# P25: THE digital radio of public safety

Jon Suen, KG6K

Presentation for RARS, December 10, 2025

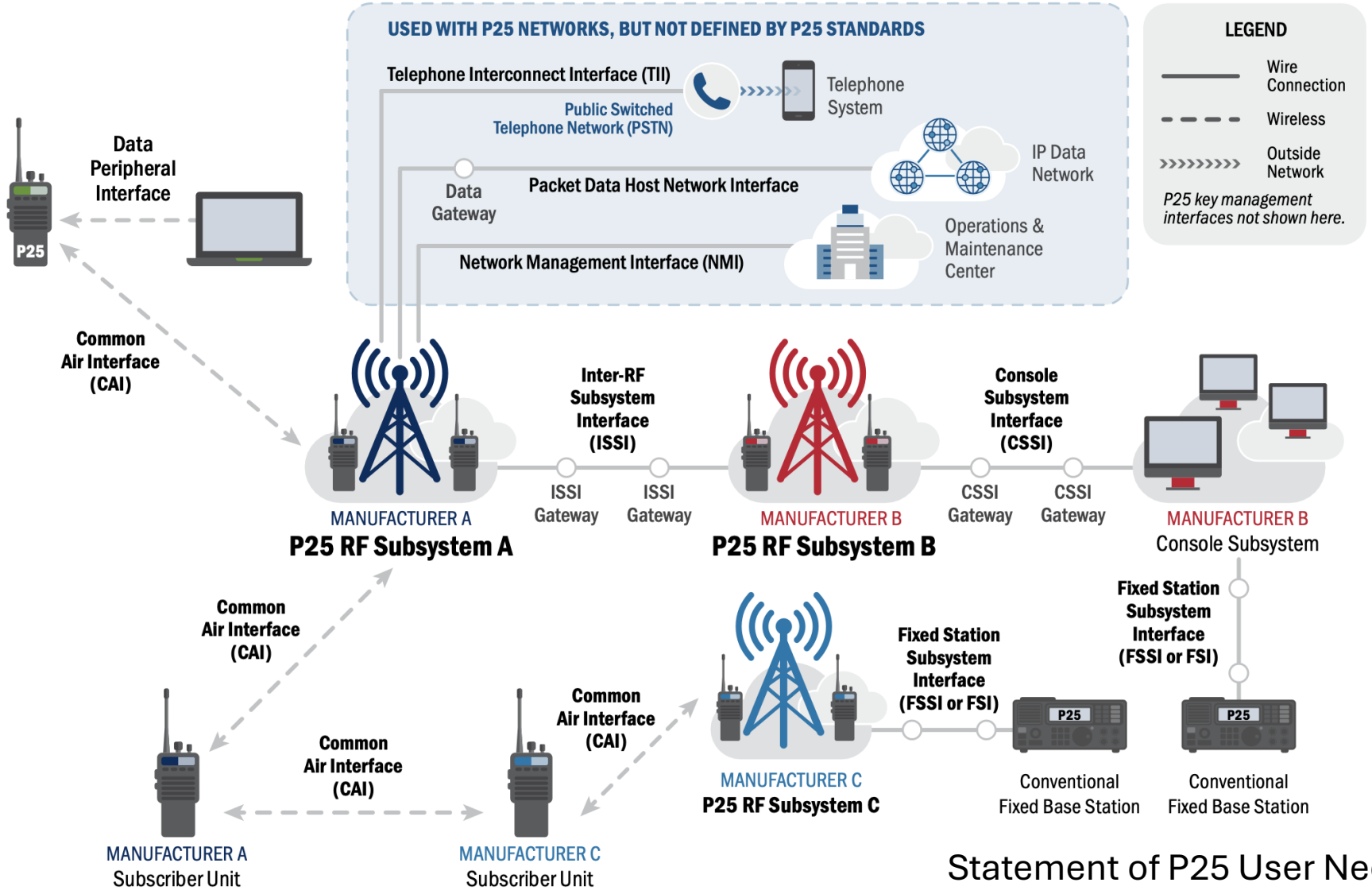
# What is P25?

- APCO Project 25 (P25) is the US standard for digital land mobile radio for public safety
  - Mandated for Federal Government funding (9/11 legislation), and by FCC Part 90 for certain frequencies (90.548)
  - Reasons: Encryption, open trunking, voice quality at 7/800 MHz
  - Interoperable with analog FM (dual-mode repeaters, patches)
- Found worldwide: Canada, Mexico, Australia, New Zealand, Brazil, Taiwan, Israel
  - Robust for long distances
  - Scalable for low-capacity systems
- Used by hams

# P25 is open!

- Developed by the Association for Public Safety Communication Officials as their 25th major project
  - Preceded by APCO-16 for analog
  - Started 1989, first release 1993
  - Standardized as ANSI EIA/TIA-102
  - **(Almost) all patents have expired from the original spec**
- Heavy government, public-safety input
  - Fixes pain points, avoids vendor lock-in
  - Significant standardization of the entire system
  - DHS runs compliance assessment program (CAP)
- Yaesu System Fusion (YSF) is P25!
  - Modifications for ham use

# P25 Interfaces



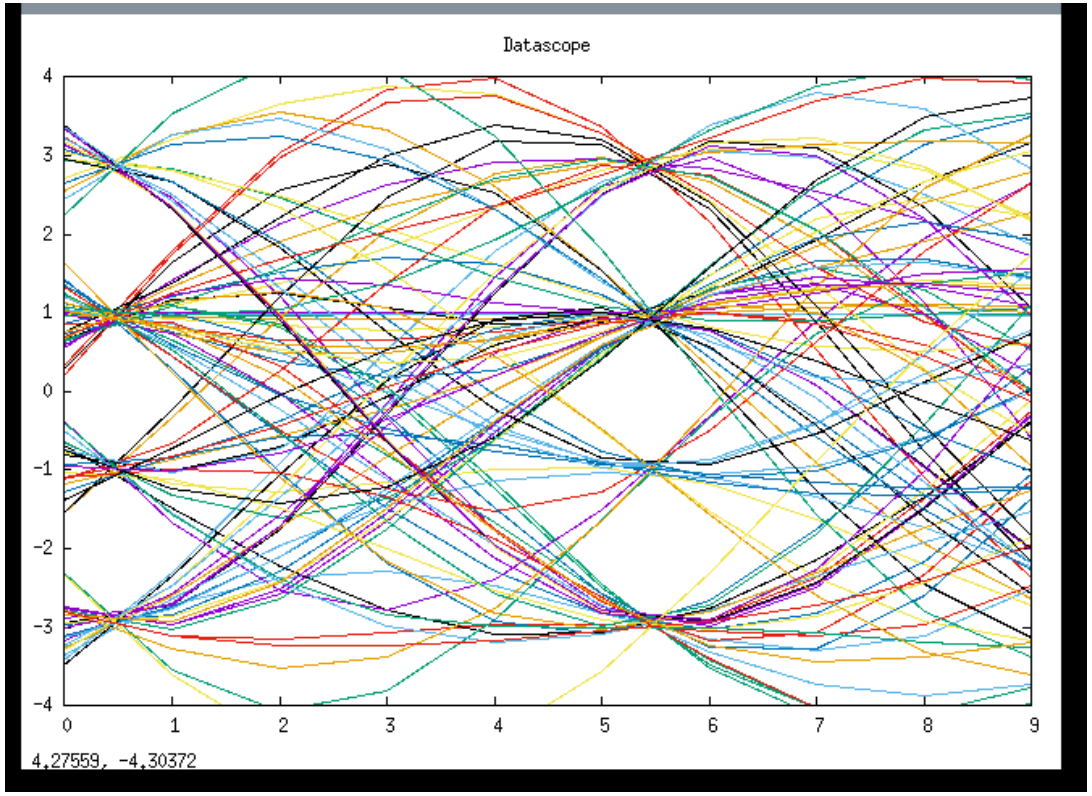

Statement of P25 User Needs, CISA

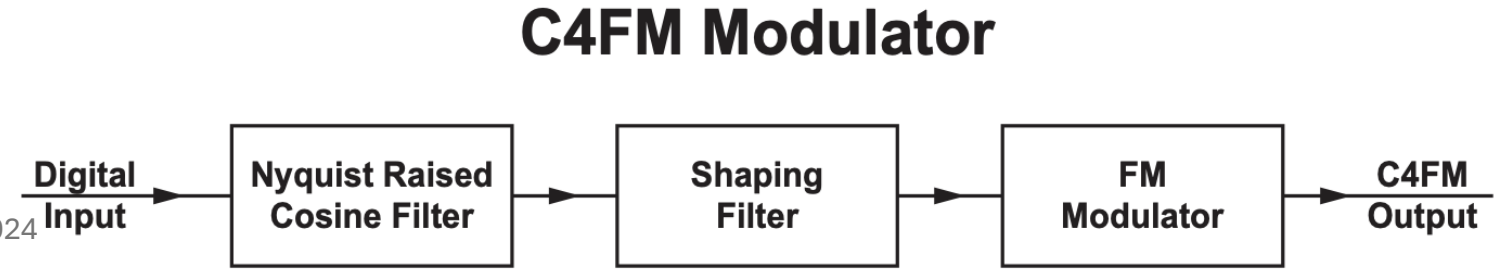
# P25 Phases

- P25 Phase 1 (1993)
  - Conventional: direct and repeater operation
  - FDMA Trunked
- P25 Phase 2 adds TDMA Trunking (2011)
  - 12.5 kHz channel split into 2 timeslots (like DMR)
  - Meets 700 MHz 6.25e FCC requirement
  - Codec, modulation changes
- What is trunking?
  - Trunked radio systems dynamically assign radio resources (*talkpaths*) to SU's.
  - A control channel receives requests for calls and directs SU's to appropriate talkpaths.
  - A *talkgroup* is a group of stations transmitting and receiving the same voice traffic.
  - P25 allows wide-area trunking: statewide (NC VIPER) and nationwide systems are in operation.
  - Sites (zones) only transmit talkgroup traffic when at least one station is *affiliated*.
- TETRA is P25's European competitor
  - 4-slot TDMA in 25 kHz
  - Fundamentally trunked, very limited direct-mode operation
  - Conceptually similar to Motorola's iDEN (NEXTEL)

# Layer 1: Physical layer

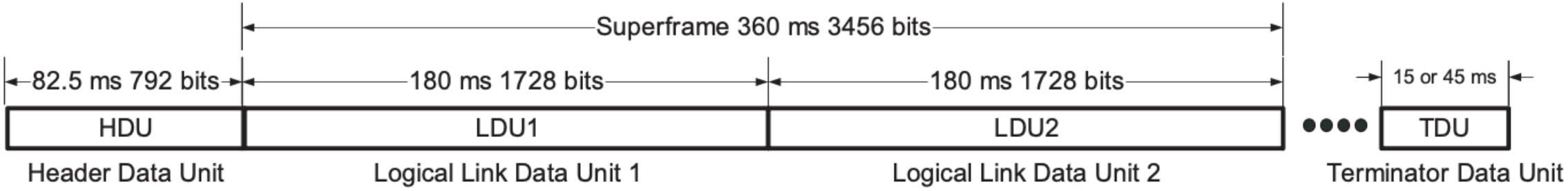
- Phase 1: Compatible Four-state Frequency Modulation (C4FM)
  - Constant-envelope 4FSK, ±600, 1800 Hz deviation
  - 9600 bps (4800 baud, 208 µs)
  - Higher-order modulation gives very good delay spread tolerance (multipath)
    - 60 µs Phase 1, 28 µs DMR, 15 µs TETRA
  - Always 12.5 kHz channel
    - **Ham myth**: 25 kHz/wideband P25
    - Intended for simulcast systems
  - **YSF**: 1.5x deviation



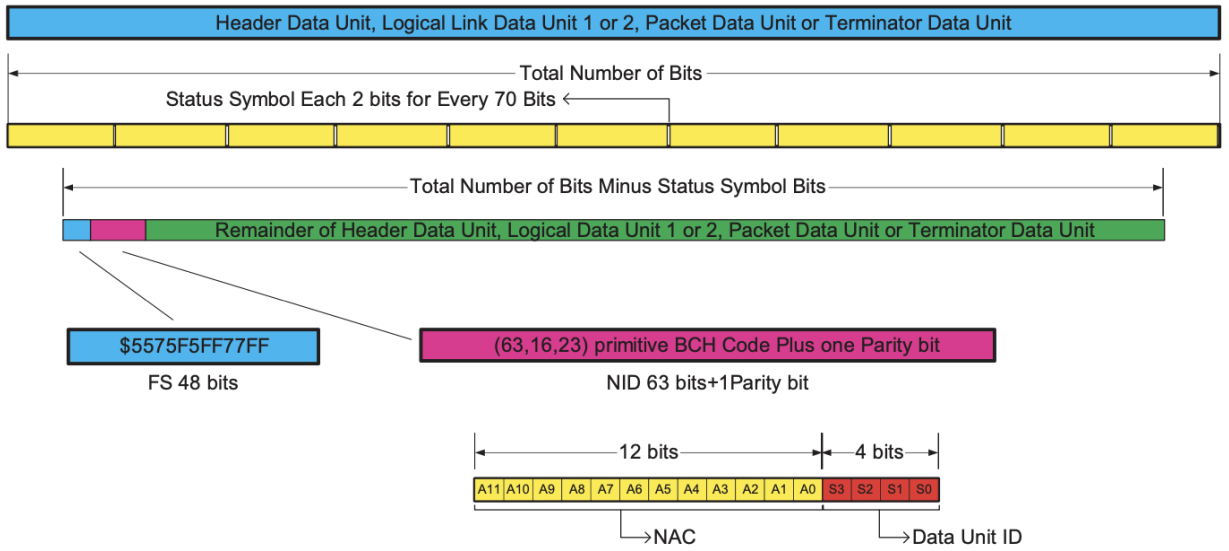
# Layer 2: Anatomy of a Call

- A voice call consists of a header data unit, logical data units and a terminator data unit
- Most manufacturers add a non-standard 40-80 ms preamble
- Repeater demodulates, corrects all errors and retransmits
- **YSF**: Only one type of LDU, Different names



# Frames and Status

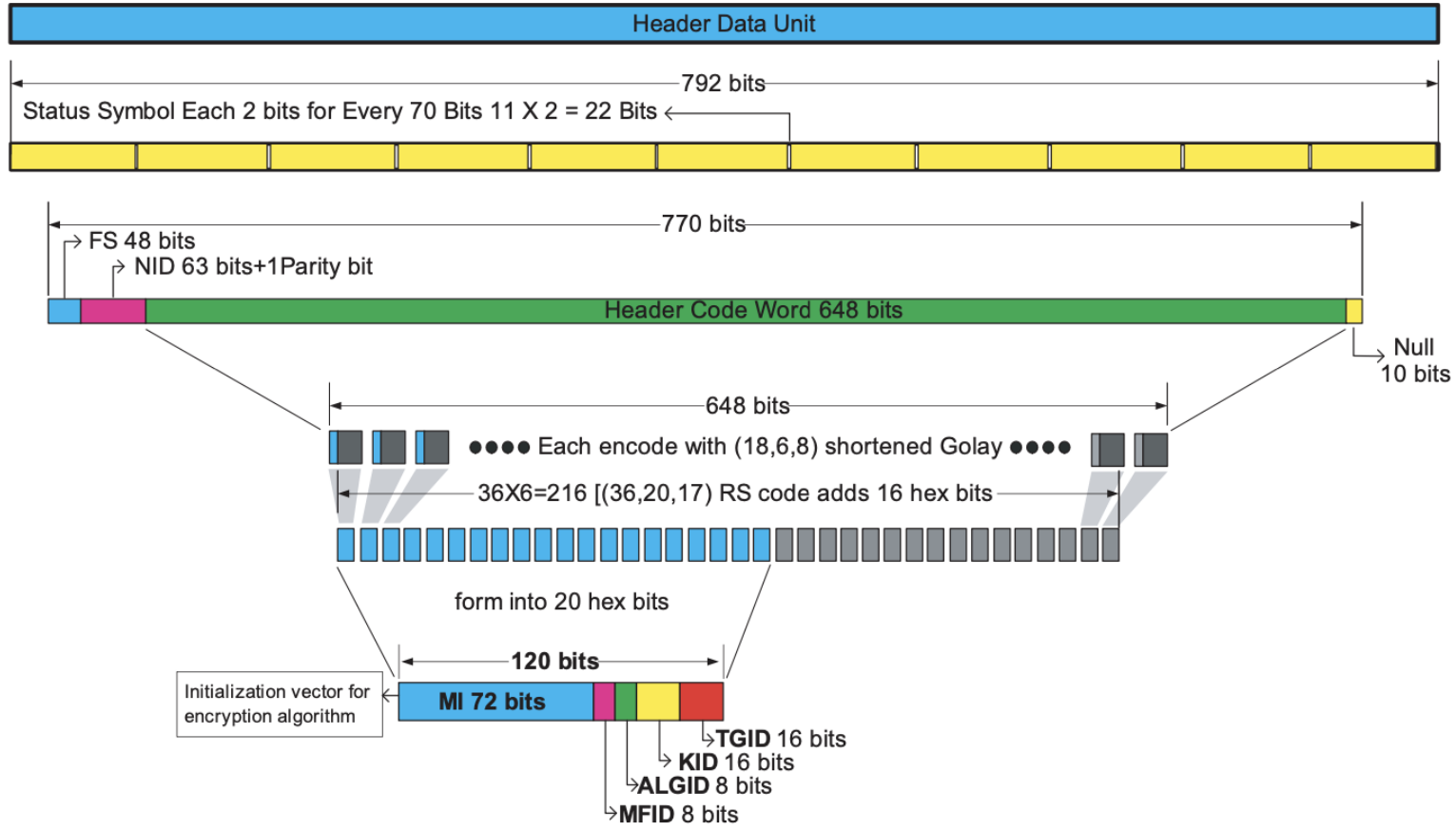
- 3 items always start: frame sync, NAC and Data Unit ID
- 12-bit Network Access Code (NAC) prevents co-channel interference (Similar to DMR color code, PL tones)
- **Ham annoyance:** Do not use default $273 NAC on repeaters. PL 88.5 Hz = $375 (See NIFOG)
- **YSF**: Shortens FS to 40 bits, all frames are 960 bits (100 ms)




- Status symbol transmitted every 70 bits
  - 01 Repeater inbound busy (TX inhibit)
  - 11 Repeater inbound idle
  - 00 Subscriber in talkaround
  - 10 Unknown/SU Inbound (TX inhibit)
- 7/800 MHz AFC, Interruptible repeater
- **Ham annoyance**: radios don't have per-repeater TX admit

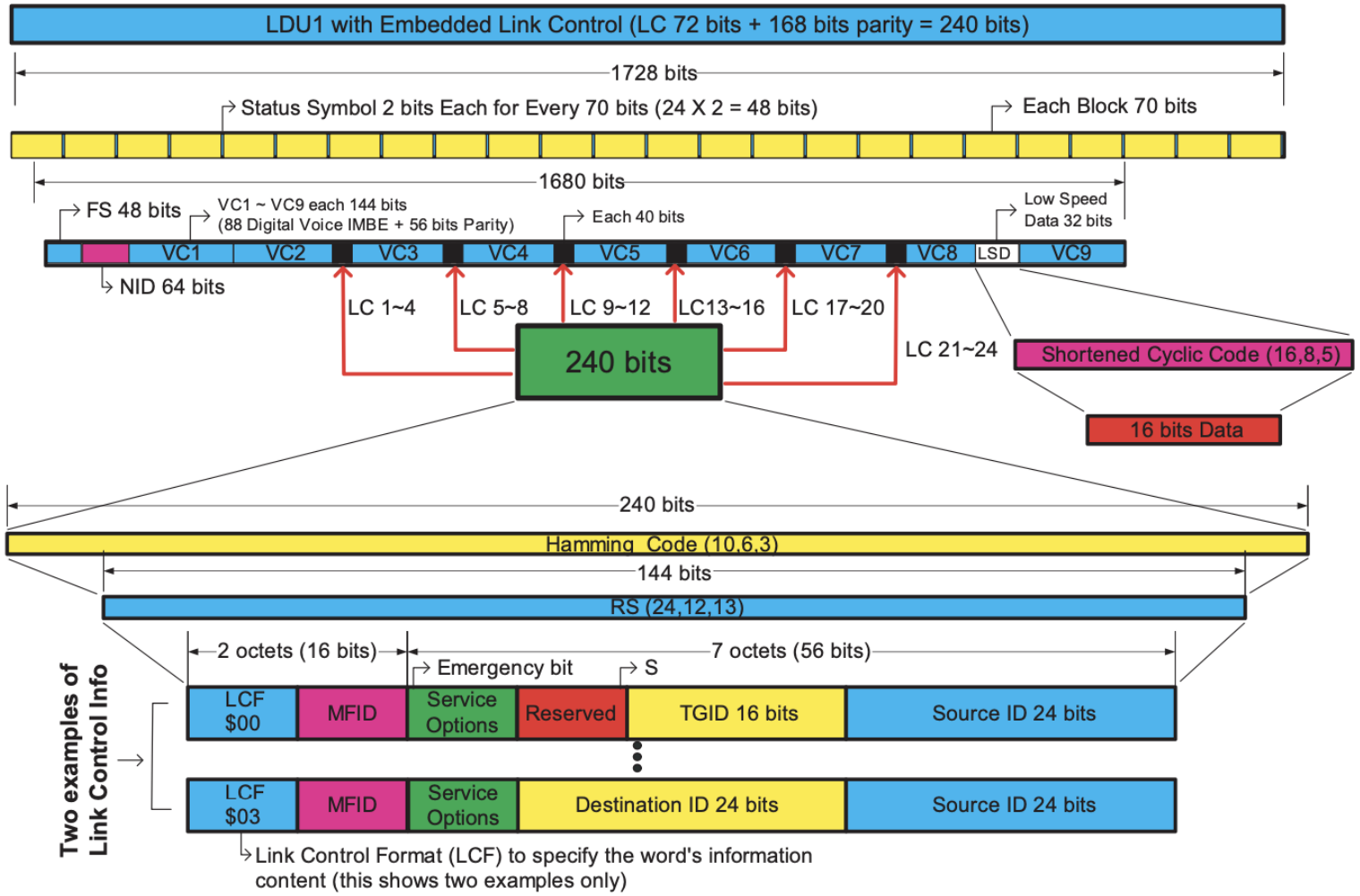
# Header Information

- HDU provides encryption and destination
  - Manufacturer ID (8b)
  - Encryption Alg ID (8b)
  - Encryption Key ID (16b)
  - Encryption Message Indicator (72b)
  - Talkgroup ID, Private/Group call (16b)
- Receiver decides immediately whether to unmute to following voice frame



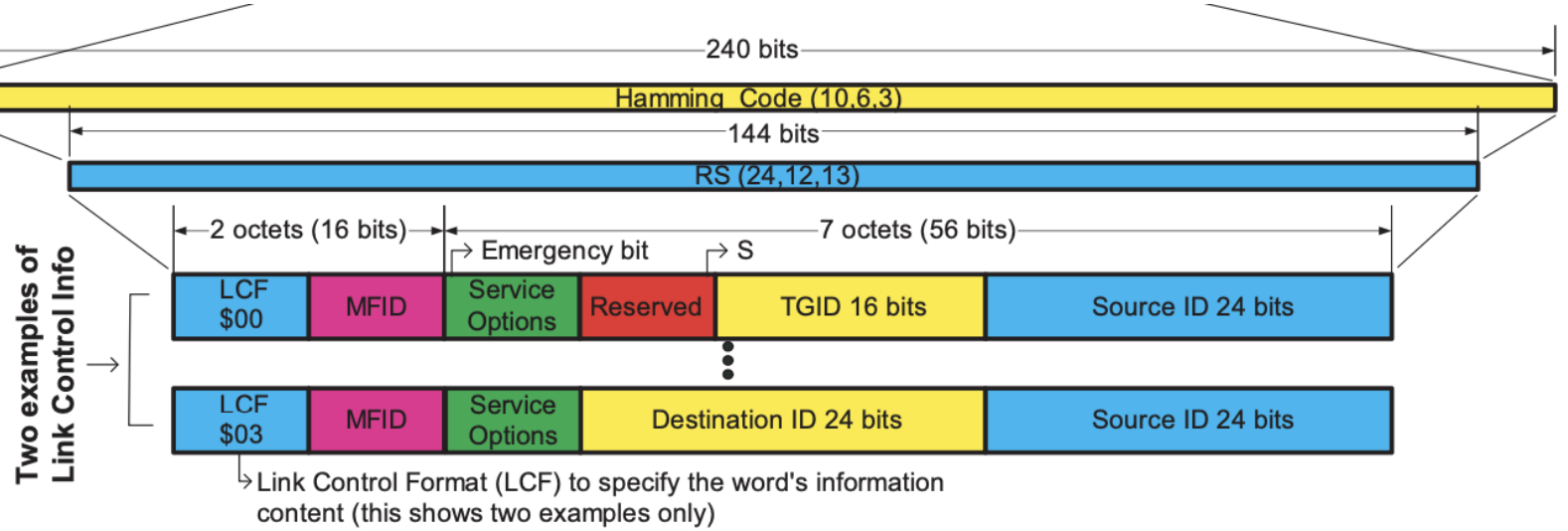
# LDU1/2

- 1728 bits, 180 ms
- Voice Codewords
- Interleaved Link Control Word
- Slow Data



# Link Control Word

- Contains call routing
  - Manufacturer ID
  - Service Options
    - Emergency flag
    - Priority level (3 b)
  - Source: 24-bit ID
    - Hams use Radio ID, like DMR
  - Destination
    - 24-bit ID for private call
    - 16-bit Talkgroup ID
    - Talkgroup 1 when not needed
  - **YSF**: Talkgroup reduced to 7 b (DG-ID), no source/dest ID (handled in embedded data instead)




- The LCW is repeated throughout the entire call for *late entry*
  - Carried in LDU1, every other LDU (320 ms)
- The Terminator Data Unit consists of the LCW.

# LDU2

- The second 180 ms contains encryption data
  - Alg ID, Key ID, Message Indicator (Initialization Vector)
  - AES 256, DES, RC4 (ADP) supported
  - Keys are loaded with a hardware keyloader
- A full late entry takes up to 320 ms
  - Selective squelch: only unmute to proper TG/private call (wait for LDU1)
  - Normal squelch: unmute to proper NAC (LDU1 not required)
  - *Late Entry Fast Unmute*: assume no encryption is used (treat call as unencrypted until LDU2 received)
- **YSF:** No encryption, LDU2 completely removed, frames shortened to 100 ms

# Voice Coding

- P25 Phase 1 uses the DVSI IMBE/AMBE+2 Full Rate codec (same as NXDN 12.5)
  - 4400 bps voice + 2800 bps FEC = 7200 bps total
- P25 Phase 2 uses AMBE+2 Half Rate (same as DMR, NXDN 6.25)
  - 2450 bps voice + 1150 bps FEC = 3600 bps total
- 20 ms frames, provides own FEC
- **Ham myth:** Both codecs are fully documented (ANSI TIA-102.BABA)
- Phase 1 codec was published in 1993. Patents should have expired. Implemented in `mbelib`.
- **YSF**: Voice Wide = Full Rate, Digital Narrow = Half Rate
  - In DN mode, 1600 bps additional FEC is added by 3-way repetition of high-priority AMBE bits
  - 2000 bps used for embedded data
- **P25 Weakness**: Initial implementations were not well-tested with public safety noise sources
- PASS alarms most troublesome. Police car sirens, diesel engine noise known issues
- Successive IMBE versions and SU models remove noise before it gets to the codec
  - AGC
  - Noise reduction
  - Beamforming (up to 4 mics)
- Voice quality significantly better on newer models
  - TIA-102.BABG provides performance tests
- AMBE introduces soft-decision decode (+1.5 dB C/N)

# Low Speed Data

- LDUs carry embedded data at 88 bps
- Used for in-call GPS and callsign (soft ID)
  - Motorola soft ID is abandoned (XTS series)
  - Harris soft ID recently standardized
  - Tier 1 location services (NMEA 0183 sentences)

- **YSF**: Callsign is carried in embedded data in DN mode
  - Callsign data=480 bits, occupies at least 750 bps

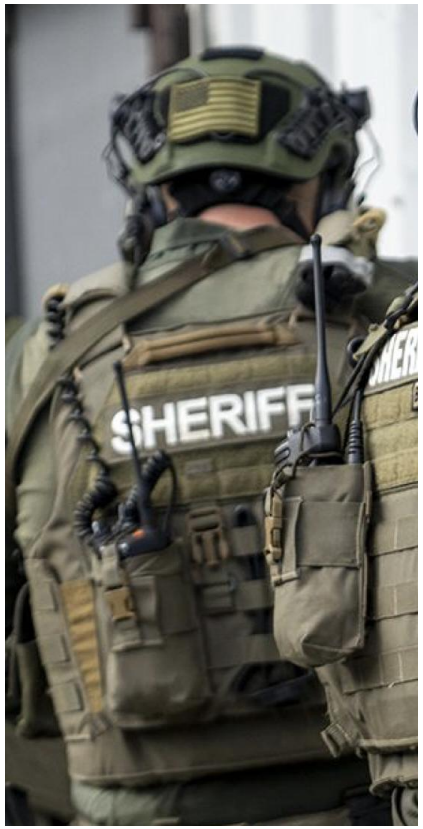
- IPv4 Packet Data
  - Tier 2 location services
  - Text messaging

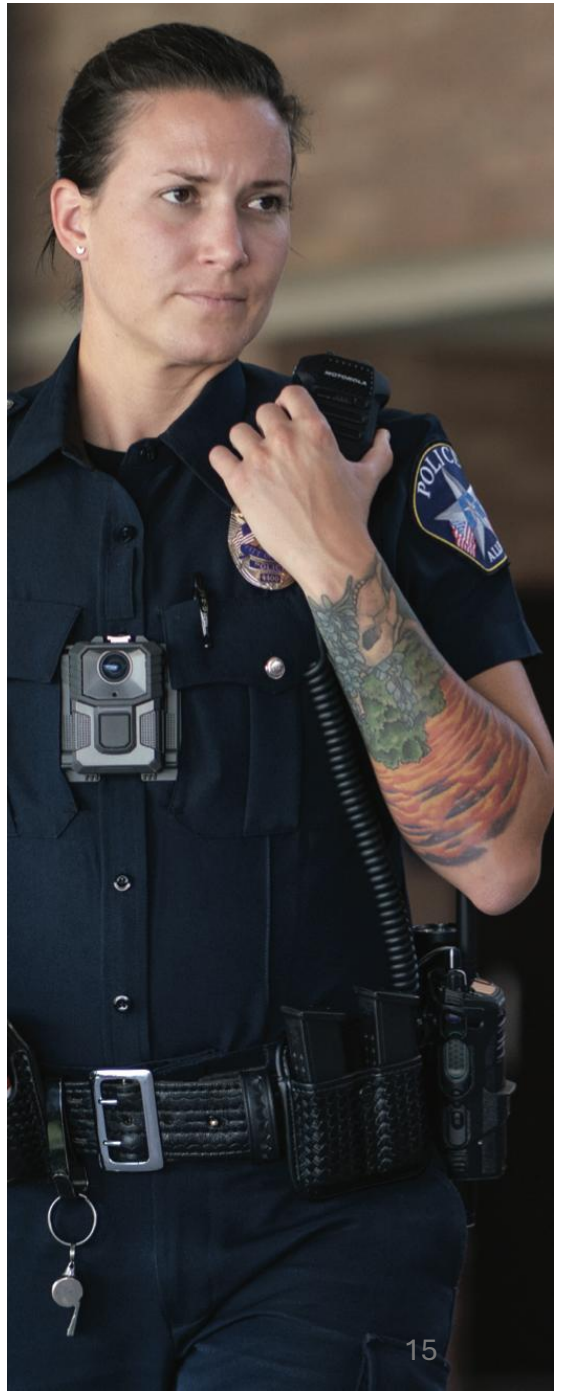
# Subscriber Units

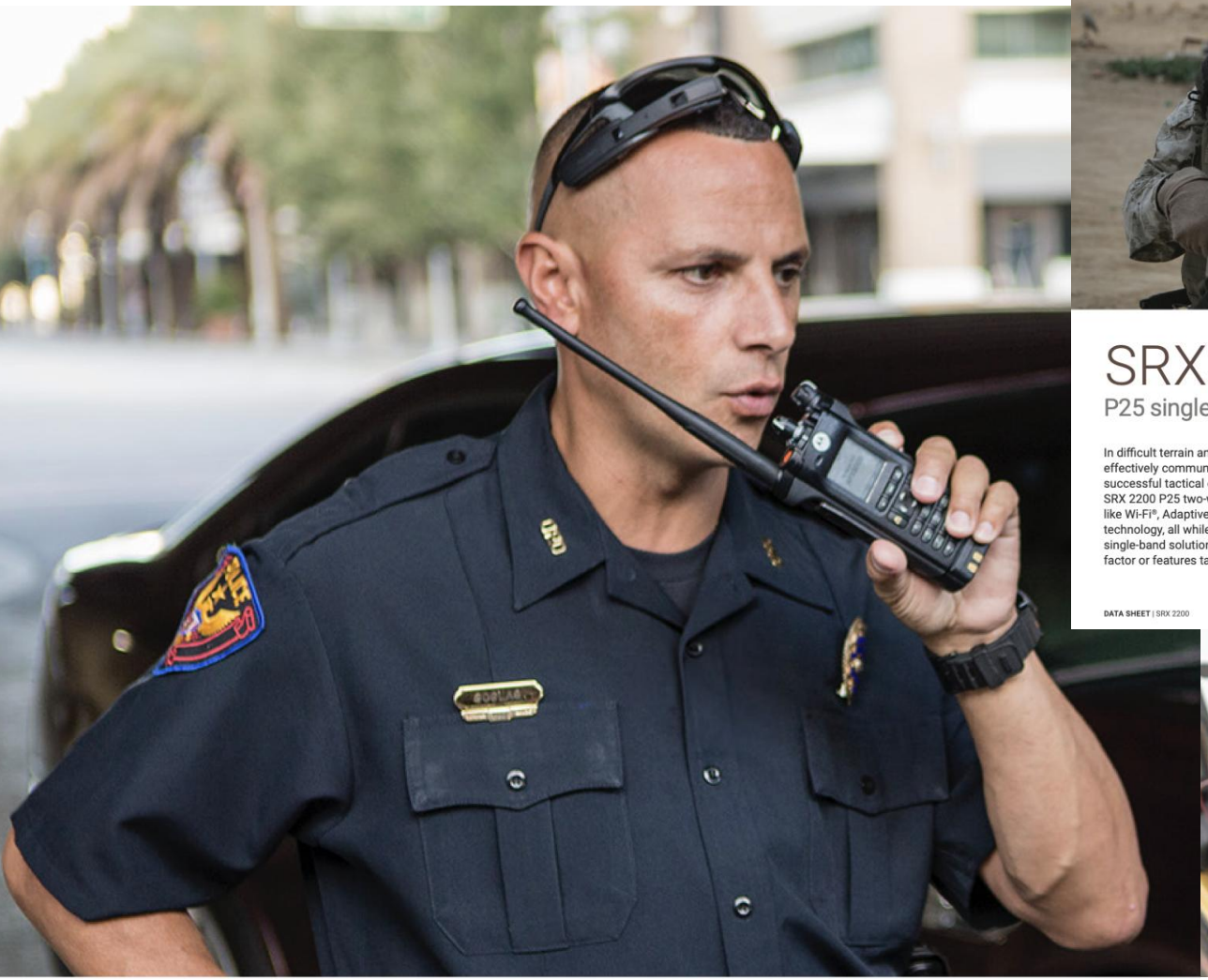
- Motorola Solutions
  - Vertex Standard
- Harris (M/A-Com, Ericsson, GE)
- Kenwood/EFJohnson
  - Tri-mode NXDN/DMR/P25
- BK Technologies (RELM)

- Tait
- Icom

- Unication Pagers





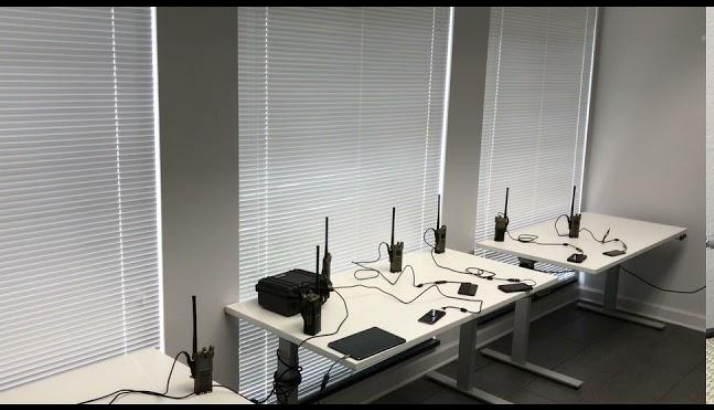
# SRX 2200

## P25 single-band portable radio

In difficult terrain and combat environments, soldiers must effectively communicate with each other to coordinate successful tactical operations and improve response time. The SRX 2200 P25 two-way portable radio supports technologies like Wi-Fi®, Adaptive Audio Engine, and Bluetooth® 4.0 wireless technology, all while delivering trusted APX™ performance in a single-band solution without compromising the combat form factor or features tactical and base personnel require.


DATA SHEET | SRX 2200

MOTOROLA SOLUTIONS

User opens ATAK chat function. Other users on left screen are identified in the chat list. User sends initial message to the team.

# Motorola Solutions

- XTS 1500/2500/5000
  - Introduced 2003, out of support 2018, Phase 1 only
  - Agencies were dumping them surplus, but that supply has declined
  - Modern Windows programming, USB
  - XTL mobiles
- ASTRO Saber/ASTRO Spectra/XTS 3000
  - Old (1993-2008)
  - ASTRO means digital; some use pre-standard VSELP codec
  - Programming is problematic, RS-232 Smart RIB

# Motorola APX Standard


- APX 900 (XPR 7550e)
- APX 4000 (1- and 2-knob)
- APX 6000 (Single band)
- APX 7000 (Dual band)
- APX 8000 (All-band)
- XE = fire model
- +500 for mobile


# Buying Motorola

- UHF R1 (380-470 MHz) vs R2 (450-520 MHz)
- APX and MOTOTRBO Firmware/CPS officially available for free
  - APX CPS is ham 25 kHz aware
  - https://www.motorolasolutions.com/en_us/support-search.html#q=000003523
- “Buy the seller, not the radio”
- Flashcode
  - Feature licensing
  - ASTRO Digital CAI
  - APX 8000 band enablement
- Tags
- Legit flashcode and tags are necessary for depot support
  - Flat rate repairs
  - End of support varies
- Advanced System Key/Password


eBay

# Off the beaten path

- Tait TP9100
  - Better scan than Motorola
  - Windows programming
  - Programming cable $$
- Harris XG-100P
  - Cheapest all-band
  - Firmware issues
- Unication Pagers
  - Dual band, P25/DMR
  - Used as scanner

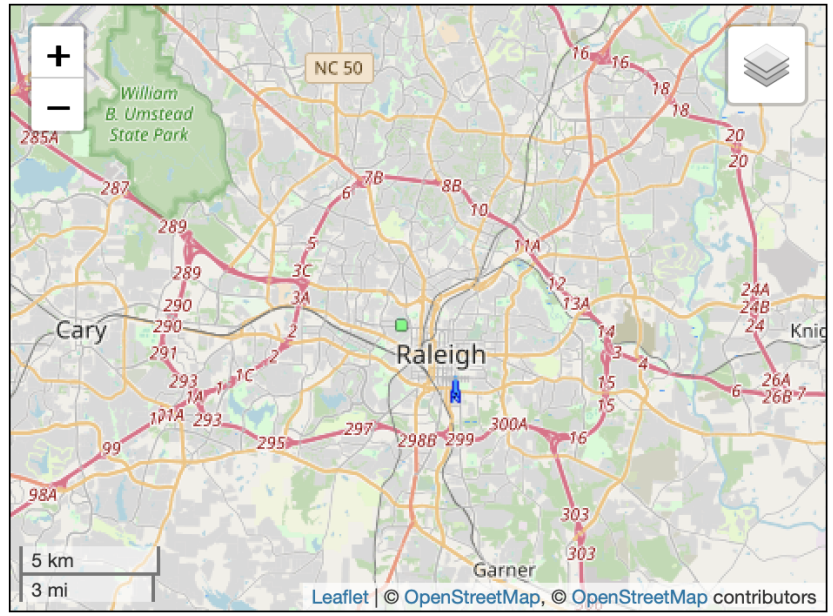


# Commercial Radio Features

- Automatic scan: select scan lists via channels
- Voice announcements
- Nuisance delete: removes channel from scan list until scan mode is exited
- Vote scan: lands on the highest RSSI channel for multicast (linked repeaters)
- PL reverse burst: prevents squelch crash
- Digital conventional TPT: Provides confidence that you’re reaching the repeater
- TX Admit: Prevents doubling
- Memory names greater than 6 characters

# Local Systems: W4BAD

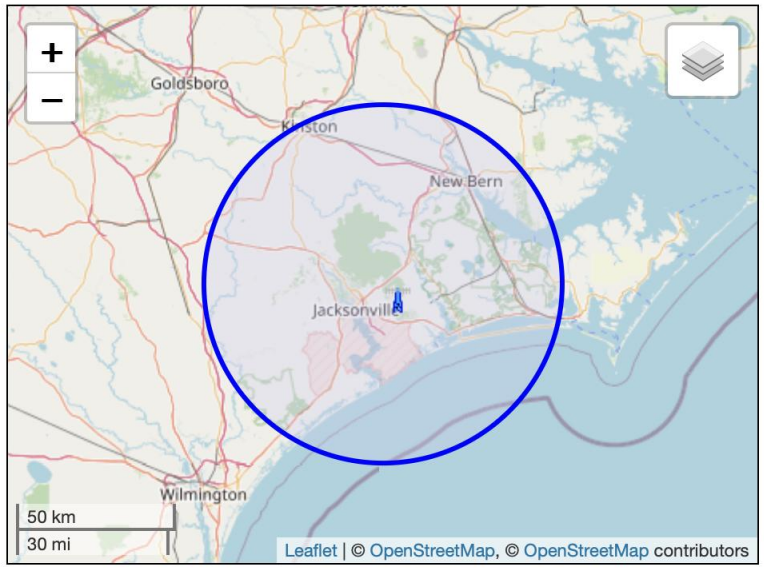
- 3 Raleigh-area linked UHF repeaters
  - Raleigh BB&T Building: Solid within beltline, handheld coverage to Wake Forest
  - Durham NC Mutual Life building: Downtown Durham, Southern edge where 15/501 splits
  - Roxboro: Person County
- MMDVM P25 reflector (27565/$6BAD)
  - Brandmeister DMR bridge (310068)
  - YSF reflector, but use YSF2P25 to avoid transcode
- Use talkgroup 27565 on the air
- Info at w4bad.com

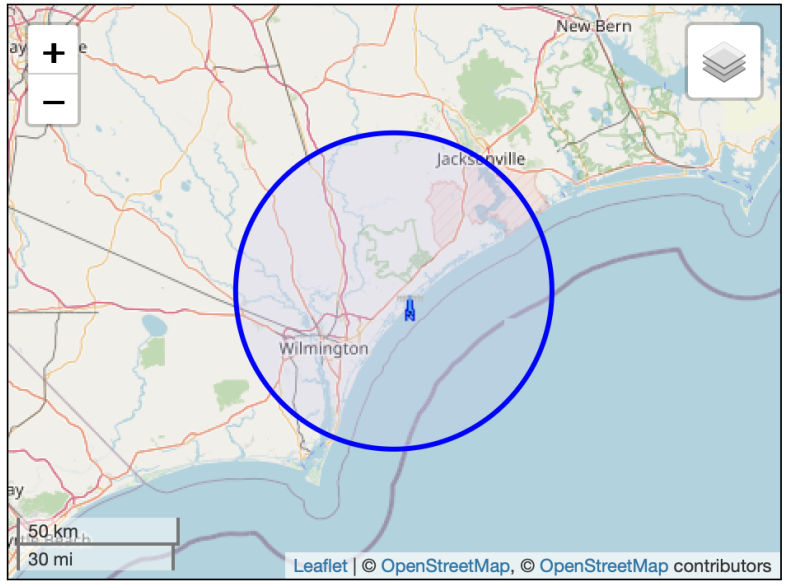


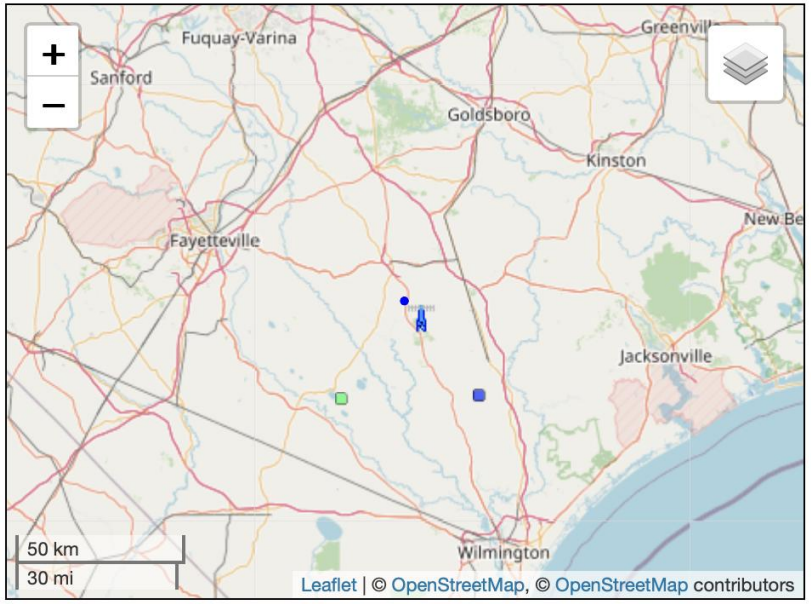

Repeaterbook

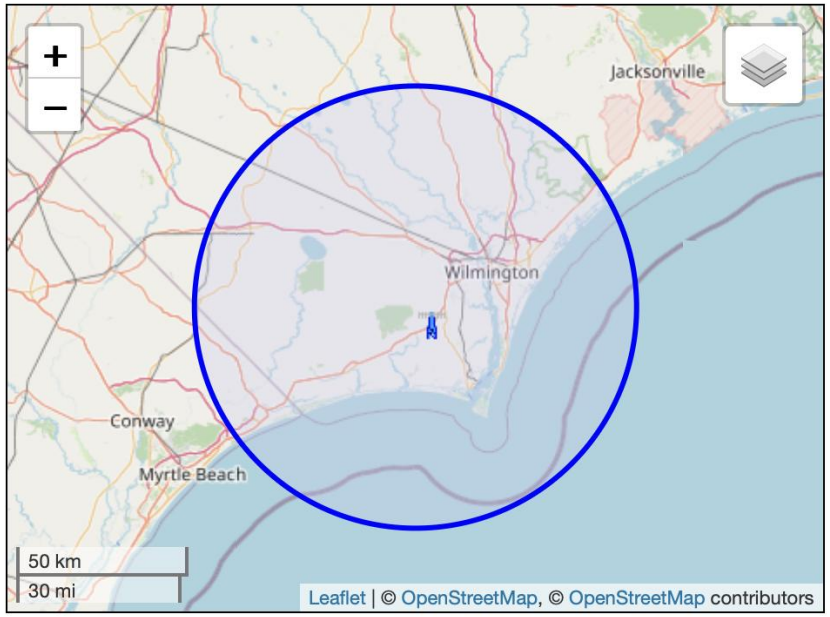
# ENC P25

- 4 linked UHF Repeaters
  - Clinton
  - Jacksonville
  - Hampstead
  - Winnabow



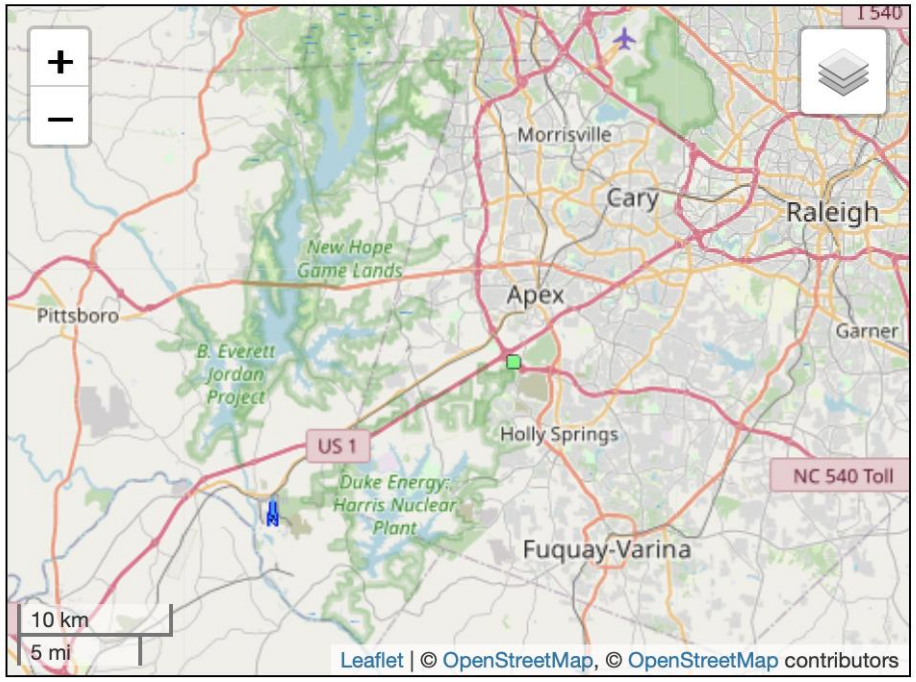



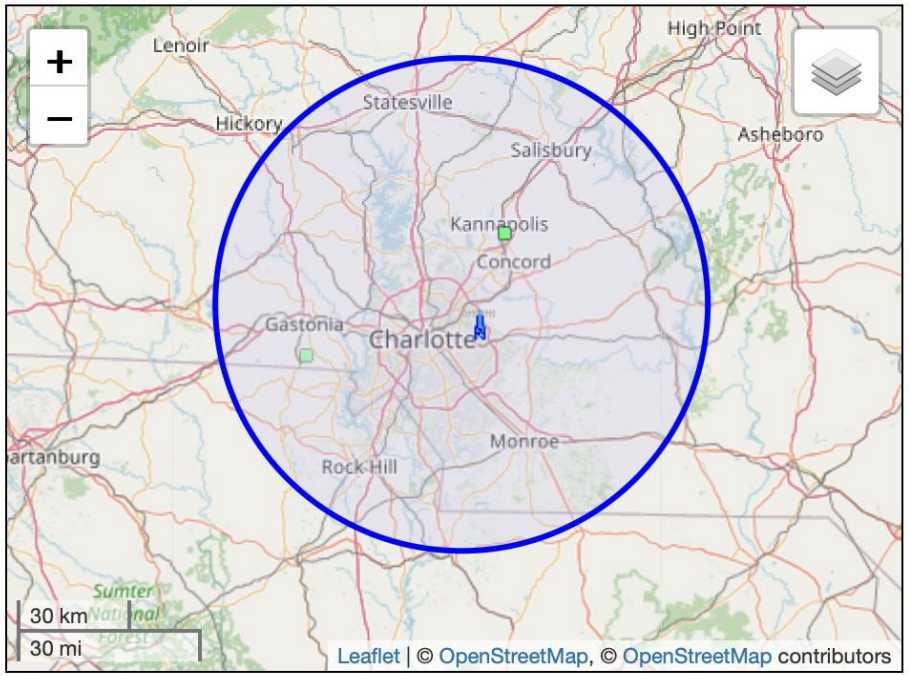



# Other P25 Systems

- W0SMT Moncure (VHF, Dual-mode): Up to Triangle Expressway
- W0UNC at UNC Charlotte (UHF, Dual-Mode)



# NC Public Safety Systems

- 7/800 MHz trunked systems (769-775/799-805, 806-816/851-861)
- Cary/Wake (Phase 1, 8 sites)
- Durham/Fayetteville (Phase 1, Durham has 4 sites)
- Franklin County (Phase 2, VHF, 5 sites)
- Johnston County (Phase 2, 5 sites)
- Rocky Mount (Phase 2, 2 sites)
- VIPER (Statewide: 236 sites, 170,000 users)
  - Granville, Harnett, Nash, Orange, Person, Vance Counties, NCSHP, Duke University
  - Counties and municipalities contribute tower space, hardware, spectrum for operation by NCSHP
  - Currently Phase 1, but switching to Phase 2
  - Motorola system, IP backbone running on microwave links managed by UNC-TV
- Duke Energy
  - Multistate Phase 2 with TDMA control
- See RadioReference DB

# MMDVM Hotspot

- Supported by MMDVM and MMDVM-HS
- MMDVM finally fixed several issues in its implementation
  - Filler HDU led to permanent late entry, Status bits work properly
  - Use a version at least `20240207`. As of December 2024, Pi-Star (4.3.0) is using an obsolete version, use WPSD.
- DVM Project implements P25 trunking and core on MMDVM hotspots
  - Centex TRS runs a trunked system on Part 90 frequencies

# Conclusion

- P25 is a standard that was developed with major influence by the end users and is mandated for US public safety.
- It is old enough that it is nearly patent-free.
- Available equipment consists of high-tier radios, repeaters and applications, which are attractive to many.

# A quick look into programming


- Part 90 radios are pre-programmed by FCC regulation. CPS software is used to build a *codeplug* to download into the radio.
- Motorola uses a hierarchy
  - Radio Wide Settings
  - Conventional System (Ham Repeaters)
  - Conventional Personality (W4BAD Net)
  - Frequency Option (Raleigh)
- Each Option mapped to a Zone and Channel corresponding to dial position