UHU TECHNOLOGIES

UHU Technologies Briefing

NavTech 22 Seattle WA

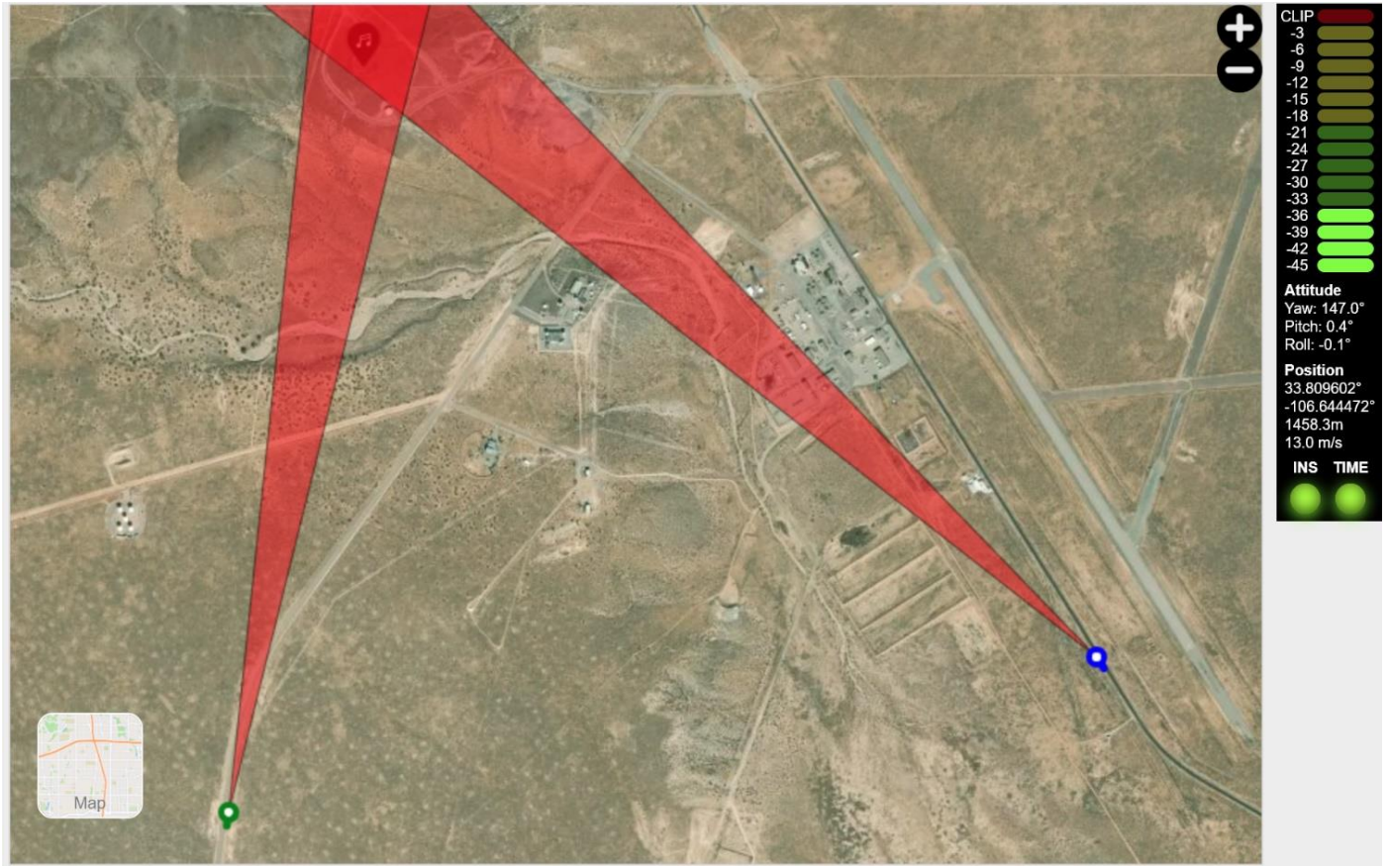
December 6th, 2022

972.905.0437

www.uhutechnologies.com

Itinerary

- GPS Spoofing Overview
- Current Market Solutions
- UHU’s Approach
- Long Beach Deployment
- Conclusion



GPS Spoofing Overview

What is GPS Spoofing?

- GPS spoofing occurs when an attacker transmits a fake GPS signal that can alter the position or time reported by a victim GPS receiver
- The GPS constellation, as well as the other GNSS constellations (Galileo, GLONASS, etc.) are highly susceptible to spoofing using readily available simulator technology
- Spoofing (unlike jamming) is extremely difficult to detect

GNSS Spoofing events: (that we know of)

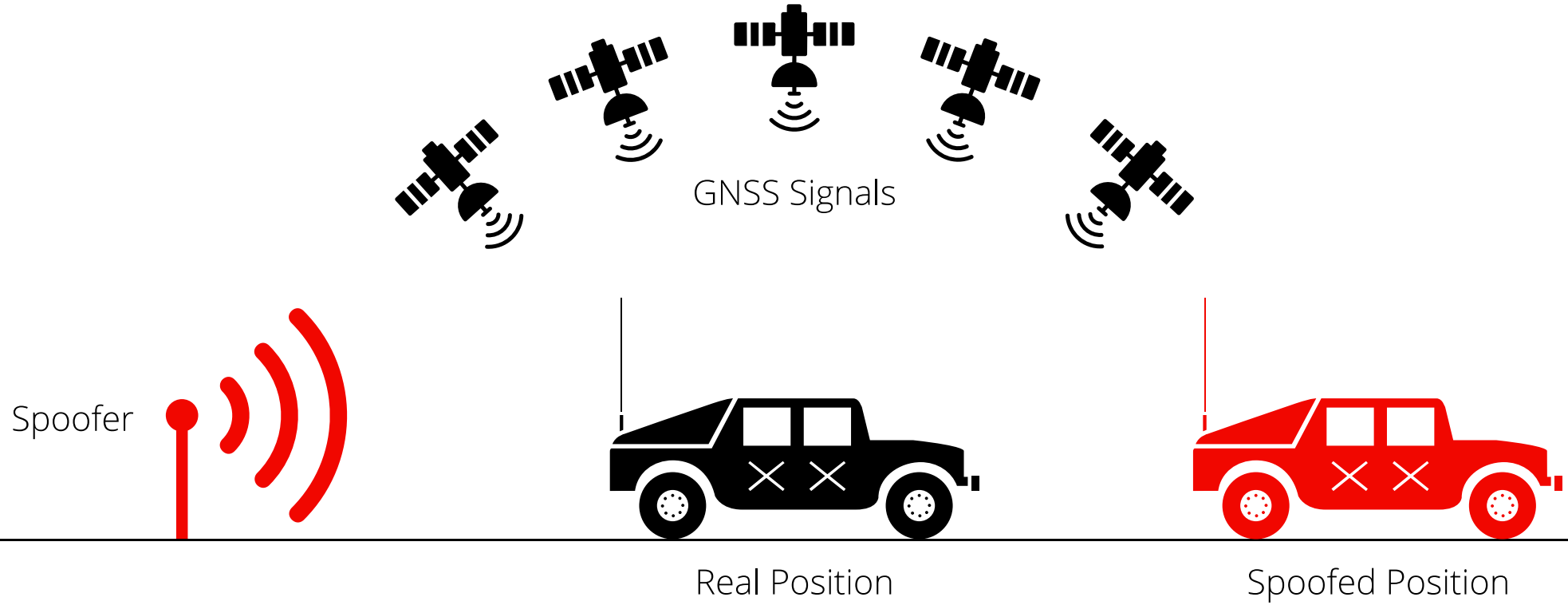
- **Ghost Ships, Crop Circles: A GPS Mystery in Shanghai - Multiple ships impacted: Nov 2019.**
- **Russia – Multiple Jamming and Spoofing events**
  - Baltic Sea, Crimean Peninsula, Syria, Kerch Strait, Mediterranean Sea…..
  - 66-page report by **THE CENTER FOR ADVANCED DEFENSE STUDIES (**C4ADS) experts listed 9,883 instances of GPS spoofing in Russia.
- **Over 400 GPS Problems reported over last 5 years.**
  - US Coast Guard Navigation Center report: Oct. 2022

GNSS Spoofing events Continued: (that we know of)

- **GPS interference caused the FAA to reroute Texas air traffic. Experts stumped**
  - October 2022 – 2 days
- **GPS outage in Denver, effected the airport, municipal rail systems and more**
  - January 2022 – 33.5 hours
- **Thousands of GNSS jamming and spoofing incidents reported in 2020**
  - Resilient Navigation and Timing Foundation report: Dec. 2020
- **Multiple Military events we can't discuss!**

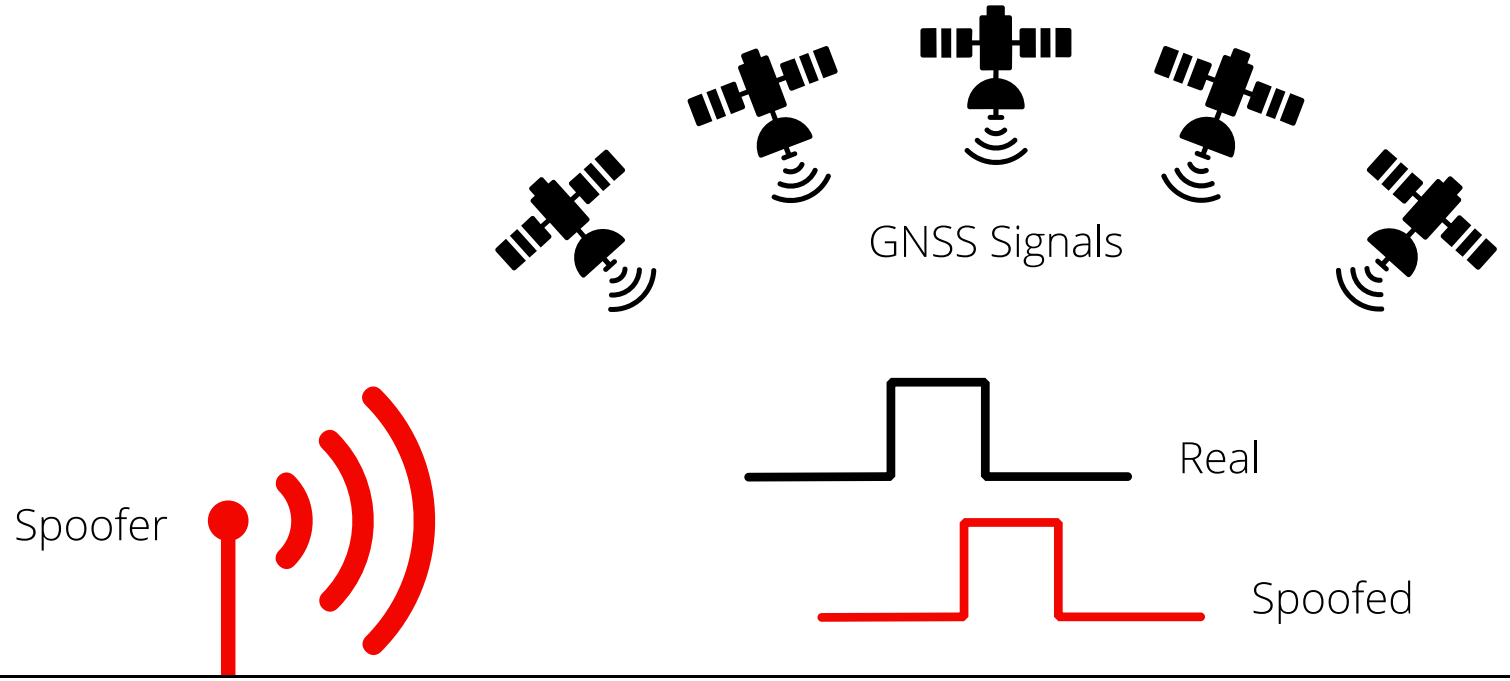
GPS Spoofing Overview

Position Walk Attack



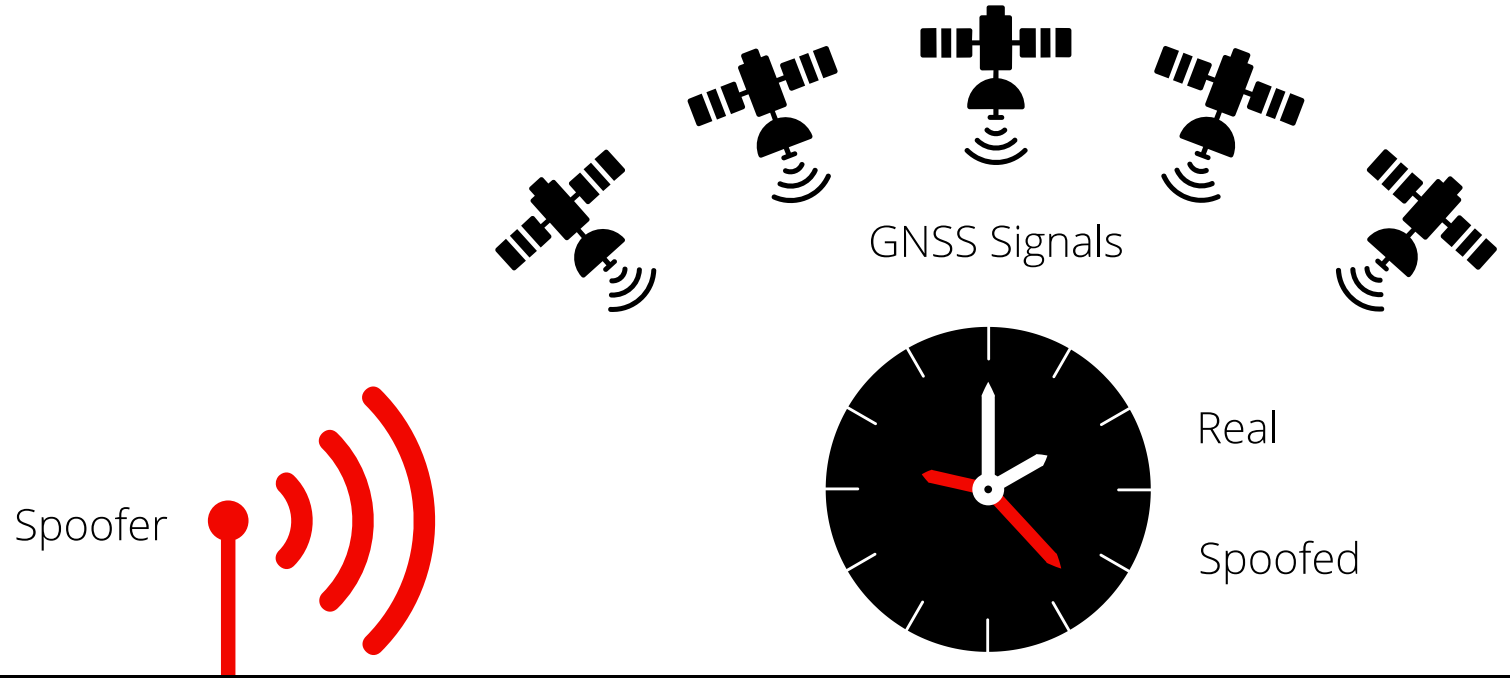
GPS Spoofing Overview

Time Walk Attack



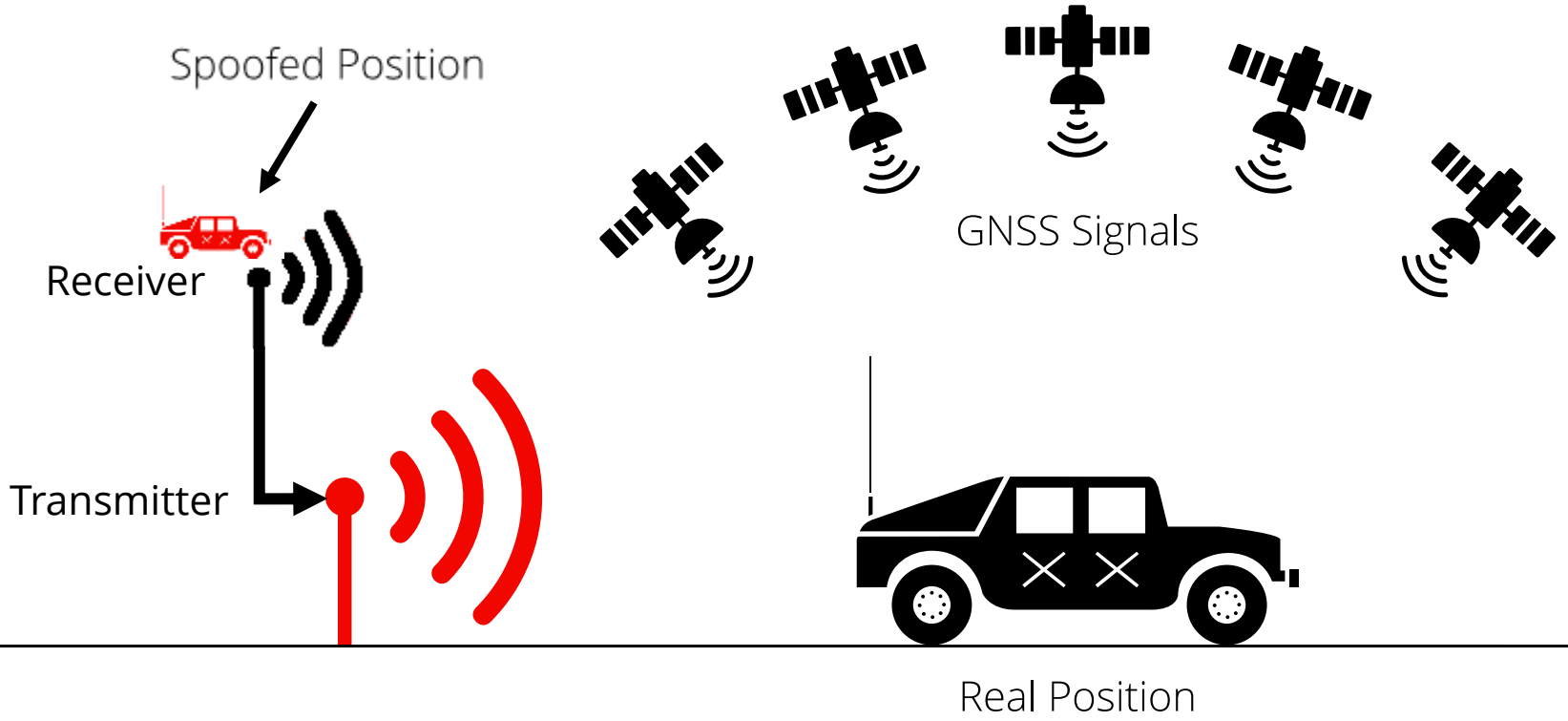
GPS Spoofing Overview

Time Jump Attack



GPS Spoofing Overview

Repeater Attack



GPS Spoofing Overview

Results of Spoofing

- Cases of documented spoofing attacks are becoming more common
- Critical infrastructure is vulnerable
- Potential impact (and liability) is extreme
- Major industries are effected: Power, Telecom, Transportation, Finance

GPS Spoofing Overview

- **Numerous GPS products claim to be resilient against spoofing attacks**
- **Spoofing protection from these products generally rely on one or more of the following methods:**
  - Analysis of downlink navigation message
  - Multi-GNSS (GPS + Galileo + GLONASS) redundancy
  - Multi-frequency (L1/L2/L5) redundancy
  - Alternate time sources (NTP, PTP, Radio, IRIG, etc.)

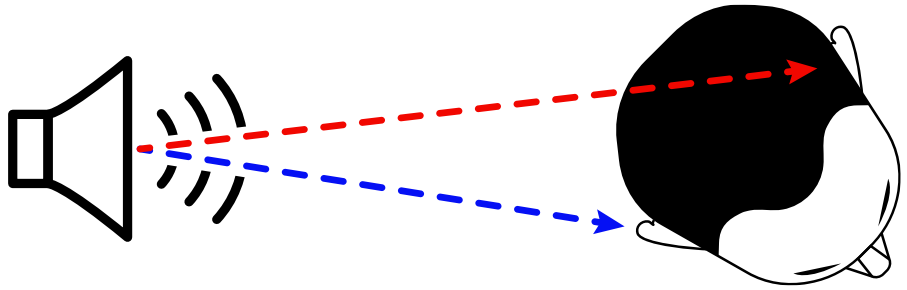
Current Market Solutions

- **Existing market solutions do not provide adequate protection for high value installations against GPS spoofing!**
  - ❌ Analysis of downlink navigation message
  - ❌ Multi-GNSS (GPS + Galileo + GLONASS) redundancy
  - ❌ Multi-frequency (L1/L2/L5) redundancy
  - ❌ Alternate time sources (NTP, PTP, Radio, IRIG, etc.)
- **UHU has developed a solution that cannot be spoofed**
  - ✅ A patented technique that guarantees the integrity of your GPS solution

UHU's Approach

Angle of Arrival – A technique borrowed from the Signals Intelligence (SIGINT) world

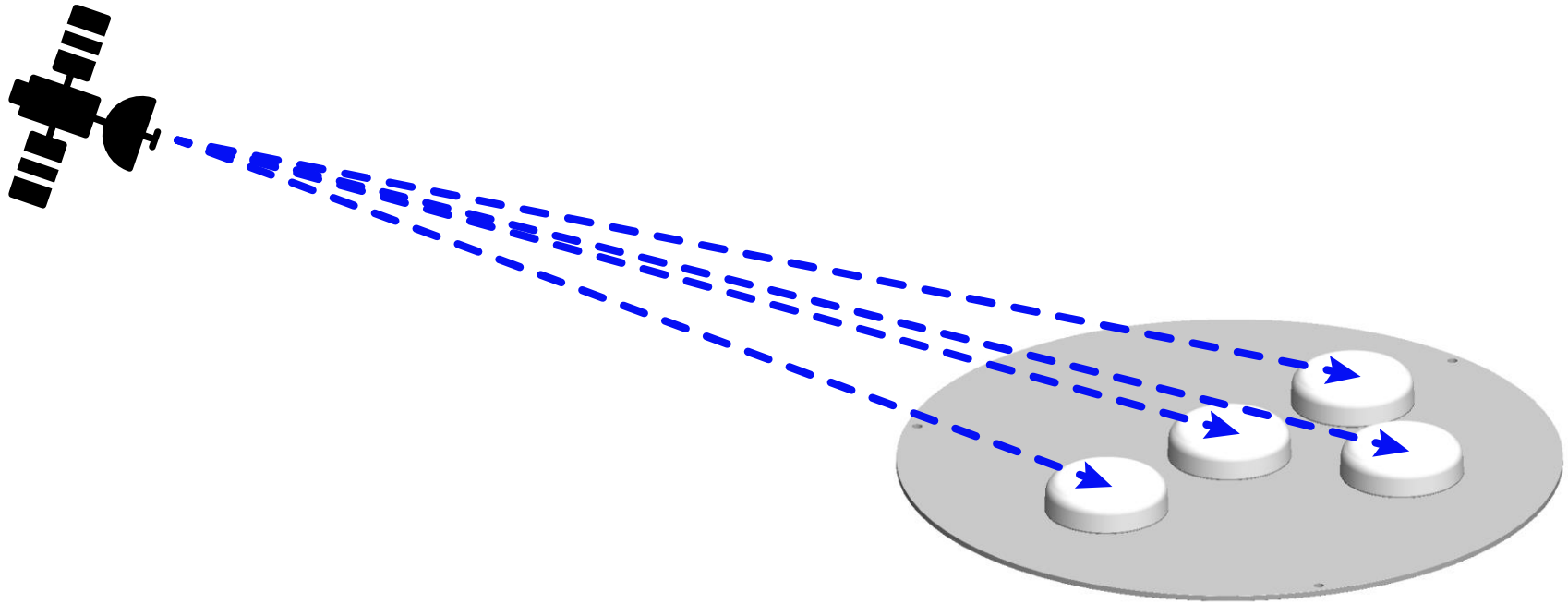
- RF (radio frequency) signals travel at the speed of light
- They can be thought of as fast-moving waves
- Just like your ears can perceive the direction of sounds, multiple antennas can be used to perceive the direction of RF waves



UHU's Approach

Angle of Arrival – How it works

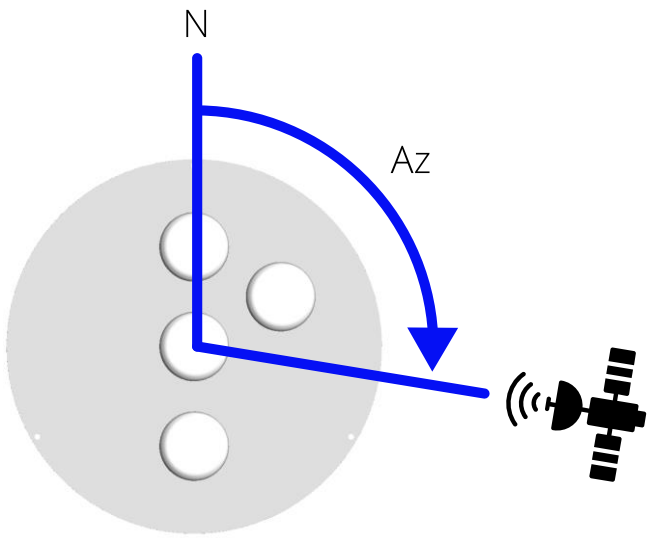
The RF wave arrives at each antenna element at a slightly different time

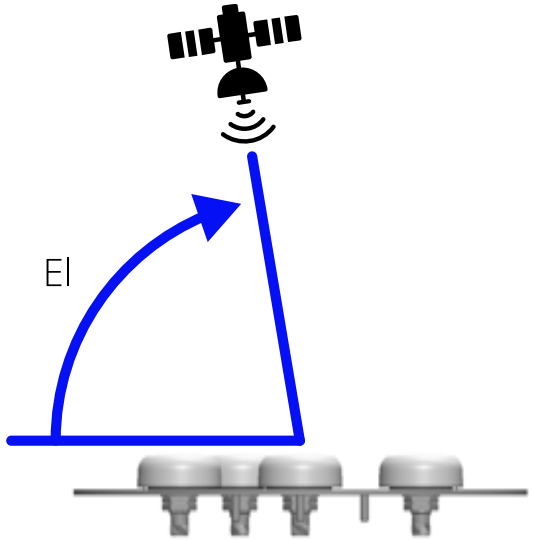


UHU's Approach

Angle of Arrival – How it works

The differences in arrival time are then used to calculate the Azimuth (Az) and Elevation (EL) of each received signal

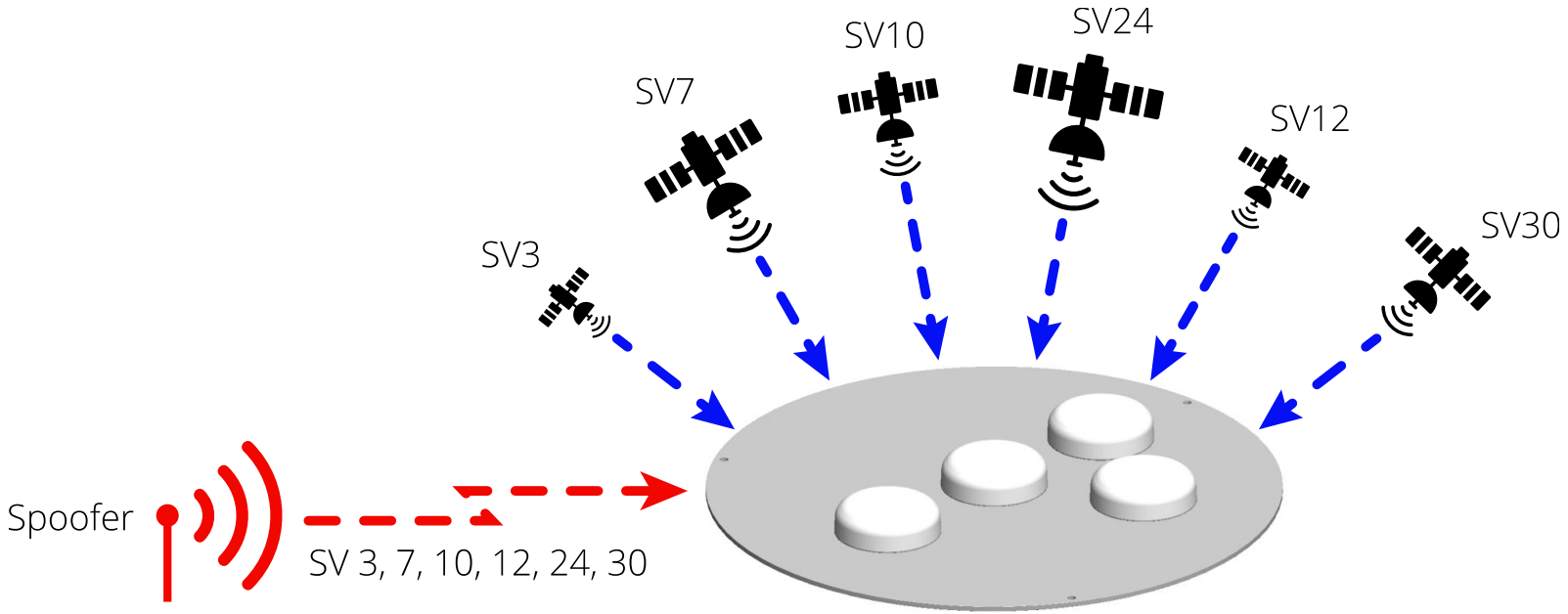




UHU's Approach

Angle of Arrival – How it works

Once the Angle of Arrival (or AOA) is calculated for each received signal, it can be determined if that signal is from a valid satellite or if it's a spoofer



UHU's Approach

- **Angle of Arrival is the only guaranteed technique to detect spoofers (also works for Jammers!)**
- **The Angle of Arrival is the only characteristic that cannot be spoofed**
- **Patent No. 10,162,060**
- **We report the Angle of Arrival of the threat**

  If multiple systems are installed in the area, the position of the threat can be geolocated (valuable information to the FCC and law enforcement)

Northstar Product

The Northstar is a 1U Rackmount GPS Health Monitor:

- The Northstar is certified by the UL (60950-1) and has passed FCC testing (Part 15 Class A)

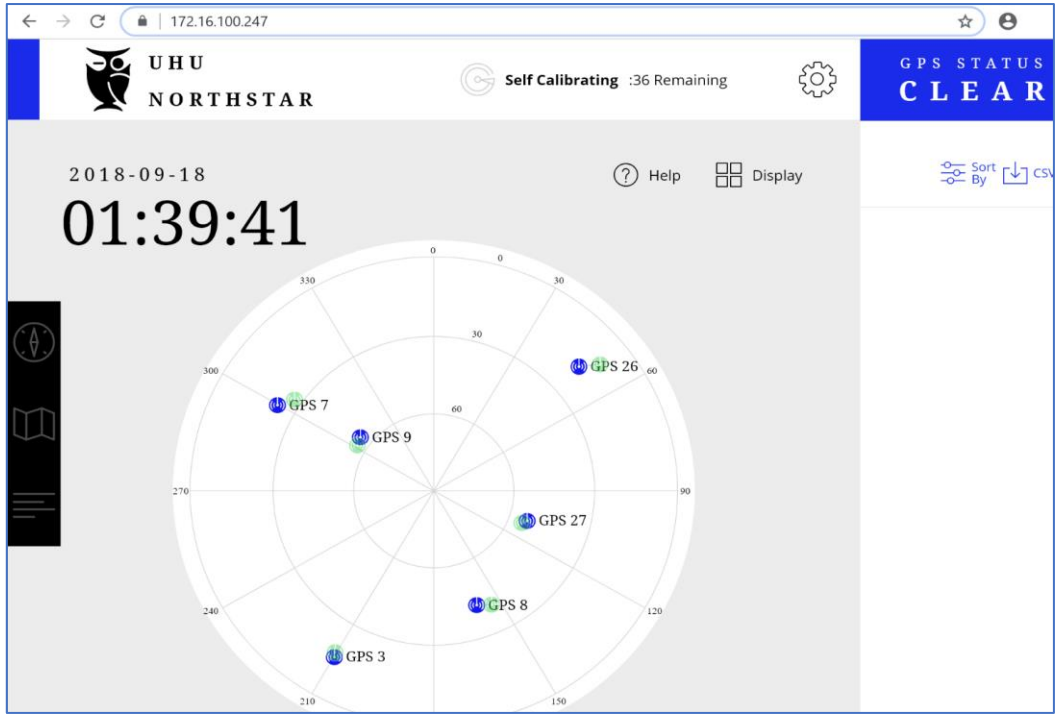
Northstar Product

The Northstar utilizes a rugged 4-element GPS antenna array:

Northstar Product

The Northstar has a built-in GUI that displays AOA's in real-time:

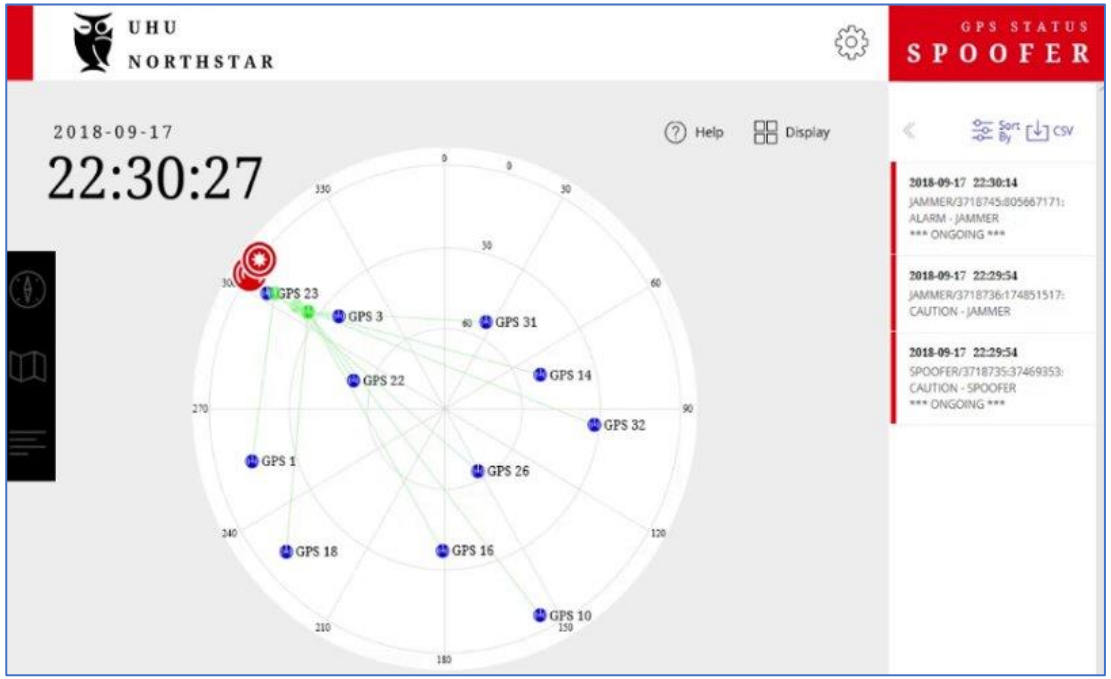
- **Green circles:** Satellite locations based on patented Angle of Arrival technique (measured locations).
- **Blue circles:** Satellite locations based on GPS almanac or ephemeris (known locations).



Northstar Product

GPS interference is prominently displayed on the GUI

- Measured satellite locations (green icons) now grouped on horizon. This is a clear indication of GPS spoofing.



Port of Long Beach – BETA Test

UHU TECHNOLOGIES

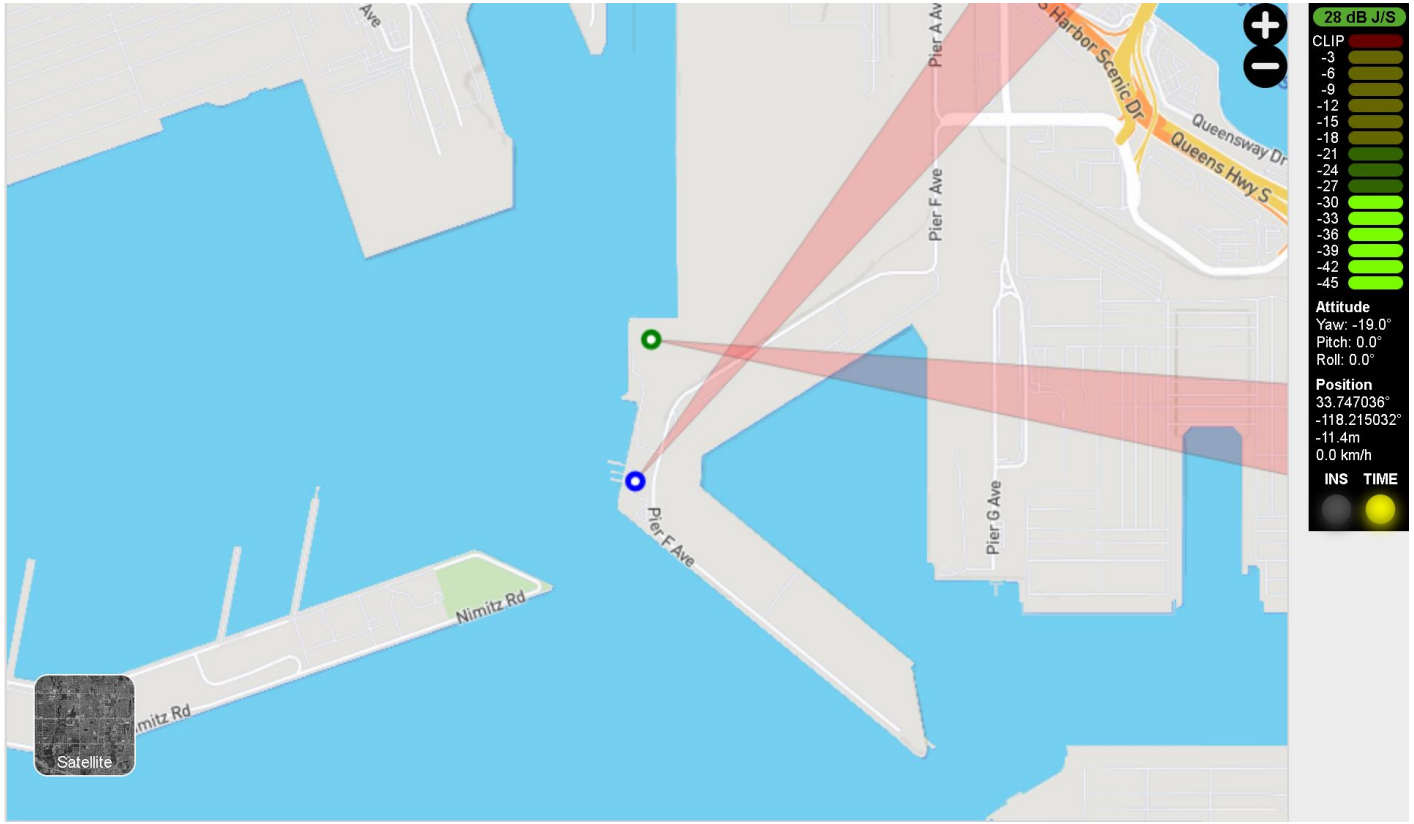
Port of Long Beach – BETA Test

UHU TECHNOLOGIES

Port of Long Beach – BETA Test

Systems are regularly identifying threats

- This event took place last Wednesday afternoon
- Jammer strength was fairly low; however, it still had the potential to interfere with nearby ships if passing through at the same time
- Only two Northstar systems installed (at this time)



Port of Long Beach – BETA Test

Multiple Systems Deployed

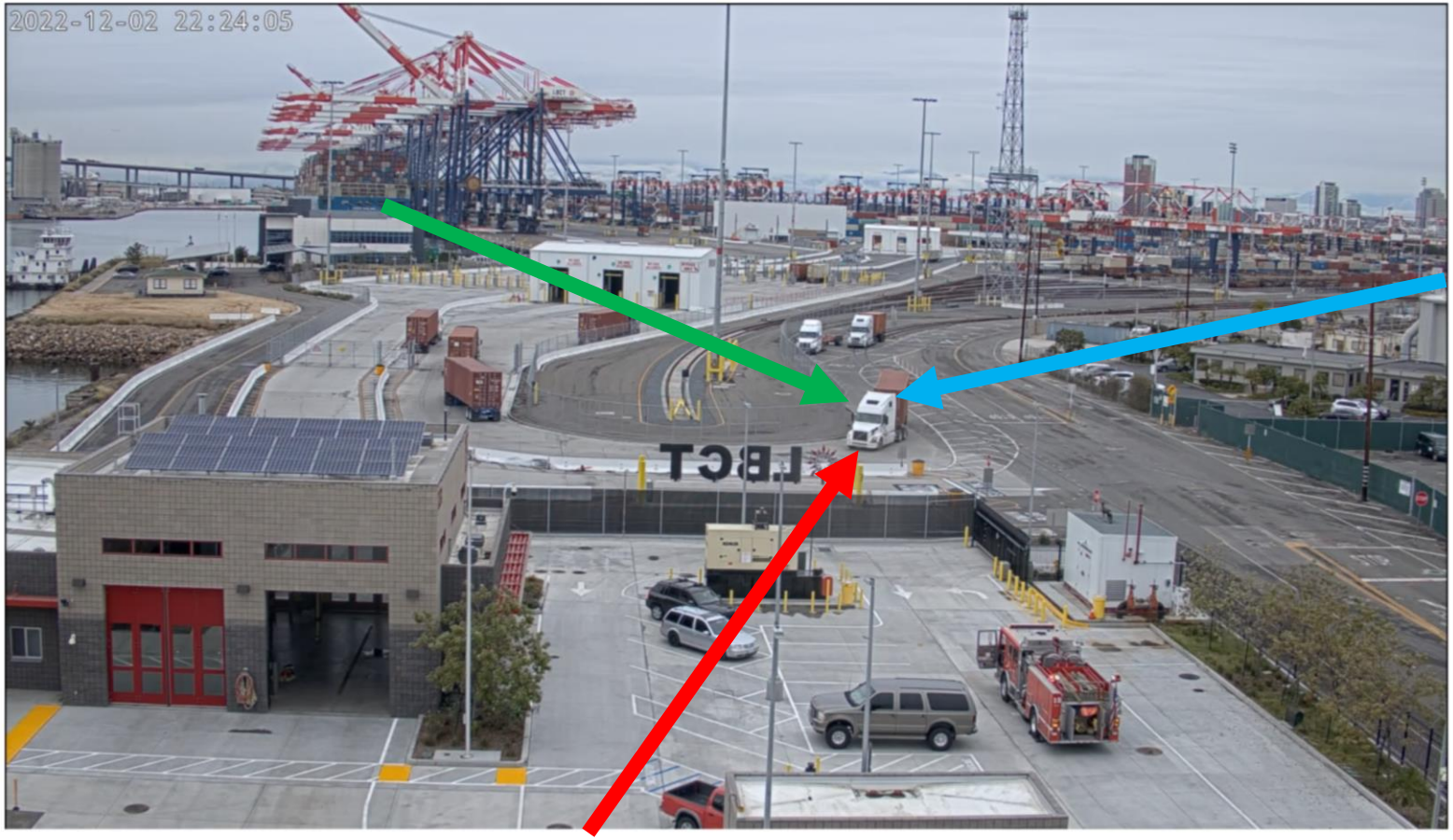
- Initial mission is to locate “personal privacy devices” used by some truck drivers
- Three systems deployed to Pier F (third system completed last Friday)

UHU TECHNOLOGIES

Port of Long Beach – BETA Test

Next Steps

- Surveillance camera installed for additional collection capabilities
- Third system now fully operational



Conclusion

WE WILL BE SHOWING VIDEOS AT OUR TABLE IN THE EXHIBIT AREA FOR PEOPLE WHO ARE INTERESTED

- **GPS spoofing is a growing threat to critical infrastructure**
- **Existing market solutions provide inadequate spoofing protection**
- **UHU's patented Angle of Arrival technique cannot be spoofed**
- **UHU's technique logs and reports threat direction for law enforcement analysis**


UHU TECHNOLOGIES
Thank you!
www.uhutechnologies.com