Mode-S Receiver and ADS-B Decoder

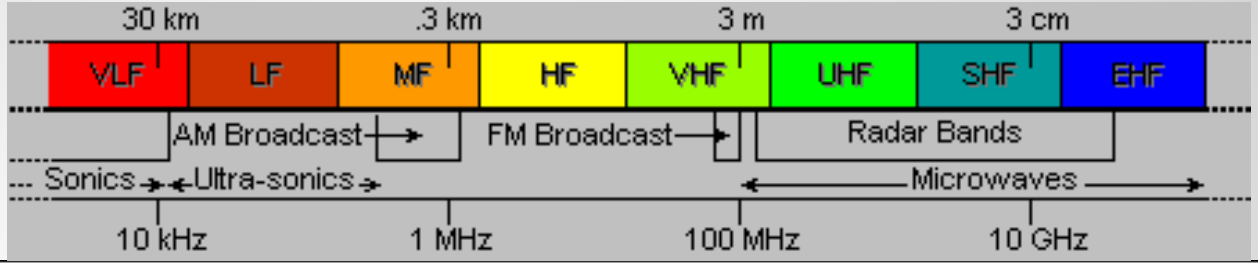
Group 24

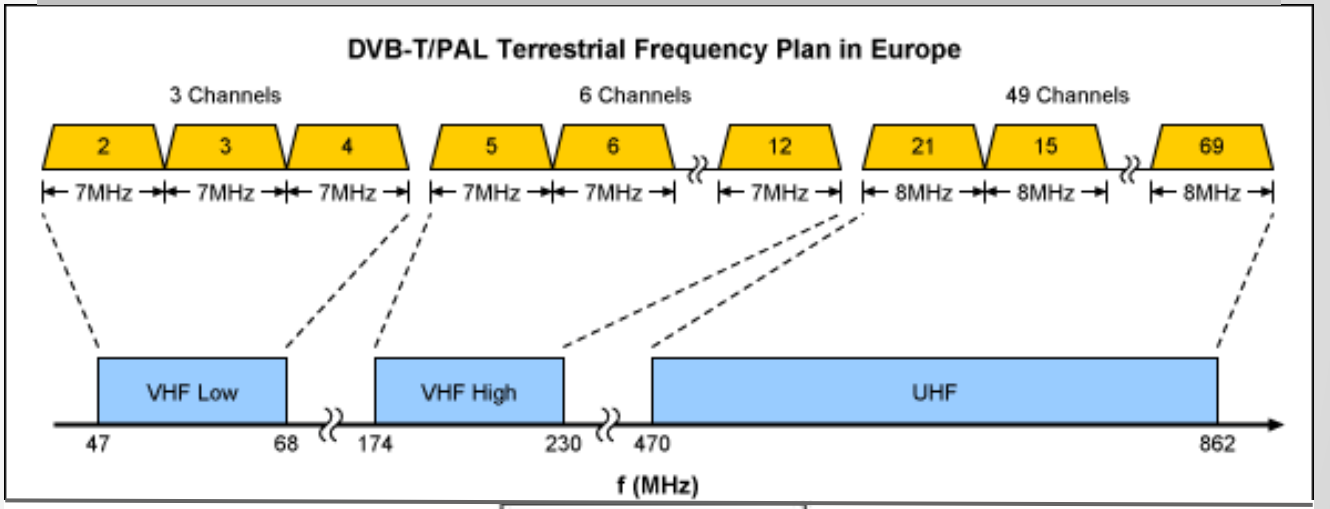
Sean Koceski, CpE
Long Lam, CpE
Michael Vose, CpE

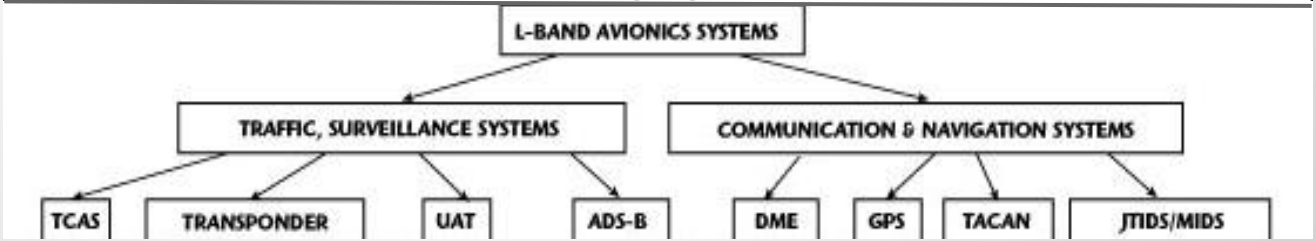
Spectrum Overload

Digital UHF TV broadcast now borders aircraft traffic control frequencies.

Devices intended to manage digital TVs are being repurposed to intercept data from aircraft. Key f=978-1090 MHz.







Loss of Control

As traditional radar is replaced with GPS-based aircraft tracking (ADS-B), all you need is an air-traffic receiver (Mode-S) to monitor the local airspace like a ground station. Private worldwide networks of these receivers now exist.

Motivators

Several national and international agencies have called for the hardening of our critical air-traffic control infrastructure. Some have proposed changes, but they don't always agree on what should be done.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF SCIENCE AND TECHNOLOGY POLICY

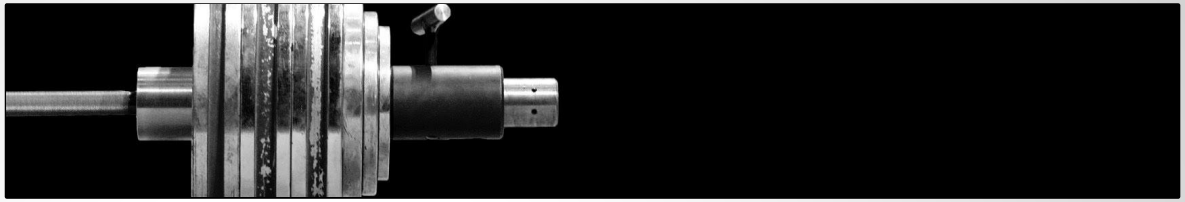
AIAA
Shaping the Future of Aerospace

ICAO • OACI • ИКАО
国际民航组织 • ايكاو

Goals & Objectives

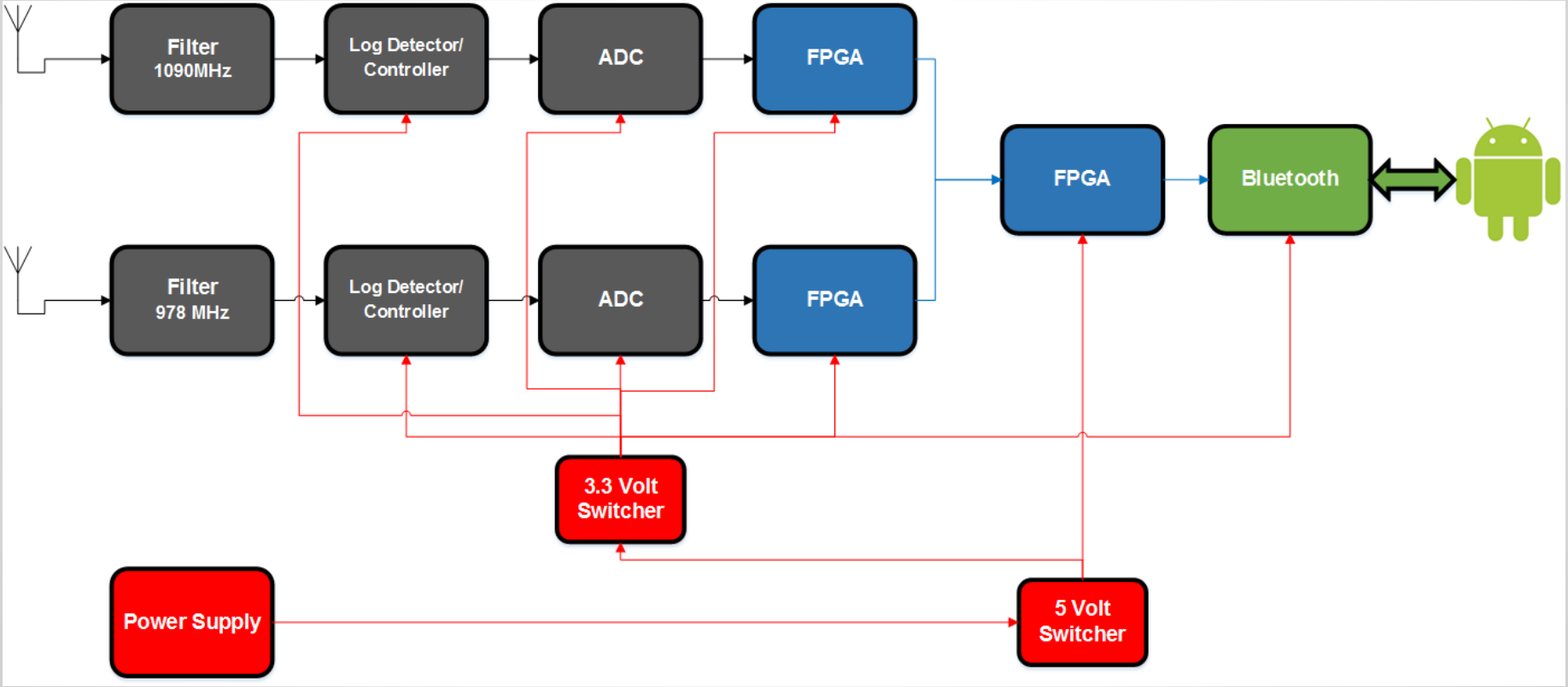
- Develop tuned antennae for the ADS-B frequencies.
- Develop a dual-frequency, programmable, microwave (Mode-S) receiver to capture and decode the ADS-B data stream.
- Transmit the data to an Android device via Bluetooth.
- Develop Android software to organize the data for geographical display.
- Develop encryption/decryption software to simulate how the ADS-B data could be protected.

Specifications



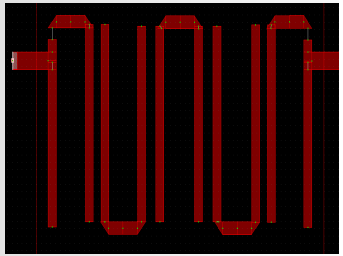
Category	Description	Target(s)
Antennae	Two frequency-tuned, coaxial, collinear masts housed in rigid plastic tubing.	f=978 MHz, f=1090 MHz.
Receiver	Dual frequency (non-tunable) microwave receiver with a large capacity for custom signal processing.	>= -25dB signal reception for an estimated range of 100 km.
Power	Battery powered.	>= 1-hour active operation.
Response	Continuously decoded/decrypted position and altitude information with minimal delay.	<= 5-second delay from reception to display.
Weight	Entire system to be carried by one person.	<= 25 lbs. (Luggable).
Cost	Low cost, (though the initial prototype may be of higher cost.)	<= $500.00

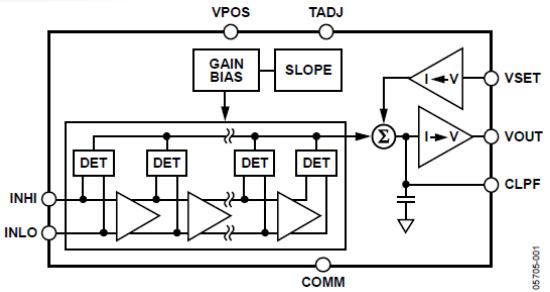
Overall Block Diagram

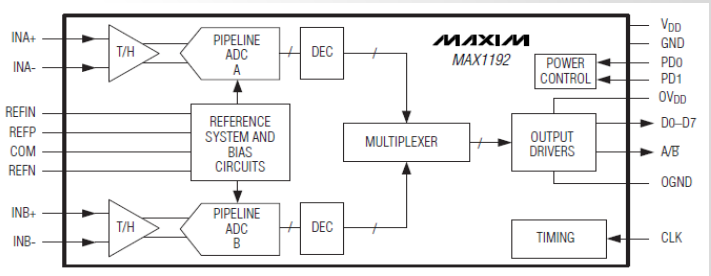


Design Approach

Tune the antennae and build a receiver using RF Detectors, ADCs, and FPGAs (rather than an SDR approach) to increase sensitivity and introduce customizable signal processing logic.

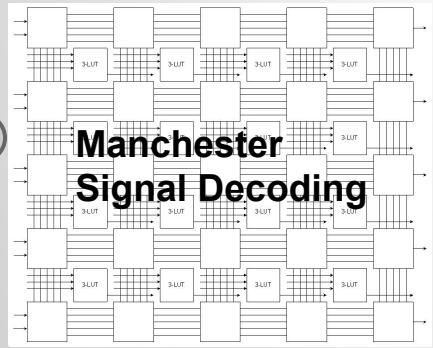


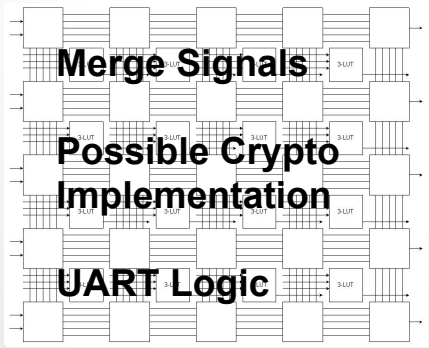


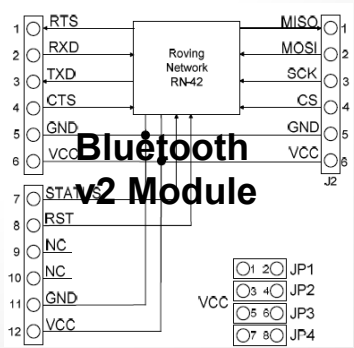


A

A

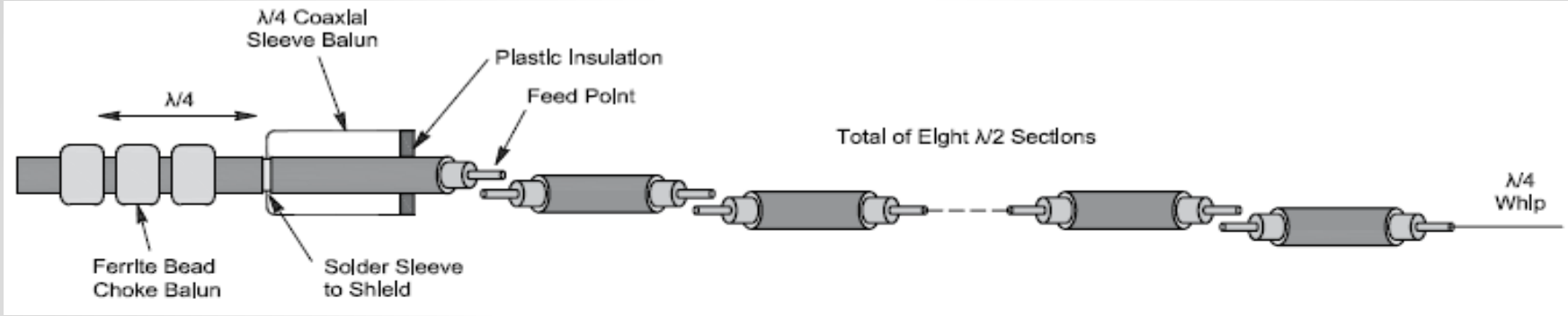




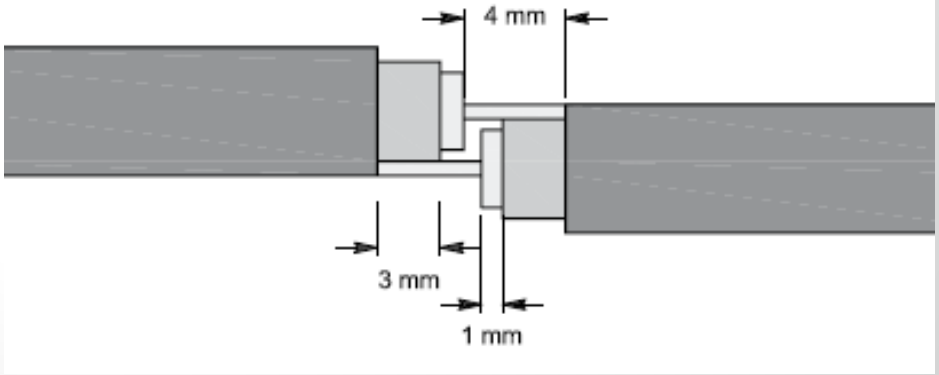


Antennae

Antennae will be stacked vertically to limit interference. In Coaxial Collinear (CoCo) Design, the lengths of the segments are specific to the frequency of the signal to be received.



Alternating the current distribution between the core and the shield in half-wavelength sections drives it to become cophasal. This yields the radiating current and a relatively large gain.

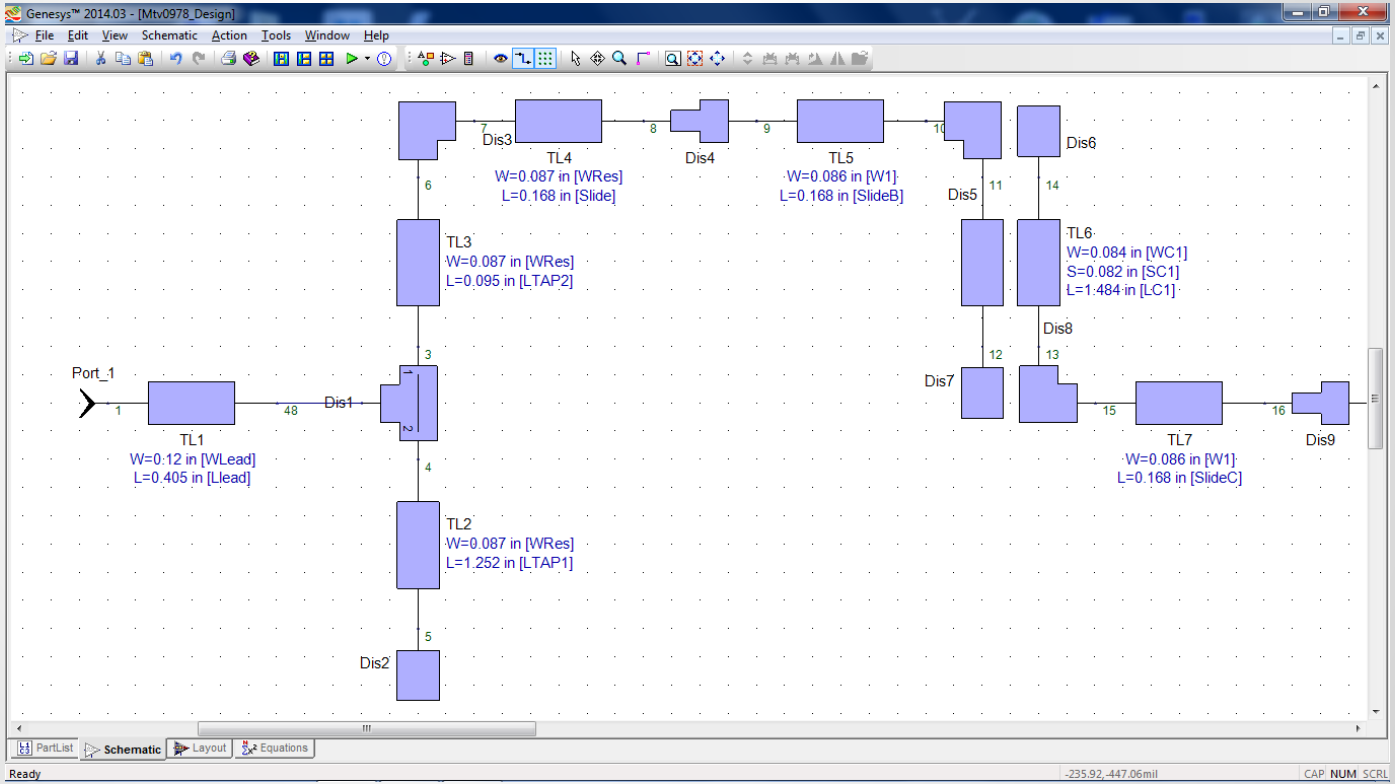


Filters

The high frequency of the desired signals prevents the use of discrete components. A transmission line model is used to design the filter and hairpin microstrips are used to build it.

This is one of three pages of the schematic for 978 MHz. The input port is shown on the left.

The other pages are omitted for brevity.



Filters Challenge

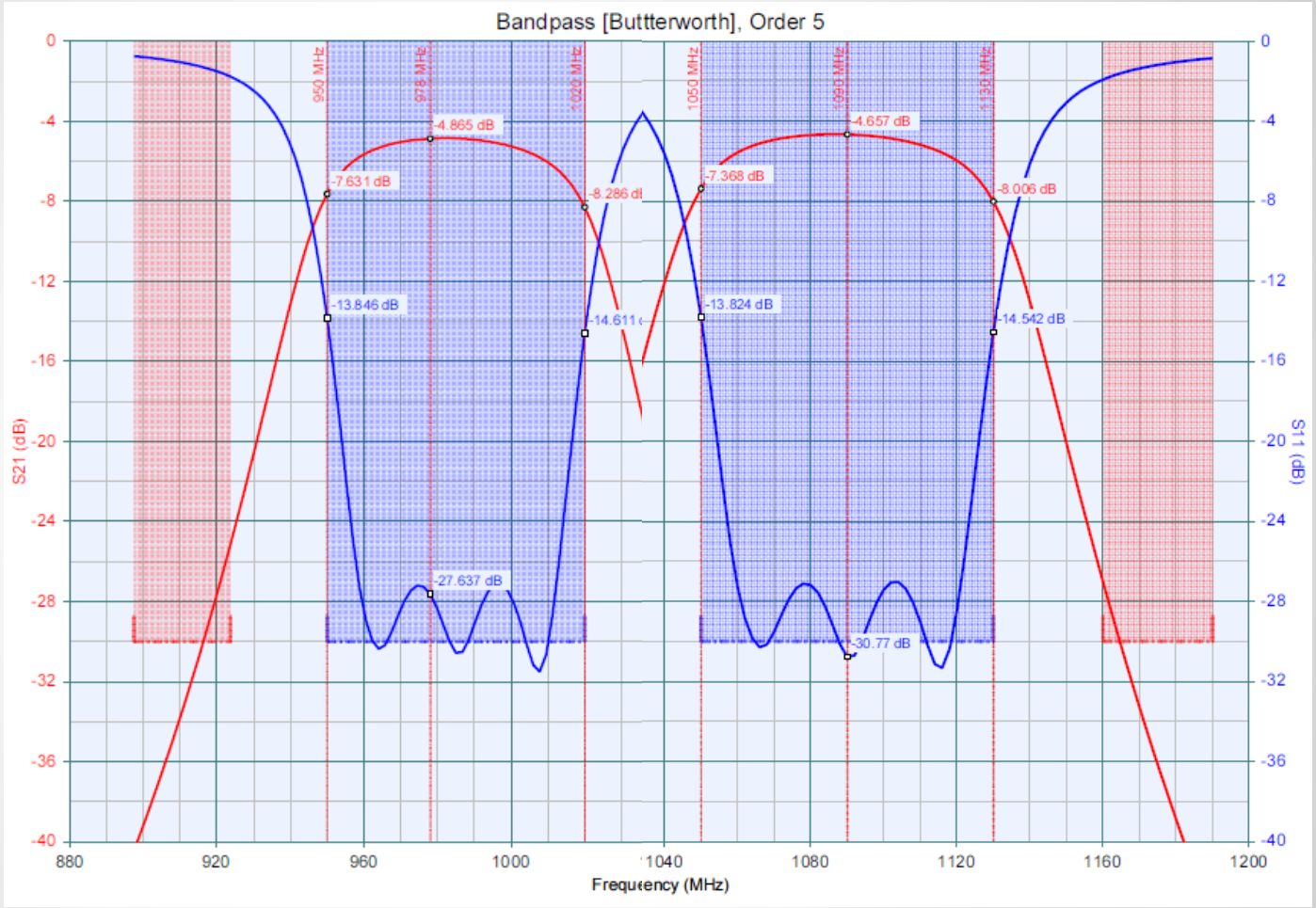
The completed, narrow BPF is of the 5th-order and adheres to a symmetric design. The actual size of the filter is roughly 3.75 x1.80 in. The 1090 MHz filter is slightly smaller.

Finding useful software to model the filters and generate the layout was a challenge and resulted in an additional sponsor:

Keysight (Agilent)

Filters

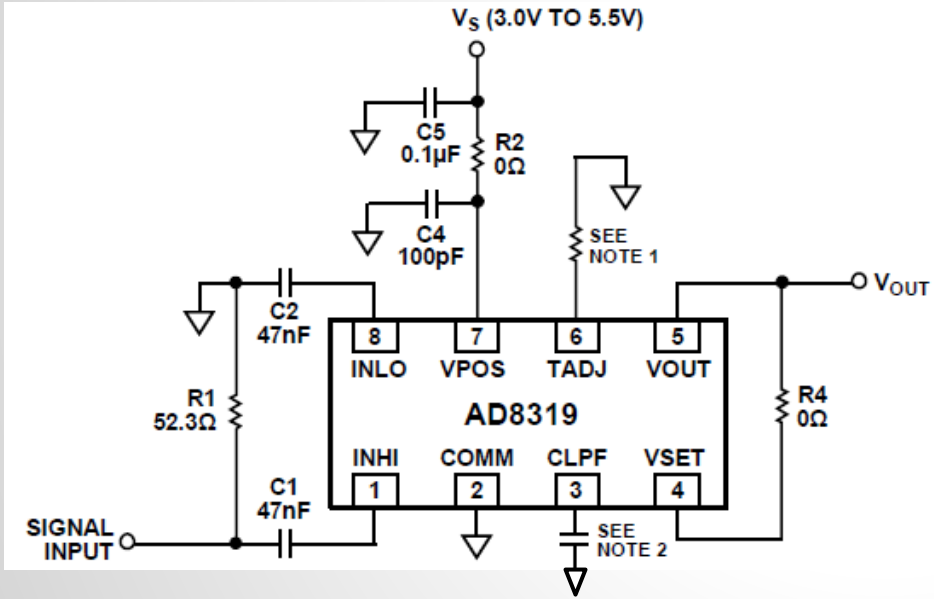
I was reluctant to squeeze my BPFs any more narrow than this ~75 MHz range due to the variable dielectric constant of the PCB laminate. Quality laminates are out of budget range for Senior Design.



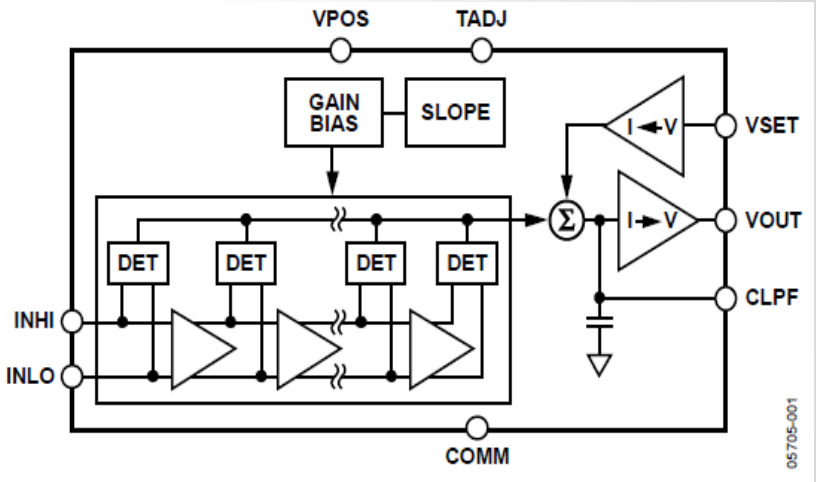
RF Detector

Analog Devices 8319 is a demodulating logarithmic RF power detector. It converts a wide-range, low-power RF input signal to a smaller-scale DC output.

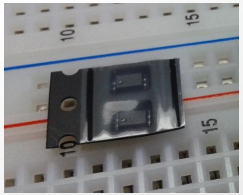
External



Internal



Actual



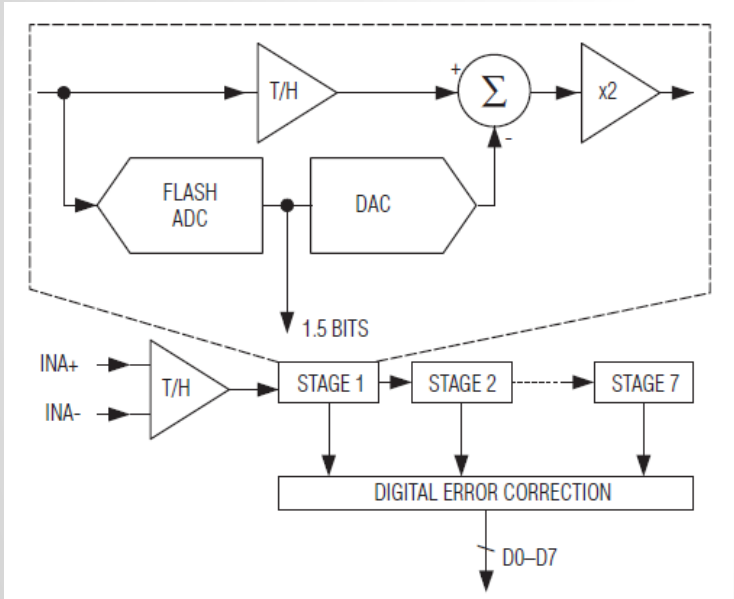
Fall/Rise response times of 6ns/10ns enables very fast voltage changes in DC output.

(Two DFNs in cut tape).

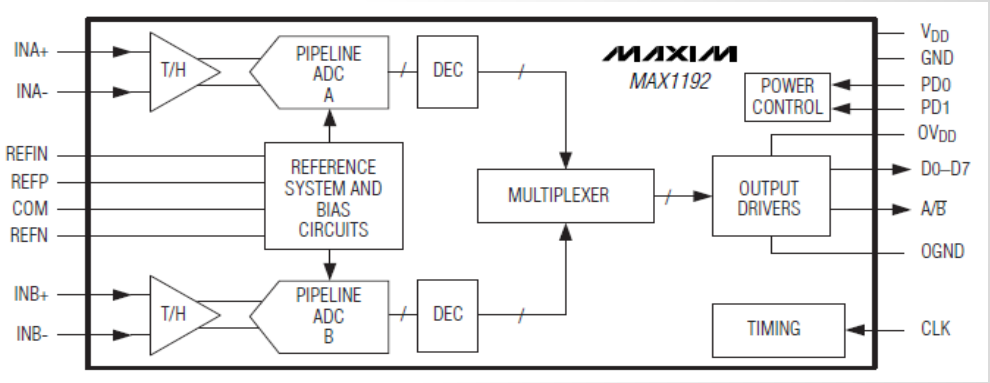
ADC

Maxim Integrated 1192 is a high speed analog-to-digital converter. At this point, our input signal is single-ended DC in the 0.5v to 1.5V range. After this step, it's 8 digital logic lines.

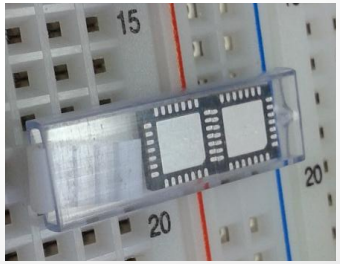
Internal-1



Internal-2



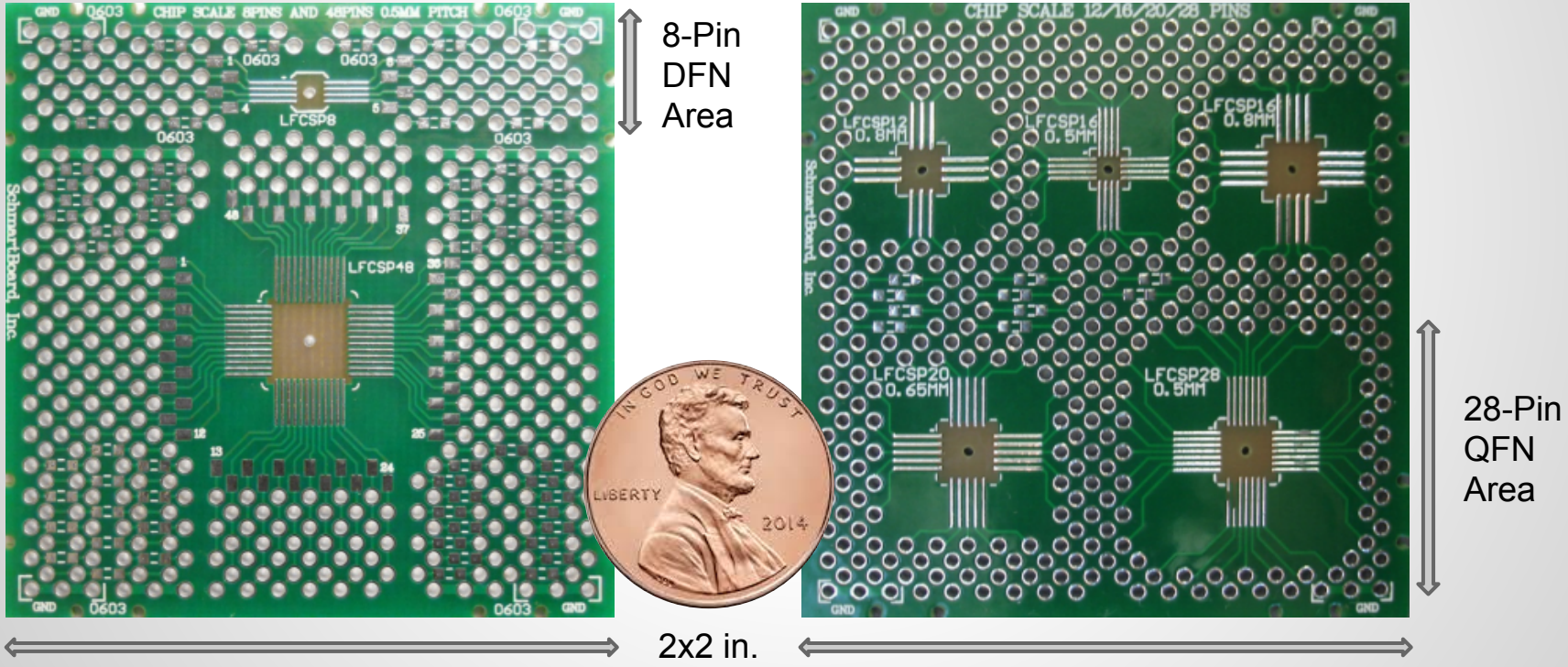
Actual



(Two QFNs in a tube).

Mounting Challenge

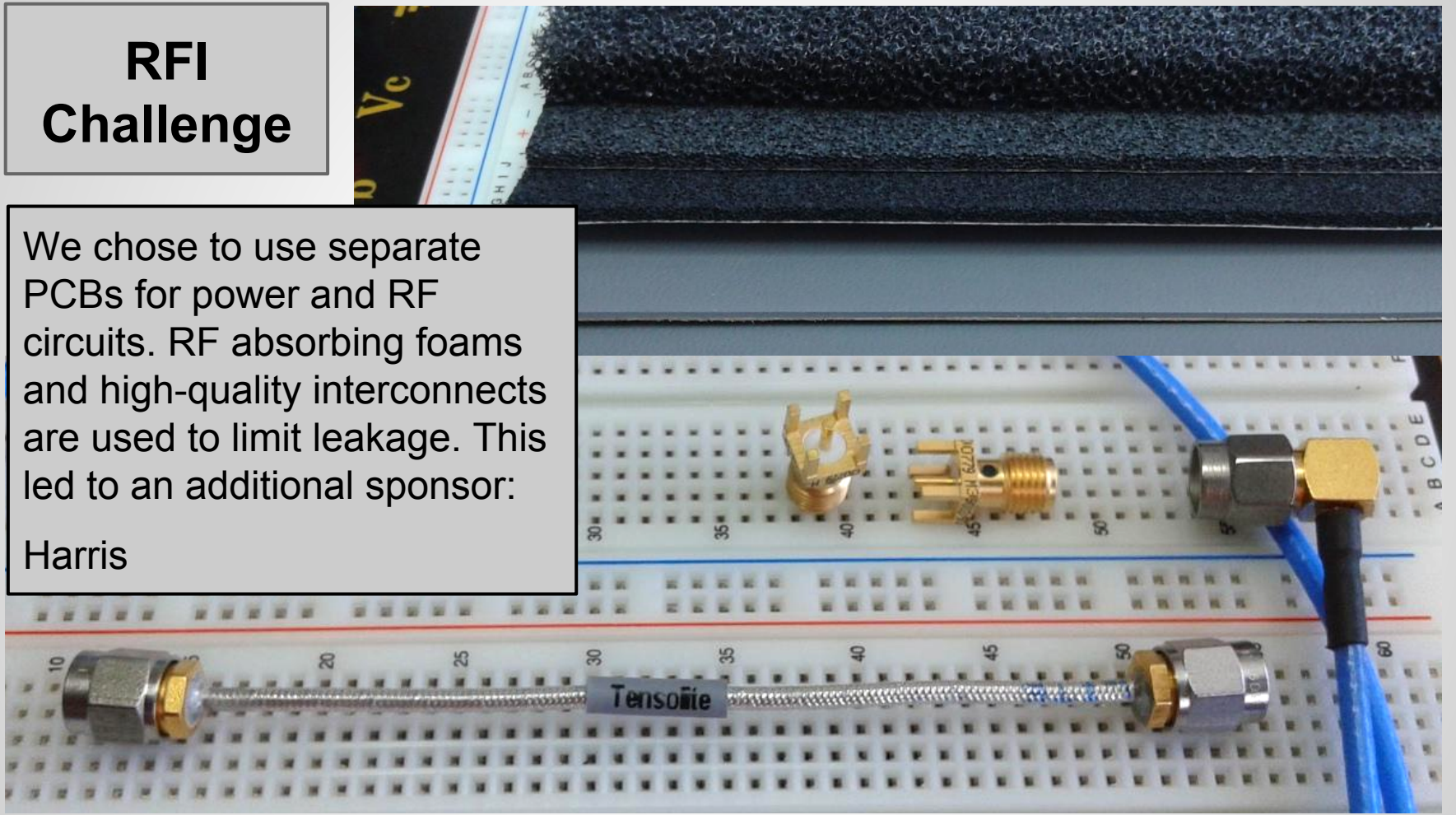
Schmartboards are pre-built, empty breakout boards for hand-soldering very small IC packages that were intended for machine mounting methods.



RFI Challenge

We chose to use separate PCBs for power and RF circuits. RF absorbing foams and high-quality interconnects are used to limit leakage. This led to an additional sponsor:

Harris

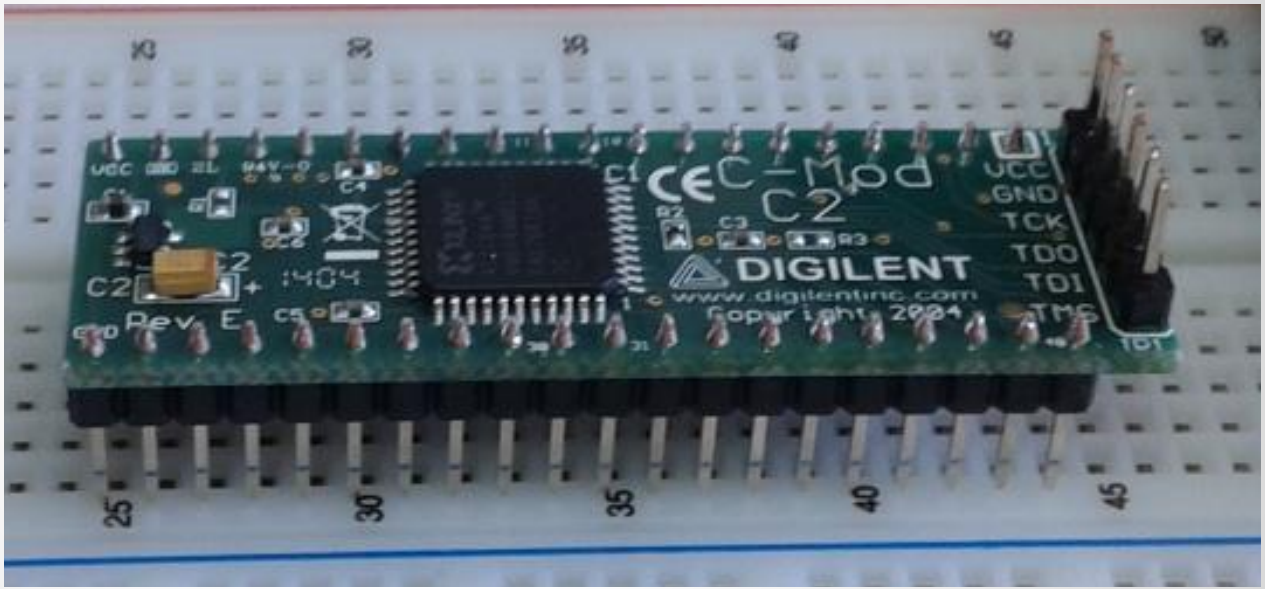


Manchester Decode

The ADS-B data stream must first be decoded before its content can be evaluated. One small FPGA follows each ADC to address this need.

The dual-inline packaging format of this FPGA breakout board simplifies testing and the physical programming of the device.

A JTAG interface header is used for programming.



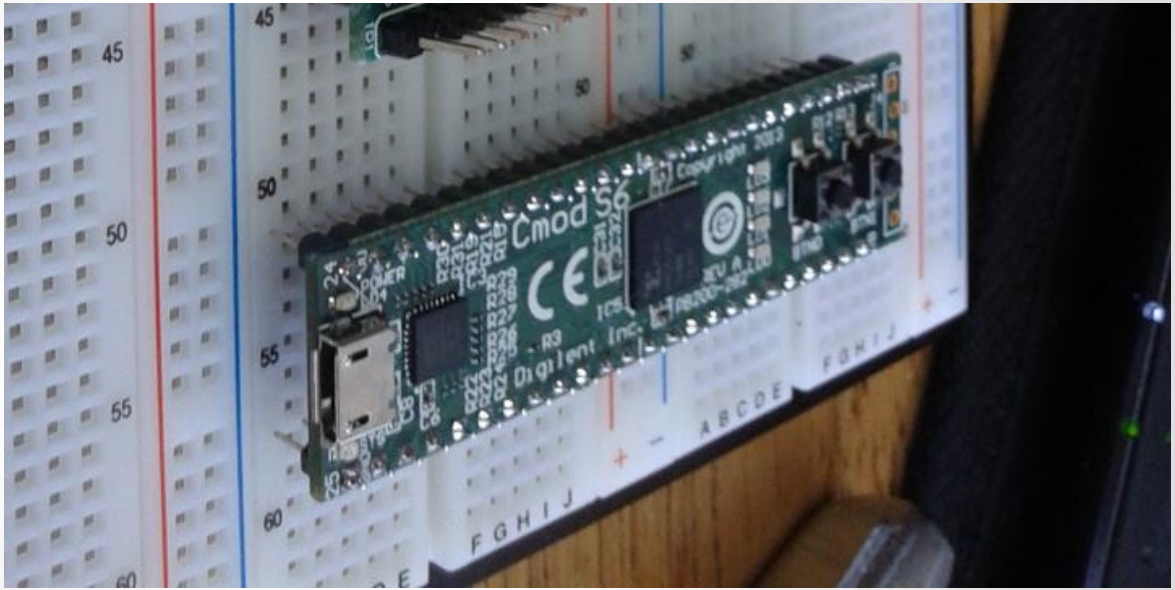
Xilinx XC2C64 in a 2.16 x 0.7 in. DIP package

Signal Merge

Before the two decoded data streams can be sent to the Android device for final processing, they must be sequenced, merged, and then buffered for a standard UART interface.

As time permits, some crypto-graphic functions may be located here for testing.

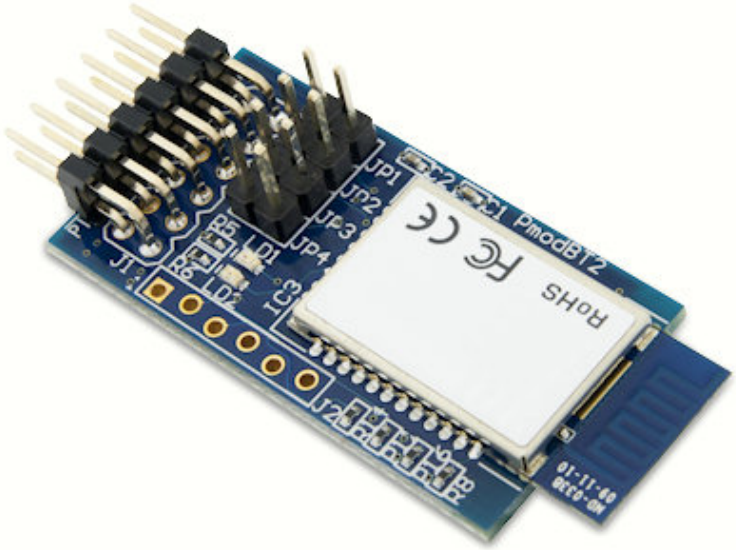
This package uses a USB programming interface.

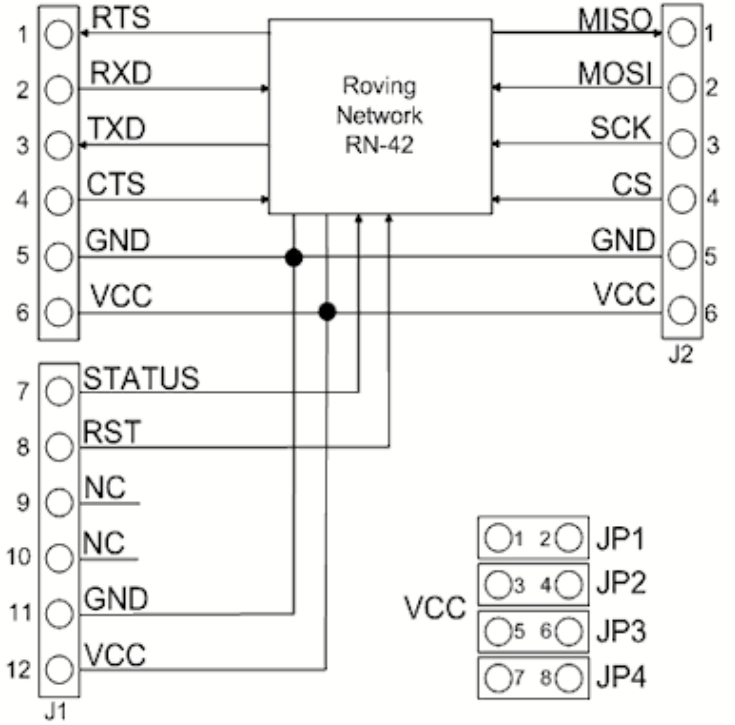


Xilinx XC6SLX4-2CPG196 in a 2.6 x 0.7 in. DIP package

Bluetooth Module

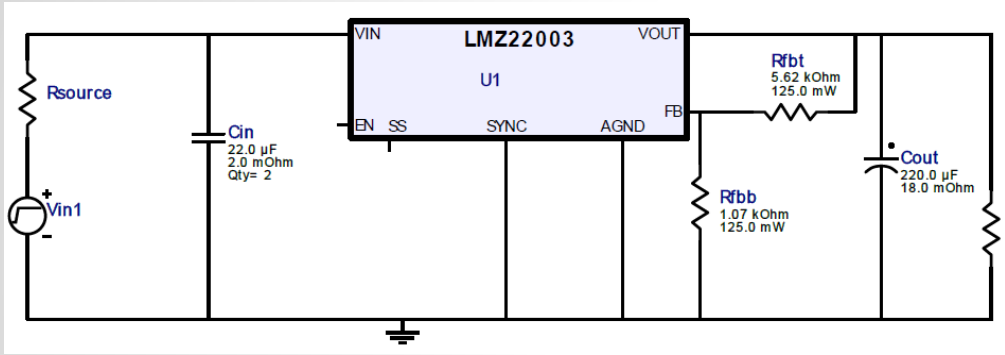
Digilent PmodBT2 receives the processed data stream and transmits the data to a connected Android device.





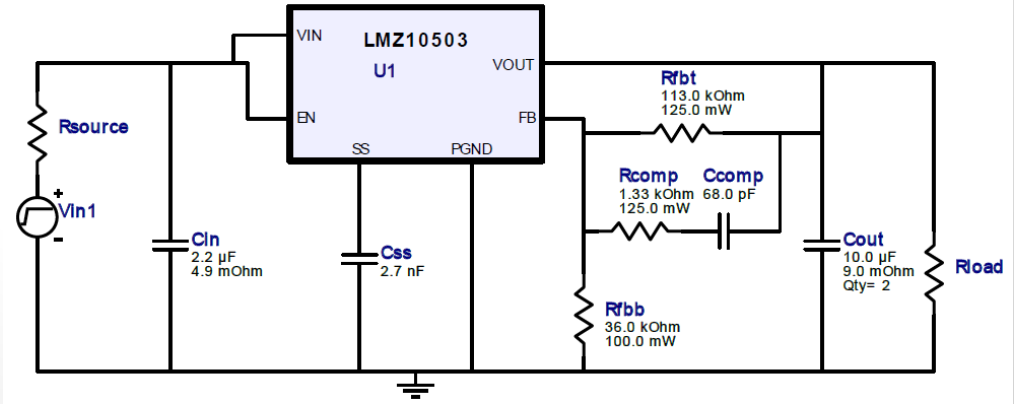
Power Circuit Diagram

The circuits below will be used to connect the receiver to the power supply.



Circuit A -- 12V to 5V

Circuit B -- 5V to 3V3

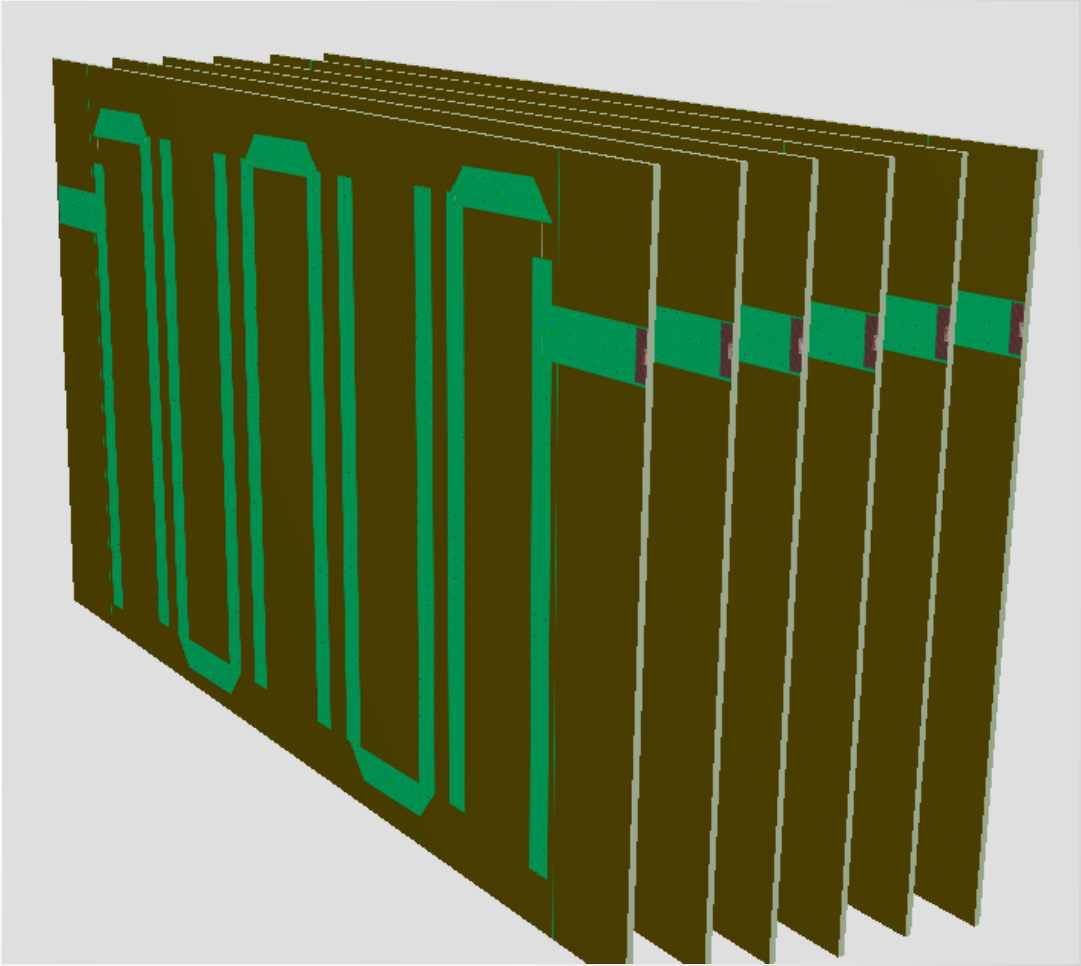


Stacked PCBs

1. Power Board
2. 1090 MHz Filter (RF1)
3. 978 MHz Filter (RF2)
4. RF1 and RF2 to Digital
5. Digital Logic to UART

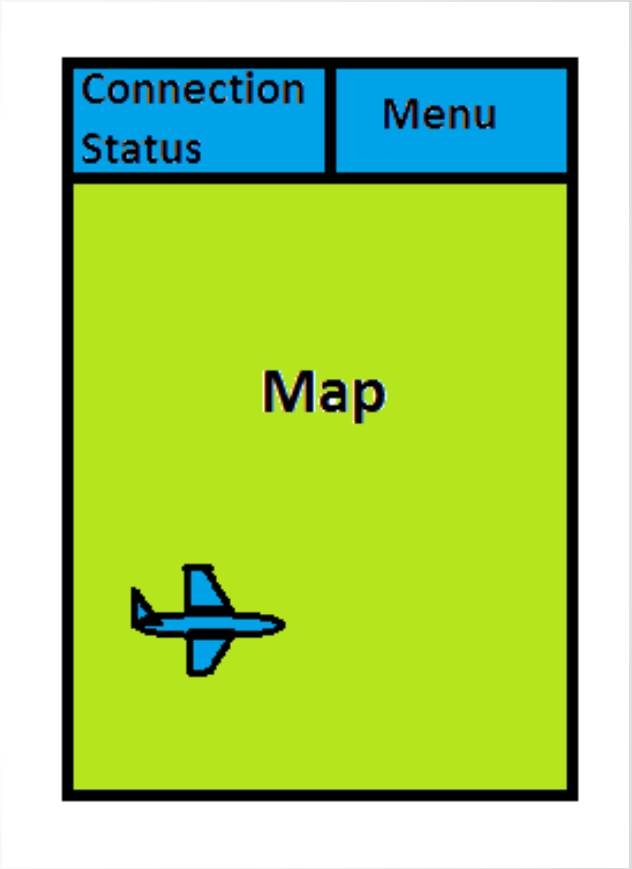
❏ Bluetooth Module

Allows independent ground planes and space for RF foam or shielding. Requires high-quality interconnects.

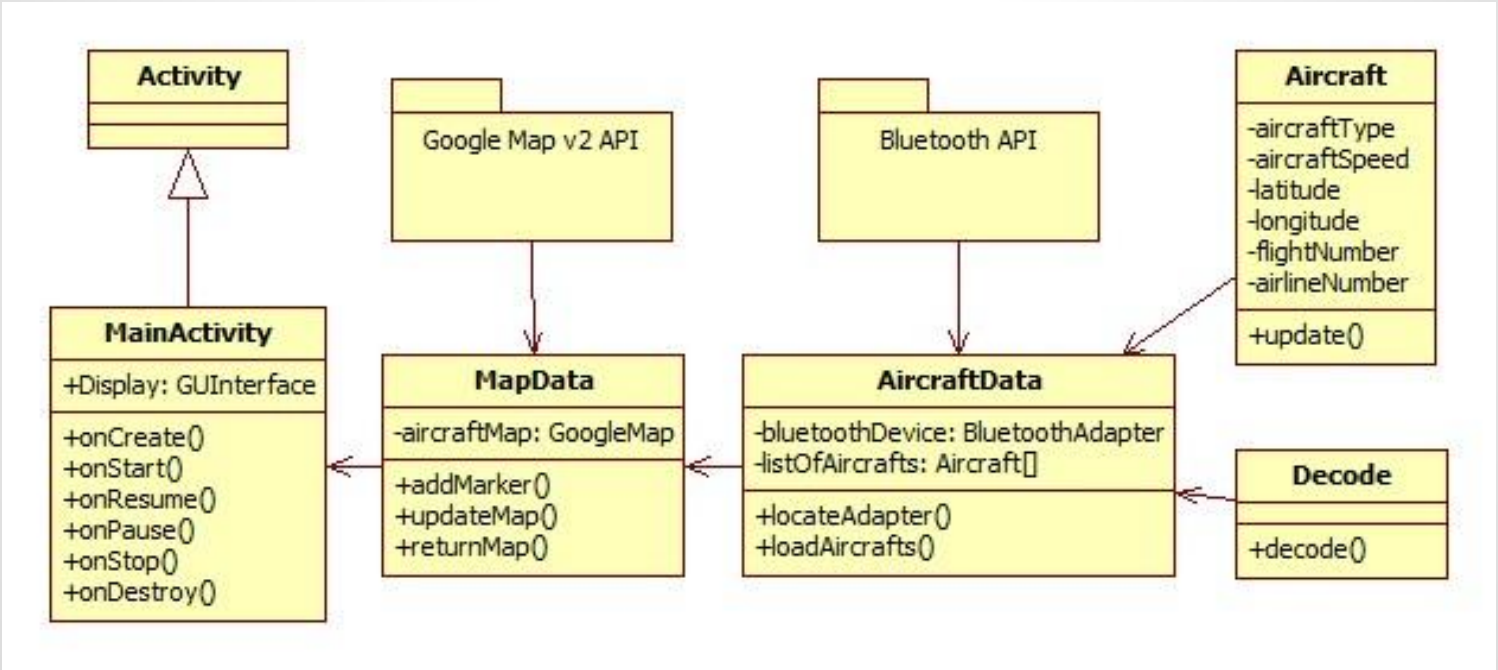


Mobile Application Features

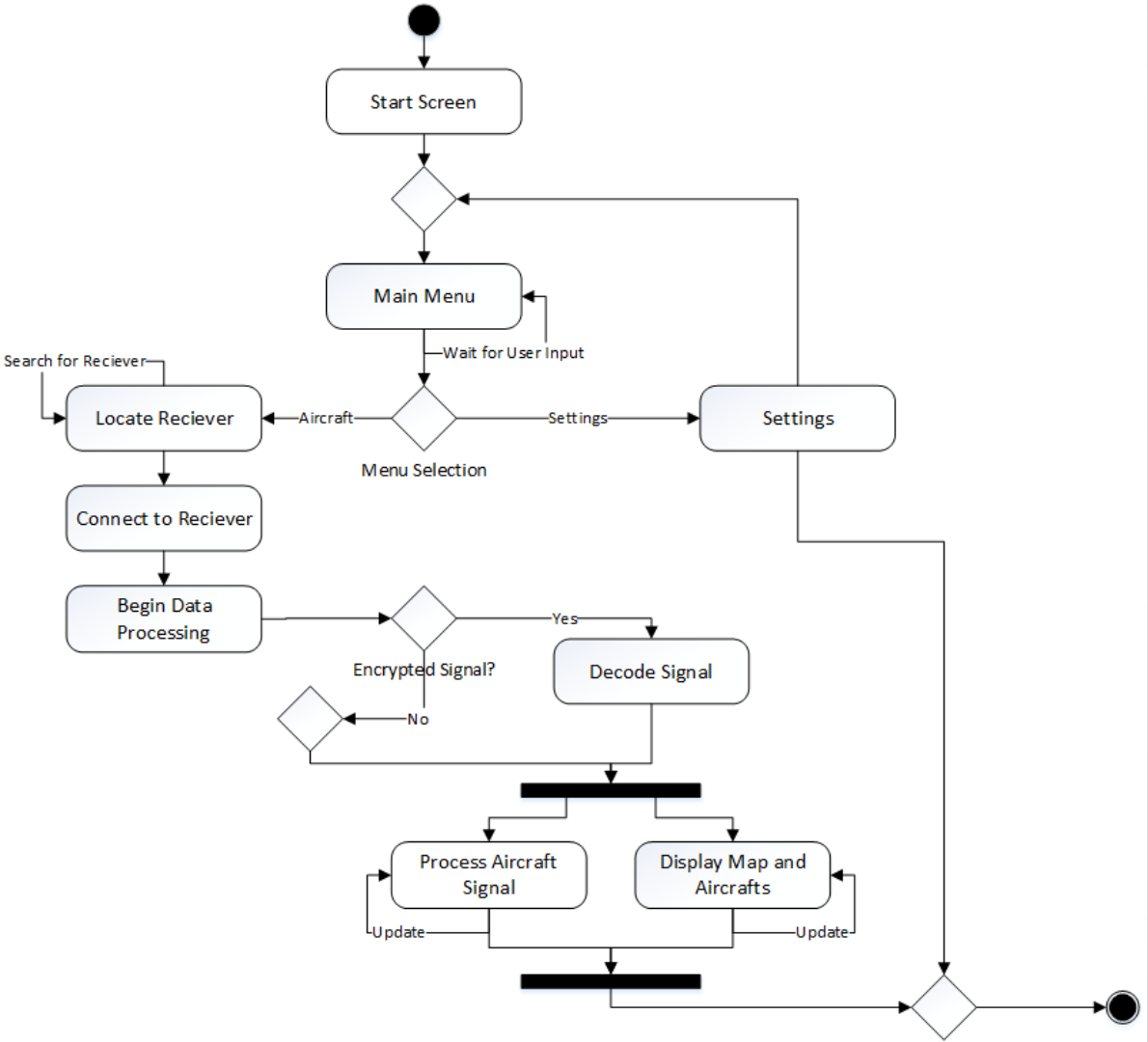
- Selection of tracking a specific aircraft
- Automatic adjustment to current location
- Manual control over viewable airspace
- Display all aircrafts within range of antenna



Class Diagram



Application Overview



ADS-B Format

ADS-B message format is referred to as extended squitter.

Message Type	Surveillance-Control	Extended Data*	ICAO Code +
5-bits	27-bits	56-bits (Format depends on message type).	24-bits

	Capability 3-bits	Largest Possible Encryption Target 104-bits

- Airborne Position Squitter
- Surface Position Squitter
- Airborne Velocity Squitter
- Aircraft Identification Squitter

- DO-260A State and Status

★ The ‘squitters’ we need occupy the extended data field one by one.

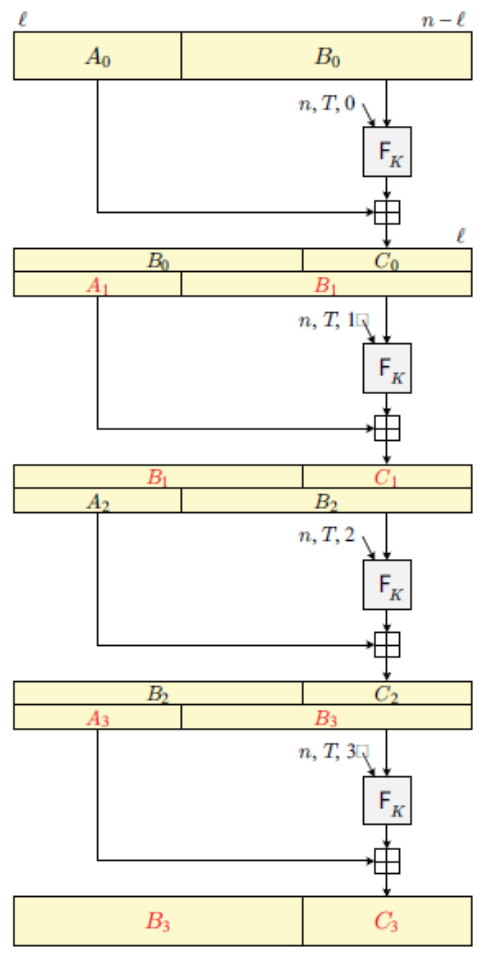
ADS-B Data Stream Encryption/Decryption

ADS-B broadcast strictly prohibited.

A test program will run on Android to capture the data stream and encrypt it as test data.

Encryption will be a modified version of the FFX algorithm. FFX is a format-preserving encryption (FPE) scheme.

The encrypted test data will be input to the Android aircraft-tracking display software.



FFX encrypts encrypted data to compensate for the inherent weakness of matching input and output data size.

The underlying encryption will start simple (XOR), and as time permits further testing, it will increase in complexity.

Summary of Major Design Decisions

- Antenna design choice
  - Two tuned antennae (CoCo) vs alternatives.
- Software Defined Radio vs an explicit ADC/FPGA
  - ADC/FPGA was selected to implement a fully programmable system.
- PCB organization/interconnects
  - Separate PCBs to better manage RFI.
- Interface options
  - Bluetooth transmission to Android.
- Encryption options
  - Format-Preserving encryption based on FFX.

Work Distribution

	Antenna	Filter	RF Detector/ ADC	FPGA	Bluetooth	Power Supply	Android Application
Mike		☆	☆	☆		☆	
Long			☆		☆	☆	☆
Sean	☆	☆					☆

Budget

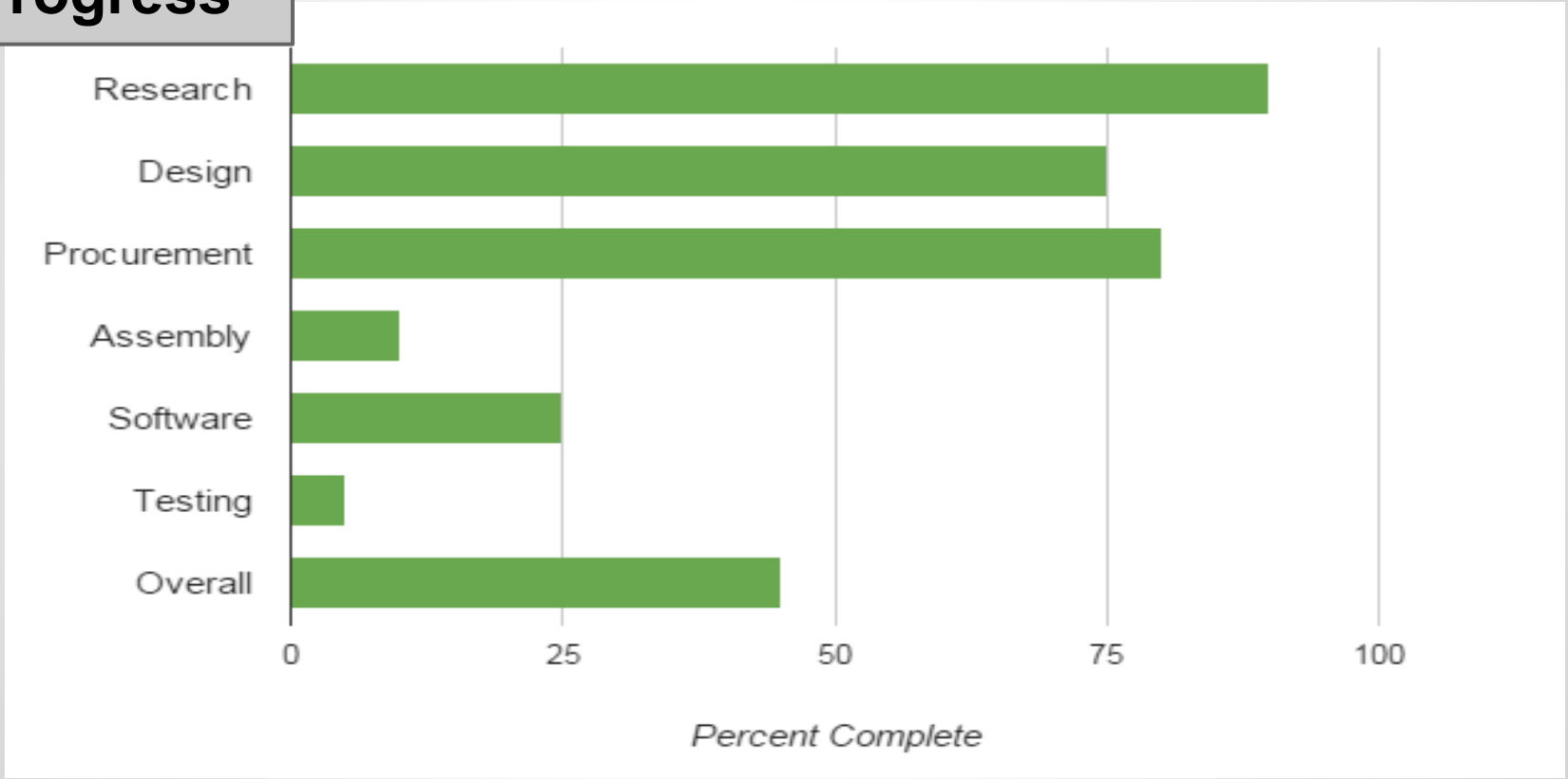
$ $

Original Estimates	
Battery	$ 32.00
Power Supply Circuits	$ 25.00
Antenna Hardware	$ 65.00
RF Receiver Circuits	$ 45.00
ADC	$ 102.00
Decoder FPGA	$ 75.00
USB or Wireless Interface	$ 45.00
Custom Printed Circuit Board	$ 105.00
Total Est.	**$ 494.00**

Comparison Costs to Date	
Battery	N/C
Power Supply Circuits	$ 34.60
Antennae Hardware	$ 13.35
RF Receiver Circuits	$ 90.37
2 RF Det. + 2 ADC	$ 93.51
3 FPGAs	$ 119.00
Bluetooth Interface	$ 68.99
PCBs / Enclosure	pending

Unanticipated Costs to Date	
Chemicals, Tools	$ 150.57
Shipping	$ 80.70
Tax	$ 8.20
RF Shielding/Interconnects	Harris
RF Filter Software	Keysight
Harris contribution, $227.20 in parts.	
Keysight Genesys license, $Thousands.	
Additional antennae costs are pending.	
Total Costs to Date	**$ 659.29**
Overbudget	**$ 165.29**

Current Progress



Immediate Plans

Hardware Phase (3-weeks):

- Complete the layout of the remaining PCBs and order them.
- Acquire the antennae housings and PCB enclosure.
- Find or rent test equipment to verify antennae performance.
- Complete parts assembly and initial hardware testing.

Software Phase (all remaining time):

- Complete ADS-B decoding and signal merge logic.
- Finish and test Android application.
- Complete encryption test software.
- Finish and test decryption feature.

RADIO FREQUENCY SPECTRUM

MICROWAVE AND RADAR USAGE UNITED STATES	OFFICIAL JCS BAND DESIGNATION	OFFICIAL ITU/GENEVA BAND DESIGNATION	MILITAR APPLICAT
W-BAND 56,000-100,000	M 60,000-100,000	BAND NO.11 EHF 30,000-300,000	MILSTAR E COMMUNIC
V-BAND 46,000-56,000	L 40,000-60,000		
Q-BAND 36,000-46,000		MILLIMETRIC	
K_a 33,000-36,000	K 20,000-40,000		
K-BAND 10,900-36,000			
K_u 15,250-17,250	J 10,000-20,000		SHF SUBM SATCOM D INTELSAT
	I 8,000-10,000	BAND NO.10 SHF 3,000-30,000	
X-BAND 6,200-10,900	H 6,000-8,000		SHF DSCS
C-BAND 5,200	G		
3,900 - 6,200	F		
	E		
	D 1,000-2,000		JTIDS/IFF/GPS
L-BAND 390-1,550	C 500-1,000	BAND NO.9 UHF 300-3,000	
P-BAND 225-390	B 250-500	DECIMETRIC	
G-BAND 150-225		BAND NO.8 VHF 30-300 METRIC	
I-BAND 100-150	A 0-250		
		BAND NO.7 HF 3-30	
	3-30 MHz		
	300-3,000 kHz	BAND NO.6 MF	
	30-300 kHz	BAND NO.5 LF	
	3-30 kHz	BAND NO.4 VLF	
	300-3,000 Hz	BAND NO.3 VF	
	30-300 Hz	BAND NO.2 ELF	

7,000
6,000
5,000
4,000
3,000
2,000
1,000 (1 GHz)
30 Hz

Questions?