Logan Scott, 9 December 2021, Presentation to the PNT AB

GPS & Galileo Civil Signal Authentication

Logan Scott has over 40 years of military and civil GPS systems engineering experience. He is a consultant specializing in radio frequency signal processing and waveform design.

At Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers and adaptive arrays. At Omnipoint (now T-Mobile), he developed spectrum sharing techniques that led to a Pioneer's preference award from the FCC. He is a cofounder of Lonestar Aerospace, an advanced decision analytics company located in Texas.

Logan has been an active advocate for improved civil GPS location assurance for over 20 years and was the first to describe how civil navigation signals could be authenticated using delayed key concepts central to the Chimera signal. For the past 6 years he has been developing advanced signal concepts, including Chimera, for NTS-3, AFRL, and the University of Colorado.

Logan is a Fellow of the Institute of Navigation and a Senior Member of IEEE. In 2018 he received the GPS World Signals award. He is the author of Interference: Origins, Effects, and Mitigation in PNT21 and holds 45 US patents.

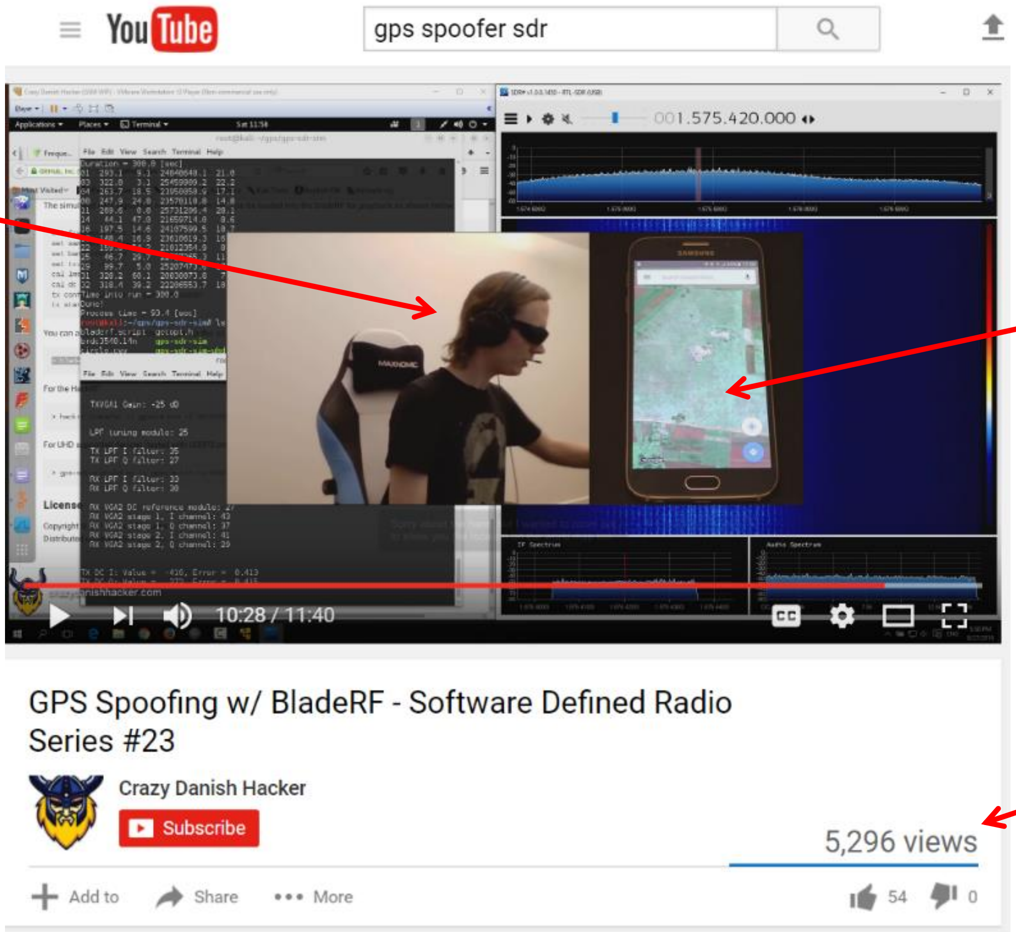
Spoofing is NOT Just About the GNSS Receiver

Spoofing Is an Attack on Perception

Zero to Operational in 10 minutes With No GPS Expertise

Step By Step Instructions from a Script Kiddy on How to Download and Run a Spoofing App

"I Wear Cool Sunglasses"



"I'm in Cuba"

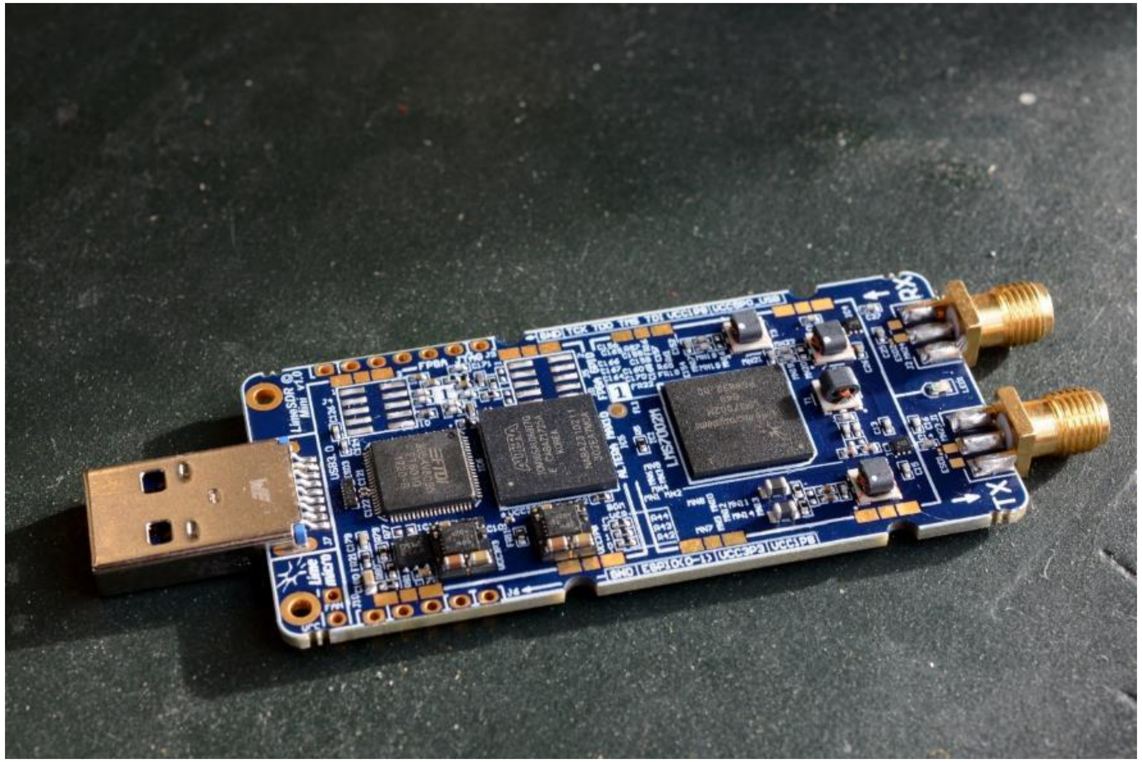
27,000 views June 2021

https://www.youtube.com/watch?v=VAmbWwAPZZo

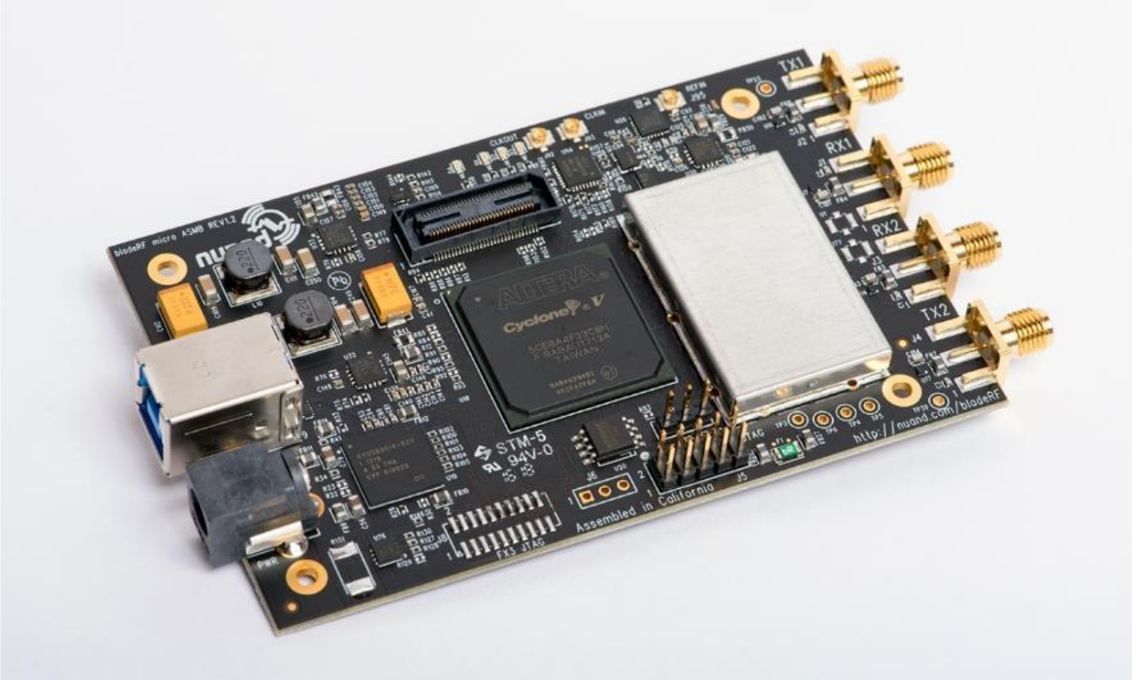
danish bladerf videoplayback.mp4

Software Defined Radios (SDR) are Inexpensive and Capable of Transmitting & Receiving Sophisticated Waveforms

LIME SDR



NUAND BLADERF



What is Location (and Time) Spoofing?
An Operational Definition

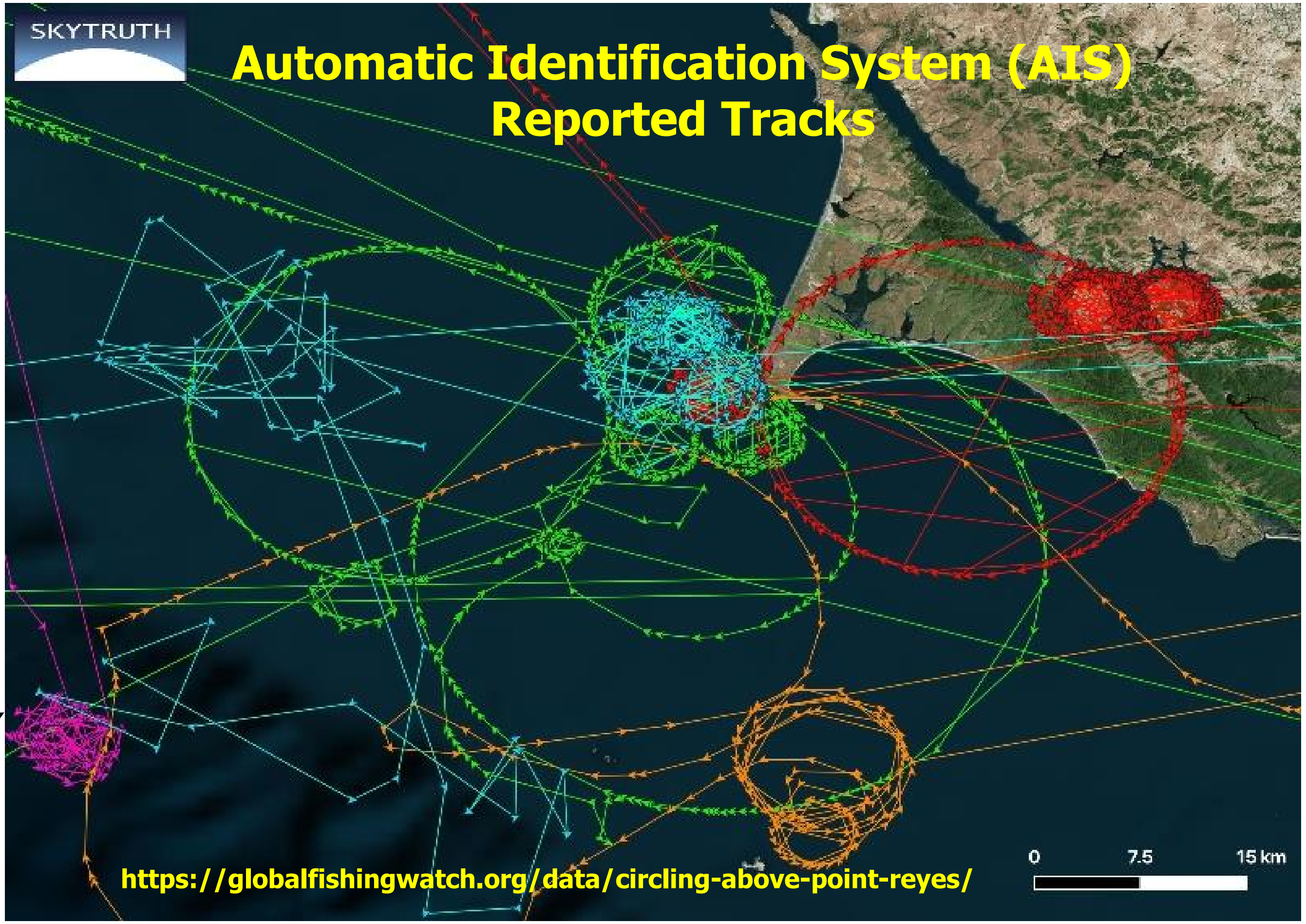
- Spoofing is a process whereby someone (or something) tries to control reported position.
- May take the form of reporting incorrect PVT to a local user, or, to a remotely located client.
  - Is Often Oriented towards Corrupting Location Keyed Databases

- **Is not of necessity an RF attack.**
  - In its most general form, spoofing can be conducted using RF as well as cyber attacks. Cyber attacks can be in the form of malicious software, falsified maps, man in the middle attacks, reference station manipulation, lying, etc.
  - RF can aid in detecting cyberattacks

Spoofing Can Cover Myriad Criminal Activities

- Illegal Fishing
- Sand Dredging Theft
- Illegal Dumping
- Smuggling

These Were Probably Insider Attacks



Crime Does Pay:
Let's Go Fishing!

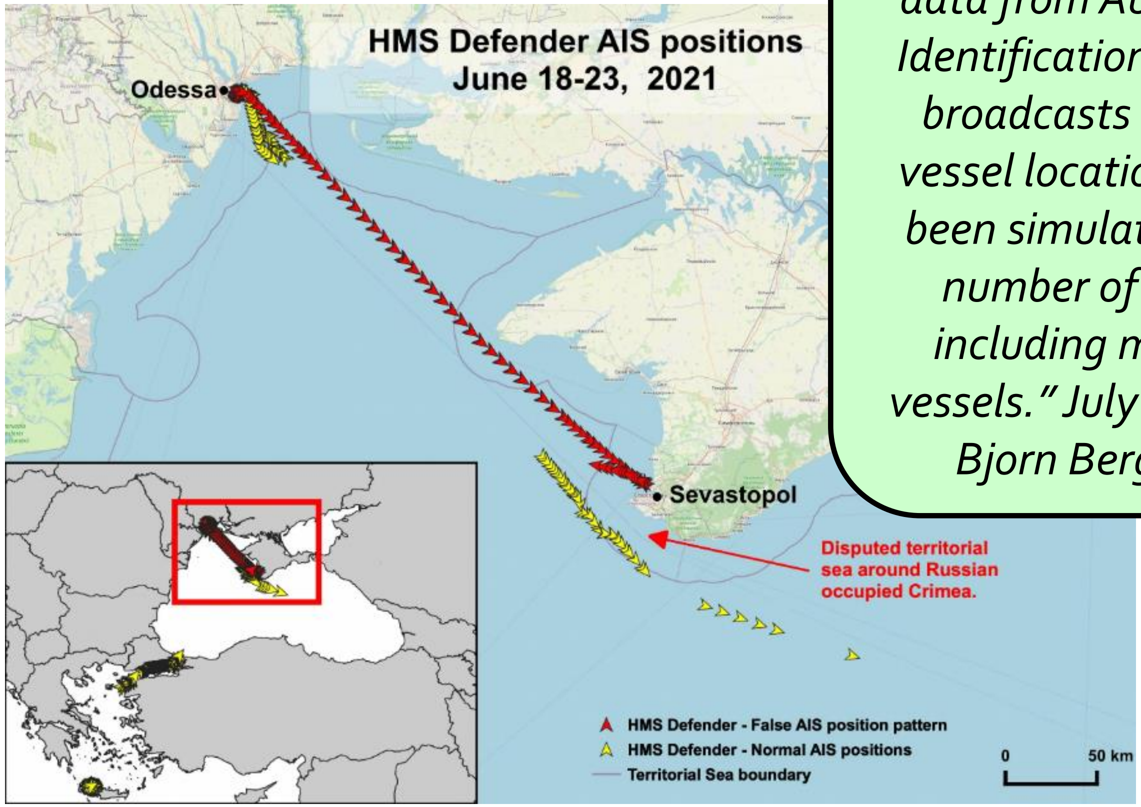
Motivation

"Experts estimate that up to $23.5 billion worth of fish enter the world market each year from illegal fishing, which averages to approximately 1 in 5 fish caught in the wild. In some regions, as much as 40 percent of the catch is thought to have been caught unlawfully." End Illegal Fishing Project, 21 January 2015

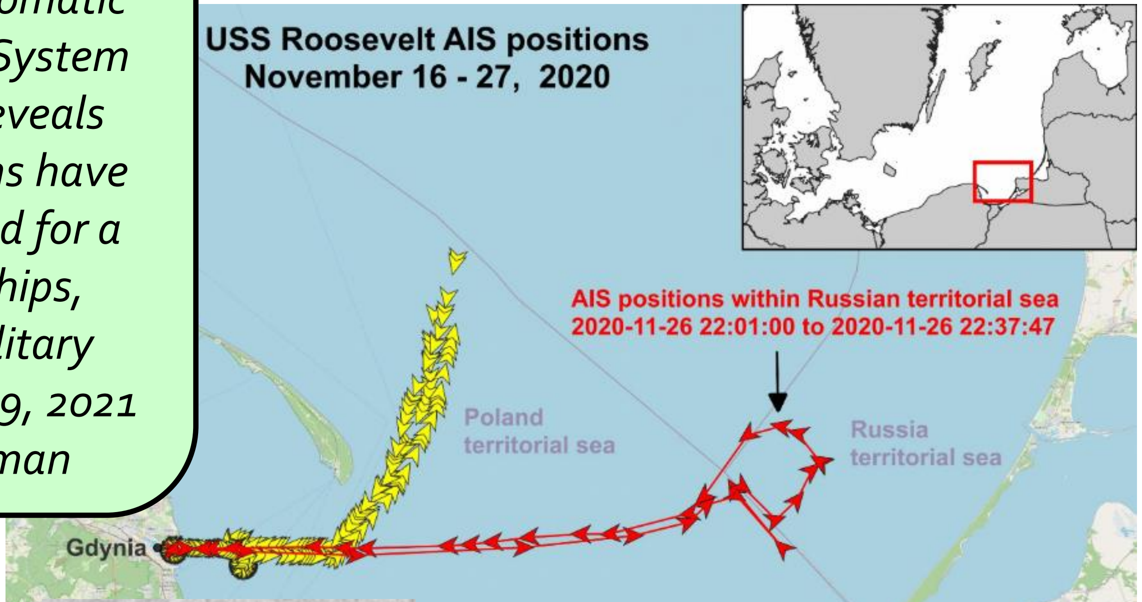
This Is Likely Identity Spoofing Combined with Lying About Location

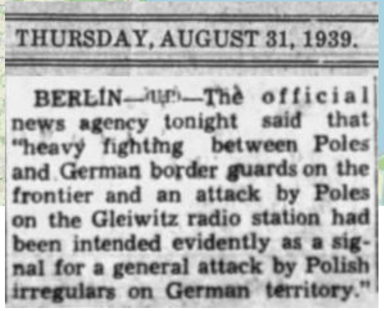
Provable GNSS Signals Can Help Detect This

"Analysis of tracking data from Automatic Identification System broadcasts reveals vessel locations have been simulated for a number of ships, including military vessels." July 29, 2021 Bjorn Bergman



https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/



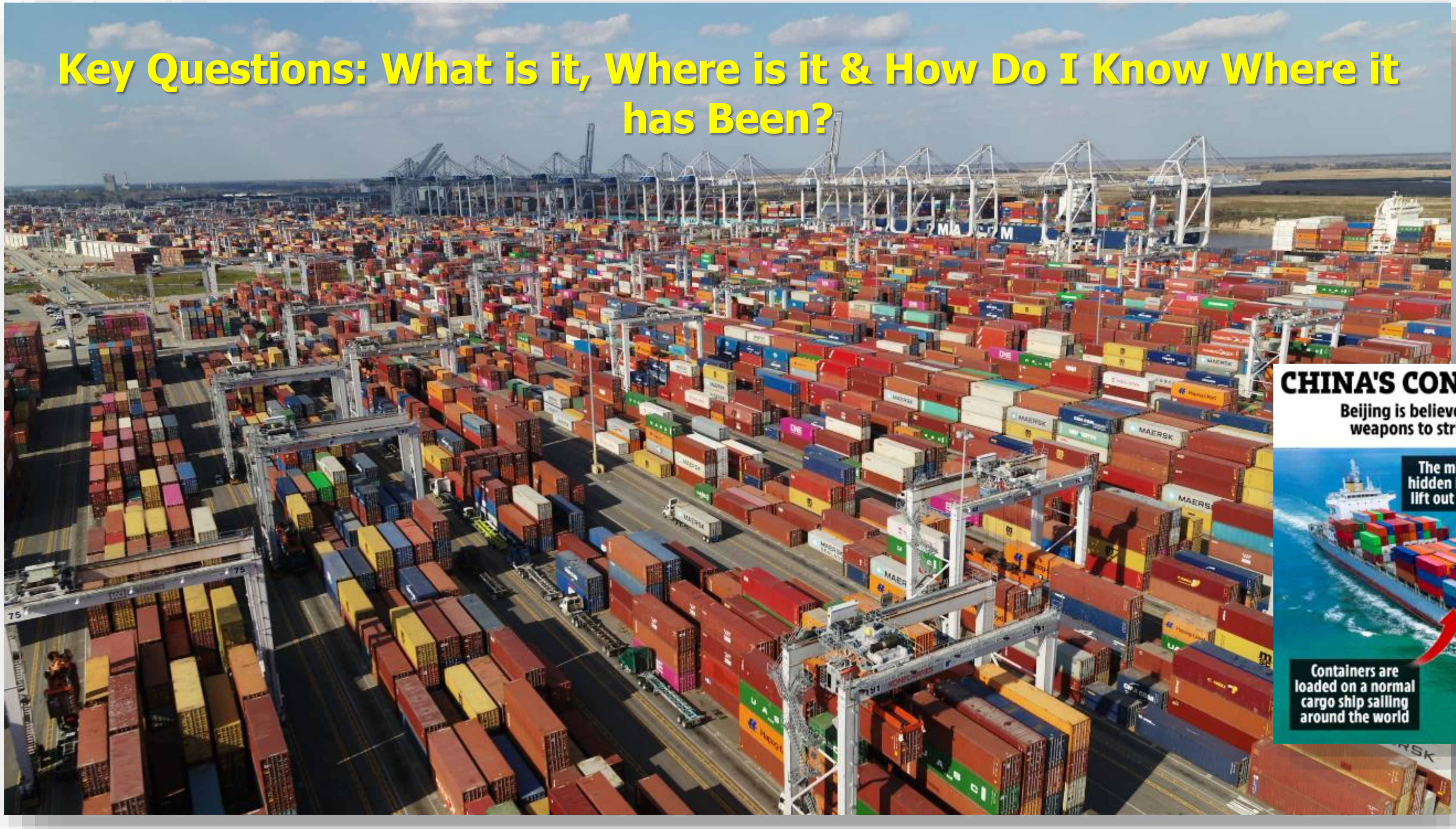

THURSDAY, AUGUST 31, 1939.

BERLIN—(UP)—The official news agency tonight said that "heavy fighting between Poles and German border guards on the frontier and an attack by Poles on the Gleiwitz radio station had been intended evidently as a signal for a general attack by Polish irregulars on German territory."

False Flag Precipitation

Spoofing Is an Attack on Perception

Civil and Military Issues are Intermeshed

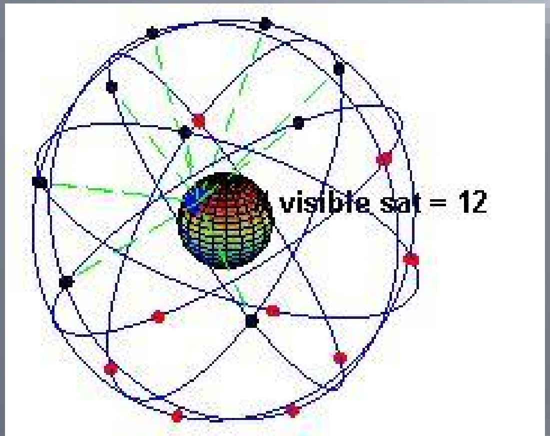


Graphic from "The US Sun" 6 December 2021

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2982&context=ils

A Good Proof of Location System*

Illuminating the Chimera Concept



At the Receiver: Anti-Spoof
At the Remote Client: Proof of Location

*** But a Not So Good Navigation System**

The SatNav System

- Encrypt Spread Spectrum Navigation Signals
  - Encrypt Spreading Sequence, Changing the Key Once Every 3 Minutes
  - Only Control Segment & Space Segment Hold Real-time Keys, NOT THE USER SEGMENT
- Release Keys to the Public 3 minutes later
  - This is Not the Same as Current Generation Military Signals Where Keys Are Released Apriori and Have to Be Held in Tamper Resistant, Secure Storage

Why This Is Good For Proof of Location and Signal Authentication?

- Spread Spectrum Signals Are Hidden Way Below Thermal Noise and are Hard to Forge Without Keys
- Can Collect and Send Raw A/D samples to other Locations Before Keys Are Released *("Time & Location Signature")*
  - Communications Links, Man-in-the-Middle, Can't Easily Forge Location Signature
- Once Keys are Released, Software Entities can Compute Sender's Location and Time
- **Secure Key Storage Is Not Required In the User Segment**
  - It Is Usable In Less Secured Environments

Why This Is A Not So Good Navigation System?

- User Segment Can't Do Anything with the Signal Except Record It or Send It Elsewhere Until The Keys Are Released
  - Navigation Solutions Have up to a 3-minute Delay
  - Also, How are the keys conveyed?

- Chimera & Galileo Overcome these Limitations by Dividing Signals Into Real-time and Delayed Access Components
  - Applicable to Any GNSS signal

Authenticatable GNSS Signals

Practicable Signal Authentication & Proof of Location Methods

Range and Data Authentication, Two Complementary Methods

- Data Authentication
  - Establishes the Provenance of Navigation Messages
  - Typically Done Using Cryptographic Digital Signing
  - Straightforward Modification to Extant Satellites
  - Easy Modifications to Receivers
- Ranging Authentication
  - Establishes the Provenance of Pseudoranging Codes
  - Typically Done Using Cryptographic Watermarking with Delayed Key Release to UE
  - Complex Modification to Non-SDR Satellites
  - Straightforward Modification to SDR Based Satellites
  - Modest Modification to Receivers (Snapshot Memory)

Galileo Has A Deployed Authentication Capability

The Key Decision: "Go Fix It"

- COMMISSION IMPLEMENTING DECISION (EU) 2017/224 of 8 February 2017
  - Signed at Brussels by Jean-Claude Juncker, President of the European Commission

- "The authentication capacity should increase the degree of safety and prevent risks of falsification and fraud in particular. Additional features must therefore be incorporated into satellite signals in order to assure users that the information which they receive does come from the system under the Galileo programme and not from an unrecognised source."

Galileo OS-NMA Is In Public Testing Phase

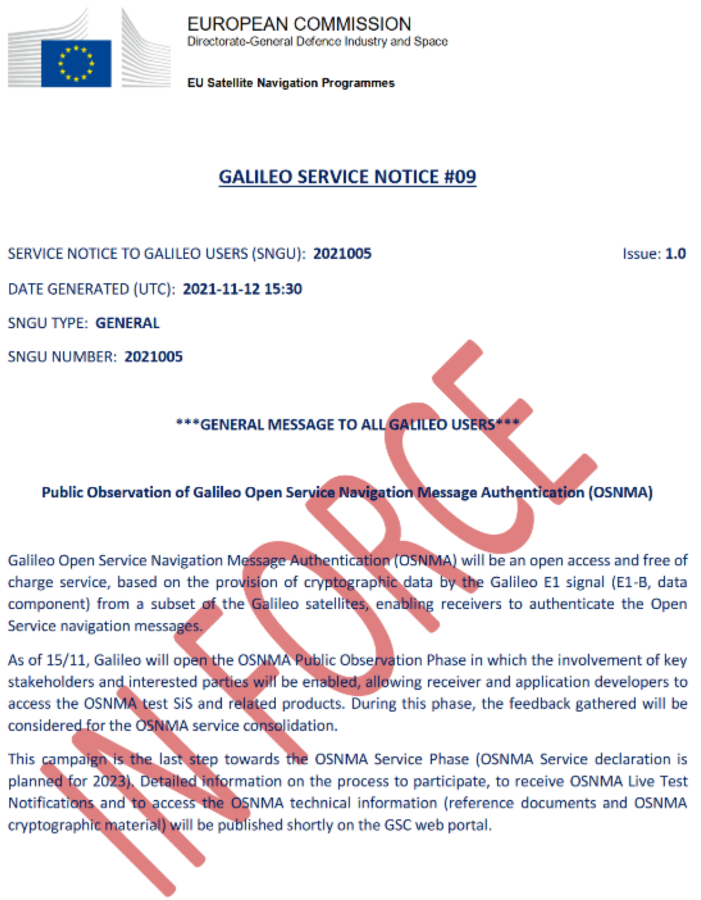
Requisite Cryptographic Key Materials are Available to the Public

2020 — LIVE TEST PREPARATION
- Validation of system and operations readiness

2021 — PUBLIC TESTING
- Publication of OSNMA Info Note V1.0
- OSNMA ICD and RX guidelines for testing
- Broadcast of OSNMA data for testing
- Testing and validation of users implementation

2023 — INITIAL SERVICE
- OSNMA ICD and RX guidelines for service
- Provision OSNMA data

There are Now 20 Galileo Satellites Currently Broadcasting OSNMA


EUROPEAN COMMISSION
Directorate-General Defence Industry and Space

EU Satellite Navigation Programmes

GALILEO SERVICE NOTICE #09

SERVICE NOTICE TO GALILEO USERS (SNGU): **2021005** Issue: **1.0**

DATE GENERATED (UTC): **2021-11-12 15:30**

SNGU TYPE: **GENERAL**

SNGU NUMBER: **2021005**

*****GENERAL MESSAGE TO ALL GALILEO USERS*****

Public Observation of Galileo Open Service Navigation Message Authentication (OSNMA)

Galileo Open Service Navigation Message Authentication (OSNMA) will be an open access and free of charge service, based on the provision of cryptographic data by the Galileo E1 signal (E1-B, data component) from a subset of the Galileo satellites, enabling receivers to authenticate the Open Service navigation messages.

As of 15/11, Galileo will open the OSNMA Public Observation Phase in which the involvement of key stakeholders and interested parties will be enabled, allowing receiver and application developers to access the OSNMA test SiS and related products. During this phase, the feedback gathered will be considered for the OSNMA service consolidation.

This campaign is the last step towards the OSNMA Service Phase (OSNMA Service declaration is planned for 2023). Detailed information on the process to participate, to receive OSNMA Live Test Notifications and to access the OSNMA technical information (reference documents and OSNMA cryptographic material) will be published shortly on the GSC web portal.

Galileo Stated Intentions

- Data Authentication
  - “OSNMA is authenticating data for geolocation information from the Open Service through the Navigation Message (I/NAV) broadcast on the E1B signal component. This is realised by transmitting authentication specific data in previously reserved fields of the E1 I/NAV message.”
- Ranging Authentication
  - “OSNMA will be complemented by the Commercial Authentication Service (CAS), which will offer range authentication in the E6 frequency band”

Why We Are Doing It

How We Are Doing It

Important OS-NMA Features

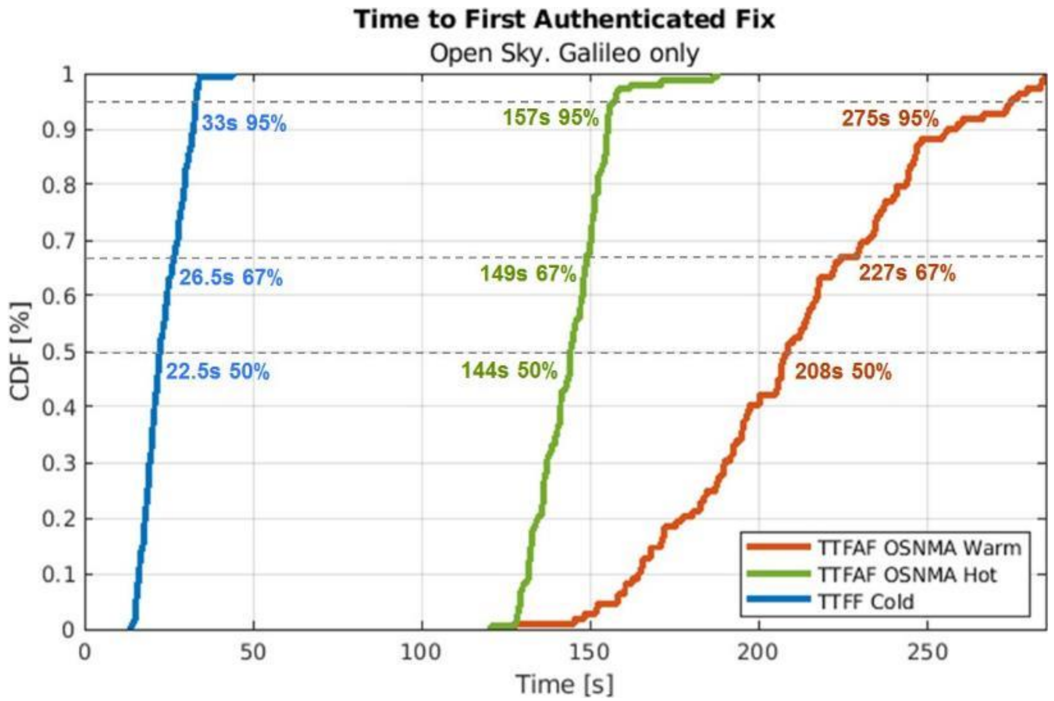
- EUROPEAN GNSS SERVICE CENTRE (GSC): Publication of the OSNMA public keys, crypto material and associated certificates in a way that can be accessible to, and trusted by, end user communities.

- The capability to store and ensure the integrity of a public key, which can be updated if and when necessary through an OTAR (Over The Air Rekeying) mechanism

- to authenticate satellites which do not transmit OSNMA data with the data retrieved from satellites transmitting OSNMA, referred to as *cross-authentication*

OSNMA SiS configuration and performance

Used By Permission:
Protecting satnav from within: Signal-in-space testing results and prospects of Galileo Message Authentication
30/11/2021 – IEEE AESS Spanish Chapter
Ignacio Fernández Hernández



Startup conditions for OSNMA:

- OSNMA Warm Start: Public Key available; TESLA Root Key not-available at startup
- OSNMA Hot Start: Public Key and Root Key available at startup

- Not optimized. Under improvement in receiver implementation

OSNMA SiS configuration and performance

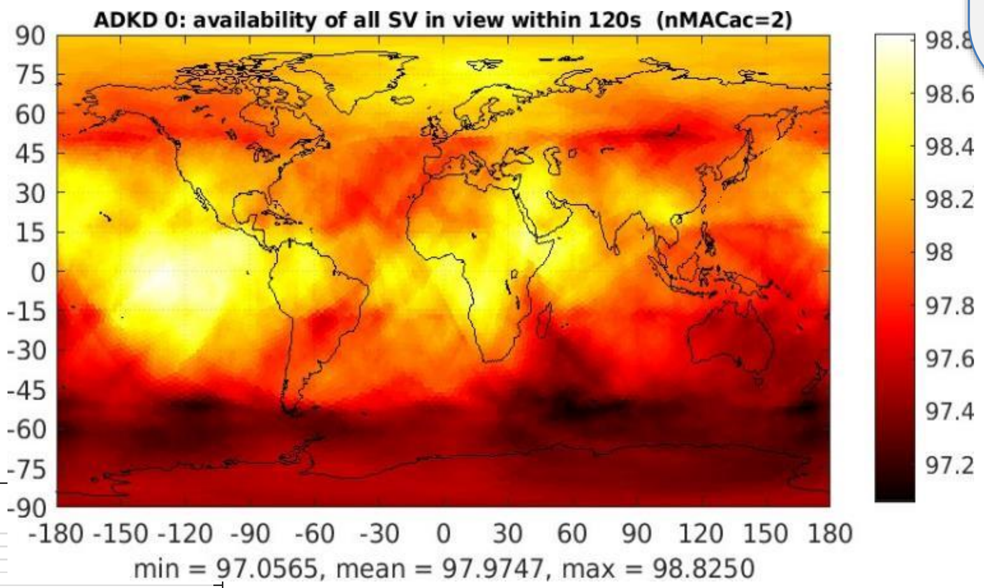
Used By Permission:
Protecting satnav from within:
Signal-in-space testing results
and prospects of Galileo
Message Authentication
30/11/2021 – IEEE AESS
Spanish Chapter
Ignacio Fernández Hernández

Tags for I/NAV ephemeris and
clock correction
for all SV in view
(every 120 sec),
August 2021

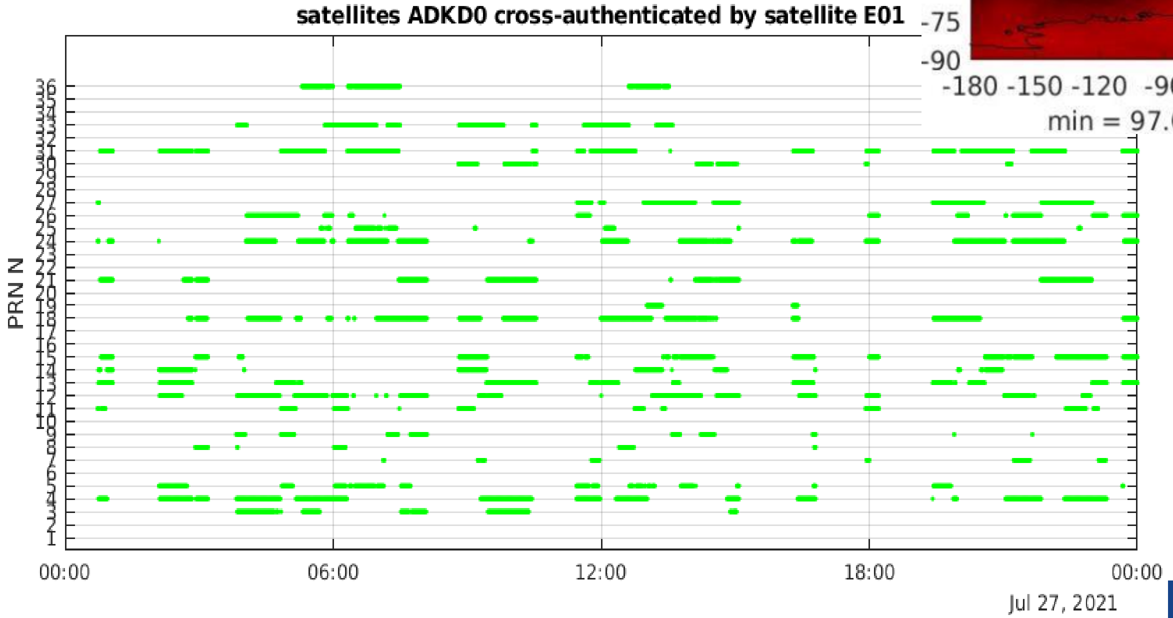
“cross-authentication” feature to increase the availability of tags at user level

Ultimate target is to provide authentication for every visible satellite at user level, and do it frequently

Residual Tag verification failure rate to be expected during the Test Phase



WUL: 97.06%
AUL: 97.97%
BUL: 98.82%



There are 20 Galileo Satellites Currently Broadcasting OSNMA

Prospects

- 2021-2023: Development and validation of the infrastructure to provide OSNMA as an *operational service:* with a service guarantee, signal set to 'operational' (currently 'test')
- 2023:
  - Initial Operation of OSNMA
  - Initial signal capability of ACAS (Assisted Commercial Authentication Service), based on semi-assisted spreading code authentication
- 2024 (TBC):
  - Full OSNMA capability
  - Initial ACAS spreading code authentication service
- Post 2024 (TBC): Galileo 2nd Generation including spreading code authentication in the Open Signal

My Assessment: Well Done and Congratulations!

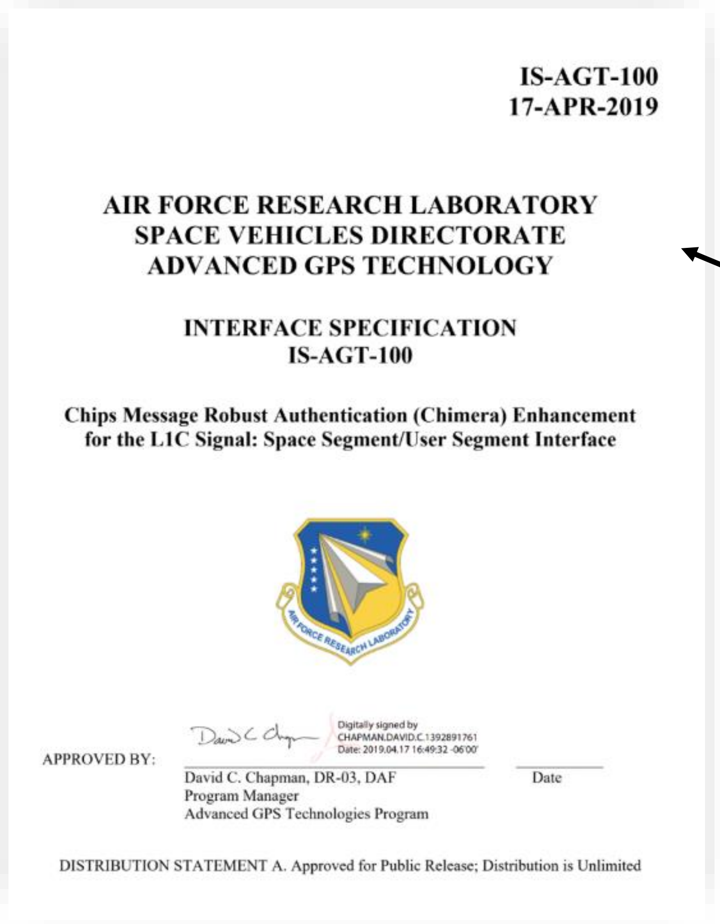
- The Galileo Team Has Done a Superb Job of Designing and Fielding the World's First Civil SATNAV Authentication Capability

- They Have a Strong Vision of How to Evolve the Design As New Satellite Capabilities Become Available and They Have the EU Leadership Support

Chimera is a Backwards Compatible Security Overlay for the L1C Civil Signal

IS-AGT-100 Defines an Experimental KISS Signal That Embodies Most Concepts from my 2003 and 2013 papers

- Data Authentication
  - Message Signing
  - KISS & TESLA Options
- Ranging Authentication
  - Fast & Slow Watermark Channels
    - 6 or 1.5 second epoch (Fast)
    - 3 or 1.5 minute epoch (Slow)



IS-AGT-100
17-APR-2019

AIR FORCE RESEARCH LABORATORY
SPACE VEHICLES DIRECTORATE
ADVANCED GPS TECHNOLOGY

INTERFACE SPECIFICATION
IS-AGT-100

Chips Message Robust Authentication (Chimera) Enhancement
for the L1C Signal: Space Segment/User Segment Interface

AIR FORCE RESEARCH LABORATORY

APPROVED BY:

Digitally signed by CHAPMAN.DAVID.C.1392891761
Date: 2019.04.17 16:49:32 -06'00'

David C. Chapman, DR-03, DAF
Program Manager
Advanced GPS Technologies Program

Date

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution is Unlimited

Had Its Origins In the Film Industry ca. 2002

Formally Proposed for L1C in 2005

Signal Specification and Select Papers are at
http://www.gpsexpert.net/chimera-specification

Chimera Will Be Broadcast by NTS-3

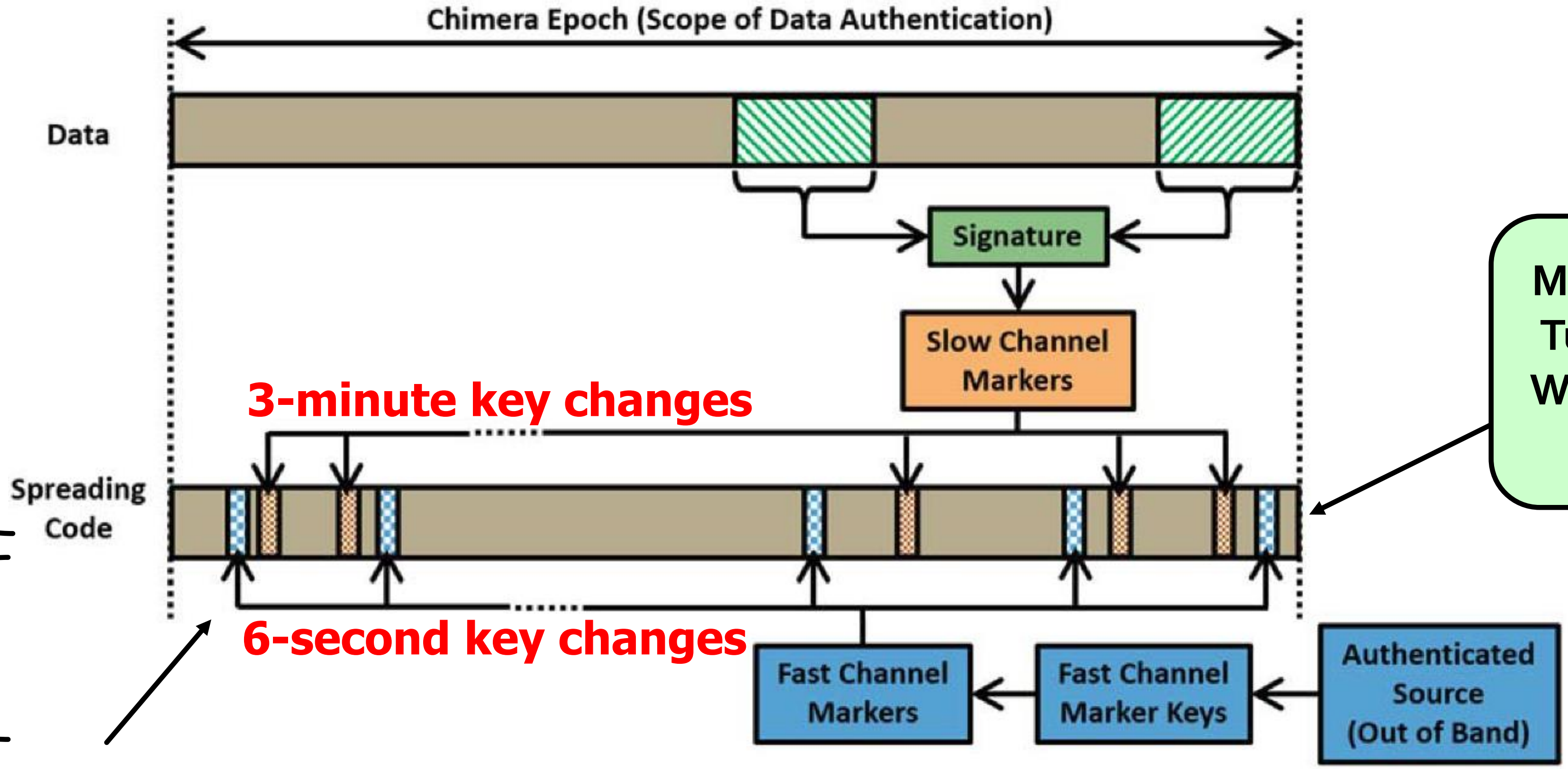
- SDR Based Navigation Satellite Planned for Launch in 2023
- Takes About 18 Months to Field a New Signal If Starting From Scratch
- Chimera and Several Variants Are Already Running

CHIMERA Signs Data Messages with ECDSA P-224 Signature

Message Signature Is Hashed to Create the Slow Channel Marker Generation Key

L_1C Data
Data Authentication
3-minute epoch

L_1C Pilot
Ranging Authentication
6-second epoch



Markers Can Be Turned OFF, In Which Case It Is NMA-Only

Markers Work Like the "Not So Good" Navigation System

From IS-AGT-100

Receiver Collects Snapshots for Watermark Detection

Several Commercial Receivers Already Have Snapshot Capability

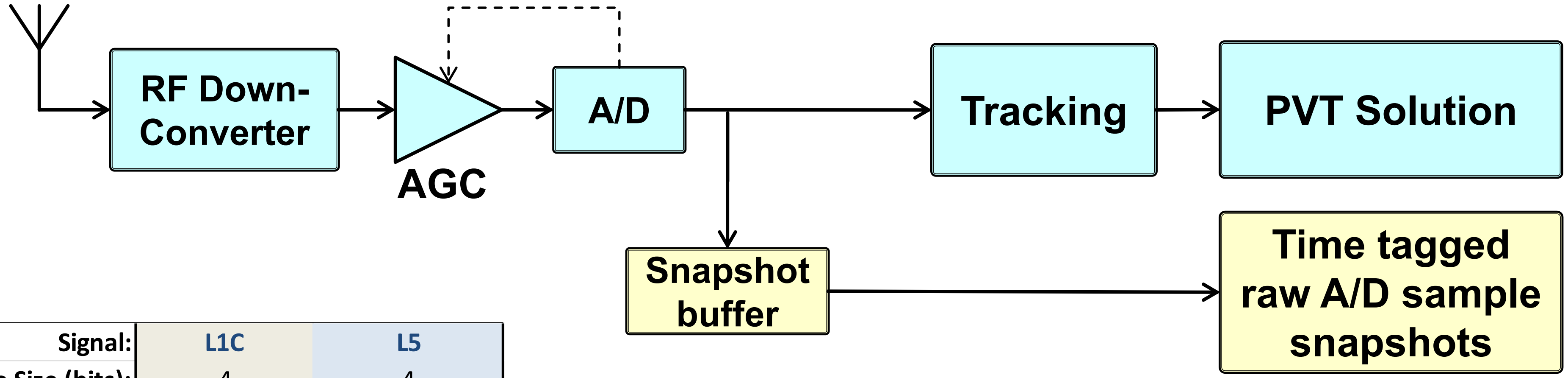


figure after Neil Gerein, Hexagon

Signal:	L1C	L5
Sample Size (bits):	4	4
Sample Rate (MHz):	10	40
Corresponding bytes/sec:	5000000	20000000
Collection Interval (sec)	Storage Requirement (Mbytes)	
0.02	0.10	0.40
0.10	0.50	2.00
0.50	2.50	10.00
1.00	5.00	20.00
2.00	10.00	40.00
3.00	15.00	60.00

[SUM_NTS_2.xlsx]Data Collection Size

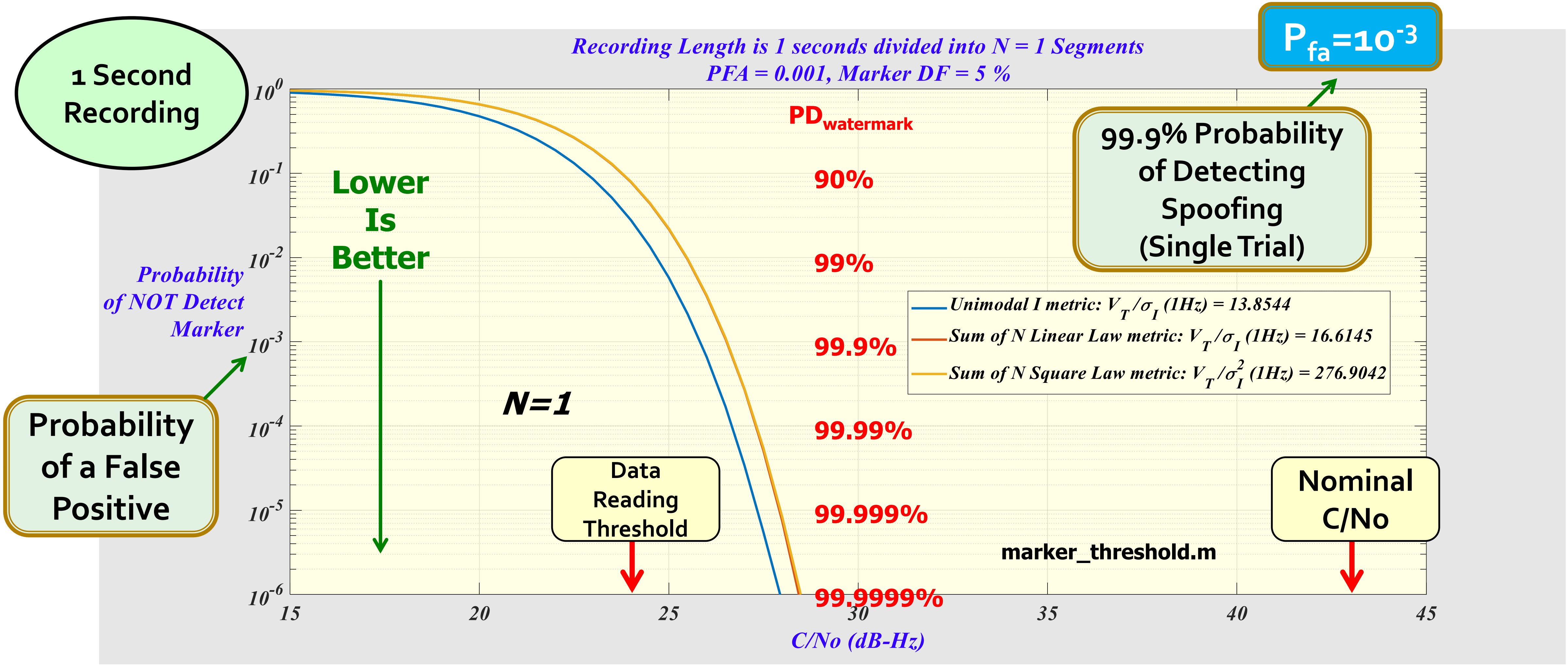
- Snapshot Collections Have Diverse Applications
  - Process Locally for Pseudorange Authentications
  - Send to Remote Locations for Proof of Location
  - Use For Jamming Signature Analysis
  - Often Part of Acquisition Engine

To Authenticate the Signal

- Data Authentication
  - Verify Data Messages Using Digital Signature Appended to Data
    - It's in Subframe 3, Message Type 8 & 9
- Ranging Authentication
  - Collect Some RF Snapshots Prior to Key Publication
  - When Marker Key Becomes Available, See if Marker Range Equals Clear Signal Range

The CHIMERA Signal Is Designed to Provide Ranging Authentication over the Full Range of Normal C/Nos

There are more sophisticated processing algorithms than these



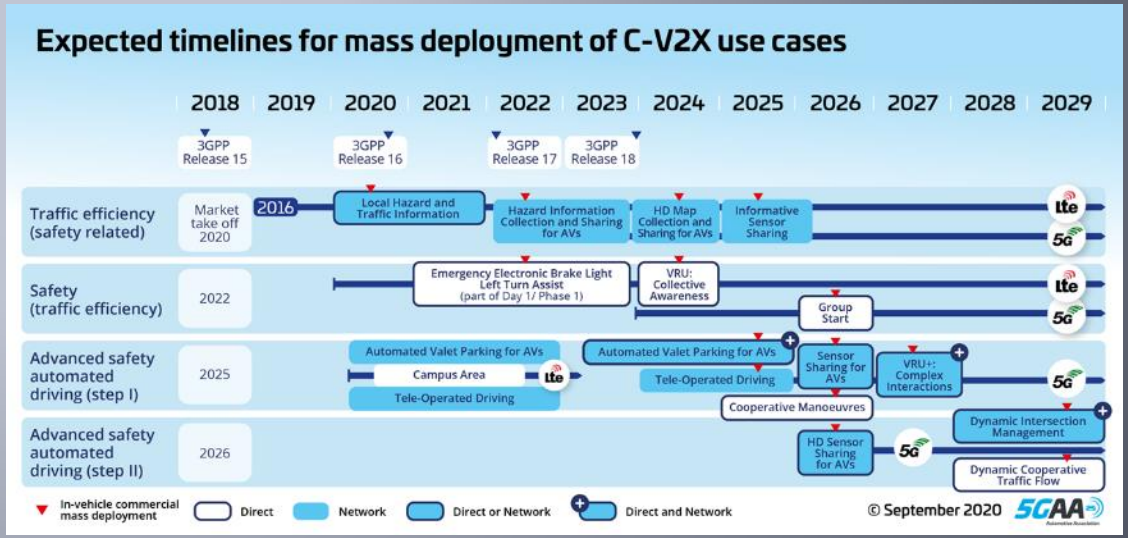
Navigation Message Authentication (NMA) Is A Step In the Right Direction But it is Not Sufficient; Need Watermarks Too

- Many Civil Receivers In Security Related Applications Do Not Read Data
  - Asset Tracking Devices
  - Snapshot Pseudoranges for Low Power Applications
- NMA Does Not Provide a Basis for Proving Location to Remote Monitors

The Role of 5G NR In Securing Civil PNT

Developments Can Happen Fast in Cellular

Positioning Is an Important Thrust in Support of Connected Vehicle and IIoT Markets



Logan Scott / LS Consulting

Target requirements for 5G NR Positioning Enhancements in Release-17 (2022)

From 3GPP TR38.857 V 17.0.0 (2021-03)

	Commercial Use Cases	Industrial IoT Cases
Horizontal Position Accuracy (90%)	< 1 meter	< 0.2 meter
Vertical Position Accuracy (90%)	< 3 meter	< 1 meter
End-to-End Latency for UE Position Estimation	< 100 msec	<100 msec (10 msec desired)
Physical Layer Latency for UE Position Estimation	< 10 msec	<10 msec

- Aggressive Performance Targets Based on Experimental Results
  - Tech Reports from Industry Leaders Huawei, ZTE, Nokia, Ericsson, Interdigital, Qualcomm, Intel
  - Diverse Techniques: TDOA, RTT, AoA, Hybrids etc.
- Significant Discussion of Integrity, Spoofing, Authentication (and Chimera)
- Very Strong Synergism between Chimera / Galileo CAS

3GPP Follows a Two-Year Major Release Cycle Upgrade Cycle Enabled by SDR

Unlike GPS, the Basestations are SDR. This Enables Rapid, Needs Based, Evolutionary Path

2021	2022				2023				2024	
Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2

TSG#94-e	TSG#95-e	TSG#96	TSG#97	TSG#98	TSG#99	TSG#100	TSG#101	TSG#102	TSG#103
Dec.	Mar.	Jun.	Sep.	Dec.	Mar.	Jun.	Sep.	Dec.	Mar.

Rel-18 Package (content) Approval

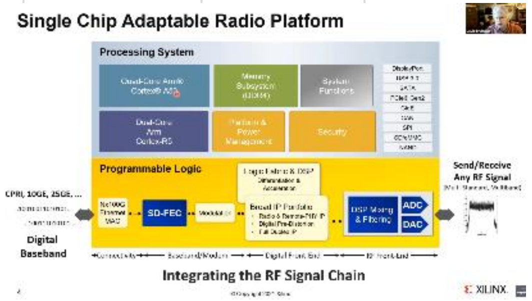
Rel-17 Stage 3 Freeze

Rel-17 Protocol Coding Freeze (ASN.1, OpenAPI)

Rel-18 Stage 2 Functional Freeze

Rel-18 Stage 3 Freeze

Rel-18 Protocol Coding Freeze (ASN.1, OpenAPI)

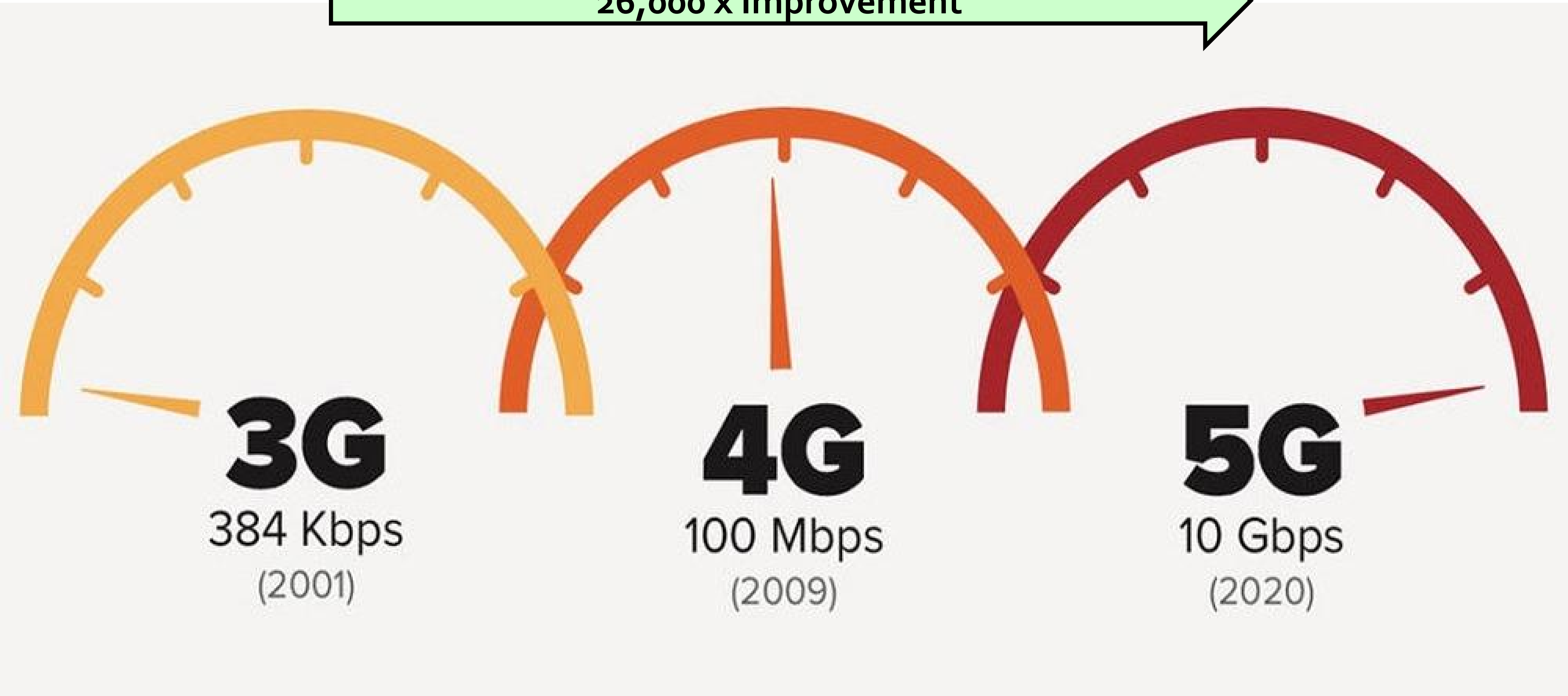


https://www.3gpp.org/release18

Sept. 2021

An SDR Evolutionary Scale

26,000 x Improvement



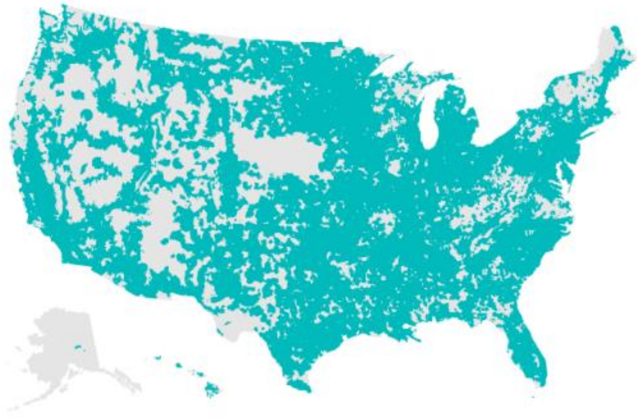
Graphic from: https://www.whatmobile.net/Opinion/article/difference-3g-4g-5g

In Developing a Comprehensive Strategy, Don't Overlook the Role of Cellular in Civil PNT

- There are 417,000 Cellular Base Stations in the US*, Mostly with Power and Timing Backups
  - $30 Billion Capital Expenditure in 2020*

- There are GPS Dependencies But there are also Good Alternatives for Required Timing
  - GNSS Diversity
    - It is Extremely Unlikely All 4+ Systems will Fail Simultaneously
  - IEEE P1588
    - Precision Clock Synchronization Protocol
  - LF (eLoran Frequencies)
    - New secured signal structures optimized for timing radiocalibration
  - Several Others

Current 5G Deployment*



* https://api.ctia.org/wp-content/uploads/2021/07/2021-Annual-Survey-Highlights.pdf

A Parting Recommendation

The Greatest Risk is Taking Insufficient Risk

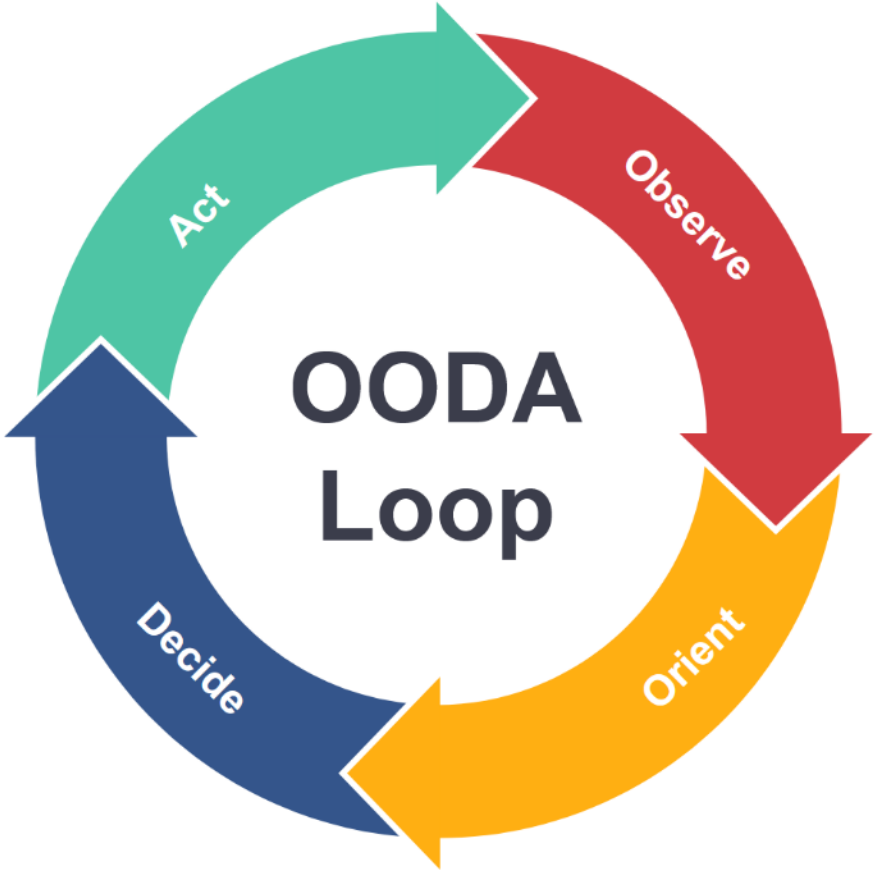
The Chimera Saga Illustrates a Much Larger Issue in Resiliency

- One of the riskiest things we can do as a nation is launch SatNav satellites without software defined radio (SDR) but with a projected lifetime of > 15 years
- With an SDR on orbit, from inception to first broadcast takes about 18 months
  - Can Respond to Unforeseen Needs
- Without SDR, we are betting that we can see > 20 years into the future

"A strong wind may topple the sturdy oak, but the willow bends and lets the wind pass through" Lao Tzu

Backups

3 Years or 20 Years?



Observe

What is the current situation? What is the reason you want to change? how bad do you want to change?

Orient

Where are you currently at relative to where you want to go? How far is it to your destination?

Decide

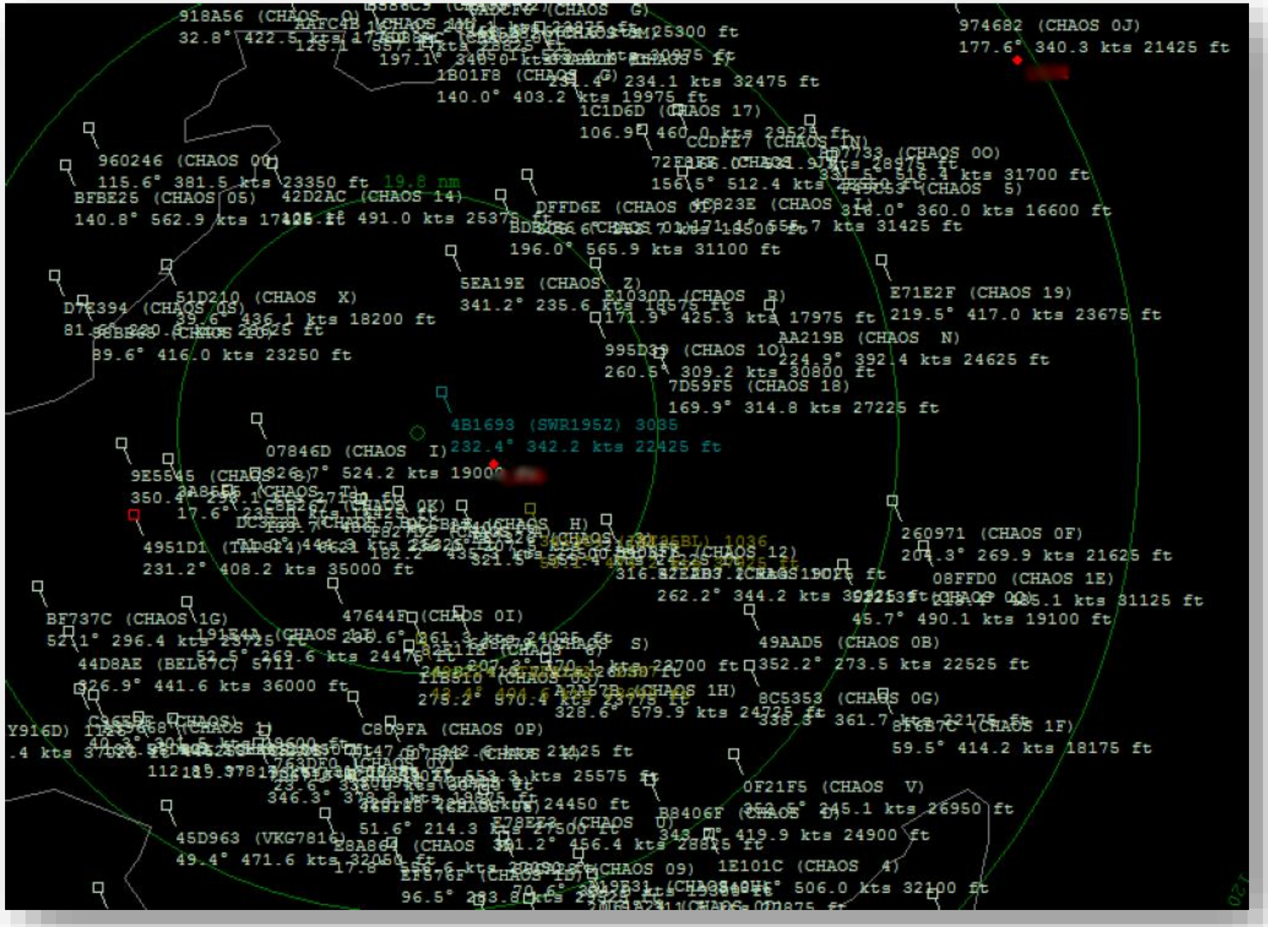
What is the exact path you are going to take? How are you going to handle challenges and set backs?

Act

What's the approach and method you will take to implement the decisions? What is your action plan?

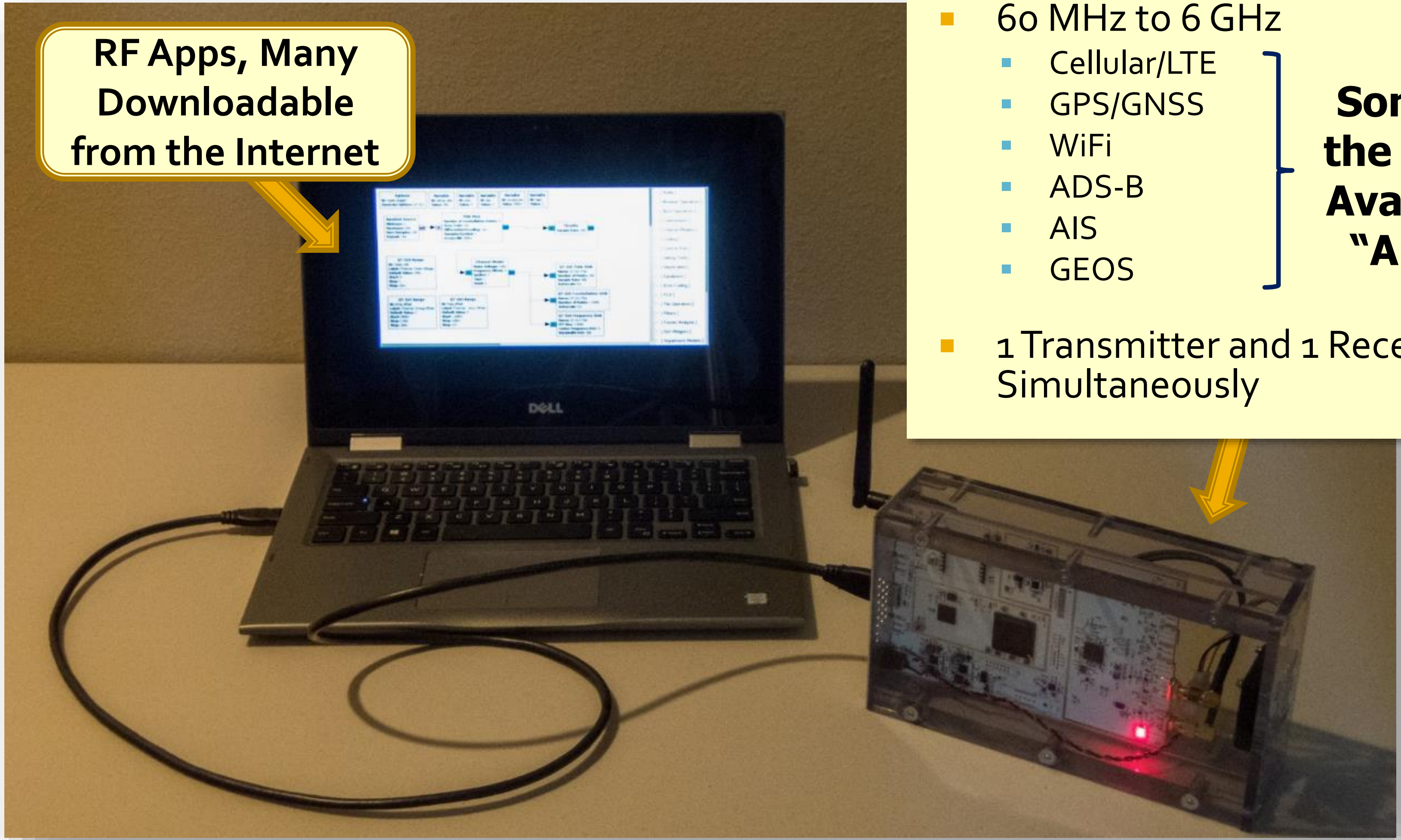
Ghost Aircraft Injection Into an SBS-3 ADS-B Receiver Using a USRP N210 SDR

An Example of Why Existence Proofs are Needed



From: Matthias Schäfer, Vincent Lenders, and Ivan Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication", 11th International Conference, Applied Cryptography and Network Security 2013, Banff, AB, Canada, June 25-28, 2013

Software Defined Radio (SDR) is the Radio Equivalent of a Microphone (Receiver) and a Speaker (Transmitter)



- 60 MHz to 6 GHz
  - Cellular/LTE
  - GPS/GNSS
  - WiFi
  - ADS-B
  - AIS
  - GEOS

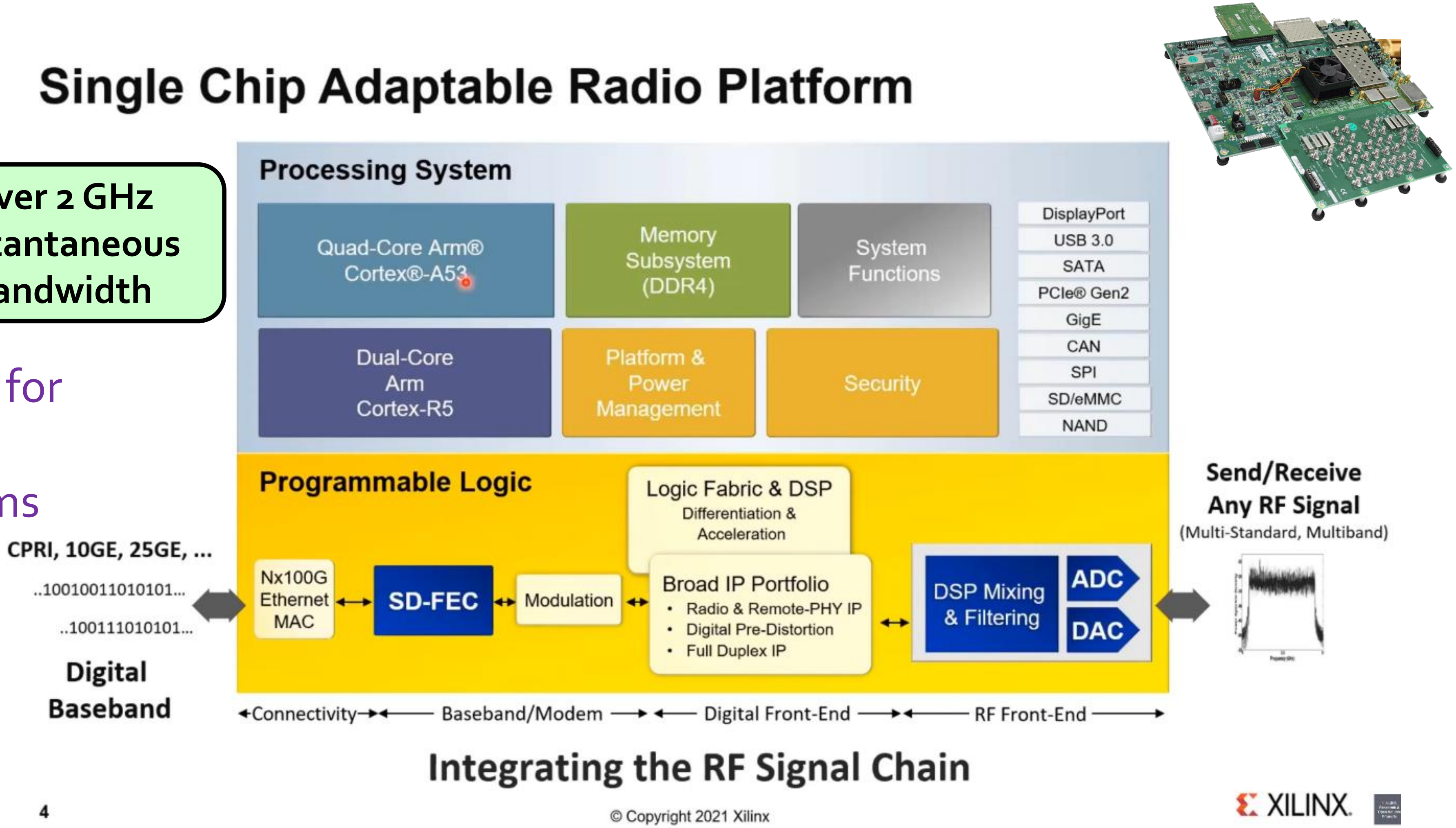
Some of the many Available "Apps"

- 1 Transmitter and 1 Receiver Simultaneously

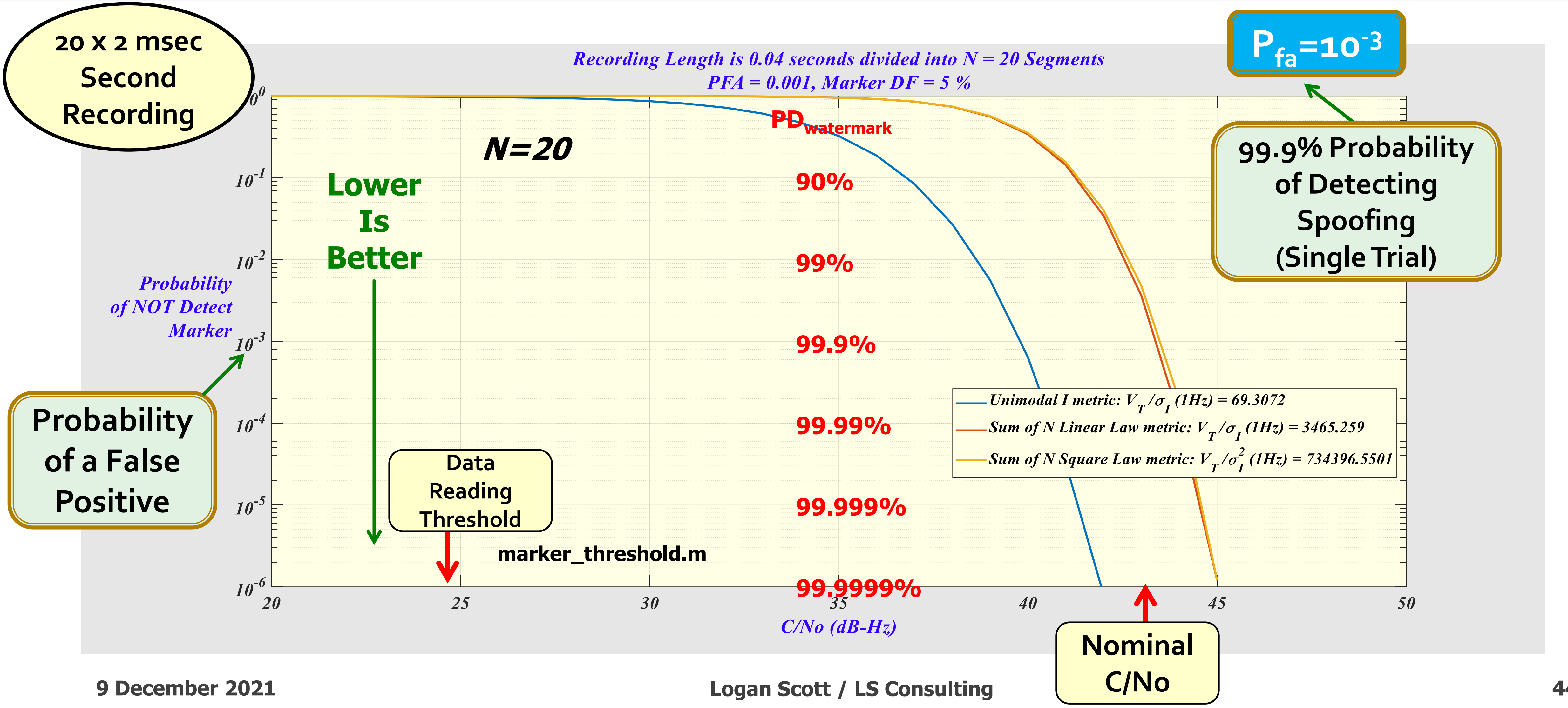
Advanced SDR Can Comprehensively Spoof RF Environment
The Cellular Industry Is a Key Driver in Software Defined Radio Development

- ZU28DR (Gen1)
  - 4 GHz ADCs (8)
    - 12-bit
  - 6.5 GHz DACs (8)
    - 14-bit
  - Large FPGA Optimized for DSP
  - ARM Processing Systems
  - 2 Gbit/sec FEC Decode
    - 38.212 Compliant
  - 9 – 50 Watts?
    - Depends on what you implement

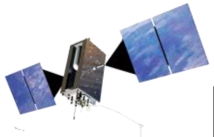
Over 2 GHz Instantaneous Bandwidth



Short Recordings Can Authenticate Signal When Operating at Nominal C/No



Apriori Receiver Time Uncertainties and Marker Generation Key Time of Publication Determines Which Markers Can Be Used in Authentication



Satellite

Marker Key$_{N-1}$ Used To Generate Markers	Marker Key$_{N}$ Used …

Receiver

Marker Key N-1 Published

Markers Potentially Collected By Receiver

Adversary Could NOT Have Had Marker Generating Key *(OK to Use These for Authentication)*	Adversary Could Have Had Marker Generating Key

Reachback

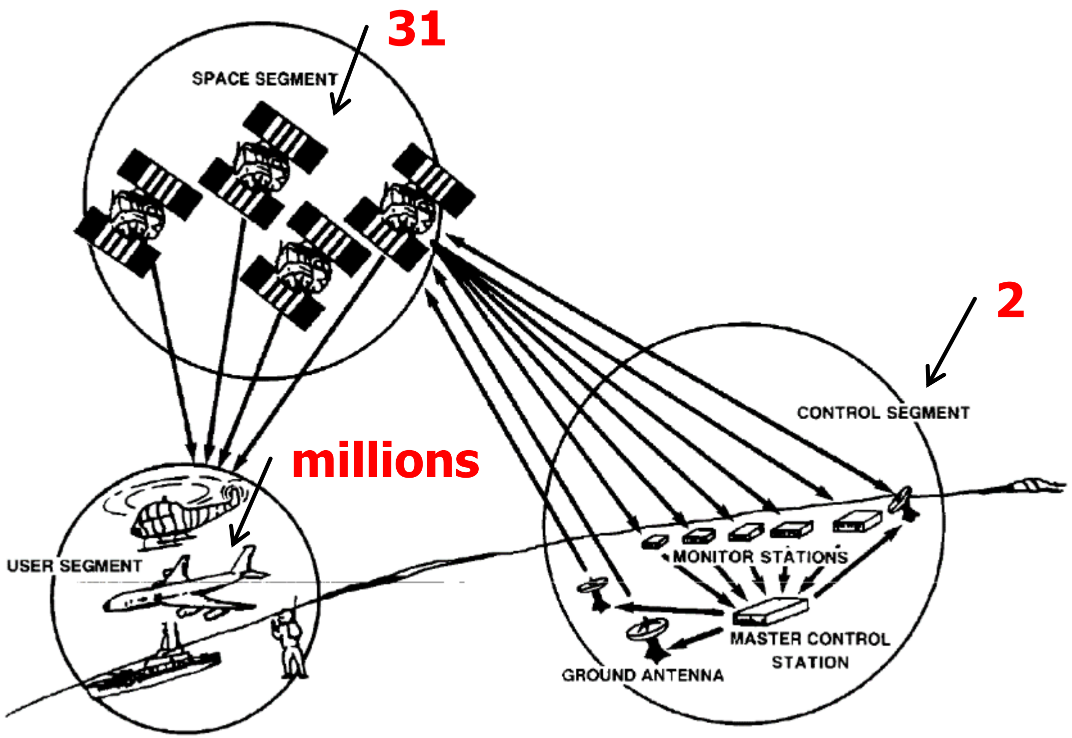
Receiver Knows Time to Be In This Range

Time

Receivers Must Establish & Maintain Golden Time

SatNav Architectures Are Based on One-Way Communications

- SatNav Signal Authentication Is Via
  - Pre-shared Symmetric Keys
    - Military/Authorized
  - Delayed Keys
    - Watermarks
  - Other Signals
    - GNSS
    - IMU
    - etc



Two-Way Communications Supports Superior Identity and PNT Authentication

1. UE sends a Nonce (Random Number) to the gNodeB
2. gNodeB signs Nonce using its Private Key
3. UE authenticate Nonce using gNodeB's Public Key (Certificate)
4. Now the UE Knows Who it is Talking To

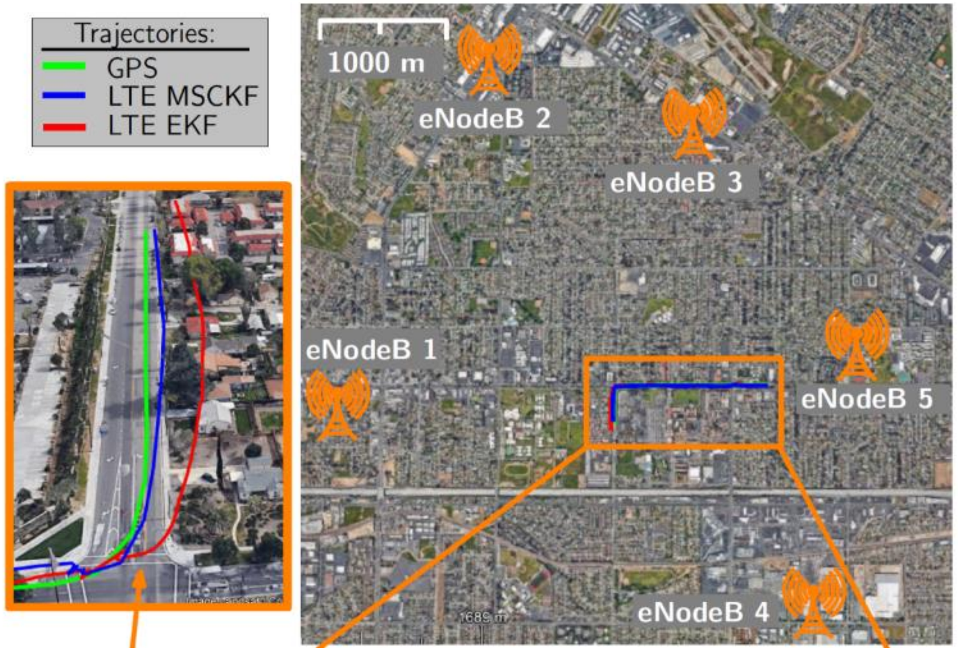


Figure from: Positioning Performance of LTE Signals in Rician Fading Environments Exploiting Antenna Motion
Kimia Shamaei, Joshua J. Morales, and Zaher M. Kassas
31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 24-28, 2018

The State of Play on Civil SatNav Authentication

- The EU has Done a Really Fine Job of Designing and Deploying OS-NMA
- Data Authentication is a Major Step In the Right Direction But Insufficient
  - Both E1-B I/NAV and Chimera Support This
  - Securing L1 C/A Code LNAV Presents Unique but Solvable Challenges
- Ranging Authentication is Needed
  - Chimera and E6C (and Probably E1-C) Support this
  - Snapshot Receivers That Do Not Read Data
  - Proofs of Location

A Tip for Receiver Manufacturers: Implement OS-NMA In Your Receivers. You will Learn a Lot and Be Prepared for a Coming Market Shift

- Deployment Timeframes for Combined Data/Ranging Authentication
  - Would be About 2 – 3 Years With SDR Based SatNav Satellites
  - >10 Years with Non SDR Satellites
    - Replenishment Schedules

An Action Plan for the US on Authenticatable Signals

- Put Data Authentication Capability on L1C, L2C, L5, and WAAS
  - Potentially Workable with Current GPS Satellites
  - Use cross authentication techniques to cover L1 C/A & Galileo
- Put Ranging Authentication on WAAS, L1C, & L5
  - There are diverse marker strategies
- Take Advantage of Deployed 5G Infrastructure
  - There are Extremely Powerful Synergies between Chimera & 5G for Securing and Assuring PNT
  - Opportunities for Input to 5G Standardization Process