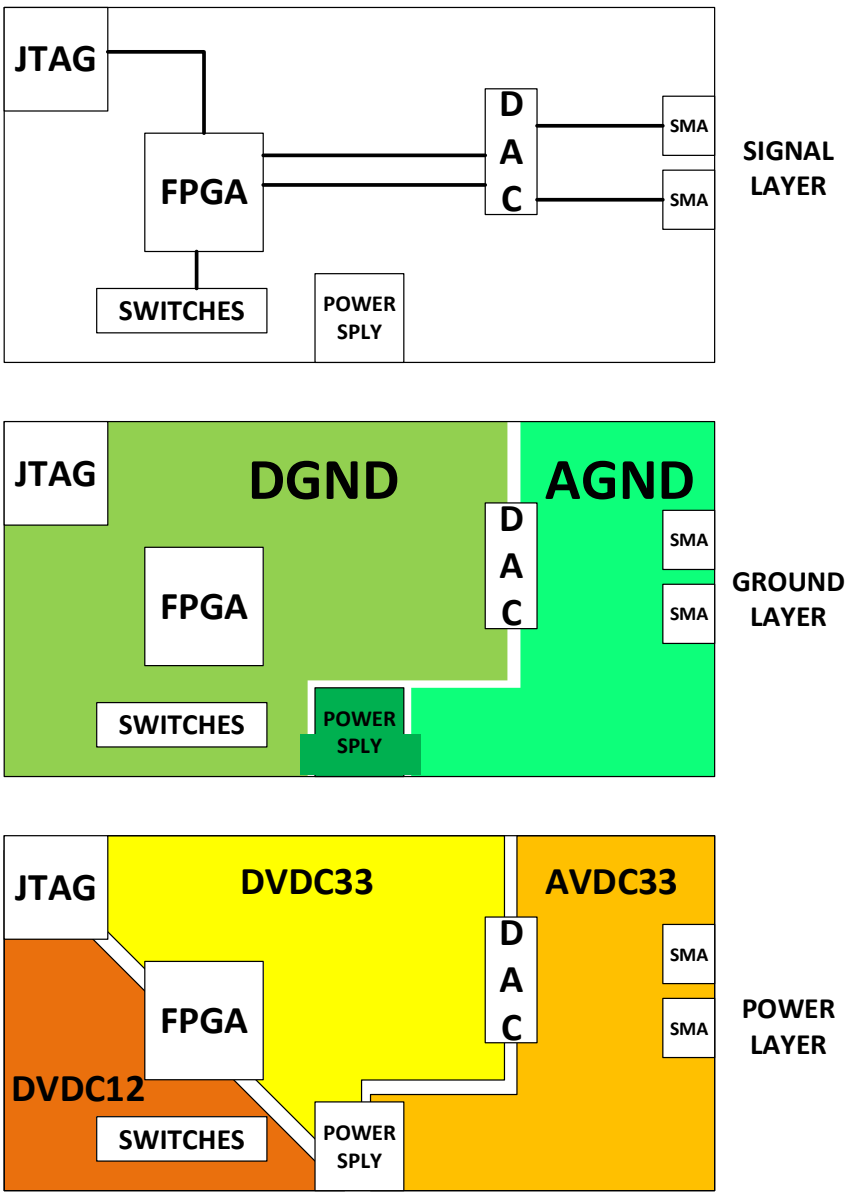


Figure 3-22: Digital Synthesizer Layout Plan

To start the layout all the components were placed on the 4x5 inch board following the layout plane. The power supplies were moved to the upper right-hand corner of the board due to space limitation. From there the major signals were routed along with any terminations or pull up/down resistor networks. These signals included the FPGA to DAC data signals and 20 ohm terminations, the JTAG communication wiring, the switch to FPGA signals along with the pull up

network, the headers for mode selection and troubleshooting, and the DAC to SMA signal with the 50 ohm shunt terminations.

Trace width was important for the highspeed signals to ensure a 50 ohm characteristic impedance. The traces on the board were designed as coplanar wave guides to help reduce the trace width when compared to a microstrip line. A coplanar wave guide is a single trace separated by a substrate over a ground plane just like a microstrip line but with additional ground planes surrounding the trace. Figure 3-23 shows the physical differences between the two traces.

Figure 3-23:Microstrip Trace (left). Coplanar Wave Guide (right) [23]

To calculate the impedance of the coplanar wave guide, the trace width (W), substrate thickness (H), substrate dielectric constant (Er), conductor gap (G), and trace height are needed. Saturn PCB Design, Inc – PCB Toolkit was used to calculate the trace width. With 6 mil gaps, 10 mil substrate thickness (manufacturer standard for 4-layer board see Figure 3-21), a dielectric constant of 4.6 (FR-4 Standard), and a total of 1.5 oz trace height (roughly 2.1 mil, manufacturer standard) a trace width of 16 mils is required to achieve a 50 ohm characteristic impedance. Results can be seen on Figure 3-24 [23].

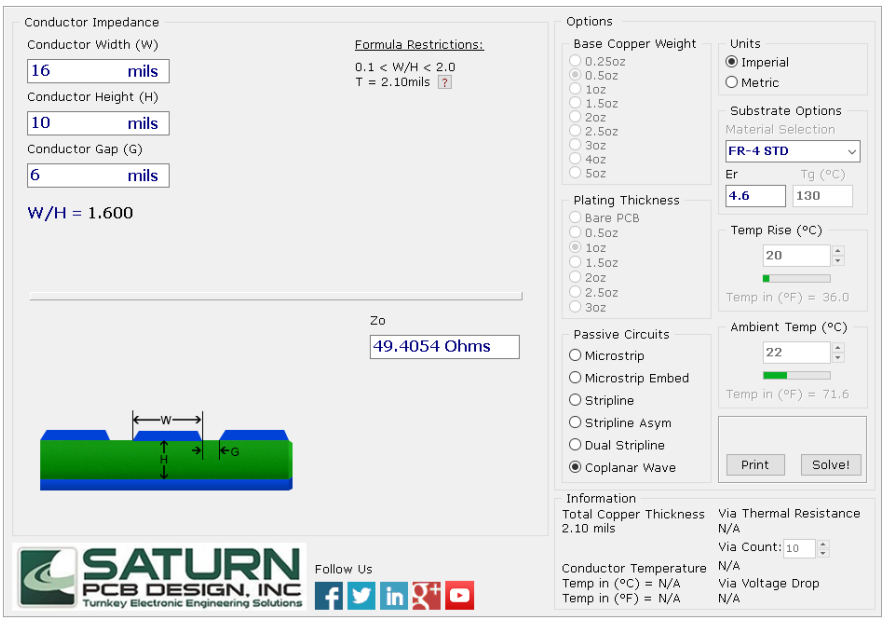


Figure 3-24: Coplanar Wave Guide Trace Width using Saturn PCB Toolkit [23]

Following component and trace placement, the ground and power planes were created. A total of three separate ground planes were created, the digital ground plane, the analog ground plane, and the incoming power ground plane. The digital and analog planes are connected at the incoming power ground plane. The ground planes separate the analog components from the digital ones by cutting through the DAC from the bottom of the IC out through pin 24 (one of the digital ground pins). The split ground plane layout matches the split used in the AD9740 development board [17]. The comparison can be seen in Figure 3-25. The power planes were separated into a total of 6 planes: incoming power, switched power, digital 1.2 VDC, digital 3.3 VDC, analog 3.3 VDC, and a ground plane under the SMA connectors. The DVCC33 plane wraps around the outer left edge of the board to power the JTAG programmer, the oscillator, and the FPGA 3.3VDC auxiliary power. The DVCC12 plane comes into the center of the FPGA to power the internal 1.2VDC pins. Lastly the AVCC33 plane covers the right portion of the board. Figure 3-26 shows the power plane layout for the Digital Synthesizer.

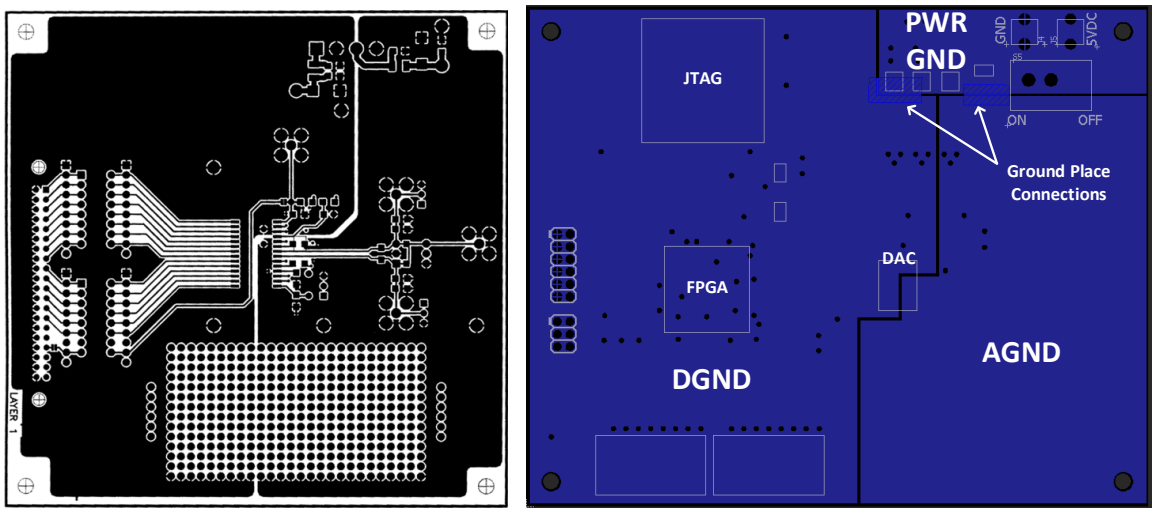


Figure 3-25: AD9740 DAC Layout (right). Digital Synthesizer Ground Plane Layout (left)[17]

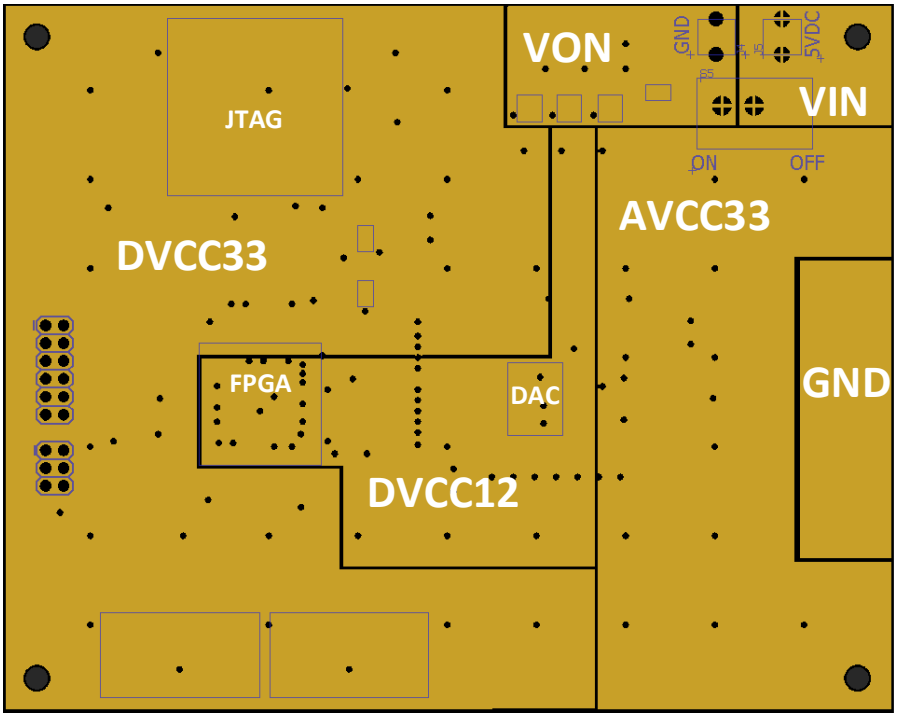


Figure 3-26: Digital Synthesizer Power Plane Layout

Note that all planes are large and free of traces. Any trace bisecting the planes could have an adverse effect on the circuit. The ground plane is the return current path for all DC and AC signals. The low speed signals choose the path of low resistance (shortest return path) while the highspeed signals follow the path of least inductance meaning the return current follows the same

path as the trace above the ground plane. If a trace is present in the ground or power plane and it crosses a return path, it could cause the current to deviate which could potentially lead to the radiation of highspeed signals throughout the board. Figure 3-27 demonstrates this effect.

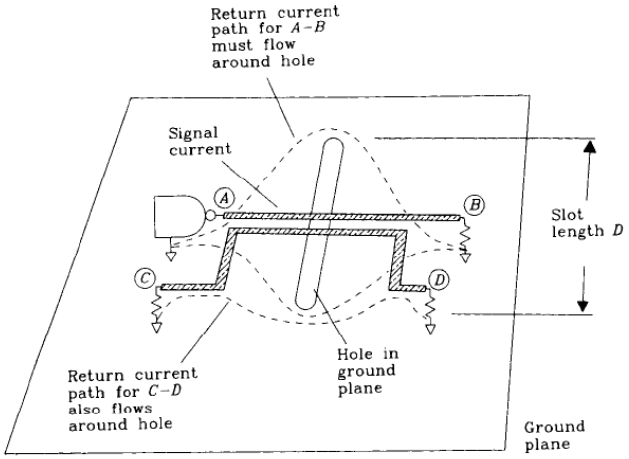


Figure 3-27: Effects of Discontinuities in Ground Plane [21]

All the bypass capacitors were placed on the board closest to their respective power pins. Proximity is crucial to reduce the inductive power lead from the capacitor to the power pin. The longer the power trace is, the grater the inductance is. The inductance counteracts the effect of the bypass capacitor. Additionally, vias to the power plane and ground plane were used to reduce the overall inductance. Figure 3-28 shows how the power and ground pins were connected.

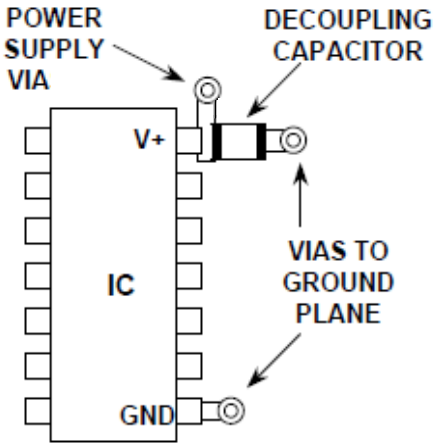


Figure 3-28: Bypass Capacitor Layout for Power and Ground Pins [24]

Advance Circuits Design from Arizona was selected to manufacture the board due to the 4-layer student special price and the fast lead time. The webpage information was referenced to match the manufacturing abilities to the Design Rules Check on Eagle to ensure the board could be manufactured. In addition, Advanced Circuit Design has a Free DFM tool that checks the layout Gerber files to guarantee proper manufacturing. After checking both resources, the board was ordered. **Error! Reference source not found.** shows the final Digital Synthesizer board layout. Figure 3-29 shows the received PCB board.

An Eagle parts list was exported to an excel file where part numbers were matched to the corresponding reference designators. The parts list was modified to include Digikey part numbers and prices to calculate the total cost of the parts on the board. When ordering parts on Digikey some extras were purchased of the smaller and cheaper components, slightly changing the overall cost. APPENDIX D shows both the estimated cost parts list and the final Digikey order parts list.

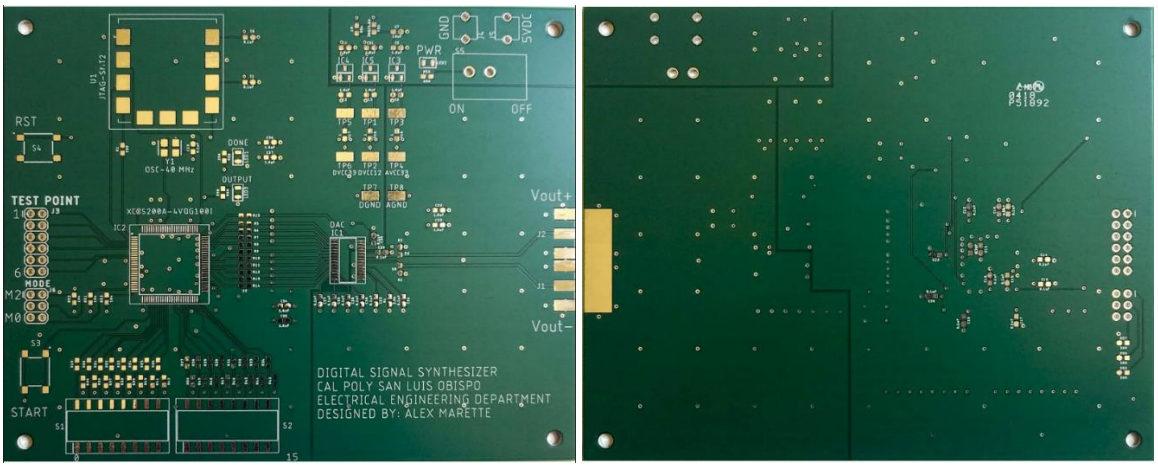


Figure 3-29: Bare Digital Synthesizer PCB Board Top (left) & Bottom (right)

3.6 Building and Testing

Due to the many systems on the board, the building and testing was done in a careful order. Additionally, building the board in steps and checking each part for proper functionality is

desired to troubleshooting of entire board. If all board components were populated and a malfunction occurred, identifying the source of the error would be very difficult. The following list details the order of the building and testing applied to the digital synthesizer board.

1. Install all components required to power the board: Banana Connectors, Switch, Linear Regulators, Test Points.
    a. Omit the ferrite bead and install no-load bypass resistor
    b. Omit the series resistors for current measuring
2. Characterize all three voltage regulators
    a. Vout vs Iout
    b. Noise Rejection (PSRR)
3. Populate entire digital section of digital synthesizer board
    a. Series no load resistors to power digital control board.
4. Load test bitstream into FPGA to verify JTAG configuration and proper FPGA functionality.
    a. Test proper switch operation
    b. Test proper LED operation
    c. Test proper push button operation
5. Apply series no load resistor to analog power circuit to power analog portion.
6. Populate remaining analog components
7. Load Synthesizer code and run.
    a. Check for appropriate output.
8. Run Full characterization of Digital Synthesizer board
    a. Signal tone at all frequencies
    b. 1 tone, 2 tone, 4, 8, 16 tone tests using VSA
9. Replace series no-load resistors with appropriate resistors for current measurement.
    a. Measure current for all sources with output off.
    b. Measure current for all sources with output on.
10. Replace series resistors with no-load resistors after power calculations.

The power supply circuit load stability was first tested after the power supply circuits were soldered. This was done by applying different loads to the power supplies via the test points. The load ranged from a minimal amount down to a load that created to the maximum rated output current for the specific power supply. Figure 3-30 shows the results of the load stability test. The 1.2 V power supply has a 50 mV drop across the full output range while the 3.3 V supplies had a 20 mV drop across the full output range. Both supplies had desirable results with minimal change in the supply voltage. Note that under normal operation none of the supplies will reach the max current output.

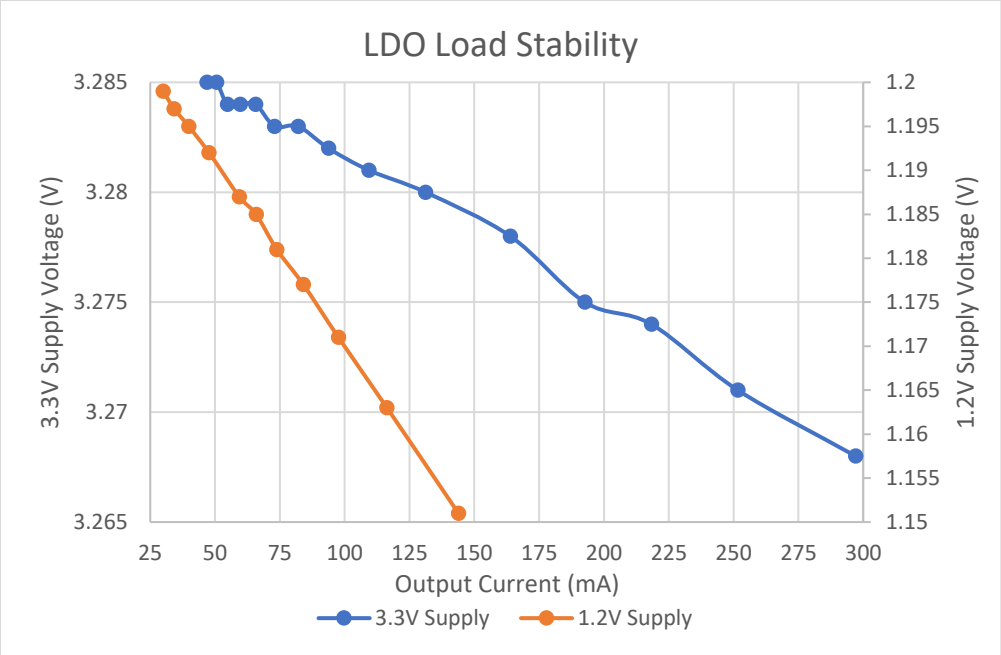


Figure 3-30: Power Supply Load Stability Test

A test was devised for measuring the power supple rejection ratio (PSRR). The idea was to connect a function generator in series with a DC power supply into the input of the power supplies and then measure the AC coupled signal at the output of the power supply. The ratio of the ac power at the output over the ac power at the input would then be the PSRR. Unfortunately, the function generators could accept little to no DC power. To deal with this issue, the AC and DC power supplies were summed using a summing resistor. Figure 3-31 shows the schematic for testing the power supplies' PSRR. Using a function generator and oscilloscope proved to be an issue due to frequency limitations and discrete frequency stepping. Vector network analyzer can be set up for a similar test, but they require additional tools that are not available.

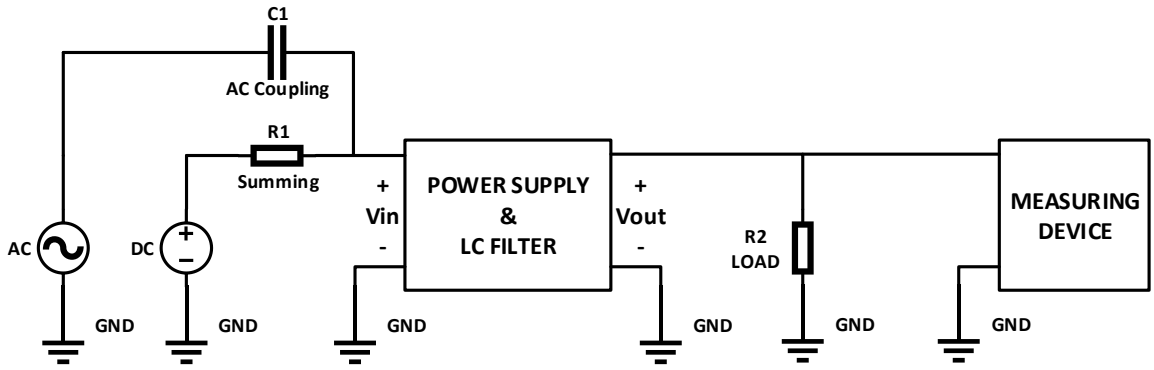


Figure 3-31: PSRR Test Schematic

A new spectrum analyzer that had a built-in tracking generator (TG) was used. This allows the spectrum analyzer to be used as a scalar network analyzer. The output of the spectrum analyzer was used for the AC supply and the input was the measuring device. The analyzer swept from 0 to 400 MHz at a power level of -20 dBm. Figure 3-32 shows the results of the test on the digital and analog 3.3 V power supplies. The digital 1.2 V and 3.3 V had similar results. As expected the PSRR on the analog circuit is better than the digital circuit due to the extra filtering. The digital PSRR is roughly 20 dB while the PSRR for the analog circuit is roughly 30 dB.

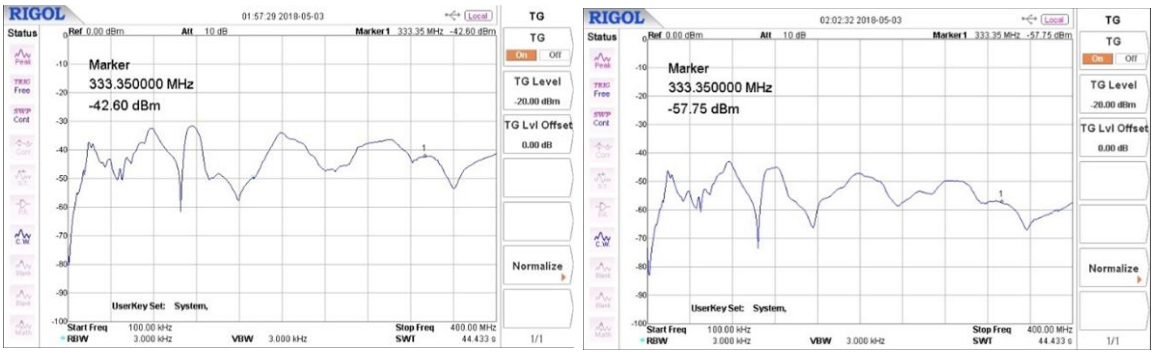


Figure 3-32: Power Supply PSRR Results: Digital 3.3 V (left) Analog 3.3 V (right)

After confirming proper power supply performance, the FPGA, JTAG and other digital circuit components were installed. Three test codes were created for the FPGA. The first code tested the JTAG programming, the switch integration, and the LED integration. The internal pull up resistor worked as expected so the pull up network was not used. The code simply illuminated the

OUTPUT LED when switch 0 was in the on position. This worked as desired. Additionally, the reset button was tested and the DONE LED properly illuminated when configuration was complete. The other two programs tested the switches, ON push button, and the oscillator by flashing the OUTPUT LED at 1 Hz when either the switch or the push button were in the active position. Both codes also worked as expected.

The previous test showed that the entire digital portion of the board worked as expected. Next the DAC and all analog components were soldered to the board. The full FPGA synthesizer code was configured into the FPGA. When the ON button was pressed, the OUTPUT LED flashed a few times, remained off, and no DAC output was present. A few more attempts showed inconsistent results when the ON button was pressed. The OUTPUT LED would at time remain on and other time remain off after the button was release. The FSM was suspected to be the culprit, so the current state was output to the test pins where “00” was IDLE State, “01” was LOAD1, “10” was LOAD2, and “11” was LOOP. The test pins were displayed on the oscilloscope and showed that at times the FSM would end at the LOOP state and other times it would end at the IDLE state. It was suspected that the push button was bouncing. A software debounced was added to the input of the push button. The debounce required a 0.5 s press to send a high signal. After the debouncer was added, the FSM cycled properly. This can be seen in Figure 3-33.

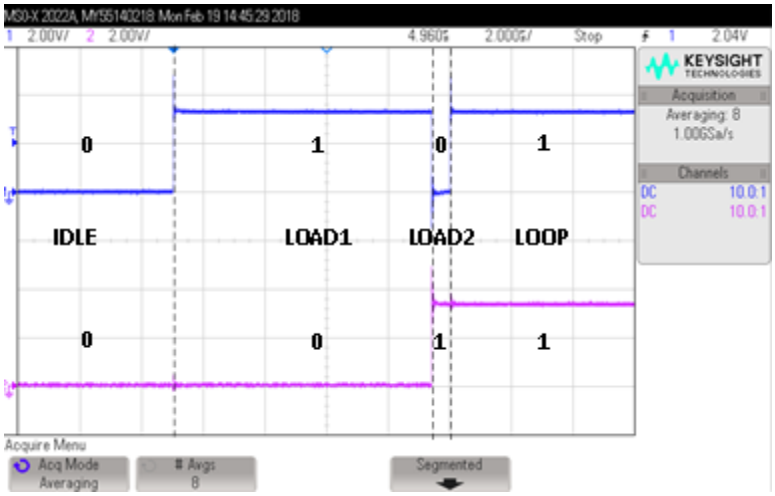


Figure 3-33: FSM State Test

Although the FSM was working correctly, the DAC still had no output. The signals to the DAC, including the clock, are too highspeed to check using an oscilloscope. The clock speed was lowered to 40 MHz and then the DAC clock signal was probed. The oscilloscope showed no signal on the clock signal while the DAC data lines did have a signal. Looking at the constraints file showed that the DAC clock was not routed to the DAC clock pin. The output constraint was added to the file and then the DAC had the proper output. Figure 3-34 shows the DAC output on the signal analyzer.

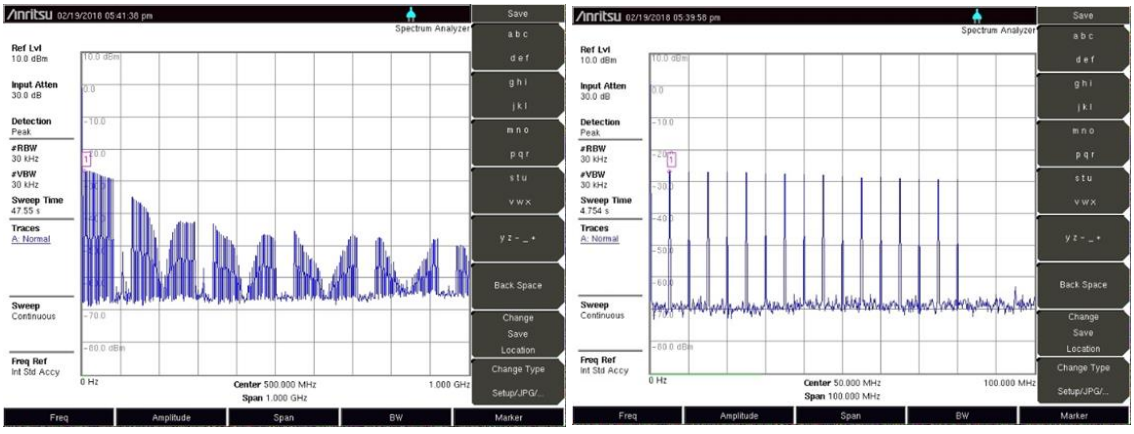


Figure 3-34: DAC Output with Sink Roll-Off View (left) and Close View 0-100 MHz (right)

Captures were taken to measure the power of each individual signal as well as the power per tone with 1 to 16 tones on. This data was plotted along with the expected power on Figure 3-36 and

Figure 3-37. The expected power was calculated by calculating a single tone out of the DAC full scale range using differential outputs across a 100 ohm load. Figure 3-35 shows the output circuit of the DAC which was 100 ohm differential terminated. Equations 3-5 to 3-8 show that the differential power through a 100 ohm load is the same as the single ended power through a 25 ohm load. The single tone power was calculated to be roughly -0.45 dBm. The differential output of the DAC had to be converted to a single ended output to view on the spectrum analyzer. The Balun used had an S21 and S31 of roughly -2.3 dB meaning than the measured single tone power should be roughly -2.85 dBm.

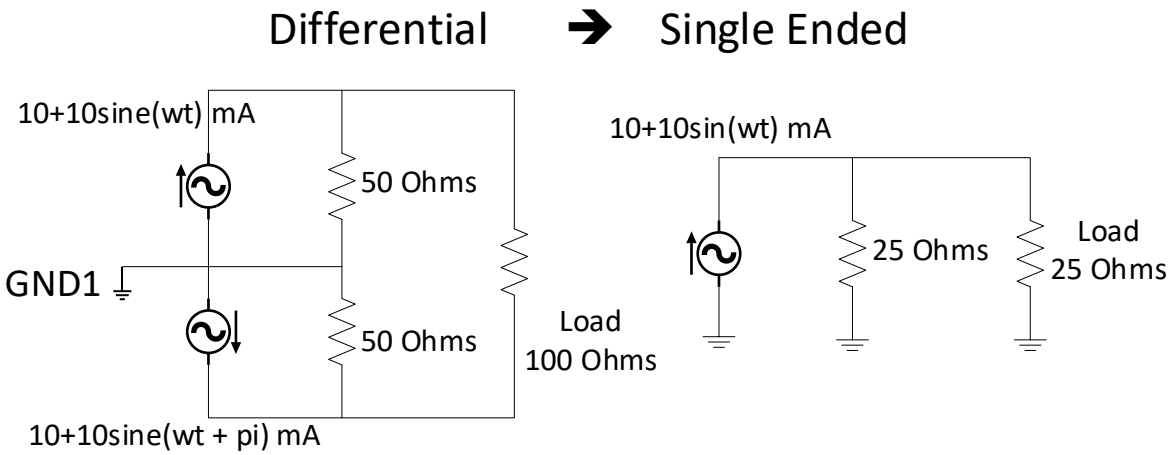


Figure 3-35: Differential to Single Power Schematic

$$Pload = \frac{(V_{rms}^{+} - V_{rms}^{-})^2}{100} = \frac{4V_{rms}^2}{100} = \frac{V_{rms}^2}{25} \tag{3-5}$$

$$I_{source_{rms}} = \left(\frac{1}{T}\int_0^T \left(10 + 10\sin\left(\frac{2\pi}{T}t\right)\right)^2 dt\right)^{\frac{1}{2}} = 12.25\ mA \tag{3-6}$$

$$V_{source_{rms}} = V_{load_{rms}} = I_{source_{rms}} \times R_{eq} = I_{source_{rms}} \times 25||25$$

$$= 12.25mA \times 12.25\ \Omega = 150mV \tag{3-7}$$

$$P_{load} = \frac{V_{load_{rms}}^2}{R_{load}} = \frac{150^2\ mV^2}{25\Omega} = 0.900\ mW = -0.45\ dBm \tag{3-8}$$

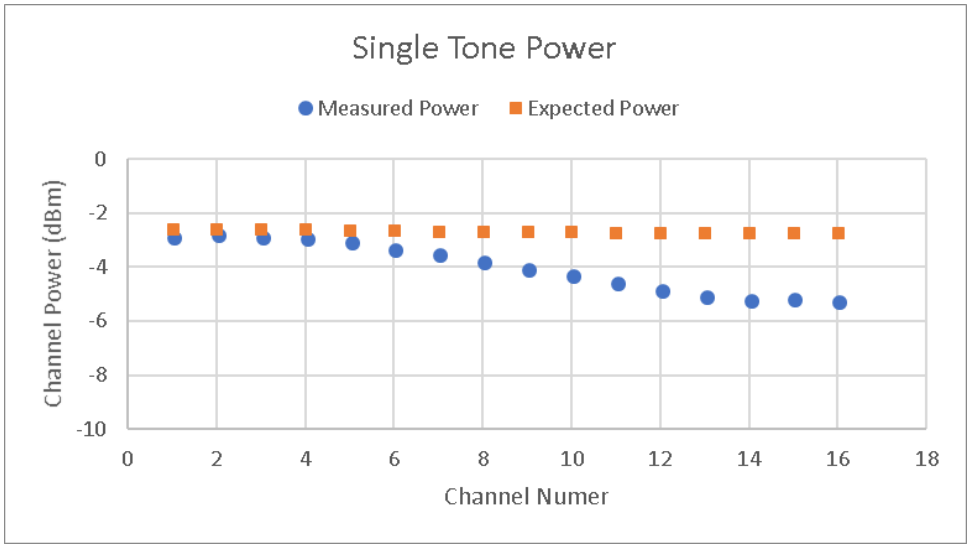


Figure 3-36: DAC Output Single Tone Power

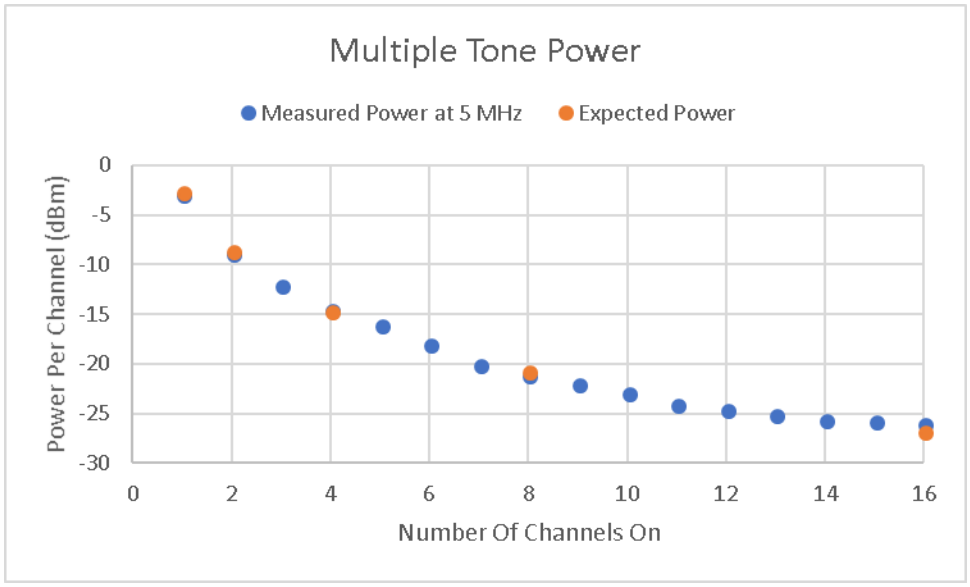


Figure 3-37: DAC Output Multiple Tone Power

Figure 3-36 shows some discrepancies between the measured and expected output. This is believed to be caused by the sinc roll off estimated by the FPGA simulation. It could also be caused by digital error in quantizing the signal and the close to Nyquist sampling rate. Figure 3-37 shows how the power drops by a factor of 4, or roughly 6 dB, when the number of tones is doubled. One half drop in power is caused by adding a new tone which creates a large peak

followed by much smaller oscillations, and the other half is caused by the normalization done within the FPGA SUM and NORM block. The Digital Synthesizer board functions as expected. An image of the fully built Digital Synthesizer device can be seen in Figure 3-38.

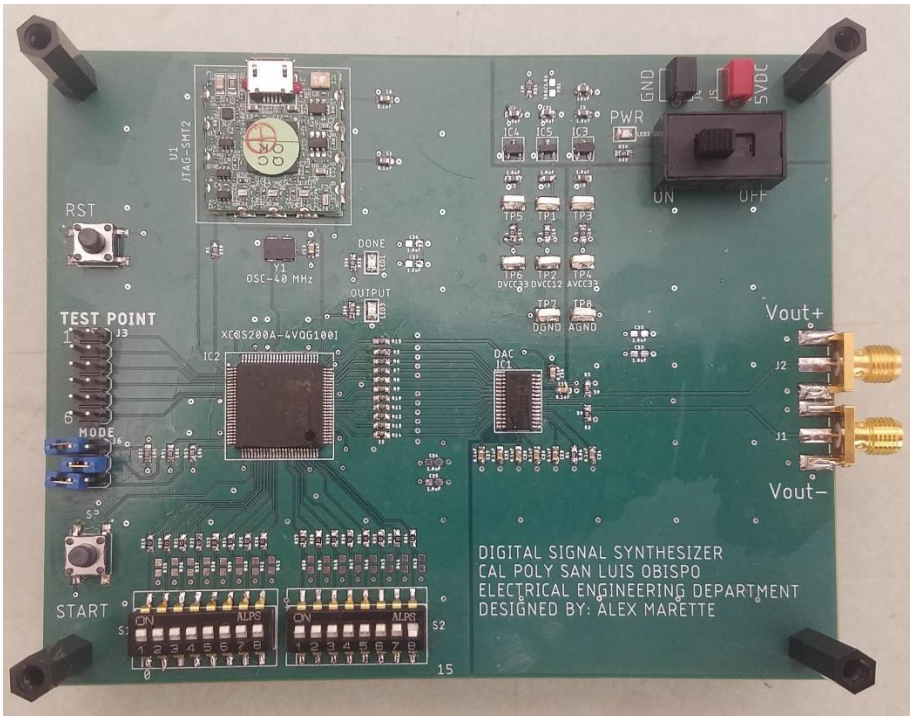


Figure 3-38: Completed Digital Synthesizer Device

After confirming full functional operation of the Digital Synthesizer, the current sense resistors were installed to measure the board current. Figure 3-39 shows the measured current and calculated power of the board with the output off and on. The difference between the two states can be used as a dynamic power estimate. Also, the off state can be estimated as the quiescent power. When comparing with the estimates on with Figure 3-12 The current draws for the 1.2 V digital supply and the 3.3 V analog supply match the original estimation. The current draw for the 3.3 V digital supply was 112 mA lower than estimated. This seems to be caused by incorrect dynamic power estimations for the FPGA.

Supply	Vrsence (mV)	Isupply (mA)	Power (mW)
Digital 3.3 Output Off	66.45	132.9	438.57
Digital 3.3 Output On	86.4	172.8	570.24
Digital 1.2 Output Off	8.06	16.12	19.344
Digital 1.2 Output On	17.17	34.34	41.208
Analog 3.3 Output Off	17.25	34.5	113.85
Analog 3.3 Output On	17.33	34.66	110.912

State	Total Current (mA)	Total Power (mW)
Output Off	183.52	571.764
Output On	241.8	722.36
Difference	58.28	150.596

Figure 3-39: Digital Synthesizer Board Current and Power Consumption

4 ANALOG UPCONVERTER DESIGN

4.1 Overview

The purpose of the Analog Upconverter Board is to take the differential signal from the Digital Synthesizer Board, mix it up to 2.4 GHz, and then amplify the signal before it is radiated through the antenna. This design is exclusively analog so there are no mixed signal design concerns to deal with however at 2.4 GHz there are many new concerns to deal with. Since parasitics capacitance and inductance are a function of frequency, at 2.4 GHz the parasitics are much higher than in the digital design. Additionally, at 2.4 GHz the wavelength become much smaller, decreasing the distance in which lumped elements become distributed. In other words, terminations and matching networks are crucial to ensure proper signal propagation.

4.2 Choosing Parts

As mention in Section 3.2, components must be selected before the design can begin. As seen on the block diagram in Figure 4-1, there are four main components to the design. The mixer will mix the 5 MHz - 80 MHz signal up to 2.405 MHz - 2.480 MHz using the VCO (Voltage Controlled Oscillator) as the LO (Local Oscillator) which will be set a 2.4 GHz. Next a VGA (Variable Gain Amplifier) is needed to amplify or attenuate the signal and to adjust the output power to determine the minimum power needed to jam a ZigBee device. Lastly, an antenna is needed to radiate the jamming signal out to the Zigbee device(s).

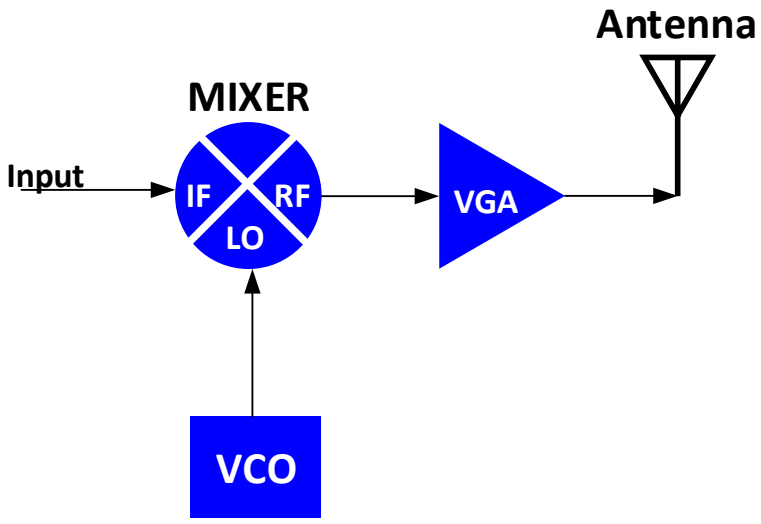


Figure 4-1: Simple Analog Upconverter Block Diagram

Additional auxiliary components are necessary to complete the design such as power supplies, matching networks, voltage references for the VGA and VCO, potentiometers to adjust the VGA and VCO, and lastly a balun to convert the differential signal to single ended.

When searching for a suitable mixer the most constraining parameter was the frequency range. For this application the IF frequency needs to span the 5 MHz to 80 MHz range while the RF is required to reach up to 2.480 GHz with a LO of 2.4 GHz. Furthermore, a differential input was desired (not required) since the output of the Digital Synthesizer board was also differential. The Linear Technologies LT5560 is a low cost active mixer that has an input and output range of 0.01 MHz to 4GHz. The power supply ranges from 2.7 V to 5 V which give more options when searching for the amplifier and VCO. Additionally, with active mixing no mixing loss occurs which means less amplification will be required down the line. The downside to the LT5560 is the lack of internal impedance matching and the harder to solder DFN (dual flatpack no lead) package [25].

When choosing the variable gain amplifier, the main requirement is the gain and the 1 dB compression point. The 1 dB compression point should be larger than the minimum required output power of -31.9 dBm found in Equation 2-2. The minimum required amplification was

found by taking the difference between the minimum output power and the 16 tone output power coming from the DAC. Figure 3-37 shows the 16 tone output power is -26 dBm therefore, the minimum required amplification is -5.9 dB, or 5.9 dB of attenuation as seen in Equation 4-1.

$$P_{AMP} = P_{Out\ Min} - P_{Out\ DAC} = -31.9\ dBm - (-26\ dB) = -5.9\ dB \quad (4\text{-}1)$$

Additionally, the amplifier was required to use a 2.7 V to 5 V power supply to match the mixer. Having only one power supply will help with the PCB design. The VGA is also required to be controlled with an analog interface instead of digital so that no additional microprocessor would be required. The VGA selected was the Analog Devices ADL5330. It is an analog controlled VGA with a maximum gain of 10 dB to16 dB and an output 1dB compression point of 9 dBm to 14 dBm over a range of 2.2 GHz to 2.7 GHz. The ADL5330 has a maximum attenuation of 30 dB. It requires a supply voltage of 5 V. The differential inputs and outputs of the VGA are matched to 50 ohms, helping to reduce the number of matching networks required [26].

A 2.4 GHz VCO is required to the LO input of the mixer. The typical LO input power range is -6 to 1 dBm therefore the selected VCO must have an output power that matches this range [25]. The only available VCO under $30 was the Maxim Integrated MAX2750. The MAX2750 is a 2400-2500 MHZ VCO with a 2.7 to 5 V input supply voltage, and a 50 ohm matched output with an output power of -3 dBm [27].

Both the VCO and the VGA require a tune voltage to control the output. This requires a stable voltage reference as to not cause frequency modulation or amplitude modulation cause by any power rail noise. To control the voltage reference, a digital push button potentiometer was selected to reduce any fine-tuning issues. The VGA has an input tuning range of 0.6 V to 1.4 V while the VCO has a tuning range of 0.4 V to 2.4 V. The Linear Technology LT6650 voltage reference can output a stable voltage from 0.4 V up to the input voltage which in this case will be 5 V. The voltage reference will be controlled by the Maxim Integrated DS1809 pushbutton potentiometer [28], [29].

The last device selected was the power supply. With all other components selected, a current estimation can be made using the datasheets of the components. Figure 4-2 shows the current draw estimation. With nearly 250 mA current draw, a safe 100% overshoot power supply current would be 500 mA. All the devices can be powered by the same power supply with a 5 V output. As with the Digital Synthesizer board, the power supply efficiency is not a concern while the power supply noise is a large concern. This makes a low drop out linear regulator the best choice. The Analog Devices ADM717X is an ultralow noise power supply with current output ratings of 0.5 A, 1 A or 2 A. The 1 A supply was selected to power the board and have plenty of additional current sourcing abilities to power an inline amplifier if one would be required later down the road.

Device	Current (mA)	# of Devices	Total (mA)
MAX2750 VCO	17	1	17
ADL5330 VGA	215	1	215
DS1809 POT	1	2	2
LT6650 Reference	0.015	2	0.03
LT5560 Mixer	12	1	12
Total Current			246.03

Figure 4-2: Analog Upconverter Current Estimation

Other miscellaneous parts were selected such as pushbuttons, power switches, SMA connectors, headers, test points, and an Antenna. Two special purpose passive components had to be chosen as well: an RFC inductor and an AC coupling capacitor. Extra consideration had to be taken when selecting these components due to the high frequency. Standard capacitors will act like inductors at high frequencies and standard inductors could act like capacitors at high frequencies. To avoid this issue, special inductors and capacitors had to be selected with self-resonant frequencies near or above 2.4 GHz. For the RCF, the Murata LQW18AN56NG8ZD 56 nH inductor with a self-resonant frequency of 2.6GHz was selected. For the AC coupling capacitors, the KEMET CBR06C100F5GAC 10 pF inductor with a self-resonant frequency of 2.4 GHz was selected.

4.3 Matching Networks

One major challenge when creating the schematic was the difference in impedance terminations and characteristic impedances. The characteristic impedance from the DAC is 100 ohms differential, the characteristic impedance from the VCO is 50 ohms single ended, and the characteristic impedance going into the VGA is 50 ohms differential. The three devices connect into the LT5560 mixer which is not terminated in any way. This means that the impedance at the ports of the LT5560 is complex and changes with respect to frequency. Between all three components and the LT5560, a matching network is required to help the signal propagate with minimal reflections. Figure 4-3 shows the block diagram containing the three matching networks.

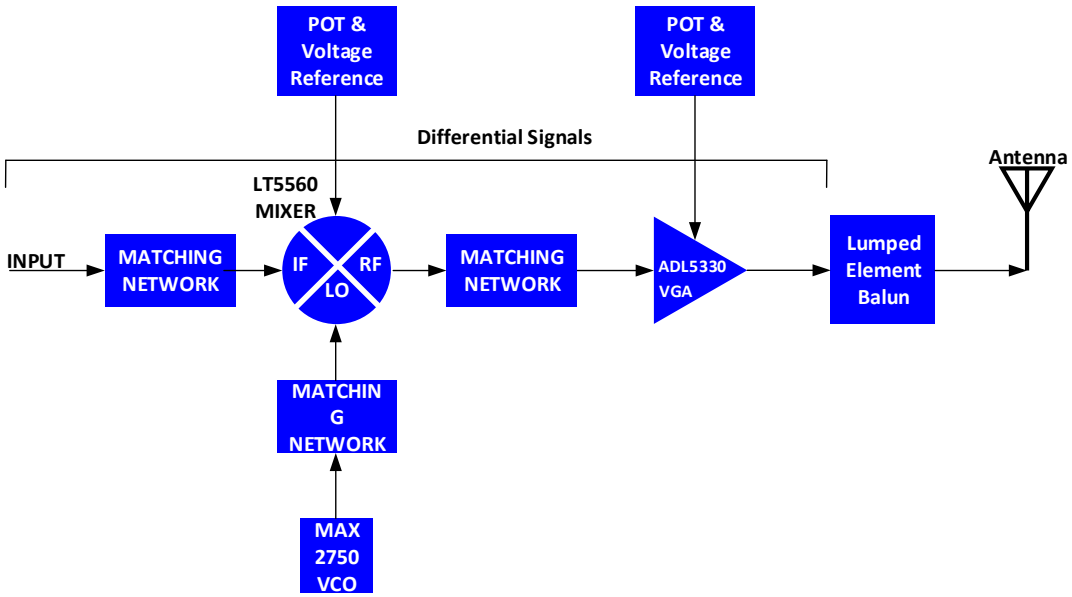


Figure 4-3: Complete Analog Upconverter Block Diagram with Matching Networks

The two matching methods used on this design were lumped element matching and single stub line matching. The lumped element matching was used for the 5 to 80 MHz input range while the single stub line matching was used for the higher 2.4 GHz matching.

The DAC output uses two 50 ohm impedance traces which can be represented as 100 ohm source impedance. The LT5560 datasheet states that at 70 MHz the differential input impedance is 28.5

+ j0.8 ohm. The matching network will serve to match the DAC output impedance to the mixer's input impedance while also serving as a low pass filter to help eliminate some of the harmonics and sinc roll off from the DAC. To design the differential lumped element matching network, the network will be split into two single ended networks. This can be seen on Figure 4-4 [25].

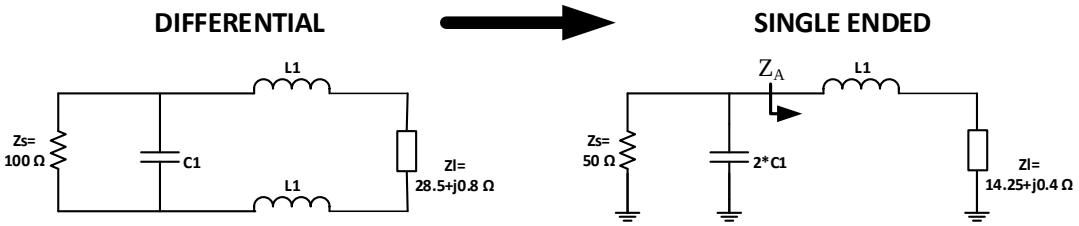


Figure 4-4: Differential to Single Ended for Matching Network Design

A Smith chart was then used to calculate the impedances for C1 and L1. All the hand drawn Smith chart work can be seen in APPENDIX E. Equations 4-1 to 4-3 show the calculation of the passive L1 and C1 components from the impedances and the center input frequency.

$$L_1 = \frac{Z_l Z_o}{2\pi f_c} = \frac{j0.45 \times 50}{2\pi \times 42.5E6} = 84.5\ nH \tag{4-2}$$

$$2C_1 = \frac{Y_c}{2\pi f_c Z_o} = \frac{1.59}{2\pi \times 42.5E6 \times 50} = 119\ pF \tag{4-3}$$

$$C_1 = 59.5\ pF \tag{4-4}$$

The results were simulated using ADS along with AC coupling capacitors and RFC (radio frequency choke) inductors required by the LT5560 to insure the input ports had no DC power. Figure 4-5 shows the simulation schematic and Figure 4-6 shows the simulation results.

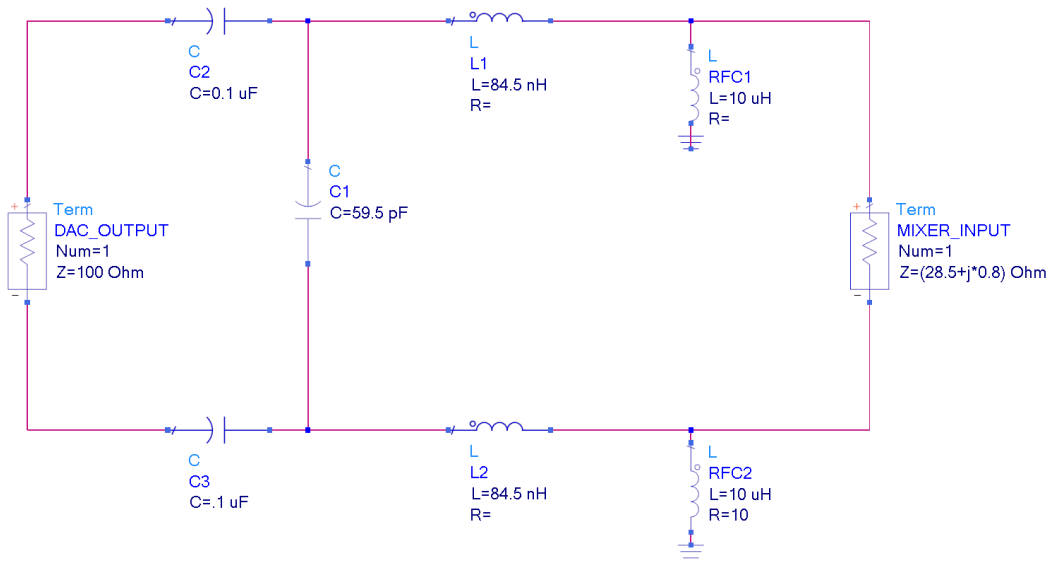


Figure 4-5: ADS DAC to Mixer Matching Network Simulation Schematic

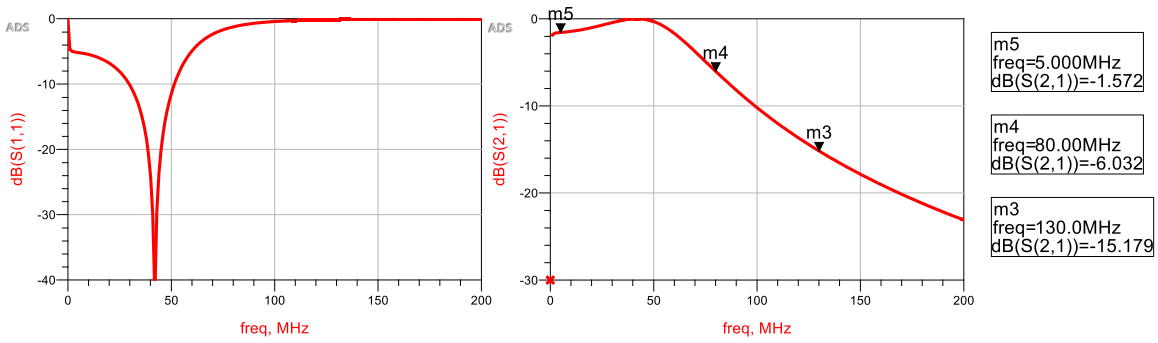


Figure 4-6: ADS DAC to Mixer Matching Network Simulation Results

The results show that there is a good match up to about 55 MHz but not all the way up to 80 MHz. Fc, the frequency used to calculate the component values from the impedances was increased to 60 MHz. This increased the width of the pass band at the cost of a slower roll off. This trade off was acceptable as the passband had to include all the jamming tones from 5 to 80 MHz. The new C1 value changed to 42 pF and the new L1 value changed to 60nH. The new simulation results can be seen on Figure 4-7. Some further analysis shows the small passband ripple is beneficial in smoothing the sinc roll off from the DAC. See Figure 4-8.

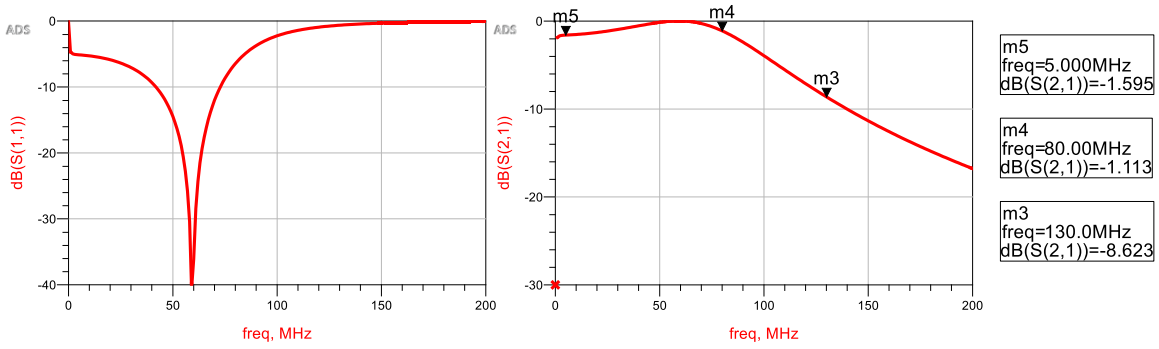


Figure 4-7: ADS DAC to Mixer Matching Network Updated Simulation Results

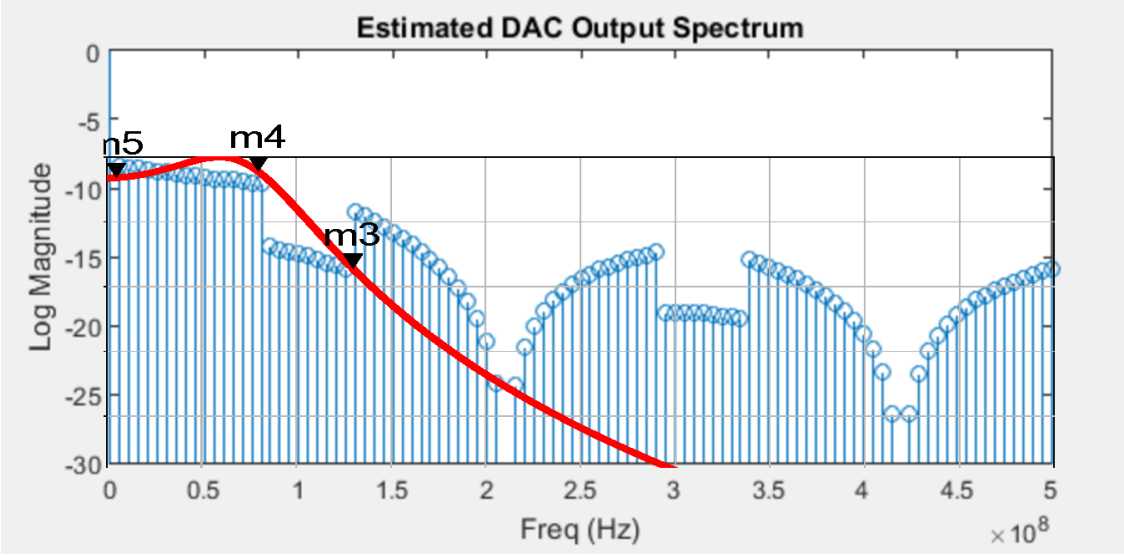


Figure 4-8: ADS Matching Network Simulation Superimposed on MATLAB DAC Output Simulation

The next matching network designed was the 50 ohm terminated VCO output to the LO input of the mixer. The LO input impedance of the mixer is 51 ohms in parallel with -j91 ohms at 2.21

GHz. Which is roughly 38-j21 ohms. This signal is a single ended signal which helps simplify the design however this design cannot be completed using lumped elements. Component value from impedance is inversely proportional to the frequency meaning that at such high frequencies the matching network would require pH and fF components making the network hard to tune. Additionally, at such high frequencies, the parasitics of the components would over power the desired properties causing the network to not work as simulated. The solution is to use a single stub line matching network. Figure 4-9 shows the schematic for the single stub line matching network [25].

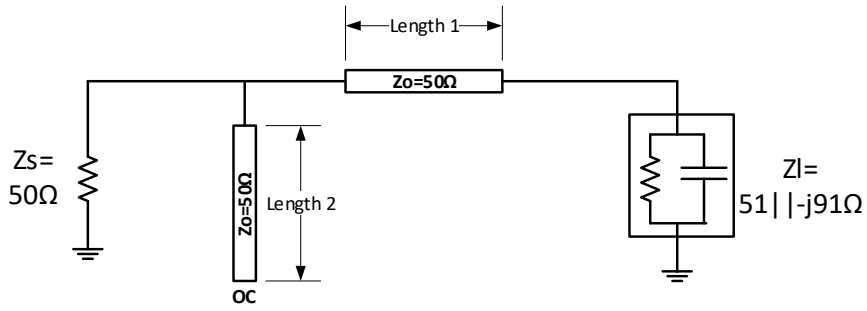


Figure 4-9: Single Stub for VCO to Mixer LO Matching Network

A Smith chart was used to find the electrical lengths for the microstrip traces. The electrical length for length 1 was 0.211 wavelengths and the electrical length for length 2 was 0.079 wavelengths. Using the desired characteristic impedance, the electrical lengths, and the PCB board properties, the physical width and length of each trace can be found. This was done using the ADS tool, LineCalc.

To use LineCalc, the PCB properties described in Section 3.5 must be entered along with the desired characteristic impedance and the desired line phase change. Equations 4-5 and 4-6 show the conversions from wavelength to phase in degree. The phase parameters were entered in LineCalc and the physical results for Length 1 can be seen in Figure 4-10. The physical line lengths were used to create a schematic in ADS which can be seen in Figure 4-11. The simulation

results, Figure 4-12, show that the match is not perfectly centered at 2.4 GHz although at 2.4 GHz the S11 is -17.9 dB which is considered a good match.

$$Phase_1 = 0.211\lambda\left(\frac{360°}{\lambda}\right) = 75.96° \tag{4-5}$$

$$Phase_1 = 0.079\lambda\left(\frac{360°}{\lambda}\right) = 24.44° \tag{4-6}$$

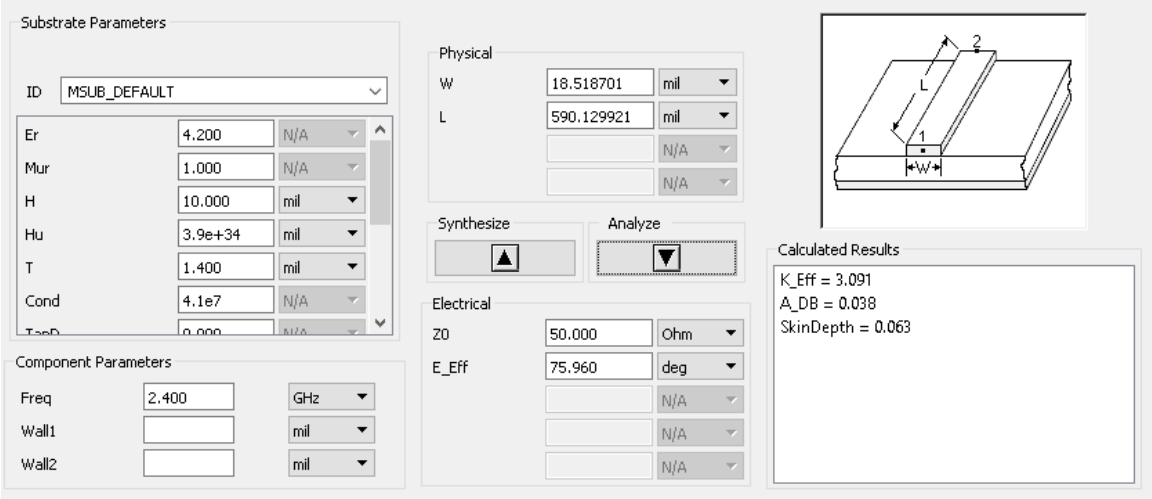


Figure 4-10: ADS LineCalc

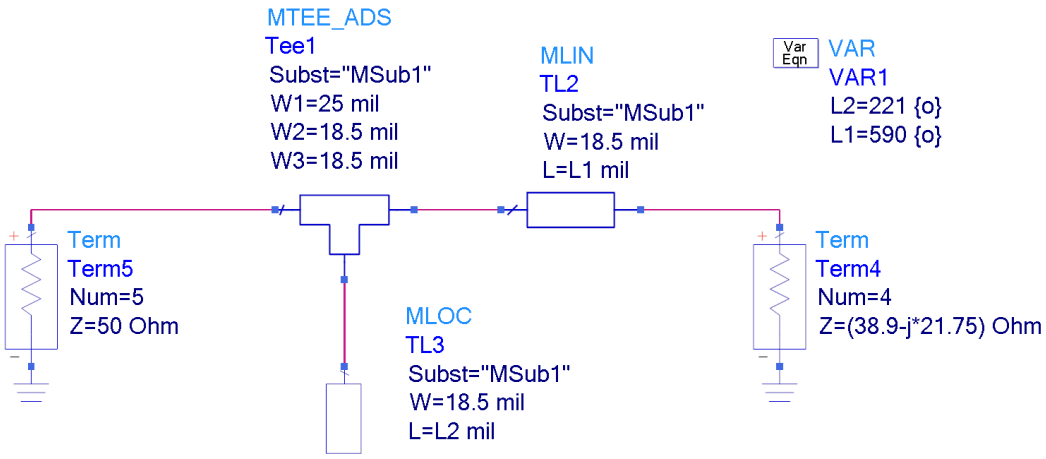


Figure 4-11: ADS VCO to Mixer Matching Network Simulation Schematic

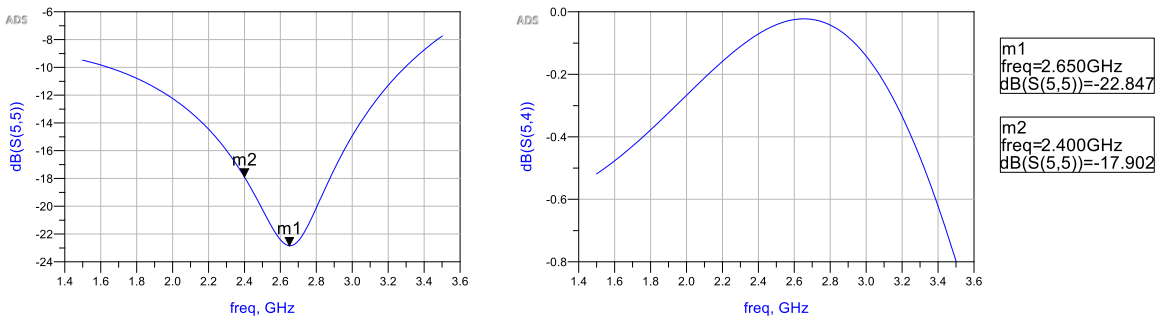


Figure 4-12: ADS VCO to Mixer Matching Network Simulation Results

The simulation was later altered to include the 25mm pads used to connect the AC coupling capacitors. The pads from the AC coupling capacitors add length and a different characteristic impedance to the total single stub line design. This needs to be compensated for which is often easier to implement in an optimization. An optimization was conducted to compensate for the AC coupling capacitor pads and to shift the center of the match to 2.4 GHz. The final physical detentions can be seen in Figure 4-13 and the final simulation results can be seen in Figure 4-14 .

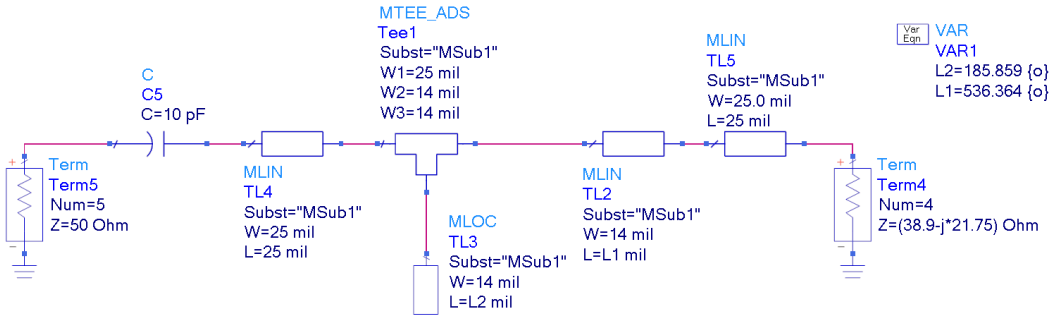


Figure 4-13: ADS VCO to Mixer Optimized Matching Network Simulation Schematic

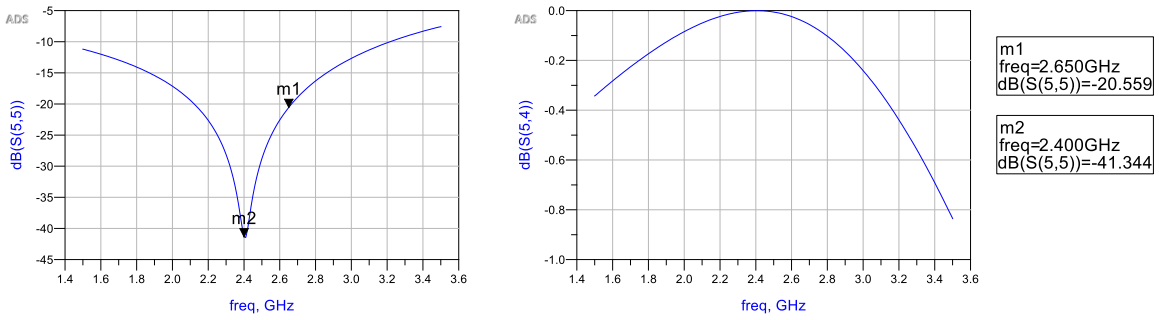


Figure 4-14: ADS VCO to Mixer Optimized Matching Network Simulation Results

The last matching network is from the output of the mixer to the input of the VGA. This is both a high frequency signal and a differential signal, so the design uses the differential technique used for the DAC to mixer network and it uses the single stub matching network discussed in the VCO to mixer network. The differential output impedance of the mixer is 612 ohms in parallel with -j95.7 ohms or 14.6-j93.4 ohms. As before the network was designed using a Smith chart, simulated, and then optimized. Figure 4-15shows the final optimized matching network along with the decoupling capacitors and the 5 V biasing RFC required by the VGA datasheet. The original Smith chart simulation results is the red trace on Figure 4-16 and the optimized result is the blue trace on the same figure.

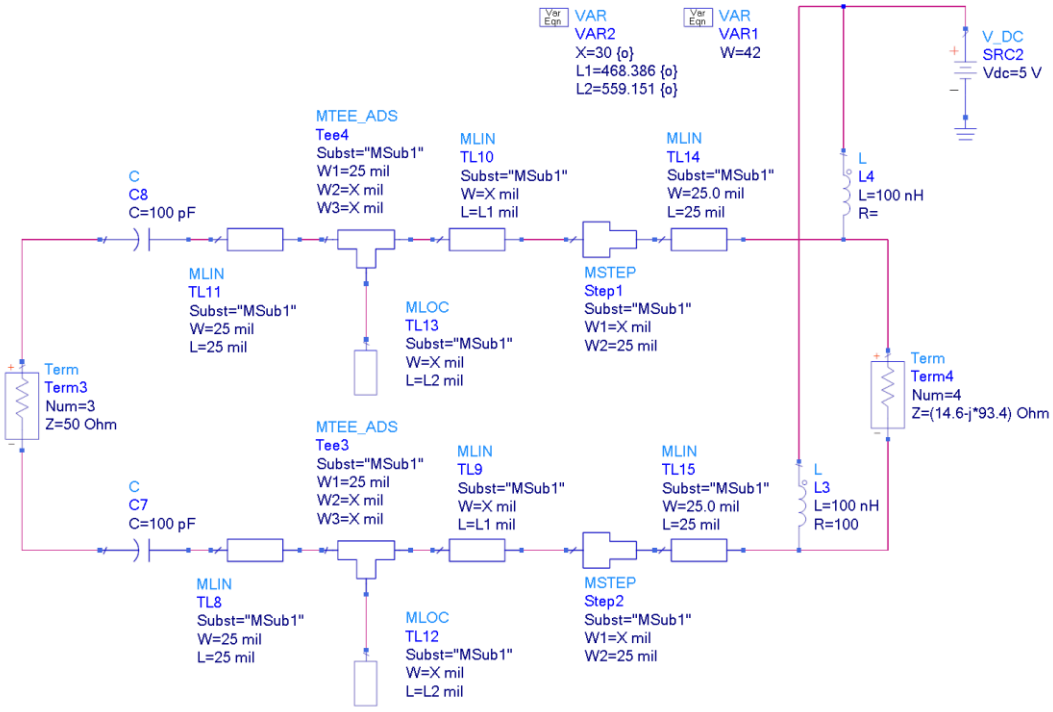


Figure 4-15: ADS Mixer to VGA Optimized Matching Network Simulation Schematic

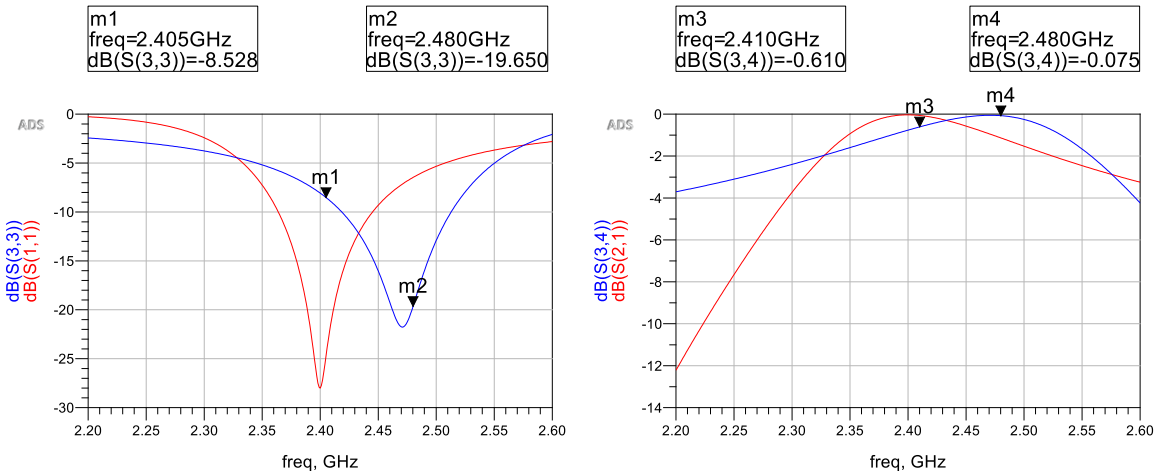


Figure 4-16: ADS Mixer to VGA Matching Network Simulation Results. Optimized (blue) Original (red)

The challenge with single stub microstrip design is that it is very narrow band. Trying to have a bandwidth of 80 MHz was a challenge. To further help the effect of the sing roll off on the DAC the best match was placed at the higher channel frequencies where the sinc roll off had the largest effect.

A balun is required to transform the 50 ohm differential signal to a 50 ohm single ended signal. There are many ways to create this balun including the reference on the ADL5330 VGA datasheet which can be seen in Figure 4-17. This was considered and simulated on ADS using the recommended values. The simulation results seen in Figure 4-18 show that the match is very good with a reflection coefficient less than 15 dB throughout the passband. Ultimately, this design was scrapped after selecting the Murata LDB182G4505C-110 all in one filter and balun designed for 2.4 GHz to 2.5 GHz [26], [30].

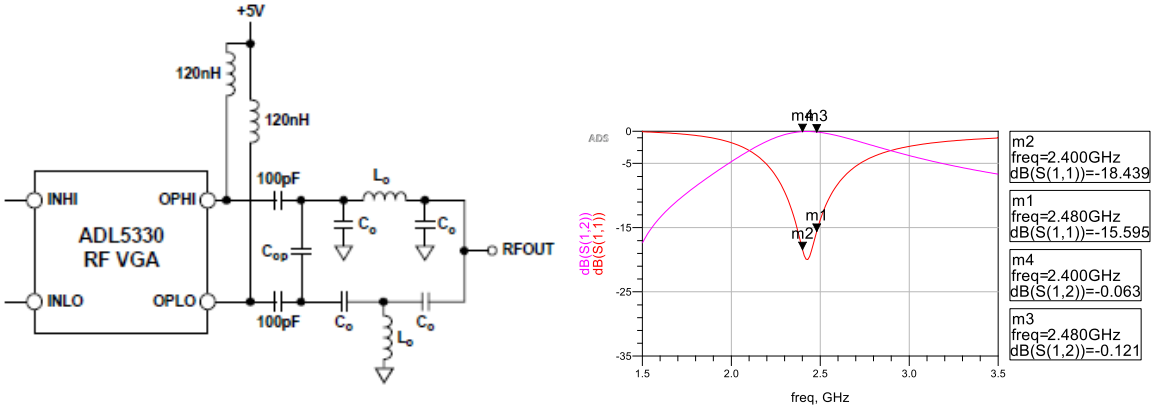


Figure 4-17: ADL3550 VGA Lumped Element Balun[26] *(left)*
Figure 4-18: Homebrewed Balun Simulation Results (right)

4.4 Schematic Design

Many of the same schematic design techniques used in the Digital Synthesizer design were also used in the Analog Upconverter schematic design. As with the Digital Synthesizer, the component datasheets and development board schematics were referenced as a guide for selecting properly sized components such as RFC, inductors, bypass capacitors, and decoupling capacitors. Also, the component symbols and layouts were collected by using the libraries provided by Digikey, libraries requested from Symacsys Component Search Engine, and libraries created manually using Eagle.

Creating the stub lines in Eagle proved to be a challenge. This is because Eagle does not have an RF transmission line tool as some of the other more advanced PCB design software. The solution was creating a matching network library that contained a schematic symbol and a layout footprint with the desired trace widths and lengths. An example of one of the components can be seen in Figure 4-19.

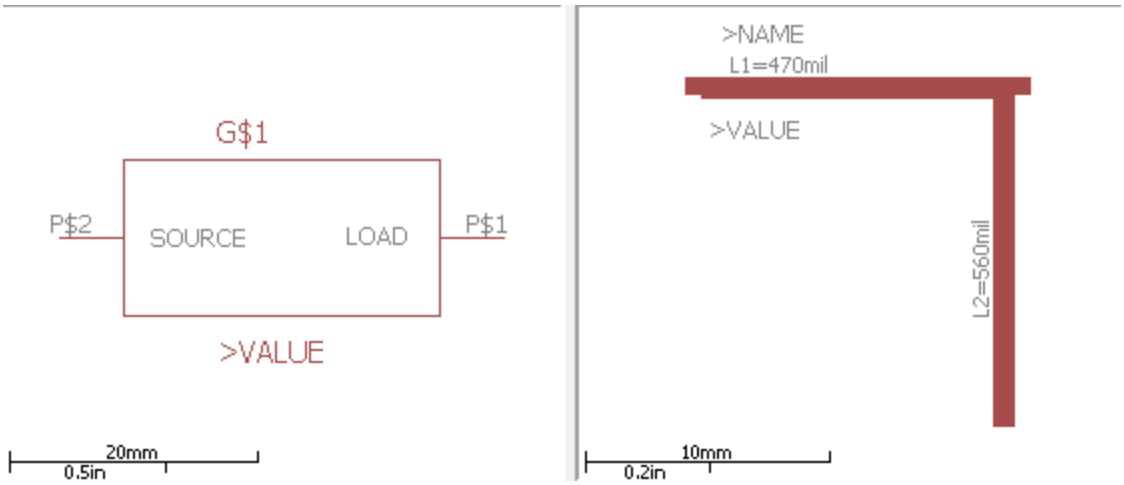


Figure 4-19: One of two Mixer to VGA Matching Network Schematic Symbol (left) and Layout Footprint (right)

The first component placed in the schematic was the mixer and all three matching networks that attach to it. The decoupling capacitors and RFC to ground and VCC were also added. The schematic can be seen in Figure 4-20. Note that the input matching network consists of lumped elements as described in the matching network between the DAC and the mixer. Also note that the MN2 and MN3 are part of the same differential matching network from the mixer output to the VGA input.

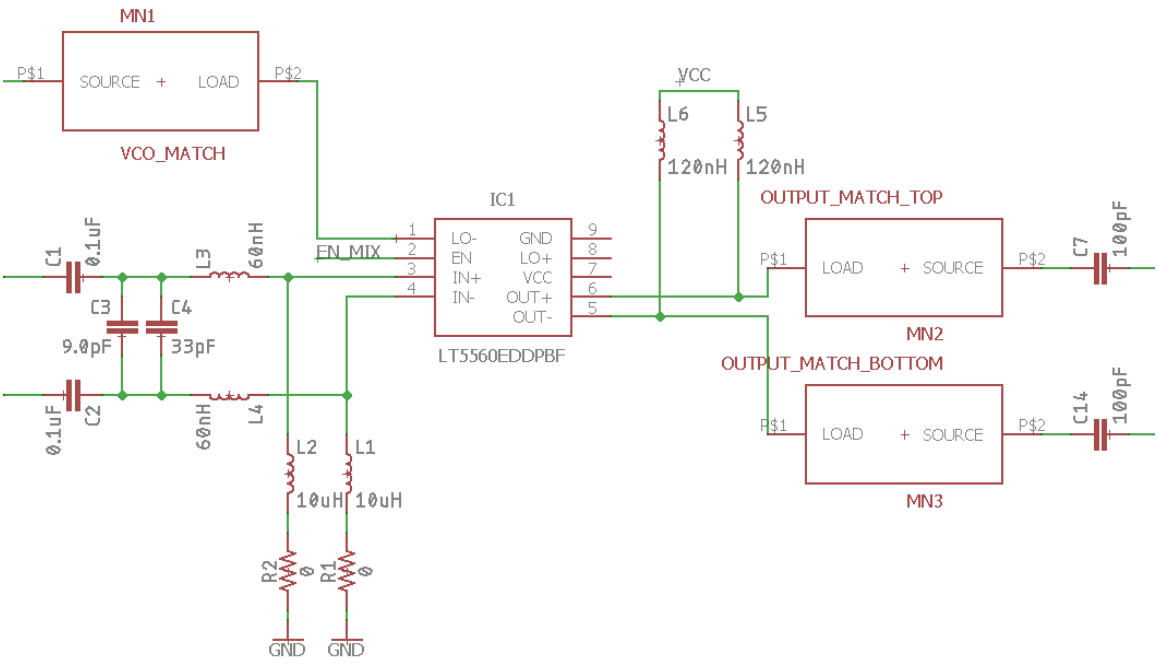


Figure 4-20: LT5560 Mixer Schematic and Matching Networks Schematic

Next, the ADL5330 VGA was added to the schematic along with the Murata balun. The input of the VGA was connected to the mixer matching networks and the output was connected to the balun using decoupling capacitors and RFCs to bias the amplifier. This portion of the schematic can be seen in Figure 4-21

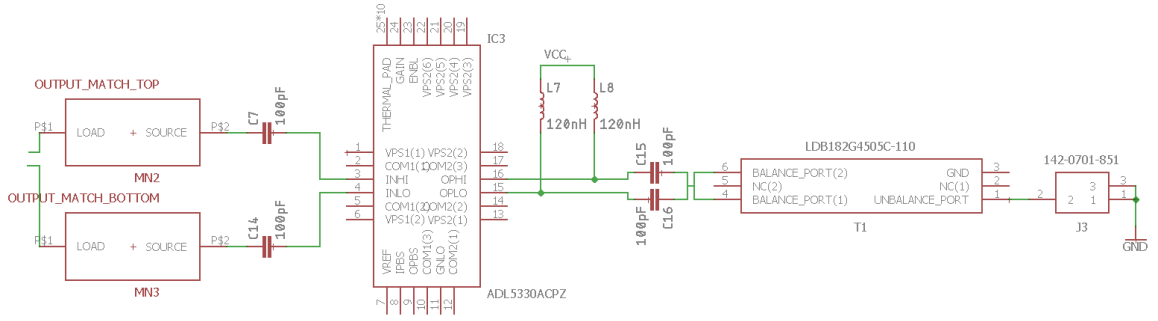


Figure 4-21: VGA and Balun Schematic

The two tuning circuits were designed in tandem with only small changes between the two to account for the different required tuning voltages. As mention in Section 4.2, the VCO has a tuning range of 0.4 V to 2.4 V and the VGA has a tuning range of 0.6 V to 1.4 V. The digital potentiometer has 64 discrete positions which limits the gain and frequency resolutions. For example, from 0.4 V to 2.4 V with 64 steps and a tuning gain of roughly 115 MHz/V creates a 3.6 MHz step as seen in Equations 4-7 and 4-8. This would not work well as the IEEE 802.14.5 channel bandwidths widths are 2 MHz. Less than 0.5 MHz steps were desired.

$$\frac{\Delta V}{\Delta \text{step}} = \frac{2.4 - 0.4}{64} = 0.03125 \frac{V}{step} \tag{4-7}$$

$$\frac{\Delta F}{\Delta step} = 115 \frac{MHz}{V} \times 0.03125 \frac{V}{step} = 3.6 \frac{MHz}{step} \tag{4-8}$$

By referencing he VCO tuning curve found on the VCO datasheet the tuning voltage range was reduced to 0.75 V to 1 V which corresponds to a frequency range of 2390 MHz to 2415 MHz. This leads to a frequency step of 0.45 MHz which allows for much better VCO tuning. Figure 4-22 shows the basic schematic for the voltage reference. Equation 4-9 shows the output voltage as a function of RF and RG in which RF is the series combination of the potentiometer and the resistor R. Knowing that the desired output voltage is 0.75 V to 1 V and that the potentiometer ranges from 0 to 50 kohms, the values for RG and R can be found. See Equations 4-10 to 4-12.

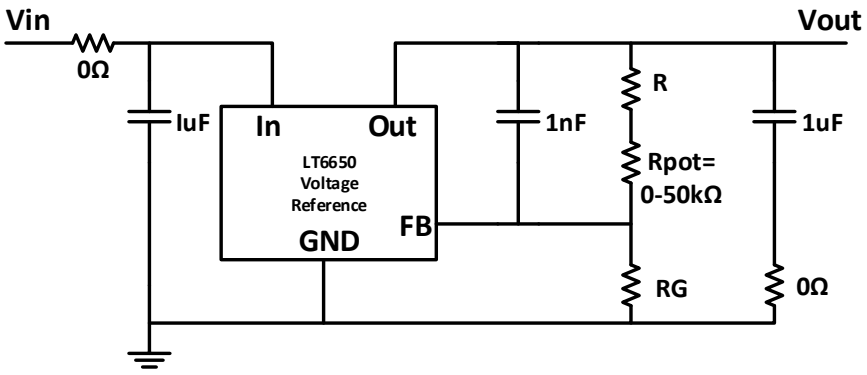


Figure 4-22: Voltage Reference Circuit Schematic

$$V_{out} = 0.4\left(1 + \frac{RF}{RG}\right)\mathrm{V} = 0.4\left(1 + \frac{R_{pot} + R}{RG}\right)\mathrm{V} \tag{4-9}$$

$$\left(\frac{RF}{RG}\right)_{high} = \frac{\mathrm{R} + 50000\Omega}{\mathrm{RG}} = \frac{V_{out_{high}}}{0.4\mathrm{V}} - 1 = 1.5 \tag{4-10}$$

$$\left(\frac{RF}{RG}\right)_{\mathrm{low}} = \frac{\mathrm{R} + 0\Omega}{\mathrm{RG}} = \frac{V_{out_{\mathrm{low}}}}{0.4\mathrm{V}} - 1 = 0.875 \tag{4-11}$$

$$RG = 80k\Omega \qquad R = 70k\Omega \tag{4-12}$$

The same steps were taken to find the resistor values for the VGA tuning voltage.

Both the voltage reference and potentiometers were placed in the schematic using the datasheet recommended values for the bypass capacitors. The digital potentiometer has a memory that can save the position of the wiper. The digital potentiometer has an autostore option which saves the last wiper position in memory when the device is powered down. This is done by adding a Schottky diode and capacitor to the storage enable pin as seen in Figure 4-23. Figure 4-24 shows the completed tuning schematic for the VCO along with a test point, bypass capacitors, and the required pushbuttons.

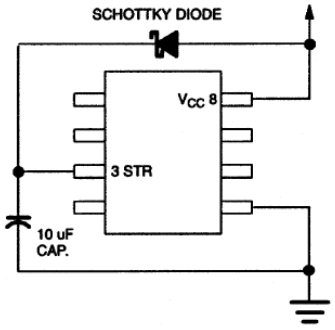


Figure 4-23: Digital Potentiometer Autostore Configuration [29]

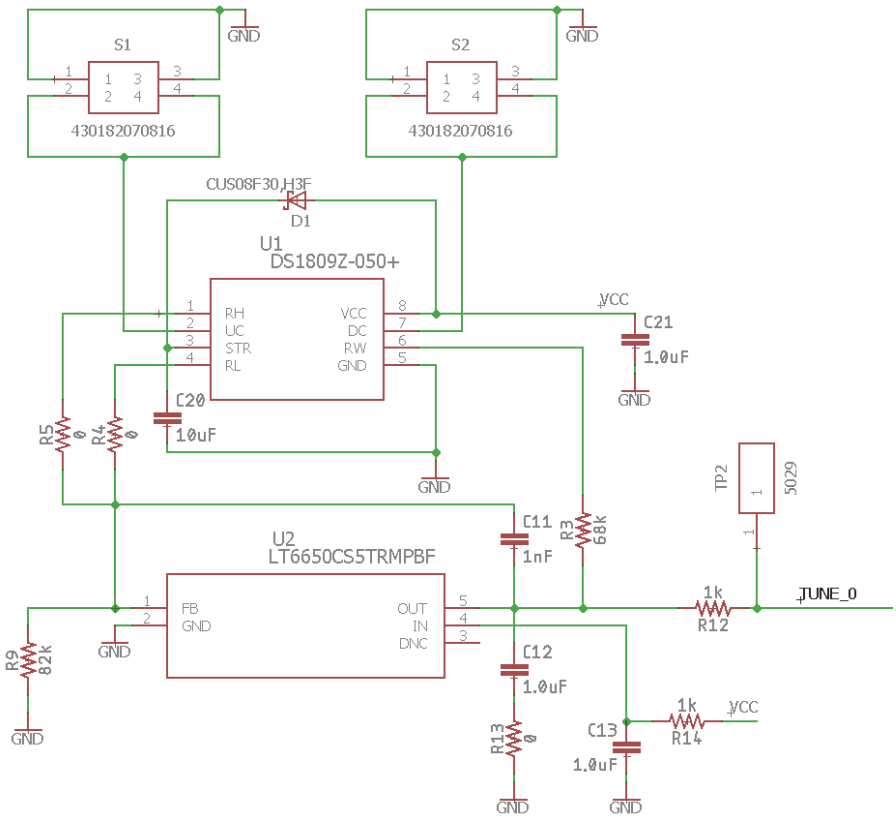


Figure 4-24: Complete VCO Tuning Circuit

Lastly the power supply was added to the schematic. As with the digital board, bypass capacitors were added to all supply ports of the components in the schematic. In addition, a power LED, current sensing resistors, test points, and power headers were added to the schematic. An output power header was added in case a clean 5 VDC supply was needed for an inline amplifier. To help troubleshoot the circuit, an enable header was added to control the mixer, oscillator, and amplifier. Monitoring the current draw while enabling he individual components can help identify a problem. The schematic for the power circuit and enable circuit can be seen in Figure 4-25. The complete schematic for the Analog Upconverter board can be seen in APPENDIX B. As with the digital design, the parts list was exported from Eagle and formatted to calculated expected cost. The Eagle parts list and the final Digikey parts list can be seen in APPENDIX D.

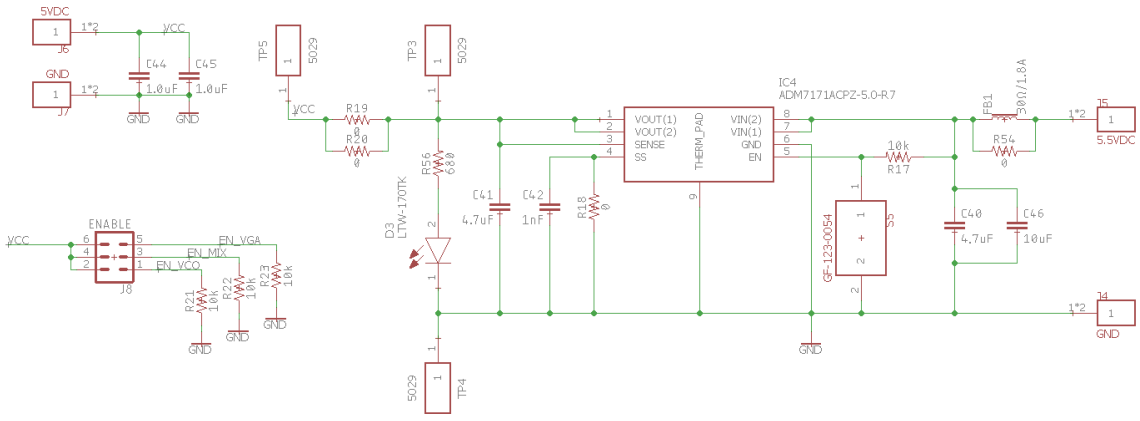


Figure 4-25: Analog Upconverter Power Schematic

4.5 Layout Design

When compared to the layout design of the Digital Synthesizer, the Analog Upconverter is quite simple. As in the digital design, a 4-layer stack with a signal, ground, power, and signal layer was selected. Since there are no digital signals, a split ground plane was not required. Additionally, since there is only one power supply, a split power plane was not required. This greatly simplifies the design work. The only major consideration was component placement.

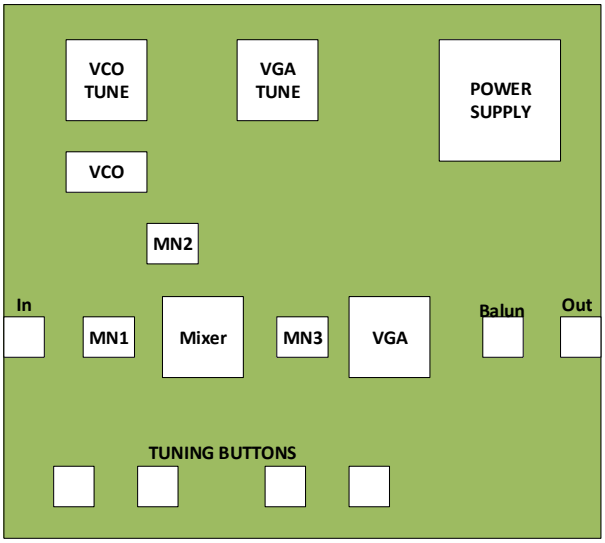


Figure 4-26: Analog Upconverter Layout Plan

When converting the schematic into the layout, the first step was to place all the major components to match as best as possible the layout plan shown in Figure 4-26. Traces and AC coupling capacitors were placed to connect all the components to one another. As with the digital design, careful attention to the trace widths was taken to ensure proper trace characteristic impedances. For the analog design, a microstrip trace was used instead of the coplanar wave guide. At the 2.4 GHz range, for the top signal layer ground plane and the ground plane below it to seem as on solid continuous ground plane, the via spacing would have to be less than 7.5 mm apart or 1/8 of a wavelength. This would require a large number of vias which is often raises the price of the board manufacturing [31]. Microstrip lines were also selected because of the single stub matching networks which had been designed for microstrip traces and not coplanar waveguides. Using the microstrip traces leads to more loss and thicker traces but allows for a cheaper and simpler design [32]. In Figure 4-27 note that the ground plane stops short of the high frequency signal traces allowing them to act as microstrip traces instead of coplanar wave guides.

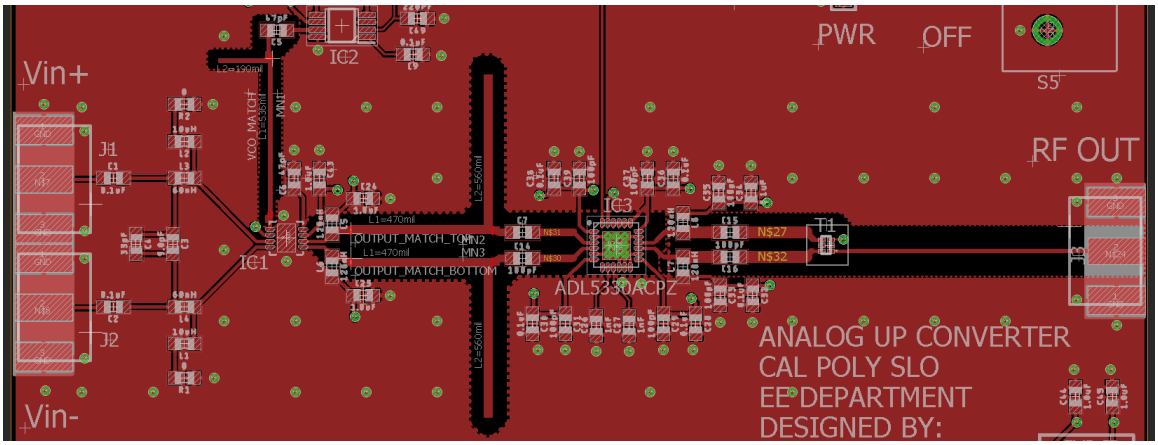


Figure 4-27: High Frequency Traces on Analog Upconverter Layout

For this design, Bay Area Circuit was selected to manufacture the board dude to the tighter tolerances on dielectric thickness and dielectric constant. This helps reduce variation in the trace characteristic impedance in the manufactured board from the desired characteristic impedance. The Bay Area Circuits design rules were checked with Eagle's DRC and additionally the board

Gerber files were checked with the Free DFM web service provided by Bay Area Circuits. The board passed both checks and was ready to be manufactured. The Analog Upconverter final board layout can be seen APPENDIX C. The bare Analog Upconverter PCB can be seen in Figure 4-28.

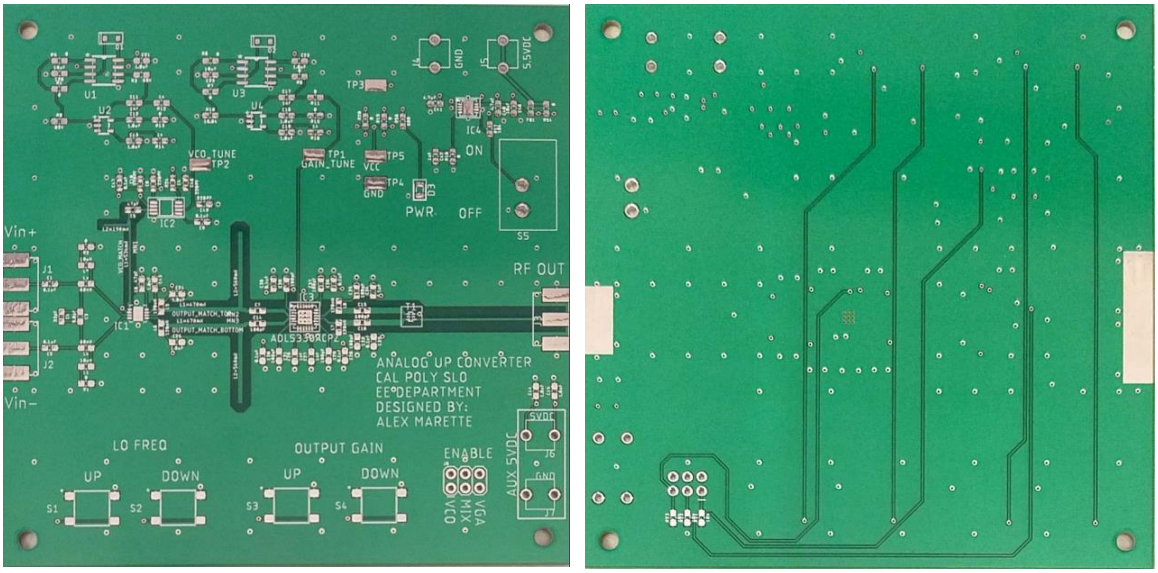


Figure 4-28: Analog Upconverter Bare PCB Board Top (left) & Bottom (right)

4.6 Building and Testing

Similarly, to the Digital Synthesizer board, the multiple systems on the board, a build and test order was devices. This helps ensure each system is working as desired before moving to the next one. This greatly helps the troubleshooting process. The three main systems for this board is the power supply system, the VCO and VGA tuning circuits, and finally the RF upconverter and amplifier system. The build order was as follows.

1. Install all components required to power the board: Banana Connectors, Switch, Linear Regulator, LED, Power Supply Bypass Capacitors, and the Test Points.
    a. Omit the series resistors for current measuring
2. Characterize the voltage regulator
    a. Vout vs Iout
3. Populate the components required for both tuning circuits: Potentiometers, Voltage References, Switches, Test Points, Schottky Diode, and other passive components.
    a. Record tuning voltage after each button press with both circuits.

    b. Adjust tuning circuits if necessary by changing R and RG.
4. Populate all remain circuit board parts. Test individual RF components.
    a. Remove the Enable headers from all three RF components.
    b. Power up the board and monitor board input current.
    c. Individually enable each component and check for proper change in current draw.
5. Run Full characterization of Analog Upconverter board
    a. Measure single tone output at minimum and maximum gain at all desired frequencies.
    b. Measure carrier isolation.
    c. Measure frequency change and gain change per potentiometer step.
6. Replace series no-load resistors with appropriate resistors for current measurement.
    a. Measure current for single tone with VGA at minimum and at maximum gain.
    b. Measure current for all tones with VGA at minimum and at maximum gain.
7. Replace series resistors with no-load resistors after power calculations.

Due to the no lead packaging, the power supply (along with the mixer, VGA, and balun) had to be soldered using solder paste and a heat gun. The technique is relatively simple with a few important things to consider. The amount of solder paste should be minimal. Just a small dab on each lead is enough. If too much was placed, a needle or toothpick was used to remove the excess and move around the solder paste. Also, if the solder stop layer was well designed, the solder paste will find the pad when heated if it is slightly off. Lastly, a proper heating profile should be followed as shown in Figure 4-29. This helps reduce the risk of damage to the component and the board when soldering the components. For the preheat section, the heat gun was roughly 10 inches over the board at 300 degrees C for about 2 minutes. Then the gun was slowly brought to about 2 inches from the board until the solder reflowed (usually less than 30 seconds). Finally, the gun was pulled back to 10 inches for another two minutes to slowly bring the board temperature back down.

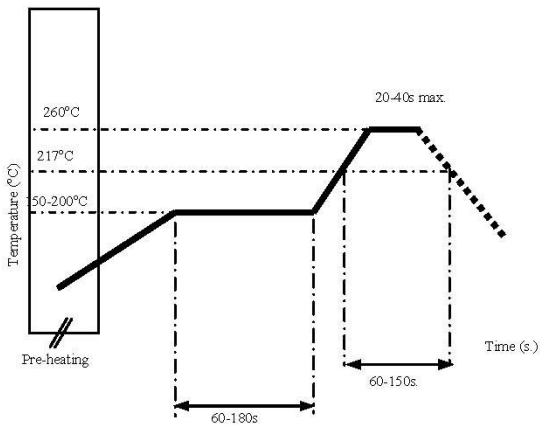


Figure 4-29: Reflow Solder Heating Profile[33]

After soldering, the power supply circuit was tested using a variable resistive load. The load was adjusted to produce a current from 50 mA up to the limit of 1000 mA. The power supply output voltage was measured after each load step. Figure 4-30 shows that from 50 mA to 1000 mA, the output only deviated a total of 80 mV. Note that the step appearance of the plot is caused by the limited resolution of the measuring device used. This test shows that the output voltage will stay within the desired range when going from the estimated current draw of 250 mA to a larger load caused by an in line amplifier.

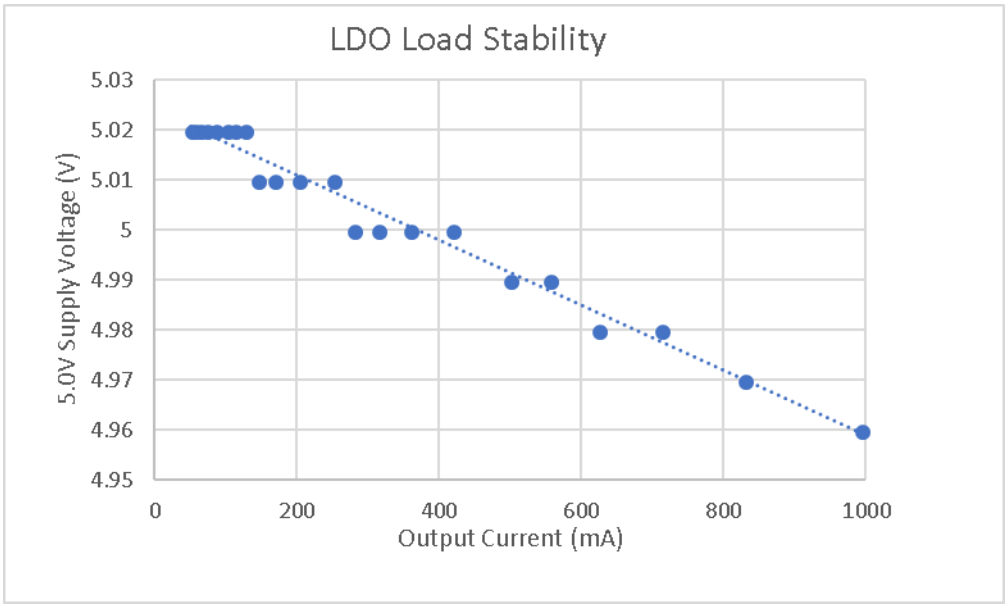


Figure 4-30: Analog Upconverted Power Supply Load Stability

Next both tuning circuits were built and tested. During the test, the output voltage was recorded after every step of the potentiometer. The results were compared to the original calculations preformed in Section 4.4 and can be seen in Figure 4-31. With both circuits, the measured output seems to be non-linear as is deviates from the expected more as the potentiometer position increased. This was expected as Equation 4-9 is a simplified output equation found in the datasheet which ignores the FB pin current. Both designs pass through the desired voltage range and therefore no adjustments were made.

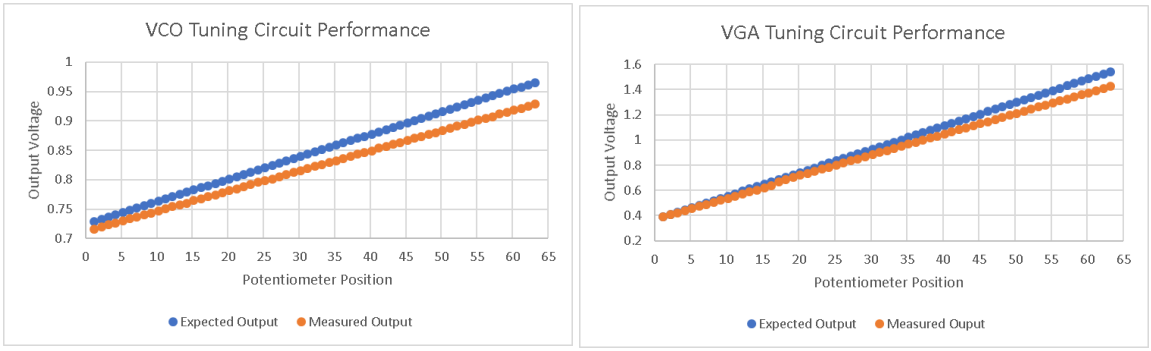


Figure 4-31: Tuning Circuit Performance: VCO (left) VGA (right)

After proper power supply and tuning circuit operation was confirmed, the remaining components of the device were soldered into place. The mixer, VGA, and balun used the same reflow procedure mentioned in the power supply soldering section.

After all components were soldered, the board was powered up with all three enable headers removed and 50 ohm terminations added to the inputs and output. One at a time, the VCO, mixer, and then VGA were enable and the difference in current was measured. The measured currents, differences, and expected values can be seen in Figure 4-32. The results show that all major RF devices power on properly.

Components On	Total Current (mA)	Device Current (mA)	Expected Device Current(mA)
Power Supply & Tune Circuits	1	1	1-4
Add VCO	10	9	11
Add Mixer	15	5	10
Add VGA	150	135	100-215

Figure 4-32: Power On Test Results

After confirming the that all components powered up properly, a frequency and power sweep was done to characterize the performance of the Analog Upconverter. Both sweeps were done with the LO frequency at 2.4 GHz and the amplifier at maximum gain. The characterization results can be seen in Figure 4-33. By looking at the results, it was apparent that some things were wrong. The most apparent problem noticed while looking at the spectrum analyzer was the high-power carrier signal. As a double balanced mixer, the carrier signal should be suppressed. In the case of 1900 MHz, the LO signal should only have a -36 dBm leakage according to the datasheet. Another issue is the difference in performance when comparing the upper side band to the lower side band. The plan was to use the upper side band for this design, but the upper side band is between 2 and 12 dB less than the lower side band depending on the input frequency. The last major issue is the tone output power. This design consists of an active mixer with a gain of roughly 1 dB and an amplifier with maximum output of roughly 10 dB at the 2400 MHz range, yet the output signals range from 20 to 40 dB less than the input power.

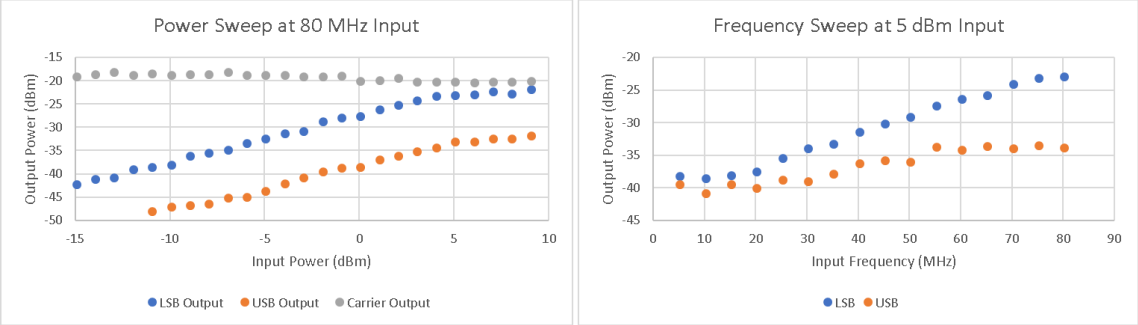


Figure 4-33: RF Component Characterization Result

According to the datasheet, the lowest amount of output LO (carrier) leakage occurs when the DC resistance from the input ports to ground must be equal. After probing on the input pins and input matching network it was found that L1 in Figure 4-20 was soldered only on one side but not the other causing a poor electrical contacts and therefore a high impedance path to ground from the input pin (pin 4) [25].

While trying to understand the poor upper side band performance it was noted that all high frequency AC characteristics were found using the lower side band while the low frequency AC characteristic tests used the lower side band. There is no text which states the upper and low side band should be used for a specific application, but the characteristic trends lead to using the lower side band for high frequency output mixing. Lucky the VCO has an output range of 2400 MHz to 2500 MHz which means the VCO can be set to 2485 MHz and the lower side band can be used. The only changes need to be made are with the VCO tuning circuit and the FPGA switch order since now channel 16 (2480 MHz) requires a 5 MHz input and channel 1 (2405 MHz) requires an 80 MHz signal.

To change the tuning circuit, first the zero load resistor connected the tuning circuit to the VCO tuning input was removed. Then using an external power supply, the tuning voltage was adjusted until the carrier was at 2485 MHz. The tuning voltage was recorded to be 2.05 volts. Using a 3 V sing, the low and high tuning voltages were set to 1.9 V and 2.2 V. Then using the same steps found in Equations 4-9 to 4-12, the two resistor values, R and RG, were found to be 250 kOhms and 66.7 kOhms respectively.

After the completing the two fixes, the Analog Upconverter was characterized again. This can be seen in Figure 4-34. After the two fixes the maximum single tone output power increased from -22 dBm to -14 dBm when just looking at the LSB. When considering the switch from the upper sideband to the lower sideband, then the fix increased the output power by 18 dB. Also note that the carrier power decreased from roughly -20 dBm to roughly -50 dBm. Another difference is the flatness of the frequency response on the lower side band. Before the fix the lower side band had

roughly 15 dB roll off through the desired frequencies while after the fix, the lower side band has less than 3 dB roll off.

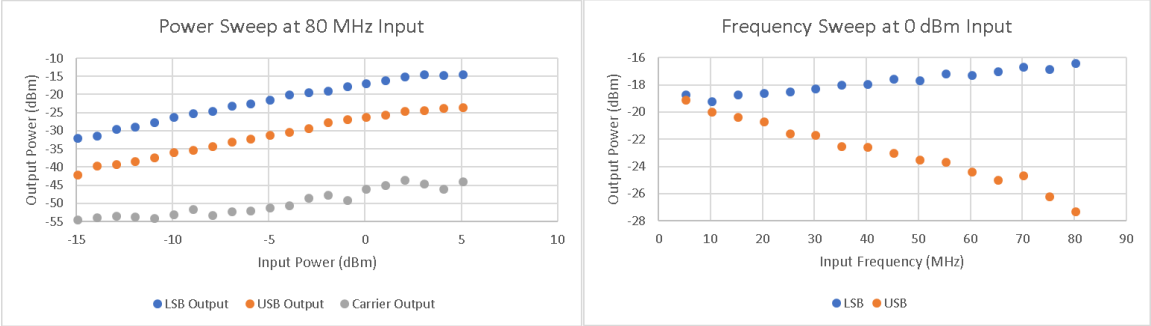


Figure 4-34: RF Component Characterization Results after Fix

The two fixes caused a significant increase in performance; however, the overall performance of the device is worse than expected. The board consists of an active mixer with 1 dB gain and a VGA which has a maximum of 10 dB gain. At an input power of 0 dBm, one would expect the output power to be 11 dBm. With a maximum power of -16 dBm with 0 dBm input, the output is 27 dB less than the expected output.

Between the input and the output of the Analog Upconverter board there is a loss of 27 dB. This is a very difficult problem to troubleshoot and can only be tackled via trial and error. Typically, there are just a few ways in which RF energy is lost in a design which include reflections, radiation, conductor, and dielectric losses. When looking at just one matching network or just one components such as an amplifier, the reflection can be measured using a network analyzer but when dealing with a system of components this is not possible. Therefore, impedance mismatches and reflections were ruled out assuming all matching networks worked as desired. To test for radiation, a small loop was created by across the inner and outer connectors of a coax cable. This cable was attached to a spectrum analyzer and the loop is placed close to the board as seen in Figure 4-35. When moving this loop across the board only one small peak of -35 dBm was found at 2.485 which was the VCO frequency, see Figure 4-36. This power was a maximum when the loop was directly over the coupling capacitor between the VCO and the mixer. To address this the

coupling capacitor was replaced with one of a larger nominal value (from 47 pF to 100 pF) which should also decrease the series impedance. This made no difference in the output. Note that the radiation measurement was made within a faraday cage to remove any wireless power from the busy 2.4 GHz range.

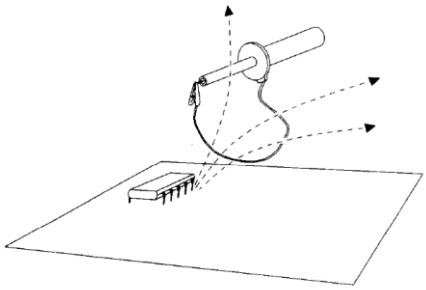


Figure 4-35: PCB Magnetic Field Testing [21]

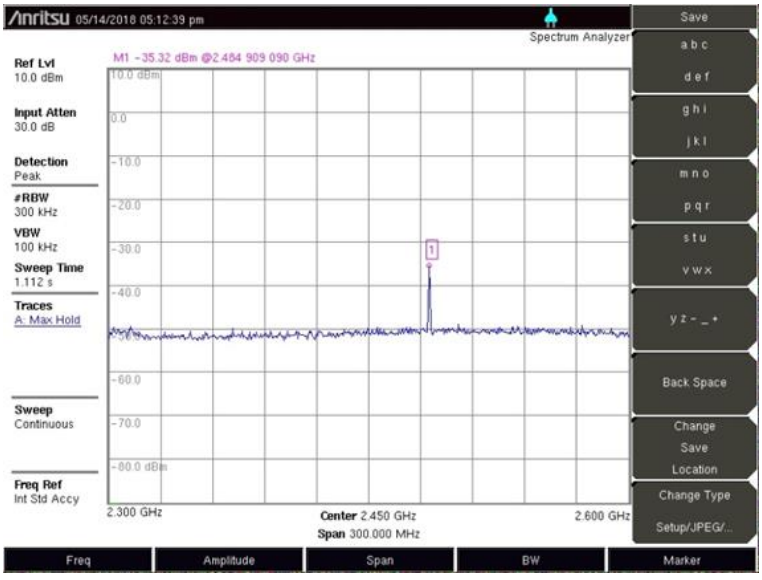


Figure 4-36: Results of Radiation Test

Another problem could be power loss through the RFCs into the DC circuit. If the selected RFC inductors did not perform as expected with respect to inductance and self-resonance frequency, it could cause RF power to pass through the RFC into the DC circuit and then ground out through the bypass capacitors. First the DC was measured again using a spectrum analyzer inside a faraday cage to see if there was any RF power in the DC circuit. There was no notable RF power

in the DC circuit. Just to be sure, all RFC were replaced by a smaller 14 nH inductor with self-resonance at 3.6 GHz. This made no difference.

One last attempt to find the issue was by increasing the AC coupling capacitors from 100 pF to 1000 pF which should decrease the series line impedance by a factor of 10. This also had no effect on the output power. At this point no more time could be allotted for the Analog Upconverter troubleshooting. With a series of inline amplifiers, there should still be enough power to successfully jam a ZigBee network. An image of the completed Analog Upconverter can be seen in Figure 4-37.

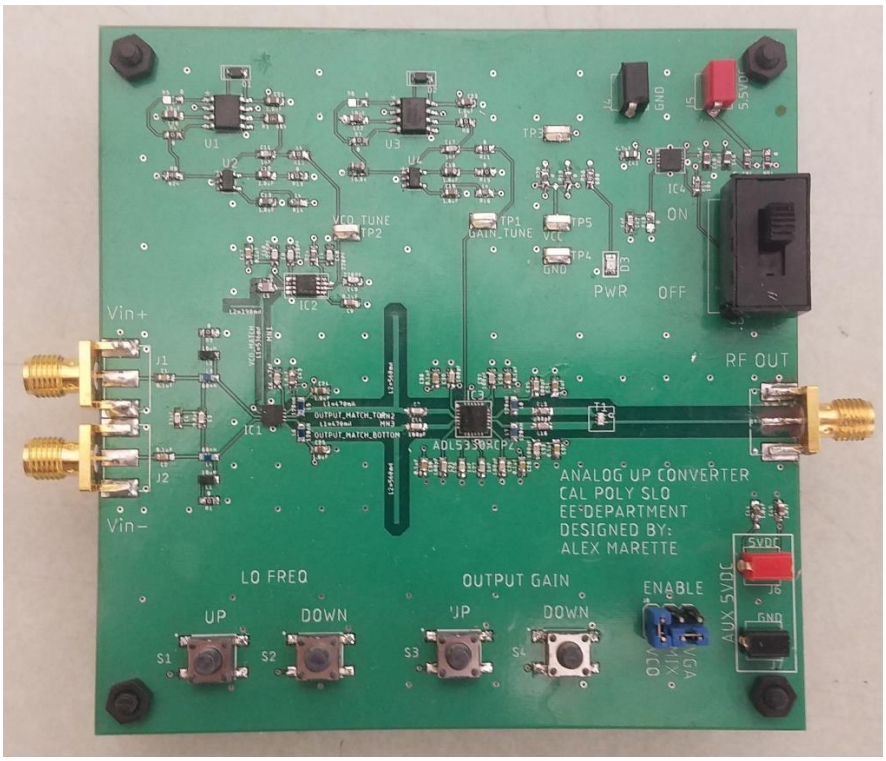


Figure 4-37: Completed Analog Upconverter Device

Lastly, the Analog Upconverter board current draw was measured. Two parallel 0.1 Ohm resistors replaced the parallel no load resistors for current sensing. The voltage across the resistors was measured for each of the following conditions:

- Power on with all enable headers off (only the tuning circuits)
- VCO enable header added
- Mixer enable header added
- VGA enable header added with the tune voltage set for minimum gain
- VGA tune voltage set for maximum gain
- Added on external amplifier
- Added a second external amplifier

By using a current sense resistor, much more accurate current readings can be made when compared to simply using the power supply output current reading. Figure 4-38 shows the total current draw as each new component is enabled. The current draw for just the board is under 250 mA as expected. This leaves plenty of extra current capacity for the use of external inline amplifiers to compensate for the board's poor RF performance.

Case	Sense Voltage (mV)	Board Current (mA)	Board Power (mW)	Resistor Power (mW)
All Headers Off	0	0	0	0
VCO Enabled	0.377	7.54	37.7	0.00284258
VCO & Mixer Enabled	0.98	19.6	98	0.019208
All Enabled w/ Min Gain	6.9	138	690	0.9522
All Enabled w/ Max Gain	12.22	244.4	1222	2.986568
One Extra Amp	19.14	382.8	1914	7.326792
Two Extra Amps	25.61	512.2	2561	13.117442

Figure 4-38: Analog Upconverter Current Draw

5 SYSTEN TESTING & CHARACTERIZATION

After building and characterizing each individual design, the two boards were integrated into the complete jamming device. The integrated jamming device can be seen in Figure 5-1. This device was characterized in a similar way as the Digital Synthesizer board by using a spectrum analyzer to measure the tone powers under different output conditions. This output was compared with the expected results which do not account for the poor performance of the RF Analog Upconverter board.

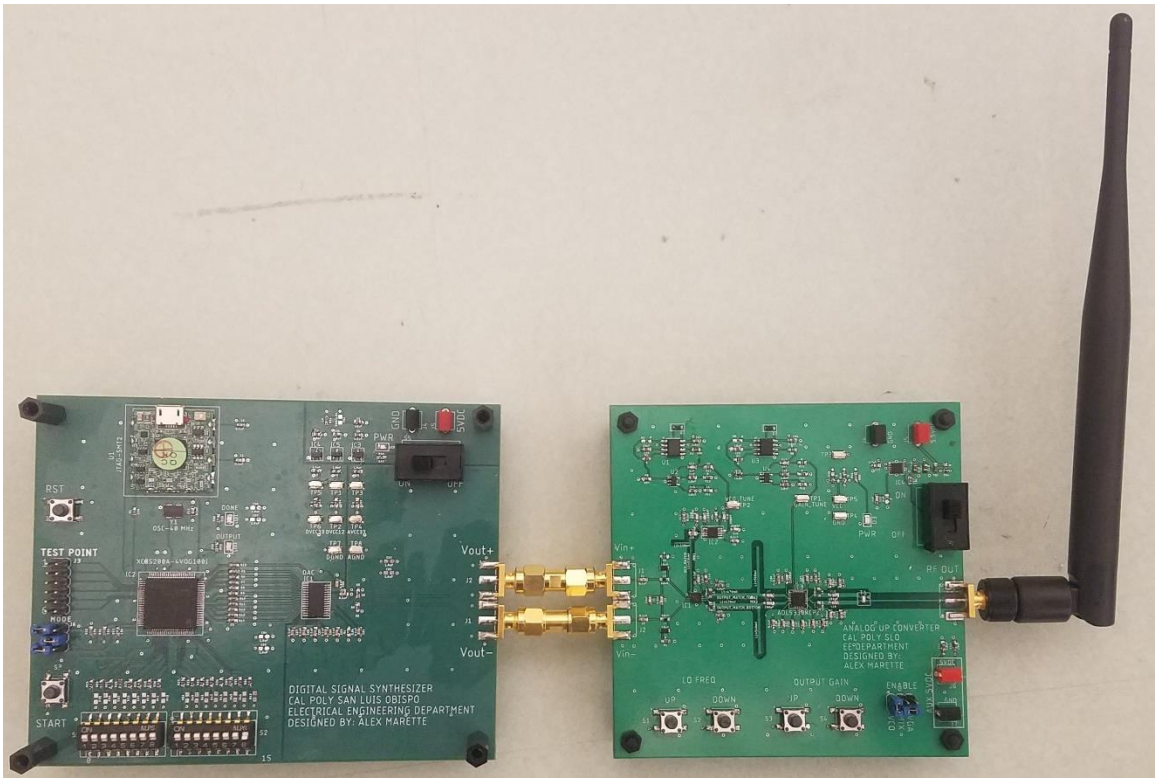


Figure 5-1: Integrated Jamming Device

The expected results were calculated by taking the measured Digital Synthesizer output power levels from Section 3.6 and applying the ADS simulated LPF matching network from Section 4.3 and then adding the 11 combined dB of gain expected from the mixer and VGA at maximum gain as seen in equation 5-1.

$$P_{out\,expected} = P_{out\,Synth} + G_{filter} + G_{mixer} + G_{VGA} \quad (5\text{-}1)$$

As with the Digital Synthesizer output measurements, the output characteristics were measured in two ways. First, by applying a single tone at all channel frequencies and second by increasing from one tones to 16 tones taking a measurement after each new tone added. The results from the test can be seen in Figure 5-2 and Figure 5-3 respectively. The results in the single tone power test show that the input matching network and lowpass filter did work as expected in smoothing out the sinc roll off. Despite being -25dB less than expected, the measured single tone response matches the curve of the expected frequency response. The multitone response also had a similar relationship to the expected response where the responses are very similar despite the large loss in the measured value.

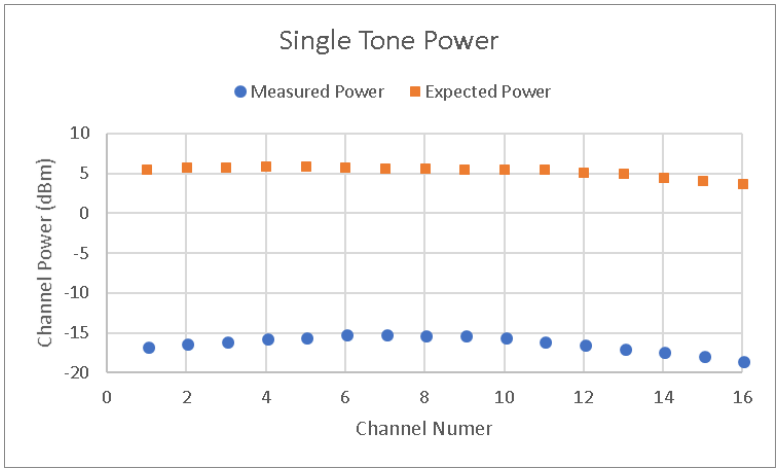


Figure 5-2: Single Tone Output Test for Complete Jammer

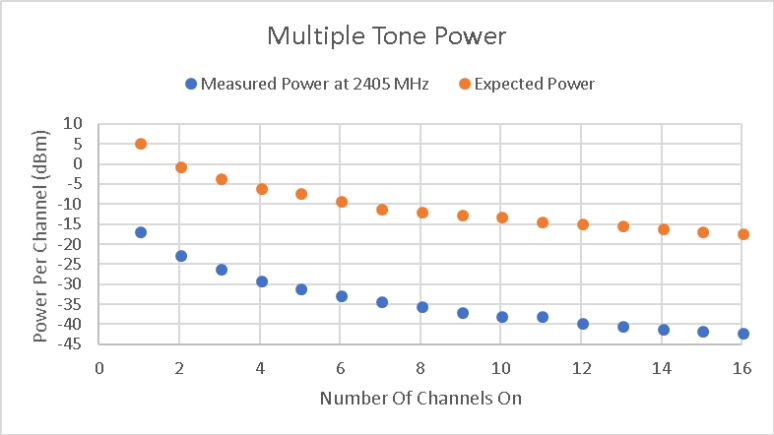


Figure 5-3: Multi Tone Output Power for Complete Jammer

Another problem noted when viewing the output signal on the spectrum analyzer was the high upper side band power which extended into the 2.5 GHz and up range. This a problem for two reasons. One is that when amplifying the signal, much of the power is wasted amplifying the unwanted signal resulting in poor efficiency. The other problem is that the unlicensed band used ranges from 2.4 GHz to 2.5 GHz. Figure 5-4 shows that a large amount of the signal power is located after the 2.5 GHz range. This causes the device to be less discreet and easy to detect since the power above 2.5 GHz will be easily stand out.

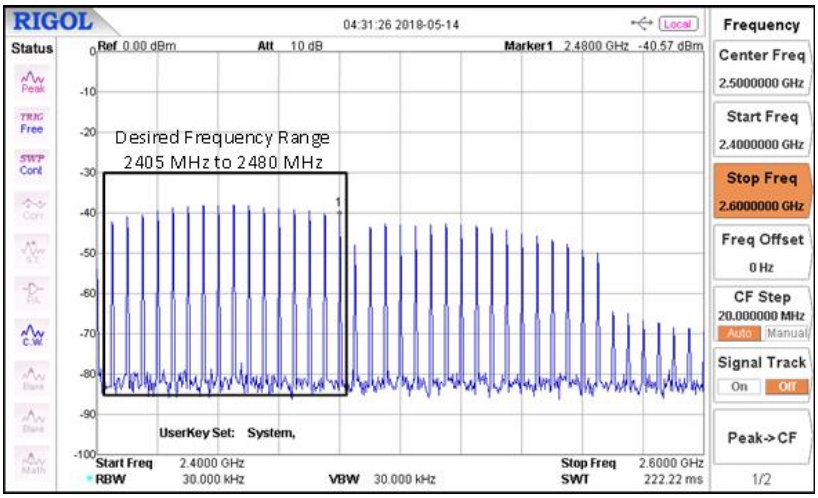


Figure 5-4: Spectrum Analyzer Capture of Jamming Signal

At -40 dBm per tone external inline amplifiers had to be used to increase the power to meet the requirements from Section 2.3. Two 10 dB AH1 amplifiers were used. Figure 5-5 shows the spectrum capture with the additional inline amplifiers. Equation 5-2 shows that the jamming power at the receiver is -65 dBm which is above the minimum threshold of -75 dBm.

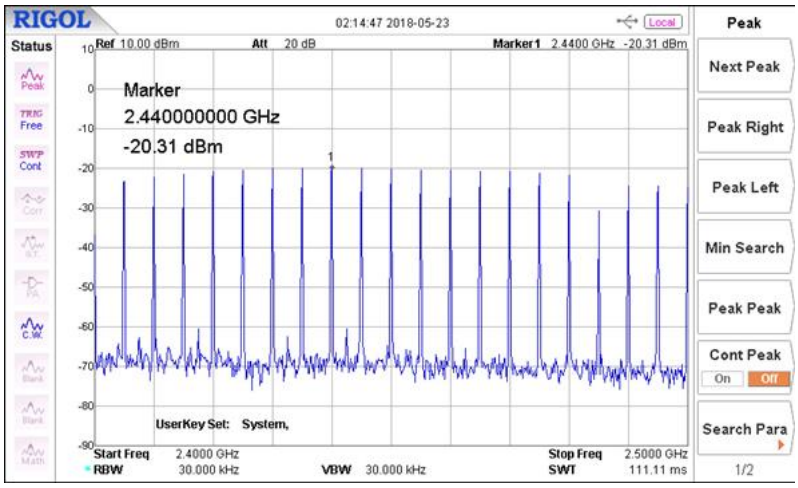


Figure 5-5: Spectrum Analyzer Capture with 20 dB Additional Gain

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2} = \frac{10^{-2.2} \times 10^{0.5} \times 10^{0.15} \left(\frac{2.998 \times 10^8}{2.4 \times 10^9}\right)^2}{(4\pi \times 3)^2} = -65.1 \text{ dBm} \qquad (5\text{-}2)$$

6 ZIGBEE NETWORK JAMMING

6.1 Overview

When testing a jammer, there are four typical metrics used [3]. The first metric is power efficiency which is more important for mobile or battery powered jammers. The second metric is probability of detection[3]. Low probability of detection is required for networks which employ jamming defense methods. The third metrics is the ability to completely disrupt communications also known as denial of service (DoS) which is the overall goal of a jammer. The last metric is the strength against PHY techniques such as the direct sequence spread spectrum used in 802.15.4 [3]. Testing for these metrics proved to be challenging due to hardware limitations, environmental interferences, inconsistencies in results, and unclear jamming attacks.

6.2 Testing Challenges

Digi Xbee ZigBee radios were used to test the jamming device. The radios can be connected to microprocessors for configuration and custom network setup but for quick and simple radio configuration the Xbee Configuration and Test Utility (XCTU) can be used. The main challenges with testing the jammer came from the limited abilities of the XCTU. This software was used to configure the radios as the coordinator, router, or end device, adjust output power, limit the channel scan range, change the channel scan time, and more. It was also used to establish a serial communication link between two computers by automatically translating typed ASCII characters into proper ZigBee packets. This software had useful tools such as a radio spectrum analyzer display and a throughout measurement tool, but it did not have a tool to measure the packet delivery ratio (PDR) or the packet send ratio (PSR). These two measurements are crucial for measuring the third metric, the DoS. Equations 6-1 and 6-2 show how the two ratios are calculated [3].

$$PSR = \frac{Packets\ Sent}{Packets\ Intended\ to\ be\ Sent} \tag{6-1}$$

$$PDR = \frac{Packets\ with\ no\ Errors}{Total\ Received\ Packets} \tag{6-2}$$

The XCTU only supplies information on packets intended to be sent and packets received with no error. By assuming all packets in the wireless medium are received, the XTCU quality metric can be shown to be the product of the PDR and PSR. See Equation 6-3.

$$XCTU\ Ratio = \frac{Packets\ Received\ with\ no\ Error}{Packets\ Intened\ to\ be\ Sent} = PSR \times PDR \tag{6-3}$$

The information from the XCTU helps show whether a signal was jammed and to some extent how well the signal was jammed but it does not show in which way the signal is jammed. Recall that the planned attack is on the MAC layer of 802.15.4 consisting of denying channel access by placing power in all channels. This is also considered an attack on the transmitter. However, the constant on design of the jammer creates an attack on the PHY layer by raising the noise floor and therefore increasing the probability of corrupting a symbol. This is considered an attack on the receiver. By using the PDR and PSR one can distinguish the type of attack. Under a perfect and ideal transmission and jamming conditions, Figure 1-1 the expected PSR and PDR measurements from a MAC and PHY layer attack. Without these measurements no definitive decision could be made on the type of jamming that occurred.

Attack Type	PDR	PSR
PHY	0	1
MAC	N/A	0

Figure 6-1: Ideal PSR and PDR Measurements for PHY and MAC Attacks

Another challenge when testing the effects of the jammer was the environment. The 2.4 GHz band is packed with many signals such as those from WIFI and Bluetooth. This causes issues when distinguishing the effects of the jammer from the effects of another 2.4 GHz device which may be operating in a nearby channel. Unfortunately, the tools required such as computers,

spectrum analyzers, and power supplies required this test be conducted in a lab. Additionally, there was no access to a faraday cage large enough to for the physical radio layout during the test. This environmental issue caused many inconsistencies when testing and therefore many tests were conducted multiple times on different ZigBee channels to help verify the results. Lastly, this jammer is meant to design ZigBee in a real-world environment and therefore the inability to run test in a clean environment may be a better description of the jammer's abilities.

6.3 Testing

During the testing of the ZigBee radios and the jammer, a general physical test layout was used. Figure 6-2 shows the layout. Depending on the type of test being conducted, Radio 1 and Radio 2 could be either the Coordinator or the Router. Under most tests, distance B was always roughly 15 feet, while distance A ranged from 10' down to 6".

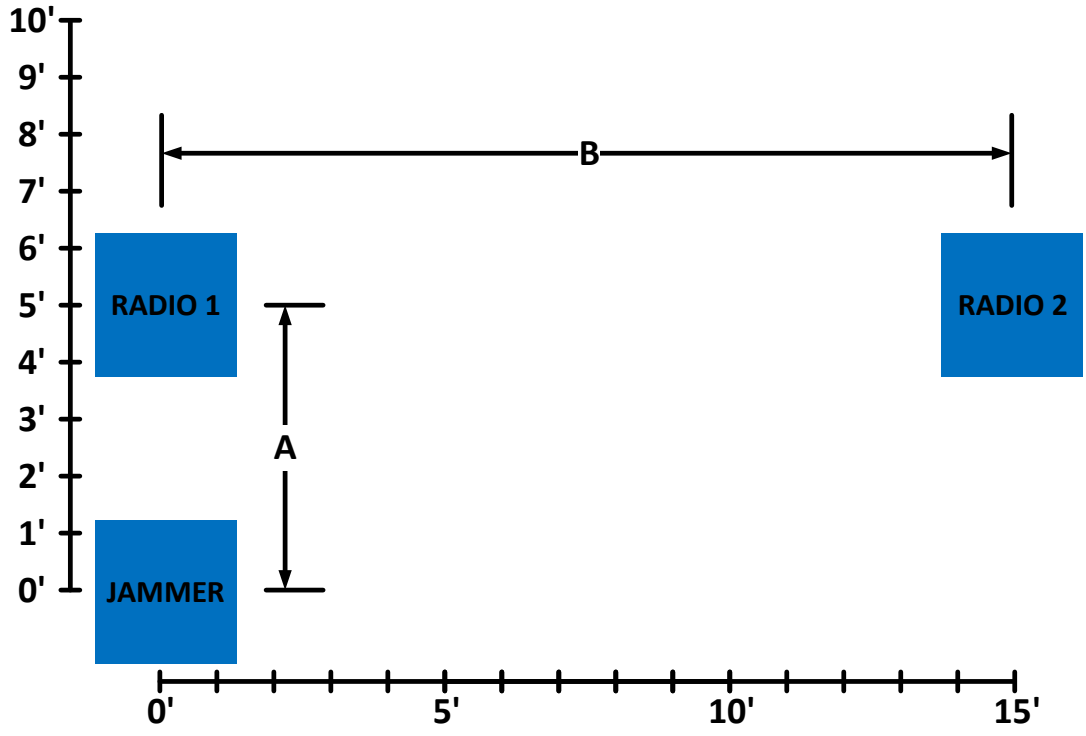


Figure 6-2: Physical Test Layout for ZigBee Jamming

The jammer consisted of the Digital Synthesizer integrated with the Analog Upconverter. Two additional 10 dBi AH1 were added to the output to increase the total jamming power. To monitor the jamming signal as well as radiate the jamming signal, a 10 dB coupler was used following the two amplifiers. Lastly, the antenna was connected to the 10 dB coupler. The complete jamming test device can be seen in Figure 6-3.

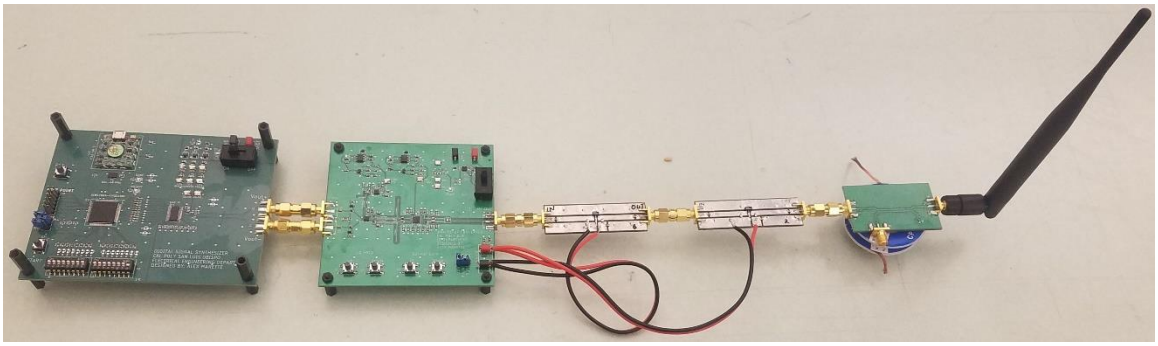


Figure 6-3: Jamming Device Test Setup

Without the PSR or PDR, other methods were devised to check the type of jamming that was occurring. This first test conducted was to attempt to prove proper MAC layer jamming by forcing the Coordinator to choose a specific channel. Upon the startup of a new network, the Coordinator will perform an ED channel scan through the selected channel in the channel list. If using CCA mode 1, the coordinator will decide an occupied channel if the peak power in the channel is larger than a set threshold as described in Section 2.1 [10]. To test for this operation, the Coordinator was set as Radio 1 with a distance A of 1 foot. No Radio 2 was used for the test. The jamming device was set to jam 15 of the 16 channels and then the Coordinator was reset to force it to perform a channel scan. The coordinator was expected to choose the only remaining channel that wasn't being jammed. This was not the case. It seemed as if the channel selection was in no way effected by the jammer. This possibly indicates that the Xbee Coordinator radio was using another mode of CCA in which the PHY also checks for similar modulation and spreading schemes. Nothing in the XTCU manual or Digi Xbee manual indicate CCA mode selection or identification [34], [35].

The previous test suggested that the jammer was not affecting the MAC layer as anticipated however the next test did suggest an unexpected type of MAC layer jamming. The next test was conducted by adding the Router as Radio 2 after the previous test. The jammer was set to output a single tone of -30 dBm at the current Coordinator channel. After both the jammer and the Coordinator were established, the Router was turned on. While the jamming signal was on, the router channel and PANId were read to be 0 and xFFFF respectively. This is an indication of an active channel scan set on by the MAC layer. Upon normal activation, the router will perform an active channel scan in which it requests a beacon transmission from all coordinators within range on all channels on the scan list. Following the scan, the Router will choose a channel with the desired Coordinator. During the test, this did not happen, and the router stays in the active scan mode indefinitely. Shortly after the jammer is disabled, the Router establishes a connection on the same channel as the Coordinator. See Figure 6-4 and Figure 6-5. This test was repeated 10 times with 100% consistency in the results.

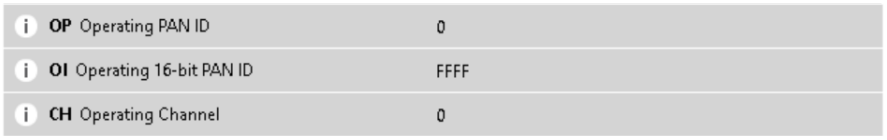


Figure 6-4: Router PANId and Channel During Attack

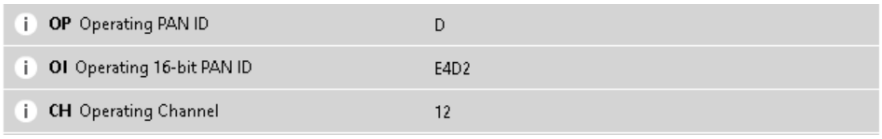


Figure 6-5: Router PANId and Channel After Attack

As stated before, with the current setup there is no way in knowing why or how the channel scan and beacon signals do not get through. It could be that the router is not sending any beacon request on that channel because it suspects the channel is in use from the jammer. It could also be that the jammer is degrading the beacon request signal within the medium. Both cases assume that the coordinator does not receive the beacon request from the router. Two other possibilities

can be explored where the Coordinator does receive the beacon request, but the Router does not receive the beacon itself. Again, this could be caused by the Coordinator not sending the beacon or because the beacon signal is degraded in the wireless medium. Regardless this is considered a MAC layer attack because the Router does not establish an official communication channel.

The next test conducted was an attack on an already established network. This test was conducted twice, once with the attack on the Coordinator (receiver) and once with the attack on the Router (transmitter). For the attack on the Coordinator, the Coordinator was placed as Radio 1 and the Router was placed as Radio 2. Distance A was set to 10 feet and distance B was set to 15 feet. This was conducted as a blind jamming attack assuming the transmission channel was unknown. Therefore, all tones (except for channel 16) were activated on the jammer at a maximum power of -23 dBm per tone. An attack was performed at 10 distances starting at A=10 feet down to A=1 foot. Each attack had up to four tests. The first test was a jammer off test in which a clean unjammed communication signal was sent and received. The next 3 tests were conducted with the jammer on. Figure 6-6 shows the results from this test.

Distance A (ft)	Distance B (ft)	Test 1 Unjammed Transmission	Test 2 Jammed Transmission	Test 3 Jammed Transmission	Test 4 Jammed Transmission
10	15	PASS	FAIL	FAIL	FAIL
9	15	PASS	PARTIAL	FAIL	FAIL
8	15	PASS	PASS	PARTIAL	PARTIAL
7	15	PASS	PARTIAL	PARTIAL	PARTIAL
6	15	PASS	PARTIAL	PARTIAL	PARTIAL
5	15	PASS	PASS	PARTIAL	PARTIAL
4	15	PASS	PASS	PARTIAL	PARTIAL
3	15	PASS	PASS	PASS	PASS
2	15	PASS	PASS	PASS	PASS
1	15	PASS	PASS	PASS	PASS

Figure 6-6: Attack on Coordinator Results

Note that for Test 1, a PASS indicates that the unjammed message from the Router successfully transmitted to the Coordinator and that the Coordinator successfully decoded the message. For tests 2,3 and 4, a PASS indicates that the signal was completely jammed meaning zero bytes of the message was received. A PARTIAL indicates that the signal was partially jammed where

some bytes were received but not all bytes. Lastly a FAIL indicates that all bytes of the message were received while he jammer was on.

Analysis of the results concluded that the successful jamming attacks were attacks on the PHY layer. With a MAC layer attack, one would expect none of the packages to be sent. The presents of partial reception events indicate that some of the message packets were corrupted by the jammer in the wireless medium and some were not.

The previous test was repeated after switching the locations of the radios. For testing the attack on the Router, the Router is places as Radio 1 and the Coordinator is placed as Radio 2. The same 4 tests are repeated the distance A changing from 10 feet down to 1 foot. Figure 6-7 shows the results of the jamming attack on the Router.

Distance A (ft)	Distance B (ft)	Test 1 Unjammed Transmission	Test 2 Jammed Transmission	Test 3 Jammed Transmission	Test 4 Jammed Transmission
10	15	PASS	FAIL	FAIL	FAIL
9	15	PASS	DELAYED	FAIL	DELAYED
8	15	PASS	DELAYED	PASS	FAIL
7	15	PASS	DELAYED	DELAYED	DELAYED
6	15	PASS	PASS	PASS	PASS
5	15	PASS	DELAYED	DELAYED	DELAYED
4	15	PASS	DELAYED	DELAYED	DELAYED
3	15	PASS	DELAYED	DELAYED	DELAYED
2	15	PASS	PASS	PASS	PASS
2	15	PASS	PASS	PASS	PASS
1	15	PASS	PASS	PASS	PASS
1	15	PASS	PASS	PASS	PASS

Figure 6-7: Attack on Router Results

As with the previous attack on the Coordinator, a PASS on test 1 indicates that while unjammed, the Router can send a message to the Coordinator. For tests 2, 3, and 4, a PASS indicates a complete successful attack in which the Coordinator receives no bytes from the Router message. A FAIL indicates that the Coordinator receives all bytes from the Router within 2 seconds of attempting to transmit. Note that instead of a PARTIAL field, there is a DELAY field. During the attack test on the router, no partial bytes were received. Either the entire message was received or none of the message was received. Instead a significant delay period was introduced during some

of the transmission attempts. To measure this, a stop watch was started after the first byte of the message was entered to be transmitted and stopped when the same first byte appeared at the receiver. Under normal unjammed conditions, this was almost instantaneous and therefore not measurable with the stop watch. When a delay occurred, it would take 1-5 seconds for the first byte to appear at the Coordinator. Note that after the first byte, the remaining portion of the message appear instantaneously.

At distance A equal to 6 feet, the message was consistently jammed but the message was consistently delayed at 5 feet. This is believed to be caused by an increase of 2.4 GHz RF power at that location. In other words, it is believed that this message jamming was caused, or partially caused, by the busy 2.4 GHz environment and not solely by the jamming device.

The different characteristics from the attack on the Router can lead to the deduction that this is a MAC layer attack. The biggest indicator of this is the lack of partially received messages as seen in the Coordinator attack. This means that either all packets sent from the Router were corrupted in the wireless medium or that no packets were transmitted at all. Noting that the Router transmission power is 8 dBm and the jamming signal is -23 dBm, it is unlikely that the packets were corrupted during transmission.

6.4 Additional Exploration

The previous tests conducted attempted to characterize the type of attack that was occurring. Additionally, the test conducted attempted to characterize the last two metrics of a jammer, DoS and the strength against the DSSS PHY technique. A small amount of additional exploration was conducted into the strength against attack defense metric and the efficiency metric. This additional exploration was also used to demonstrate the flexibility of the FPGA synthesizer.

Two common defenses against attacks is the channel surfing defense and the spatial retreat defense [3]. After detection of the attack, a Coordinator will choose to leave the channel into a new predetermined channel. The Coordinator will then send a beacon on the new channel inviting

the other devices onto the same channel. This defense would not work against this jammer as under normal conditions, the jammer will transmit a tone at all channels. If the network is using a spatial retreat defense, the jammed radios with move away from the jammer until the attack is no longer affective. This defense would be affective against the jammer.

Another defense technique is the implementation of a digital filter [36]. The ZigBee bandwidth for one channel is 2 MHz while the bandwidth of a jamming tone is typically less than 100 kHz. Figure 6-8 shows the single tone bandwidth of the jammer over a 2 MHz span. By implementing a digital notch filter, the single tone can be removed from the signal before the chip to symbol conversion. This is a defense against a PHY layer attack. It is an effective defense although it also degrades the signal and therefore should be used dynamically only when an attack is sense.

To counter this defense, a jamming signal with a wider bandwidth is required. This was attempted by using a triangle wave instead of a sine wave. The frequency response of a sine wave is a single delta function while the frequency response of a triangle function is a sinc squared function. With the wider frequency response of the triangle wave, the digital filter would not be able to completely remove the jamming signal. In Figure 6-9 the bandwidth of the triangle wave shown to only be 6 kHz wider than that of the single tone.

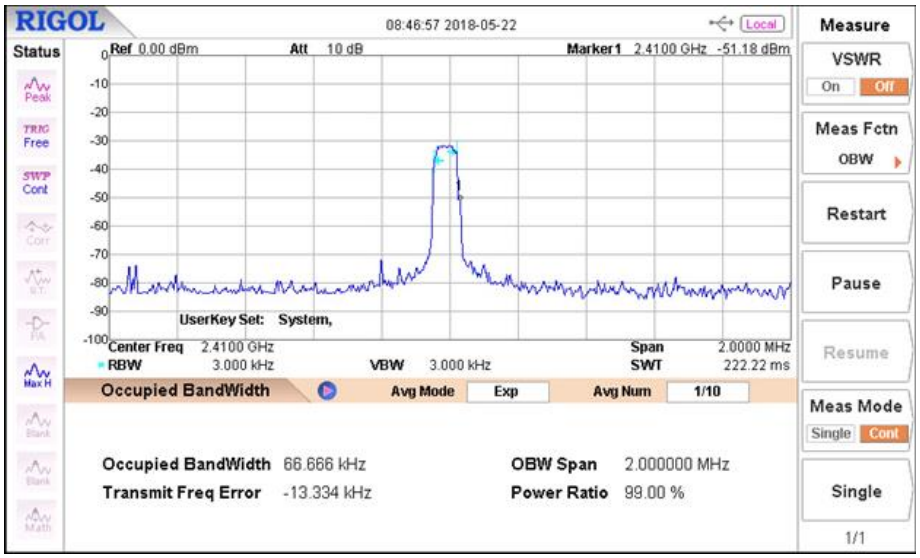


Figure 6-8: Single Sine Tone Bandwidth over a 2 MHz Span

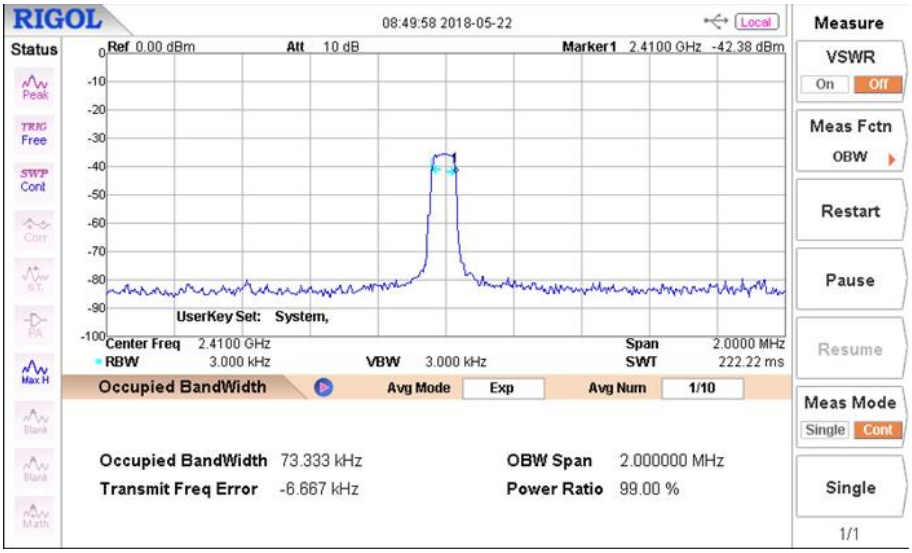


Figure 6-9:Single Tone Triangle Wave Bandwidth over a 2 MHz Span

Using the triangle wave did not increase of bandwidth of the jamming signal to the degree that was expected. However, this shows the flexibility of the FPGA controlled jammer and the ease of making changes to it. Within the FPGA some digital modulation could be performed to further widen the bandwidth of the jamming signal and therefore counter the filter defense.

Efficiency and ease of detection are two important parameters to considers when designing a jammer. If the jammer is to be a mobile jammer or a battery power jammer, power efficiency is a large focus on the design. Without a constant source or endless power, a battery powered jammer must implement new methods to increase efficiency. Previously, defense against jamming attacks were described. A counter against a defense is not needed if the attack is hard to detect. Many jammers attempt to reduce the ease of detection by using smart and dynamic jammers which listen for packets and then intercept them [3]. This method is very effective, but it is costly and complex.

Periodic jamming is an easy and effective jamming method which help reduce the ease of detection and increase the efficiency. Detection is often implemented by creating a ratio of the RSS (Received Signal Strength) and the PDR. A large RSS and a low PDR would indicate the possibility of a jamming attack [37]. Periodic jamming switches on and off the jamming signal at

a predetermined period and duty cycle. This reduces the overall power consumed and reduces the average RF power transmitted into the wireless medium, effectively lowering the RSS.

Note that this technique only works as a PHY attack and not a MAC attack. This attack works by degrading one symbols worth of chips. If all chips in one symbol are jammed, the probability of a successful chip to symbol conversion is low. IEEE 802.15.4 requires all symbols in a packet to be received or the packet is discarded [36]. Therefore, by creating a periodic jamming signal in which the period is the length of one packet and the on time is at least 2 times the symbol length, then the transmission will be successfully jammed. See Figure 6-10.

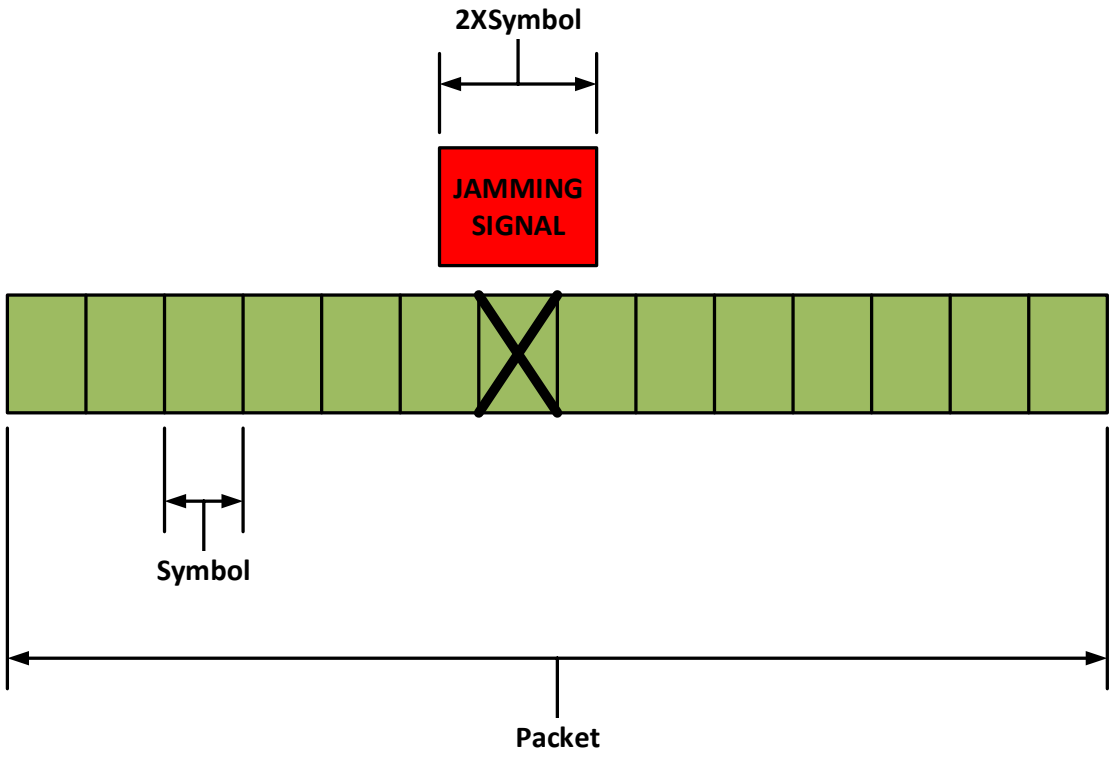


Figure 6-10: Periodic Jamming Representation

With a symbol rate of 62.5 kSymbols per second, the jammer time on was calculated to be 32 us. See Equation 6-4. A counter block was added to the FPGA in which a signal, JAM, was set high and low depending on the value of the counter. Equations 6-5 and 6-6 show how the counter values were selected. The output of the block multiplexed the DAC_CLK output between the 210

MHz clock and 0. The JAM output was also routed out of the FPGA onto a test pin to confirm the T_{jam} and the duty cycle. This output was also used on the ENABLE pins on the VGA and mixer further increase efficiency.

$$T_{jam} = 2T_{Symbol} = \frac{2}{62.5\frac{kSym}{s}} = 32\mu s \tag{6-4}$$

$$Cycles_{jam} = T_{jam} \times CLK_{FPGA} = 32\mu s \times 5MHz = 160\ Cycles \tag{6-5}$$

$$Cycles_{off} = \left(\frac{Cycles_{jam}}{DutyCycle}\right)100 - Cycles_{jam} \tag{6-6}$$

Two tests were performed with the periodic jamming, an attack on the Coordinator and an attack on the Router. The device attacked was placed as Radio 1 and the other device was placed as Radio 2. The distances were held constant at A=1 foot and B=15 feet. The duty cycle was changed from 50% down to 1%. The jammer was set to jam all channels at a maximum power of -23 dBm. The jamming results along with current measurements can be seen in Figure 6-11

Duty Cycle (%)	Output Off Current Draw (mA)	Output On current Draw (mA)	Attack on Coordinator	Attack on Router
100	700	760	PASS	PASS
50	580	640	PASS	FAIL
40	560	610	PASS	FAIL
30	530	580	PASS	FAIL
20	500	560	PASS	FAIL
15	480	540	PASS	FAIL
10	470	530	PASS	FAIL
5	460	520	PASS	FAIL
1	450	510	FAIL	FAIL

Figure 6-11: Periodic Jamming Results

On the period jamming results, a PASS indicates a complete successful attack in which no information was received. A FAIL indicates all other outcomes including full message reception, partial messaged reception, and delayed message reception. The result from this test show an impressive ability to jam the Coordinator (receiver) even at a 5% duty cycle. The Router (transmitter) showed no affect from the periodic attack except for a delayed transmission at 50% duty cycle. This again helps to reinforce the idea that the jamming device is attacking the PHY

layer when attacking the Coordinator and that it is attacking the MAC layer when attacking the router.

Successful jamming occurred down to 5% duty cycle. The total average jamming power in the wireless medium would then be 5% of the constant on power. This indicates that the RSS measurement could decrease by as much as a factor of 20, greatly reducing the chance of detection. As shown by Figure 6-12 at 5% duty cycle the total jammer power reduced by 32%. The greatest power reduction came from the ability to switch the VGA on and off as well as the digital circuit. The external amplifiers had no enable pin and therefore were not able to be switched on and off periodically. If enable control on the external amplifiers was a possibility the power reduction would further increase. Figure 6-12 also shows the power reduction when ignoring the power from the external amplifiers. This case shows a power reduction of 50%.

Condition	Duty Cycle (%)	Jammer Current (mA)	Jammer Power (W)	Power Reduced (%)
Including External Amps	100	760	4.18	32.89
Including External Amps	5	510	2.81	
Excluding External Amps	100	492.2	2.71	50.79
Excluding External Amps	5	242.2	1.33	

Figure 6-12: Power Reduction from Periodic Jamming

The two additional explorations in ZigBee jamming were possible due to the flexibility of the Digital Synthesizer board. This board could be paired with a mixer at any frequency to produce many different RF signals that could be used for jamming, spoofing, or even testing of other systems.

7 CONCLUSION

7.1 Reflection

The goal of this thesis project was to design, build, and test a jammer for attacking the IEEE 802.15.4 standard and the staked ZigBee protocol. By taking advantage of the carrier sense multiple access, it was believed that a MAC layer attack would prevent any device from gaining access to a channel. The attack came from a multi-tone signal in which each tone was the center of the 2.4 GHz IEEE 802.15.4 channels. To create the jamming device, two boards were design. The first board was the Digital Synthesizer board and the second was the Analog Upconverter board.

Each board design came with new challenges. The Digital Synthesizer board was a mixed signal design requiring extra steps and precautions to keep the two components separated. This included split power and ground planes and careful component placement. Implementing the FPGA on a custom board required careful design work insuring all components would integrate properly with the FPGA. The FPGA digital design required many hours of simulation to insure the tight timing requirements were met. The Analog Upconverter had unique challenges as it did not have a digital component but instead a high frequency component. At 2.4 GHz new consideration had to be considered. Most of the work went into the matching network designs which matched the 3 mixer outputs to the correct characteristic impedance. AC coupling capacitors and RFC inductors had to be carefully selected as to keep the component self-resonance above the design 2.4 GHz. The Digital Synthesizer board was tested to work as designed while the Analog Upconverter showed to have an output power roughly 27 dB less than expected. Two 10 dB inline amplifiers were used to increase the output power so that the test could continue.

The jamming device successfully attack the ZigBee radios consistently while being within 2 feet of the router or 3 feet of the Coordinator. While attacking the Coordinator, incomplete message reception indicated a PHY layer attack and while attacking the Router, all or nothing message

reception along with message delays indicated a MAC layer attack. Upon network startup, the Coordinator was not affected by the jammer and the channel choice was not influenced by the jammer as expected. Upon startup, the router was unable to join a channel while being jammed most likely due to incomplete beacon processes. Modifications were made to the FPGA design to allow for additional jamming exploration. By switching the output from a sinewave to a triangle wave, it was believed that the bandwidth of the tone would increase significantly. This would reduce the effect of a jamming defense in which the jamming tone is filtered out. The bandwidth of the triangle tone was wider, but the change was not significant enough to counter the filter defense. The FPGA was further modified to allow for periodic jamming. This helped reduce power consumption and ease of detection while successfully jamming the ZigBee Coordinator down to 5% duty cycle. This test also helps reinforce that an attack against the Coordinator (receiver) was a PHY layer attack while an attack against the Router (transmitter) was a MAC layer attack.

7.2 Future Works

If time permitted, further work into three sections would continue. A new board design would be performed. More time would be taken to analyses the issues in the Analog Upconverter board and a new board would be designed. The matching networks would be built separately and individually tested and tunes before implementing them on the integrated design. A more compact all in one design would be considered where the entire jamming device would fit a 4 in by 4 in PCB. Lastly, the LO mixer input would have an optional input SMA connecter to allow for other mixing frequencies, further increasing the designs flexibility.

Further exploration into ZigBee jamming would continue. This exploration would emphasize FPGA modification. The goal would be to convert the constant on jammer into a deceptive jammer in which real packets of information fill up all channels. This MAC attack would help

against the mode 2 CCA and further reduce the ease of detection. the flexibility of the FPGA should allow for adding modulation schemes into the transmitted output.

Lastly, the Digital Synthesizer could be pair with a 1500 MHz mixer to attempt GPS spoofing. GPS spoofing is the attempt to deceive a GPS receiver by broadcasting false GPS information. The GPS information could be encoded into a signal using the FPGA and then upconverted using a new mixing design.

The overall outcome of this project was successful. The ZigBee radios were jammed using both PHY and MAC layer attacks. Ultimately the most important outcome of this project is the Digital Synthesizer board as it can be implemented for many RF broadcasting tasks. It is expected that both designs be used for future student projects, proof of concepts, and educational demonstrations in the wireless communication field.

8 REFERENCES

[1] S. Ray, J. Park, and S. Bhunia, “Wearables, Implants, and Internet of Things: The Technology Needs in the Evolving Landscape,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 123–128, 2016.

[2] International Electrotechnical Commission *et al.*, “Internet of Things: Wireless Sensor Networks,” *Int. Electron. Commision*, no. December, pp. 1–78, 2014.

[3] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of Service Attacks in Wireless Networks: The Case of Jammers,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[4] T. Zillner, “ZigBee Exploited - The Good, the Bad and the Ugly,” *Black Hat*, vol. 16, no. 2, p. 6, 2015.

[5] NXP Laboratories UK, “Co-existence of IEEE802.15.4 at 2.4GHz application note,” no. November, p. 28, 2013.

[6] J. T. Adams, “An Introduction to IEEE STD 802.15.4,” *2006 IEEE Aerosp. Conf.*, pp. 1–8, 2006.

[7] M.-S. Pan and Y.-C. Tseng, “ZigBee Wireless Sensor Networks and Their Applications,” *Sens. Networks Config. Fundam. Stand. Platforms, Appl.*, pp. 349–368, 2007.

[8] K. D. Jha, M. Srivastava, and Y. V. Varshney, “A Comparitive analysis of Wireless Sensor Network With Zigbee Transciever,” pp. 3–5.

[9] C. Neuhaeusler, “Generation of IEEE 802.15.4 Signals.”

[10] I. Howitt and G. Jore A., *IEEE 802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, vol. 2011, no. September. 2011.

[11] V. Associates and B. Division, “Step-recovery-diode frequency multiplier,” no. 2, pp. 2–3.

[12] T. Doluca, D. Dwelley, V. Jain, and L. Owen, “Maxim Integrated,” 2018.

[13] S. T. Antenna, “Delta 6B Delta 6B,” vol. 44, no. 8405712, pp. 5–7, 2008.

[14] “Artix-7 FPGA Family.” [Online]. Available: https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html. [Accessed: 18-Apr-2018].

[15] Xilinx, “Spartan-3A FPGA Family,” *Xilinx*, pp. 1–132, 2010.

[16] Texas Instruments, “DAC31x1 Single-Channel, 14-,12-, and 10-Bit, 500-MSPS, Digital-to-Analog Converters.” 2018.

[17] Analog Devices, “10-Bit, 210 MSPS TxDAC® D/A Converter AD9740.” 2005.

[18] SiTime, “SiT5001 1-80 MHz MEMS TCXO and VCTCXO,” vol. 94085, no. 408, 2015.

[19] UG332, “Spartan-3 Generation Configuration,” *Xilinx User Guid.*, vol. 332, 2015.

[20] Digilent, “JTAG-SMT2 ™ Programming Module for Xilinx ® FPGAs,” pp. 1–12, 2017.

[21] H. Johnson and M. Graham, “High-speed digital design: a handbook of black magic,” *Aerospace Conference, 1999. Proceedings. 1999 …*. p. 446, 1993.

[22] Yuden Taiyo, “Notice for TAIYO YUDEN products CHIP BEAD INDUCTORS FOR POWER LINES (FB SERIES M TYPE),” no. October, 2016.

[23] K. J. Wood, “Saturn PCB Design, Inc. - PCB Toolkit.” 2018.

[24] Analog Devices, “Decoupling Techniques,” *Appl. Note, Analog Devices*, pp. 1–14, 2009.

[25] Linear Technology, “LT5560 Datasheet.” pp. 1–28, 2006.

[26] Analog Devices, “ADL5330 10 MHz to 3 GHz VGA with 60 dB Gain Control Range.” 2005.

[27] Maxim Integrated, “2.4GHz Monolithic Voltage-Controlled Oscillators,” pp. 1–7, 2017.

[28] Linear Technology, “LT6650 - Micropower, 400mV Reference with Rail-to-Rail Buffer Amplifier in SOT-23.” pp. 1–12.

[29] Maxim Integrated, “DS1809,” pp. 1–10.

[30] Murata, “LDB182G4505C-110,” pp. 1–3, 2018.

[31] S. Hageman, “Via spacing on high-performance PCBs,” pp. 6–10, 2013.

[32] Altium, “Pros and Cons of Different High Frequency Transmission Line Types | Blog | CircuitStudio.” [Online]. Available: https://resources.altium.com/pcb-design-blog/pros-

and-cons-of-different-high-frequency-transmission-line-types. [Accessed: 10-May-2018].

[33] Johnson Technology, “Soldering Profiles and Guidelines for SMT Ceramic Components.” [Online]. Available: https://www.johansontechnology.com/soldering-profiles-and-guidelines-for-smt-ceramic-components.html. [Accessed: 11-May-2018].

[34] DIGI, *XCTU Configuration and Test Utility Software User Guide*. 2016.

[35] DIGI, “ZigBee RF Modules User Guide,” p. 106, 2014.

[36] B. Debruhl and P. Tague, “Digital Filter Design for Jamming Mitigation in,” vol. 23, 2011.

[37] B. Debruhl and P. Tague, “How to jam without getting caught: Analysis and empirical study of stealthy periodic jamming,” *2013 IEEE Int. Conf. Sensing, Commun. Networking, SECON 2013*, pp. 496–504, 2013.

9 APPENDICES

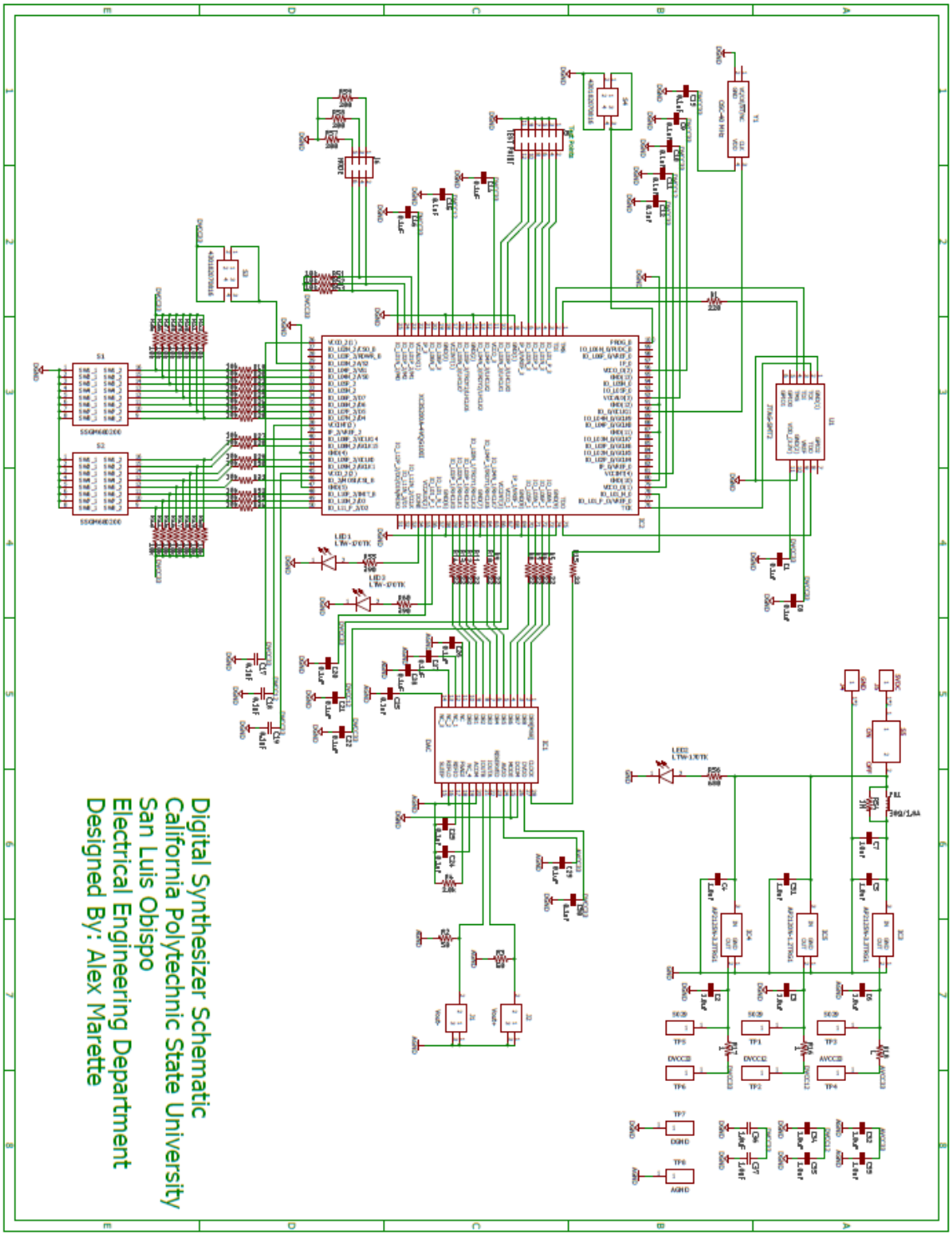
APPENDIX A MATLAB Scripts

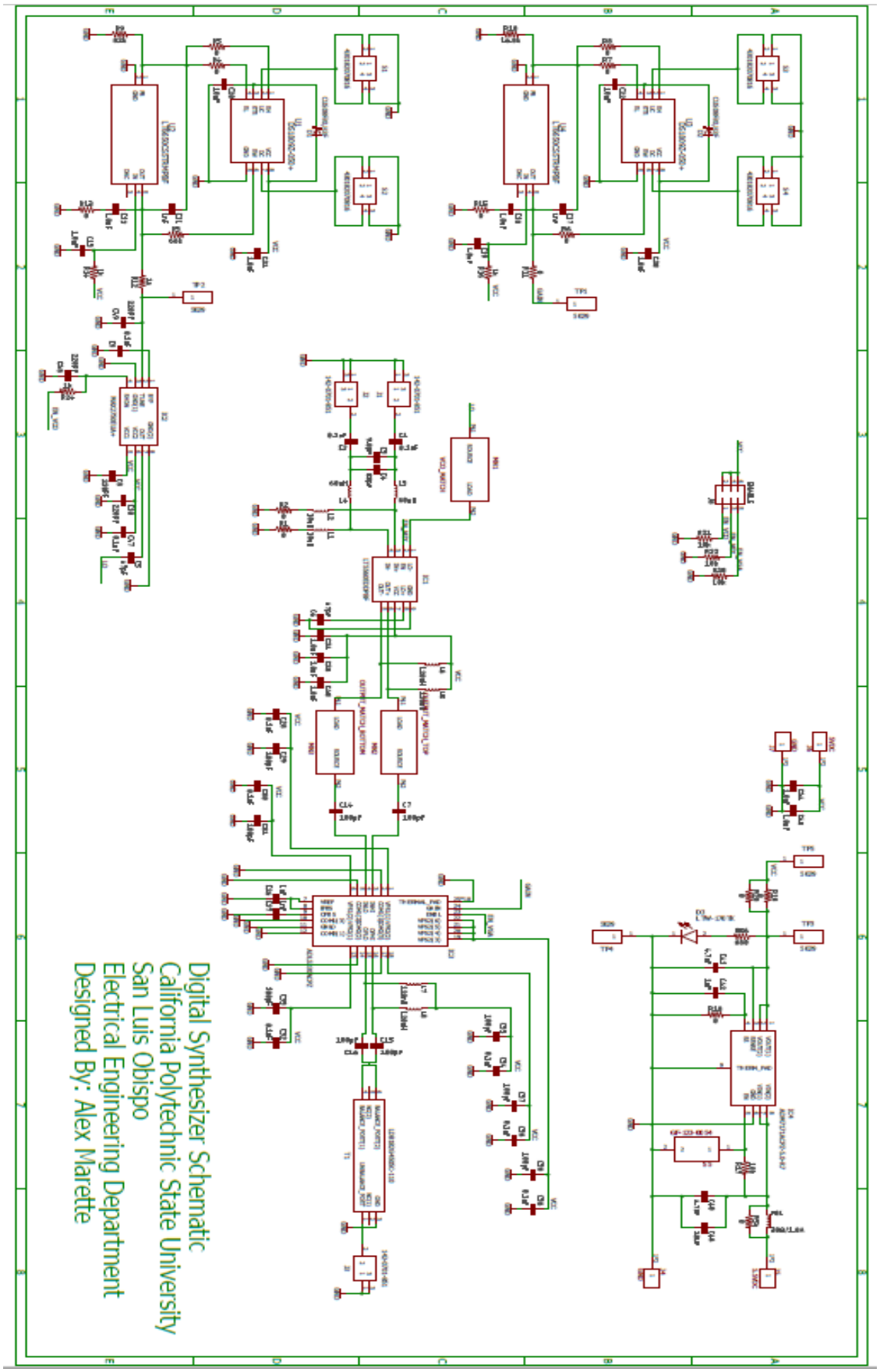
```
%This MATLAB script takes inputs: Fs, Frequencies, and bits and returns
%text files for each of the desired frequencies. The text files contain
%the discrete sine waves for the frequencies with the desired sampling
%rate and bit width. All the files contain the same number of samples which
%is the number of samples required to create one full period of the lowest
%frequency desired

%Digital Tone Creation at Specified Sampling Rate
Fs=210e6;                    %sampling rate
frequency=1e6.*(5:5:80);     %desired frequencies
bits=10;                     %bit width
words=Fs/frequency(1);       %number of samples
N=(0:words-1)./Fs;           %time array
%initialize output
data=zeros(length(frequency),words);

%loop for each of the desired frequencies
for  i=1:length(frequency)
    %create the time domain sine arrays
    data(i,:)=round(((2^bits)-1).*(0.5+0.5.*sin(2.*pi.*frequency(i).*N)));

    %Create and write the data to a text file
    file=cellstr(dec2bin(data(i,:)',10));
    fid = fopen( ['Channel_' num2str(i) '.txt'], 'wt' );
    fprintf(fid,'(');
    fprintf(fid, ' "%s",',file{:});
    fprintf(fid,');');
    fclose(fid);

    %Create and write the data to a coe file
    fid = fopen( ['Channel_' num2str(i) '.coe'], 'wt' );

fprintf(fid,'memory_initialization_radix=16;\nmemory_initialization_vector=');
    for word = 1:words-1
        fprintf( fid, '%x,',data(i,word));
    end
    fprintf(fid,'%x;',data(i,words));
    fclose(fid);

    %plot the data
    subplot(4,4,i),plot(N,data(i,:)),title(['Channel ' num2str(i)])
end
```

```
%This MATLAB script takes the output from the FPGA simulation
%and plots it in both the frequency and time domain. It also
%takes the output and converts it into a sample and hold output
%and then oversamples the time domain to get an accurate
%true output estimation.

%Outputs from iSim FPGA Simulation
%all switches on
Output_1 =[512,891,593,550,612,509,567,539,517,556,507,536,528,507,539,...
           505,521,523,500,529,502,511,520,493,522,499,501,517,483,515,...
           494,487,515,466,505,483,455,513,410,472,429,131];
%sw 1 and 13 off
Output_2 =[512,906,619,555,569,495,575,479,478,562,450,482,531,467,479,...
           504,508,468,498,546,461,511,561,476,524,554,514,518,524,555,...
           491,540,573,460,544,543,447,527,453,467,403,116];
%sw 5, 9,  and 15 off
Output_3 =[512,883,594,542,643,552,549,579,599,528,456,491,494,587,579,...
           473,567,534,480,515,404,511,618,507,542,488,455,549,443,435,...
           528,531,566,494,423,443,473,470,379,480,428,139];

%frequency and time arrays)
freq=(0:1/42*210e6:210e6-(210e6)/42);
time=(0:1/210e6:41/210e6);


figure (1)
%plot time domain
subplot(211)
plot(time,Output_1)
hold on
plot(time,Output_2)
plot(time,Output_3)
hold off
ylabel('10 bit Digital Output')
xlabel('Time (s)')
legend('All Switches On','SWs 1 & 13 Off','SWs 5, 9, & 15 Off')

%plot frequency domain
subplot (234)
spec=abs(fft(Output_1));
stem(freq,spec)
axis([0 100e6 0 5e3])
title('All Switches On')
xlabel('Freq (Hz)')
ylabel('Magnitude')
subplot (235)
spec=abs(fft(Output_2));
stem(freq,spec)
axis([0 100e6 0 5e3])
title('SWs 1 & 13 Off')
xlabel('Freq (Hz)')
ylabel('Magnitude')
subplot (236)
spec=abs(fft(Output_3));
stem(freq,spec)
axis([0 100e6 0 5e3])
title('SWs 5, 9, & 15 Off')
xlabel('Freq (Hz)')
ylabel('Magnitude')
```

```
figure (2)
%upsample
ups = 5;
frequ=(0:1/42*(210e6):(ups*210e6)-(210e6)/42);
timeu=(0:1/(ups*(210e6)):(41/210e6)+(ups-1)/(ups*210e6));
y = upsample(Output_1,ups);
h = ones(ups,1);
z = filter(h,1,y);

%plot time domain
subplot(211)
stem(timeu,z,'--x')
hold on
stairs(time,Output_1)
hold off
ylabel('10 bit Digital Output')
xlabel('Time (s)')
subplot(212)

%plot frequency domain
z = ((2.*z.*0.020./1023./sqrt(2)).^2).*50;
stem(frequ,10*log10(abs(fft(z))),'BaseValue',-35)
title('Estimated DAC Output Spectrum')
xlabel('Freq (Hz)')
ylabel('Log Magnitude')
axis([0 500e6 -30 0])



%function created to make a triangle function with the same parameters
%as the MATLAB sine function

function y = tri(t)
y = abs(mod((t+pi)/pi, 2)-1);
end
```

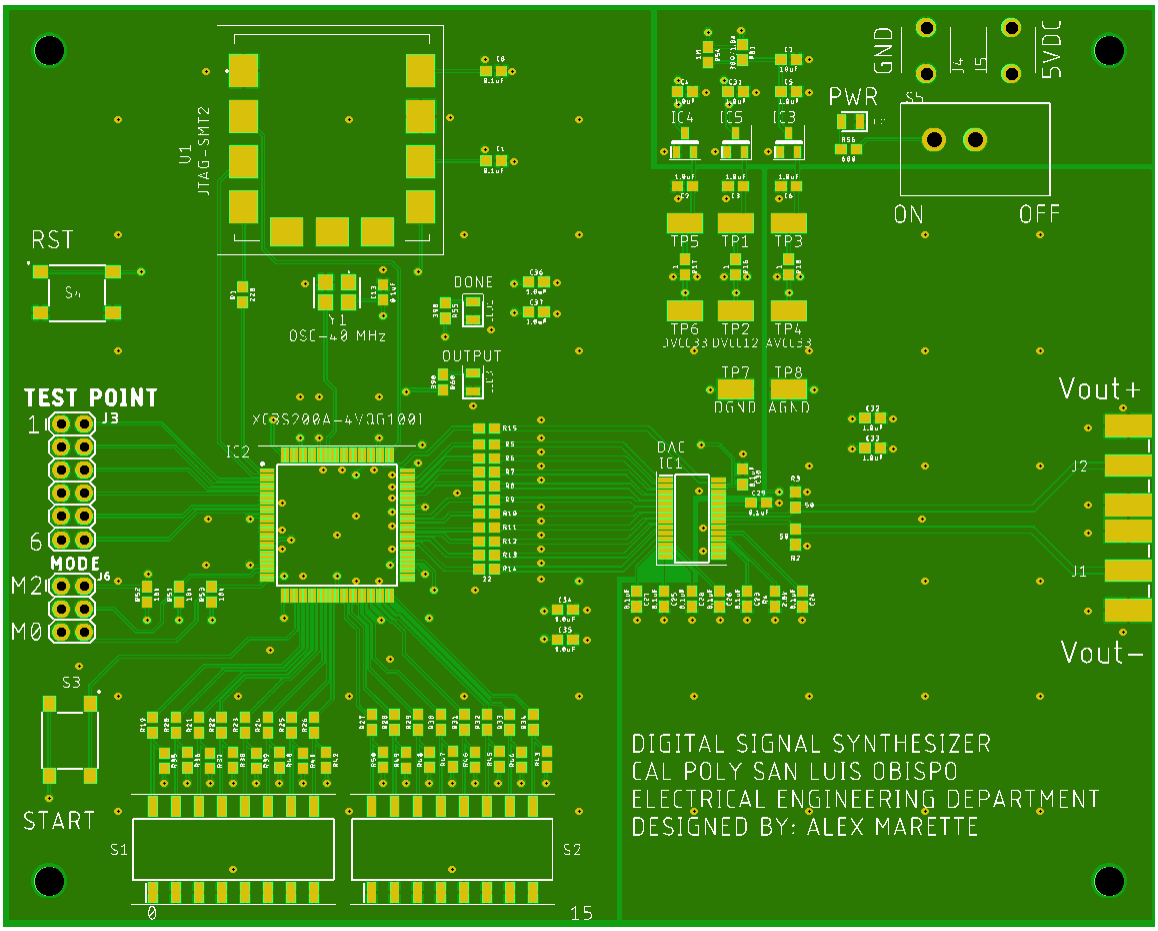
APPENDIX B Schematics



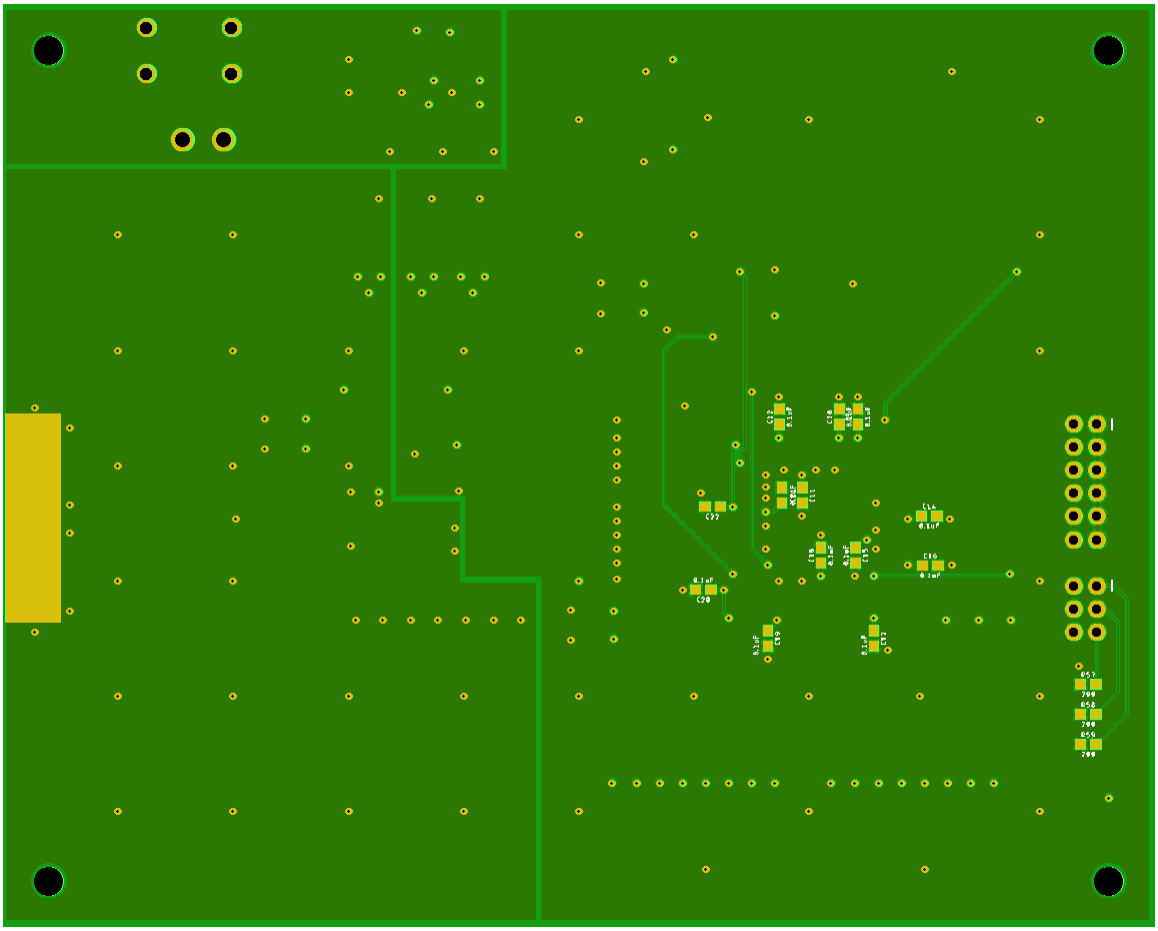

Digital Synthesizer Schematic
California Polytechnic State University
San Luis Obispo
Electrical Engineering Department
Designed By: Alex Marette

APPENDIX C Layout

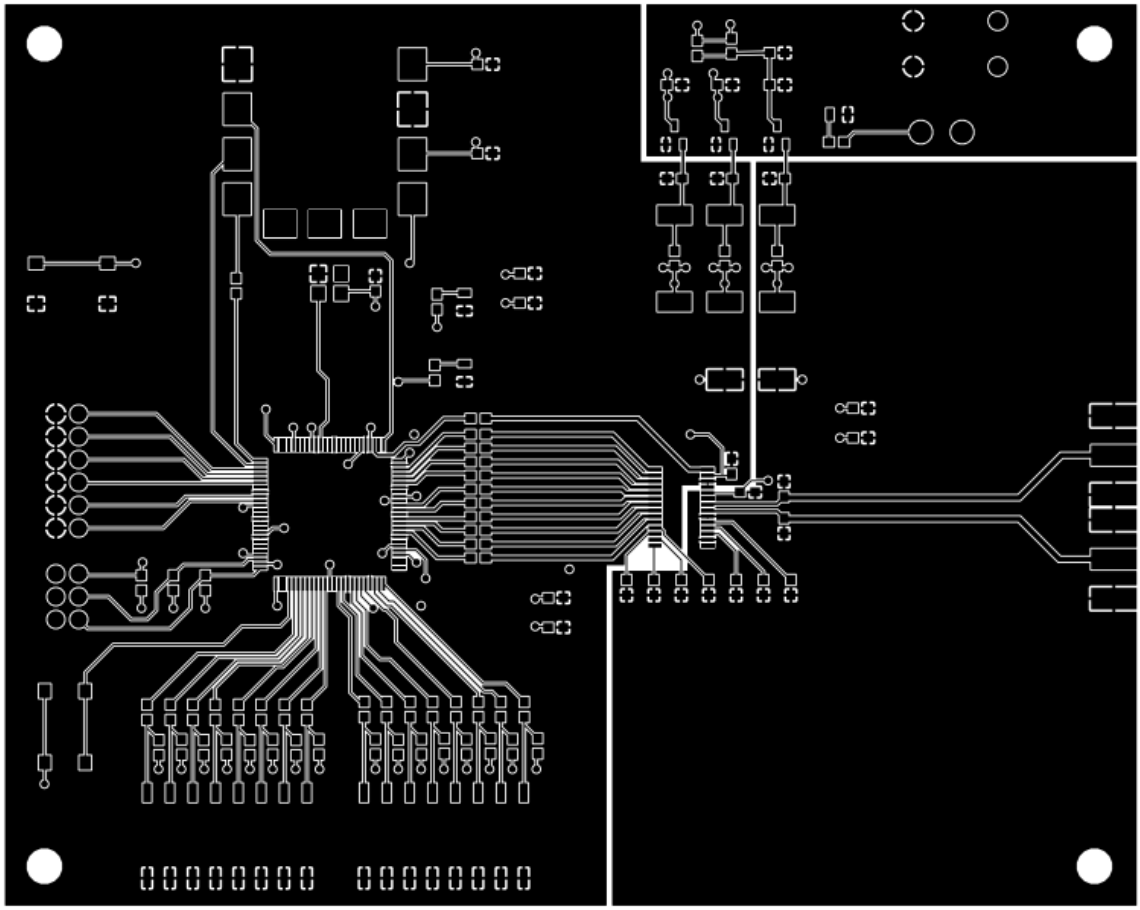
Digital Synthesizer Top Side



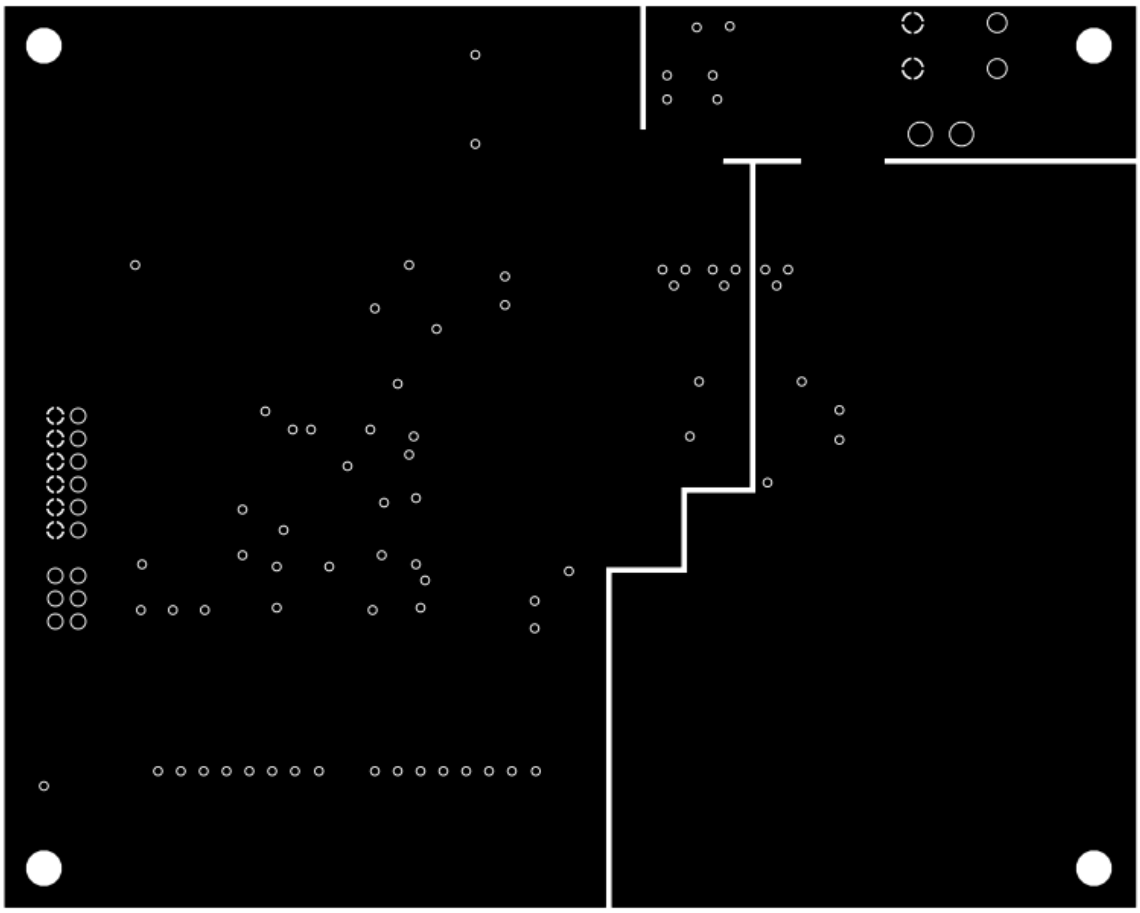
Digital Synthesizer Bottom Side



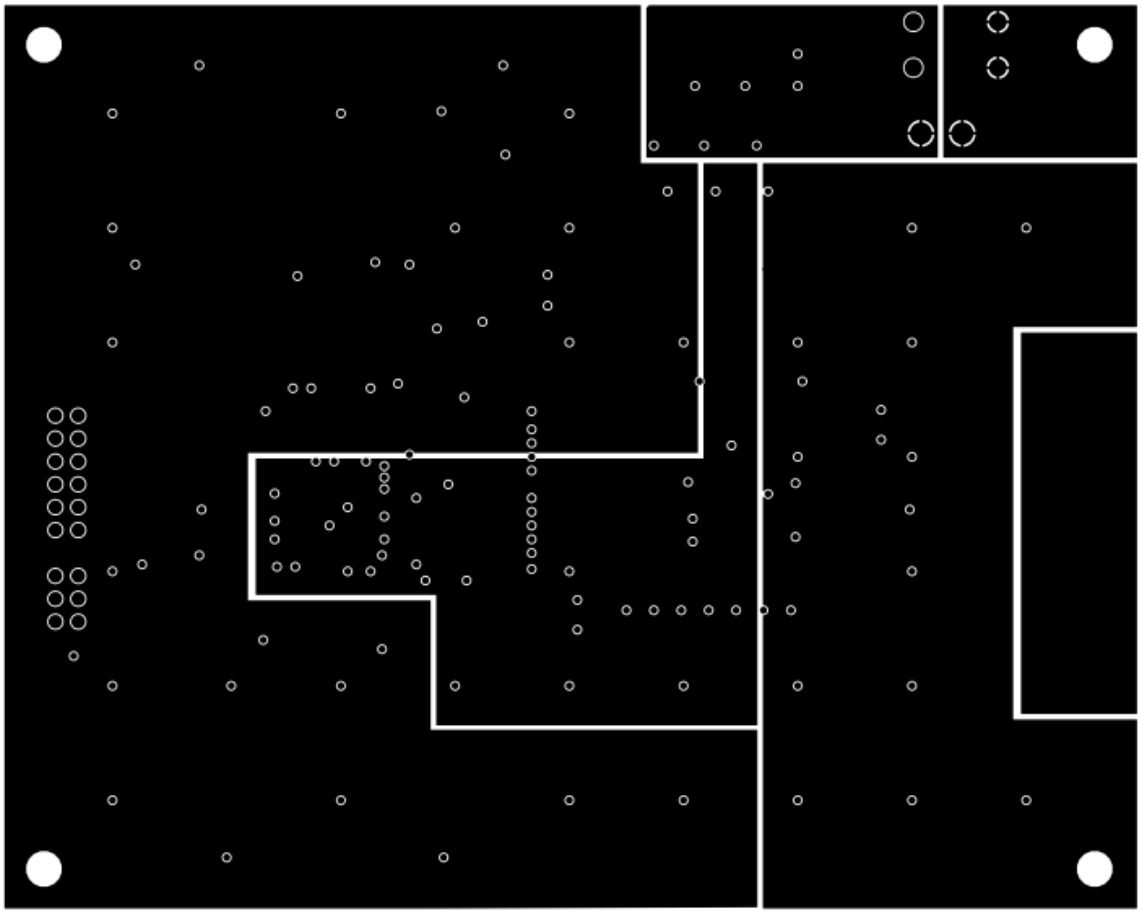
Digital Synthesizer Top Layer



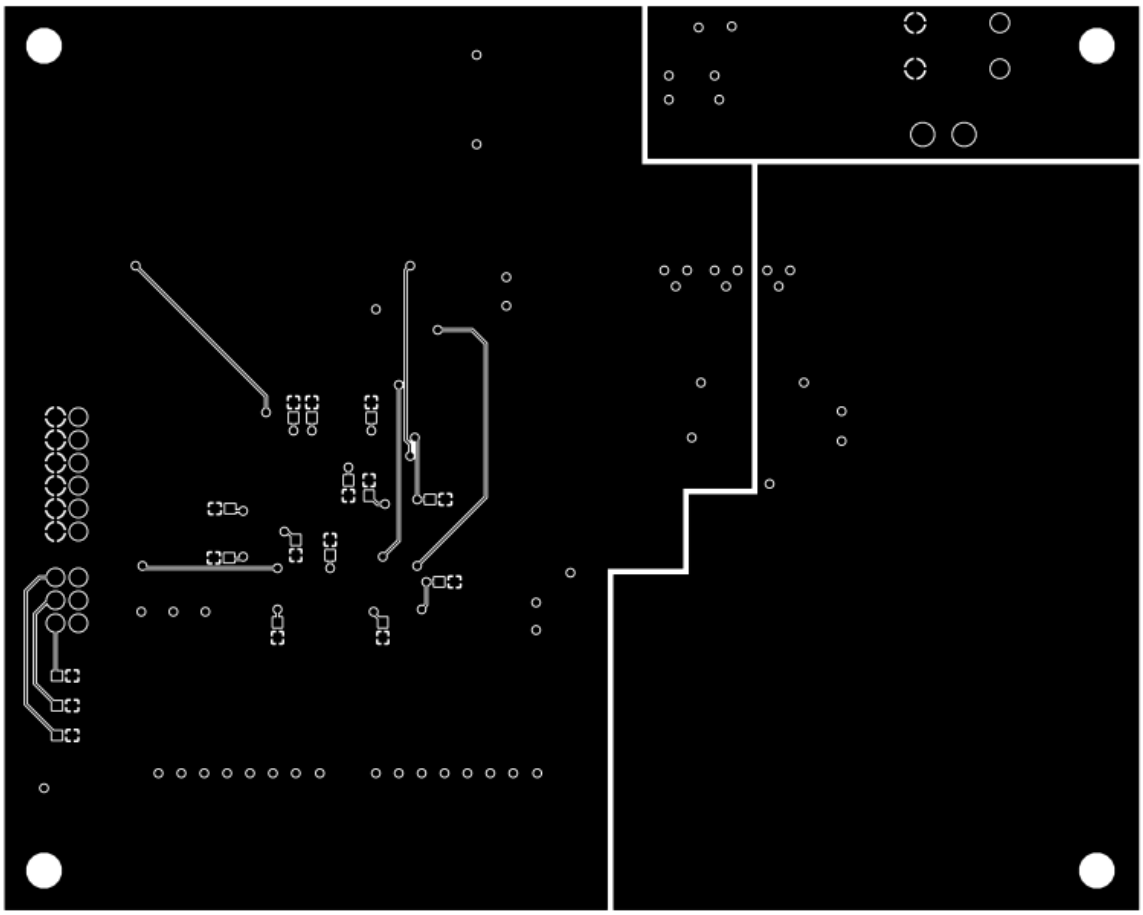
Digital Synthesizer Ground Layer



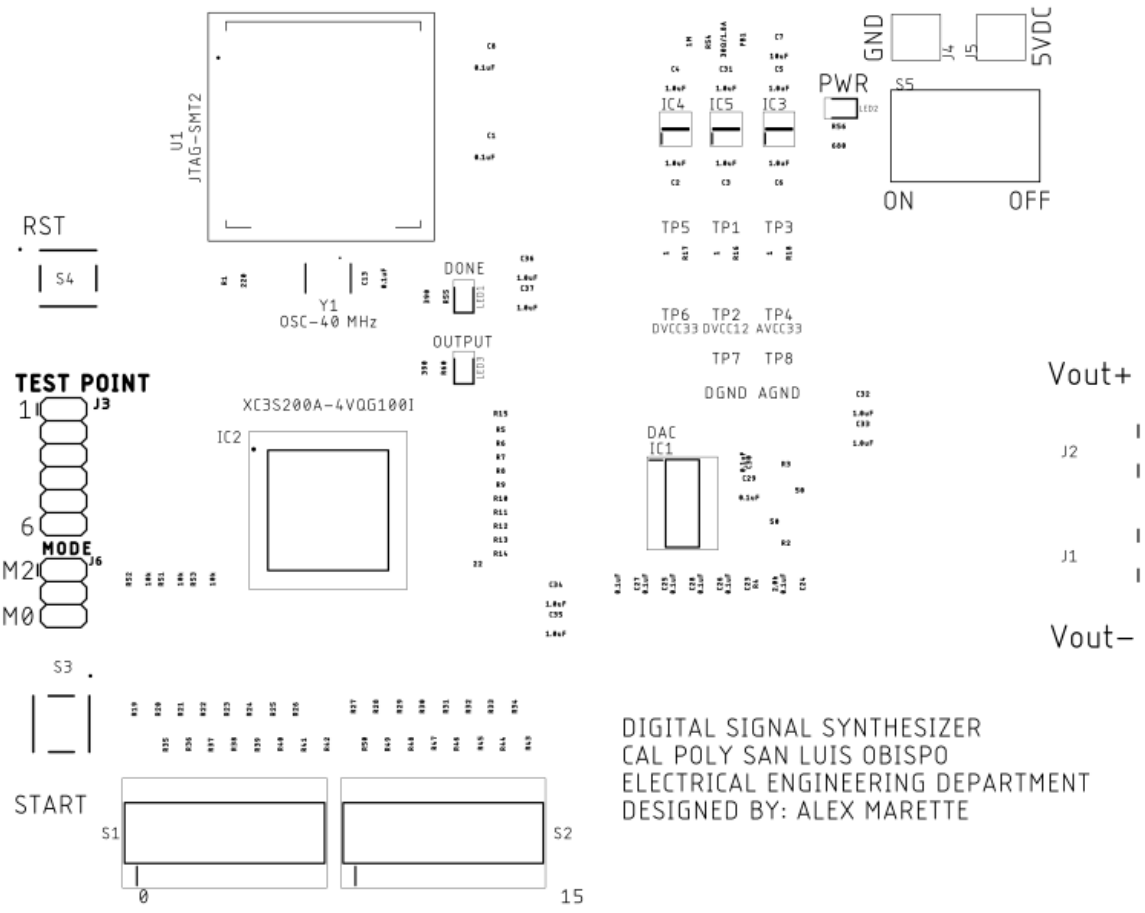
Digital Synthesizer Power Layer



Digital Synthesizer Bottom Layer

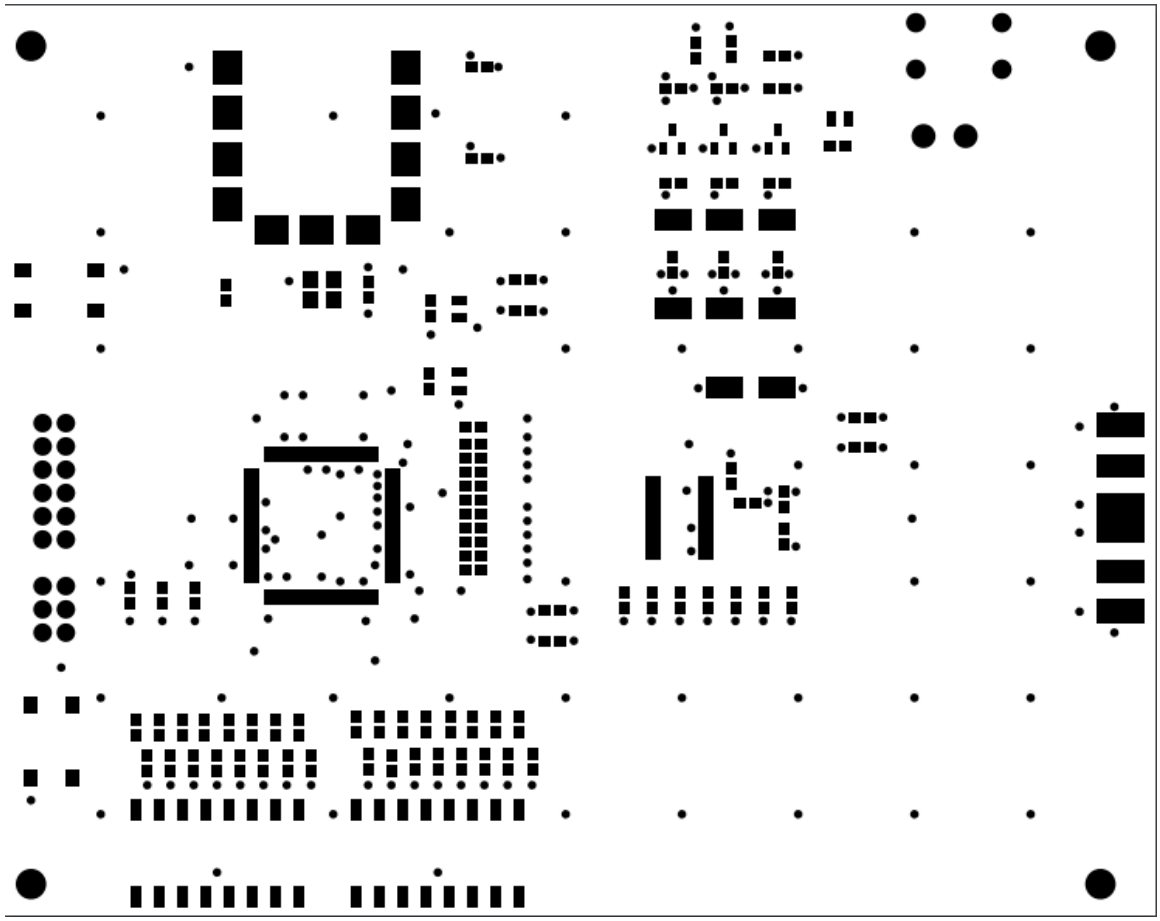


Digital Synthesizer Top Silk

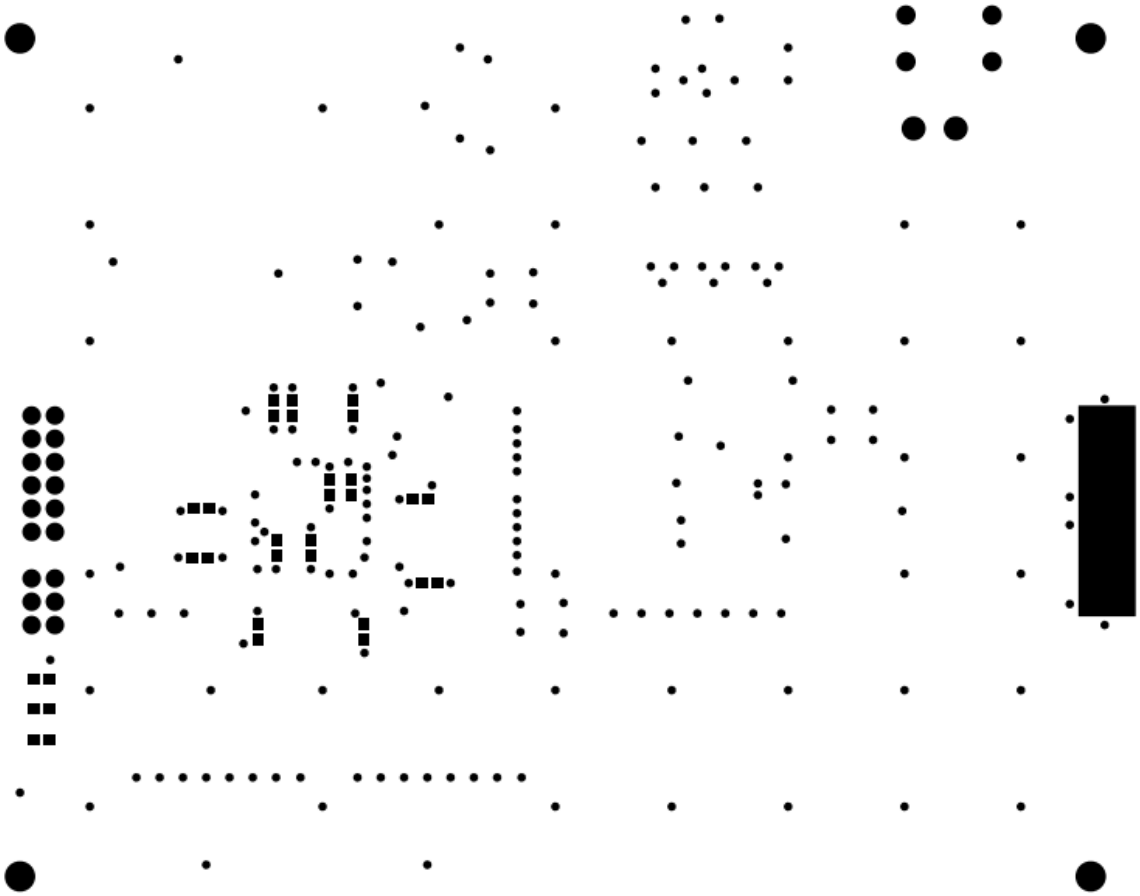


Digital Synthesizer Bottom Silk

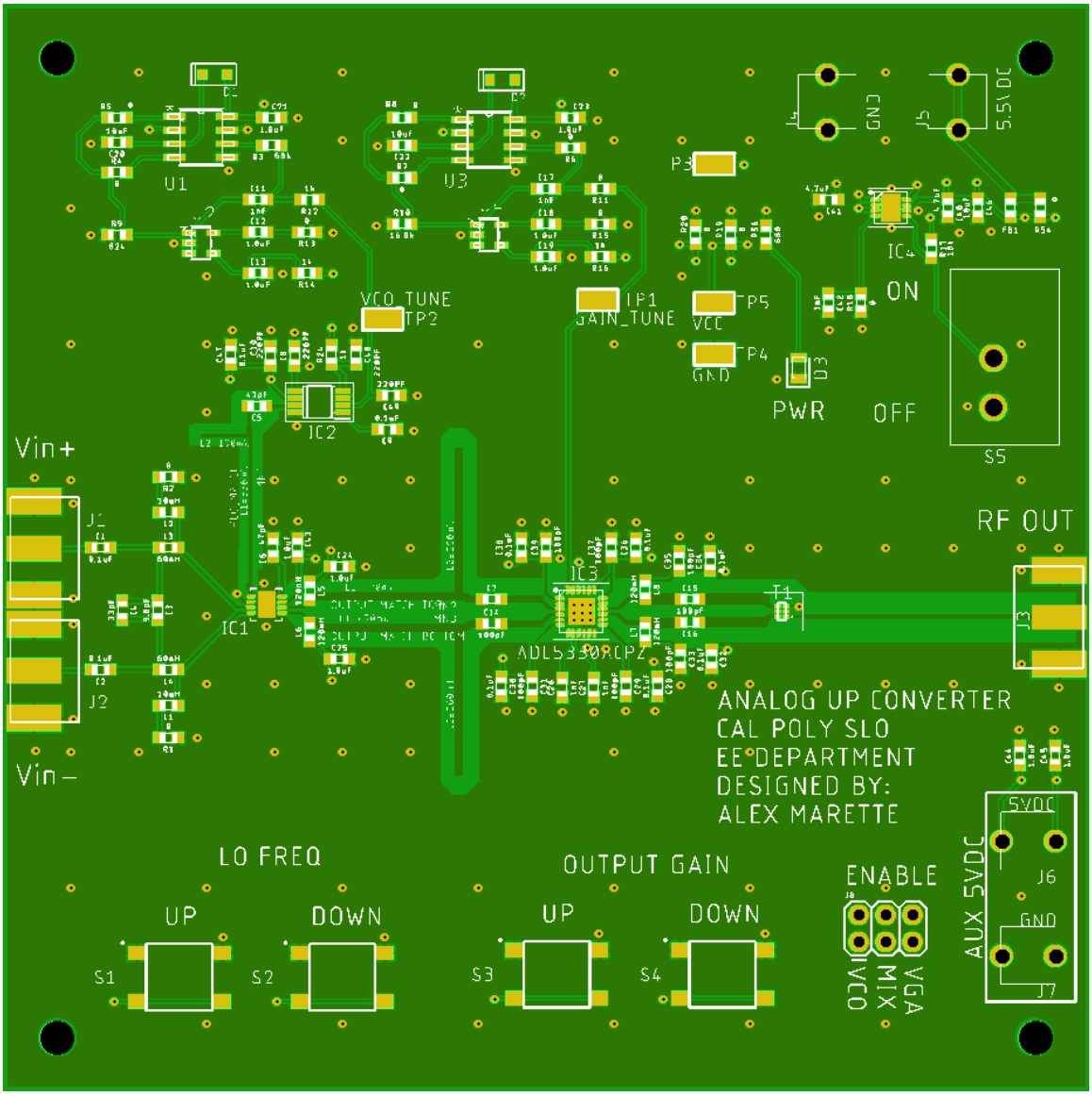
Digital Synthesizer Top Solder Mask



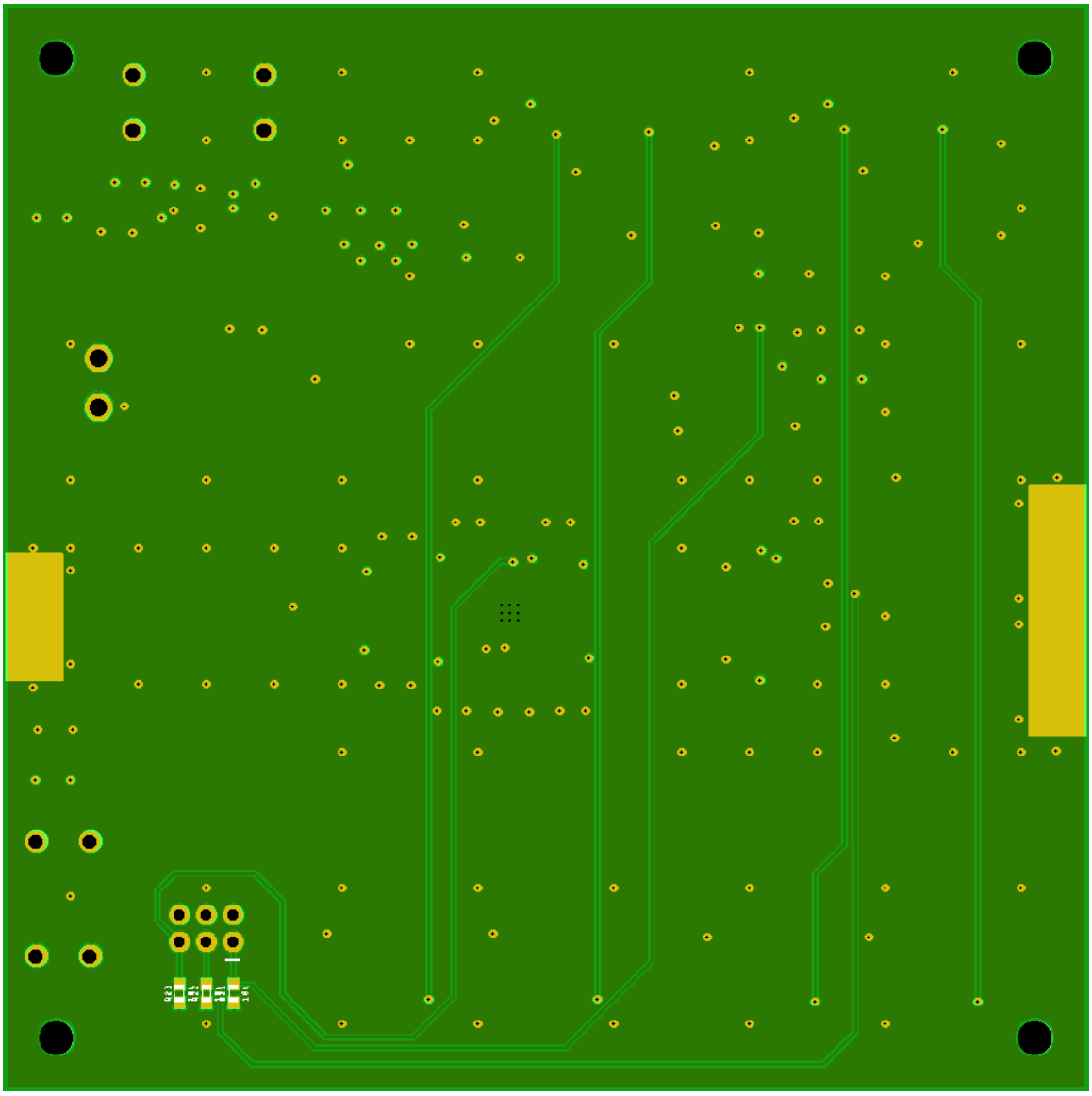
Digital Synthesizer Bottom Solder Mask



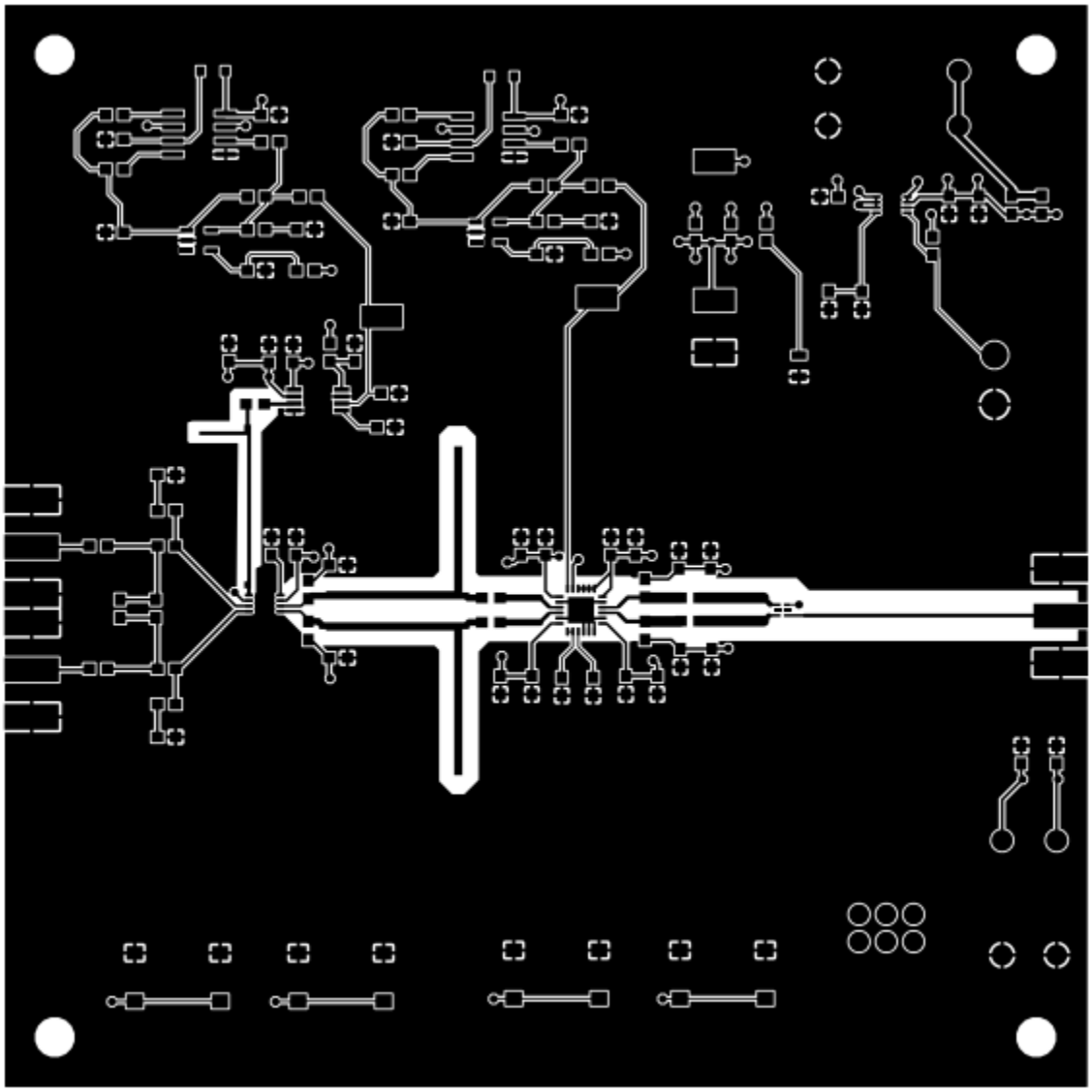
Analog Upconverter Top Side



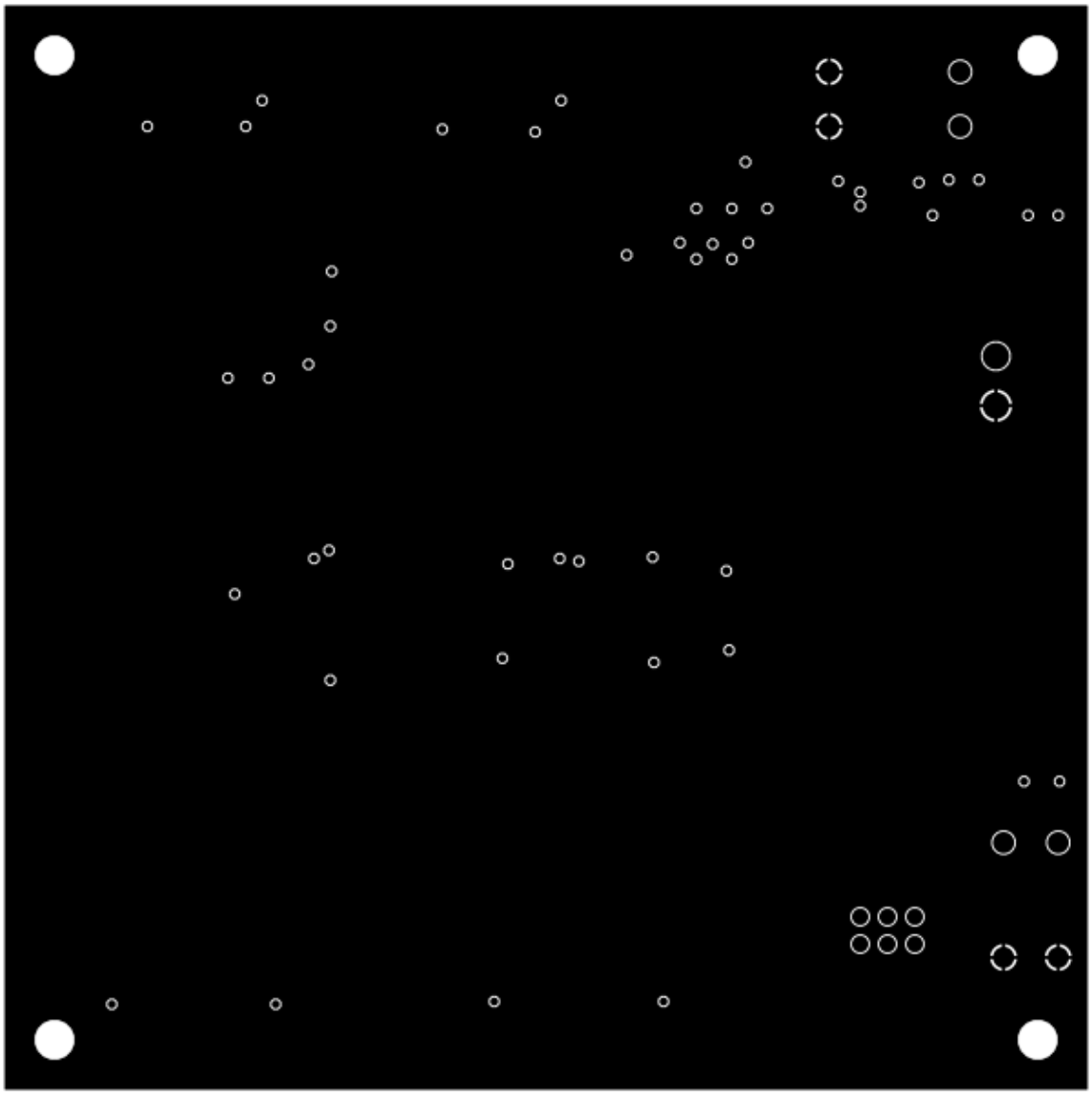
Analog Upconverter Bottom Side



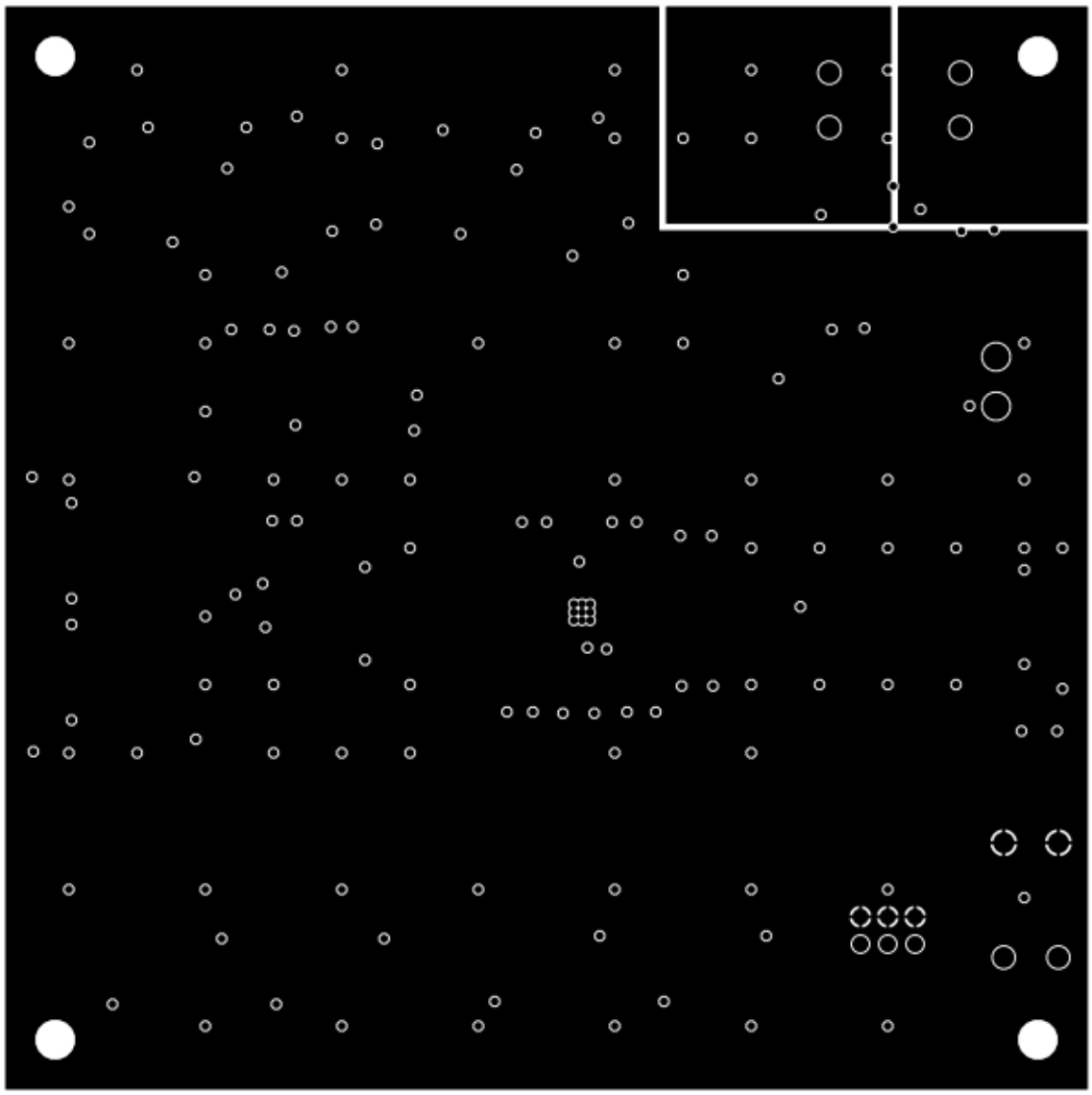
Analog Upconverter Top Layer



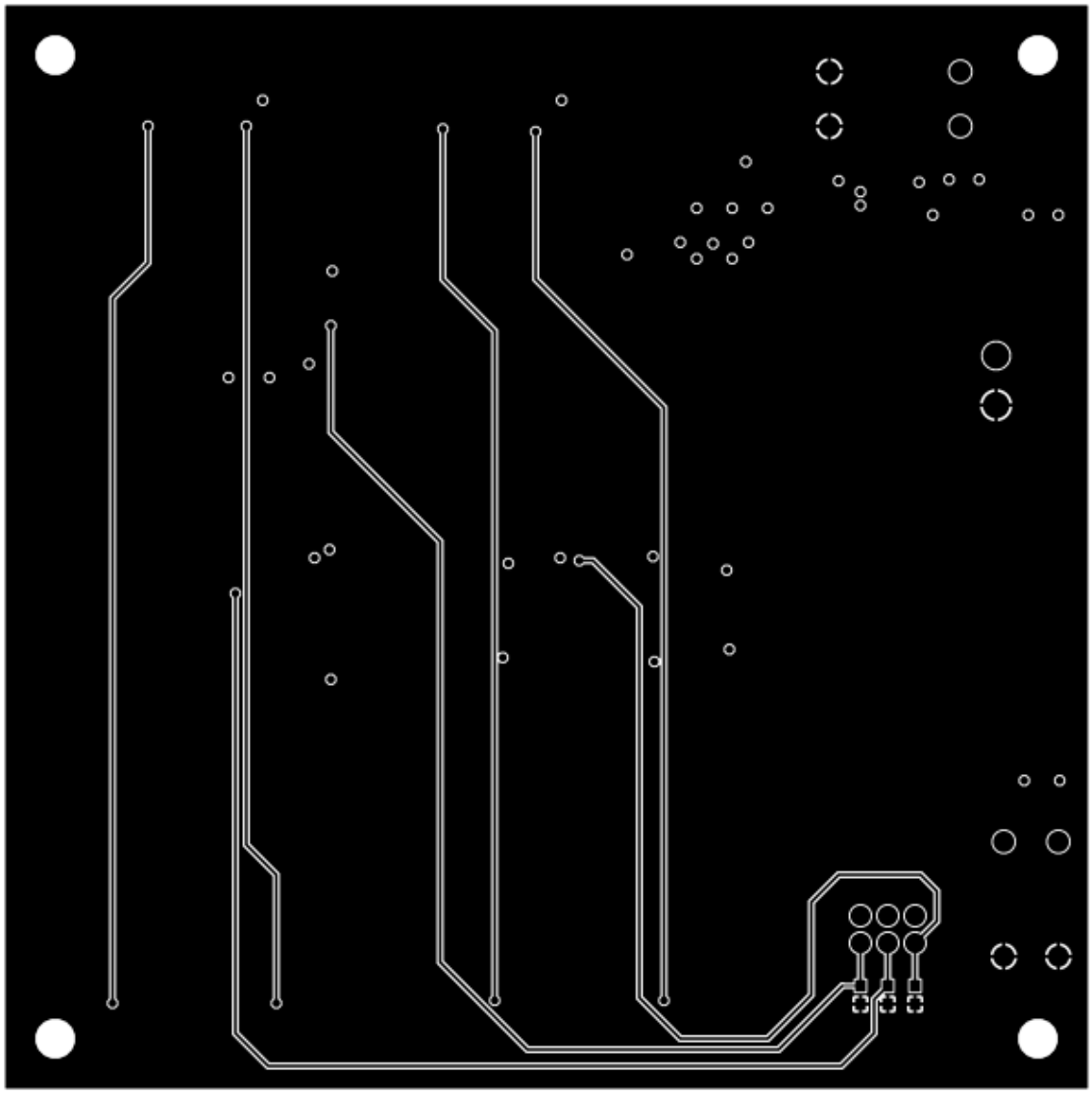
Analog Upconverter Ground Layer



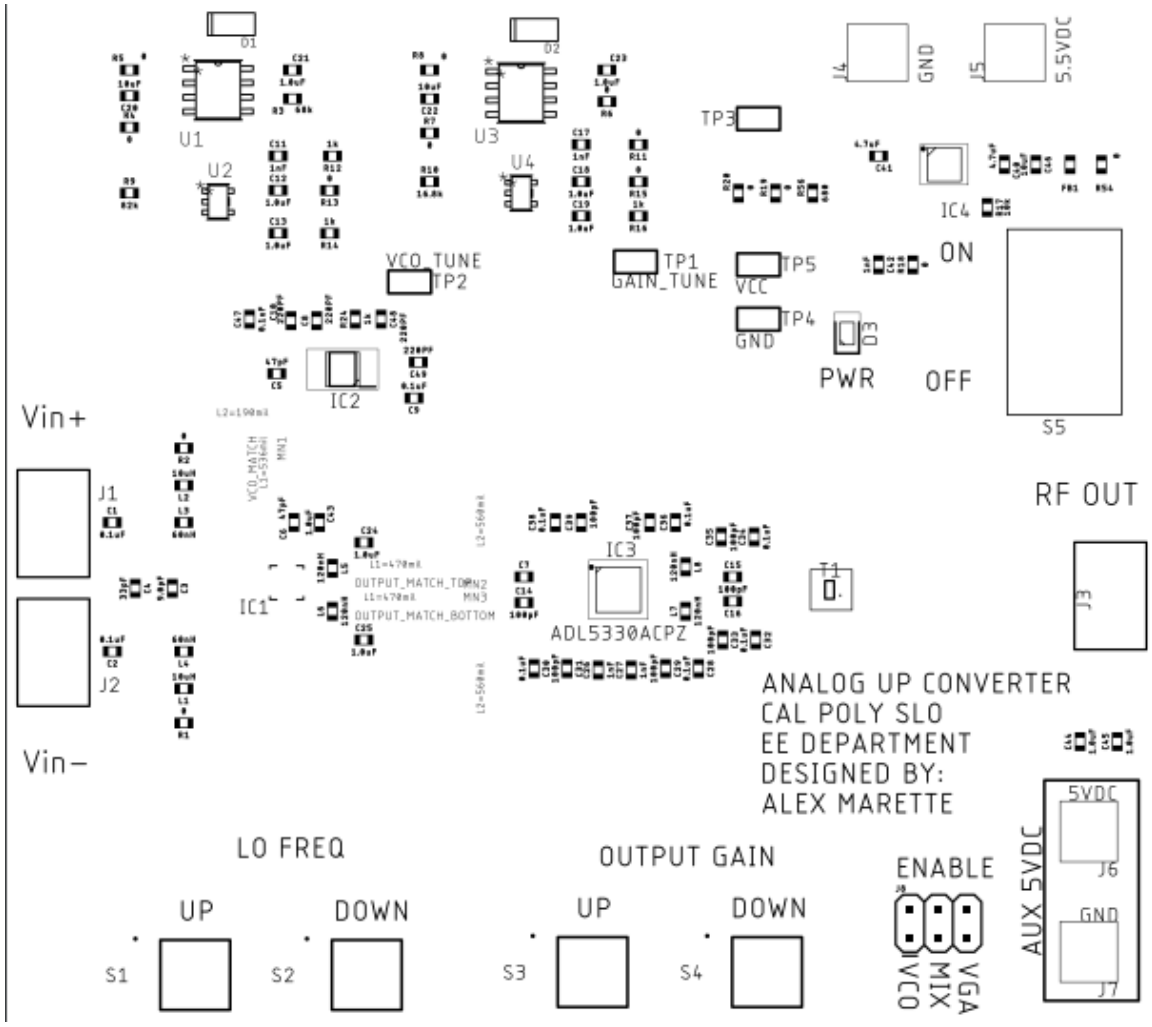
Analog Upconverter Power Layer



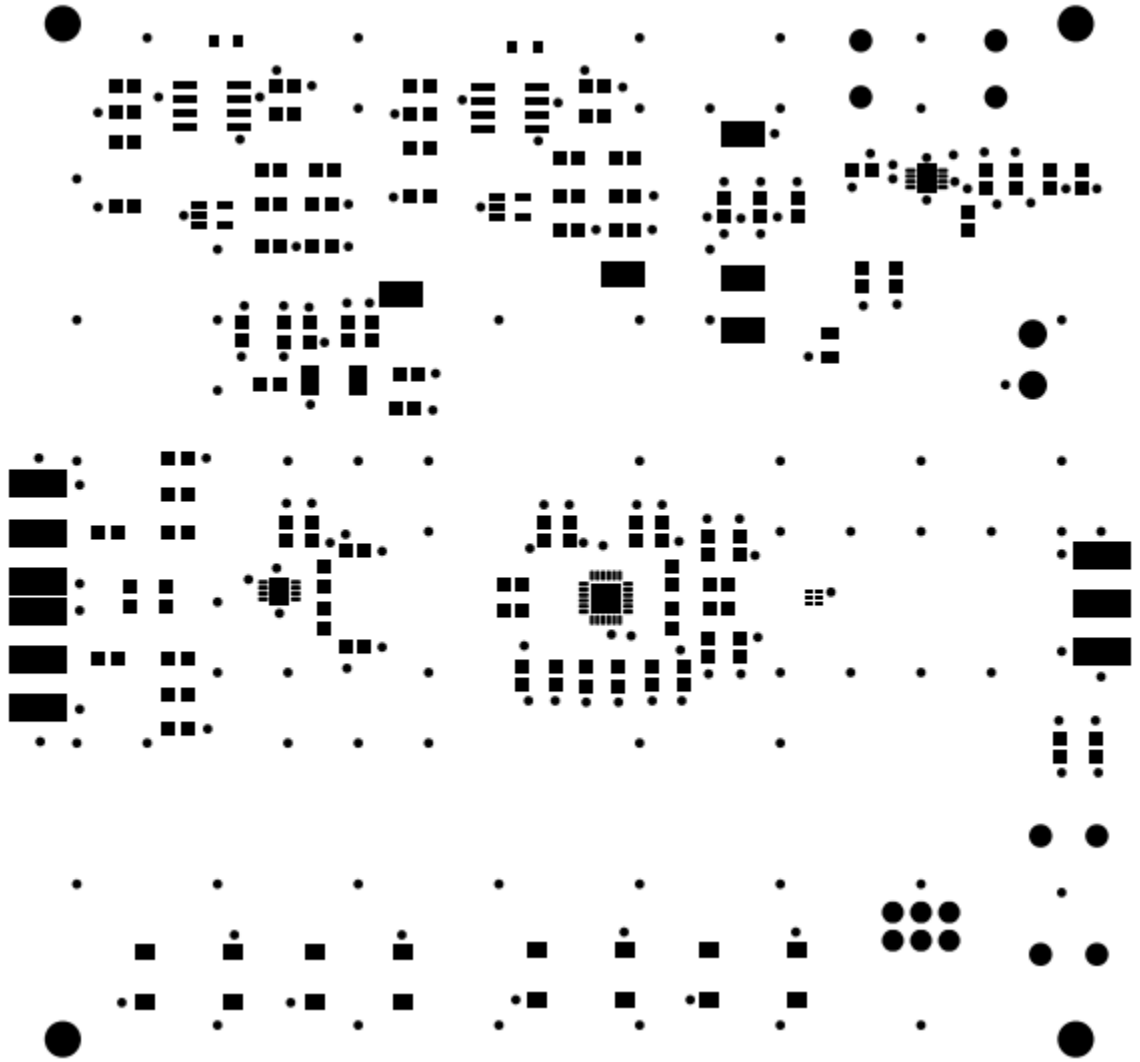
Analog Upconverter Bottom Layer



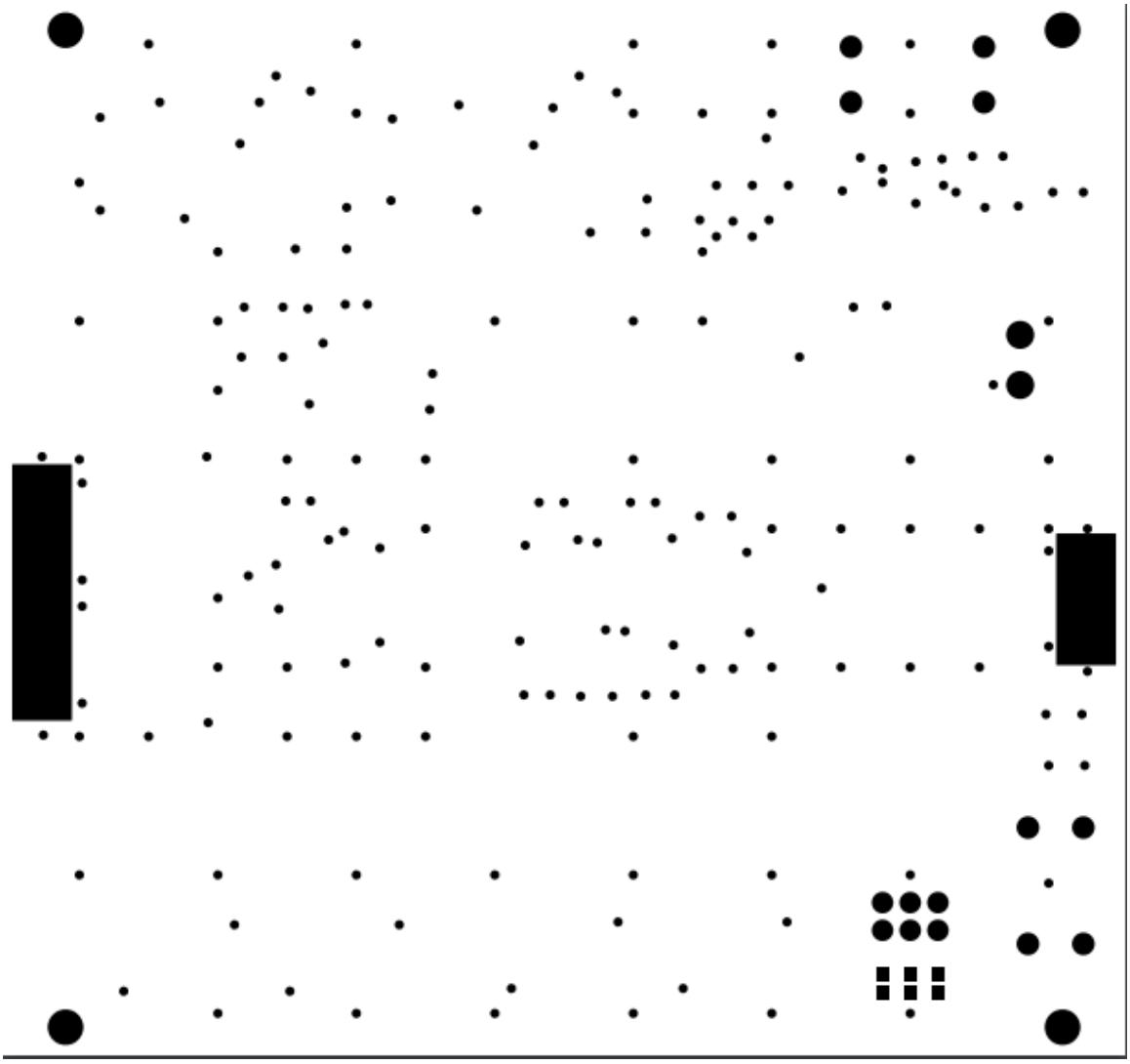
Analog Upconverter Top Silk



Analog Upconverter Top Solder Mask



Analog Upconverter Bottom Solder Mask



APPENDIX D Parts List

Digital Synthesizer Estimated Parts List							
#	MANUFACTOR	PART #	DISCRIPTION	QUANT	REF DES	PRICE EACH	TOTAL
1	KEMET	C0603C104K8RACTU	0.1uF Cap 0603	24	C1,C8-C30	$0.10	$2.40
2	KEMET	C0603C105K8PACTU	1 uF Cap 0603	12	C2-C6, C31-C37	$0.10	$1.20
3	KEMET	C0603C106M8PAC7867	10 uF Cap 0603	1	C7	$0.52	$0.52
4	Taiyo Yuden	BKP1608HS121-T	100 Ohm @ 100 MHz Ferrite Bead	1	FB1	$0.10	$0.10
5	Analog Devices	AD9740ARUZRL7	DAC 10bit 210MSPS	1	IC1	$11.86	$11.86
6	Xilinx	XC3S200A-4VQG100C	FPGA	1	IC2	$16.31	$16.31
7	Diodes Incorperated	AP2125N-3.3TRG1	3.3V LDO	2	IC3-IC4	$0.48	$0.96
8	Diodes Incorperated	AP2120N-1.2TRG1	1.2V LDO	1	IC5	$0.37	$0.37
9	Cinch	142-0701-851	SMA 50 Ohm End Launch Jack Receptacle	2	J1,J2	$5.22	$10.44
10	Sullins	PRPC040DAAN-RC	CONN HEADER .100" DUAL STR 80POS	1	J3, J6	$1.32	$1.32
11	Cinch	105-1102-001	Red BANANA JACK	1	J5	$0.69	$0.69
12	Cinch	105-1103-001	BLK BANANA JACK	1	J4	$0.66	$0.66
13	N/A	N/A	RED LED 0805	3	LED1, LED2, LED3	$0.00	$0.00
14	Yageo	RC0603FR-07220RL	220 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	1	R1	$0.10	$0.10
15	Yageo	RC0603FR-0722RL	22 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	11	R5-R15	$0.10	$1.10
16	Yageo	RC0603FR-0749R9L	49.9 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	2	R2, R3	$0.10	$0.20
17	Yageo	RC0603FR-072KL	2 kOhms ±1% 0.1W, 1/10W Chip Resistor 0603	1	R4	$0.10	$0.10
18	Yageo	RL0603FR-070R5L	500 mOhms ±1% 0.1W, 1/10W Chip Resistor 0603	3	R16-R18	$0.32	$0.96
19	Yageo	RC0603FR-0710kL	10 kOhms ±1% 0.1W, 1/10W Chip Resistor 0603	35	R19-R53	$0.10	$3.50
20	Yageo	RC0603FR-07390RL	390 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	2	R55, R60	$0.10	$0.20
21	Yageo	RC0603FR-07680RL	680 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	1	R56	$0.10	$0.10
22	Yageo	RC0603FR-07200RL	200 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	3	R57-R59	$0.10	$0.30
23	ALPS	SSGM680200	DIP Switches / SIP Switches DIP ON OFF 8P 8 Top Slide	2	S1, S2	$1.71	$3.42
24	Wurth	430182070816	SWITCH TACTILE SPST-NO 0.05A 12V	2	S3, S4	$0.47	$0.94
25	C&K	L101011MS02Q	SWITCH SLIDE SPST 4A 125V	1	S5	$1.65	$1.65
26	Keystone	5029	PC TEST POINT MINI SMD	8	TP1-TP8	$0.32	$2.56
27	Digilent	210-251	JTAGSMT2 FPGA PROGRAMMER	1	U1	$54.00	$54.00
28	SiTIME	SIT5001AC-3E-33N0-40.000000X	OSC MEMS TCXO 40.000MHZ LVCMOS	1	Y1	$4.98	$4.98
29	Yageo	RC0603JR-070RL	RES SMD 0 OHM JUMPER 1/10W 0603	20		$0.10	$2.00
30	DNI	DNI	Do Not Instal	1	R54		
			Total	146			$122.94

Digital Synthesizer Purchased Parts List

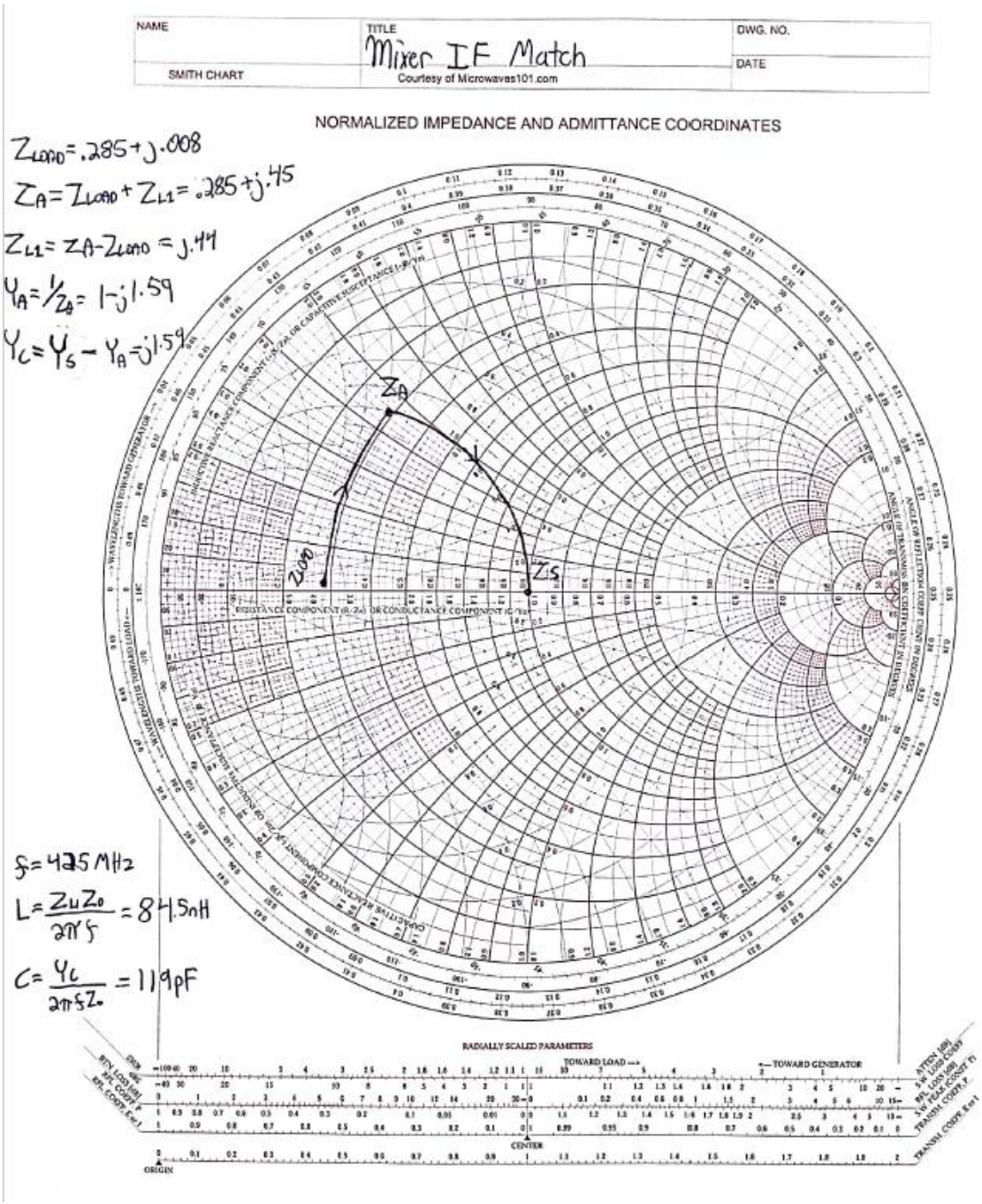
#	Quantity	Part Number	Manufacturer Part Number	Description	Unit Price (USD)	Extended Price (USD)
1	30	399-1095-1-ND	C0603C104K8RACTU	CAP CER 0.1UF 10V X7R 0603	0.03	0.87
2	20	399-3118-1-ND	C0603C105K8PACTU	CAP CER 1UF 10V X5R 0603	0.05	0.98
3	5	399-14945-1-ND	C0603C106M8PAC7867	CAP CER 10UF 10V X5R 0603	0.52	2.60
4	3	587-1923-1-ND	BKP1608HS121-T	FERRITE BEAD 120 OHM 0603 1LN	0.10	0.30
5	1	AD9740ARUZRL7CT-ND	AD9740ARUZRL7	IC DAC 10BIT 210MSPS 28-TSSOP	11.86	11.86
6	1	122-1594-ND	XC3S200A-4VQG100C	IC FPGA 68 I/O 100VQFP	16.31	16.31
7	4	AP2125N-3.3TRG1DICT-ND	AP2125N-3.3TRG1	IC REG LINEAR 3.3V 300MA SOT23-3	0.48	1.92
8	2	AP2120N-1.2TRG1DICT-ND	AP2120N-1.2TRG1	IC REG LINEAR 1.2V 150MA SOT23	0.37	0.74
9	2	J658-ND	142-0701-851	CONN SMA JACK STR 50OHM EDGE MNT	5.22	10.44
10	1	S2011EC-40-ND	PRPC040DAAN-RC	CONN HEADER .100" DUAL STR 80POS	1.32	1.32
11	2	J576-ND	105-1102-001	CONN JACK TEST HORIZ INSUL	0.69	1.38
12	2	J577-ND	105-1103-001	CONN JACK TEST HORIZ INSUL	0.66	1.32
13	10	311-220HRCT-ND	RC0603FR-07220RL	RES SMD 220 OHM 1% 1/10W 0603	0.02	0.15
14	15	311-22.0HRCT-ND	RC0603FR-0722RL	RES SMD 22 OHM 1% 1/10W 0603	0.02	0.23
15	10	311-49.9HRCT-ND	RC0603FR-0749R9L	RES SMD 49.9 OHM 1% 1/10W 0603	0.02	0.15
16	10	311-2.00KHRCT-ND	RC0603FR-072KL	RES SMD 2K OHM 1% 1/10W 0603	0.02	0.15
17	5	311-.5QCT-ND	RL0603FR-070R5L	RES 0.5 OHM 1% 1/10W 0603	0.32	1.60
18	100	311-10.0KHRCT-ND	RC0603FR-0710KL	RES SMD 10K OHM 1% 1/10W 0603	0.01	0.60
19	10	311-390HRCT-ND	RC0603FR-07390RL	RES SMD 390 OHM 1% 1/10W 0603	0.02	0.15
20	10	311-680HRCT-ND	RC0603FR-07680RL	RES SMD 680 OHM 1% 1/10W 0603	0.02	0.15
21	10	311-200HRCT-ND	RC0603FR-07200RL	RES SMD 200 OHM 1% 1/10W 0603	0.02	0.15
22	4	732-7006-1-ND	430182070816	SWITCH TACTILE SPST-NO 0.05A 12V	0.47	1.88
23	2	CKC5106-ND	L101011MS02Q	SWITCH SLIDE SPST 4A 125V	1.65	3.30
24	10	36-5029CT-ND	5029	PC TEST POINT MINI SMD	0.30	3.03
25	1	1286-1028-ND	210-251	JTAGSMT2 FPGA PROGRAMMER	54.00	54.00
26	2	1473-1518-1-ND	SIT5001AC-3E-33N0-40.000000X	OSC MEMS TCXO 40.000MHZ LVCMOS	4.98	9.96
27	20	311-0.0GRCT-ND	RC0603JR-070RL	RES SMD 0 OHM JUMPER 1/10W 0603	0.01	0.20
28	15	311-10.0HRCT-ND	RC0603FR-0710RL	RES SMD 10 OHM 1% 1/10W 0603	0.02	0.23
					Total	125.97

er Estimated Parts List

#	MANUFACTOR	PART #	DISCRIPTION	QUANT	REF DES	PRICE EACH	TOTAL
1	KEMET	C0603C104J4RACTU	CAP CER 0.1UF 16V X7R 0603	9	C1,C2,C9,C28,C30,C32,C34,C36,C38	$0.12	$1.08
2	KEMET	C0603C105K3RACTU	CAP CER 1UF 25V X7R 0603	11	C12,C13,C18,C19,C21,C23,C24,C25,C43,C44,C45	$0.24	$2.64
3	KEMET	CBR06C101F5GAC	CAP CER RF 100PF 50V +/-0.1 PF C0	10	C7,C14,C15,C16,C29,C31,C33,C35,C37,C39	$0.67	$6.74
4	KEMET	C0603C106M8PAC7867	CAP CER 10UF 10V X5R 0603	3	C20,C22,C46	$0.52	$1.56
5	KEMET	C0603C102J4GAC7867	CAP CER 1000PF 16V NP0 0603	5	C11,C17,C26,C27,C42	$0.34	$1.70
6	KEMET	C0603C221J4GACTU	CAP CER 220PF 16V C0G/NP0 0603	2	C10,C8	$0.28	$0.56
7	KEMET	C0603C330F5GACT	CAP CER 33PF 50V C0G/NP0 0603	1	C4	$0.26	$0.26
8	KEMET	C0603C475K8PACTU	CAP CER 4.7UF 10V X5R 0603	2	C40,C41	$0.29	$0.58
9	KEMET	CBR06C510F5GAC	CAP CER RF 51PF 50V +/-0.1 PF C0	2	C5,C6	$0.89	$1.78
10	KEMET	CBR06C909BAGAC	CAP CER 9PF 250V C0G/NP0 0603	1	C3	$0.55	$0.55
11	TOSHIBA	CUS08F30,H3F	DIODE SCHOTTKY 30V 800MA USC	2	D1,D2	$0.36	$0.72
12	N/A	N/A	LED	1	D3	$0.00	$0.00
13	Linear Technology	LT5560EDDPBF	IC MIXER 10KHZ-4GHZ UP/DWN 8DFN	1	IC1	$3.20	$3.20
14	MAXIM	MAX2750EUA+	IC OSC VOLT CNTRL 8-UMAX	1	IC2	$6.06	$6.06
15	ANALOG DEVICES	ADL5330ACPZ-REEL7	IC AMP/ATTENUATOR RF VAR 24LFCSP	1	IC3	$11.22	$11.22
16	ANALOG DEVICES	ADM7171ACPZ-5.0-R7	IC REG LINEAR 1A 8LFCSP	1	IC4	$3.28	$3.28
17	Cinch	142-0701-851	SMA 50 Ohm End Launch Jack Receptacle	3	J1,J2,J3	$5.22	$15.66
18	Cinch	105-1102-001	Red BANANA JACK	2	J5,J6	$0.69	$1.38
19	Cinch	105-1103-001	BLK BANANA JACK	2	J4,J7	$0.66	$1.32
20	Murata	LQW21HN2R2J00L	FIXED IND 2.2UH 75MA 6.5 OHM SMD	2	L1,L2	$0.50	$1.00
21	Murata	LQW18AN62NG00D	FIXED IND 62NH 280MA 510 MOHM	2	L3,L4	$0.19	$0.38
22	Murata	LQW18AN56NJ8ZD	56 nH, 2.6GHz reasonance,RFC	4	L5-L8	$0.28	$1.12
23	Yageo	RC0603JR-070RL	RES SMD 0 OHM JUMPER 1/10W 0603	16	R1,R2,R4,R5,R6,R7,R8,R11,R12,R13,R15,R16,R18,R19,R20	$0.10	$1.60
24	Yageo	RC0603FR-07680RL	680 Ohms ±1% 0.1W, 1/10W Chip Resistor 0603	1	R56	$0.10	$0.10
25	Yageo	RC0603FR-0710kL	10 kOhms ±1% 0.1W, 1/10W Chip Resistor 0603	1	R17	$0.10	$0.10
26	Yageo	311-16.9HRCT-ND	RES SMD 16.9 OHM 1% 1/10W 0603	1	R10	$0.10	$0.10
27	Yageo	RC0603FR-071KL	RES SMD 1K OHM 1% 1/10W 0603	1	R14	$0.10	$0.10
28	Yageo	RC0603FR-0768KL	RES SMD 68K OHM 1% 1/10W 0603	1	R3	$0.10	$0.10
29	Yageo	RC0603FR-0782KL	RES SMD 82K OHM 1% 1/10W 0603	1	R9	$0.10	$0.10
30	Wurth	430182070816	SWITCH TACTILE SPST-NO 0.05A 12V	4	S1,S2,S3,S4	$0.47	$1.88
31	C&K	L101011MS02Q	SWITCH SLIDE SPST 4A 125V	1	S5	$1.65	$1.65
32	Murata	LDB182G4505C-110	TRANSFORMER BALUN 2.45GH	1	T1	0.4	$0.40
33	Keystone	5029	PC TEST POINT MINI SMD	5	TP1-TP5	$0.32	$1.60
34	MAXIM	DS1809Z-050+	DIGITAL POT	2	U1,U3	$1.90	$3.80
35	Linear Technology	LT6650CS5TRMPBF	VOLTAGE REFERENCE	2	U2,U4	$3.13	$6.26
36	Yageo	PT0603FR-7W0R1L	RES 0.1 OHM 1% 1/5W 0603	10	DNI	$0.31	$3.06
37	Taiyo Yuden	BKP1608HS121-T	100 Ohm @ 100 MHz Ferrite Bead	1	FB1	$0.10	$0.10
			Total	116			$83.74

Analog Upconverter Purchased Parts List					
#	Quantity	Manufacturer Part Number	Description	Unit Price (USD)	Extended Price
1	15	C0603C104J4RACTU	CAP CER 0.1UF 16V X7R 0603	0.088	$1.32
2	15	CBR06C101F5GAC	CAP CER RF 9.9PF 50V 1% C0G 0603	0.674	$10.11
3	5	C0603C106M8PAC7867	CAP CER 10UF 10V X5R 0603	0.52	$2.60
4	10	C0603C102J4GAC7867	CAP CER 1000PF 16V NP0 0603	0.235	$2.35
5	5	C0603C221J4GACTU	CAP CER 220PF 16V C0G/NP0 0603	0.28	$1.40
6	3	C0603C330F5GACTU	CAP CER 33PF 50V C0G/NP0 0603	0.26	$0.78
7	4	C0603C475K8PACTU	CAP CER 4.7UF 10V X5R 0603	0.29	$1.16
8	4	CBR06C510F5GAC	CAP CER RF 51PF 50V +/- 0.1 PF C0	0.89	$3.56
9	2	CBR06C909BAGAC	CAP CER 9PF 250V C0G/NP0 0603	0.55	$1.10
10	4	CUS08F30,H3F	DIODE SCHOTTKY 30V 800MA USC	0.36	$1.44
11	1	LT5560EDD#PBF	IC MIXER 10KHZ-4GHZ UP/DWN 8DFN	3.2	$3.20
12	1	MAX2750EUA+	IC OSC VOLT CNTRL 8-UMAX	6.06	$6.06
13	1	ADL5330ACPZ-REEL7	IC AMP/ATTENUATOR RF VAR 24LFCSP	11.22	$11.22
14	1	ADM7171ACPZ-5.0-R7	IC REG LINEAR 1A 8LFCSP	3.28	$3.28
15	3	142-0701-851	CONN SMA JACK STR 50OHM EDGE MNT	5.22	$15.66
16	3	105-1102-001	CONN JACK TEST HORIZ INSUL	0.69	$2.07
17	3	105-1103-001	CONN JACK TEST HORIZ INSUL	0.66	$1.98
18	4	LQW21HN2R2J00L	FIXED IND 2.2UH 75MA 6.5 OHM SMD	0.5	$2.00
19	4	LQW18AN62NG00D	FIXED IND 62NH 280MA 510 MOHM	0.19	$0.76
20	6	LQW18AN56NJ8ZD	FIXED IND 56NH 770MA 260 MOHM	0.28	$1.68
21	25	RC0603JR-070RL	RES SMD 0 OHM JUMPER 1/10W 0603	0.0072	$0.18
22	10	RC0603FR-07680RL	RES SMD 680 OHM 1% 1/10W 0603	0.015	$0.15
23	10	RC0603FR-0710KL	RES SMD 10K OHM 1% 1/10W 0603	0.015	$0.15
24	10	RC0603FR-0716R9L	RES SMD 16.9 OHM 1% 1/10W 0603	0.015	$0.15
25	10	RC0603FR-071KL	RES SMD 1K OHM 1% 1/10W 0603	0.015	$0.15
26	10	RC0603FR-0768KL	RES SMD 68K OHM 1% 1/10W 0603	0.015	$0.15
27	10	RC0603FR-0782KL	RES SMD 82K OHM 1% 1/10W 0603	0.015	$0.15
28	5	4.30182E+11	SWITCH TACTILE SPST-NO 0.05A 12V	0.47	$2.35
29	1	L101011MS02Q	SWITCH SLIDE SPST 4A 125V	1.65	$1.65
30	3	LDB182G4505C-110	TRANSFORMER BALUN 2.45GHZ 0603	0.4	$1.20
31	6	5029	PC TEST POINT MINI SMD	0.32	$1.92
32	3	DS1809Z-050+	IC DALLASTAT 50K 8-SOIC	1.9	$5.70
33	2	LT6650CS5#TRMPBF	IC VREF SERIES 0.4V TSOT23-5	3.13	$6.26
34	10	PT0603FR-7W0R1L	RES 0.1 OHM 1% 1/5W 0603	0.306	$3.06
35	2	BKP1608HS121-T	FERRITE BEAD 120 OHM 0603 1LN	0.1	$0.20
36	15	C0603C105M4RACTU	CAP CER 1UF 16V X7R 0603	0.157	$2.36
				total	$99.51

APPENDIX E Smith charts



NAME	TITLE Mixer RF Match	DWG. NO.
SMITH CHART	Courtesy of Microwaves101.com	DATE

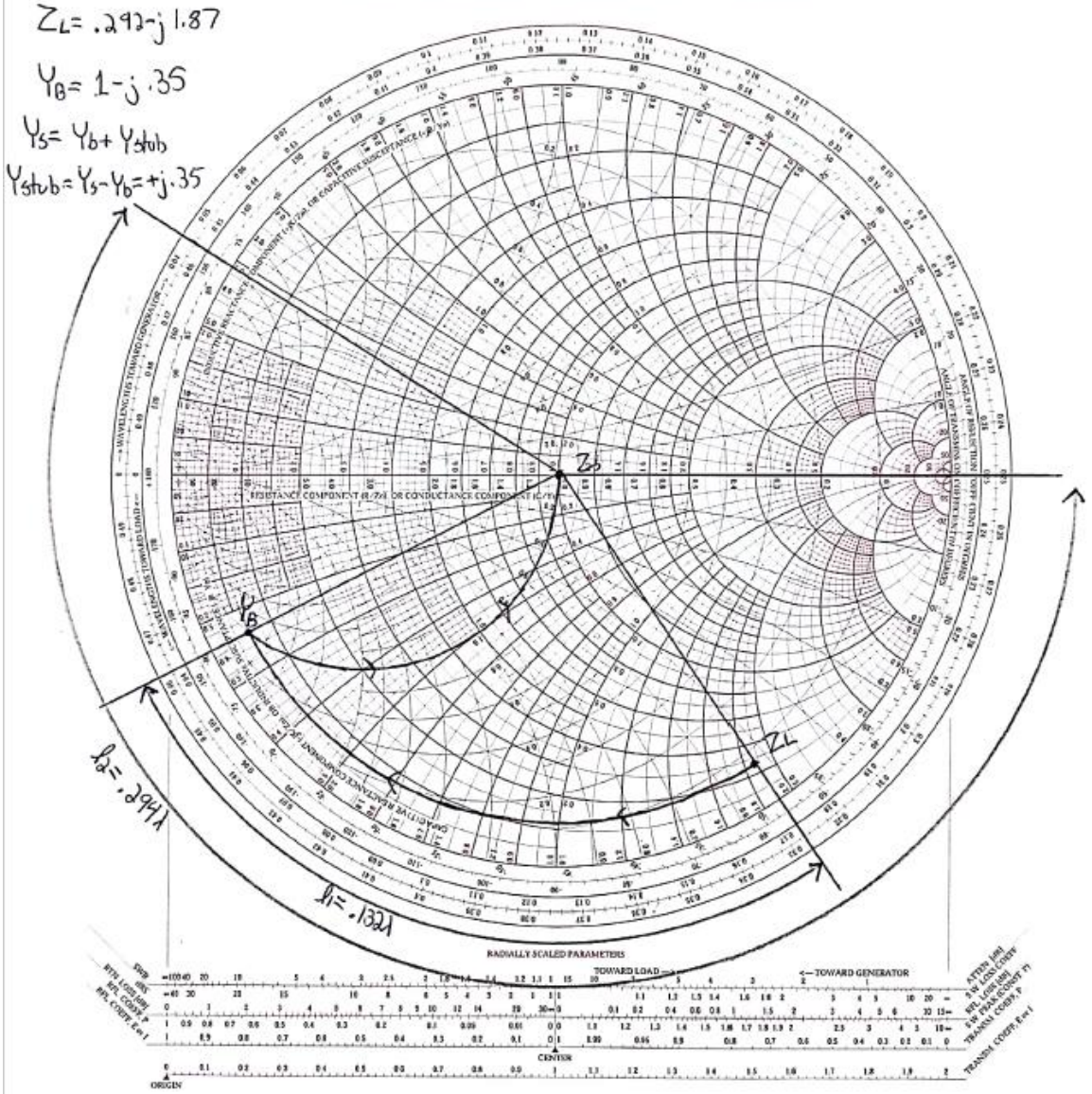
NORMALIZED IMPEDANCE AND ADMITTANCE COORDINATES

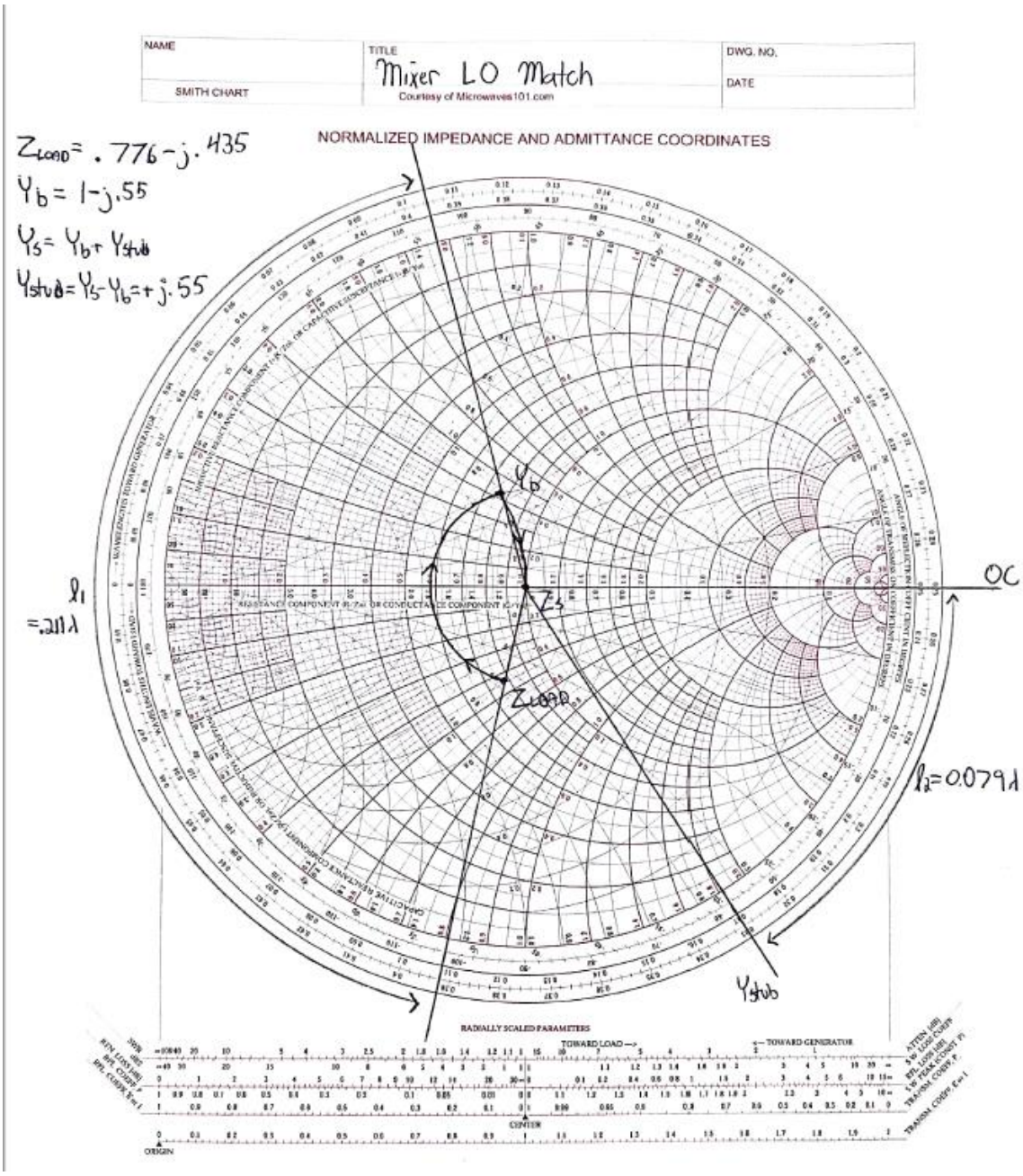
$Z_L = .292 - j\,1.87$

$Y_B = 1 - j\,.35$

$Y_S = Y_B + Y_{stub}$

$Y_{stub} = Y_S - Y_B = +j\,.35$




NAME
SMITH CHART
TITLE
Mixer LO Match
Courtesy of Microwaves101.com
DWG. NO.
DATE
NORMALIZED IMPEDANCE AND ADMITTANCE COORDINATES
Z_LOAD = .776 - j.435
Y_L = 1 - j.55
Y_S = Y_L + Y_stub
Y_stub = Y_S - Y_L = + j.55
l1 = .211λ
OC
l2 = 0.079λ
Y_L
Z_S
Z_LOAD
Y_stub
RADIALLY SCALED PARAMETERS
TOWARD LOAD —>
<— TOWARD GENERATOR
CENTER
ORIGIN