This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2022-7707C

LEGRange

ISM-Band Pseudolite Network for GPS Security Research

Daniel Payne
Dr. Nathan Green
LeTourneau University

LeTourneau University

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

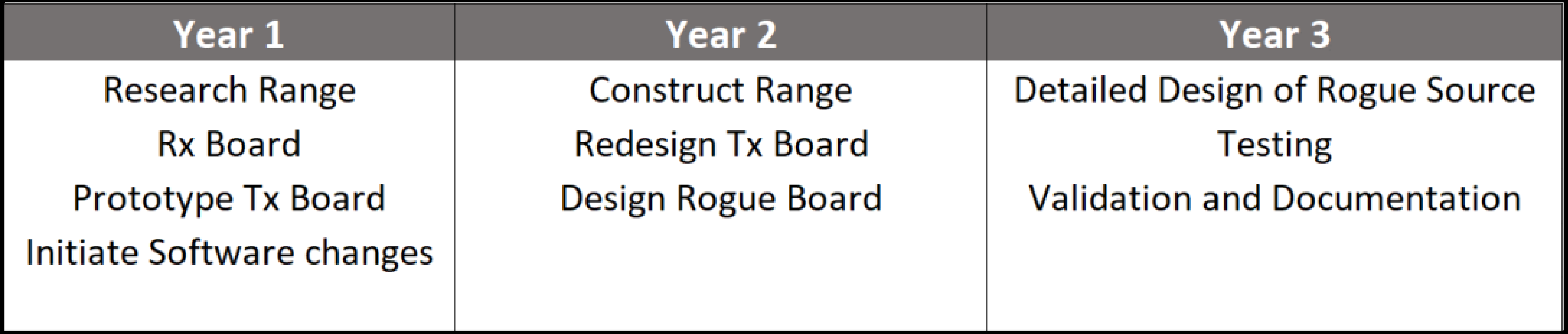
Why LeTourneau? Why LEGRange?

- There is a grave shortage of PNT trained engineers
- LeTourneau is a Primarily Undergraduate Institution (PUI) with a M.S. program
- Lab focus is PNT, SDR, and Estimation theory
- Graduates now at Raytheon, L3, Garmin, USAF, Rice University, Auburn University, Sandia National Labs

LeTourneau University

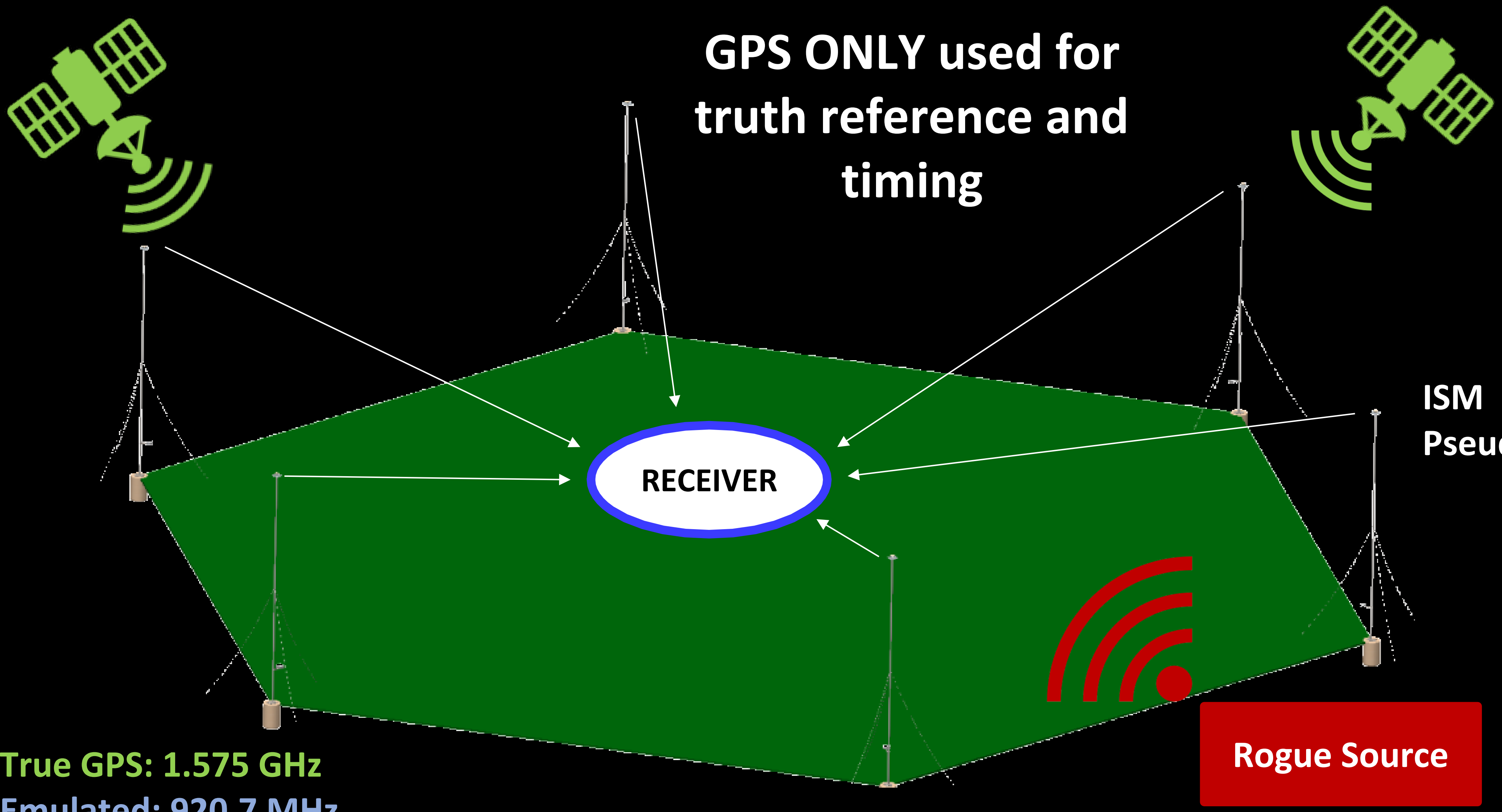
LEGRange

- Project Scope: Develop a wireless, license-free, navigation security testing platform with a non-GPS rogue source and analysis software.
  - Three-year research effort executed by 3 Senior Design teams and 2 M.S. students



Year 1	Year 2	Year 3
Research Range Rx Board Prototype Tx Board Initiate Software changes	Construct Range Redesign Tx Board Design Rogue Board	Detailed Design of Rogue Source Testing Validation and Documentation

System Overview



GPS ONLY used for truth reference and timing

RECEIVER

ISM Pseudolite

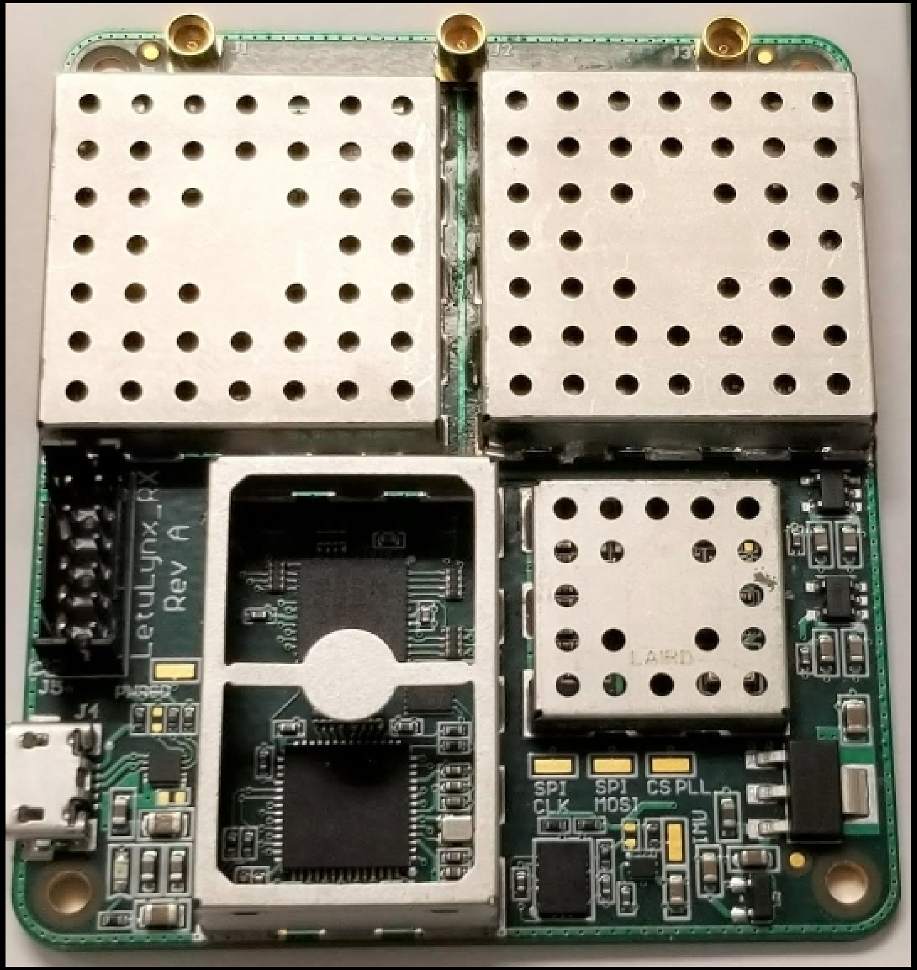
Rogue Source

True GPS: 1.575 GHz

Emulated: 920.7 MHz

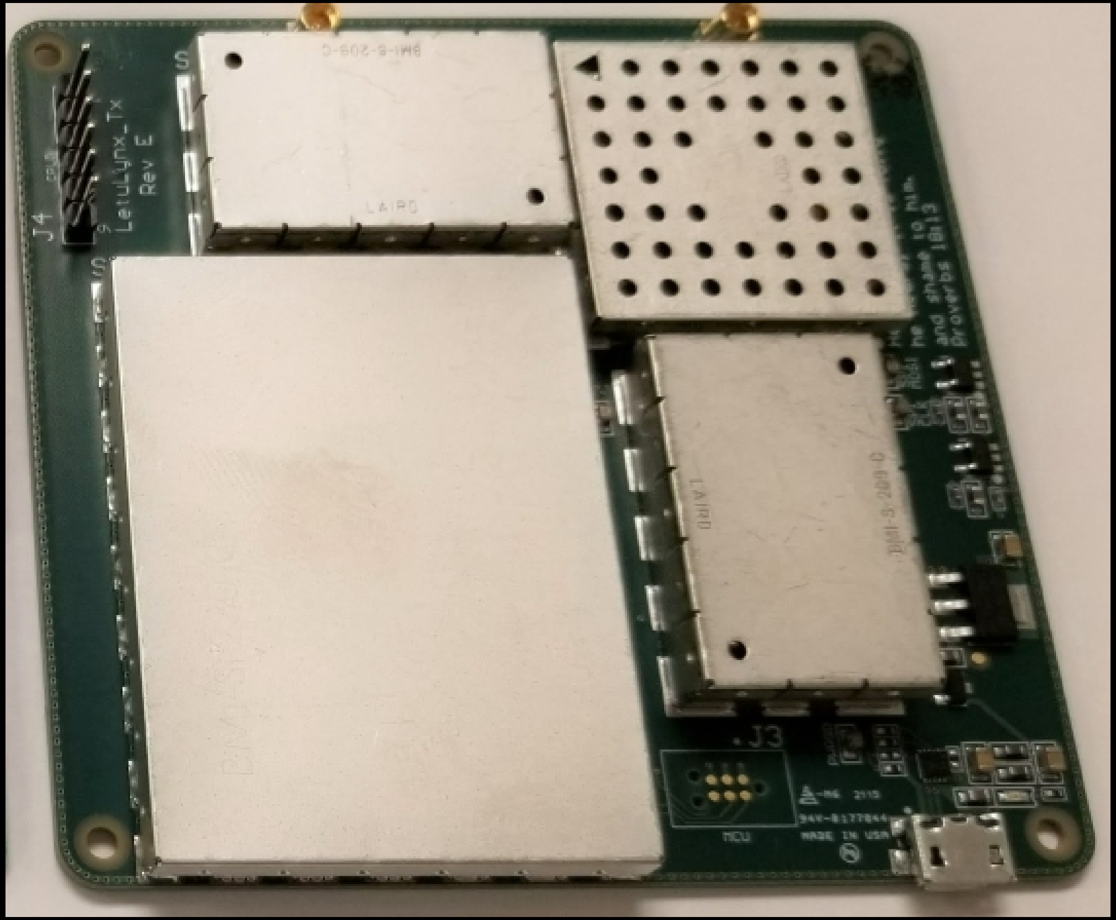
Dual GPS-ISM Receiver Design

- Process GPS as truth reference
- Mix ISM signal up to GPS L1 and process with identical receiver chain
- USB 2.0 interface to PC
- Process both with the pprx SDR licensed from UT Austin Radionavigation Lab
- Coherent clocking from TCXO

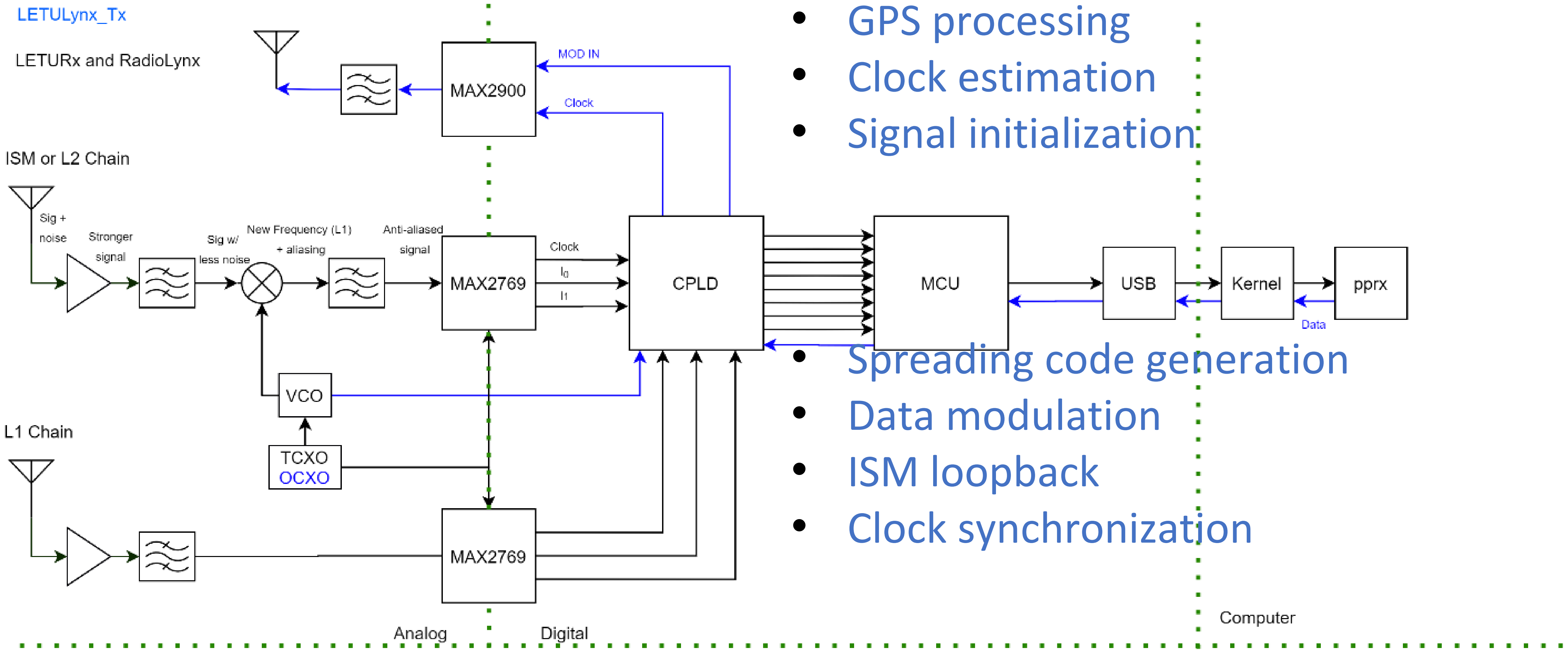


ISM Pseudolite Concept

- Broadcast a GPS-like signal at 90x10.23 MHz
- Different carrier
- L1-like PRNs (but not specific GPS L1 PRNs) using a similar BPSK signal structure
- Simplified (non-GPS) nav message unique to ISM band – leverages Subframe 1 Nav data structure for ISM -band localization processes
- Use GPS to synchronize clocks
- Use OCXO for reasonably stable frequency standard



ISM RX/TX Block Diagram



- GPS processing
- Clock estimation
- Signal initialization

- Spreading code generation
- Data modulation
- ISM loopback
- Clock synchronization

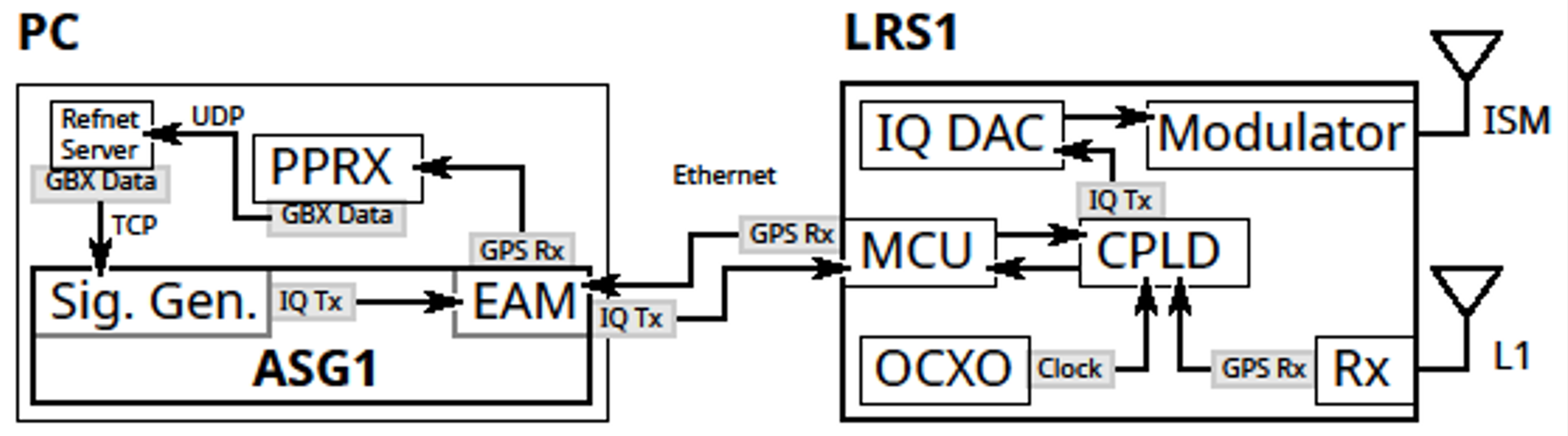
ISM Pseudolite Functional Allocation

MAX 2769	CPLD	MCU	MAX 2900	Software
GPS Mixing	Clock Division	Board Config	Modulation	GPS processing
GPS Filtering	Clock Distribution	Signal Buffering		Clock Estimation
GPS Sampling	Gen. ISM PRN Code	USB Interface		ISM-self tracking
	Apply ISM Nav Data bits			ISM Signal Init
	Re-init sig. gen.			
	Loopback ISM			
	Sample alignment			
	Nav Data			

ISM Pseudolite and ISM Receiver Testing

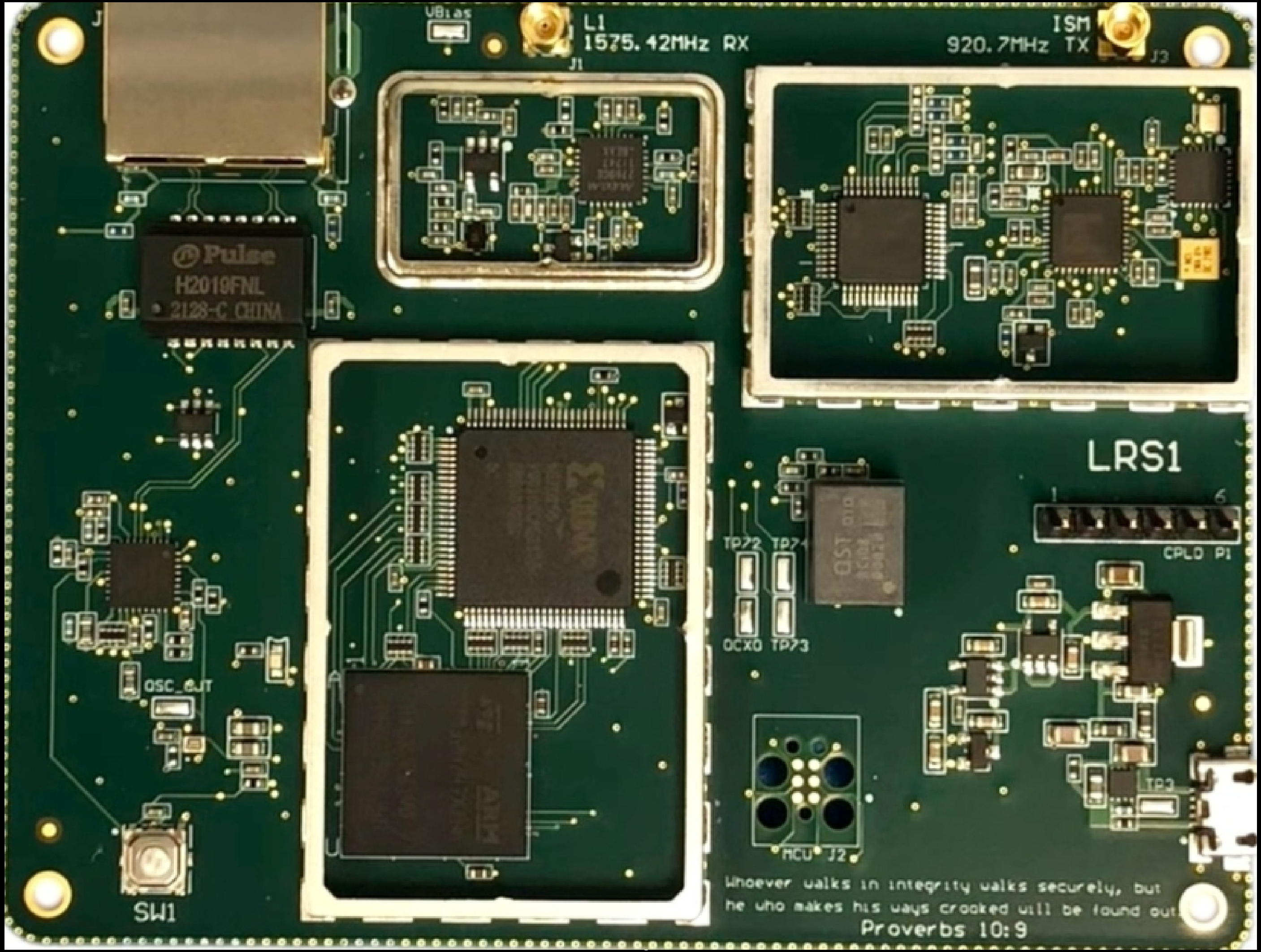
- ISM Receiver successfully acquires and tracks the ISM pseudolite transmitted signal
- Spectrum analyzer shows no out of band signal power
- Current limitation
  - USB DMA transfer rate too low, prevents full function of ISM pseudolite

ISM Rogue Source Block Diagram

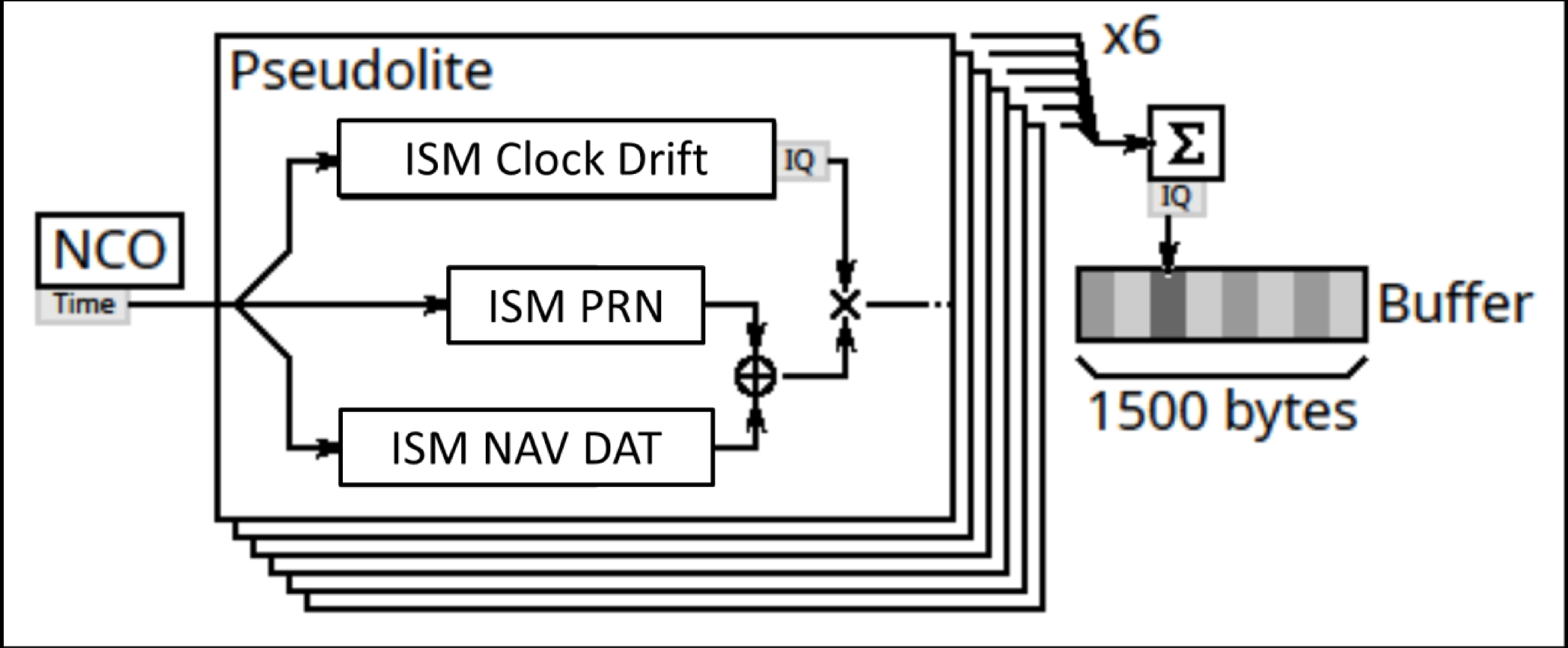


ISM Rogue Source PCB Design

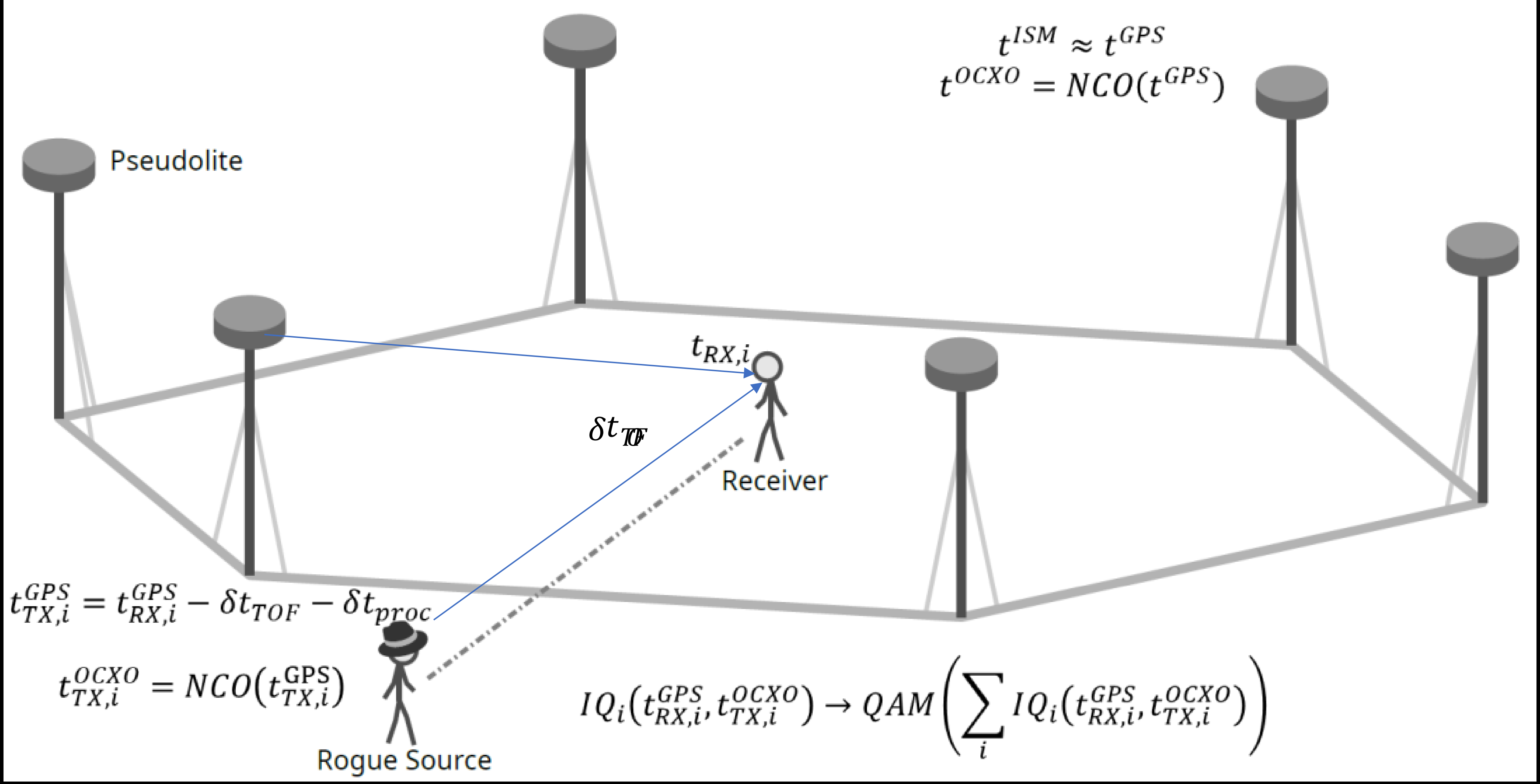
- L1 GPS Chain for Clock Synch
- Ethernet for full-duplex, high speed interface
- OCXO for frequency stability
- Custom QAM modulation for flexible signal transmission
- Programmable TX power level
- CPLD distributes clocks and aligns samples



ISM Baseband Signal Generation



ISM Rogue Source Signal Timing


$t^{ISM} \approx t^{GPS}$
$t^{OCXO} = NCO(t^{GPS})$
Pseudolite
$t_{RX,i}$
δt_{TOF}
Receiver
$t_{TX,i}^{GPS} = t_{RX,i}^{GPS} - \delta t_{TOF} - \delta t_{proc}$
$t_{TX,i}^{OCXO} = NCO(t_{TX,i}^{GPS})$
Rogue Source
$IQ_i(t_{RX,i}^{GPS}, t_{TX,i}^{OCXO}) \rightarrow QAM\left(\sum_i IQ_i(t_{RX,i}^{GPS}, t_{TX,i}^{OCXO})\right)$

Future Work

- Resolve ISM Psuedolite USB/DMA issues
- Finalize Full-Duplex Ethernet for ISM Rogue source
- Develop specific theoretical attacks
  - Tone, Swept CW jammers
  - Other