Physical Security Center of Excellence (PSCOE)

Exceptional service in the national interest

Security Challenges: Unmanned Aerial Vehicles

Presented by:
Chad Monthan, Sandia National Laboratories

On Behalf of:
Mr. Sly Harris, NNSA – Defense Nuclear Security

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

SAND2018-1388 PE

UAS Use Cases

- UASs are the fastest-growing sector within the U.S. aviation industry
    - Almost 2,000,000 sold in the U.S. in 2015 alone

Delivery

Policing

Safety/Monitoring

Farming

Security

Movie Production

Wildlife Management

R&D and Aerial Photography

Tourism

Disaster Response

Search and Rescue

Illicit Uses
⋮

Evolving Threat

- Increase in UAS populations, ease of acquisition, and new capabilities have led to many instances of concern toward potential illicit uses
  - Near misses happening regularly
    - Dozens can fly > 9,000 ft AGL (hobbyist ceiling is 400 ft)
    - First unconfirmed mid-air collision with manned aircraft

Hexacopter:

- 4 lb payload
  - 10–12 min
- 10 lb
  - 5 min

Octocopter:

- 12 lb payload
  - 10–12 min
- 20 lb
  - 5 min

Speed = 60–80 mph

Fixed wing carry >> payload for >> distances

Future Direction for Unmanned Systems

- Autonomy – rapid technology evolution
  - No communications link
    - No signal to sense or manipulate
    - Attribution?
  - Rapid, reactive control
    - Low and fast
    - Autonomous Sense and Avoid technology
    - Randomizes behavior from blue perspective
  - Push-button swarms
    - One individual controlling many platforms
    - Tactical speeds and objectives are achievable today (DJI4)
  - Machine-speed detect/assess/respond
- Commercial payload and component integration
  - Advanced, one-off payload development (additive manufacturing)
- Multi-purpose platforms (ground, sea, and air)

Google: Internet from the Sky

Photo courtesy of Google, Inc.

Photo: Sandia National Laboratories

Issues with Small/Unmanned Systems

Policy, Legal, and Technical Challenges

Policy

- Current UAS technologies were not developed to comply with existing FAA airworthiness standards

Legal

- What is considered trespassing with small UAS?
- Delicate balancing act: public/privacy concerns vs. national security
- What are the legal issues associated with interfering with an unmanned system?

Technical

- Technology revolution has moved development from graduate laboratories to high school student basements
  - Additive manufacturing
  - Open-source software
  - Ubiquitous, advanced, cost-effective, miniaturized, and integrated control hardware/firmware
- Current research is poised to continue transforming this threat (rapid evolution)
- Detection and timely assessment of small UASs at range is challenging, with no immediate solution
- Neutralization is problematic due to policy and collateral damage
  - Operations within the U.S. may limit availability/use of some technologies
  - Swarm threat?
- Not just a UAS issue
  - Multi-modal, advanced autonomy, no RF link to exploit

Privacy Concerns

Approx. Payload = 9 lb

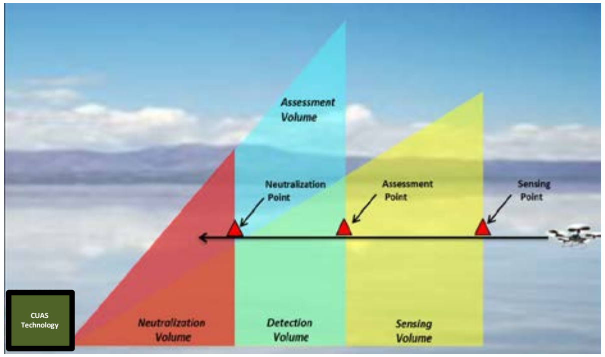
PSCOE

Airspace Control and Situational Awareness

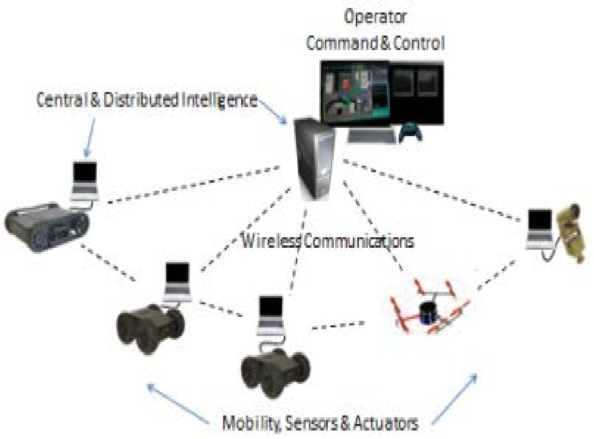
- Multiple government and international agencies are struggling with understanding who/what is in their airspace
  - Is it a hobbyist or is it a UAS with malicious intent and with a threatening payload?
- Eyewitness accounts do not guarantee accurate assessment of who/what is flying over sites
  - Need a reliable UAS detection and assessment system
- Need the capability to distinguish friendly from non-friendly assets
  - Establishing no-fly zones to assist in determining intent
  - Capability to neutralize UASs identified as a threat

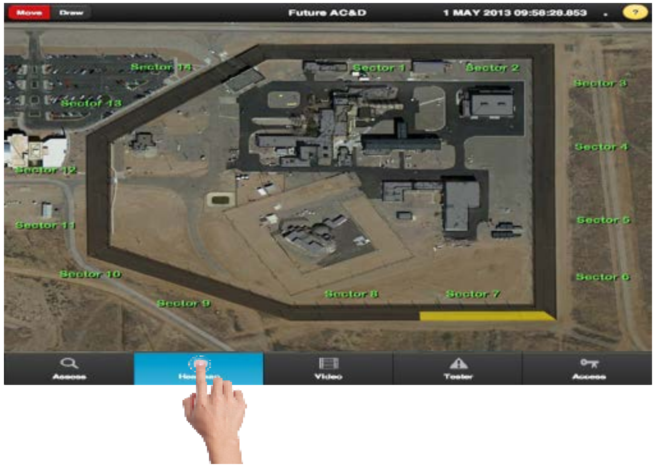
Security Operational Needs

- CUASs



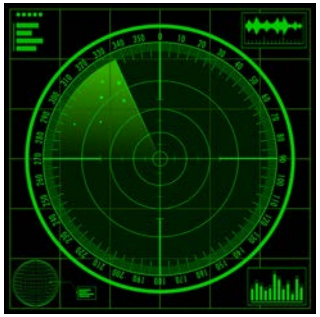
- Security Operations – Use of Unmanned Systems


Operator Command & Control
Central & Distributed Intelligence
Wireless Communications
Mobility, Sensors & Actuators



CUAS Technologies

- Detection
  - Radar – integrated COTS systems
  - Passive acoustic/seismic
  - Passive RF – spectrum analyzer
  - Imaging
  - Human ears and eyes



- Assessment
  - Imaging cameras
  - Library matching (passive RF, acoustic)
  - Human eye

- Neutralization
  - RF techniques
  - High-power lasers
  - Projectiles
  - Net capture (from air or ground)
  - Guided missiles
  - Passive barriers (hardened/buried structures)

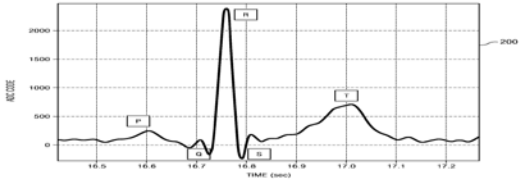


FIG. 2

CUAS Considerations

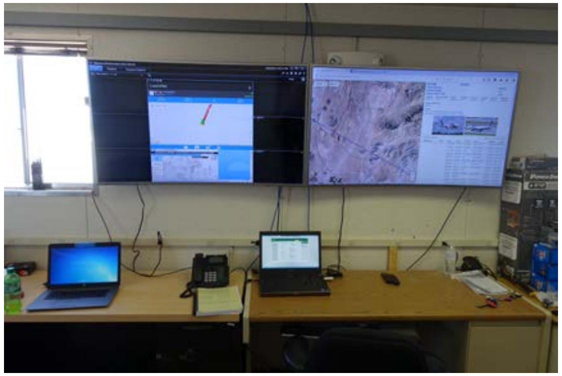
- Counter-systems must coexist and complement existing systems (security, operations, communications, etc.)
- Neutralization methods cannot interfere with or disrupt current security operations
- No immediate solution currently exists
  - Requires differing technologies
    - There are pros/cons of various technologies as well as site-specific considerations
  - Technology maturity level: Manufacturer's claimed capabilities may not represent actual capabilities
    - Must test these systems to understand the full range of CUAS capabilities
- Operational considerations
  - Emerging capabilities – requires continuous re-evaluation of capabilities

National Nuclear Security Administration

PSCOE

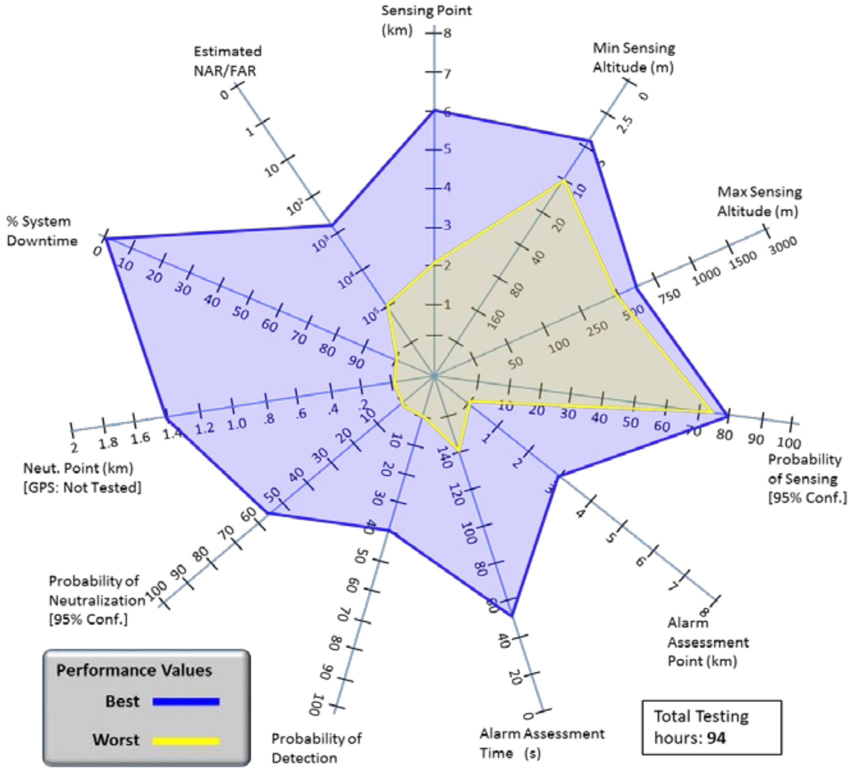
Considerations for UAS Security Capabilities

- UASs can enhance existing security functions
  - Increased situational awareness (imaging, sensors, audio, etc.)
  - Quicker and safer assessments by security personnel
  - Platform for additional mobile sensors
  - Can be used to inspect security elements throughout a facility
- Operational considerations
  - Security operations of UASs must coexist and complement existing systems (security, operational, communications, air traffic, etc.)
  - Operational modes (24/7, limited-use, pilot-controlled, fully autonomous, tethered vs. untethered, communication protocols, data, etc.)
  - Sensory overload concerns for operators
  - Training
  - Certifications (pilots, aircraft)
  - Maintenance
  - Legal/policy
  - Emerging capabilities require continuous refreshing



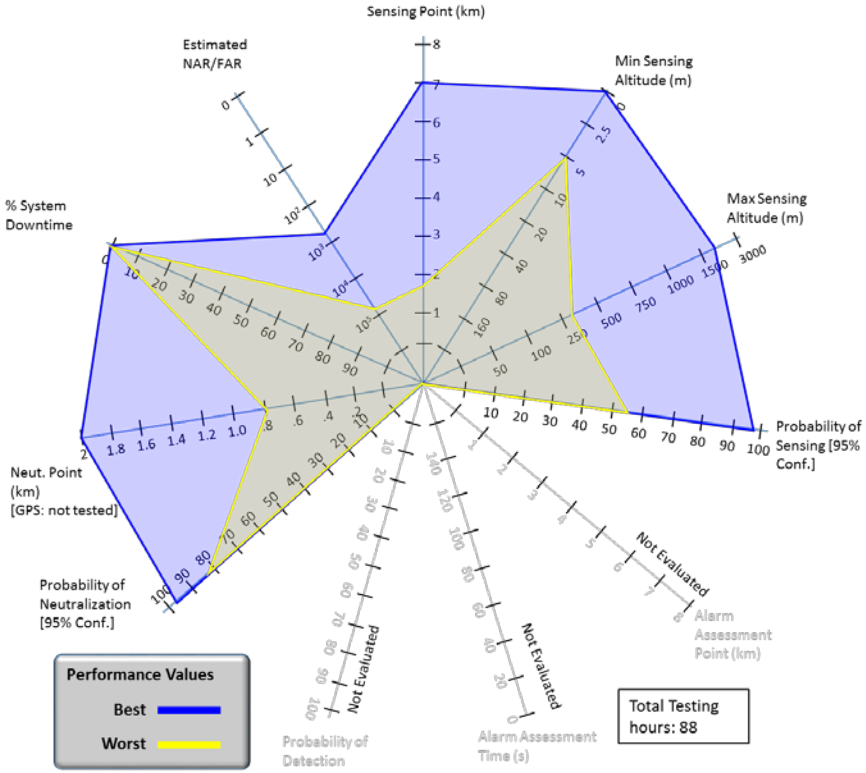
Notional CUAS Performance from Testing

- Radar/camera-based detection and assessment systems with RF jamming (Example = CUAS 1)



Total Testing hours: 94

- RF sensing/detection systems with RF jamming (Example = CUAS 2)



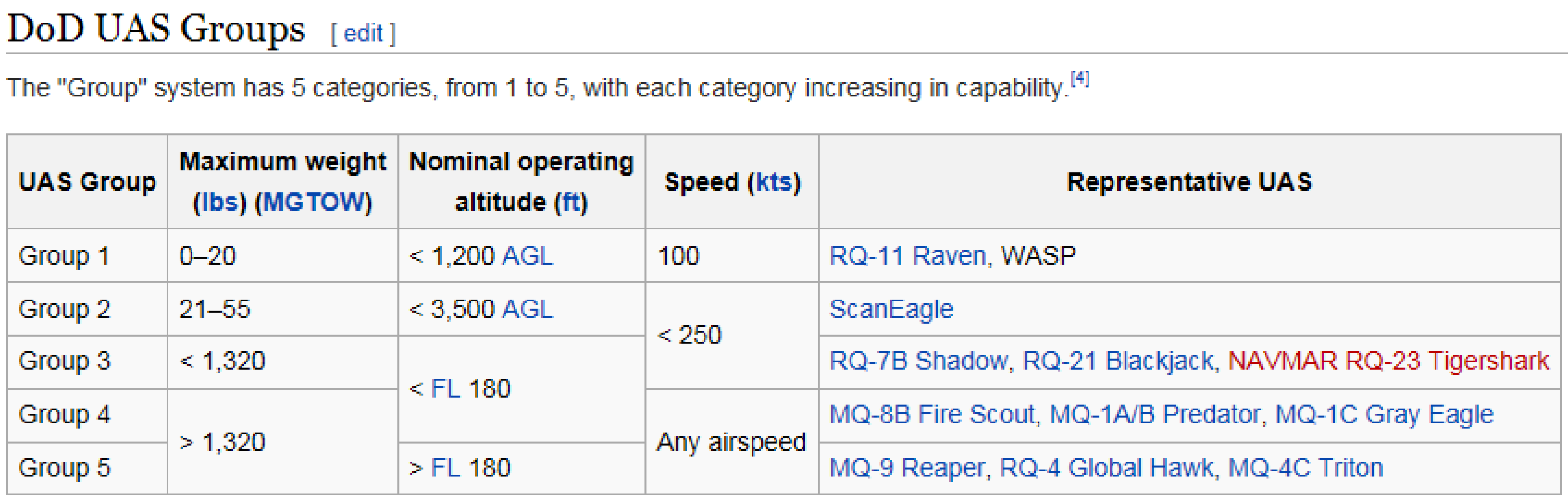
Total Testing hours: 88

Lessons Learned

- Need airspace situational awareness
- No immediate CUAS solution – will require more technology development
- Policy is struggling to keep up with the pace of UAS technologies
- UAS and CUAS research is a long-term commitment
- Need to create a consistent and repeatable test approach to understand the capabilities and limitations of UAS and CUAS technologies
- Need to recommend and seek partnerships with multiple stakeholders to leverage resources and lessons learned in the pursuit of a solution

Questions?

BACKUP SLIDES



DoD UAS Groups [edit]

The "Group" system has 5 categories, from 1 to 5, with each category increasing in capability.[4]

UAS Group	Maximum weight (lbs) (MGTOW)	Nominal operating altitude (ft)	Speed (kts)	Representative UAS
Group 1	0–20	< 1,200 AGL	100	RQ-11 Raven, WASP
Group 2	21–55	< 3,500 AGL	< 250	ScanEagle
Group 3	< 1,320	< FL 180		RQ-7B Shadow, RQ-21 Blackjack, NAVMAR RQ-23 Tigershark
Group 4	> 1,320		Any airspeed	MQ-8B Fire Scout, MQ-1A/B Predator, MQ-1C Gray Eagle
Group 5		> FL 180		MQ-9 Reaper, RQ-4 Global Hawk, MQ-4C Triton