DETECTION, RECOGNITION AND COUNTER MEASURES AGAINST UNWANTED UAVS

Igor Tchouchenkov, Florian Segor, Matthias Kollmann, Rainer Schönbein[1]
Thomas Bierhoff[2] and Mark Herbold[3]

[1]*{igor.tchouchenkov, florian.segor, matthias.kollmann, rainer.schoenbein}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, SystemTechnologies and Image Exploitation (IOSB),
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *thomas.bierhoff@atos.net*
Atos IT Solutions and Services, Heinz-Nixdorf-Ring 1, 33102 Paderborn (Germany)

[3]*mark.herbold@atos.net*
Atos Nederland B.V, Papendorpseweg 93, 3528 BJ Utrecht (Netherlands)

Abstract

Small Unmanned Aerial Vehicles (UAVs) are getting better, cheaper and more accessible. As a result, they become more and more used in new areas of application. A side effect of this development an increasing number of more or less hazardous incidents with these systems can be noticed. Not only illegal activities as spying and drug transportation, but also disturbance or even simple mishaps which can happen with any technical system can lead to dangerous situations.

In this paper a concept of new Low Altitude Air Surveillance Control (LASC) system is described, which can be utilized to keep urban air space controlled and safe.

The LASC concept is based on multi-sensor detection, localization, tracking and classification or identification of small UAVs integrated in a scalable system providing interactive threat and risk assessment as well as selection possibilities for adequate counter measures.

Keywords: UAV, air, surveillance, counter measure, multi-sensor, distributed system.

1 SITUATIONAL OVERVIEW AND PRESENT PROBLEMS

Unmanned aerial vehicles are an emerging technology with a great potential to disruptively change our lives. They have by far exceed the capabilities of the niche products of radio controlled aircraft models with their ability in terms of payloads, flight duration and range, self-stabilizing and auto pilot capabilities, automated collision protection and video transmission capabilities. Leveraged with new technologies (e. g. high capacity battery packs, low energy consuming motors, diverse sensors and matchbox sized high computing power) small UAVs have started exceeding the toy and entertainment domain while entering more and more real business and scientific applications (e. g. surveillance, reconnaissance and rescue mission support, video production, logistics and delivery, biology, archaeology, etc.) [1], [2], [3]. This development has in parallel been boosted by a constantly rising commercial market for UAVs providing broad accessibility and diversity at a low cost scale.

Furthermore, with the broad availability and low cost aspect of UAVs, a common and unforeseeable use of this technology is expected in the private sector.

As always, each technology comes along with drawbacks and potential for abuse and this is in particular true for UAVs. With their inherent risk of crashing, causing damage and harm to people, each application has to be assessed seriously in terms of security issues and constraints.

This will in turn demand for new laws, rules and enforcement technologies [4], [5] to keep the low altitude air space controlled and safe. To enforce regulations and timely and efficiently react to violations and emerging security risks, new technologies are required to detect and interfere with these systems.

To find efficient solutions and to provide a future-proof holistic system design a joint project between AToS SE and Fraunhofer IOSB has been set up and the concept for a Low Altitude Air Surveillance Control (LASC) system for control of small UAVs has been developed using multi-sensorial data utilization and background knowledge to assess and evaluate risks and provide situation dependent adequate counter measures.

2 ONGOING RESEARCH AND POSSIBLE SOLUTIONS

A boost of interest for solutions to detect and interfere with small aircrafts has originated from the increase in dangerous or unlawful UAV activities that could be observed recently. On the one hand it concerns the research and development of new sensor concepts which generally admit the detection and location of such systems as far as their payload and, on the other hand, also the search for suitable counter measures because small aircraft cannot be efficiently countered with conventional (e.g. military) systems not only in urban areas, but also in most other cases.

2.1 Detection of small UAVs

A simple but efficient detection and identification technology would be a standardized IFF system deployed in all UAVs. A transponder integrated into the electronics of the UAV collects the current GPS position, altitude, heading, speed and broadcasts the information periodically (or on demand) together with a unique identification number on a specific radio channel. But the standard IFF system is not usable on small UAVs.

Video based airspace surveillance is a promising approach but it comes with challenging requirements – especially for urban areas. The air space must be observed in all directions mostly without any fixed point and working distance to detect a small UAV in a video feed. Existing commercial systems use mostly easy change detection [6] and can often generate false alarms. Fraunhofer IOSB has done comprehensive research on robust computer vision algorithms allowing the detection and primary classification of different flying objects within the range of the sensor in real time [7].

Air space surveillance solutions are available within the visible spectrum of light as well as the infrared spectrum range, allowing the tracking by heat emissions with less sensitivity to weather conditions and poor visibilities.

Sound pattern emitted by UAVs are also representing a promising supplementary source for detection and even classification. Engines and rotors of UAVs are producing characteristic sound emissions, which can be caught by directional microphones [6]. Deploying digital signal processing with matched digital filters adjusted to the characteristic sound frequency spectrum, a UAV sound signal can be unveiled. Its direction is given by the alignment of the directional microphone and can be supported by distance estimation by the signal strength or triangulation. By this, the location of a potential UAV can be determined and based on level of compliance with the characteristic sound spectrum, a UAV classification can be sometimes provided, but the payload cannot be analyzed on this way.

Radar technology is always tailored to its application scene (e.g. detection range, size of object, material, etc.). It shows the advantage of being insensitive to environmental conditions (poor visibility, no light at nighttime, rain, fog, etc.) which makes it applicable in almost any environmental situation. Long range air surveillance radar operating at 1 to 2GHz (L-Band) for long range (<400km) and large objects (>10m) are not suitable for the LASC system as UAV's small size, its low EM-wave reflecting composite material and low flying altitudes are not providing sufficient radar cross sections to get detectable reflection signals.

More suitable radar technologies are found in the K- and Ka-Band operating with frequencies between 20 and 40 GHz as far as in the W-Band between 60 to 120 GHz. But the detection and recognition of small UAVs with radar are still a topic of research. Applied in urban areas, reflection by infrastructures and building are representing the major challenge for development of appropriate radar surveillance sensor systems.

Passive electromagnetic radiation based detection procedures for UAV are promisingly and partially already in application [8]. The Achilles' verse of every remote controlled UAV is its up-/downlink to the ground control station. Control commands are sent with specific communication technologies from there to the UAV and sensor data like position, system state and in particular video signals are sent back. If the typical frequency bands are scanned, characteristic communication can be identified showing transmission activities with reasonable signal strength. Based on the detected radio transmissions, a rough identification of the drone's type can be retrieved. In conjunction with triangulation capabilities of a cooperating sensor network, the position and heading of a UAV can be determined as well.

If no continuous control- and signal transmission is used as the UAV is autonomously following a preprogrammed GPS or image based flight path, the detection of control- and sensor signals will most likely fail. In this case, more sophisticated technologies needs to be applied to detect electromagnetic background radiation of the UAV emitted by its electronic equipment.

2.2 Counter measures against small UAVs

Possible counter measures against small UAVs can be divided into two categories: "soft" and "hard" measures.

Possible "soft" measures include first of all jamming of remote control link and GPS spoofing. There are already first counter-UAV systems using jamming [9]. The problem of these measures is that the behavior of diverse UAVs can be very different. By jamming some UAVs try to fly near to their start position, but other UAVs can land immediately. Without knowing the behavior, jamming can bring even more problems as a flying unwanted UAV itself – for example if the UAV lands on an unsuitable place or if other important communication systems are unavailable because of the jamming.

GPS spoofing is often efficient [10], but it can be overtaken by remote control of UAV, and fast shifting of GPS position can also force UAV to immediately landing. Afterwards, the spoofing can disturb other important systems, so that it should be used with directed antennas only.

More efficient, but also much more challenging solution is a control overtaking. By success, the UAV of interest can be landed on suitable place. For some WIFI controlled UAV there are usable solutions [11]. Unfortunately, most UAV don't use usual WIFI, and there are a lot of remote control types. By digital control links UAV and remote control unit are matched while configuration, so the hacking is very challenging.

"Hard" interception technologies are based on physical touchdown enforcement with different physical effects and levels of collateral endangerment [12]. These technologies are representing the "last line" of defense and shall only be deployed if any other defense line has failed and collateral damages impacts are evaluated definitively less than the threat itself (explosive or chemical payload).

3 LOW ALTITUDE AIR SURVEILLANCE AND CONTROL CONCEPT

The major functional objective of a LASC system is the surveillance of the today uncontrolled air space below ca. 500m within urban areas. The space beyond the 500m is already been in control by conventional air traffic control mostly based on long-range radar technologies. In order to guarantee seamless information exchange (e.g. some UAVs may enter the high altitude air space and endanger the air traffic), LASC system must be integrated into conventional air traffic control.

The common workflow of LASC is depicted in Figure 1. The LASC system starts with a continuous monitoring of the air space with multiple sensors. Once a sensor detects a flying object, the system will try to locate it (e.g. by triangulation of sensor signals) and ensure tracking by orchestrating multiple sensors. Once the location and tracking is established, the back end IT system of LASC needs to carry out the classification and if applicable the identification of the detected object. Once this is executed, the LASC backend system starts the evaluation of the drone’s authorization to fly through the current air space corridor. If no authorization is given, system will prepare reaction options considering the estimated threat classification and risk assessment (disturbing, illegal or endangering). The system provides decision support to a human operator who is in charge of initiating the counter measures. All this activities will be automated to a high degree in order to guarantee a real time execution of the process and to enable high scalability in terms of multiple events.

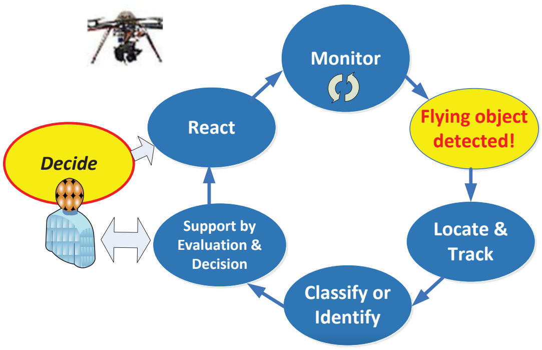

Figure 1: Common workflow of the LASC system

3.1 Flight Activity Monitoring

Distributed LASC system can contain both mobile and stationary LASC sub-systems to monitor flight operations in the low altitude air space (<500m) within a pre-defined area (10m-5km). Depending on the application scheme, the area of the air surveillance is scalable by adding further sensor- and counter measure devices to the LASC systems or new sub-systems. This modular approach will provide a broad field of application ranging from a single building to an entire suburb air surveillance, turning LASC into a flexible and highly adaptable solution. Monitoring flight operations covers detection, identification and tracking. Therefore, a multimodal sensor network based on the technology stack recapitalized in chapter 2.1, must cover a certain part of the controlled air space providing day- and night time operations and coping with bad visibility conditions. The next step after UAV detection is its identification based on sensor signal evaluation or by IFF signals broadcasted by the UAV. Once identified, the LASC system needs to reconcile the information with a LASC based central UAV flight register to see if the UAV’s flight is already registered and further information is given covering payload, mission, flight path, destination and operator. If the UAV is registered, its flight register record must be updated by time stamp, current position, altitude and speed for consistent tracking. If there is no suitable UAV record found in the LASC registration, a new one must be created with all available information (e.g. time stamp, current position, altitude and speed). In order to approve UAV flight authorization, its position needs to be mapped to pre-defined air space corridors, which will show permanent or temporarily valid restrictions or prohibitions. This is essential as different UAVs may have different air space transit rights (e.g. police drone may enter the corridor while an unregistered one may not). The last step of monitoring flight operations is represented by continuous tracking and updating the LASC register's records. Once a UAV is leaving the observation windows of a sensor or a LASC system, it might enter another one. The hand-over of such tracking must be supported by a LASC intelligence, which provides analysing and predictions of flight path and identification of potential sensors, which might detect the UAV soon.

3.2 Air Space Regulation Enforcement

The second objective of the LASC system is the downstream air space regulation enforcement for unauthorized UAV. Therefore, the violation of the air space must be unveiled, which must trigger a threat and risk analysis to determine appropriate reaction and counter measures possibilities. Based on the classification of risks and the availability of interception capabilities in reach, a decision support must provide human operators with suitable enforcement and interception solutions. As the interception is always related to potential collateral risks, it always needs to be initiated, monitored and controlled by a human operator. Therefore, the operator needs access to the sensor network (e.g. video/IR camera) of the LASC system to leverage assessment of the situation and to gain a reliable decision base. Furthermore, he needs GIS support for geo-referenced situational awareness (e.g. show locations of and distances to critical infrastructures in reach). All this needs to be integrated into the command and control center of the LASC system.

The major challenge of the LASC interception operation is the avoidance of collateral damage. Military interception solutions for low-altitude flying objects (e.g. shells or rocket defence systems) are not acceptable in urban areas. The new ways of soft interception techniques as introduced in chapter 2.2 need to be researched and integrated into the LASC solution. Another challenge is the ability of UAVs to takeoff almost everywhere. In case of an abuse, the UAV might take off near its destination reducing reaction time drastically down to seconds. Therefore, most LASC system functionalities must be automated by computer-based support, delivering alerts and decision support to the operator within seconds.

3.3 LASC System Design

The general system design and major building blocks for a full-blown LASC system providing comprehensive monitoring, intelligence and interception functionalities are depicted in Figure 2. Subsequently the functions of the building blocks and their interaction are introduced in order to provide a general picture about the LASC architecture and its mode of operation.

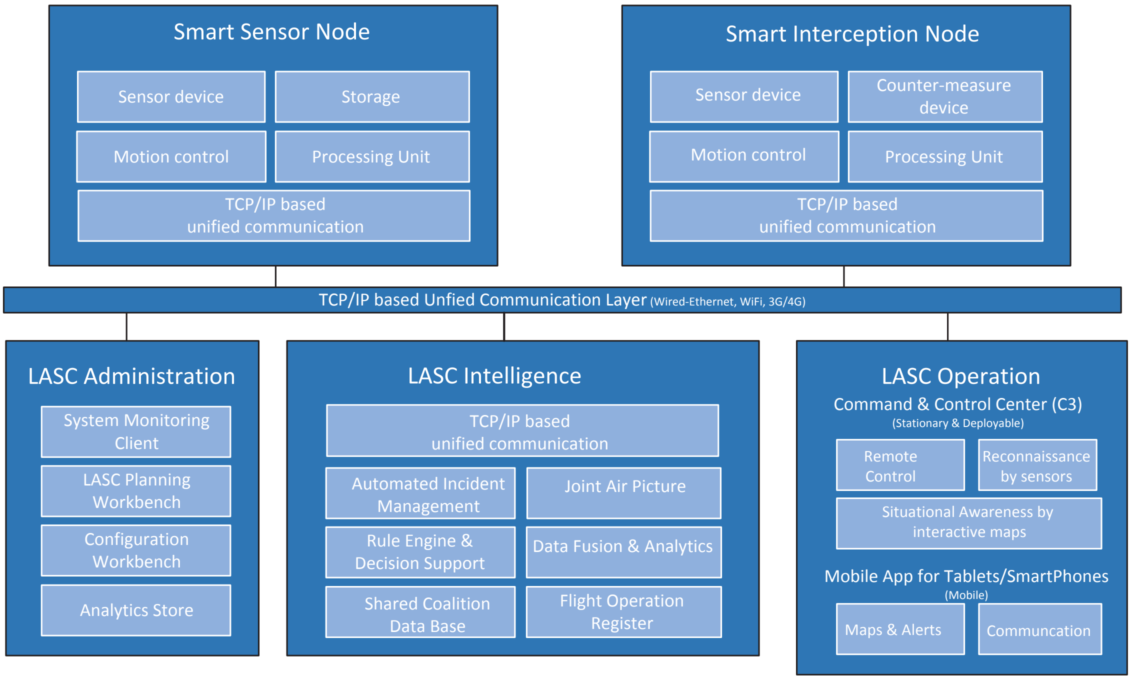
Smart Sensor Node
Sensor device
Storage
Motion control
Processing Unit
TCP/IP based unified communication
Smart Interception Node
Sensor device
Counter-measure device
Motion control
Processing Unit
TCP/IP based unified communication
TCP/IP based Unfied Communication Layer (Wired-Ethernet, WiFi, 3G/4G)
LASC Administration
System Monitoring Client
LASC Planning Workbench
Configuration Workbench
Analytics Store
LASC Intelligence
TCP/IP based unified communication
Automated Incident Management
Joint Air Picture
Rule Engine & Decision Support
Data Fusion & Analytics
Shared Coalition Data Base
Flight Operation Register
LASC Operation
Command & Control Center (C3)
(Stationary & Deployable)
Remote Control
Reconnaissance by sensors
Situational Awareness by interactive maps
Mobile App for Tablets/SmartPhones
(Mobile)
Maps & Alerts
Communcation

Figure 2: System concept with major building blocks

A field device of the LASC system covers the distributed network of smart sensor and interception nodes. The appropriate choice of the technology is strongly depending on the application and the environmental constraints (free space and the line of sight above roof tops, or covered and thus with a limited line of sight within urban canyons). So deploying various sensors and interception technologies in a multimodal approach must be considered because different technologies are cooperating and extending their capabilities among each other during a parallel operation.

Smart sensor nodes are distributed on appropriate places across the observed area and equipped with data storage and processing units to pre-process sensor raw data using specific algorithms and embedded system technology. This will decrease the data volume to be transmitted into a ground station by far, as only derived smart data in terms of an event needs to be transmitted. The derived information, analyzed data and detected events are provided via web services hosted in the sensor node and end-to-end secured (SSL, VPN) TCP/IP based communication channels. In addition, remote control and diagnose of the sensors is also enabled through the web services.

Smart interception nodes are distributed across the observed area, placed stationary on buildings, infrastructures, balloons or on vehicles (e.g. cars, drones, etc.) to provide deployable interception capabilities. Similar to the sensor nodes also mobile interception nodes can be used. The interception nodes are based on the same subcomponents as the sensor nodes except that the data storage is replaced by a counter measure device. The sensor device, deployed in the interception node, in conjunction with an embedded processing unit will enable automatic interception process preparation and support (e.g. semi-automated aiming and motion control).

Beside the field devices, the LASC system will contain three further major building blocks covering the domains administration, intelligence and operation.

The LASC administration block covers all kind of tools to configure, monitor and maintain the LASC system infrastructure and its components. It comes along with automated system monitoring and observation clients, which enable the survey of the operational state of sensor and interception nodes, allows load balancing of the intelligence platform and even supports the configuration of the intelligence itself (e.g. setup of analytics chains). Another part of the LASC administration is the LASC planning workbench, which provides simulation-based design support for arranging the sensor- and interception node network across a defined area in order to achieve a certain degree of air surveillance performance.

The LASC intelligence is the core block of the entire system. Its major task is the data fusion of streams from the sensor network and appropriate fast data analytics and complex event processing to provide a joint air picture (JAP) of the observed area in real time. The JAP represents the georeferenced description of all detected and tracked UAVs including all restricted and/or prohibited air corridors. Utilizing a shared coalition database and the flight operation register, the LASC tries to identify a detected UAV automatically. If this fails, the LASC intelligence provides all available information (mainly video streams) for manual identification by a human operator using decision support tools. Once an air space violation is unveiled, an automated incident management provides several options for the operator to react appropriately to the incident. This incident manager utilizes a rule engine including pre-defined decision trees, risk assessments and potentially applicable counter measure nodes in reach. Once the LASC intelligence platform is deployed on virtualized server infrastructure, its service-orientated architecture provides the performance to handle tremendous amount of sensors (>1000), process their data in real time and provide all kind of information's to multiple authorized operation.

The last building block presents the operation clients of the LASC system, which can be distinguished into stationary/deployable command and control centers (C3) and mobile apps supporting mobile access to the LASC intelligence information system. It can be developed e.g. based on AMFIS ground control station [13]. All clients are connecting to the LASC intelligence platform via secured end-to-end encrypted (VPN, SSL) TCP/IP based communication channels and utilize its web service provision to access data and control. The C3 clients are based on rich internet or desktop applications that provide interactive maps visualizing the joint air picture to support situational awareness. Once an incident is detected, alerts are shown and the feature icon of the detected incident is highlighted to focus the operator's attention. The operator can request decision support from the LASC intelligence and real time video streams from optical sensors in the reach. All counter measure activities can be initiated and controlled by the C3 client software and are sent via the LASC intelligence control proxy to the selected interception node.

For mobile solutions (e.g. police man equipped with tablet, smartphone) client apps running on smart phones and tablets are provided to inform the operator about incidents in the near environment and/or transmit instruction for further action (e.g. evacuation).

4 CONCLUSION AND FUTURE WORK

The LASC system concept includes multi-sensor detection, localization, tracking and classification or identification of small UAVs integrated in a scalable distributed system. Beneath the detection, the classification of threats and the safe identification and separation of legal UAVs is a challenging task. Not only the current position and the type of a suspicious UAV must be recognized to assess the risk – much more important in these cases is the payload. A selection of suitable "hard" and "soft" counter measures for different situations and threats is based on comprehensive predictive analysis of danger of UAV and its payload. Preferred are "soft" countermeasures like communication based mission distortion and interruption. LASC system provides fast interactive threat and risk assessment as well as selection possibilities for adequate counter measures supported by user-friendly interface.

The scalable architecture of the distributed LASC system has open interfaces wherever it is possible and includes data analysis and fusion modules, coalition shared database as well as interactive visualization and decision support components. The LASC system must be integrated into conventional air traffic control to prevent possible incidents because of intersecting air spaces.

The system concept was developed in a joint project between AToS SE and Fraunhofer IOSB. In the next steps major components of LASC as well as system framework will be developed and tested in different situations.

REFERENCES

[1] Vasagar, J. (2014). *DHL to use 'paracelcopter' drones for delivery.* Finanical Time http://www.ft.com/cms/s/0/c00bd8e2-44ad-11e4-bce8-00144feabdc0.html#axzz3RtVgsK6d

[2] Wikipedia, *Amazon Prime Air* (2013). http://en.wikipedia.org/wiki/Amazon_Prime_Air

[3] Molina, P., Eulalia, M. et. al. (2012). *Drones to the Rescue*. InsideGNSS Journal, pp. 37-47.

[4] Lardinois F. (2015). *FAA proposed rules to open sky to some commercial drones*. TechCrunch. http://techcrunch.com/2015/02/15/proposed-faa-rules-will-open-the-sky-for-some-commercial-drones-but-delivery-drones-remain-grounded/

[5] Federal Aviation Administration (2015). *Overview of small UAS Notice of Proposed Rulemaking.* http://www.faa.gov/regulations_policies/rulemaking/media/021515_suas_summary.pdf

[6] DeDrone (2015). *Multi-Sensor-System zur Erkennung von Drohnen*. http://www.dedrone.com/de/dronetracker/drohnen-alarm-system

[7] Fraunhofer IOSB. *Experimental setup for object recognition and tracking*. http://www.iosb.fraunhofer.de/servlet/is/24431/

[8] DDC LLC (2015). *The Basic Drone Detection System*. http://www.ddcountermeasures.com/products.html

[9] Unmanned System Technology (2015). *New Anti-UAV Defence System Successfully Detects, Tracks, & Disrupts UAVs*. http://www.unmannedsystemstechnology.com/2015/06/new-anti-uav-defence-system-successfully-detects-tracks-disrupts-uavs/

[10] The University of Texas at Austin (2015). *Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV*. http://www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav

[11] Pleban, J.-S., Band, R. and Creutzburg, R. (2014). *Hacking and securing the AR.Drone 2.0 quadcopter - Investigations for improving the security of a toy.* In Proc. SPIE 9030, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications.

[12] Tchouchenkov, I., Segor, F., Schönbein, R. (2012). *Einsatzmöglichkeiten und Abwehr kleiner unbemannter Fluggeräte*. POLIZEI-heute, Nr. 3.

[13] Bürkle, A., Segor, F., Kollmann, M. and Schönbein, R. (2011). *Universal Ground Control Station for Heterogeneous Sensors*. In Journal On Advances in Telecommunications, IARIA, Volume 3, Numbers 3 & 4, pp. 152–161.