Drones in Land Border Missions: Benefits and Accountability Concerns

Boris Shishkov
IMI – BAS, IICREST /
TBM – TU Delft
Bulgaria / The Netherlands
b.b.shishkov@iicrest.org

Stefan Hristozov
Institute of Robotics
BAS
Bulgaria
stefan.hristozov@gmail.com

Marijn Janssen
Faculty of Technology, Policy and Management, TU Delft
The Netherlands
M.F.W.H.A.Janssen@tudelft.nl

Jeroen van den Hoven
Faculty of Technology, Policy and Management, TU Delft
The Netherlands
M.J.vandenHoven@tudelft.nl

ABSTRACT

Drone technology can potentially be useful for land-borer security - unmanned drone missions could be performed in the sky, supported by embedded sensors and data processing. Algorithmic rules can be incorporated in the drone software to make instant decisions, whereas other decisions might be made on the ground on the basis of monitoring data received from the drone. This allows for achieving context-awareness: the operation of the drone depends on the situation at hand. The mix of algorithmic and human decision-making distributed over many components raises questions that concern accountability - who would be responsible in case of an accident or a 'wrong doing': the hardware or software developers, the ground station managers, the law (regulations) makers, or the ones who have decided to use drones in the particular situation? In the current work we analyze the usability of drones with regard to land border security, featuring benefits and corresponding accountability concerns. To achieve this, we have studied drone technology and in particular: the technical features as well as the corresponding actor-roles and relationships, considering a land-border-security-related application scenario. On that basis we have carried out an analysis from an accountability perspective.

KEYWORDS

Drone technology; Accountability; Public values; Value tensions; Land border security

ICTRS'17, November 6–7, 2017, Delft, Netherlands

ACM ISBN 978-1-4503-6364-8/17/11...$15.00
https://doi.org/10.1145/3152808.3152820

1 INTRODUCTION

`Drones` of different kinds (from industrial drones to military ones that realize sophisticated operations in dangerous environments) reveal promising potential for facilitating domains of high societal relevance [15]. One such domain is **`land border security`** [27] - unmanned drone border security missions could be performed in the sky, supported by embedded sensors and data processing [14]. Often such missions assume possible communication transmission failures, delays, and so on, this in turn requiring a certain level of **`autonomy`** (autonomic behavior could possibly be supported by algorithmic rules that can be incorporated in the software spanning over the drone and the ground control station) that is helpful as it concerns instant decision-making, whereas other decisions can be made on the ground, on the basis of monitoring data received from the drone. This allows for achieving **`context-awareness`** [3]: by this we mean that the operation of a drone (piloted remotely) would depend on the situation at hand. We hence argue that an application of drone technology exhibits autonomic behavior and incorporates context awareness. This already assumes a high degree of autonomy not only in the sky (where the drone is operating) but also on the ground (where often automated generations of instructions take place, based on run-time incoming data), this leading to only limited human control on what is going on [10]. Thus, even though technology has developed, many questions have not yet been answered, including: *Is current drone technology indeed reliable if used in critical (rescue) operations? Is the human navigating a drone responsible for what the drone would do? Who is responsible in the case of autonomic drones? Who is responsible in the case of malfunctioning? Who is responsible if a malicious party establishes control over a drone? Are current software platforms running on*

drones powerful enough to cover all possible situations that may pop up in the sky? In general, it is important to know who is the responsible 'party' (or a combination of parties) – the hardware or software developers, the ground station managers, the law (regulations) makers, or the ones who have decided to use drones in the particular situation? Also, what measures can be expected and from which party, in order to ensure safe and secure operations.

This points to **accountability** as a desired **value** that is supposed to adequately balance the technical features against corresponding societal expectations, as according to **Value-Sensitive Design – VSD** [8]. VSD accounts for human values in a principled and comprehensive manner [9], featuring values as non-functional requirements that are to be integrated in the design process. In this way they are not to be post-implemented as 'additions' but they are to be weaved in the design since the very early stages of the technology development life cycle [29].

Accountability is a key value in this regard, concerning a relationship between two or more parties, where one party is held responsible for the performance with regard to some objective and the use of resources to accomplish this objective. Accountability implies the obligation with regard to one's actions or inactions, aligned with corresponding responsibility and possibly leading to consequences [24]. As drone technology is concerned, this could be the malfunction of a drone, but it could also refer to the inability to test software and/or ensure proper security, and so on. Hence, accountability refers to a situation in which a party has a duty and there is another party assessing that duty's fulfilment and possibly even imposing sanctions [30]. This requires clear expectations and agreements among parties. There is no consensus about what makes up a good accountability system in general [24]. Particularly, in situations in which many parties are involved and there are many dependencies, creating a good accountability system is challenging.

Looking at drones, there are many parties involved (in launching and controlling drone missions) while the corresponding responsibilities and duties are not as well-defined as needed for accountability. This makes it complex to establish accountability in that domain. Therefore it is needed to understand the dependencies among subsystems (taking into account that drone technology is featuring both automated and human decision-making) as well as to adequately map those dependencies on corresponding actor roles and role-to-role relationships. We claim that only then the accountability relationships would become clear.

It is therefore interesting to us how technology is allowing for building autonomous and intelligent drones functioning for the benefit of Society and also how Society in turn is demanding (and establishing) accountability on top of that, such that it is known who is responsible and who is to be punished in case of a failure and/or a wrong-doing.

Since analyzing this would inevitably be domain-specific (because in our view such technological possibilities and corresponding societal demands differ from domain to domain), we are limiting our scope to the security application domain, in general and particularly, to land border security.

Hence, in the current work **we analyze the usability of drones with regard to land border security**, featuring benefits and corresponding accountability concerns. To achieve this, we have studied drone technology and in particular: the technical features as well as the corresponding actor-roles and relationships, considering a land-border-security-related application scenario. On that basis **we have carried out an analysis from an accountability perspective**, considering (among other things) tensions between technical possibilities and the accountability value and also possible **tensions** between accountability and other relevant values.

The remaining of the current paper is organized as follows: In Section 2, we introduce and discuss the technical aspects of drones, proposing a general reference architecture. In Section 3, we map the reference architecture onto a higher-level reference entity model that is considered an adequate basis for a further accountability-driven analysis. Thereafter, in Section 4 we present a motivating application scenario featuring land border security. In Section 5, we carry out a corresponding analysis from an accountability perspective. In Section 6, we analyze related work and in Section 7, we present the conclusions.

As for Section 2, it is backed by the following references: [1,2,4,6,7,12,13,19,28].

2 DRONE TECHNOLOGY - BACKGROUND

Based on previous work [14], we present in the current section technical features concerning drone technology; most of them are claimed to be relevant to accountability.

Drone, **Ground control station**, and **Satellites** as subsystems are considered important for drone technology: (i) drones themselves are devices that can act with certain degree of autonomy and as mentioned before, depending on the particular technical/technological solution considered, there may be lower or higher degree of autonomy; (ii) in order for a drone to operate, it needs a ground control station from where flight commands and instructions are generated for the sake of controlling and navigating the drone; (iii) in order for the ground station to be able to control and navigate drones, satellite communication and positioning are needed.

Nevertheless, even though drones are capable of operating (flying) with certain autonomy, there would always be a human decision-making / responsibility involved (delivered from the ground control station), this is even in cases of high degree of drone autonomy. 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, and a human operator would often be closely controlling those processes.

Still, as already mentioned, the human involvement might be partially or even completely interrupted - connection might be lost or there might be communication delays, or something else. As a consequence, the drone would need to operate

autonomously, possibly being supported by GNSS satellites ('GNSS' stands for: 'Global Navigation Satellite System'); satellites are also used sometimes for facilitating the communication between the drone and the station (or the communication with third parties). The following technical facilities are important for such an autonomous operation of a drone:

- 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;
- Aircraft proximity warning "Sense and Avoid" systems;
  - including automatic detection and avoidance equipment to be used as a mitigation means in case the drone cannot avoid C2-link-loss during EVLOS (Extended Visual Line of Sight) and BVLOS (Beyond Visual Line of Sight);
- Automatic flight control systems;
- Navigation equipment (Inertial/GPS);
- Location tracking (GPS) systems;
- Sensor technology, such as weather sensors, for example, installed depending on the weight category of the particular drone.

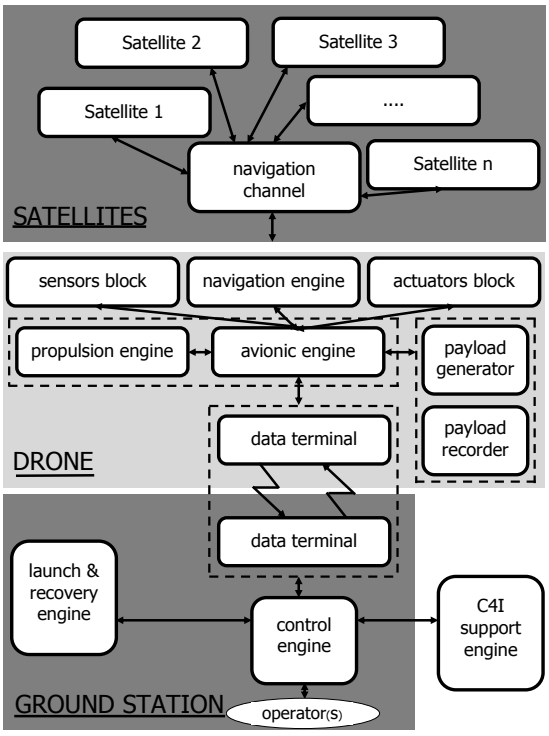

Figure 1: Drone technology – reference architecture.

This all concerns autonomic flight situations even though we are not limiting our research to such situations. Instead, we aim at deriving a **general reference architecture** featuring drone technology, that could be instantiated accordingly depending on the particular application. Hence, by 'reference architecture' we mean a system abstraction showing the main elements that can be used as reference for implementations.

Our derived architecture (exhibited in Figure 1) is featuring the three subsystems mentioned above (for the sake of brevity, we use the label 'ground station', instead of 'ground control station') and we argue that all current drone technology solutions would be consistent with that architecture.

As it concerns a **drone**, there are six main building blocks, namely: the *flight block* (in the middle, in the light-grey part of the figure), the *command block* right in the light-grey part of the figure), the *data block*/*terminal* (under the flight block), as well as above the flight block - the *sensors block*, the *actuators block*, and the *navigation engine*. The flight block in turn is composed of two components, namely: PROPULSION ENGINE (responsible for the mechanical aspects of the flight of the drone) and AVIONIC ENGINE (featuring the drone's electronics + corresponding software). The command block is also composed of two components, namely: PAYLOAD GENERATOR (triggering the commands driving the drone) and PAYLOAD RECORDER (running the logging).

The avionic engine is bridging between the commands (referring to the payload) and the realization of those commands (referring to the mechanics of the drone), and it is also *linking the drone to the ground station through* the DATA TERMINAL. Further, the avionic engine is linked to sensors and actuators (SENSORS BLOCK and ACTUATORS BLOCK) allowing for monitoring the surrounding environment and enabling actions accordingly. Finally, a NAVIGATION ENGINE is supporting the satellite-driven navigation of the drone.

As it concerns the **ground station**, there is an essential component there, namely the CONTROL ENGINE – it is responsible for navigating the drone (if the drone has not switched to an 'auto-pilot' (autonomous) mode), using intelligent algorithms as well as monitoring information (being in turn received from the drone). The control engine is backed by a LAUNCH AND RECOVERY ENGINE that helps in triggering the drone and/or reacting to system failure situations. Further, there are OPERATORS – humans who are capable of manipulating the control engine and through it – the drone; nonetheless, human interventions are rare and they concern mainly exceptional situations. Finally, the ground station is linked to external support units, such as the C4I ENGINE ('C4I' standing for: 'Command, Control, Communications, Computers, and Intelligence') that delivers advanced (cloud-based) computing and/or communication services upon request. Actually, C4I is externally supplied if the C2 is insufficient as performed by the control engine in the ground station ('C2' standing for: 'Command and Control').

A drone would communicate with the subsystem **satellites**, using a dedicated NAVIGATION CHANNEL. Nevertheless, it would be incomplete taking into account only the navigation channel when considering the communication-related activities of a drone. At least two other essential communication-related activities are to be mentioned in this regard: (i) sensing the environment (at payload level it would be determined what type

of data the drone can collect), and (ii) streaming data to the ground station (possibly supported by 'C2' means from the control engine). Thus, sensor technology and data-streaming technologies need to be applied in combination.

Further, this all (and in general – most processes concerning the operation of a drone) assumes support delivered by the software facilitating the drone and the ground station, providing a set of functions as follows:

- Translation of messages exchanged between the control engine and the drone;
- Data packing/unpacking for the sake of optimizing the transmission bandwidth;
- Servicing corresponding databases;
- Managing interfaces for data link messages, control, and monitoring;
- Managing interfaces for launch and recovery operations;
- Managing the analogue-to-digital conversions of sensor data.

Finally, with regard to accountability, it is needed to know where the decision-making about the drone actions is taking place. This concerns the technical explanations (see above) as well as several focused questions that are to bridge the content of the current section to the content of sections 3 and 5:

Looking at the interactions between the drone subsystem and the satellites subsystem:

- SATELLITES are navigating the drone through the navigation channel and the navigation engine but who is responsible if:
  - the satellite data is incorrect?
  - the drone navigation engine is operating inadequately?

Looking at the drone subsystem and its interactions with the ground station:

- SENSORS capture run-time information that is delivered to the ground station from where corresponding instructions are transmitted in turn to the drone but who is responsible if:
  - the information gathered is of insufficient quality to be useful and this leads to something undesired?
  - the information gathered is wrongly interpreted at the ground station and this leads to something undesired?
  - the information is not received or arrives too late?
- ACTUATORS are drone's 'instruments' to implement particular actions, such as directing a camera, sending off an audio or even shooting but who is responsible if an actuator implements wrongly what is desired or another effect is created not the one that was intended?
- The PROPULSION ENGINE is the mechanics driver of the drone but who is responsible if the drone breaks down mechanically which might cause undesired consequences?
- The AVIONIC ENGINE is the electronics 'brain' of the drone, facilitated also by software but who is responsible if:
  - the avionics would crash due to malfunctioning of the software?
  - a DDoS (Distributed Denial of Service) attack would cause the avionics to stop working properly?
- The COMMAND BLOCK is about triggering and archiving the commands executed by the drone but who is responsible if the commands are inadequately generated?
- The DATA running between the drone and the ground station as well as between the drone and satellites is of crucial importance but who is responsible if the connection breaks down?

Looking at the ground station subsystem and its interactions with the drone:

- The CONTROL ENGINE on the ground is to guarantee that the drone's operation in the sky is adequate to the safety requirements, to the Law, and so on but who is responsible if the control engine appears to be unable to affect undesired things happening in the sky (concerning the drone)?
- The LAUNCH AND RECOVERY ENGINE (that is basically a catapult, catching device or landing gear) is to provide support to the control engine in the case of launching a drone mission and/or in the case of a system failure but who is responsible if
  - the needed support is not provided?
  - the battery/power supply goes down?
- The Human OPERATOR(S) on the ground monitor the work of the ground station and the drone's mission in the sky and are supposed to intervene if the mission gets out of control but who is responsible if
  - such an intervention fails?
  - the drone accidentally passes a country border?
  - the drone falls form the sky and causes damages or event causalities?

Looking at the external support provided to the system:

- The C4I ENGINE is to provide computing and/or telecommunications support to the ground station upon request but who is responsible if such support is needed (and requested) but not received in time or not received at all?

Hence, there are different subsystems which are dependent on each other and are designed or operated by different parties. Some of the accountabilities here are straightforward, whereas others are insufficiently clear. Some of the issues can be overcome, by tackling them in the design, whereas other issues assume explicit agreements among parties to ensure clear accountabilities.

In the next section, we will reflect the above-discussed technical features and details in corresponding actor roles and role-to-role relationships, such that we are able to analyse drone technology from an accountability perspective.

3 IDENTIFYING AND ANALYZING ACTOR ROLES

The identification of actor roles that we carry out in this section, is inspired by the reference architecture - see Figure 1. We consider actor roles (**`roles`**, for short) rather than considering actors, because even though one role could be fulfilled by different actors and also one actor could fulfil different roles, it is the role that corresponds to the specification of what is being done and this in turn relating to corresponding responsibilities [25].

Further, since we conceptualize technology that is already there and also it is reflected not only in atomic lowest level technical modules but also at architectural level, we would not go bottom-up in our modeling neither would we go top-down. Instead, we are taking a **`middle-out modeling perspective`**. This means that the reference architecture (more technology-specific) is to be restricting our higher level models (more abstract and therefore - conceptual) which models would help us reasoning further. We therefore map each entity onto a corresponding role as follows, starting from the drone (**d**) subsystem:

- The payload generator points to the role *ENABLER* (**dE**, for short) since it is the payload that is generating a command triggering the drone.
- The payload recorder points to the role *RECORD-KEEPER* (**dR**, for short) since it is the payload recorder that is recording all commands as archival data.
- The avionic engine points to the role *COORDINATOR* (**dC**, for short) since through its electronics and software, the avionics is coordinating all processes within the drone.
- The navigation engine points to the role *NAVIGATOR* (**dN**, for short) since using satellite information, the navigation engine is navigating the drone.
- The propulsion engine points to the role *PERFORMER* (**dP**, for short) since it is the propulsion engine that empowers drone's flying.
- The actuators block points to the role *MANIPULATOR* (**dM**, for short) since through its actuators, the drone realizes manipulations, such as moving a camera, for example.
- The data terminal points to the role *DATA MANAGER* (**dD**, for short) because it is the data terminal that helps managing all data running through the drone.
- The sensors block points to the role *SENSOR* (**dS**, for short) since sensors are capturing (visual) information that is used by the ground station in support of its controlling the drone's operation.

Then, with regard to the ground station (**gs**) subsystem:

- The data terminal points to the role *DATA SUPPLIER* (**gsD**, for short) because through the data terminal, the ground station mainly supplies command information towards the drone.
- The control engine points to the role *COMMANDER* (**gsC**, for short) since it is the control engine that essentially executes the drone's mission, by pushing forward commands.
- The launch & recovery engine points to the role *SUPPORTER* (**gsS**, for short) since that engine is providing support to the control engine.
- We also have the role *OPERATOR* (**gsO**) fulfilled by the human agent(s) who are operating the control engine.

Finally, regarding the satellites (**s**) subsystem:

- The navigation channel through which the satellite data is delivered points to the role *POSITIONER* (**sP**, for short) since through this channel, the drone positioning is established, that in turn empowers the navigation of the drone.

Those are the main EXPLICIT ROLES that we have identified, staying at the granularity level of the reference architecture entities and abstracting from anything that is outside the system, for example – the C41 support engine; exception to this is the role USER pointing to the one in whose benefit the drone mission is running. Further, we acknowledge also IMPLICIT ROLES that even though not straightforwardly map-able from the reference architecture, are to be considered and have been discussed before in the paper – those are the roles relating to the hardware-software developers and the policy-makers; the hardware/software developers are enabling some technical components that are explicitly reflected in roles (see above) while the policy-makers have influence over the system regulations and the ground station operator(s).

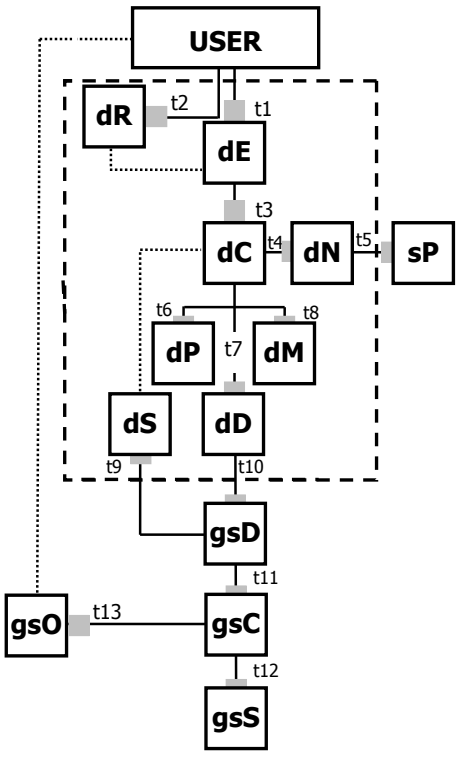

Figure 2: Drone technology – reference entity model.

Further, sticking to the roles-transactions modeling as considered by Shishkov [25], we envision two essential modeling constructs, namely:

- **ENTITIES**, featuring the identified roles;
- **TRANSACTIONS**: a transaction is a finite *sequence of coordination acts* between two actors, concerning the same *production fact*. The actor who starts the transaction is called the *initiator*. The general objective of the initiator of a transaction is to have something done by the other actor, who therefore is called the *executor* [5].

Hence, next to identifying the roles, we are also identifying the role-to-role transactions, by reflecting accordingly corresponding relationships from the reference architecture (Figure 1).

The identified entities (roles) are 13 (see above, namely: dE, dR, dC, dN, dP, dM, dD, dS, gsD, gsC, gsS, gsO, and sP plus the USER, related among each other through 13 corresponding transactions:

- **t1** (the *executor* is dE): the enabler is triggering the drone;
- **t2** (the *executor* is dR): in parallel, the record-keeper is maintaining logs;
- **t3** (the *executor* is dC): this is triggering the coordinator to initiate in parallel the navigation, the drone flight, the corresponding data exchanges and (if needed) manipulations;
- **t4** (the *executor* is dN): the navigator starts navigating the drone, for which the navigator triggers the positioner to provide positioning data;
- **t5** (the *executor* is sP): the positioner in turn delivers positioning data to the navigator;
- **t6** (the *executor* is dP): on that basis, the performer runs the mechanics of the drone, such that the drone could start up its mission in the sky;
- **t7** (the *executor* is dD): this triggers the data manager to start the data exchange between the drone and the ground station;
- **t8** (the *executor* is dM): once the drone is up and flying with data flowing accordingly between the drone and the ground station, the manipulator is triggered (if necessary) for the sake of enabling the drone to perform particular actions in the sky;
- **t9** (the *executor* is dS): this relates to triggering the sensor that delivers (visual) data captured in the sky to the ground station;
- **t10** (the *executor* is gsD): on that basis, the data supplier generates command information delivered to the drone in support of its operation;
- **t11** (the *executor* is gsC): this commands generation is to be 'fueled' by the commander that essentially runs the drone from the ground;
- **t12** (the *executor* is gsS): this may require support from the supporter, especially when the drone is launched and/or a failure occurs;
- **t13** (the *executor* is gsO): this all assumes a human operator controlling the commander, especially in extreme situations.

This all is depicted in Figure 2 where: (i) the user is represented as rectangle on top; (ii) the entities (roles) are presented as named boxes; (iii) the corresponding transactions are represented as solid lines with labels corresponding to the transaction numbers (see above); (iv) the small grey boxes at one of the ends of each solid line indicate who is the executor of the particular transaction; (v) the dotted lines indicate indirect relationship between two entities (for example: in order for maintaining a command data log, it is necessary that commands have been generated); (vi) finally, the dashed rectangle delineates those entities that are inside the drone.

We consider the realized identification of actor roles and transactions as well as the corresponding analysis featuring them (based on the reference architecture) a useful basis for reasoning about accountability. Nevertheless, as already mentioned, to be effective in this, it is important to have a particular domain focus. That is why in the next section we present accordingly a motivating application scenario.

4 APPLICATION SCENARIO

The domain focus in this paper is inspired by the current scenario that is not only supposed to illustrate the usability of drones but it is also considered helpful in identifying accountability issues to be reflected in the analysis in Section 5. The scenario is featuring a case example in land border security, that has been studied by Shishkov et al. [26] and for the sake of brevity we only partially reflect the case information in this section, still considering sufficient level of detail in order to have a good basis for adequately performing our accountability-related domain-specific reasoning concerning the usability of drones. In particular: A land border segment is focused, spanning between two border crossing control points. It is only allowed to cross the border at a border crossing control point and it is forbidden to cross at any other point along the border.

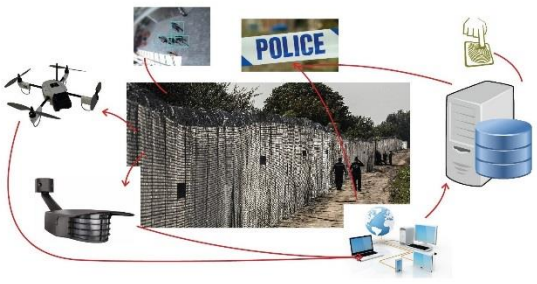

Figure 3: A case example featuring land border security.

For this reason, a wired fence facility has been installed along the border, between the border crossing control points. Further, there is a road along the wired fence, allowing for border police officers and/or vehicles to move along the border. This is illustrated in Figure 3.

As it is suggested by the figure, there are border police officers supported by technology and devices (possibly including drones),

who are MONITORING the border along the wired fence; further, DIRECT ACTIONS against possible violators are to be realized by border police officers only (hence, it is impossible that drones are directly involved in confronting violators). Still, it is possible that drones get indirectly involved, by identifying illegal border crossings and signaling corresponding border police officers accordingly, by playing audio warnings against identified violators, and possibly in other ways.

Monitoring that particular land border segment is a continuous process and no matter how many border police officers are sent to the border, it would be physically impossible to guarantee police presence at any time anywhere along the border segment (there are very many such segments featuring the considered land border, this all spanning over hundreds of kilometers). There are *sensors and other (smart) devices*, realizing surveillance – some of them are part of the infrastructure fixed to the wired fence and adjacent facilities while others are part of the equipment of drones that may realize border surveillance missions in the sky. We assume the possibility that a device would perform local processing + artificial reasoning – based on this, it may generate contentful messages to be transmitted to corresponding human agents.

With regard to this and visioning the possible contribution of drones, we consider the following relevant action types:

- In a 'normal situation', a drone is flying along the border and above the wired border fence, recording video that is kept as archive.
- If while a drone is flying, a border crossing violation occurs that is in the scope of the drone's sensors/cameras, then the drone starts transmitting video/images to the ground station where that data is processed, applying pattern recognition facilities, and:
  - If the conclusion is that what was observed is not a border crossing violation, then the drone is instructed to ignore the 'alarm' and continue the mission in 'normal' mode.
  - Otherwise, the drone is triggered to immediately play an audio warning intended to explicitly inform the potential violators that they are acting against the Law and should therefore assume all corresponding consequences if ignoring the warning AND the drone is triggered to precisely locate (position) the violators, such that a border police unit is dispatched there immediately.
- If violators would confront the border police officers, then a border police officer is to trigger alarm that among other things triggers in turn the drone to start video-recording the 'scene' and transmitting in real-time video to the ground station. Such a video's usefulness might be two-fold:
  - If in the future, a violator would be prosecuted, then such a video could be used as evidence in the court (for example, disclosing that the violator has hit a border police officer);
  - Or a video could disclose information featuring the behavior of border police officers (showing, for example, that a border police officer has acted beyond the legal regulations and/or against the human rights of a violator).
- If a drone gets hit somehow, it would be triggered to establish its position and transmit positioning information to the ground station accordingly, and then it is to immediately destroy itself in order to avoid the risk that third parties obtain sensitive security-related information, by capturing the drone.

Hence, the above-presented case example is featuring the core vision on using drones in land border missions. Nevertheless, for the sake of brevity, we have abstracted from some minor details. For more land-border-security-specific information, interested readers are referred to [26].

We consider that case information to be sufficient as a basis for reasoning from an accountability perspective, taking into account the reference architecture (see Section 2) and the higher-level entity reference model (see Section 3). This is done in the next section.

5 ANALYSIS FROM AN ACCOUNTABILITY PERSPECTIVE

Even though drone technology is insufficiently mature yet, it is already subject to the air law makers and authorities [11]. Hence, it is expected that any design/maintenance/operational failure would be easily traceable and reportable, thus leading to corresponding accountabilities. This could also concern the responsibility for triggering the drone to destroy itself if attacked, as discussed in the previous section – failing in this could result in chances that a malicious party establishes control over the drone, possibly even through intervening in the C2 link communication between the drone and the ground station, reaching as far as the control engine. Hence, preventing this from happening, even if the drone has been unsuccessful in destroying itself, would have been responsibility of the human operator who is expected to intervene in any extraordinary situation. Nevertheless, it is also possible that such undesired developments result from software problems – it is to be mentioned that the software 'volume' increases tremendously over the last years, reaching more than 6 million lines of code as is the case with the latest Boeing airliners [11]; even though software running on drones would not be that bulky, it is still 'heavy' enough to pose risks and in the cases of software failure, it would not be easy to establish accountability because there are different software versions, updates, and maintenance requirements, and the reason for the failure could well be put in any of those directions.

Accountability requires the curation of software and algorithms [16]. The algorithms and their impact on the drone functioning should be scrutinized to understand decision-making. Also the failure of components should be traced. Hence the logging of the interactions among the components is a typical task

that needs to be realized in order to audit the history and determine accountabilities.

Another accountability perspective concerns the decision to use drones in a particular situation, and with regard to land border security, there are several relevant problem types:

- If a drone mission is triggered in poor weather conditions, this might put at risk both the mission effectiveness and the drone. The human operator(s) at the ground station would usually be responsible in such a case. It is also possible nevertheless that the human operator has followed recommendations from the ground station, delivered by external support parties (see Figure 1) and if this would be the case, then those providing the supporting facilities should be considered responsible since their delivered Quality-of-Service may have been below the agreed 'levels'.
- If a drone would be allowed to fly so close to people (even if they are violators) such that it is capable of video-recording privacy-protected (facial) information, then the human operator navigating the mission would be responsible.
- If a drone land border mission would lead to a diplomatic (spy) conflict with the neighboring country, then the authorities who have established the ground station without explicitly instructing the human operator, would be responsible.

Hence, in tackling accountability at the land border with regard to drone missions, we should distinguish between two essential situation types:

(i) situations when decision-making is in the hands of humans;

(ii) situations when decision-making is (partly) left to 'intelligent' systems that are supposed to contribute to human/business goals.

It is easier to tackle (i) because tackling (ii) should assume adequate traceability of requirements that is ensured during the design and implementation process. Nevertheless, establishing such traceability becomes more and more difficult with current data-driven intelligent systems because often the used (machine learning) algorithms arrive at strange 'conclusions' and this may lead to actions that were not foreseen by the design.

Still, we argue that the DESIGN should be important and for this reason, we lean towards weaving accountability in the drone system design. This represents a **Value-Sensitive Design – VSD**, mentioned already in the current paper.

Our VSD-inspired view on accountability's implications with regard to land border drone missions is depicted in Figure 4. As it is seen from the figure: (i) at design time we specify what is DESIRED while at run time (during operation) it shows up what ACTUALLY HAPPENED (what was observed; (ii) if the observed performance corresponds to what was desired, then the drone mission has been successful; (iii) otherwise, the desired performance was not achieved and corresponding ACCOUNTABILITY would need to be considered and this would only be possible if the accountability value has been reflected in the design, such that the user can effectively trace back what happened and identify the responsible actor(s).

Finally, empowering accountability could possibly lead to some value tensions if for example tracing back what happened would lead to:

- disclosing privacy-sensitive information and/or classified information;
- making technical data explicit including such data that represents copyright-protected 'know-how';
- reducing the system availability (during the traceability-related actions).

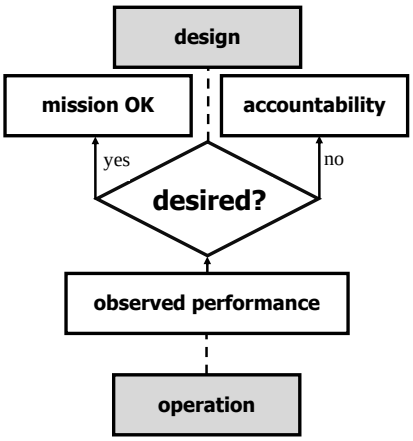

Figure 4: Accountability implications.

6 RELATED WORK

Drone technology is relatively new and there is not enough research being done in this area; still, different EU/US institutions often lean towards using drones in military missions, even though legislation featuring drones is yet not mature enough [11]. Further, drone usability know-how and requirements are currently being considered by emergency responders and disaster relief workers in the context of limited usage of drones in rescue operations [2]. Since accountability is relevant to both mentioned application areas (military and rescue operations), our study on related work presented in this section is considered particularly useful.

As it concerns military, drones are visioned as relevant to the EU security and the idea on integrating drones in the state security systems is currently receiving more and more attention within the European Union, as according to the European *Capability Development Plan* [6]. The Concept for Air Surveillance and Reconnaissance of the Bulgarian Armed Forces is consistent with this vision [23]. This all mainly points to military and surveillance missions, which is not surprising taking into account the experience of military air-force units concerning unmanned air vehicles – the military experience concerning drones is much

greater than the corresponding civil experience. This unfortunately assumes higher level of secrecy and lower level of CIVIL accountability, in our view.

Considering further the military usability of drones, it is to be mentioned that in USA, both the *Air Force* and the *Navy* view drones as a completely new vector of capability development, coming with new employment constrains: from technology (telecommunications and autonomic computing), through *battle units' considerations* (organization, mission planning, and shared responsibilities) to *personnel issues* (qualification and routines), this all assuming high degree of responsibility traceability [22]; this would hopefully make up good foundations for establishing accountability standards in the future.

Reaching beyond the military applications, Gambold [11] considers the public acceptance vs drawbacks of drone technology; this concerns mainly *emergency responders* and *disaster workers*. The American Red Cross [2] and the European Emergency Number Association [7] analyze requirements and give corresponding policy recommendations – as part of this: new categorizations are proposed and investigations / experiments are carried out, ethical issues are discussed (touching upon citizen's privacy and surveillance data considerations), and so on. In the context of emergency response Tanzi et al. [28] are proposing drone fleet architectures.

Further, the actual modeling of *drone dynamics*, the *weather impact*, and *sensor capabilities* have been studied by Menthe et al. [21]. Moreover, real data concerning drone usage is considered by Guerra and McNerney [13], featuring five years of drone service in the US National Guard. Other relevant examples have been considered by Kolev [17,18].

7 CONCLUSIONS

In the current paper, we have studied drone technology, taking a middle-out approach according to which we firstly identified relevant technical components and then on that basis we derived a corresponding domain-independent roles-relationships model. We then considered an application domain (namely: land border security) and analyzed the usability of drones from that perspective, complementing this by a survey featuring related work. Even though we conclude positively about the usability of drones in land border security missions, we acknowledge that the involvement of many subsystems raises concerns about the relationship among them and about who is accountable for proper operations and in case of failure. Accountability concerns answerability and responsibility for actions

It is considered particularly useful that we have decomposed the 'drone technology system' (from a technical perspective and then from the perspective of roles and relationships) to understand how the subsystems would influence the overall behavior. The failure of one component might result in an overall system failure. Hence, clarity is needed regarding the functioning expectations that concern the drone technology subsystems. Stakeholders need to build together a reliable system in which the responsibilities are well-defined and agreed upon.

As it concerns land border drone missions, accountability is considered crucial because failure consequences could be very negative (such as: omission of security, privacy compromises, disclosure of classified information, and so on) and this asks for adequate mechanisms for identifying who is responsible (in case of failure) such that (s)he is kept accountable.

A contribution of the current work is that we have provided an adequate modeling basis for reasoning about values (including accountability) and we have made such a reasoning explicit particularly featuring land border security.

A serious limitation of our work is that we have not proposed explicit design solutions that assume weaving in of accountability-related features in the drone system specifications. This challenge will inspire our further research activities.

ACKNOWLEDGEMENTS

This work was supported by Delft University of Technology (Faculty of Technology, Policy, and Management) and Bulgarian Academy of Sciences ("Supporting Young Scientists" Programme).

REFERENCES

[1] 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).

[2] American Red Cross, 2015. Drones for Disaster Response Relief Operations Study. American Red Cross, USA.

[3] AWARENESS, 2008. Freeband AWARENESS Project. http://www.freeband.nl.

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

[5] Dietz, J.L.G., 2006. Enterprise Ontology, Theory and Methodology, Springer. Heidelberg, 1st edition.

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

[7] European Emergency Number Association, 2015. Remote Piloted Airborne Systems (RPAS) and the Emergency Services. Europ. Emergency Number Assoc., Belgium.

[8] Friedman, B., 1996. Value-Sensitive Design. In ACM Interactions Magazine 3(6): 16-23. Association for Computing Machinery Publishing.

[9] Friedman, B., Borning A., 2002. Value Sensitive Design as a Pattern: Examples from Informed Consent in Web Browsers and from Urban Simulation. In DIAC'02 Directions and Implications of Advanced Computing Symposium. CPSP.

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

[11] Gambold, K., 2011. UAS Access to National Airspace. Technical & Air Safety Committee GAPAN, USA.

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

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

[14] Hristozov, S., Shishkov, B., 2017. Usability Assessment of Drone Technology With Regard to Land Border Security. In BMSD'17, 7th International Symposium on Business Modeling and Software Design. SCITEPRESS.

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

[16] Janssen, M., Kuk, G., 2016. Big and Open Linked Data (BOLD) in Research, Policy, and Practice. In Journal of Organizational Computing and Electronic Commerce 26(1-2): 3-13. Taylor & Francis, USA.

[17] Kolev, Z., 2014. RPAS for European Border Surveillance – Challenges for Introducing RPAS in an Operational Context Land Border Surveillance Domain. Blyenburgh & Co, France.
[18] Kolev, Z., 2013. RPAS for European Border Surveillance – Challenges for Introducing RPAS in an Operational Context. Blyenburgh & Co, France.
[19] Lacher, A., Maroney, D., 2012. A New Paradigm for Small UAS. Published by the MITRE Corporation, USA.
[20] LBS, 2012. LandBorderSurveillance, the EBF, LandBorderSurveillance Project: http://ec.europa.eu.
[21] Menthe, L., Hura, M., Rhodes, C., 2014. The Effectiveness of Remotely Piloted Aircraft in a Permissive Hunter-Killer Scenario. Published by the RAND Corporation, USA.
[22] NATO, 2017, the website on the North Atlantic Treaty Organization, NATO: http://www.nato.int.
[23] Nedyalkov, D., 2012. Concept for Air Surveillance and Reconnaissance with UAS. Ministry of Defence of Republic of Bulgaria, Bulgaria.
[24] Roberts, J., 2005. Agency Theory, Ethics and Corporate Governance. Advances in Public Interest Accounting, Emerald Group Publishing.
[25] Shishkov, B., 2017. Enterprise Information Systems, A Modeling Approach, IICREST. Sofia, 1st edition.
[26] 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.
[27] Shishkov, B., Mitrakos, D., 2016. Towards Context-Aware Border Security Control. In BMSD'16, 6th International Symposium on Business Modeling and Software Design. SCITEPRESS.
[28] 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.
[29] Van den Hoven, J.,Vermaas, P.E., Van de Poel, I. (Eds.), 2015. Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains. Springer Verlag.
[30] White, F., Hollingsworth, K., 1999. Audit, Accountability and Government. Clarendon Press.