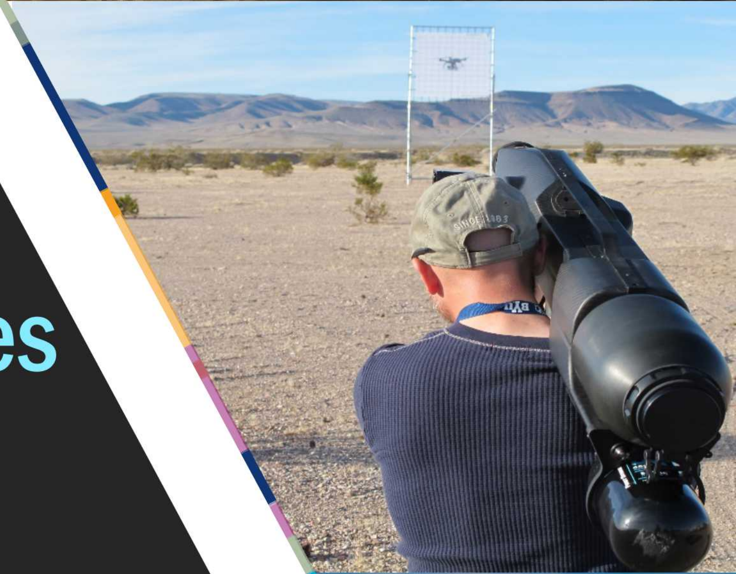
SAND2019-10022PE

Sandia National Laboratories

Exceptional service in the national interest

Physical Security Center of Excellence (PSCOE)

Emerging UAS and Counter-UAS Technologies



Presented by:
Scott Brooks
Manager, 6514 Technology Development

SAND2019-9016 PE
SAND2019-4372 PE
R&A 998953

U.S. DEPARTMENT OF ENERGY NNSA

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.

WE SUPPORT DOE IN ALL ASPECTS OF COUNTER-UAS

DOE/NNSA CUAS Program

Research and Development

Policy & Requirements

- Program Planning
- **Threat Characteristics**
- Classification Guidance
- Safety
- **Perf. Requirements**
- Risk Analysis and Management
- CONOPS

Testing & Evaluation

- Baseline MOPs
- Degradation MOPs
- Site/background Surveys
- **Test Plan and design**
- **Testing**
- **Results & Reporting**
- **Trends, Gaps, and Recommendations**

Design and Deployment

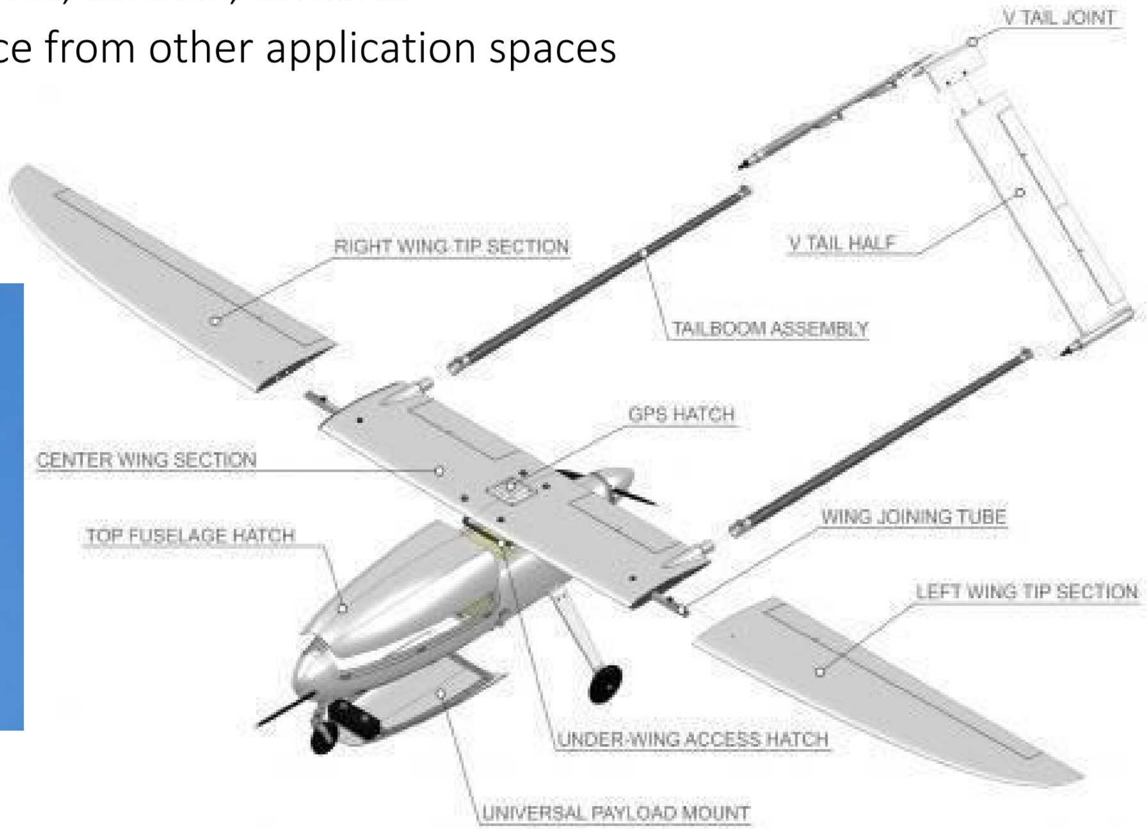
- **Acquisition**
- **Design & Installation**
- Evidence Packages and Approvals
- **Training**
- **Performance Testing**
- Life Cycle Management /Sustainment

UAS: What are they?

Flying Robots

Why so popular now?

- Proliferation of low cost, high performance electronics
- Open-source software / configurable
- Tipping points in batteries, sensors, cameras
- Technology convergence from other application spaces



What Makes It a System?

UAV - Vehicle

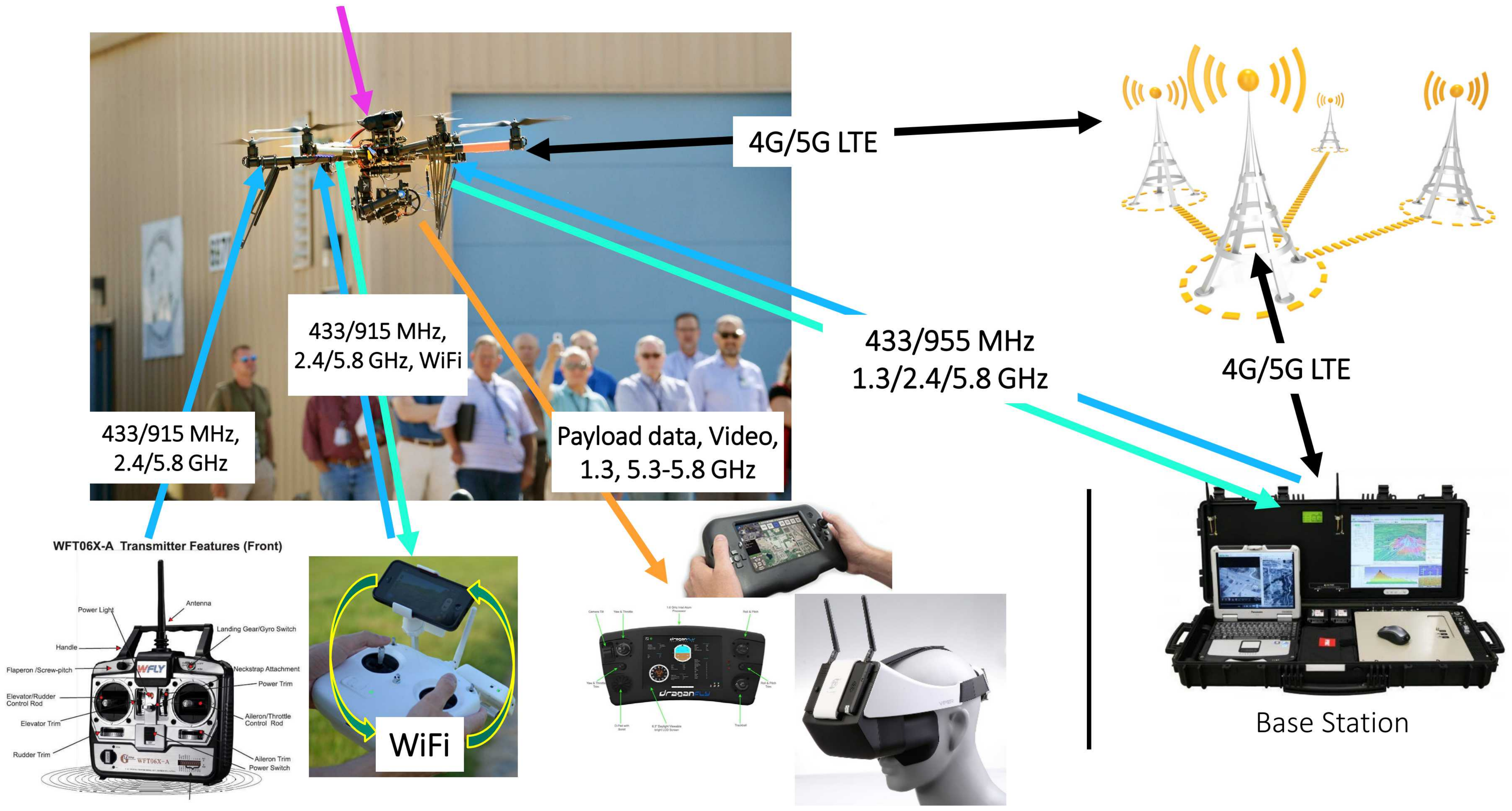
Payload

Unmanned Aircraft
SYSTEM

Hand Controllers

Base Station
(optional)

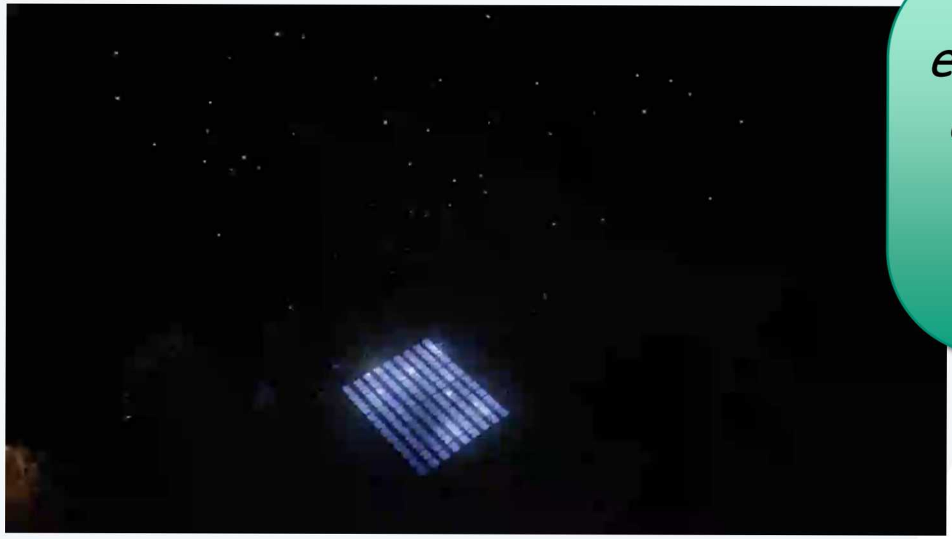
RF-based Control/Navigation Link Options



OPEN SOURCE ARCHITECTURE ENABLES NEW CAPABILITIES

Technologies are evolving faster than our ability to keep up with them! (Especially Autonomy)

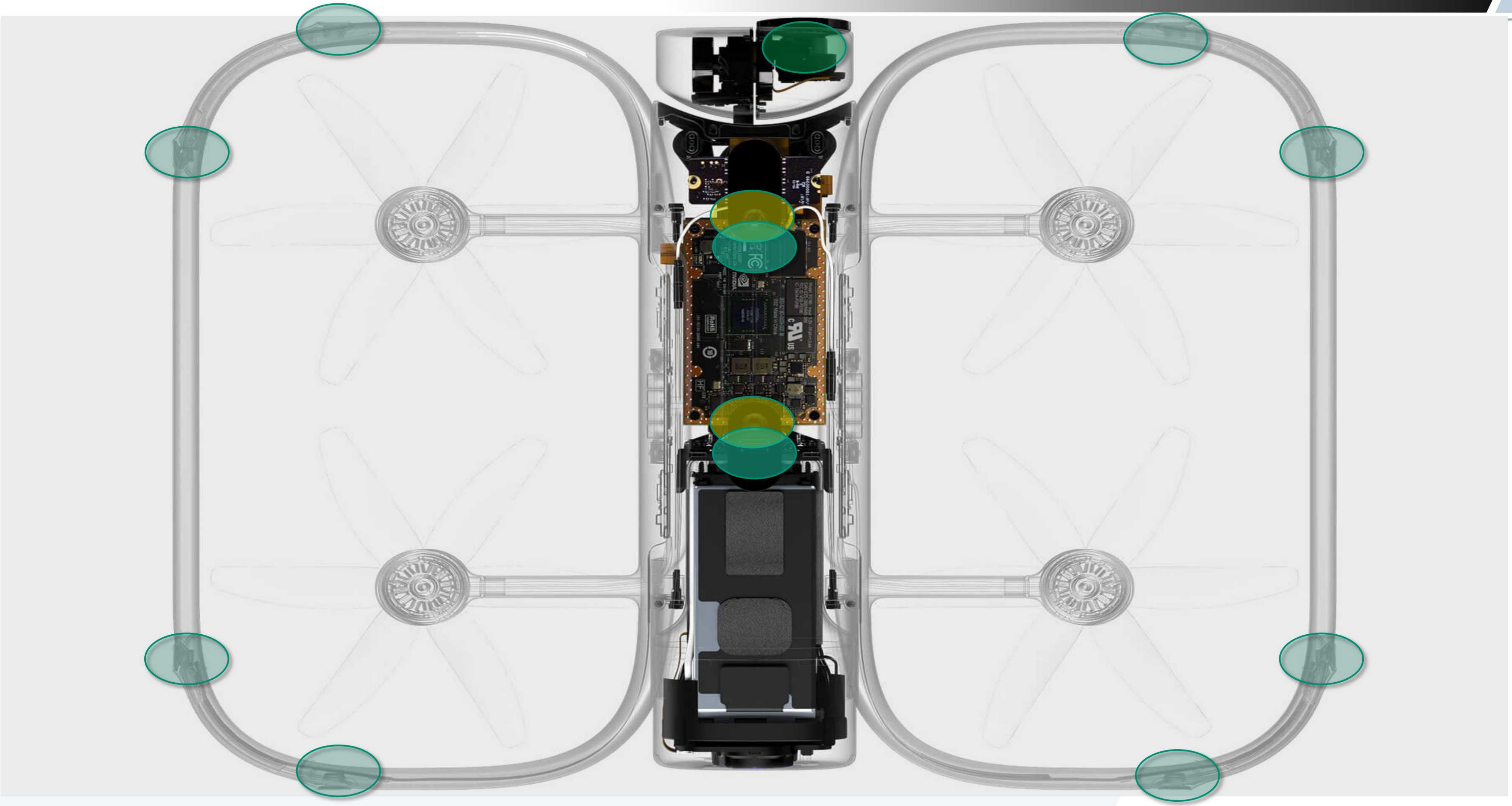
Octokaidecacopter – lifting a person



Intel Fields 500 Small UAS for a light show

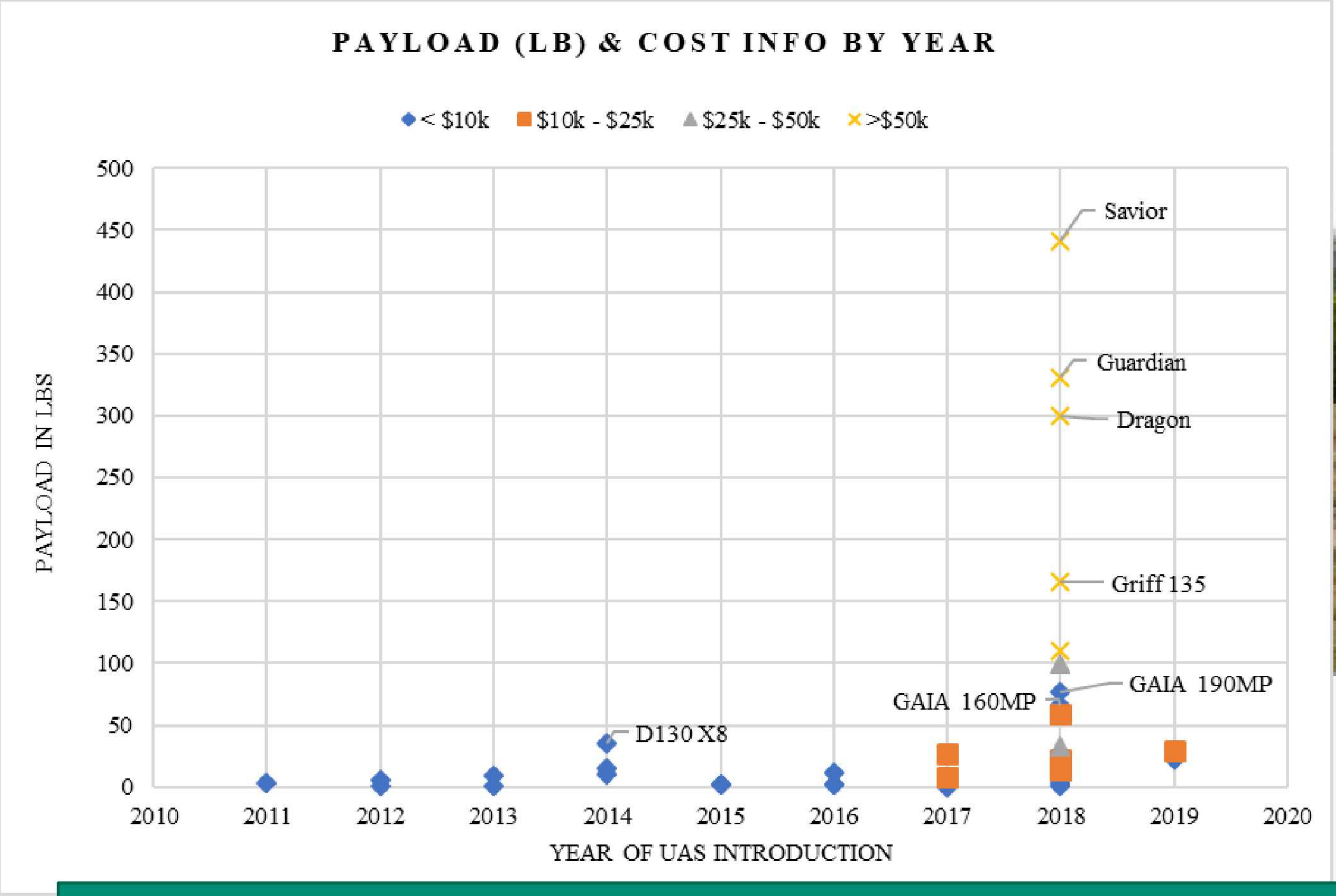
UAS enabled with deep learning / object recognition

Zapata Flyboard (manned with unmanned tech!)



Skydio R1 - Autonomy via Computer Vision

RAPID PAYLOAD GROWTH AND PRICE DROP

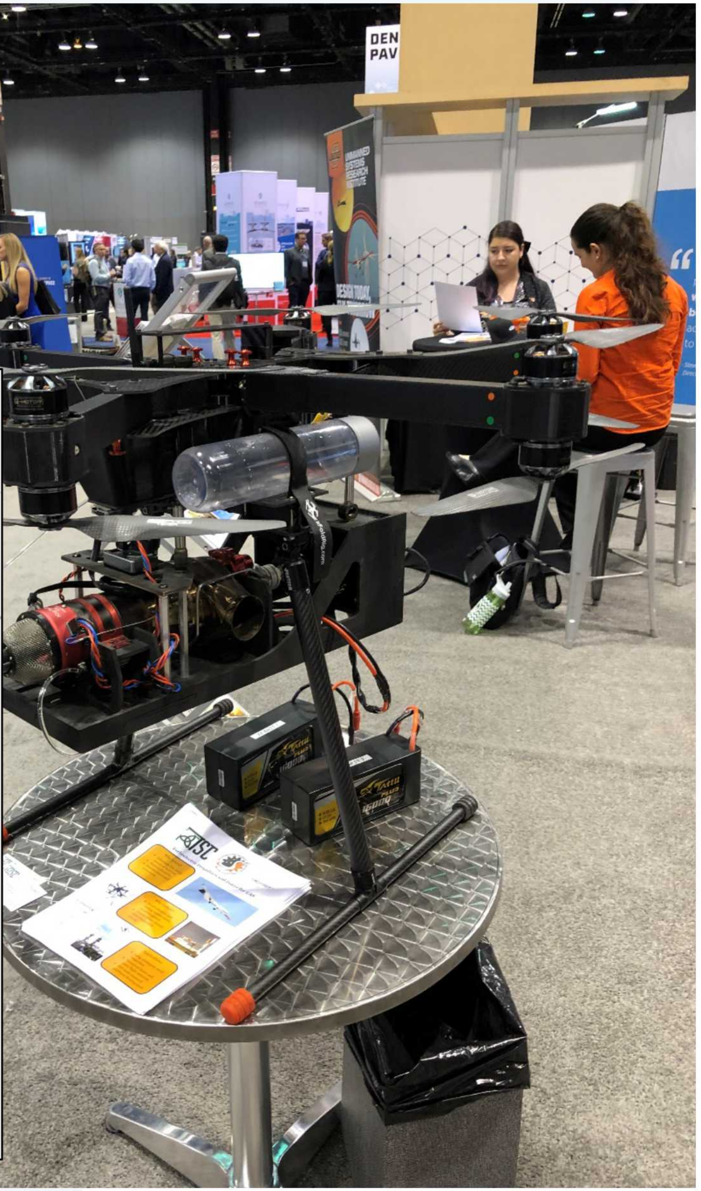


Source: Youtube.com

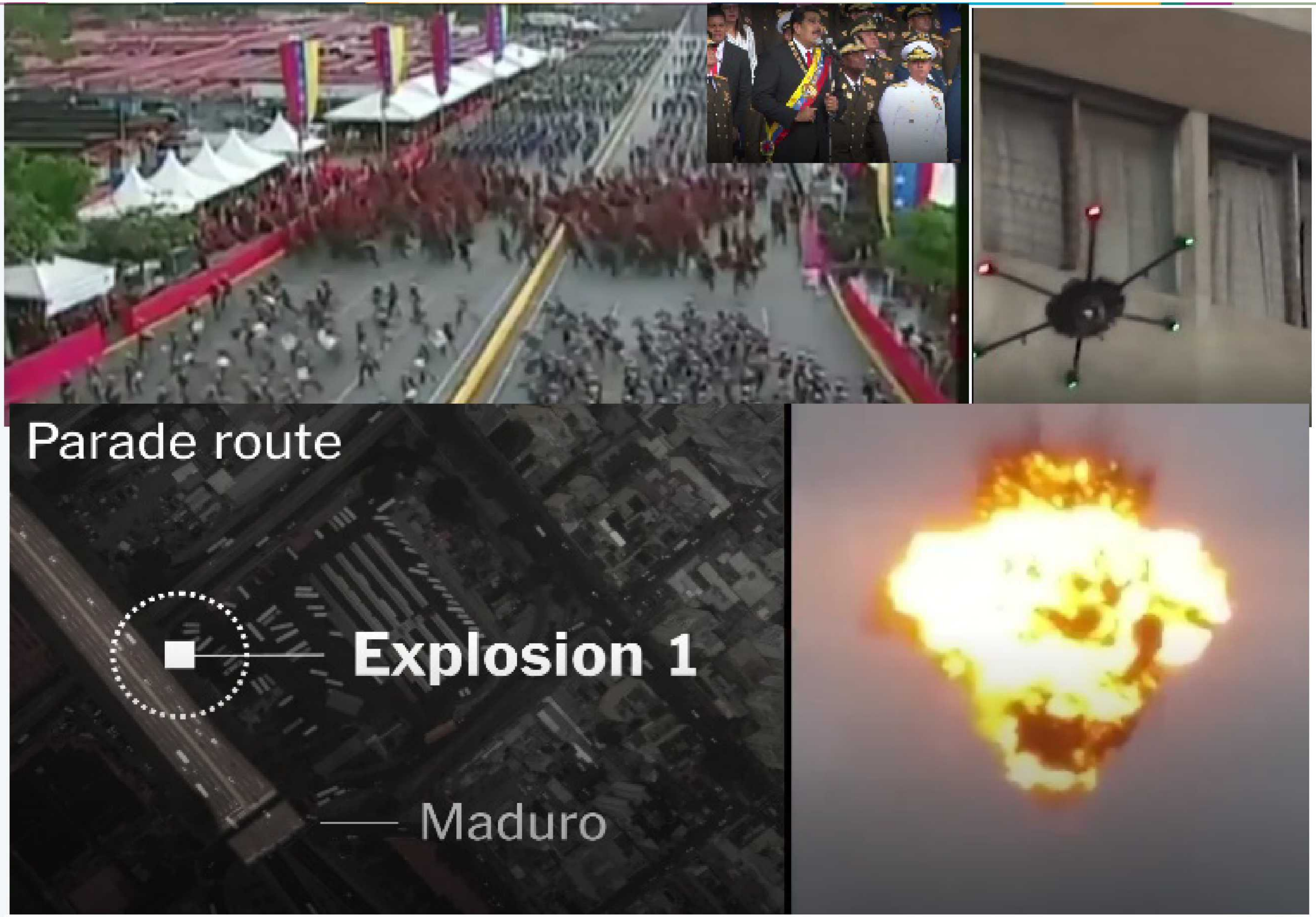
•Foxtech Gaia MP line of UASs ($3,600 to $9,700) has payload capabilities from 35 to 60lb
•Hybrid gas/electric UAS are available in the $25k-$45k range with up to 30lb payloads
•Video shows a $9k Hexacopter flying with a > 50lb payload

HYBRID POWER, HYBRID FLIGHT

Payload is loaded onto platform; hoists raise it into the fuselage



REAL WORLD EVENT



Images of Maduro attack taken from media

Attack on President Maduro of Venezuela – August 4th 2018

TERRORISTS LIKELY TO ATTACK U.S. WITH SMALL UASS – FBI DIRECTOR CHRIS WRAY

On Oct. 10, 2018, FBI Director Christopher A. Wray, testified to the Senate Committee on Homeland Security and Governmental Affairs (see Figure 5) that the FBI is convinced that terror groups will use small UASs to carry out attacks on American soil. Wray told a Senate committee hearing the threat of small UASs and other unmanned aircrafts is "steadily escalating" due to their widespread availability and ease of use[1].

"The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering," Wray said in written testimony to the Senate Homeland Security and Governmental Affairs Committee, using an acronym for unmanned aircraft systems.

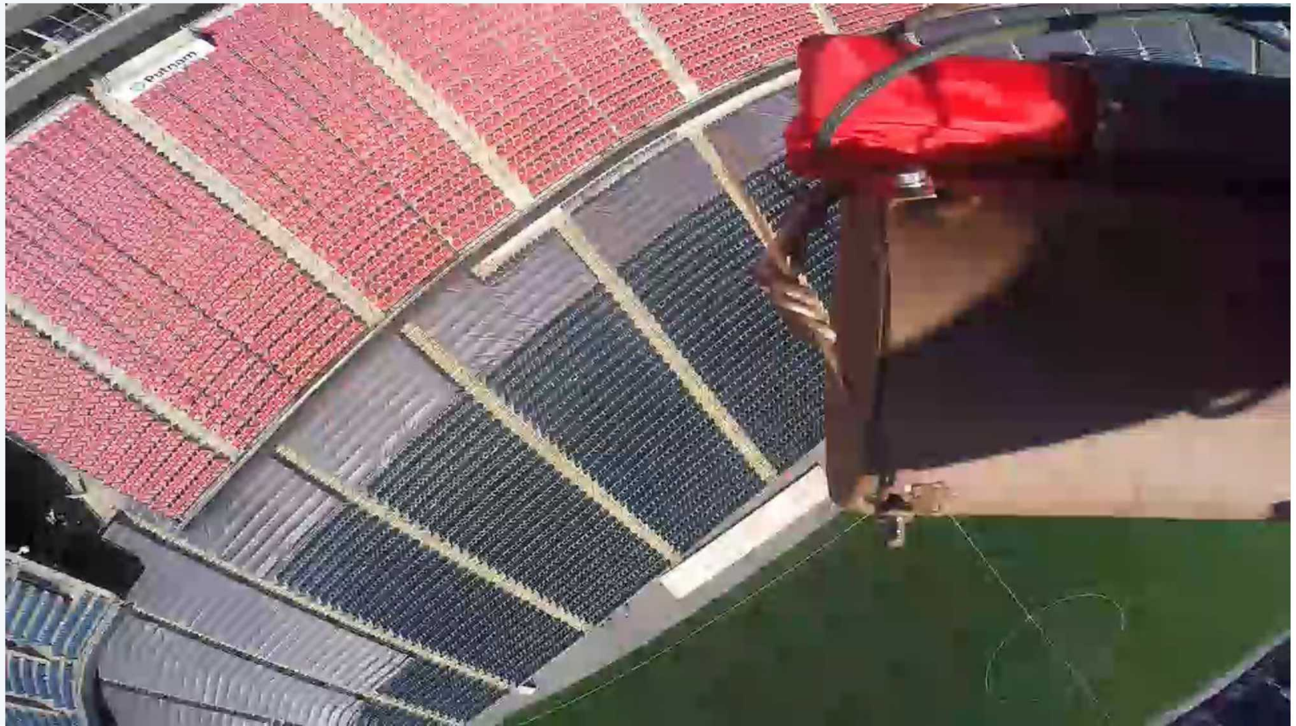
[1] https://www.nbcnews.com/politics/national-security/new-law-would-give-federal-government-right-shoot-down-private-n912381

14

RED TEAM CAPABILITY VIDEOS

Precision Drop

Rapid Launch & Drop



TRENDS IN CUAS POLICY, LEGAL, AND TECHNICAL CHALLENGES

Policy

Limited **mitigation authorities**, few acceptable mitigations

CONOPS, rules of engagement are in early stages of development

Risk acceptance / tradeoffs

Legal

Ambiguity of intent - **what is considered 'trespassing' with small UAS**?

Balancing public/privacy concerns vs. national security

Legal consequences of interfering with an unmanned system

Technical

'**Maker community**' has moved development into high school student homes

- Open-source flight control software
- Ubiquitous, advanced, cost-effective, miniaturized, and integrated control hardware/firmware

Detection and timely assessment at long ranges ($5 000 - $5 000 000,00 USD)

Alternative navigation methods, **high-speeds**

Domestic law/policy/regulations may limit mitigation options

Privacy Concerns

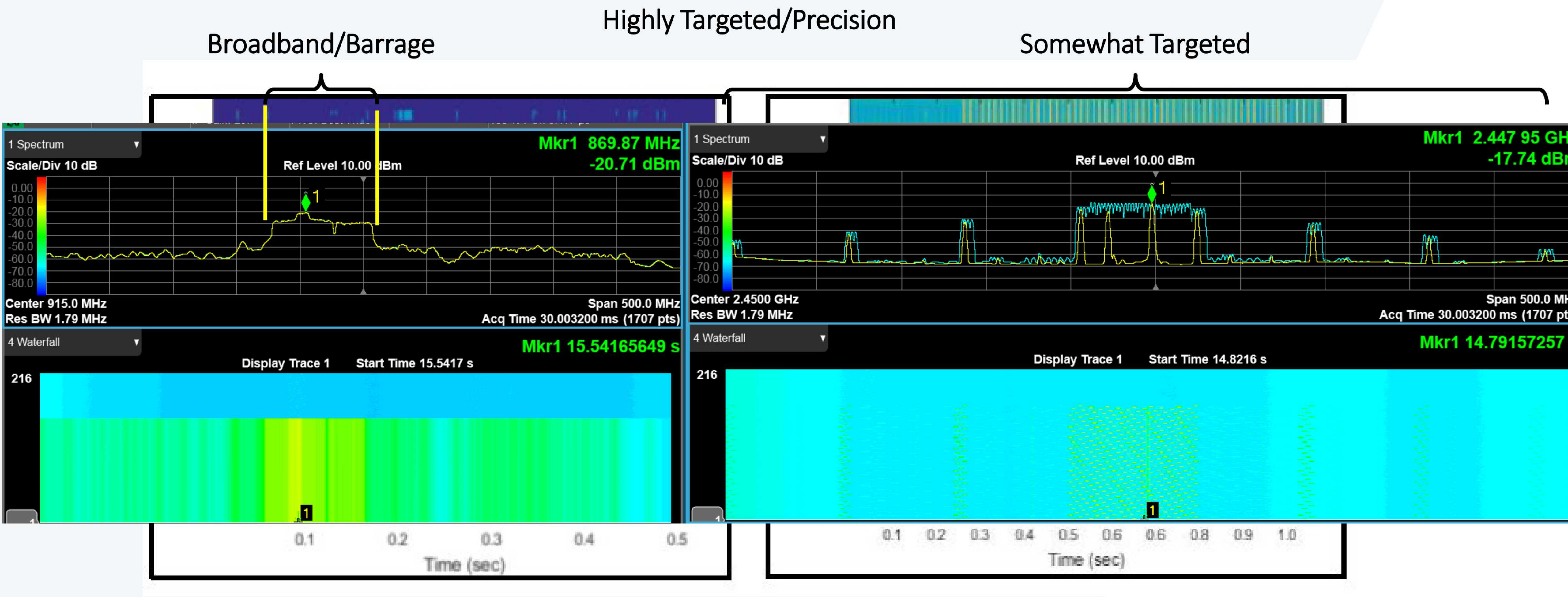
C-UAS Sensing Technologies and Characteristics

	Acoustic / Seismic	Passive RF	Active RF (RADAR)	Optical (imaging)
Sensing Mode	Microphone arrays sense UAS sound waves	Reception and analysis of RF transmissions (video, control, telemetry, Wi-Fi)	Active detection of reflected radio signals	Reflections or emissions of visible to infrared (IR) light wavelengths
Sensor Field of View	90-360°	360°	90-360° (H) 3-90° (V)	variable, very small to 360° (WAMI), imager dependent
Weather	Susceptible (wind)	Small attenuation	Moisture/rain can cause high nuisance alarms	Susceptible (depending on wavelength; IR is much less susceptible)
Range (small UAS)	Low	Variable, low to very high	Variable, typically Medium to High	Low to High (imager dependent)
Geolocation Accuracy	Low, line of bearing (LOB) only	Medium, LOB to 2D geolocation	High, 3D location	LOB (no distance information)
Tracking Accuracy	Medium	High	Very High	High
Night Operation	Same as day	Same as day	Same as day	No degradation for IR wavelength systems
Autonomous UAS Sensing	Yes	No	Yes	Yes
Weaknesses	Limited range	Potential latency; NAR, not all signals easily recognizable	Birds and weather may cause high NAR	Generally needs coupling with another tech; expense
Strengths	Does not require line of sight	Long-range, can ID specific protocols, intercept video	Multi-target tracking with no latency	Useful, easily interpretable data for human decision-making

C-UAS Mitigation Technology Characteristics

	Electronic RC Countermeasures	GNSS Countermeasures	Net Capture (Ground)	Net-Capture (Aerial)	Ballistic Projectiles	Directed Energy
Mitigation Mode	Interference, kill commands, takeover (RC /navigation)	Interference, spoof (prevent auto waypoint navigation)	Net intercepts and entangles the UAS	Entanglements fired from or carried by an intercepting UAS	Munitions or projectiles fired from ground	Damage to airframe, electronics via deposition of energy
Weather	No effect	No effect	Susceptible	Susceptible; UAS-dependent	No effect	Rain/clouds can attenuate/reflect
Range	Variable (low-very high), depends on many factors	Very high	Variable, but typically very low	Low-medium, UAS dependent	Low	Depends on many factors, generally low-medium
Multi-shot/targets	Yes	Yes	Limited	Limited	Yes	Yes
Night Operation	Same as day	Same as day	Reduced range	Reduced range	Depends on targeting method	Same as day
Mitigates Dark UAS?	No	No (for non-GNSS navigation)	If it can be targeted/tracked	If it can be targeted/tracked	If it can be targeted/tracked	If in range and can be targeted/ tracked
Potential Weakness	Must know band; lower bands harder to mitigate; dark UAS	Collateral damage; does not immediately stop a FW; dark UAS	Range, speed of target; limited rounds; human operation	High-speeds; autonomous operation still developing	Policy, collateral damage, safety/liability	Policy, collateral damage, safety/liability, evading UAS are a challenge

EMERGING TRENDS IN CUAS – RF MITIGATION



19

RF MITIGATIONS VS. UAS NAVIGATION OPTIONS

Focus of nearly all COTS solutions

COTS solutions partially address; collateral damage is problematic

Manual Control (in-band)

[RC, 802.11, ISM, etc.]

Manual Control (out-of-band)

(e.g., 4G LTE)

?

GNSS Way Point (including dynamic mission upload)

Optical 'Active Tracking' (e.g., DJI, Skydio) + sense & avoid/hunt [AirSpace, Fortem]

GNSS Way Point + Optical Navigation / Sense & Avoid

GNSS + IMS + RTK Nodes

?

Autonomous Optical Flow, and Others being developed…

?

ADDRESSING CUAS GAPS: DETECTION AND ASSESSMENT/CLASSIFICATION

Background

- Typical industry methods rely on RF, Radar, or Acoustic signals
- Assessment against common nuisance alarms is challenging
- Need UAS-based signatures for autonomous or manned assessment

Project Purpose

- Leverage spatio-temporal time frequency characteristics of UAS from video data [Temporal Frequency Analysis (TFA)] to improve our ability to sense and classify UAS threats
- Humans – need 8 pixels on target to classify as threat
- TFA – needs only 3 pixels on target to classify as threat

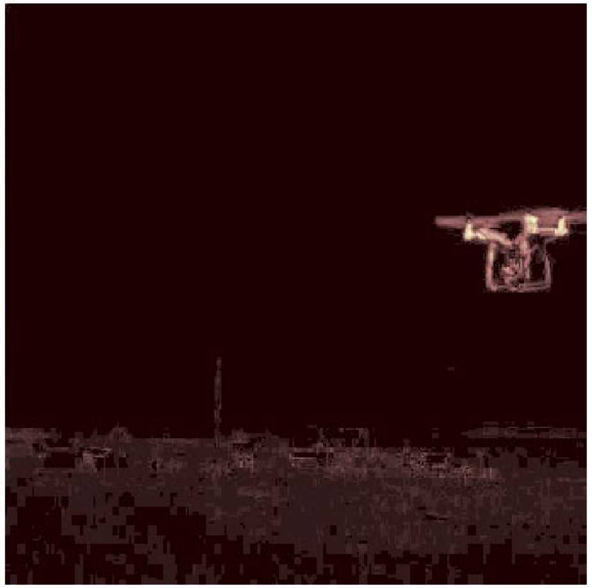
Preliminary Results

Bird-NoTFA

Bird-TFA

P4Still-NoTFA

P4Still-TFA

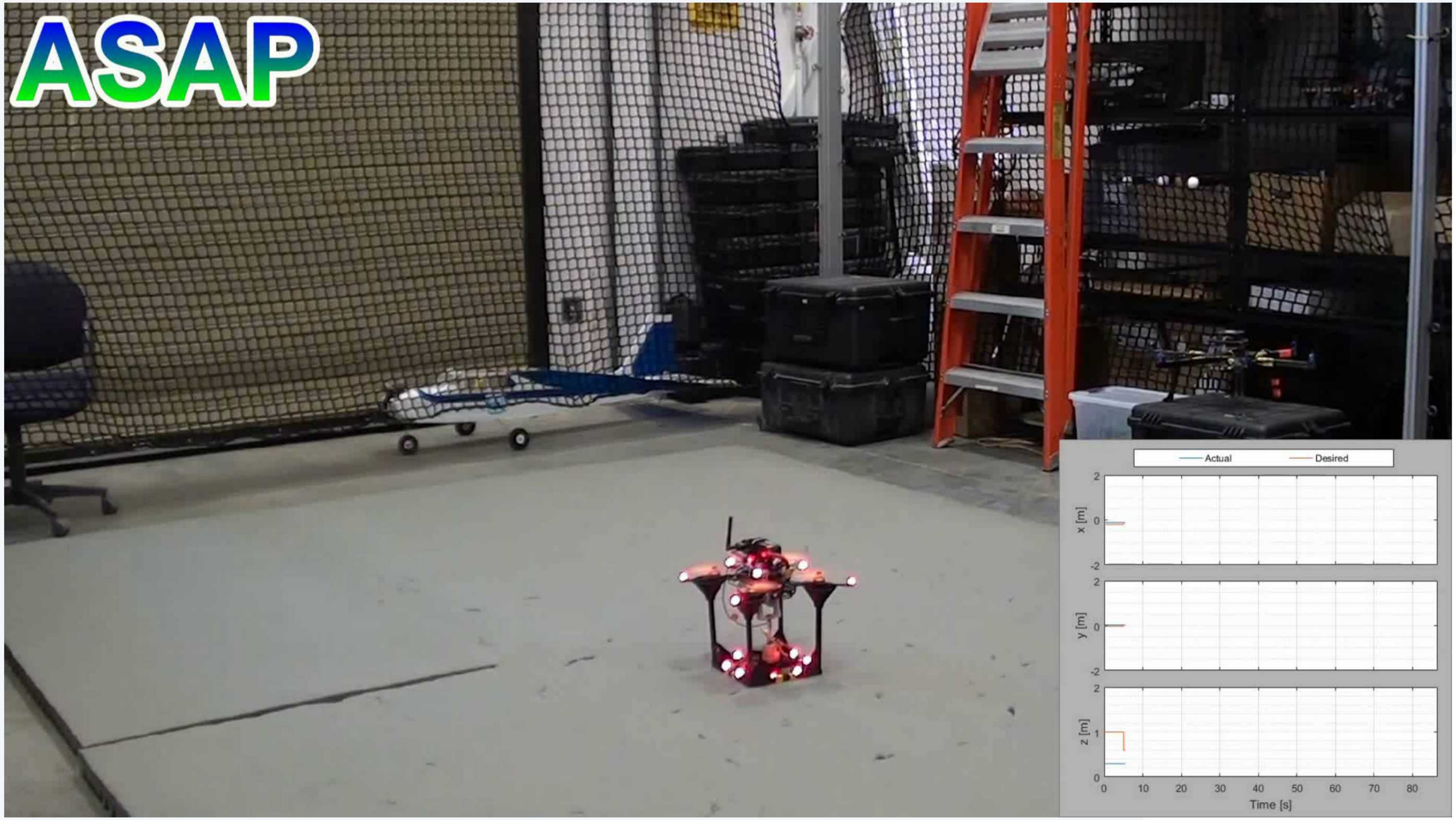


21

ADVANCES IN UAS VS. UAS

Smart-Net: Control theory / algorithms supporting coordinated UAS-on-UAS actions

- Ability to extend ground based systems and bring localized effects to targets



22

OTHER EMERGING TRENDS / FUTURE CUAS CAPABILITIES

- Localized effects
- Acoustic mitigations
- Kinetic options with reduced collateral damage (self-terminating)
- Distributed directed energy
- Bird-on-bird terminal navigation technologies
- Improved RADAR techniques
- Satellite communications for BVLOS

23

LESSONS LEARNED, GAPS & CONCLUSIONS

24

LESSONS LEARNED, GAPS & CONCLUSIONS

1. Only partial solutions exist today. Multiple/complementary sensing, assessment, and mitigation will enable greater probabilities of success
2. Define your program and requirements before looking for solutions / capabilities
3. Some airspace situational awareness is better than none. Later improvements can close gaps
4. Neutralization methods may interfere with or disrupt current operations
5. Test design is critical. Ensure a standardized, repeatable test approach, mapped to requirements, in a neutral environment to enable direct comparison across domains
6. Never test more than 2-3 systems concurrently
7. Most vendors have not tested: at night, above 400 ft AGL, under ‘no-notice’ conditions, or false-positive rates. False positive rates are high for most CUAS by DOE/NNSA standards

25

LESSONS LEARNED, GAPS & CONCLUSIONS

1. Claimed capabilities may not represent the actual capabilities
2. Have the vendor train you to set up & operate; have them leave during testing
3. You can't afford to test every scenario; instead pursue standardized baseline performance characterization and degradation testing to capture limitations/gaps
4. Use virtual testing, assessments, and training capabilities for sensitivity analysis & design
5. RF mitigation methods are sunsetting
6. Successful deployment, operation, maintenance and improvement is a long term investment
    1. Periodic re-evaluation of needs / requirements, threats, gaps
    2. Product spirals require re-evaluation
    3. A national CUAS test bed that can support this is needed; we're currently working on this

QUESTIONS?

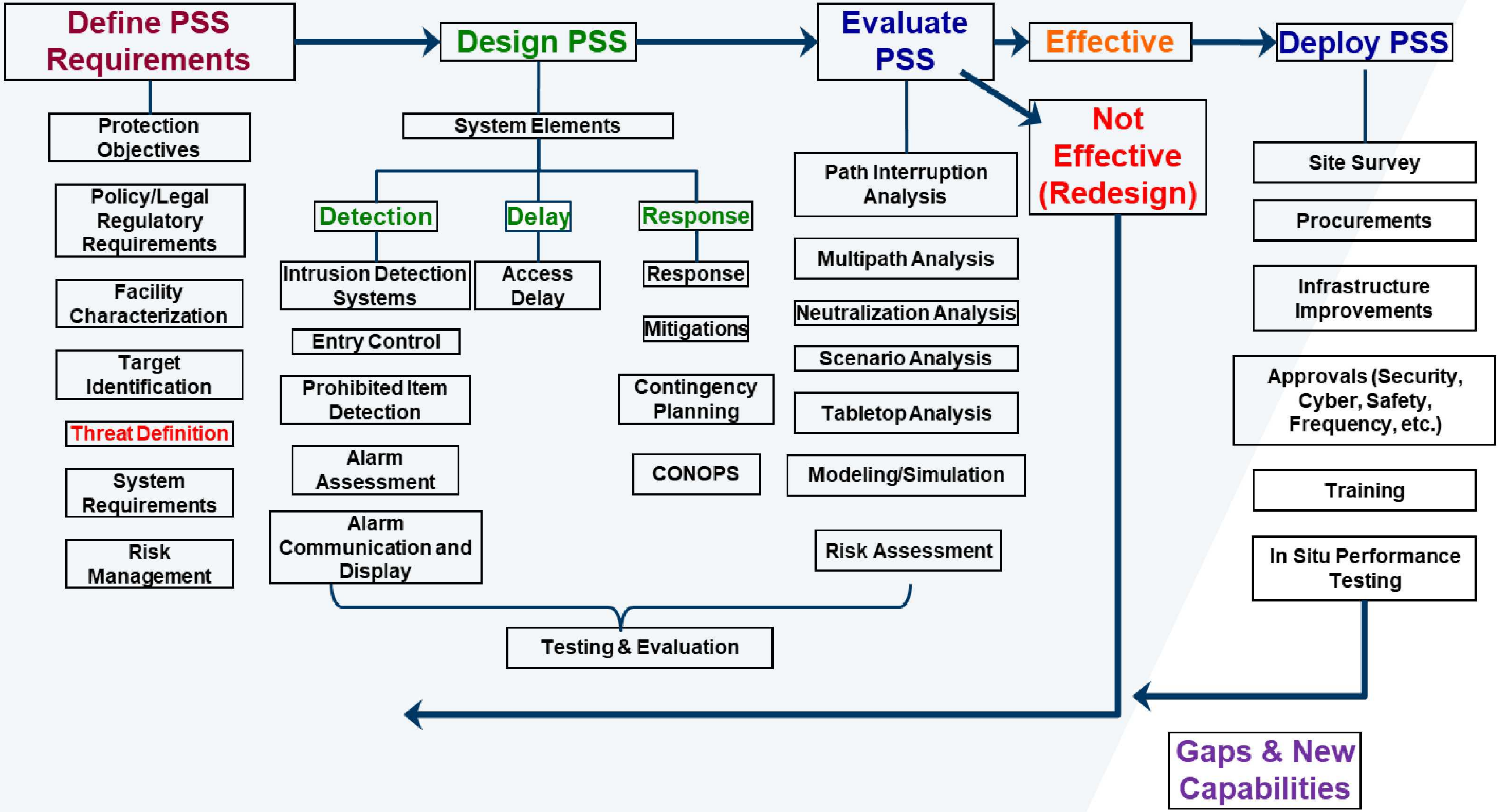
Sandia National Laboratories
Jon Salton, Manager
Weapon and Force Protection, Physical Security Center of Excellence
Scott.brooks@sandia.gov
505-844-7089 (o)
505-250-7876 (m)

Sandia National Laboratories
Scott Brooks, Manager
Weapon and Force Protection, Physical Security Center of Excellence
Scott.brooks@sandia.gov
505-844-7089 (o)
505-250-7876 (m)

SNL CUAS
Excellence in RDT&E

27

SYSTEMS ENGINEERING FRAMEWORK FOR THE DESIGN AND EVALUATION OF PHYSICAL SECURITY SYSTEMS (AND COUNTER-UAS)



28

OUR CUAS TEST & EVALUATION APPROACH

Objective

Find effective solutions to *Common* National CUAS needs by leveraging *Shared Resources* and *Shared Results*

Why

- Inform executive decisions
- Inform industry of gaps and needs
- Prioritize future tech investments
- Understand ROI (performance based analysis) of enhancements & investments
- Leverage economies of scale across the government

How

Structured test methodology ensuring

- Repeatable, quantitative, and comparable results across domains
- Scalable (cost, schedule, risk tolerance, industry vs agency, etc.)
- Adaptable to a wide range of application spaces.
- Identify differences in claimed vs actual vs desired performance
- When possible: leverage needs & collaborations across stakeholders

29

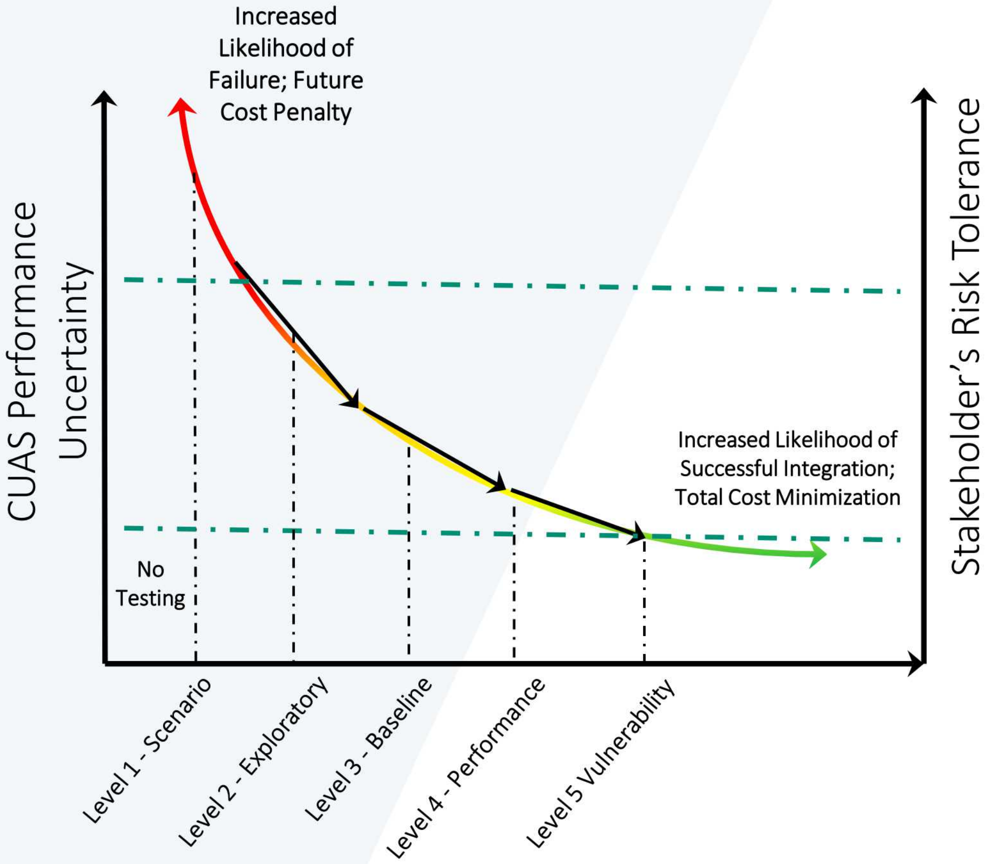
GRADED/SCALABLE T&E APPROACH

Provides credible, scalable, consistent, and comparable results across disparate technologies. Reduces overall deployment risk.

R&D (Lower TRL)

- Level 1 – Scenario Based
- Level 2 – Exploratory
- Level 3 – Baseline Characterization
- Level 4 – Performance (statistical confidence levels)
- Level 5 – Degradation / Vulnerability
- Post-Install: Certification and Periodic Performance Testing

T&E (Higher TRL)

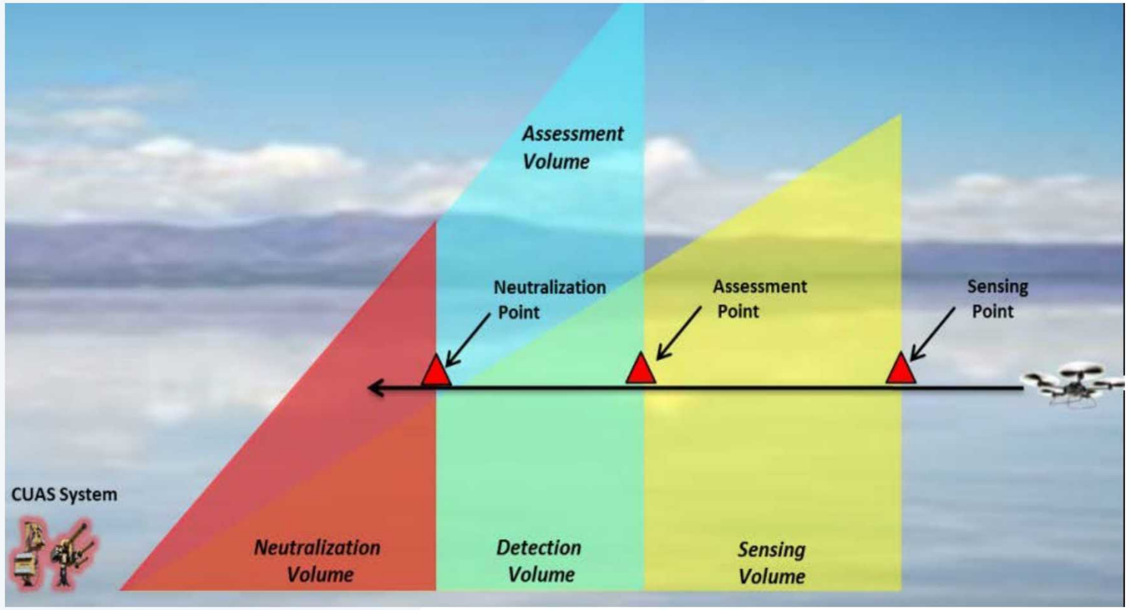


30

HOW: LEVERAGE PROVEN T&E PROCESS FOR SECURITY SYSTEMS to EVALUATE KEY PERFORMANCE METRICS

- Define test variables and metrics
- Characterize <u>system</u> performance from the first point of sensing through neutralization (sense, assess, track, classify, neutralization)
  - Advance notice and <u>no-notice</u> tests
  - Distance, time, and probability (or rate) for each metric
- Use defined, standardized <u>flight paths</u>
  - Throughout the entire performance envelope
  - Specific altitudes, distances, and repeats
  - Neutral test environment
- Standardized UAS <u>threat profiles</u>
  - COTS Group 1 & 2 fixed wing, multi-rotor
  - Standard approach path and altitudes
  - Identify associated signatures (RF, Radar Cross Sections, Imaging, etc.)

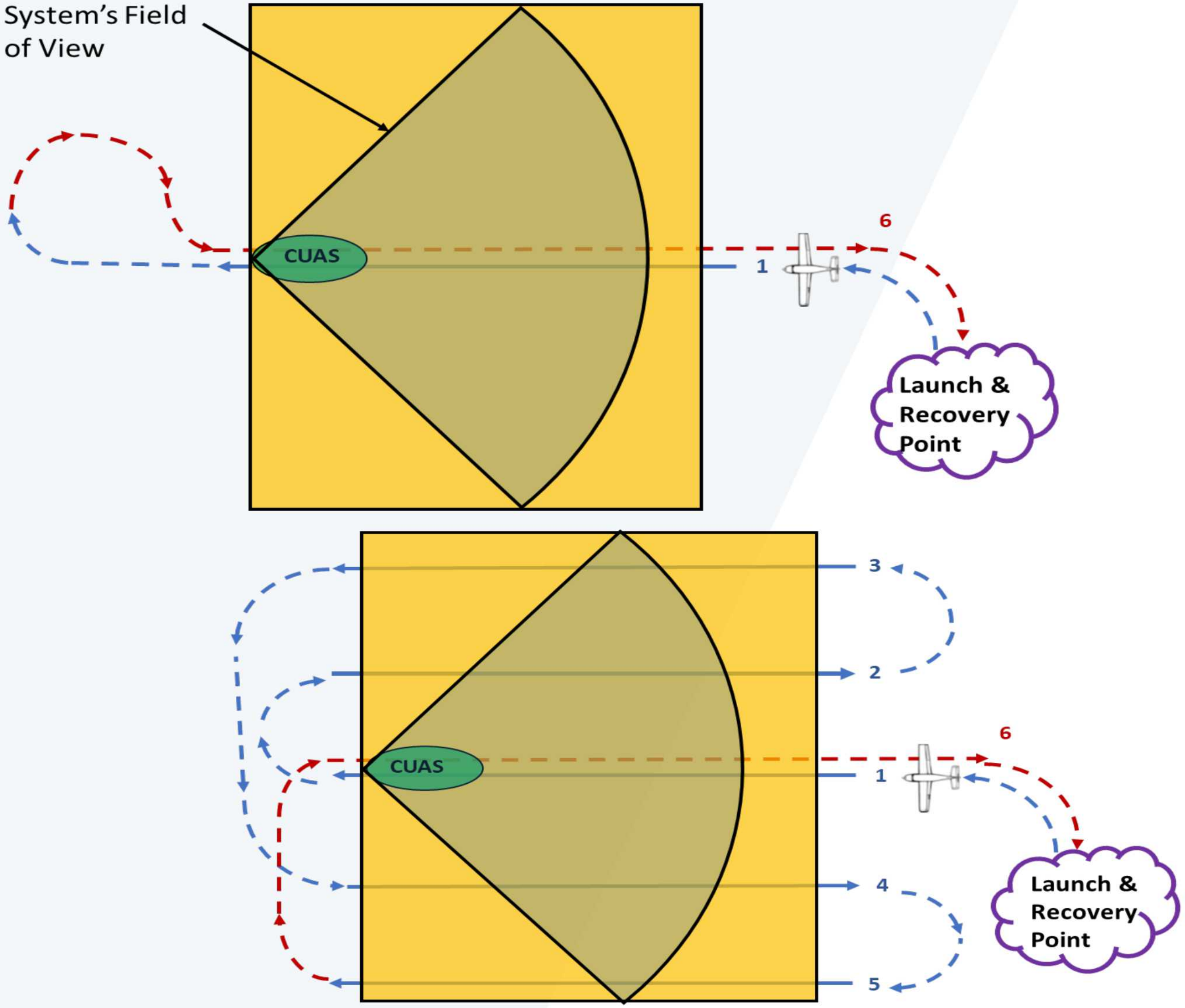
- <u>Degradation</u> testing
  - Characterize limits of performance, gaps
  - Characterize false positive rate
  - Multiple and mixed UAS, signatures
  - Inclement weather, degraded operations



31

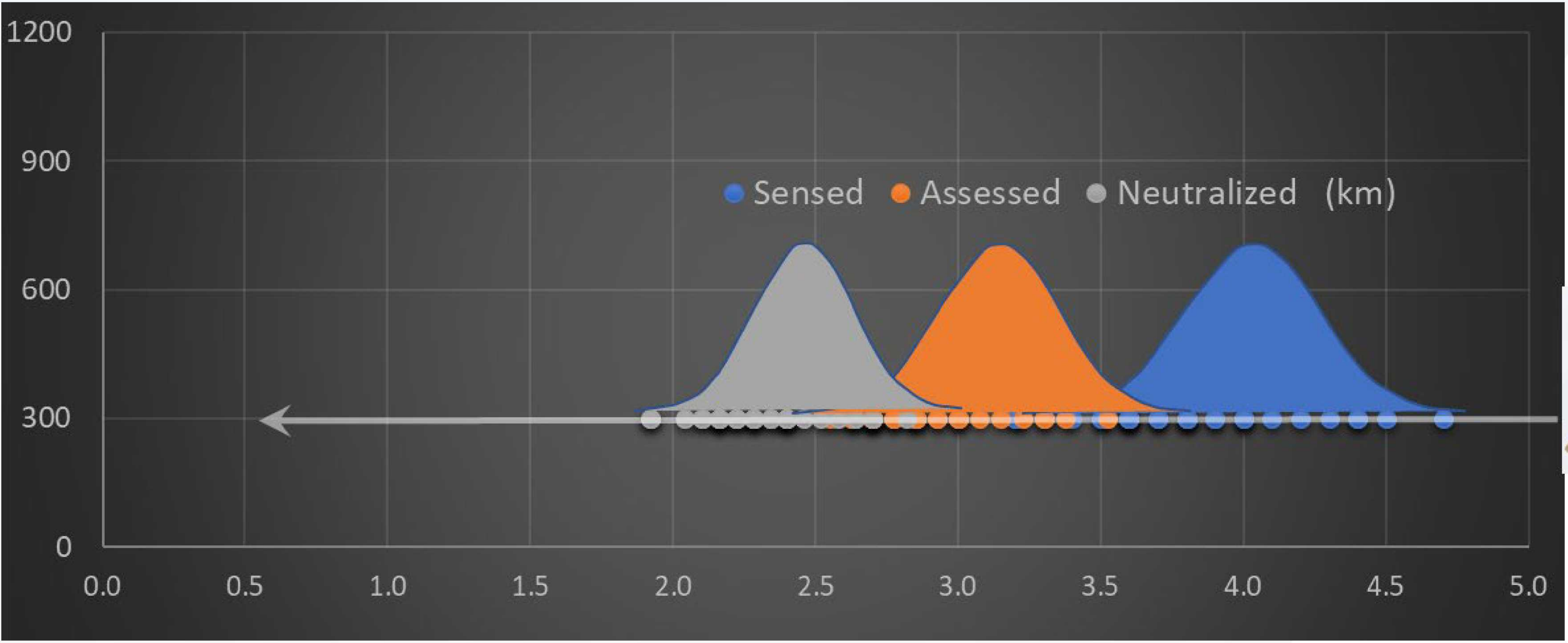
STANDARD FLIGHT PROFILES

- Calibration
- Circular
- Pop-up
- Approach



32

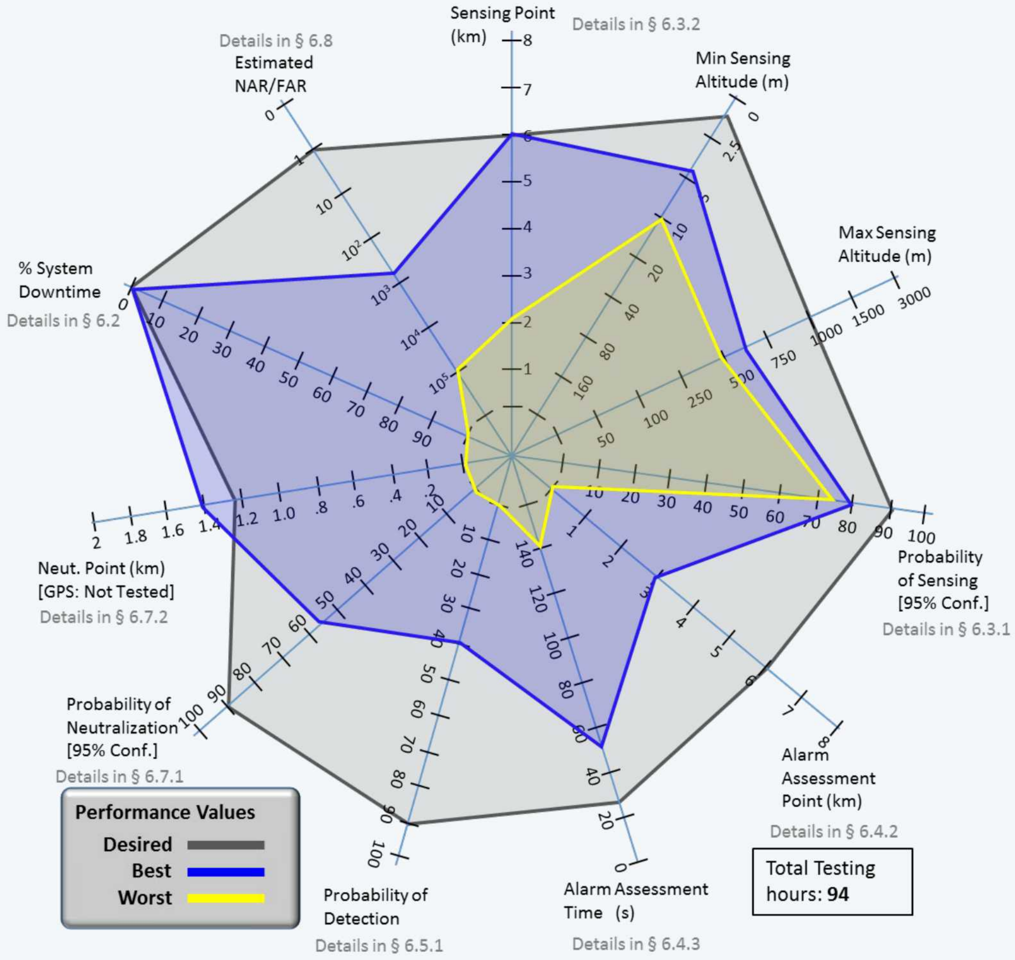
CUAS PERFORMANCE METRICS AND CHARACTERIZATION



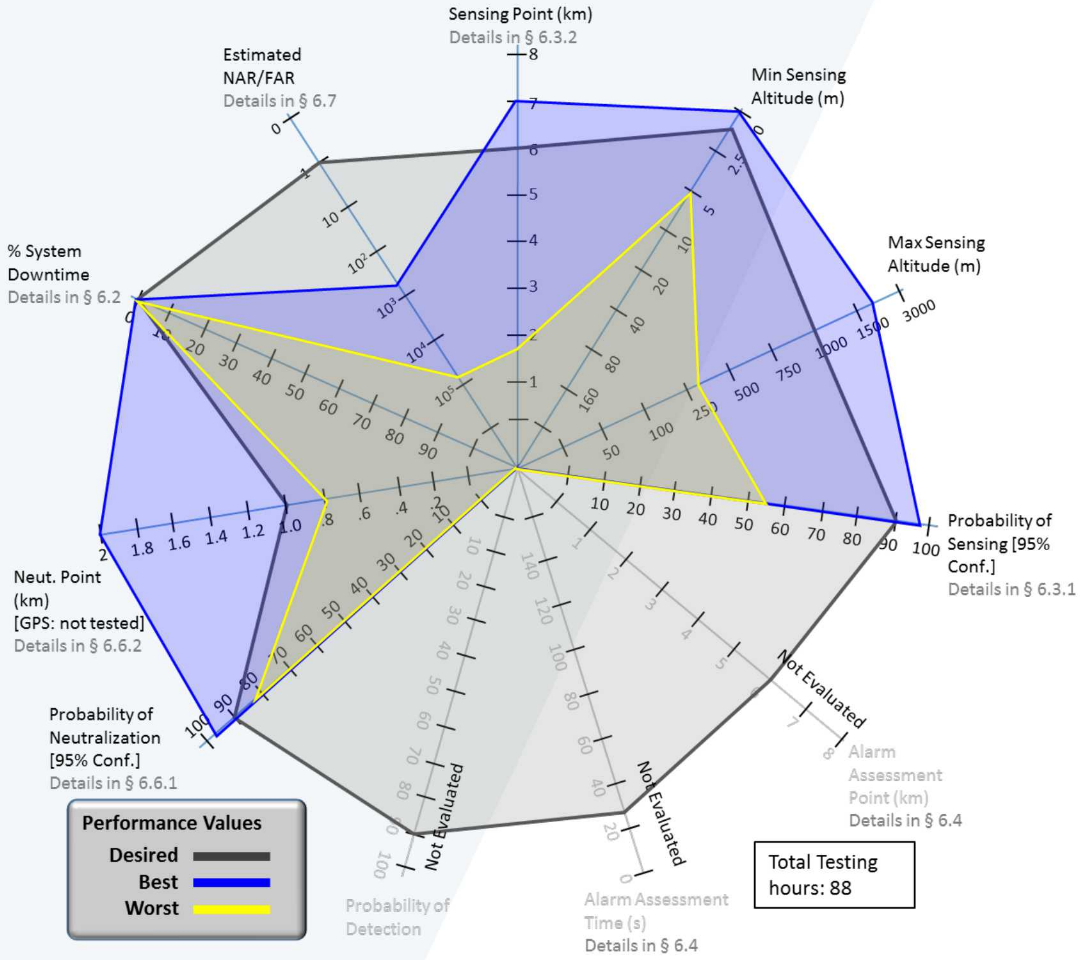
"The Probability of Assessed Detection (P_D) for the FinWing Sabre UAS operating at 300m altitude, 23 m/s, and [additional characteristics] was .90 at the 95% confidence level, with assessed detection occurring on average at 3.2 km."

RESULTS – COMPARISON ACROSS TECHNOLOGIES

Radar/Camera Based Detection/Assessment Systems with RF Jamming (Example = CUAS 1)

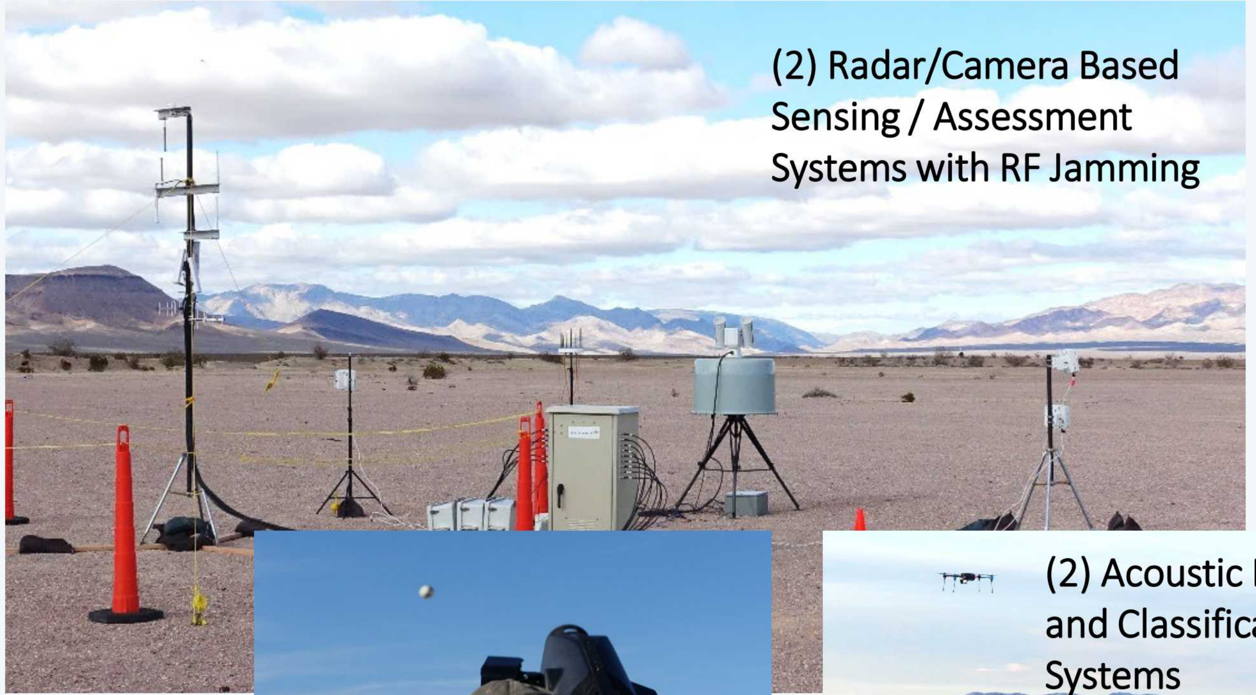


RF Sensing/Detection Systems with RF Jamming (Example = CUAS 2)

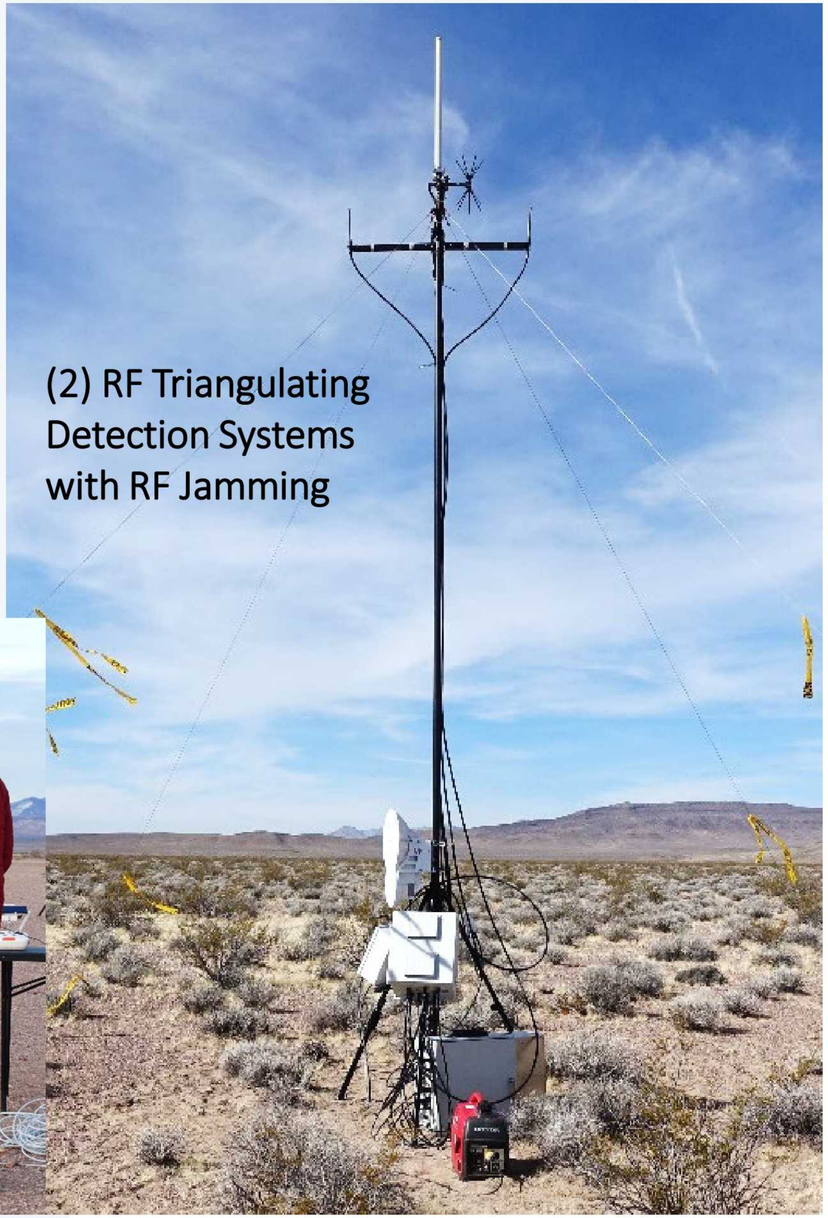


34

EXAMPLES OF SYSTEMS TESTED (FOR NNSA)

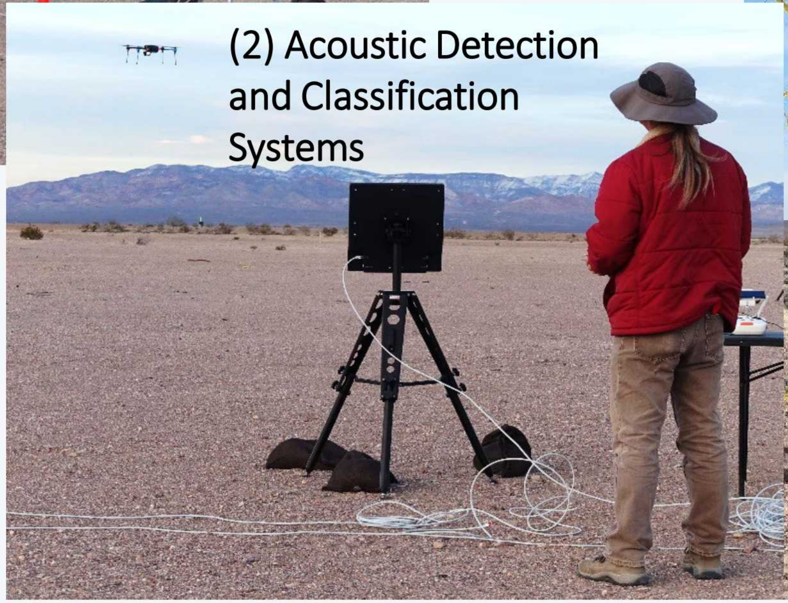


(2) Radar/Camera Based Sensing / Assessment Systems with RF Jamming



(2) RF Triangulating Detection Systems with RF Jamming

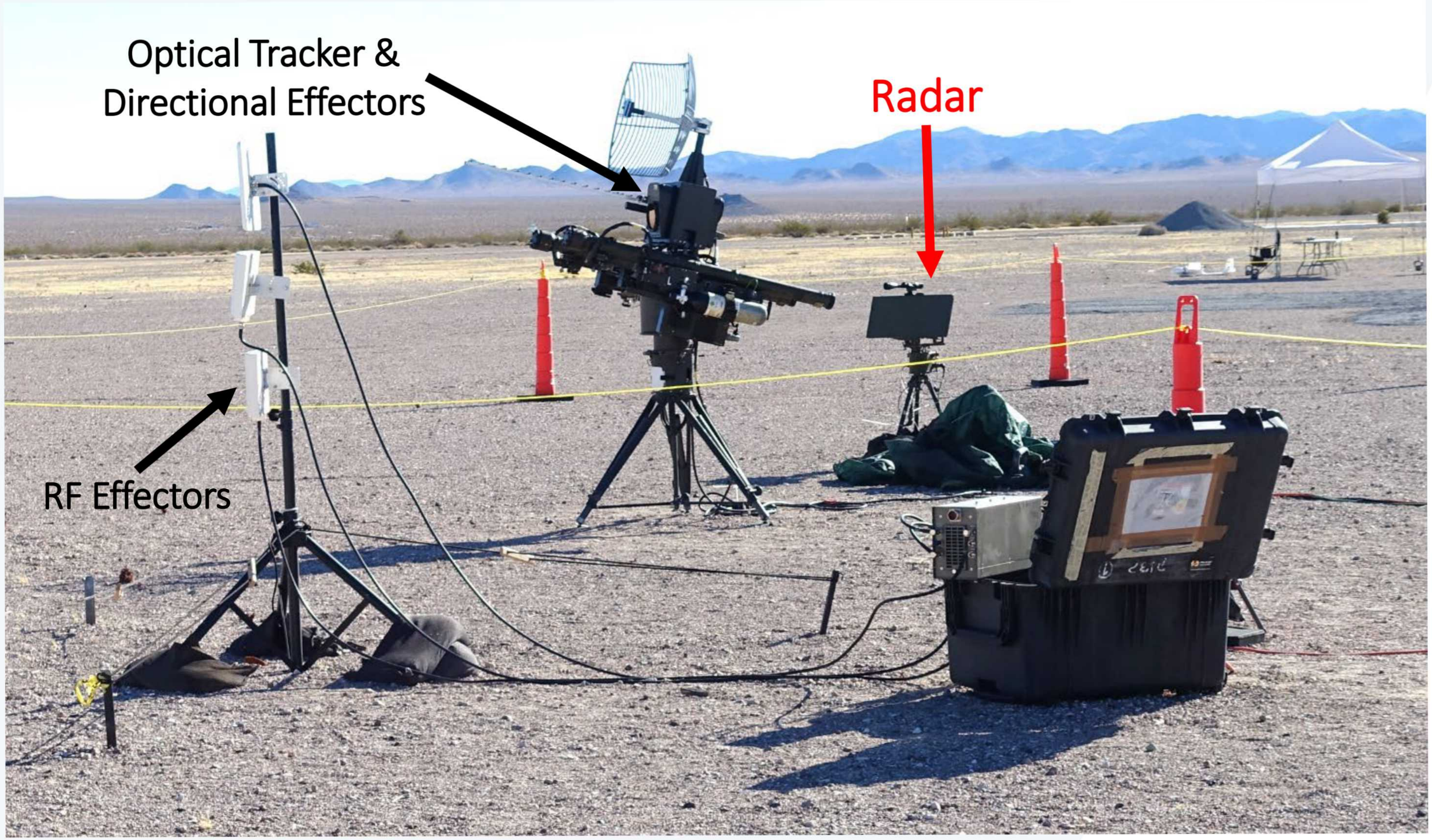
(2) Net-Capture Systems

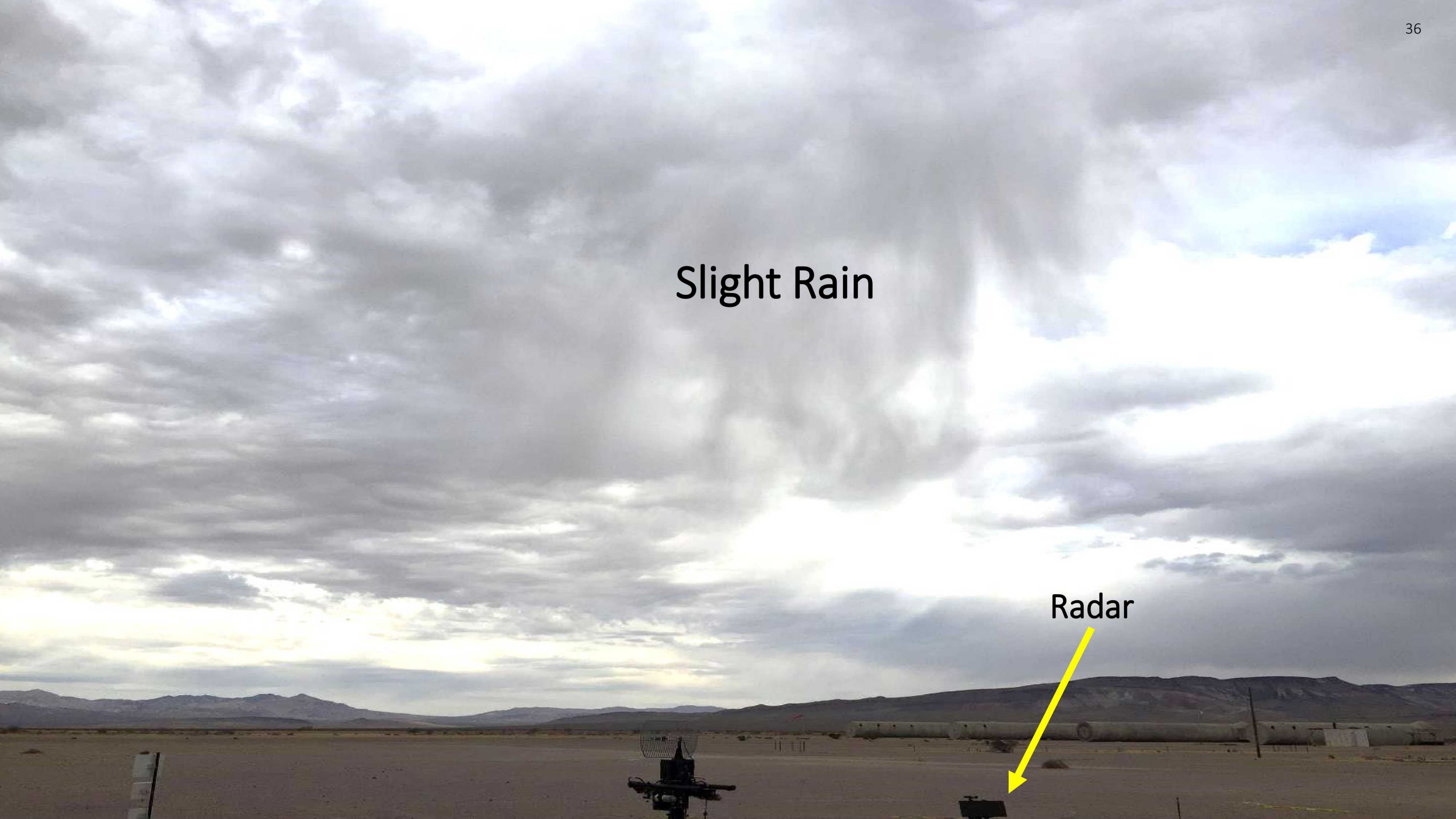


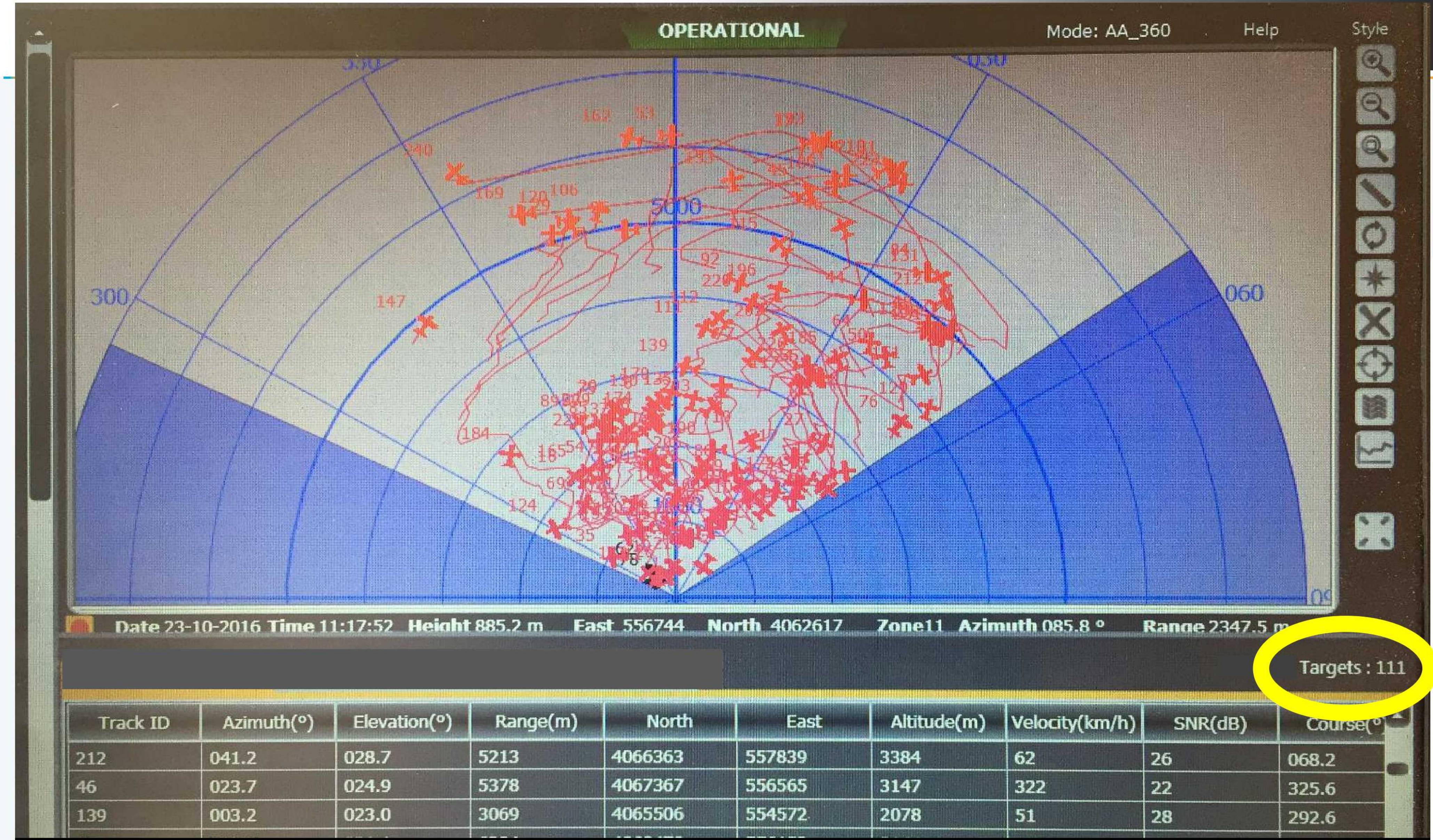
(2) Acoustic Detection and Classification Systems

35

WHY TESTING IS IMPORTANT



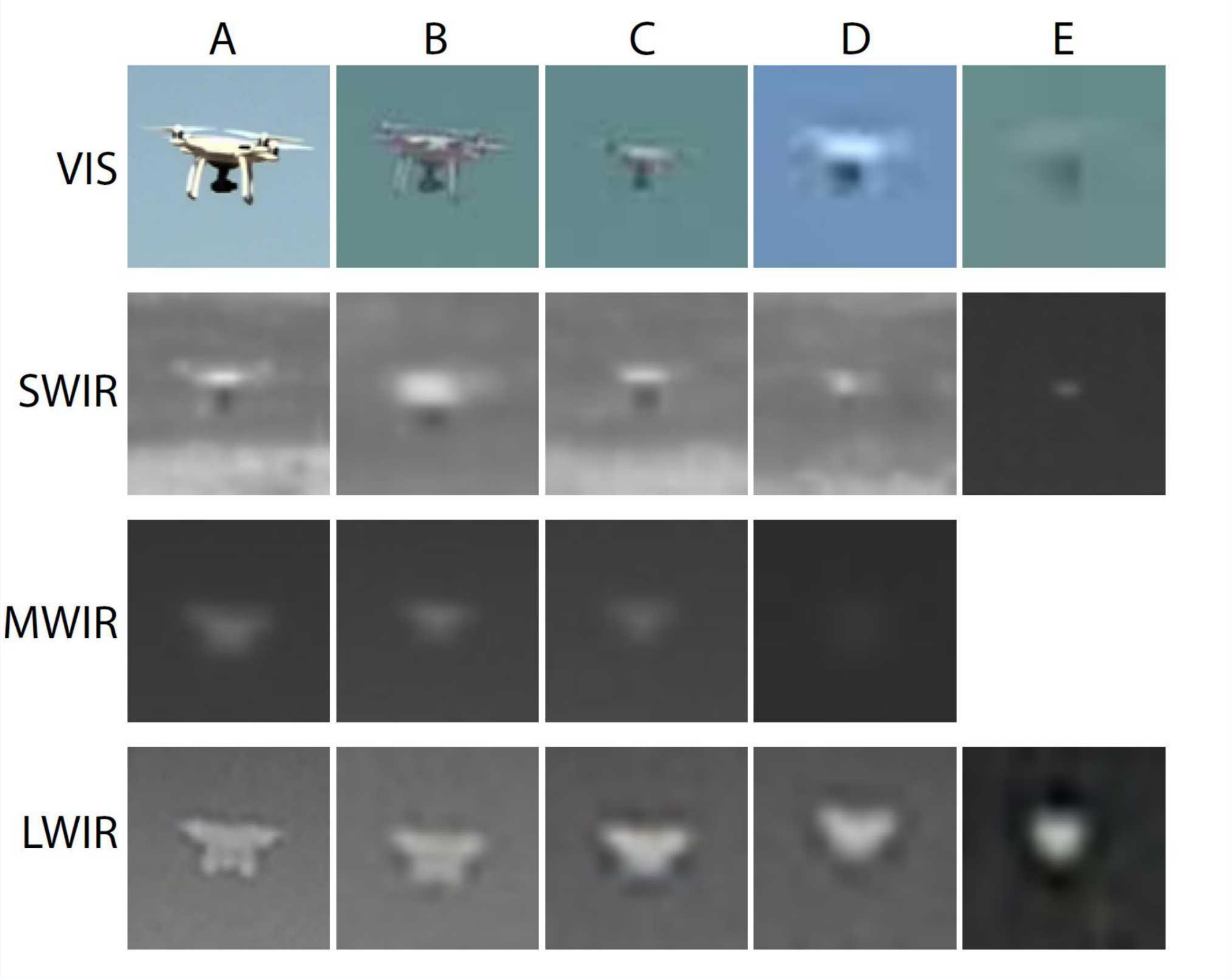

Slight Rain
Radar



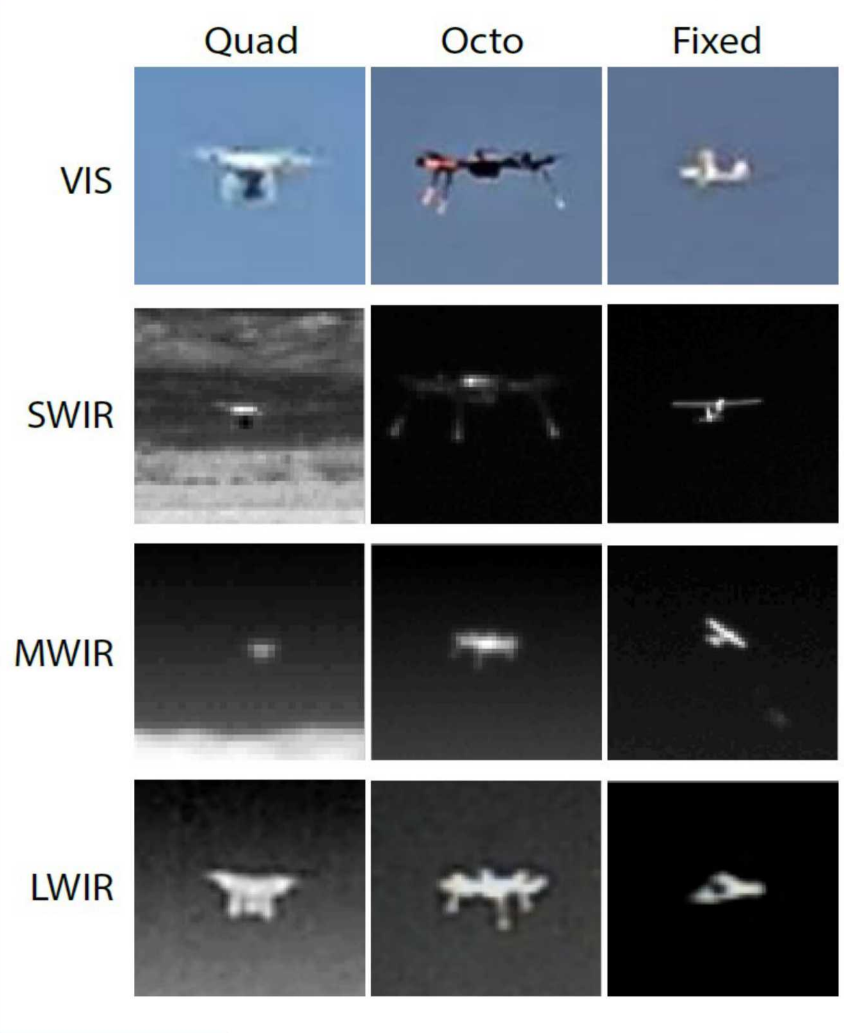
How would this impact an Operator? CONOPS?
Which (if any) is a true UAS intrusion alarm?

38

T&E OF THERMAL IMAGERS FOR SUAS ASSESSMENT



Comparison of # of pixels on target



Comparison of spectral bands