Ports of Entry - UAS Risk Assessment Guideline

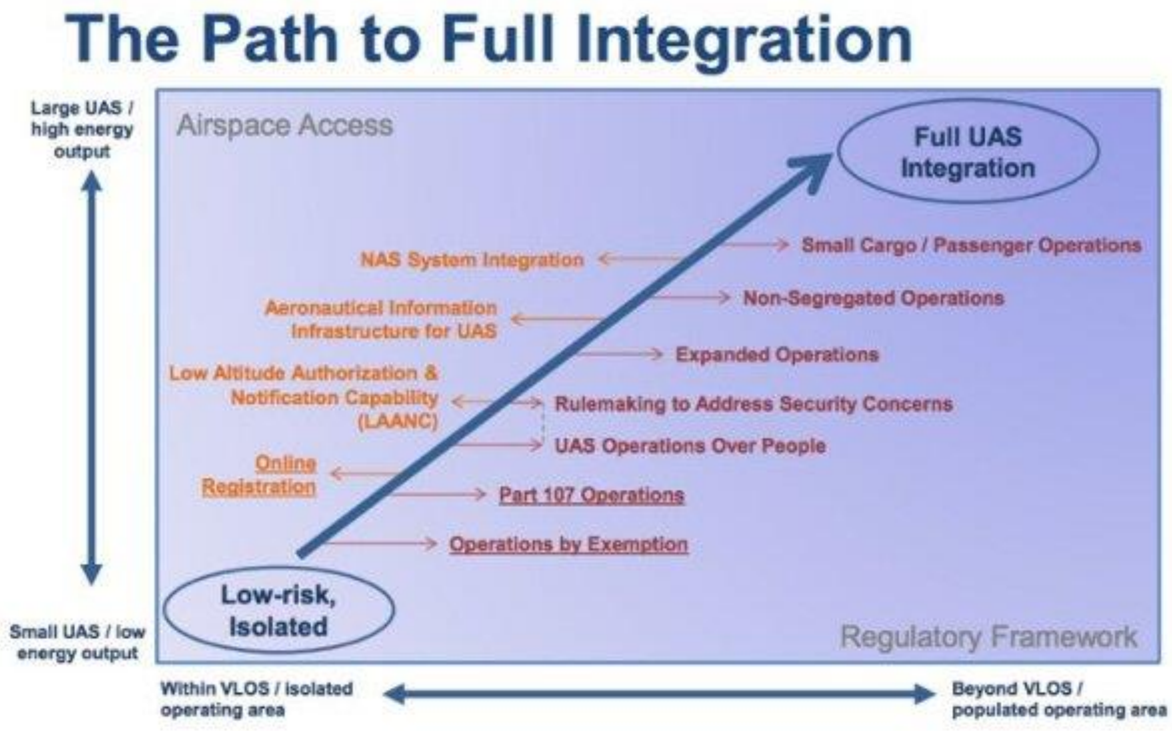
Airports and marine ports are vital components to the U.S. economy, these ports of entry control the flow of goods and people, support millions of jobs, and contribute to economic growth.

In 2014, civil aviation accounted for 5.1 percent of U.S. gross domestic product (GDP), and generated $1.6 trillion and supported 10.6 million jobs. In 2014, marine cargo activity generated around $4.6 trillion of total economic activity, or about 26% of the nation’s GDP.

Air, sea, and river ports make a huge contribution to the US economy by facilitating trade and tourism, providing jobs, and supplementing the energy need. Seaports are arguably the most critical nodes in the global supply-chain and hence have a central role in business continuity.

With the volume of people and products going through these ports, an attack would be disastrous on a global scale. The high level of economic impact makes airports and seaports attractive targets for terrorist. Aging facilities and security gaps leave ports of entry vulnerable to the very real threat of terrorist attacks.

FAA Path to UAS Integration


The Path to Full Integration
Large UAS / high energy output
Small UAS / low energy output
Airspace Access
Full UAS Integration
Small Cargo / Passenger Operations
NAS System Integration
Non-Segregated Operations
Aeronautical Information Infrastructure for UAS
Expanded Operations
Low Altitude Authorization & Notification Capability (LAANC)
Rulemaking to Address Security Concerns
UAS Operations Over People
Online Registration
Part 107 Operations
Operations by Exemption
Low-risk, Isolated
Regulatory Framework
Within VLOS / isolated operating area
Beyond VLOS / populated operating area

Resource: FAA Unmanned Aircraft Systems (UAS) Update (p. 9)

The FAA is attempting to establish an appropriate balance in their regulatory approach that will achieve safety objectives while imposing the least burden on society.

The nationwide expansion of the LAANC program is set to begin April 30, 2018. The digital authorizations will be rolled out to nearly 300 air traffic control facilities representing approximately 500 airports across the United States, opening up to 78,000 miles of airspace for commercial drone operations.

Police departments and other agencies are adding drones to their standard equipment. In the past year, there has been a steady increase in drones being used successfully in search and rescue and in other life-saving situations. Beyond Visual Line-of-Sight (BVLOS) drone operations are being tested and used in commercial operations.

The FAA approved first responders at the fourth busiest airport in the world, Dallas/Fort Worth International Airport to fly their drones directly over the airfield. DFW Airport will be the first airport in the US that is allowed to do so.

Current Drone Laws

Federal

FAA Drone/Airport Guidelines

It is a popular misconception that recreational drone pilots are not allowed to fly within 5 miles of an airport. The FAA states that recreational drone pilots wishing to fly within 5 miles of an airport must give notice to two entities prior to flight:

1. The Airport Operator/Manager AND
2. Air Traffic Control (if the airport has an air traffic control tower)

However, recreational operations are not permitted in Class B airspace around most major airports without specific air traffic permission and coordination.

States

Currently, ten states have enacted specific laws that prohibit the flying of drones near or over critical facilities or infrastructure. These states include Arkansas, Arizona, Delaware, Florida, Louisiana, Nevada, Oklahoma, Oregon, Tennessee, and Texas. A few of these states specifically define critical infrastructures to include ports. Delaware, Oklahoma, Tennessee, and Texas specifically include “port” in their definition of a critical infrastructure.

Many drone owners are uninformed about the laws and regulations, and drone operators seeking to do harm will disregard regulations and laws altogether.

1. Identify UAS Risk

The first step in preparing a UAS risk management plan is to identify the risks drones pose to your facility. Understanding the scope of possible risks and threats will help you develop realistic, cost-effective strategies for dealing with them.

Ways to identify UAS risks to your organization:

Consider these kinds of questions: “why?”, “what?”,” when?”, “where?”, “how?”

- Why would my port be threatened by a drone?
- What would happen if a drone hacked my port?
- When will this happen, could it happen again?
- Where are my security gaps that would allow such an attack?
- How could my facility be impacted by drones?

Brainstorm with different departments to gather a comprehensive view of drone risks, drone incidents will impact different areas of your organization. Discuss the types of questions above in your brainstorming session. For instance consider the following - Will a drone cyber attack: disrupt your daily business activities? cause a PR nightmare? lead to financial losses?

Use these questions to think about event-based scenarios that could happen to your airport or marine port. Then think about how these events would impact your organization. Risk identification involves establishing three key concerns: sources of risk, areas of impact, and consequences.

Sources of Risk

The Department of Homeland Security (DHS) Risk Lexicon, defines a threat as "a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property." Drone threats are a risk that airports, helipads, and marine ports face, and left untreated these hazards pose problems on various levels.

The risks associated with drones are mainly external. External drone threats to critical facilities could originate from unintentional or targeted sources.

1. Unintentional: Negligent/Errant Drone Pilot
2. Targeted: Domestic/International Terrorist, Hacker, Nefarious Actor/”Lone wolf”

Areas of Impact

Both airports and marine ports have many areas of impact to consider when identifying risks. Areas of impact to consider include: human life, operations, service delivery, financial, legal concerns, and brand/reputation.

Consequences

Brainstorm with a team, include various levels of employees that work in the different areas of impact. Think about all consequences - ranging from a mild inconvenience to a worst-case scenario.

Security experts have warned that drones could be used by terrorists to surveil or assist in carrying out an attack on critical facilities, such as ports of entry. These facilities include marine ports and airports. The FBI and DHS have warned about attacks on the nation’s critical infrastructures. Late 2017, agencies released a joint statement, warning about recurring cyber attacks to critical infrastructures and their partners.

Could a drone be used to attack my port or airport?

International or homegrown terrorists could adapt and refine the tactics they use in conflict zones like portable unmanned aerial systems or drones with explosives to attack key facilities, the ability to attach an improvised explosive device (IED) to a drone has already been demonstrated by terrorists.

In November of 2017, Homeland Security released an updated terror bulletin that highlights the threat of weaponized drones, chemical attacks, and the continued targeting of commercial planes.

Port security is one of the underpinnings of the US economy and a terrorist attack may deliver a serious blow to supply-chain operations and continuity of business. About 90 percent of the world's goods are shipped on the ocean and enter through ports. Any attack that slows or halts operation has the potential to significantly impact the global economy. Some of the goods shipped are time sensitive, such as medicines and perishable foods, disruptions to the supply chain have a domino effect disrupting businesses and daily lives.

Resources:
Youtube: FBI director discusses threats of terrorist drones
Entire committee hearing: Threats to the Homeland Committee Hearing Video
U.S. Defense Intelligence Agency: WORLDWIDE THREAT ASSESSMENT (page 32)

What would happen if a drone was used in a cyber attack against my port?
Ports across the globe have been experiencing cyber attacks. Last year, Maersk was the victim of a large global cyber attack. 17 of Maersk's shipping container terminals worldwide were hacked and the company had to deliberately shut down a number of its IT systems.

One of those ports was the Port of Los Angeles, which resulted in its largest terminal being shut down for three days. Maersk estimates that the attack cost it between $200 million to $300 million, and disrupted operation for two weeks.

Resource:
L.A. Times

What would happen if a drone struck an airliner?

The Alliance for System Safety of UAS through Research Excellence (ASSURE) researched what happens when a sUAS collides with and an airplane.

The research team evaluated the potential impacts of a 2.7-lb. quadcopter and 4 lb. quadcopter; and a 4-lb. and 8-lb. fixed wing drone on a single-aisle commercial transport jet and a business jet.

ASSURE conducted its research with two different types of drones on two types of aircraft through computer modeling and physical validation testing.

Researchers determined the areas of manned aircraft most likely to be impacted:

- the leading edges of wings
- vertical and horizontal stabilizers
- Windscreens

Researchers also concluded that a high-speed collision with a drone would leave an airliner with more structural damage than if a bird of similar weight struck the plane. The structural damage severity levels ranged from no damage to failure of the primary structure and penetration of the drone into the airframe.

There has been an increase of drone sightings near airports, and an increase of near-collisions between airplanes and drones. Unauthorized drones flying near airports can put aircrafts, pilots, and passengers in danger.

Resources:
ASSURE: ASSURE report
FAA: FAA ASSURE Release, Drone Sightings

Risk cannot be eliminated entirely from the environment, but with careful planning, it can be managed and reduced. When identifying the risk, it is a good idea to examine facility vulnerabilities and security gaps.

2. Analyze the Level of Risk

The next step is to identify the level of risk. The level of risk can best be understood as the probability of the event occurring and the product of the consequence of an event: Risk = Probability x Consequence.

Level of Risk = Probability x Consequence

The assessment of probability and consequence is somewhat subjective but subjectivity can be lessened by using data or facts collected from a range of available internal and external information.

Probability

When determining the likelihood of an event or risk, it can seem hard to have a precise frequency. For instance, you may want to determine the frequency of drones operating near or above your facility. First, you can ask employees of all levels to report drone sighting and keep records of the events. These records may not give you an exact number but can indicate if there is a problem, or if it's a growing concern.

Another way to determine the frequency of drone sightings is to monitor drones with drone detection technology. Reputable companies will allow you to try out or rent drone detection equipment for a trial period (30-day or 60-day trial), this will give the most accurate numbers to analyze the actual probability. Accurate probability will help you evaluate the priority of the risk and how it should fit in your overall security plan.

Probability Scale

Level	Probability	Description
4	Very likely (frequent)	Has occurred 2-3 times in the past year
3	Likely (probable)	Occurred more than 4-5 times over 5 years in this organization or in other similar organizations; is known to have occurred in the past year
2	Unlikely (uncommon)	Has occurred 2 or 3 times over 10 years in this organization or similar organizations
1	Very unlikely (rare)	Has never happened in this industry

Consequence

Consequences will range from marginal (slight inconveniences) to major (catastrophes). Determine how the events will impact different areas of your organization: daily operations, information and technology, financial, marketing and PR, human/public/national safety.

Consequence Scale

		Areas of Impact		
Level	**Consequence**	**Operations**	**Financial**	**Human/Safety**
4	Severe	Complete shutdown of operation; halt core operations;	Severe financial loss; Significant budget overrun with no capacity to adjust existing budget/resources	Death(s)/compromises to national security
3	High	Shutdown of key operations; service delays	Major financial loss; Requires significant adjustment to budgets	Severe injuries, sickness. Compromises public safety
2	Moderate	Reduced performance may result in minor revenue loss; Organization existence is not threatened	Significant financial loss; Impact may be reduced by reallocating resources	Minor injuries, non life-threatening compromise to public
1	Low	No impact to daily operations, Minimal impact on non-core operations.	Minor financial loss; Unlikely to impact budget or business activities	Little actual impact to public or national security; no injuries

Note: Ratings may vary for different types of facilities. The scales above use 4 different levels; however, the number of levels can be adjusted to meet the organization’s need. Also use descriptors that suit your purpose (e.g. you might measure consequences in terms of human health, dollar value, data loss, time loss).

3. Determine Risk Mitigation

Once the level of risk is established, analyze the risk and identify solutions. Risk mitigation involves determining what the acceptable and unacceptable risk levels are for your facility. It also involves identifying solutions or ways to treat the risks. Unacceptable risks range in severity; some risks will require immediate solutions while others can be monitored and treated later.

For example, you may decide the probability of a terrorist using a drone to attack a port is 'unlikely' (a score of 2) and the consequences are 'severe'' (a score of 4). Using the tables and formula above, a 'terrorist drone attack on port' has a risk rating of 8 (i.e. 2 x 4 = 8).

Risk Rating Table

Risk rating	Description	Action
12-16	Severe	Needs immediate corrective action
8-12	High	Needs corrective action within 1 month; monitor risk and re-evaluate at a later date
4-8	Moderate	Needs corrective action within 3 months; monitor risk and re-evaluate at a later date
1-4	Low	Does not currently require corrective action; monitor risk

4. Risk Management Strategies

Risks can be managed by one of four distinct methods: risk acceptance, risk avoidance, risk control (or reduction), and risk transfer (deflection).

	Definition
Risk Acceptance	An explicit or implicit decision not to take an action that would affect a particular risk.
Risk Avoidance	A strategy or measure which effectively removes the exposure of an organization to a risk.
Risk Control (or reduction)	Deliberate actions taken to reduce a risk's potential for harm or maintain the risk at an acceptable level.
Risk Transfer (or deflection)	Shifting some or all of the risk to another entity, asset, system, network, or geographic areas.

Source: Homeland Security: Risk Management Fundamentals (page 23)

It is up to owners and stakeholders to determine what risk level is acceptable and unacceptable. Severe risks that cause a high degree of loss and occur frequently should be avoided at all costs. Minor risks with a low degree of loss may be acceptable. Not all the risk strategies can be implemented easily, discuss the best course of actions for your organization with your security team.

Risk Acceptance

Accept all risk of the event and consequences that come with the event occurring. Regarding drone risk, you accept the risks of a cyber or physical drone attack and the impacts it comes with, which could be loss of life, financial, economic disruptions, and legal liability.

Risk Avoidance

How might you remove your facility from exposure to a drone? It is almost impossible to remove a building or facility with outside exposure from aerial threats completely. One method of avoidance for an airport would be to ground flights, reroute aircrafts, or delay landings when a drone is sighted.

Risk Control (Reduction)

Facility managers can reduce risk through staff training, preventative maintenance, and development of a risk management plan as the standard operating procedure.
Communicate with all levels of employees the risk, from maintenance workers to high-level managers; everyone needs to be aware of the dangers. If a maintenance worker sees a drone flying near your facility, they need a procedure on who to tell; they need to be able to talk to those in the chain of command to report the incident.

Facility and operations managers can assess the risk, and if they determine it needs a more advanced solution, a drone detection system can integrate into existing security protocols. As stated before, reputable companies will allow you to set up drone detection systems on a trial basis before investing in an expensive system.

Drone threats and risks impact the whole organization not just one team, all teams can allocate or budget money to mitigate the costs. This will control the risk while reducing the financial burdens.

Risk Transfer (Deflection)

Sometimes managers will want to transfer the risk to someone else who is willing to assume the risk. Insurance is the most applicable way to transfer risk.

Risk management is an ongoing process. Whether you take action now or choose to monitor the situation for an extended period, decision makers must re-evaluate threats, vulnerabilities, or potential consequences on a continuous basis. With rapidly changing technology and new exploits, critical facilities such as marine ports and airports, must prepare to reduce security gaps and evolve their physical security standards.