SIA EDUCATION at ISC

Counter-Unmanned Aircraft Systems (CUAS) in the Commercial Sector

The Challenges and Solutions in the Commercial Space

Dr. Richard Pettegrew, General Manager, IEC Infrared Systems

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

Introduction to the UAS Problem

- Commercial UAS Usage & Adoption
- Understanding the Threat
- Issues Caused by UAS in the Commercial Space
- Regulatory Challenges for the CUAS Mission

UAS Usage and the Need for CUAS

- The global commercial UAS market growth was valued at USD 8.77 billion in 2022.
- Projected to grow to USD 54.81 billion by 2030, at CAGR of 25.82% (Fortune Business Insights).
- A survey by the Federal Aviation Administration (FAA) estimated more than 1.7 million UAS registrations in the United States at end of 2024.
- Importance of CUAS:
  - The prevalence of UAS requires CUAS to stop incursions that could pose risks to public safety.
  - The FAA reported more than 1,300 UAS-related incidents involving aircraft in the U.S. from 2015 to 2020.
  - High-profile incidents, such as unauthorized UAS flights at Gatwick Airport in 2018, demonstrated significant operational disruption and economic impact, resulting in cancelled flights and financial losses, reinforcing the need for effective CUAS strategies.

Commercial Adoption of UAS

The usage of UAS is rapidly increasing across all sectors.

Commercial and Industrial UAS Usage

- Amazon and Google: Actively testing drone delivery, with Amazon Prime Air aiming to deliver packages in 30 minutes or less. Trials show up to 90% reduction in delivery times.
- Agricultural drones cover vast areas, collecting data for precision farming. AUVSI survey shows nearly 70% of U.S. farmers are interested in using drones for crop monitoring and field analysis.
- Estimated 80% of construction firms in the U.S. use drones for site surveys, with an average of 5% to 10% savings in costs and time by using drone technology (DroneDeploy).
- Energy Sector: The oil and gas industry is using drones for pipeline inspections, reducing inspection times by up to 90%. Drone inspections can cut costs by up to 50% (Price Waterhouse Cooper).

Commercial Adoption of UAS

Drones are here to stay, with widespread and growing commercial adoption.

Other Areas

- Emergency Services: Drones deployed by emergency services (e.g., police, fire departments) have increased significantly. A survey revealed about 80% of public safety agencies are utilizing drones to assist in search and rescue operations, fire response, and aerial reconnaissance.
- 62% of Americans believe drones can help improve emergency response services (Pew Research Center).
- Real Estate Marketing: Drones are transforming the real estate sector, with over 75% of real estate agents using aerial drone images in listings to attract potential buyers.
- An estimated 81% of organizations that use drones stated they improved operational efficiency and reduced costs (Pew Research Center).

Problems caused by drones (both accidental and malicious) are also here to stay.

Understanding the Threat

Unmanned Aerial Systems (UAS) are Usually Defined by Size and Performance

U.S. D.o.D. UAS Group Definitions			
UAS Group	**Max Weight (lbs)**	**Nominal Operating Altitude (ft)**	**Max Airspeed (knots)**
Group I	0-20 lbs	<1,200 ft	100 knots
Group II	21-55 lbs	<3,500 ft	<250 knots
Group III	<1,320 lbs	<18,000 ft	<250 knots
Group IV	>1,320 lbs	>18,000 ft	Any airspeed
Group V	>1,320 lbs	>18,000 ft	Any airspeed

In the commercial world, the vast majority of UAS ***threats*** will be in Class I or Class II: Small, inexpensive Commercial Off The Shelf (COTS) drones!

Understanding the Threat

Commercial Off The Shelf (COTS) UAS

- Low cost
- Easy accessibility (easy to buy, many on Amazon)
- Easy to fly with excellent autopilot and pilot assistance capability
- Anyone can fly them, with little to no training
- Simple but high-quality navigation capability
- Easy to modify
- Payload carry capacity can vary, but many have lift capacity of 1 to 15 Kg or more

Commercial Spaces Affected by Drones

A wide variety of commercial facilities and locations have vulnerabilities to UAS threats:

- Airports
- Stadiums and Public Events
- Industrial Sites
- Power Plants & Energy Facilities
- Amusement Parks



Risks that drones present to these sites include:

- Flight disruptions and danger to manned aircraft
- Operational disruptions/delays
- Danger (unintentional or intentional) to crowds
- Damage to facilities
- Industrial espionage/loss of trade secrets
- General privacy issues


Example: Commercial Airport Drone Incursions

Multiple high-profile drone incursions at major airports occurred in recent years.

Gatwick Airport, UK (December 2018): Gatwick closed for around 36 hours due to drone sightings delaying over 1,000 flights and approx. 140,000 passengers.

Heathrow Airport, UK (January 2019): Following the Gatwick incident, a drone was sighted near Heathrow. Flights were briefly delayed.

JFK Airport, New York, USA (December 2019): Drones spotted near JFK Airport led to temporary ground stops for departing flights.

Dubai International Airport, UAE (January 2020): Dubai International Airport delayed operations due to drone activity in its airspace, delaying flights.

San Diego International Airport, USA (December 2021): Drone sighting near the San Diego International Airport caused multiple flight delays.

No damage or loss of life occurred from these incidents, but the potential was there for major disaster!

Regulatory Challenges for UAS and CUAS Operations

Operating a drone is much easier than countering one.

Federal Aviation Administration (FAA) Rules

- Register your drone with the FAA
  - Maintain updated registration to avoid penalties
  - Study and pass the FAA Part 107 exam

Safety Guidelines

- Follow the FAA's safety guidelines for drone operation
  - Fly below 400 feet
  - Keep the drone within visual line-of-sight
- Complete the required FAA TRUST test for hobbyists

Airspace Awareness

- Learn to read and interpret airspace maps
  - Identify controlled and restricted airspaces using sectional charts
- Use LAANC for flights within controlled airspaces, such as near airports

Regulatory Challenges for UAS and CUAS Operations

In the U.S., drones are considered 'aircraft' by the FAA, just like an airliner.

You CANNOT interfere with a drone in flight

- Even if it is hovering over your property, looking into your windows!
- Even if the drone is doing something illegal, it is illegal for you to interfere/disrupt its activities!
- Regardless of the altitude or range of the drone.
- It may be flying illegally (too close to people or structure), but you still are NOT allowed to capture/shoot down/swat down, etc. Cannot legally interfere with it…at all.

You CANNOT jam its guidance signals

- FCC requires licensing for radio signal transmissions.
- If you jam a drone, that constitutes 'interference' from an FAA standpoint.

Regulatory Challenges for UAS and CUAS Operations

Effects of these regulatory issues: Commercial CUAS efforts are currently very limited, but it's likely only a matter of time until that changes.

- The cost of most CUAS sensors/systems, coupled with the severe legal limits on what can be done to counter the threat has led to limited commercial use of CUAS systems in the U.S.
- There are limited Governmental exceptions where certain CUAS actions are allowed: Departments of Defense, Energy, Justice and Homeland Security, under limited conditions
- **Many people believe the restrictions will be lessened, but likely *only after an incident involving a drone causes serious consequences.***

What CAN be done (from a technology standpoint), if the laws change?

- The remainder of this presentation addresses technologies and techniques which are used for the detection, tracking, and mitigation of UAS.

How to Detect and Counter a UAS Threat

- The CUAS Kill-Chain
- Detection/Tracking Technologies
- Mitigation Capabilities
- User Interface/User Assistance
- Clutter Mitigation
- Deep Learning AI: Neural Networks

Countering the Threat

The UAV Threat is Complex.
What technologies are needed to counter It?

UAVs are asymmetric: The threat is less complex and costly than the solution.

UAVs are:

- Small, fast, hard to detect
- Can ‘hide’ within bird populations (as seen by some sensors)
- Cheap, easy to fly, commonly available

To counter such a threat, you need:

- Advanced sensor and effector systems
- Layered technologies, to provide robust coverage
- System integration: making the sensors and effectors work together
- Effective data processing and handling, to minimize operator workload

Countering the Threat

What is the CUAS Kill Chain?

Due to the complexity of the CUAS problem, it's useful to break it into a series of tasks, often called the Kill Chain.

For this presentation, the Kill Chain tasks are defined as:

- Target Detection: Determine if something is there
- Clutter Mitigation: Get rid of clutter (usually, birds)
- Target Assessment & Tracking: Examine and track the threat
- Target Mitigation: Counter the threat using the appropriate response

The following slides will break down the types of technology used in these tasks.

CUAS Detection & Tracking

RF Detection Systems

Tracking the Control & Video Signals from the Drone & Controller

- Passively detect RF signals from drones and controllers
- Some systems can de-code the signals, and provide location, heading, speed, and ID info
- Most are library based - must have the electronic signature of the drone in their memory or cannot detect it.
- Many options/manufacturers in this trade space
- Some have a limited ‘direction finding’ capability, giving a general direction or quadrant that the target may be in. Some systems can (broadly) do that for unknown signals in the RF bands generally used for remote controls.

CUAS Detection & Tracking

RF Detection Systems

Tracking the Control & Video Signals from the Drone & Controller

- Multiple bands used from 400MHz up to 6 GHz.
- Common spectral bands:
  - WiFi bands: 1.3, 2.4, 5, 6 GHz
  - 400-900 MHz
  - Most GPS-type signals (including Beidu, Galileo, GLONASS (and other foreign sources) generally are around 1.2-1.6 GHz.
- May or may not be able to provide precise target location.

Advantages of RF Detect Systems

- Passive, no licensing needed
- No clutter. Birds don't emit!
- Can offer significant ranges, in many cases
- Can be cost effective, compared to other technology

Disadvantages of RF Detect Systems

- If not in library, generally NO detection
  - Drones flying waypoints would not have to emit
- Often, somewhat slow update rates (on order of secs)
  - Slow update can make pointing a camera at the target a challenge.

CUAS Detection & Tracking

Acoustic Detection Systems

Listening for the Sounds of Rotors and Motors

- Uses directional microphones to sense rotors & motors
- Completely passive, emits nothing
- Can give general direction to target, but not precise location information

Advantages of Acoustic Systems

- Passive, no licensing needed
- Operate in complex geometric environments where line of sight is limited (forests, urban areas)
- Detect 'RF dark' drones that are not emitting (flying waypoints, etc.)

Disadvantages of Acoustic Systems

- Limited range, compared to RF and radar systems
- Susceptible to local noise sources, such as vehicles, machinery, etc.
- May be sensitive to adverse weather, such as wind or rain.
- Cannot give precise target position information.

CUAS Detection & Tracking

Optical Detection Systems

Optical Change Detection

- Uses either spinning/scanning imager, or an array of imagers
- Often thermal, but can use visual spectrum as well
- Completely passive, emits nothing
- Can give direction, but not range to target

Advantages of Optical Systems

- Passive, no licensing needed
- Operate in complex RF environments (many RF sources)
- Detect 'RF dark' drones that are not emitting (flying waypoints, etc.)
- Can be a complimentary sensor in a layered system
- Thermal imaging can operate in total darkness

Disadvantages of Optical Systems

- Limited range, compared to RF and radar
- May have high false alarm rate from clutter sources such as birds or distant air traffic
- Can give azimuth and elevation, but not range to target
- Sensitive to adverse weather, such as rain/snow/fog
- Can be expensive (particularly long-range thermal)

CUAS Detection & Tracking

Radar Detection Systems

Active Electronic Detection

- Operates by emitting an RF signal, then analyzing the bounce back (return) signal.
- Can use either fixed (staring) panels, or scanning sensor
- Many options in this trade space
- Can offer significant range, accurate location & speed information

Advantages of Radar Systems

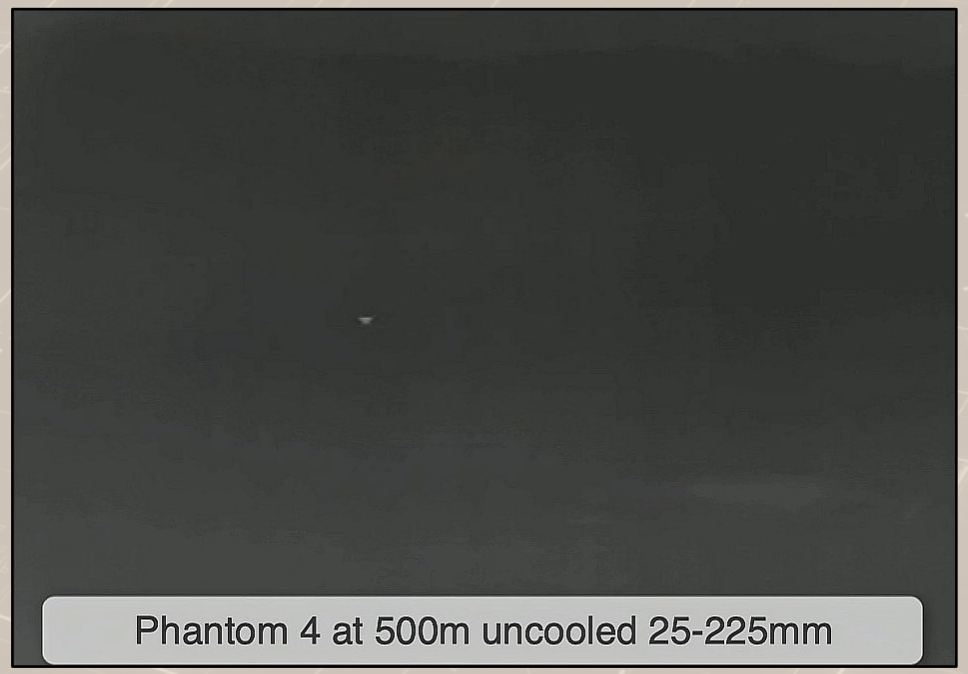
- High update rates
- Accurate location and range data
- Can offer significant range
- Works well in a layered system

Disadvantages of Radar Systems

- Active RF emitter, can be detected
- May require FCC licensing
- May have high false alarm rate from clutter sources such as birds or distant air traffic

Target Tracking/Visualization

Thermal Target Tracking and Assessment



Examples of thermal imaging: Drone at different distances with both uncooled and cooled thermal imagers

- Long focal length thermal imaging must use cooled (MWIR) systems.
- LWIR is typically uncooled but must use shorter lenses.
- Uncooled are less expensive but have limited range compared to cooled imagers.

Target Tracking/Visualization

Thermal Target Tracking and Assessment

- Cameras need lots of pixels on target (PoT) to determine anything: both AI and humans need that.
- A wide Field of View (FoV) is needed for broad area detection, but a very narrow FoV is needed for identifying anything.
- Need thermal to see at night effectively (also works well in day)
- Optical tracking: works well in good conditions, questionable others
- Some use narrow FoV imaging with AI for clutter discrimination, but this carries limitations:
  - Can only look in one direction at a time
  - Cannot use one imager to stay on one target: must keep scanning
  - Typically, camera must dwell on target for several seconds: if there is lots of clutter, may take too long to “figure it all out”

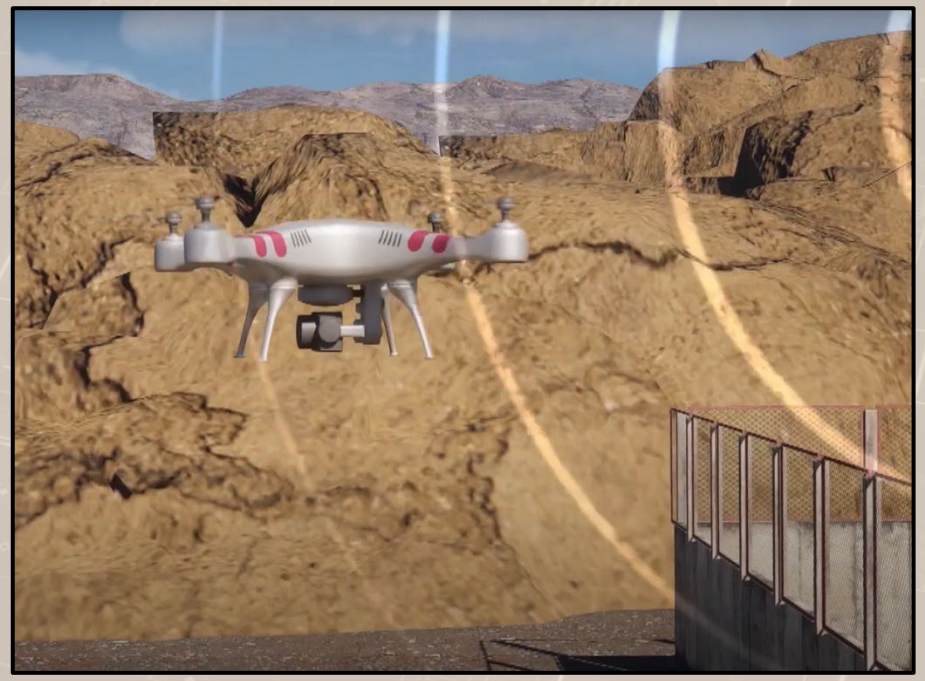
Drone Mitigation

Radio Frequency Methods

Non-kinetic, low physical damage

- Targeted jamming: ‘attack the network’
  - Some RF detection systems can take over a drone; force it to land or fly away
  - Only works if target is in its library
  - Will not affect other drones or devices in the area

- Barrage jamming: overpower the drone controller’s signals.
  - Can operate on multiple frequencies (control, video, nav)
  - Can be omni-directional or directional
  - Will have effects on anything in its area/direction
  - Disrupt WiFi, and/or GPS signals



Drone Mitigation

Physical (Kinetic) Methods

Soft Kinetic

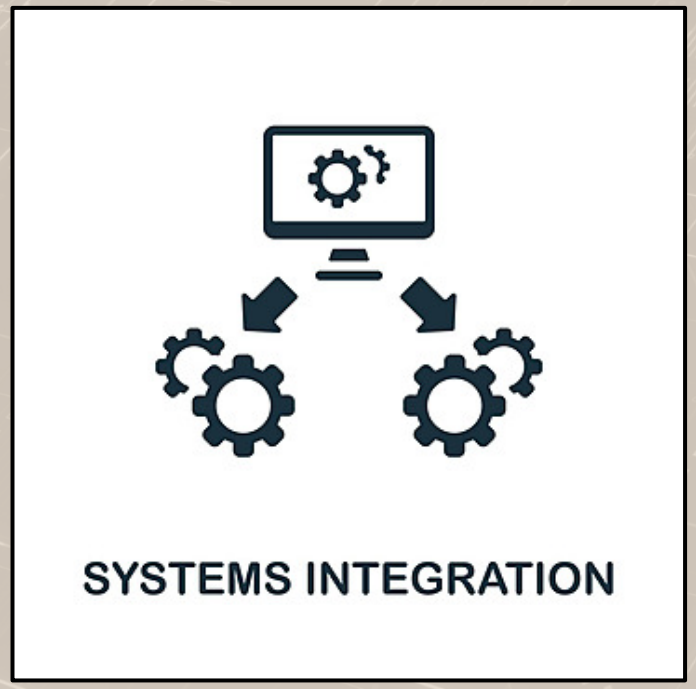
- Interceptor drones, shooting a net
- Guided to target by ground-based radar
- Low/zero collateral damage
- Target can usually be carried back to a designated location

Hard Kinetic

- Gun/missile solutions
- Radar or optically guided
- Risk of high collateral damage from fallout/missed rounds

System Integration

Connecting subsystems to form a complete solution.

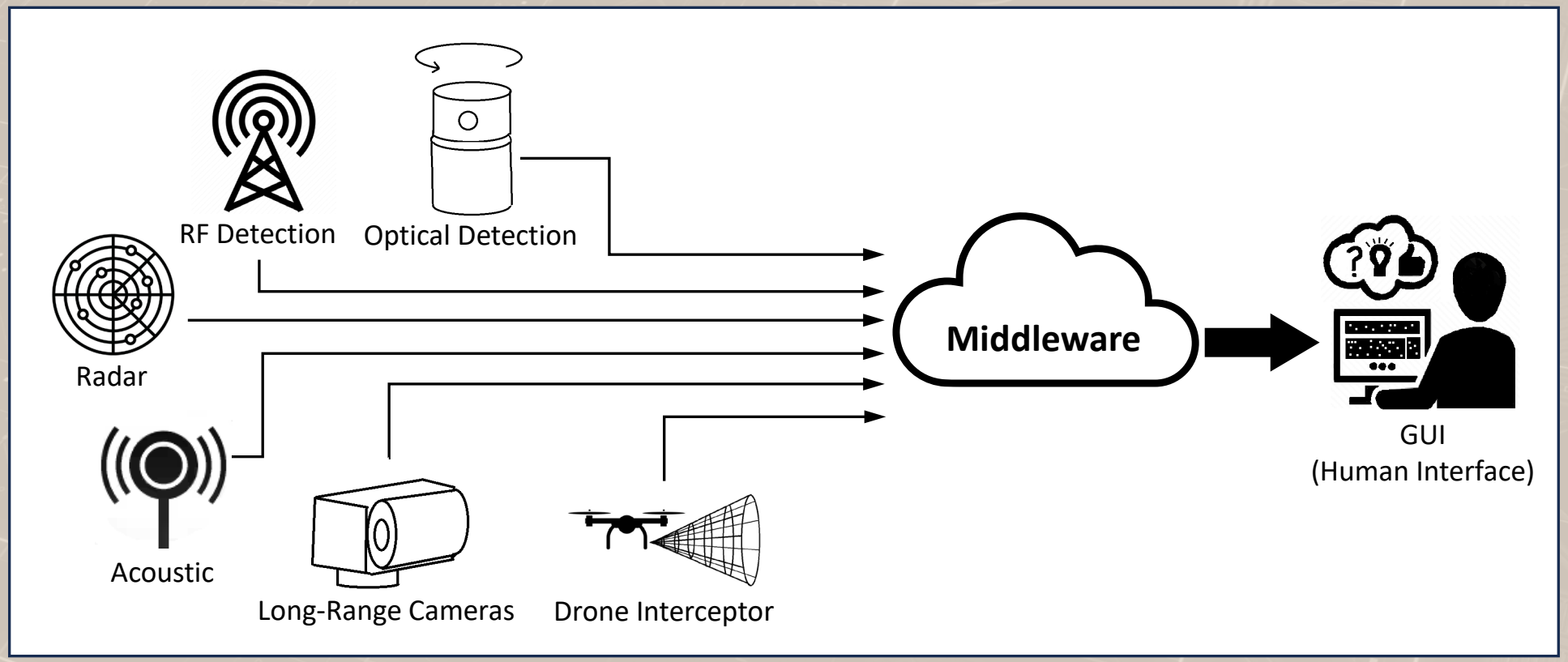


- Layered approach to CUAS provides robust system: various sensors complement each other
- Multiple sensors & subsystems need to be integrated to provide practical, coordinated interface to user.
- Complex sensor systems, but don't want to have expert operators
- While you strive for automation, most systems will require a dedicated operator. Especially true if any form of mitigation is used.
- Scalability: need systems that can increase in scope and range as needs change.

System Integration

What is Middleware?

Middleware:
A combination of software and hardware interfaces that allow connection of multiple sensors and subsystems, to form a combined, coordinated system.

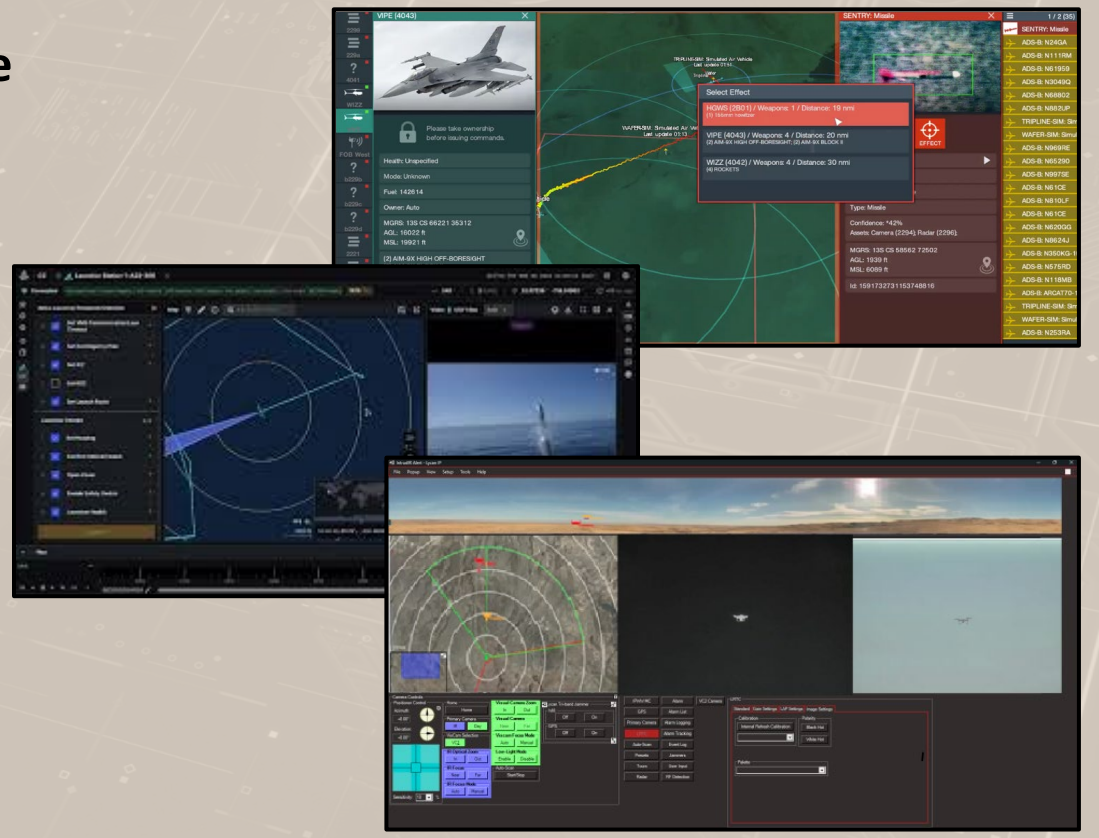


System Integration

What is Middleware?

Middleware acts as the glue layer, pulling all of the system sensors and elements together.

- Coordination & control of multiple sensors
- Data handling & processing
- User Interface (GUI)
- User assistance:
  - Track merging (from multiple sensors)
  - Clutter mitigation
  - Target prioritization



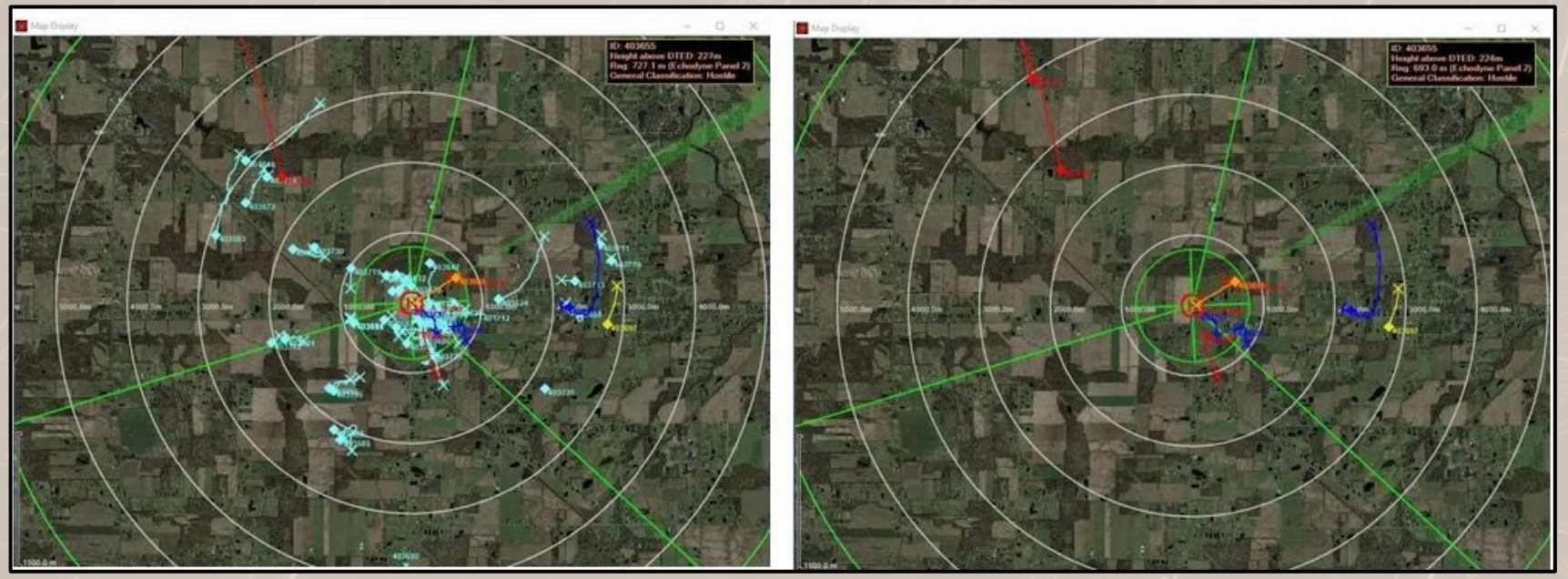
Clutter Mitigation

Why is clutter mitigation important?

Radar-based systems are effective at detecting everything, including birds; In this context, anything that the radar detects that is not a drone is clutter.

- If the operator is constantly shown lots of clutter, they will become desensitized and start ignoring *everything*.
- Any radar-based system must have an effective clutter-mitigation strategy, or it will be useless!

Effective Clutter Mitigation



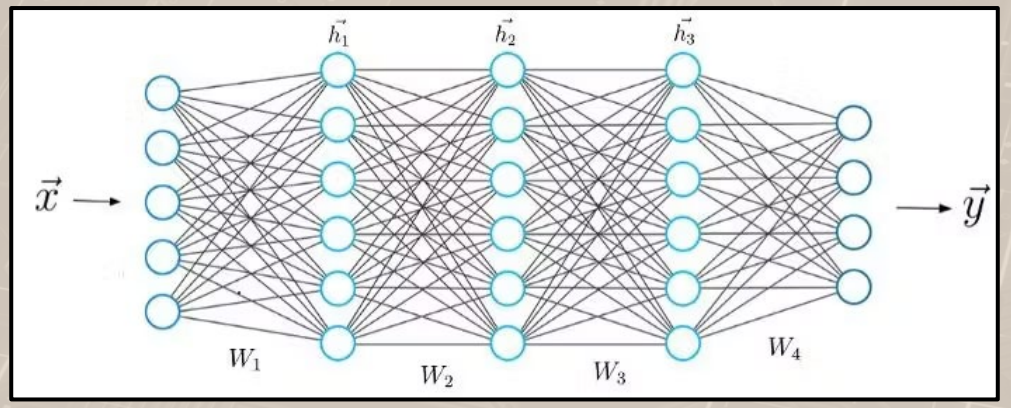
Both images are same radar image, less than 1 sec apart. Left image shows all radar hits, right image shows de-cluttered radar image.

Clutter Mitigation

How do CUAS systems handle clutter?

Deep Learning (Neural Network) Artificial Intelligence (AI)

- AI Neural Networks have been pitched as the solution for many problems. We've all heard about it, but what does it really do?
- At the end of the day, AI provides one basic thing: pattern recognition.



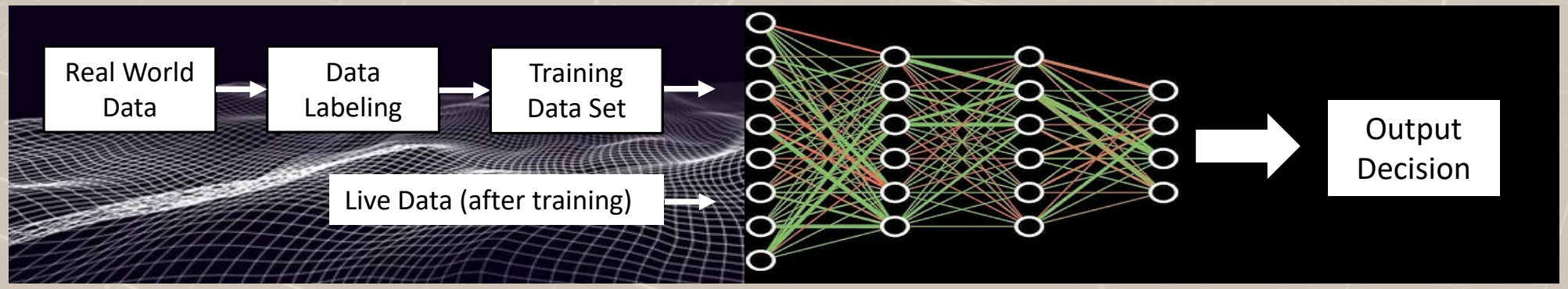
Computers can be very good at repetitive tasks such as pattern recognition *if they are trained properly*.

- Neural networks are intended to mimic the way neurons in the human brain process information.
- Neural networks excel in finding patterns in deep, multi-variable data that are difficult for humans to see.

AI in Clutter Mitigation

Deep Learning-Neural Networks

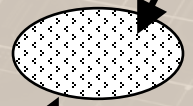
- Comprehensive training is the key to successfully implementing a Neural Network.
- Often, why a Neural Network is successful may not be obvious – it found patterns in the data that humans can't easily detect.
- Neural Networks work great in some situations: for example, machine vision for inspection of product on assembly lines.
- Why does it work well in that case? In a controlled environment like an assembly line, all possible trade space of the variables can be trained.
- Where does it NOT work well? In situations where it cannot be extensively trained over the entire variable space



AI in Clutter Mitigation

Deep Learning-Neural Networks

Training Space: Controlled Environment



Each mark within the ellipse represents a training case. With the given set of variables at that point, the system was taught the proper outcome.

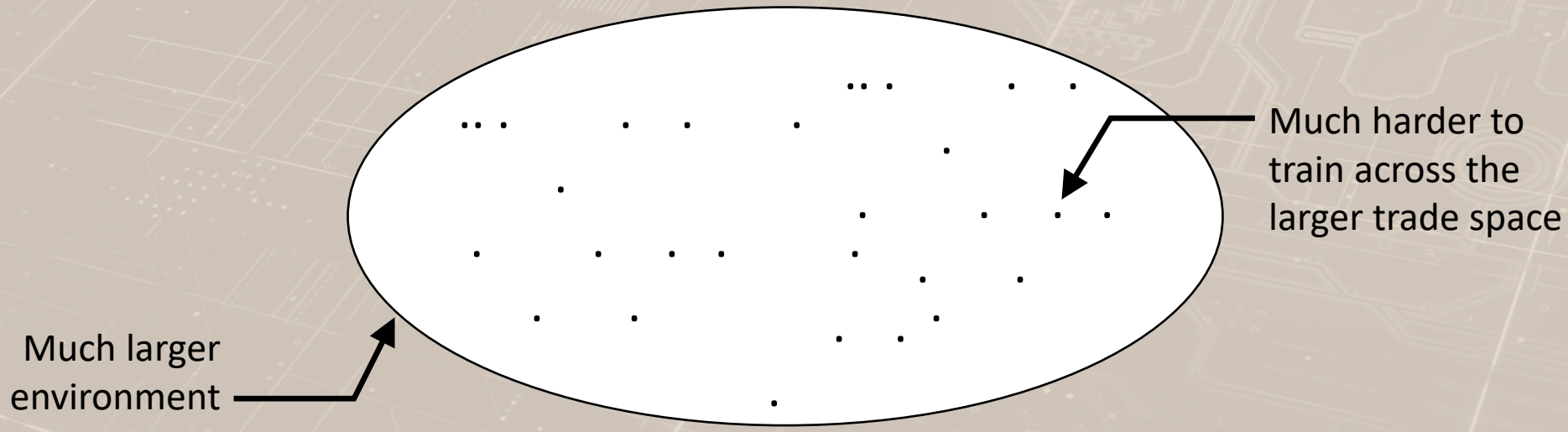
Consider the ellipse to represent the trade space of all possible variables within the system.

With limited variables (controlled environment), you can train effectively over the whole domain, teaching the system how each variable affects the outcome. This leads to effective decision making by the system.

AI in Clutter Mitigation

Deep Learning-Neural Networks

Training Space: Uncontrolled Environment



Without proper training on all possible trade space, the system doesn't fully understand the environment; by making inferences on incomplete training data, its accuracy is severely compromised. Even worse, it will STILL give a result, and the operator may not know that its result was based on poor training.

AI in Clutter Mitigation

Training a Neural Network

The trade space that must be trained is large…

False Targets (Clutter)

- Unknown number of birds at any time/place (from singles to flocks)
- Variety of bird sizes (small sparrows/finches, up to large hawks or vultures)
- Fly in any/all patterns and altitudes
- Bird activity varies by time of day

True Targets (Drones)

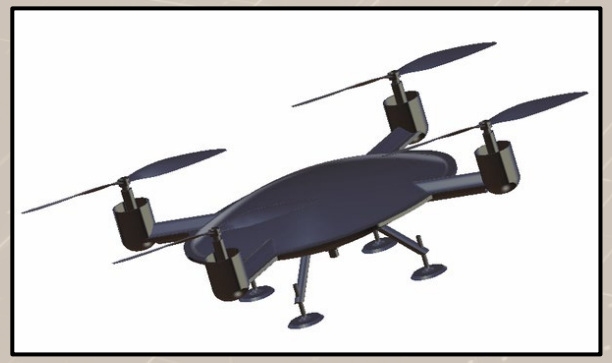
- Unknown number, though number is far less than clutter (birds)
- Fly at any time
- Can be swarm (from one direction or many directions)
- Fly at range of altitudes, nearly any pattern

Taken over time, the ratio of clutter targets to true targets is likely to be:

$$\frac{\textbf{Many thousands (clutter targets)}}{\textbf{Very small number (true targets)}} \Rightarrow \textit{>99.99\% clutter}$$

AI in Clutter Mitigation

Training a Neural Network



How are these system trained? What is meant by "training"?

- Deep Learning systems utilize unguided training. They are shown examples of data and told what the object is.
- This can be applied to either radar or optical data, or both.
- They aren't told what aspects of the data make it a 'bird' or a 'drone', just that it is. *The system is expected to figure out the pattern.*

- Systems that use this approach on optical (thermal or visual) data also need to learn the target from many possible viewing angles, which requires even MORE data.
- Must have an appropriate balance of data (bird and drone), otherwise the system will become biased towards simply saying that everything is a bird (which is right >>99% of the time!).
- Some suppliers will say 'the system gets better with time' as it is used (and trained by the operator). This adds tasks to the operator and still doesn't guarantee that the entire trade space is properly covered and represented!

In theory, deep learning can work: In practice, be wary!

Pros and Cons

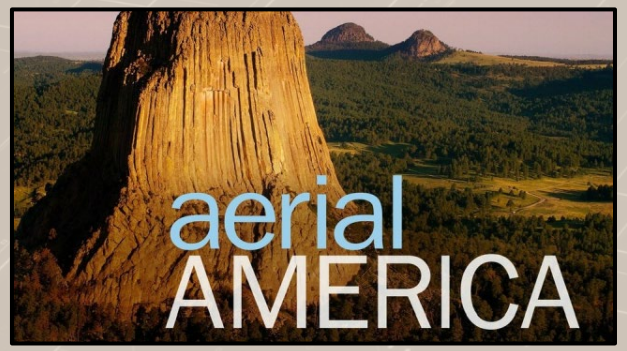
What sensors should you use for the CUAS mission?

- Optical & acoustic sensors: short range, very affected by environment
- *Radar and RF Detect are the most practical CUAS detection sensors.*
- Radar vs. RF detect
  - Radar more robust detection, but clutter is the problem
  - Clutter mitigation strategies: AI is popular but be wary.
- No sensor is perfect: all have strengths and weaknesses.
- *Layered, multi-sensor, fully integrated system is the most robust solution.*
  - Sensors are complimentary and confirmatory
- Cost, location, and other considerations (including legality) drive the choices
  - How bad do you need it?
  - What is the UAS risk in your case?

Summary and Conclusion

Where do we go from here regarding UAS threats?

Drones are Everywhere!



Drones are here to stay!
They have many good uses:

- Agriculture
- Remote inspection: power lines, pipelines
- Survey/mapping
- Package delivery
- Photography/cinematography (e.g., *Aerial America* show)
- Recreation

Drones are cheap, easy to buy, easy to fly

- Only becoming MORE widespread

Drone Usage Also Has a Darker Side

- ‘Accidental’ intrusion by hobbyists into controlled airspace
- Personal privacy concerns
- Corporate privacy concerns
- Direct malicious attacks
- Prison contraband intrusions
- Corporate privacy concerns

What Can You (or Can't You) Do About a Drone?

- The threat has evolved faster than the legislative environment
- Under current U.S. legal environment:
  - Drones are considered aircraft, just like a manned aircraft
  - ***Can't interfere with a drone, for any reason.***
    - This is true, even if the drone is intruding on your personal or corporate privacy
  - This includes:
    - Physical interference
    - RF jamming
    - Using lights or lasers

This is likely to change only after a major incident.

If It Were Legal, What Could Be Done, Technically?

Characteristics of the threat require a sophisticated, layered technical solution!

- RF detection: highly effective, if drone is in its library
- Radar: detects all drones, but subject to clutter problems (birds)
  - Clutter mitigation technologies are available but be careful of the claims: See it work in a relevant environment!
- Combination of Radar and RF detection is quite robust
- Long range imagers (cued by radar/RF detect) are useful for assessment, tracking
- Mitigation: RF jamming can be highly effective, multiple bands
- Effective net-launching interceptors exist, though expensive

The Bottom Line

- For many businesses, the cost of effective CUAS makes it impractical, given that you can't mitigate!
- However, the commercial community needs to recognize the threat and convince their elected officials to make the needed changes!
- One way to do that: legal advocacy! One such group:

The Alliance for Drone Safety and Security Solutions

Coalition of stakeholders such as:

- Manufacturers
- State and Local Law Enforcement
- Critical Infrastructure owners/operators
- Others

Focused on legislative action to enable use of drone safety & security technologies, including detection and mitigation systems. Working to influence Federal legislative, regulatory and funding outcomes on these issues.

For more info, contact Rob Ehrich:
rob@slipstreamstrategies.com
(202) 285-7987

Thank You!

Dr. Richard Pettegrew
General Manager
IEC Infrared Systems
www.iecinfrared.com

Contact me at:
rick.pettegrew@iecinfrared.com
(440) 382-1135

Thank you!

Have thoughts about SIA Education@ISC?

Scan the QR Code on the left to provide your feedback on SIA Education@ISC Sessions at ISC West

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses