Usability Assessment of Drone Technology With Regard to Land Border Security

Stefan Hristozov[1] and Boris Shishkov[2,3]
[1]*Institute of Systems Engineering and Robotics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria*
[2]*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria*
[3]*IICREST, 53 Iv. Susanin Str., 1618 Sofia, Bulgaria*

Keywords: Usability, Drone Technology, Land Border Security.

Abstract: Some years ago, it would have been amazing to see a drone flying and behaving 'on its own', not knowing whether it is distantly navigated by a human or it is somehow autonomic. Currently we observe that: (i) Youngsters can easily buy toy drones and navigate them distantly; (ii) Military drones realize sophisticated operations in dangerous environments. This indicates for impressive advances in the technologies underlying drone developments, and that is all about ICT – Information and Communication Technology: current ICT is often embedded in services and/or devices. It is ICT that brings together hardware, software, and net-ware features, to enable useful solutions in different domains, such as aviation. As it concerns particularly drones, they represent complex devices comprising mechanical and ICT 'components'. Current drones can be piloted remotely. Further, being equipped with video cameras, they can provide fast access to images (and/or real-time videos) from a range of locations. Finally, advanced solar power supplies make it possible for drones to stay up for a very long time. Hence, this all makes current drone technology societally relevant. At the same time, many questions have not yet been answered (even though technology developed) – several of those questions are: Is current drone technology indeed reliable if used in critical (rescue) operations? How is the human navigating a drone responsible for what the drone would do? Who is responsible in the case of autonomic drones? Are current software platforms running on drones powerful enough to cover all possible situations that may pop up in the sky? To answer those and other related questions, it is necessary to 'step in the shoes' of a particular application domain since those issues are domain-specific – an answer concerning one domain is not necessarily valid for another domain. Hence, inspired by another paper in the current proceedings, we focus on land border security. We therefore aim at studying the usability of drone technology, with regard to the mentioned domain. For this reason, we firstly discuss drone technology in general and then we analyze its usability in land border security. This analysis is a contribution of the current position paper and inspiration for further research featuring the development of advanced context-aware drone platforms.

1 INTRODUCTION

Some years ago, it would have been amazing to see a drone flying and behaving 'on its own', not knowing whether it is distantly navigated by a human or it is somehow autonomic. Currently we observe that: (i) Youngsters can easily buy toy drones and navigate them distantly; (ii) Military drones realize sophisticated operations in dangerous environments (IoTDI, 2017). This indicates for impressive advances in the technologies underlying drone developments, and that is all about ICT – Information and Communication Technology: current ICT is often embedded in services and/or devices (AWARENESS, 2008). It is ICT that brings together hardware, software, and net-ware features, to enable useful solutions in different domains, such as aviation. As it concerns particularly drones, they represent complex devices comprising mechanical and ICT 'components'. Current drones can be piloted remotely. Further, being equipped with video cameras, they can provide fast access to images (and/or real-time videos) from a range of locations. Finally, advanced solar power facilities make it possible for drones to stay up for a very long time (Gavrailov, 2014). Hence, this all makes current drone technology societally relevant. At the same time, we argue that many questions have not yet been answered (even though technology has developed) – several of those questions are: Is current drone technology indeed reliable if used in critical (rescue) operations? How is the human navigating a drone responsible for what the drone would do? Who is responsible in the case of autonomic drones? Are current software platforms running on drones powerful enough to cover all possible situations that may pop up in the sky? To answer those and other related questions, it is necessary to 'step in the shoes' of a particular application domain since those issues are domain-specific – an answer concerning one domain is not necessarily valid also for another domain (IoTDI, 2017). Hence, inspired by another paper published in the current proceedings (Shishkov et al., 2017), we focus particularly on land border security (FRONTEX, 2017). We therefore aim at studying the usability of drone technology, with regard to the mentioned domain. For this reason, we firstly discuss drone technology in general and then we analyze its usability in land border security. This represents the contribution of the current position paper and an inspiration for further research featuring the development of advanced context-aware drone platforms.

As for current drones, they are unmanned aircraft often operated distantly (but it is also possible that drones are to some extent autonomic), as mentioned before. Drones come in different sizes and shapes – from microUAVs that can be held in the palm of one's hand to large airships that rival the size of traditional piloted craft (Gavrailov, 2014). As already mentioned, drones are empowered by mechanical, software, hardware, and net-ware components, and are designed to: primarily collect data (in the context of diverse tasks), trigger some actuators, and so on. Depending on their main function, drones can be designed based on different aircraft styles, such as: fixed wing, rotary-wing, tilt-rotor, ducted fan, and so on. Drones may be piloted remotely (as mentioned already) and are often equipped with video cameras.

Drones are partially used in military operations, rescue actions, and so on. Nevertheless, there is insufficient justification to date on the real value and reliability of drone technology, for example, in the area of security (Drent at al., 2014).

For this reason, the usability analysis presented in the current paper, is considered actual.

The remaining of the paper is organized as follows: We firstly introduce and discuss drone technology, taking a black-box perspective towards drones: stressing on the functionality of drones with respect to their environment (Section 2) and then taking a white-box perspective with regard to a drone, analyzing its internal components, processes, and rules (Section 3). Then, in Section 4, we analyze the usability of drone technology especially in land border security, featuring particular relevant strengths of this technology. Finally, we present the conclusions in Section 5.

As for Section 2 and Section 3, they are backed by the following references:

- Adams and Friedland, 2011;
- American Red Cross, 2015;
- Bravo and Leiras, 2015;
- Drent et al., 2014;
- European Emergency Number Association 2015;
- Gavrailov, 2014;
- Guerra and McNerney, 2015;
- ICARUS, 2012;
- Lachar and Maroney, 2012;
- OCHA - UN, 2014;
- SenseFly, 2016;
- Tanzi et al., 2016.

2 DRONE-TECHNOLOGY

In introducing and discussing drone technology, we start from a more abstract view and move to a more concrete view. This we do in order to keep good traceability to concepts, such that comparison with and/or alignment to other technologies is possible.

2.1 Conceptual View

Essentially, drones are devices themselves and in order to be able to function, they need distant command and satellite navigation. Hence, there are interactions: (i) between a ground control station and a drone; (ii) between a drone and a satellite. This points to a conceptual entity-to-entity model featuring collaborations with three types of entities, namely: drone, satellite, and ground control station, as illustrated in Figure 1:

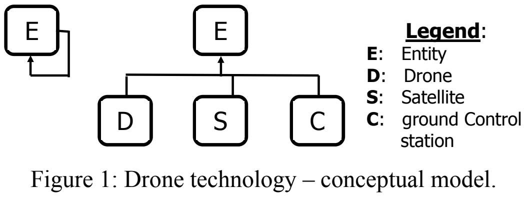

Figure 1: Drone technology – conceptual model.

As it is seen from the figure (left), there are entity types and one entity can interact with another entity; as it is also seen from the figure (right), there are three entity sub-types, namely: DRONE, SATELLITE, and GROUND CONTROL STATION. This is a simplified view on drone technology and performance; still, since only essential concepts are reflected in the presented model, it is possible to add further elaborations, staying considtent with it.

In the following sub-section, we will take a technology-specific view on the above.

2.2 Technology-Specific View

Even though the technology-specific view on drone functioning is to be consistent with the conceptual view, there are more technical and operational details that are to be considered in such a technology perspective. A partial technology-specific view on drone functioning is depicted in Figure 2:

Figure 2: Drone technology – technical view.

As it is seen from the figure and as also suggested by the conceptual model: there are three layers, namely ground control stations ('stations', for short), drones, and satellites. Further, drones are capable of operating (flying) with certain autonomy; nevertheless, there is always human decision-making and responsibility behind – this is conveyed through the stations (there is a bi-directional communication between the station and the drone: the drone receiving instructions (commands) from the station and the station receiving (processed) information from the drone). Still, the commands delivered from the station are not enough for allowing the drone to operate adequately since for this the drone would need precise navigation – this is provided through corresponding (GNSS) satellites; satellites are also used sometimes for facilitating the communication between the drone and the station (or the communication with third parties). With regard to this, the following technologies are important as relevant to the operation of drones:

- Data-link (up-link and down-link of data in real-time) – in order for this to be secure and protected against jamming, encryption is needed;
- The aircraft proximity warning "Sense and Avoid" systems;
  - This including approved automatic detection and avoidance equipment to be used as a mitigation means in case the drone-pilot cannot avoid C2-linkloss during Extended Visual Line of Sight (EVLOS) and Beyond Visual Line of Sight (BVLOS);
- Automatic flight control systems (and guidance);
- Navigation equipment (Inertial/GPS);
- Redundancy in critical location tracking systems such as GPS and location reporting systems;
- Sensor technology, such as Weather Sensors, for example, installed depending on the weight category of the particular drone.

Since functionally, two issues are essential when 'using' a drone, namely: (i) its collecting data from the environment; (ii) its streaming back data to the station, the *payload* concept is important – it is about determining the type of data the drone can collectit; *streaming back* data is important as well and this is done via the C2 (Communication and Control) link.

All this concerns sensor technology and data-streaming technology. The products diversity related to the mentioned technologies justifies the design of various drones, in terms of size and weight (including very small ones).

As mentioned already, those issues (and other related issues, such as the quality and the requirements for the sensor pack) are domain-specific.

2.3 Classification of Drone Platforms

There are different drones for a wide range of applications with different sizes. Drones can be classified in many ways: Use (civil vs military), Lift (fixed-wing vs multi-rotors), MTOW (maximum take-off weight), and so on. For a conceptual approach, a good way is to look at drone's performance, so it becomes easier to understand the underlying capabilities. We claim that drones could be usefully classified based on their size and payload since those are essential features from a functional point of view. For this reason, we are considering a US classification that reflects those features:

- Hand-launched, lightweight, low payload, multi-rotor drones, weighing less than 25 kg and flying at altitudes under 300 m. – they can handle localized imaging and be used for mapping with light payload;
- Long endurance reconnaissance and surveillance, fixed wing drones, weighing between 21 kg. and

50 kg., and flying at altitude under 3500 m. above ground level AGL - they can handle wide-area imaging and be used for mapping with light payload;

- Long endurance, large payload drones, weighing up to 1320 kg. and flying at altitudes under 8000 m. mean sea level MSL - they can handle localized imaging and be used for mapping with heavy payload;
- Heavy lift helicopter drones, often weighing more than 1320 kg. – they can be used for transportation of people and fly to remote locations;
- Long endurance, high altitude reconnaissance and surveillance drones, weighing more than 1320 kg. and having approximately the same size (and similar capabilities) as traditional manned aircraft – they can be used for wide-area searches.

All those platform choices concern corresponding platform characteristics and application needs, and often considering the trade-offs between the two is necessary, as depicted in Figure 3:

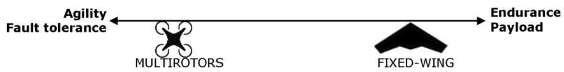

Figure 3: Trade-off between platforms and applications.

3 MAKING DRONES OPERATIONAL

Based on the functional (black-box) view on drone technology, as outlined in the previous section, we are presenting in the current section an operational (white-box) view on that, staying mainly focused on the payload aspects (that concern data capturing) and the software driving the drone, while abstracting from other engineering concerns, such as mechanics, motor, energy consumption, and so on.

Still in addressing payload and software, we are to keep in mind the particular drone mission that in turn relates to the aerial drone platform of choice. As an example: Fixed-wing platforms would be appropriate for scanning vast areas and/or for realizing long range flights, while rotor-drone platforms would be appropriate when situation-awareness is needed, featuring small areas and/or a specific target. Hence, taking this into account, we consider in the remaining of the current section payload and software as essential with regard to the operation of a drone.

3.1 Payload

While platforms dictate the drone's ability to access certain environments, its payload often determines the type of data it can collect. Remote sensors like Electro-Optical (EO) and Infrared (IR) (EO/IR) cameras can help establishing situation-awareness while communications relay payloads can be used to broadcast wireless frequencies wherever the drone travels. Other sensors are used in scanning the ground nevertheless – those are called Mapping (M) Sensors. In the remaining of this sub-section, we briefly consider EO/IR sensors and M sensors.

1. **EO/IR sensors** are the workhorses of drone-based sensing technology. These sensors provide the most commonly used data collected from drone platforms. We can consider in particular:
    - EO Sensors, mainly used for day operations; those sensors are relatively cheap and widely available; they include video cameras and high-definition photography equipment.
    - IR Sensors are excellent for night operations; those sensors detect the heat signatures of various objects; this is particularly useful for locating intruders at night and in large, open environments.
    - Dual EO/IR Sensors (combined into a dual package) can be used for both day and night operations.
2. **M sensors** scan the ground and create 2D or 3D maps of the surrounding area. Much drone-based mapping is currently geo-referenced, allowing it to be easily transposed onto existing geographical information systems (GIS):
    - LiDAR: capable of creating highly detailed topographical maps and 3D maps of border areas, useful in specifying maps of high precision.
    - Synthetic Aperture Radar (SAR): capable of providing detailed imagery of the ground day or night through cloud, fog, and smoke; also capable of detecting metal and other material.

Further, we consider **communication relay payloads** that allow drones to act as mobile communication stations, beaming Wi-Fi Internet, cellular service, radio, and other important signals to security personnel.

Hence, given their ability to quickly reach high altitudes (and hover in place for a prolonged perios – this is particularly valid for rotary-wing drone platforms), drones provide ideal stopgap solutions when communication infrastructure is unavailable.

3.2 Software

Drones need to be paired with sophisticated software – this is to improve the (data) link between the drone and its operator, but also to facilitate the streamline sharing of drone-collected data with other stakeholders. Such data can be utilized by mapping software products featuring maps and GIS – Geographic information Systems.

As for the requirements that concern drone software, they would inevitably relate to the typical drone environment – often aligned with military structures. This assumes considering three layers as follows:

- The bottom (executive) layer concerns the flight management and navigation. Therefore, the corresponding software support would be responsible for maintaining a controlled flight, often performed by an on-board autopilot. To this layer we can add also payload control systems harvesting data from the environment, such as sensors and radars.
- The tactical layer concerns the station (see Figure 2) where all the information about position, heading, speed etc. is ‘crunched’ with the mission important information from the payload and all is presented on the displays of the operators.
- The top (strategic) layer receives full real-time picture from all deployed drones and available infrastructure, for the superiors in order to make proper decisions.

4 USABILITY IN BORDER SECURITY

We refer to an application scenario featuring land border security (LBS, 2012), which is considered in another paper from the current proceedings (Shishkov et al., 2017). The scenario reflects the security protection of a land border segment equipped with wired border fence. There is no border crossing point in the considered area; this means that the security goal is to prevent any border crossings. Still, even though such a border segment could be secured professionally, it is physically impossible for border police officers to be anytime anywhere to react upon violations, if counting on traditional equipment (Shishkov and Mitrakos, 2016).

This leads to several important DEMANDS whose consideration would bring in useful results:

1. Effective monitoring of the large area around the wired fence, limited not only to the very close proximity to the fence itself;
2. Situation analysis capturing both problematic spots (for example: a crowd passing illegally) and available resources (for example: border police officers and vehicles);
3. Rescuing a border police officer (or another person) in trouble (for example: because of weather conditions).

Hence, those identified demands are basis for our analyzing the relevant strengths of drone technology.

In this regard, drones are claimed to present an attractive proposition mainly due to their providing unique viewing angles at low altitudes, something impossible to be achieved either by manned aircraft or by fixed cameras. For example, drones, flying over a border fence, are in a position to view much more that a fixed camera can, and cover a much vaster area than a human can physically cover while patrolling.

Further, drone technology is highly deployable. Drones, particularly small models, can be launched in a variety of environments without the need for a runway – this makes drone technology useful at the border where terrains are often difficult to handle.

Therefore, we consider drone technology as having good potential to usefully support border security. At the same time, we observe the need for corresponding control because as it was discussed already, drones may be autonomic to some extent and/or they may be navigated from distance – both cases assume risk of situational mis-interpretaion, in our view. Hence, establishing control should mainly be about the adequacy of task formulations and the validity of situation perception. On such a basis and taking into account the capabilities of the particular drone, it would be possible to actually involve drone(s) in particular operations at the border.

If this would be successful, then drones could indeed releave officers from some of their most dangerous duties (for example: rescuing a border police officer or another person who is in trouble). In this, a drone (representing an unmanned device) would deliver specific types of actions that can contribute to a smart and better decision making process, especially as it concerns disaster management (also in the border security context):

- Informer: A drone would often be capable of geting more information from the accident spotm which in turn would allow for a smart decision-making to be delivered accordingly.
- Helper: In some situations, a drone would be capable of delivering medication(s) and/or equipment needed in approaching an accident.

Finally, such solutions, if delivered through drones, would be cost-efficient, especially if compared to man-run helicopter actions. Also, a drone could do times more as monitoring, compared to what fixed cameras and physical persons could accomplish.

At the same time, there are particular limitations of drone-driven solutions, such as the risk of mis-interpretation of visual information as well as the flight risks in situations of strong wind / turbulence and or icing.

Summarizing the Strengths of Drone Technology

Based on our considering drone technology in Section 2 and Section 3, and inspired by the border security demands and related discussion (see above), we summarize the strengths of drone technology, particularly with regard to land border security. In doing this, we take into account that border protection uses a series of strategies, some more effective than others, to monitor huge strips of (rugged) terrain along the border: In some situations, it is needed to involve more border police officers in the protection of the border; In other situations, it would be enough to just better maintain and reinforce the fences (if any), barriers, access roads, and so on; In yet other situations, the deployment of specialized technology would be considered necessary, such that advanced monitoring can be realized (this may include high towers or radar, camera equipment, and so on) (LBS, 2012).

Hence, we identify strengths of drone technology, especially related to the **`monitoring`** challenge. Currently, *fixed towers* are used, which include radar as well as day and night cameras (mounted on a series of towers along the border). The radar and cameras transmit data to the border control center, where border police officers determine an appropriate course of action accordingly. Nevertheless, the limitations of such fixed static equipment are obvious. A wisely chosen drone platform can meet targetted demands in this regard, providing also augmentation of the existing systems via data transfer, surveillance, agility and additional flexibility over the mentioned static technologies (a surveillance would be much more effective from an aerial point of view); this would relieve personnel from missions, as well.

Further, drones can step into aviation shoes concerning aviation services for **`border surveillance and goods delivery`**, due to cost effectiveness. With regard to surveillance, drones are capable of carrying platforms for radar and long-distance cameras. With regard to goods, delivery, it is possible, depending on the drone platform of choice and corresponding weight limitations (initial testings of such deliveries have already been completed and there is an ongoing certification for them).

5 CONCLUSIONS

Aerial drones feature promising new technological solutions relevant to many aspects of our lives, security included (and in particular – land border security). At the land border, drones are capable of complementing traditional manned activities (such as patrolling, monitoring, conducting rescue operations, and so on), by helping to ensure that those activities are conducted safer, faster, and more efficiently. In particular:

- Drones are capable of providing a border police officer with situation-awareness – they can help locate intruders, perform structural analysis of damaged facilities (for example: a border fence facility) over large distances, and deliver needed supplies and equipment.
- Drones are capable of assisting with mapping and corresponding planning.
- Drones are capable of approaching dangerous zones where the safety of border police officers would be endangered.

Still, we claim that drones would be capable of being so useful only if drone roles and tasks are adequately specified not only from the engineering perspective but also from the domain perspective:

- Engineers should make sure that the user requirements are realistic with regard to the technical possibilities and related limitations of the drone platform of choice;
- Security experts should make sure that the tasks assigned to drones are complementing (rather than conflicting) with regard to the tasks fulfilled by border police officers and also that corresponding performance indicators are used, such that the information captured (by drones) as well as its interpretation are justified.

Those are the conclusions drawn in the current position paper in which we have analyzed the usability of drone technology with regard to a particular application domain (namely: land border security), inspired by a high-level study of drone technology and the consideration of the mentioned domain and a related application scenario.

A limitation of our work is that it is too high-level and insufficiently concrete as it concerns enterprise / software specifications (Shishkov, 2017) related to the enabling of drone usage at the land border. This will be the main focus of our further research.

REFERENCES

Adams, S., Friedland, C., 2011. *A Survey of Unmanned Aerial Vehicle (UAV) Usage for Imagery Collection in Disaster Research and Management*. Louisiana State University, USA (Technical Report).

American Red Cross, 2015. *Drones for Disaster Response Relief Operations Study*. American Red Cross, USA.

AWARENESS, 2008. *Freeband AWARENESS Project*. http://www.freeband.nl.

Bravo R., Leiras A., 2015. *Literature Review of the Application of UAVs in Humanitarian Relief*. In *XXXV Encontro Nacional de Engenharia de Producao*.

Drent, M., Landman, L., Zandee, D., 2014. *The EU as a Security Provider*. Clingendael Report of the *Nederlands Institute for International Relations*.

European Emergency Number Association, 2015. *Remote Piloted Airborne Systems (RPAS) and the Emergency Services*. European Emergency Number Association, Belgium.

FRONTEX, 2017, the website on the European Agency, FRONTEX: http://frontex.europa.eu.

Gavrailov, A., 2014. *Global Commercial and Civil UAV Market Guide*. Published by INEA Consulting, UK.

Guerra, S., McNerney, M., 2015. *Air National Guard Remotely Piloted Aircraft and Domestic Missions, Opportunities and Challenges*. Published by the *RAND Corporation*, USA.

ICARUS, 2012. FP7 EU Project on Integrated Components for Assisted Rescue and Unmanned Search Operations: http://www.fp7-icarus.eu.

IoTDI, 2017. *2nd International Conference on Internet-of-Things Design and Implementation*. ACM/IEEE.

Lacher, A., Maroney, D., 2012. *A New Paradigm for Small UAS*. Published by the *MITRE Corporation*, USA.

LBS, 2012. LandBorderSurveillance, the EBF, LandBorderSurveillance Project: http://ec.europa.eu.

OCHA – UN, 2014. *Unmanned Aerial Vehicles in Humanitarian Response*. Report in the *OCHA Policy and Studies Series*, United Nations Office for the Coordination of Humanitarian Affairs.

SenseFly, 2016. *Robots to the Rescue – Researching How Drones Can Help Save Lives*. Report to the *European Commission*.

Shishkov, B., 2017. *Enterprise Information Systems, A Modeling Approach*, IICREST. Sofia, 1st edition.

Shishkov, B., Janssen, M., Yin, Y., 2017. Towards Context-Aware and Privacy-Sensitive Systems. In *BMSD'17, 7th International Symposium on Business Modeling and Software Design*. SCITEPRESS.

Shishkov, B., Mitrakos, D., 2016. Towards Context-Aware Border Security Control. In *BMSD'16, 6th International Symposium on Business Modeling and Software Design*. SCITEPRESS.

Tanzi, T., Chandra, M., Isnard, J., Camara, D., Sebastien, O., Harivelo, F., 2016. *Towards "Drone-Borne" Disaster Management: Future Application Scenarios*. In *ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume III, COPERNICUS, Germany.