

WHITE PAPER

GENERAL AVIATION FLIGHT LINE AWARENESS AND SECURITY (GAFLAS)

ABSTRACT

General Aviation Flight Line awareness and Security (GAFLAS) control measures generally consists of perimeter intrusion protection, gated access, limited facility entry and roving airport security rounds. Most non-control towered airfields remain operational after hours, even without airfield personnel on site. In order for successful access to General Aviation airfields individuals could gain access under the following conditions:

- Duplicate an entry key to hangar spaces
- Steal a magnetic entry strip card for vehicle access
- Check in at base operations with a valid ID.
- Walk through base operations to the flight line without checking in.
- Visit a Flight Training School
- Rent an aircraft from the airfield
- Enter via wooded areas or water borders covertly
- Enter as a flight passenger.

Assuming the rationale for clandestine entry is either airfield sabotage or aircraft theft in order to sabotage other locations, a combination of the above entry attempts could easily result in repeated entry, stockpiling explosives on-site (either in an aircraft or hidden elsewhere on the airfield). Sufficient checks of aircraft owners and pilots are being conducted and checked against known domestic/international terrorist watch list personnel. It is likely that aircraft can be commandeered with the intention of using an explosive laden passenger/cargo section combined with aircraft fuel to create the desired terrorist effect. Many airports are extremely close to high value targets without the focused protection provided inside the Washington, DC ADIZ. Even some of those inside the ADIZ can not be adequately protected against a quick strike using close proximity airports. Example: The National Security Agency is less than 1 mile from Tipton airfield. Flight operations security protection within the ADIZ is not really functional until aircraft have taken off and are seen on radar. In the example provided a twin engine GA aircraft can take off, accelerate to 160 knots on a normal departure heading that would not indicate foul play and quickly deviate when well inside one mile from NSA. Within 20 seconds that aircraft could impact NSA while carrying 400 lbs. of fuel, and 800 lbs of explosives. The reactive timeline in this case truly begins when the aircraft first deviates from an expected flight path. This white paper describes a method of backing up the reactive timeline to the when the aircraft first left its ground tie-down position. This white paper proposes a project that provides for aircraft movement detection and tracking of all airfield vehicles at nearly no cost to the operators. This

system would provide warning of unscheduled aircraft movement, alerts to base operators or other off-site personnel. Incremental alert status warning can be provided to differentiate movement in/out of hangers, fueling areas, flight line, taxiways and runways. Expected aircraft movement can be correlated to radio calls, transponder settings, aircraft dependent surveillance broadcast or cell phone ID's such that operators need not experience delays or disruptions in order for the system to function. The implementation for such a process requires the low risk evolution of Radio Frequency Identification (RFID) technology linked to a directional RF interrogator beam.

TECHNICAL APPROACH

Current RFID tags are used to track inventory, shipping and personnel that pass through radio emissions at numerous check points. Stationary, fixed-site, low power emitters provide energy to RF transmitter tags fixed to equipment, inventory or personnel badges. Sufficient RF energy powers the tag allowing it to send back its pre-coded numerical identifier. This number is received at the emitter station and fed to a computer for appropriate processing based up the desired tracking strategy. Entire warehouse inventories can be monitored in this way. The tags are adhered to surfaces such that attempts to remove the tag render it inoperative. Items that pass through any chokepoint (doorway) must either have a RFID tag matching a known data base, or an alert is provided to appropriate personnel. GA airport security can be enhanced significantly if this approach is adjusted for ground based airplane movement tracking.

In the case of industrial parts monitoring choke points include a RF emitter with a low power transmitter providing a beam sufficient to cover the physical dimensions of the choke point. Any part moved through this choke point will be energized and send back its RF part code. For airports the RFID tag can remain essentially the same. Tags can be installed on aircraft in out of the way locations. In fact, multiple tags can be placed on any aircraft all with the same code. Tags placed along a skin seam, inside a fairing or even in plain view could not be removed without disabling the tag. This could ensure aircraft parts containing the tag could not be removed and replaced with non-tagged equivalents. Because it is difficult to ensure the aircraft passes through checkpoints, the design of the RF emitter must be improved. The focal point of new technology using the RFID process incorporates a directional narrow fan beam emitter with sufficient power to cover flight line distances. A series of two or three emitters would constantly rotate their narrow directional beam across the flight line, ramp and runway areas. As the beam passes over the RFID tags mounted on the aircraft their code is returned to the emitter site. By comparing the angular position of the returned specific codes from more than one emitter site each aircraft can be located via triangulation. A map of all aircraft locations is renewed on each subsequent revolution of the emitter beam. If an aircraft moves it new location is reported and compared to an airfield survey map. As a result any aircraft movement can be determined and compared to a historical (previous) location. Even airport support vehicles and airport personnel can be located and tracked in real time.

As this system requires a compliant host carrying the RFID tag there exists the potential to successfully disable all RF tags (both hidden and overt). If that could be done successfully, the RF system would not register the aircraft during its emitter sweeps. Airfield personnel would be alerted to this status as well as the only reason an aircraft would fall out of the identification process is when it departs the airfield or is placed inside the hangar (which could have a chokepoint emitter as well). The loss of aircraft RFID becomes an additional alert precluding deception. Fly-in aircraft could have an RFID tag installed by base operations personnel upon arrival. Aircraft servicing could be denied until a successful RFID interrogation was recorded. This activity involves no more than attaching a thin adhesive strip to the aircraft (1/16th inches thick).

As this system is linked to a computer application, interrogation results can be made available to alternate sources. An off site airport employee carrying a PDA could view errant activity. For example, Secret Service personnel would view all College Park aircraft movement in real time with awareness of specific aircraft / pilots. By linking the RFID code of the pilot's ID tag to that of the airplane(s) flown by the pilot, the system would highlight suspicious RFID tag links moving together. As this system is RF based the effects of extreme weather conditions are anticipated to be minimal. RFID emitter power requirements are somewhat dependent upon each emitter's designed coverage range. Many rotating (electronically scanned or mechanically rotated) emitter antennas linked together allow for lower transmitting power. Coverage of extended areas with only a few antenna emitters requires an increase in power output. Compliance with FCC regulations and documentation of EMI effects on airfield systems would need to be conducted.

The focus of this program requires very little RFID tag modifications and a dedicated design, construction and testing of the swept antenna beam emitter system. RFID tags currently cost less than \$0.25 each. The emitter antenna component would require an encoder to determine antenna pointing azimuth, a narrow azimuth wide elevation beam antenna, power conditioning, processing and miscellaneous hardware. It may be possible to install emitters with wireless data exchange links. If so, only power would need to be supplied at the emitter sites.

SUMMARY

Early recognition of suspicious airfield activity can begin well before pilot, crew and passengers depart the airfield. Event monitoring and alerting does not need to adversely impact the General Aviation user. GAFLAS can be provided to expedite arrival and departure processes with increased protection that may even provide for a decrease in aircraft insurance premiums resulting from the increase in theft protection. By using GAFLAS airport managers, security managers, servicing personnel, flight schools, aircraft charters all are provided with valuable airfield situational awareness that also increases the facility's security posture. General aviation security processes depend upon increasing the preventative capabilities that airports provide. GAFLAS increases the time available to employ countermeasures and is likely to provide an expanded set of additional counter measures and control measures exceeding those current incorporated.