MULTIDRONE –
MULTIple DRONE platform for media production

Project start date: 01.01.2017
Duration: 36 months
Lead contractor: Aristotelio Panepistimio Thessalonikis (AUTH)

Deliverable D2.4: Regulatory, security, technology, privacy and legal issue monitoring. Risk assessment and mitigation report

Date of delivery: 31 December 2018

Contributing Partners: Alerion, AUTH, IST, USE, DW, Thales
Version: v4

Title:	**D2.4: Regulatory, security, technology, privacy and legal issue monitoring. Risk assessment and mitigation report**	
Project:	**MULTIDRONE** (ICT-26-2016b RIA)	
Nature:	Report	**Dissemination Level:** PU **(PU**blic**, CO**nfidential, only for members of the consortium**, EU-RES** Classified RESTREINT UE**, EU-CON** CONFIDENTIEL UE **EU-SEC** SECRET UE**)**
Authors:	Grégoire Guerout (AlR), Nico Heise (DW), Rita Cunha (IST), Bruno Guerreiro (IST), Damien Lavaux (Thales), Vivi Nousi (AUTH), Ioannis Mademlis (AUTH), Vassilis Mygdalis (AUTH), Arturo Torres (USE)	
Lead Beneficiary:	Alerion (AlR)	
WP	2	
Doc ID:	MULTIDRONE_D2.4.pdf	

Document History

Version	Date	Reason of change
1.0	19/12/2018	Complete draft
2.0	19/12/2018	Final draft for internal review
3.0	20/12/2018	Revised version including internal reviewer's comments
4.0	21/12/2018	Final version to be submitted to the EU

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Table of contents

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Executive Summary

This report will analyse the technology monitoring linked to the MULTIDRONE system, hardware and software, following by the operational changes for UAV flights, broadcasting and privacy. This deliverable covers the risk assessment in regulatory, security, safety, technological and privacy aspects of the MULTIDRONE project and the presentation of the adaptations to mitigate the possible impact of the elements examined on the MULTIDRONE project.

The MULTIDRONE system has been designed and is detailed extensively in D2.3. The choices of technologies and components were the results of requirements, compromises, and availability on the market. Technology is generally progressing at a high pace, and new generation of products arrive with a hope to replace the previous generation. In the case of MULTIDRONE, some components evolved with better features. However, these new products do not meet all the requirements discussed between the partners. As a result, there are no changes in the list of components for the MULTIDRONE system.

The system safety and security are very important for the project. An analysis of the needs in terms of technical safety and operation safety was performed, as well as a description of the possible risks in terms of security of the full system MULTIDRONE.

As a European project, MULTIDRONE relies on the regulations from the partners' countries and from the European regulation. Regarding drones, each European country has their own rules. In order to simplify the drone flights across Europe, a European regulation will be released soon to give a standardised framework to the whole Europe. Before this day, national regulations still apply, and some amendments took place since the beginning of the project, especially in France.

Drones being rather new in media productions, a manual of good practices was created in this project to present all the flight operational rules adapted to the media production context.
With the entry into force of the GDPR European regulation in 2018, the MULTIDRONE project analysed the implication of the regulation evolution on its practices.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

1. Introduction

The MULTIDRONE project aims to develop an innovative system based on a swarm of drones in order to pioneer the media production applications dedicated to covering outdoor sports events. To this end, the MULTIDRONE system was designed using the state-of-the-art technologies to meet the requirements from the broadcaster partner DW and RAI detailed in D2.1, added to safety and security systems and following the regulations in drone design and operations. Moreover, the MULTIDRONE project goal is to develop a drone swarm based system to cover different types of scenarios such as a rowing competition or a cycling competition. The system is designed to fit the three scenarios by answering their operational and regulatory needs.

The drone environment and ecosystem are changing rapidly especially in terms of technology, services provided by the drones, but also regulatory. The change is even more noticeable due to the wide range of new applications using drones. To illustrate, the choice of a technology, that cannot be developed internally, depends on the state-of-the-art technologies available on the market, but it also needs to be compliant to the existing regulations on drone design. The same applies to radiocommunication technologies. On top of the technologies and the regulations, processes may evolve as well following worldwide trends. Moreover, the MULTIDRONE system will be used to film outside sports events with athletes and an audience, privacy needs to be considered seriously following the regulations and the rules of common sense, on top of the broadcasting regulations and practices.

This deliverable focus on the risk assessment and the mitigation of the regulatory, security, safety, technology, privacy aspects of the MULTIDRONE project introduced above. To do so, it will display the regulatory, safety, security and privacy concerns that can have an impact on the requirements of the MULTIDRONE system.
It may describe the evolution of the technological state-of-the-arts if the current technological choice does not allow to meet the requirements documented in D2.1, and the new technology may help to meet them. It will not describe all new developments in the aspects mentioned above but only the ones that are relevant or linked to the MULTIDRONE project.

The present document will start by giving a general overview of the scope of investigations for the technology monitoring performed. The document will then focus on the technological evolution that has an impact on the project, followed by a monitoring of the safety and security features of the system. The operational side of the project will come after by detailing the flight regulations across Europe, the broadcasting and privacy regulations and rules.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

2. Overview

Legal, ethical, safety and security issues arise upon scheduling professional UAV flight sessions, implicitly imposing challenging constraints on the shooting mission. Restrictions deriving from flight regulations, from data privacy rules and, finally, from safety and security considerations are described below, accompanied by corresponding technical solutions.

Different flight regulations apply depending on employed UAV types and their application. The regulations in many countries impose restrictions to the employed UAV weight and permitted flight radius, while also defining special prerequisite conditions (e.g., licensed pilot requirements and insurance policies). An important issue is that flight restrictions vary over different countries, while professional pilot licences and insurance policies may not be internationally valid.

UAVs are typically classified into different categories, depending on their weight. Adjusting/replacing components may impact the category classification. For instance, UAVs exceeding 2 kg of weight may be required to carry emergency parachutes in some countries. Flying UAVs exceeding 15 kg of weight might require special licence or even be prohibited. Maximum drone flight altitude is typically restricted to 400 ft or 500 ft (120 m or 150 m) within several European countries. Visual Line-of-Sight (LOS) should be maintained by the licensed pilot of the UAV, either physically, or using visual aids (e.g., VR-goggles), while the horizontal distance between the drone and the pilot may be limited to specific metres (e.g., 500 m).

In addition, due to safety considerations, outdoor UAV flight in most countries is restricted above congested areas, crowds of people and airports, leading to permissible flight zones delineated by law ("geofencing"). Inherently complying with such a complex and varying web of regulations is a challenge for all automated UAV applications.

Although UAV shooting in controlled and/or indoor settings (e.g., TV/film content) does not entail privacy considerations, privacy is an important issue in generic outdoor filming (e.g., sports or entertainment event coverage, newsgathering, etc.).

For instance, although it is intended to depict the athletes in a race, footage clearly showing the faces of nearby spectators is a prime candidate for raising privacy concerns. Capturing such footage is nearly unavoidable with UAVs, due to the wide scene portion captured by UAV-mounted cameras, as well as to their enhanced on-the-fly and in-the-field deployability.

Legal restrictions in various countries limit, or entirely prohibit, the redistribution/broadcast of footage which violates privacy guidelines. Such guidelines are already part of the current legal framework in many parts of the world.

A comprehensive example is the European Union, where the General Data Protection Regulation (Regulation (EU) 2016/679), updating and superseding the Data Protection Directive from 1995, explicitly states: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data." Such regulatory frameworks typically treat facial images as potentially identifying biometric data, thus restricting their and making their protection a necessity.

Therefore, compliance with data privacy legislation is an issue that must be taken into account in autonomous UAV shooting scenarios. Privacy protection methods for face de-identification, face detection obfuscation algorithms, or even soft/non-biometric identifiers (e.g., tattoos, skin marks, etc.) protection methods, can be employed to ensure privacy legislation compliance.

During M1-24 of the project, AUTH surveyed the current ethical/legal/safety and operational/production challenges inherent in the field, so as to present the corresponding state-of-the-art technological solutions and to showcase their limitations. This overview has been published in the form of a conference paper titled "Challenges in autonomous UAV cinematography: an overview" and presented in the IEEE International Conference on Multimedia and Expo (ICME), in July 2018 [MMNP2018].

3. Technology monitoring

This section is to address the technological evolution that can have an impact on the D2.1 requirements, on the regulation evolution in each part, and practices evolution. Technologies are evolving fast, and some that were not available at the beginning of the project may be now affordable but require another integration.

The drones of the MULTIDRONE project were designed following the system platform requirements presented by DW and RAI in the deliverable D2.1. Each of the requirements were marked with a priority level. The functional requirements were then converted into technical specification requirements and a selection of the ideal equipment, sensors and computers was established. Due to the drone constraints, as well as the budget and other requirements, a drone platform was then proposed as a compromise of all the requirements from all the partners. The main components such as the camera, the on-board computers, the lidar had to be off-the-shelf components, lightweight, within the budget, with a controllable interface, and with technical specifications that meet the main functional requirements.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

3.1 Solid State Lidar

One of the most evolving technologies at this moment is the Solid State Lidar. Though there were several manufacturers offering this at the beginning of the project, new models with better specifications came out to the market. However, the major application of this technology is in the automotive sector, since Lidars are very important sensors for autonomous cars. Thus, the relevant products are mostly designed for placement on cars and not on drones.

The Solid State Lidar technology is in a good shape in terms of 2D lidars (with a small vertical field of view, around 7º). On the other hand, 3D Solid State Lidars are not in the same page. Some models are being tested by big automotive companies, and several manufacturers promise to start selling them in the first half of 2019. Thus, the MULTIDRONE choice is still valid at this point, though probably next year there will be lighter and cheaper Solid State 3D Lidars.

3.2 Cameras

Cameras (still /video) form a very competitive market sector with significant developments every year. Within this sector, drone cameras form a niche but promising market sub-sector. However, the MULTIDRONE project requirements with respect to cameras are quite specific and thus significantly narrow the possible hardware choices. The camera to be placed on the project UAVs needs indeed to provide cinematographic quality with an accessible API, and specific recording functionalities, such as H264 video encoding, being also able to record in raw format in the SD card. The detailed specifications are noted in the D2.1.
The broadcasting requirements, and the size /weight constraints imposed by the on-drone placement, guided the consortium in selecting Blackmagic Micro Cinema Camera [BMCC] that met most of the criteria. Since this choice, no camera with an acceptable broadcasting quality, a control API, and with a very compact form factor has been released. As a consequence, the choice of the Blackmagic camera is still valid.

3.3 Energy Source

The energy source of the drone is one of the aspects that has the least progress. Most of the multirotor drones such as the MULTIDRONE ones are based on batteries using the Lithium Polymer (LiPo) technology. This technology, beside being very popular in drones, is a compromise between the cost, the equipment compatibility, the life cycles and the capacity available on the market. The gravimetric energy density remains low, especially compared to gasoline.
Some companies are now starting to provide cells using the Lithium-Metal technology. This kind of cell promises a higher gravimetric energy density to 450wh/kg. Nevertheless, companies are currently only providing cells and not batteries. Using such batteries in the project would require actually building the batteries out of the provided new technology cells. Moreover, the cost is expected to be higher than that of LiPo batteries proposed in the first version of the platform design.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Hydrogen and gasoline engines with their associated tank are rather large in volume, which contradicts the project requirement to have the smallest drone possible with regards to the payload requirement. Moreover, using this approach would add another layer of complexity.

As a result, the MULTIDRONE system will keep using the LiPo technology for its power source.

3.4 Onboard GPU

In June of 2018, NVIDIA announced the launch of its next generation embedded processing module, the Jetson AGX Xavier [XAV2018]. It is equipped with a 512-core Volta GPU with Tensor Cores, whereas the Jetson TX2, which is the current project selection for onboard GPU, has half the cores (256 CUDA cores, Pascal microarchitecture). As for the CPU, Xavier comes with a 8-core ARMv8.2 64-bit CPU, whereas the TX2 has six cores in total. However, the use of the Xavier module presents several difficulties. Although the developer's kit is quite minimal, it requires double the volume compared to a Jetson TX2 coupled with the Auvidea J140 board. In addition, the Xavier development kit weighs about 630 grams, which is about 3 times as much as the Jetson TX2 module weights. Furthermore, due to its recent release as well as the fact that the kernel provided by NVIDIA is different from the one provided for the TX2, there has not been much progress made in terms of developing software for it, for example for video streaming purposes. Moreover, the official supported version of Ubuntu is 18.04, which severely complicates the installation of ROS Kinetic (ROS version selected for the project). Although ROS Melodic can be installed without difficulties, other problems may arise the use of different ROS distributions on the Xavier and on the other modules of the MULTIDRONE system. Finally, the Xavier Module power consumption is higher than the TX2. According to Nvidia, TX2 has a power consumption of 7.5 W (Max-Q mode) whereas the Xavier module has at least 10 W and the default power consumption is 15 W+. This change in terms of drone power consumption from the computing systems may have a measurable or significant impact on UAV flight time. Thus, after thorough investigation into the use of the Xavier module, it was deemed unsuitable, mostly due to its developmental immaturity and OS incompatibility with the rest of the modules.

3.5 Platform

A general definition of drone platform would include the frame, the propulsion systems and required electronics necessary for the drone normal operations. The market of these products is slightly different now that before. Drones manufacturers are now more focusing on selling all-in-one drones, rather than drone parts, and especially drone platforms. For that reason, the number of possible high-quality drone platform is reducing. Custom-made platforms proposed by small manufacturers exist as before. They are, however, often more expensive, and the maintenance is more complicated, than the major providers. If a spare part is needed, a new custom-made one needs to be produced. Major manufacturers have industrialised the


This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

process, allowing to propose cheaper spare parts. Since the beginning of the project, no new drone platform has been released from the manufacturers known to propose high quality platforms. Ideal platforms for the MULTIDRONE project are still too expensive with regards to the budgeted cost of each drone. The compromise found between partners concerning the choice of the payload is still relevant today. It is based on the payload choice, from another perspective, the weight and power consumption of the components, the desired flight time, the budget and the drone size. As a result, the drone platform chosen for the MULTIDRONE project remains the one detailed in the deliverable D2.3.

3.6 Conclusions

As presented above, the technologies have made progress since the beginning of the project. New products were released with new technologies or providing more functionalities. However, the MULTIDRONE system has specific requirements, especially due to the constraints in building drones which are aerial systems. The new products available on the market do not fit with the platform requirements within the remaining time scope of the project.

4. System Safety

The MULTIDRONE system is composed of drones and will be used to film sports events. The safety of a system comprises and is affected by a multitude of elements from low level safety in the electronics and software modules of the drone to the operational safety. System safety can also be generic or scenario specific. This section will focus on the general safety systems that can be used in all cases. On the technical side, the MULTIDRONE system needs to have reliable systems where issues can be avoided or detected if possible. On the operational side, processes are set up to add safety to the operation.

4.1 Technical safety

The goal of a system's technical safety is to prevent possible technical failures. These can come from hardware, but also software. Also, the impact of failures can range from minor up major/severe, such as a drone crash. This is the reason why the criticality of the systems that are being designed or implemented is important for the level of safety that is needed. The MULTIDRONE software system is composed of several modules that operate together and communicate, as described in deliverable D2.3 about software specification. They are designed by different partners of the project. As a consequence, the overall safety of the system relies on the safety of each part and module, especially the critical ones such as the autopilot, the scheduler or the action executer, and on the communication between them.

The main issues that can occur and thus need attention so as to avoid safety-critical failures are the software logic errors such as coding errors, the software support errors such as a compilation error, and the hardware failures.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Since the various software modules are being developed by different partners, a good cooperation is vital to ensure the compatibility and proper synergy of each module with the rest. Off-the-shelf modules incorporated in the system shall ideally be certified to ensure their reliability, but not many modules of this kind exist. Open source software modules can be found more frequently. They do not have a safety certification, however the majority of them are validated in terms of proper functionality by the respective community and any identified flaws are patched. To ensure a high enough safety record for the included modules, extensive tests including SITL and HITL ones are performed by the consortium to detect potential failures before adding them to the drones. These steps are part of the integration process and detailed in WP5. Obviously, a significant number of tests will be performed once the drones are ready, taking all necessary safety precautions for the test flights environment, to ensure a proper and safe operation.

Procedures for the software modules regarding their inner safety and the communications between the modules were detailed in Deliverable D2.3. On this document, for each module, a presentation of the impact on the system safety for each sensible interface was performed. At this moment of the integration process, the safety procedures defined in D2.3 are still valid and applicable, without changes, to the system's software modules. Once the system is finished, safety checks can detect if all modules are behaving as they are supposed to do and send the result to the pilot.

The system safety also depends on the hardware, and especially on the drones components. More than the safety alone, the drone hardware safety often also implies availability and reliability, getting closer to the notion of dependability rather than the simple notion of safety. The hardware safety relies on the mechanical, electrical and mecatronical safety and reliability. The drone components in today's market are rarely accompanied by a quality certificate that provides safety/reliability-related information. Some components, such as some motors, do provide data that can be used to estimate the quality, and thus the safety of the product. These are, however, not common within the budget range of the MULTIDRONE drones. Theoretical studies during the design as well as testing using an appropriate context helps in testing the safety of the system.

4.2 Operational safety

The operational safety is a second level of safety, complementing the technical one. This one focuses on the mission of the drone and not its internal safety. In order to have a safe mission, the drones have to keep their integrity, but also be safe for the people in the area of the flights.
In order to allow a safe drone operation, they are not flown in adverse conditions such as wind and rain. These specific elements are checked/planned before the time slot to operate the drones and for the specific location. Moreover, as is obvious, pre/post flight checks (see deliverable D8.1) are performed and all flights will be conducted by strictly following the applicable flight regulations, which are mainly aiming towards increasing safety. On top of that, the entire MULTIDRONE system will be insured for damages to third parties (humans, property), for the unlikely event of an accident.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Besides this process, the drones should avoid crashing to an obstacle during flight. Each drone is equipped with a module in charge of detecting and avoiding possible collisions with other drones or obstacles. It is aware of the current positions and velocities of the other drones. Moreover, drones have a front facing Solid State Lidar that can detect obstacles 50 metres ahead. As stated in section 3.1, the new 3D Solid State Lidars coming in early 2019 may improve the obstacle detection both in accuracy and in terms of the detection angle. However, the current solution is enough for ensuring the safety of the system in the foreseen scenarios.

In order to have the safest flight, especially when flying in the presence of people, the MULTIDRONE system takes into account both pre-defined and automatically detected no-fly zones. It is able to calculate a safe path to move through the environment flying only over allowed areas. The drones will also have a geo-fencing implemented. The crowds will also be avoided using a crowd detection system that will be able to localize the (constantly updated) detected crowds on the 3D map of the environment (see deliverables D4.1 and D4.2).

The MUTLIDRONE system is a prototype system. Due to this fact, and due to regulations, pilots and supervisors will be present to take control of the system if something not planned happens and if the system has difficulties in handling the situation. The Supervision Station which is the main system element that is related to safety, is expected to play a critical role in this.

There is also an ongoing research and development effort in the consortium to implement new strategies for drone replacement in formation flight, with minimum impact on the shooting activity. In this way, the MULTIDRONE system can account for pre-planned replacement of drones throughout a mission to increase the endurance of the overall system. Moreover, when the energy of a drone unexpectedly goes below a given threshold, a replacement manoeuver can also be triggered to deal with this emergency scenario.

5. System Security

A drone is a complex system and can be vulnerable to unsolicited commands if not protected in an appropriate manner. Attacks can be focused on any part of the system. The system security needs to be designed as a whole.

As an unmanned aerial vehicle, the only links to a pilot are wireless communications. A special attention needs to be inclined toward the security of theses communications to make sure that the drones will only respond to the MULTIDRONE commands. The drones are unmanned vehicles flying to film sports events in the MULTIDRONE project. They are at the same time the tool to provide images for the production team, but also systems with only wireless links for the control the drones from the ground station.

Three main categories of attacks can be identified: the attackers have a physical access to the drone, the attackers can provide a malicious program to alter the behaviour of the drone, but also to take the control of the drone while in flight.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

5.1 Physical Access

While the MULTIDRONE system is on the ground, a malicious person who has access to the physical hardware could perform sabotage on any of the equipment present on the ground. This person would also be able to upload a malicious software more easily. The following section will present more in detail the malicious program risk analysis and the possible mitigation.

In order to avoid an intruder to have access to the physical equipment, only trusted people should have access to it. This applies in each partner facilities as well as during outside experimentations and demonstrations.
Each partner has their own rules regarding protection of equipment and access to computers, servers and storage systems in and outside their facilities but under each partner responsibilities.
The tests and demonstrations of the MULTIDRONE project will happen with some or all the partners. For that reason, the access rules need to be agreed by all partners.
The protection can have several layers of security depending on the event and the probability to have someone outside the partner coming. For instance, the flight tests can be run in a controlled environment dedicated to tests. Only trusted people can have access to these locations. During a sports event, more people than the production crew, and the MULTIDRONE team can be present at these locations. So another layer of protection needs to be added.

For hardware equipment during tests and demonstrations, a restrictive area needs to be set up with an access control. The process to ensure the control of the access is proportionate to the environment. In places with a high probability to have a public, barriers and a security guard can be relevant. The specific location of the demonstrations are not defined yet, so are the specific ways to handle this category of risk.

The data can be stored on the drones, or the ground station, but also in storage infrastructure. As no direct control can be granted, trusted infrastructure is mandatory.

5.2 Malicious program

If an attacker manages to break into the restrictive area or find a way to implement a undesirable program to the MULTIDRONE system, another layer of security needs to be planned.
A malicious program could be analysing private data collected during the MUTLIDRONE project, up to changing a software modules responsible in the command and control of the swarm of drones. This situation could be responsible of a drone crash.

Anti-tampering mechanisms can be used to prevent reuse of drones or ground infrastructure.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Concerning control hacking, secure and signed firmware updates can help avoid hacking of the autopilot. This way the drone will be running a verified autopilot that will prevent unpredicted behaviour.

5.3 Wireless attacks

5.3.1 Security analysis: LTE for ground-to-UAV / UAV-to-ground communications

The following security analysis aims to list LTE threats and vulnerabilities identified in the literature, their impact on the ground-to-UAV – and UAV-to-ground communication link, and the potential barriers to mitigate potential attacks.

LTE threats, vulnerabilities, and their implications to MULTIDRONE's UAVs communications

In the literature, there is already a substantial amount of work that has analysed the security and privacy of telecommunication systems. Most precisely, Hussain et. Al [HOS2018], analysed security and privacy of the three critical procedures of the 4G LTE protocol (i.e., attach, detach, and paging), and in the process, uncover potential design flaws of the protocol and unsafe practices employed by the stakeholders.

The following tables presents a summary of threat intrinsically related to LTE procedures and their implication on our considered UAV scenarios and are based on the Hussain et. Al paper [HOS2018].

Table 5.1: Attacks against LTE Attach Procedure

Attack name	Adversary assumptions	Standard/ Stakeholder slip-up	Implications for UAVs communications	Operational mitigation	Evaluated risk level
Authentication Synchronization Failure Attack	Known IMSI, malicious UE	3gpp	High impact if successful. Denial-of-attack of the drone to the ground station, or Denial-of services	Automated flight procedures (as if link unavailable)	Very low

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Implications for UAVs communications: The major implication of this attack is the service disruption suffered by the victim UE of the considered UAV. No Data is able to be transmitted between the UAV and the ground in both uplink and downlink.

Operational mitigation: Automated flight procedures should be taken when this attack occurs as the produced effects are identical to link unavailability)

Evaluated risk: The risk is considered very low, as it requires setting-up a malicious UE in very close proximity of the target UAV. There is a very low probability that an malicious attacker can be successful in flying an identified drone close the target MULTIDRONE UAV without the pilot of the target to visually notice the attack. Moreover, it is required to know the victim UE's IMSI for the attack to be exploitable. Set-up is very unpractical for attackers.

Table 5.2: LTE UE Traceability Attack

Attack name	Adversary assumptions	Standard/ Stakeholder slip-up	Implications for UAVs communications	Operational mitigation	Evaluated risk level
LTE UE Traceability Attack	Valid security mode command, malicious eNodeB	3gpp	Very Low if successful. UAVs UE can be tracked	None required	Very low risk Practical complexity

Implications for UAVs communications: This attack enables an adversary to track a particular UAV thanks to its embedded LTE UE.UE. In the considered MULTIDRONE use-cases for UAV communications, these implications have very low impact, as tracking of publicly deployed UAVs have no consequence on safety, security and integrity of control commands and payload.

Operational mitigation: no mitigation required.

Evaluated risk: Very low risk due to unpredictability to setup a rogue flying accepts point. Moreover, it is required to know the victim UE's IMSI for the attack to be exploitable. Set-up is very unpractical for attackers.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Table 5.3: Alter: LTE user data manipulation attack

Attack name	Adversary assumptions	Standard/ Stakeholder slip-up	Implications for UAVs communications	Operational mitigation	Evaluated risk level
Alter: LTE user data manipulation attack	malicious MitM relay	3gpp Lack of Integrity Protection	Very high User Data Redirection means all traffic that is send/received by the UAV can be modified and/or redirected (via DNS spoofing)	E2E encryption with AES 256 5G integrity protection	Low

Implications for UAVs communications: Very high impact for UAVs is expected. User Data redirection means all traffic that is send/received by the UAV via the LTE link can be modified and/or redirected (via DNS spoofing). If successful, the attacker can then spoof the commands, and/or payload traffic send to UAVs.

Operational mitigation: One proposed solution to protect from such an attack is to cypher all drone traffic at user-level. It means adding a security layer (such as AES 256 encryption) on top of LTE intrinsic own encryption. This should apply to mission-critical data such as UAVs data commands.

Evaluated risk: The risk is considered extremely low. It requires the attacker to not only fly a rogue base station very close to the target (highly impractical) but also equip this rogue flying UAV with a full-stack LTE Base Station (tens of kilogram minimum) to be somehow connected to a ground IP infrastructure via additional radio links. This is considered extremely unfeasible given current technology for a mid-sized drone.

5.3.2 Security analysis: 868 MHz radio link for ground-to-target / target-to-ground communications

The target hardware is responsible for collecting information on the position, orientation and velocity of the target, based on GNSS and inertial measurements, and relay them to the ground station for ground truth or as an additional measurement that can complement the

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

vision-based data obtained from the drones. RTK GNSS corrections are also sent to the target's GNSS receiver for higher accuracy of the positioning solution. As these modules are usually not in the critical path for the MULTIDRONE functions, and the weights and dimensions must be as low as possible to mitigate the influence on the athletes' performance, a 868 MHz radio link is considered. This radio link can be configured for synchronous/asynchronous communications in a fixed two-way link or in a mesh network (where the destination node might not be visible to the source node). Additionally, the data transferred through this communication link can also be encrypted for increasing security.

6. Flight regulations across Europe and standards

While the national regulations changed since the beginning of the project, the pace of new regulations has decreased due to the approaching European regulation on unmanned aerial systems. The day of the new regulation is currently unknown and the details are not set.

This section will focus on the regulations of the countries where the main flights will be performed, both the flight tests and the demonstrations. Most of the integration flight tests will be run around Alerion premises who is the partner designing and building the drones. As for the demonstrations, they will be happening either in France, in Germany or Italy depending on the location of the sports events that will be followed. The evolution of the regulations of France, Germany and Italy will be detailed in this section, as well as a monitoring of the European regulation which is currently under development.

The French regulation is the one that has evolved the most compared to the German and the Italian ones during the last 24 months.

6.1 France

The French regulation evolved quickly. The presentation of the status of the French regulation at the beginning of the project is detailed the deliverable D8.1.

In 2017, an arrêté integrates the possibilities to flight by night and some restricted areas after authorisations by the local authorities. This should not affect the MULTIDRONE Project.

Since July 2018, a set of new decrees comes into effect. Some of these regulations come into effect on the 1st of January 2019 if the drones were registered before the 1st of July 2018.
The drones above 800 g have to be registered on the official website. Details including the type of vehicle, its mass, the manufacturer, the serial number, camera sensor, presence of an autopilot, the details of the owner (natural or legal entity).
A UAV above 800g must have a system to limit its abilities and make impossible flying over 150 m. The altitude of the drone must be available to the pilot. (Dispense for experimentation)
A UAV above 800 g must have an audible warning activated by the pilot and in case of an automatic emergency landing. (Dispense for experimentation)

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

The pilot exam has been revised now dedicated to drones and multirotors.
A decree about adding a digital ID transmitted wirelessly is being developed and should have come into action in the same period as the regulations above. However, due to technical discussions, and the approach of the European regulation, this regulation is postponed.

These new regulations have a limited impact on the MULTIDRONE project. The drones are prototypes and the operations that are the tests and the demonstrations are experimentations. The drones must comply with the registration regulation. However, as the drones will be automatic and one of the aims of MULTIDRONE is to deliver a safe and reliable platform, the area, including the altitude will be limited and each drone will have a buzzer that will be used in case of an emergency landing.

6.2 Germany

The German regulation about UAVs has a little evolution since the beginning of the project. The D8.1 details the rules to follow when flying a drone in Germany.

Since then, from the 1st of October 2017, a fireproof identification tag is mandatory on the drones. This point is similar to the French rules, on the difference that the needs to be fireproof in Germany. Since the same period, the certifications required for the German drone pilots evolved, for drones above 2 kg, the pilots need the take a pilot exam, and if the drone is higher than 5 kg, the pilot needs a licence to be able to fly the drone.

As the German regulation towards identification tags is more constraining compared to the French one, the identification tags used during the MULTIDRONE project will be fireproof.

The drones of the MULTIDRONE project are above the 5 kg threshold. The German pilots will therefore need to have a licence to be able to fly the drones.

6.3 Italy

As the German regulation, the Italian one did not change drastically.
In March 2017, a new amendment was adopted clarify the competency of the Italian national aviation authority, the ENAC, in case of accidents linked to drones.

This new regulation has a very limited impact on the MULTIDRONE project as it only applies to the actions to run in case of a crash.

6.4 European Regulation

The European Union is very active to produce a regulation about all types of drones. The main goal is to have a Europe-wide regulation and processes to help the European market to develop and consolidate its drone industries by avoiding the need to apply multiple laws if the companies want to sell their products and services across Europe.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

A regulatory and strategic roadmap was handed over to the European Commission in 2013.

The New Basic Regulation of aviation was voted during the summer 2018 and entered into service in September 2018. This regulation shapes the aeronautics environment, and introduces the unmanned systems to the Basic Regulation. It mandates the European Aviation Safety Agency (EASA) to provide and supervise the technical aspects. The regulation provides as well the main specificities about the unmanned aerial systems and the operations using them.

A specific regulation on unmanned aerial systems is under development and is expected to be presented to the European parliament in the early 2019. The details of its application are not known.
This regulation is divided into a Delegated Act on technical requirements and an Implementing Act on operation and registration.

The regulation brings a risks-based approach to deal with the design and the operation of the drones. It uses the work of the JARUS group which produced the SORA methodology.

The SORA methodology is a tool to assess ground risks and aerial risks, and provides guidelines for technical and operational barriers implementation (such as parachute, human factor analysis, etc.).as well as mitigation.

The European regulation will be based on this methodology. However, this methodology is complex to set up. For that reason, standard operations are being discussed simplifying the flight authorisations. These standard scenarios are being elaborated by the EASA to simplify the work of the drone operators. If their drone operation is described in one standard scenario created, the drone operators will not have to run a risk assessment based on the SORA methodology, as the standard scenarios will already have one. However, there is a likelihood that the MULTIDRONE project will not exactly fit in one of the standard scenarios. The SORA analysis for the project will likely be able to be based on one existing standard scenario. The risk analysis will be developed alongside the demonstration planning and will take into account the standard scenarios when they will be released.
At the time of writing this report, the European regulation has not been released yet. The Delegated Act on technical requirements and the Implementing Act on operation and registration are in the form of drafts. The official documents, the dates of votes and the description of applications through the state members are not known yet.

These regulations, if they are in effect during the project, will have an impact on the procedures to have flights authorisations, and possibly on the mitigation procedures and technologies that have to be implemented on the drones. The aim is to implement the Delegated Act on technical requirements and the Implementing Act on operation and registration and the Standard Scenarios at the same time to simplify the setting up of the new regulations in each member state and by all the companies and organisations in the UAVs ecosystem.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

6.5 Other bodies: standards and recommendations

The way and processes to operate drones are not only shaped by regulations, but also from recommendations and standards from other bodies elaborated by experts. Alongside with the regulations bodies, the standards and recommendations bodies aim are to propose a common framework. JARUS and ISO are two non-regulatory bodies that work to this goal.

JARUS

JARUS (Joint Authorities for Rulemaking on Unmanned Systems) gathers regulatory bodies across the world to "recommend a set of technical, safety and operational requirements for all aspects linked to the safe operation of the Remotely Piloted Aircraft Systems (RPAS)" [JARUS]. JARUS has 7 working groups : Flight Crew Licencing, Operations, Airworthiness, Detect and Avoid, Command and Control, Safety and Risk Management, and Concepts of Operations. Their recommendations and guidance which results from the Working Groups are used by the EASA and the European Union to propose the European harmonised regulations for UAVs. As an example, the SORA methodology was developed by JARUS and promoted by EASA as a methodology that can be used as reliable way to assess risks and mitigation of drone operations.

ISO

The ISO (International Organization for Standardization) is a worldwide federation of national standards bodies. The ISO has created a subcommittee dedicated to unmanned Aircraft Systems in 2014. It is working on 5 standards: General Specifications (ISO/CD 21384-1), Product systems (ISO/CD 21384-2), Operational procedures (ISO/CD 21384-3), Categorization and classification of civil unmanned aircraft systems (ISO/CD 21895), and UAS Traffic Management (UTM) (ISO/AWI TR 23629-1). Beside the UTM standard which is in the preparatory stage, the other ones are more advanced. The standards about the General Specifications, the Product systems and the Categorization and classification of civil unmanned aircraft systems are in the Committee stage, and the Operational procedures standard is already to the next phase, namely the Enquiry stage.

The ISO standards are not regulations. They can, however, give a framework to all the countries in the world who have already or not specific regulations for drones. It also provides a guide for good practices that are not mentioned in regulations. The first standards are expected to be adopted late 2019. The versions under development can provide ideas to improve the MULTIDRONE system and processes if necessary.

7. Broadcasting

Drone cameras are a rather new means of production in media companies. Therefore, the legal and administrative framework is often still under development. Companies need to

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

choose the most suitable technology, take out the necessary insurances, train pilots and follow a number of other rules and restrictions.

In the framework of MULTIDRONE, DW has developed a drone manual containing basic rules and checklists that serves as a basis for drone operations within the project but also for further usage regarding DW media productions. The manual also can contribute to developing standards for media companies in Europe (EBU).

It is the purpose of the DW manual to facilitate the use of camera drones in a safe and successful manner. It names and describes a number of essential requirements that users need to observe when flying drones. These include (to name just a few):

- the pilot's formal qualification,
- knowledge about the relevant drone and aviation laws as well as other regulatory requirements,
- regular technical checks of drone and camera,
- the observation of weather conditions.

The DW drone manual stipulates the top priority of any drone operations in media production which is the safety of uninvolved third parties as well as DW staff. Humans should under no circumstances be put to risk. If any danger occurs during production, the operation needs to be aborted immediately. Furthermore, DW staff should always take into account that many people are sceptical about or even scared by the deployment of drones. These reservations should be taken seriously - even if the actual operation is legally permitted.

The complete drone manual can be found as Appendix 1.

8. Privacy

8.1 Monitoring and analysis of the European data protection regulation

European data protection legislation

On December 7th, 2000, The European Parliament, the Council and the Commission proclaimed the Charter of Fundamental Rights of the European Union. Article 8(1) of this charter provides that

- everyone has the right to the protection of personal data concerning him or her, and that
- such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. It adds that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

In 2016, the EU passed a *General Data Protection Regulation* (GDPR) in order to further specify these fundamental rights (Regulation (EU) 2016/679). The regulation has come into effect on May 25th, 2018 and is since then directly applicable in all member states. The

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

GDPR regulates that any processing of personal data can only be based on the data subject's personal consent or a conclusive number of other reasons laid down by law. Furthermore, the GDPR introduces strict compliance rules for data controllers as well as severe sanctions in case of any violation of the regulation itself.

Personal data

Article 4 (1) GDPR defines "personal data" as *any information relating to an identified or identifiable natural person*(the 'data subject'). An identifiable natural person in this sense *is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*. There is a legal controversy about whether a person needs to be identifiable by the specific data controller in question (who could have restricted means and sources) or whether it is sufficient that this person is *theoretically* identifiable by someone. Data protection authorities (e.g. in Germany) tend to lean towards the latter view. A ruling by the European Court of Justice from 2016 also tends to a wide understanding of personal data by declaring *dynamic ip addresses* as personal data (Judgement of the Court of October 19th, 2016 in case C‑582/14). Therefore, and in order to not to take any risks, the consortium should consider any piece of information that could somehow be related to a specific data subject as personal data. This means that the consortium should treat even anonymised or pseudonymised information or any piece of information that could theoretically (e.g. by big data analysis) be related to a specific data subject as personal data.

Data processing

According to Article 4 (2) GDPR, "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This wide definition indicates that any dealing with personal data by the consortium should be considered as "data processing" according to the GDPR.

Data processing on the basis of personal consent

The most straightforward way for obtaining legal permission for the processing of personal data, is to ask for the data subject's personal consent (Art. 6 (1a) GDPR). However, during the research phase (e.g. big data analysis, machine learning), it will be hardly possible to obtain personal consent from most of the individuals whose data might be involved. The same refers, in general, for media production. It might be possible to obtain consent from the protagonists (the athletes themselves), but it is very unlikely that we will be able to distribute consent forms to spectators and other third parties. Therefore, it will be necessary to base the processing of personal data on other legal grounds.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Data processing on the basis of legitimate interest

In order to facilitate lawful data processing in at least some of these cases, Article 6 GDPR provides a *conclusive* enumeration of additional legal grounds. Article 6 (1f) GDPR for instance, provides that the processing of personal data is lawful if it is

necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Scientific research activities might be considered as a legitimate interest that justifies the processing of personal data within MULTIDRONE. In fact, the GDPR privileges scientific research in a number of sections. For instance, data processing for archiving purposes in the public interest, *scientific* or historical *research purposes* or statistical purposes is generally not considered to be incompatible with the initial purposes (Article 5 (1b) GDPR). This means that scientific research remains possible even if it was not covered by the initial purpose and even if the data subject had not been informed about this option beforehand. Furthermore, this personal data may be stored for longer periods as long as the data will be processed solely for [...] scientific [...] research purposes (Article 5 (1e) GDPR).

On the other hand, these regulatory privileges for scientific research come along with specific and strict requirements that scientists and researchers need to observe. Especially Article 89 GDPR contains a number of safeguards relating to data processing for scientific research that aim for balancing out the fundamental rights to privacy and data protection, on one hand, and the freedom of scientific research on the other. Article 89 as well as the various other provisions in the GDPR lead to the following principles that need to be followed if the processing of personal data is based on the legitimate interest of scientific research (see *Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, DSGVO Art. 89, recital 32*):

- Datasets need to be *anonymised* before they can be processed for scientific research purposes. Only if the research purpose does not allow for anonymisation, the datasets should at least by pseudonymised. The risk of *re-identification* should be minimised as far as possible.
- The responsible researchers need to establish organisational and technical measures that safeguard a maximum of integrity, confidentiality, transparency, availability and resilience of processing systems and services.
- The processing of personal data for scientific research *without the data subject's consent* is only permitted if it is not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- Researchers are only entitled *to publish* personal data on the basis of prior personal consent.

In conclusion, research activities within MULTIDRONE might very well establish a legitimate interest in the processing of personal data. However, the consortium needs to take into account that the GDPR grants member states a considerable degree of flexibility to develop their own regulatory framework. According to Article 85 GDPR, member states shall by law reconcile the right to the protection of personal data pursuant to the regulation with

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

the right to freedom of expression and information, including processing for journalistic purposes and the purposes of *academic*, artistic or literary expression. Each MULTIDRONE consortium partner should therefore regularly check and analyse the legal situation in its specific country.

Data processing and journalism

In case of journalistic media production, data processing could be based on the so-called *media privilege*. The media privilege stipulates that journalists are not bound to data protection laws to the same extent as other parties. The background of this privilege is the fundamental principle of *freedom of the press*(see Article 11 (2) of the Charter of Fundamental Rights of the European Union). To research and verify information, to analyse and contextualise this information and to eventually publish it as news is the fundamental task in journalism. All these activities involve and actually depend on the processing of personal information and data. Consequently, journalistic work would not be possible if journalists had to observe data protection rules to the same extent as anyone else. The GDPR acknowledges this exceptional situation for journalists and the press in general by an opening clause in Article 85 (1) GDPR:

Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes.

This means that the consortium needs to refer to the law of the member states in order to assess the extent of media privileges in the context of data processing. In Germany, section 12 of the Press Code of North Rhine-Westphalia (Deutsche Welle is based in NRW) as well as Section 9c of the German Interstate Broadcasting Agreement specify the media privilege:

- Journalists are not entitled to use personal data that they have processed in the context of their work for other than journalistic purposes ("data secrecy").
- Journalists who process personal data need to be committed to observe the principle of data secrecy during and beyond their journalistic work.
- Journalists and the press in general are not obliged to observe the provisions of the GDPR apart from
    - the obligation to process personal data in a manner that ensures their integrity and confidentiality (Article 5 (1f) GDPR);
    - the obligation to install a data protection officer whose task is to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR (Art 24 GDPR);
    - the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This means, for instance, that Deutsche Welle is exempt from observing most of the GDPR's provisions *as long as personal data is processed for journalistic purposes*. However, as the experimental media production in MULTIDRONE as such will not be done for journalistic but for testing and evaluation purposes. The legal foundation for the processing of personal data will therefore be legitimate interest (scientific research). Additionally, personal consent might be an option. But the media privilege for journalists will be very relevant when it comes to an eventual further exploitation of the MULTIDRONE platform in a journalistic environment. In any case, the consortium needs to keep in mind that the media privilege might not exist in all countries or might vary considerably.

8.2 Technical means for privacy protection on UAV video footage

Within the MULTIDRONE project, interest in privacy protection methods arises from the requirements specified in Deliverable D2.1, since data collection during experimental media production involves capturing video footage of people. As unknowingly photographed individuals often wish to maintain their anonymity, companies which manage databases of such images opt for de-identification methods to provide this anonymity. This is now enforced, at least in the European Union, by the recent GDPR legislation. Therefore, a good practice would be to install privacy by design systems as close as possible to surveillance cameras, and even cameras used for entertainment purposes, such as those on drones, to ensure privacy protection.
As a person's face is amongst the most significant biometric features when it comes to person identification, both by humans, and by computers, typically face de-identification suffices for anonymity preservation. A standard de-identification method comprises face detection as a first step and blurring of the detected facial regions to achieve de-identification. Besides the fact that such blurring processes produce a visually unpleasing result, it has also been shown that such naive techniques can be defeated, for example via parrot recognition [NSM2005]. Thus, more advanced face de-identification methods, in terms of effectiveness and utility of the resulting images, must be investigated.
Perhaps the most advanced approach up to date is to exploit generative adversarial networks [SHK2017], attempting to generate synthetic samples from the distribution of all possible images that generated query segmentation. Besides face de-identification, this method can be extended for full-body de-identification in person images by also removing soft biometric and non-biometric identifiers. As another example, methods [AN2011] [TH2001] which de-identify not only the facial image but the entire person Region of Interest (ROI) has been developed. Furthermore, the aesthetic quality of the de-identified images can be improved with Machine Learning, which offers more sophisticated solutions than simple face blurring. With the recent advances of Machine Learning (ML) in face detection and recognition, face de-identification methods can become much more effective and efficient. Thus, de-identification methods can be better evaluated using learned face verification and recognition models.
Towards this end, UoB-AUTH jointly worked between M1-M6, developing a method that protects people's privacy in image/video data by hindering face detection. This method was described in a paper titled "Face detection Hindering", that has been presented in IEEE

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Global Conference on Signal and Information Processing (GLOBALSIP), Quebec, Canada, 2017, and can be found appended in deliverable D7.2. Moreover, parts of the joint UoB-AUTH work were extended in order to investigate de-identification against face recognition algorithms based on deep learning. A conference paper titled "Quality Preserving Face De-Identification Against Deep CNNs" that was accepted in IEEE International Workshop on Machine Learning for Signal Processing (MLSP), Aalborg, Denmark, 2018, summarises this work. Finally, AUTH worked on developing a lightweight de-identification method based on deep autoencoders, by fine-tuning the encoding part of a standard autoencoder to perform de-identification in the latent space. Since the developed methods involve image and video data processing, their technical descriptions and experimental results, was performed within the context of T4.3 MULTIDRONE Visual Analysis; thus it is included in Deliverable D4.2.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Published Papers

[MMNP2018] I. Mademlis, V. Mygdalis, N. Nikolaidis and I. Pitas, "*Challenges in Autonomous UAV Cinematography: An Overview*", Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), San Diego, USA, 2018.

References

[BMCC] Black Magic Micro Cinema Camera product page https://www.blackmagicdesign.com/products/blackmagicmicrocinemacamera
[JARUS] JARUS - Who We Are & What We Do, http://jarus-rpas.org/sites/jarus-rpas.org/files/storage/Library-Documents/jarus_who_we_are_what_we_do_v_8_0_210918.pdf
[HOS2018] Hussain, Syed & Chowdhury, Omar & Mehnaz, Shagufta & Bertino, Elisa. (2018). LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. 10.14722/ndss.2018.23319.

[NSM2005] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by deidentifying face images," IEEE transactions on Knowledge and Data Engineering, vol. 17, no. 2, pp. 232–243, 2005.
[SHK2017] Ivan Sikiric, Tomislav Hrkac, Karla Zoran Kalafatic, et al., "I know that person: Generative full body and face de-identification of people in images," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017, pp. 15–24.
[AN2011] Prachi Agrawal and PJ Narayanan, "Person deidentification in videos," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 3, pp. 299–310, 2011.
[TH2001] Suriyon Tansuriyavong and Shin-ichi Hanaki, "Privacy protection by concealing persons in circumstantial video image," in Proceedings of the 2001 workshop on Perceptive user interfaces. ACM, 2001, pp. 1–4.
[XAV2018] Nvidia JetsonAGX Xavier product page https://developer.nvidia.com/embedded/buy/jetson-agx-xavier

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Appendices

Appendix 1: DW Drone manual

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Appendix 1

Drone journalism and the use of camera drones in DW productions

Drone-Manual

Introduction

It is the purpose of this manual to facilitate the use of camera drones in DW productions in a safe and successful manner. The use of camera drones broadens the editorial portfolio, for instance by

- establishing new camera perspectives and a new kind of cinematography,
- enabling access to locations that are not accessible by common production technology,
- saving production costs (e.g. for a helicopter).

The top priority when using camera drones is the safety of uninvolved third parties as well as DW staff. Humans should under no circumstances be put to risk. If any danger occurs during production, the operation needs to be aborted immediately.

This manual names and describes a number of essential requirements that users need to observe when flying drones. These include (to name just a few)

- the pilot's formal qualification,
- knowledge about the relevant drone and aviation laws as well as other regulatory requirements,
- regular technical checks of drone and camera,
- the observation of weather conditions.

Furthermore, DW staff should always take into account that many people are sceptical about or even scared by the deployment of drones. These reservations should be taken seriously - even if the actual operation is legally permitted.

The manual only refers to the use of camera drones within Germany. Drone regulations in other countries sometimes diverge considerably from the legal situation in Germany and should be carefully checked before any drone operation. First information can be found here (in German): https://my-road.de/drohnen-gesetze-weltweit/

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

10 most important rules

The following list summarises the ten most important rules for the use of camera drones in DW productions. Please take into account that this list is not conclusive and will be further elaborated throughout this manual.

1. The safety of DW staff and third parties, especially their physical integrity shall under no circumstances be put to risk.

2. The pilot is solely responsible for the operation of the drone. Other DW staff, including directors and editors, are obliged to respect the pilot's decisions (including the decision to alter or abort the mission).

3. The pilot needs to present a drone pilot licence if the drone has a payload of more than 2 kg.

4. The operation of drones with a payload of less than 5 kg outside of restricted-flight zones does not require any official authorisation. However, the owners of the premises where the drone takes off and where it lands need to consent.

5. The flight conditions and the surrounding area need to be examined before each operation. This refers to eventual obstacles and other risks, weather conditions as well as to legal flight restrictions (e.g. no-fly zones). It also includes a thorough check of the technical equipment as well as an assessment of whether the pilot is fit to fly.

6. Drones with a payload of up to 5 kg are only allowed the be operated within the pilot's visual line of sight.

7. It is forbidden to approach human gatherings of more than 12 people by more than 100 metres.

8. It is forbidden to approach sensitive facilities (such as power plants, government buildings, conservation areas, motorways) by more than 100 metres.

9. It is forbidden to fly over residential properties unless the owner(s) has/have given their prior consent.

10. It is forbidden to operate drones during night-time without prior official authorisation.

Flight skills and internal training

Only DW staff that has been instructed and trained accordingly and that has been cleared in writing by the responsible DW department is allowed to operate DW camera drones.

In case of a payload of more than 2 kg, the pilot is obliged to present an official drone pilot licence. This licence is issued by specially authorised institutions and requires knowledge about

- the operation and navigation of drones,

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

- the relevant aviation regulations and the airspace management structure,
- meteorology.

The specific requirements for the training and the respective examination are provided by the German Federal Aviation Authority ("Luftfahrtbundesamt"). A number of private institutions such as the German Unmanned Aviation Association (UAV Dach e.V., http://www.uavdach.org) is entitled to carry out training and organise exams for acquiring the pilot licence.

Legal framework

Aviation law

In 2017, the German state has issued a new regulation regarding the operation of unmanned aerial vehicles. According to this regulation, the use of drones in DW productions needs to comply with the following key legal requirements:

1. Drones with a payload of less than 5 kg do not require any official authorisation. Payload is the combined weight of the drone and its load (e.g. camera).
2. The operation of drones with a payload from 5 kg to 10 kg can be based on a general authorisation by the responsible authorities. The operation of drones with a payload of 10 kg to 25 kg requires an individual authorisation for each mission.
3. The operation of drones with a payload of more than 2 kg requires that the pilot is able to present an official drone pilot licence. This licence is issued by specially authorised institutions.
4. Drones with a payload of less than 5 kg are only allowed to be operated within the visual line of sight unless the responsible authority has issued special permission. Optical aids such as screens, binoculars or VR goggles are not sufficient.
5. **Operations during night-time** with any kind of drones can only be performed on the basis of an individual authorisation and under observation of strict safety requirements.

6. It is **forbidden**
    a. to operate drones more than 100 metres above ground;
    b. to operate drones above residential properties unless the owner(s) has/have given their prior consent;
    c. to operate drones above or less than 100 metres from
        - human gatherings of more than 12 individuals;

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

- accident sides, hazardous areas and other operational locations of authorities or security forces;
- hospital borders;
- federal motorways, federal waterways and railways unless the responsible institution has explicitly agreed before the operation;
- mobile facilities and troops of the army during official manoeuvres and exercises;

d. to operate drones above natural reserves and national parks;

e. to operate drones above or less than 100 metres from the borders of industrial plants, penitentiaries and the like, military complexes and organisations as well as facilities for the generation and distribution of energy/electricity, unless the responsible institution has explicitly agreed before the operation;

f. to operate drones above or less than 100 metres from the sites of constitutional bodies of Germany or the German states, highest and high federal and state authorities, diplomatic or consular missions or of international organisations, unless the responsible institution has explicitly agreed before the operation;

g. to operate drones above or less than 100 metres from premises of the police or other security agencies, unless the responsible institution has explicitly agreed before the operation;

7. In substantiated individual cases, the responsible authorities are entitled to issue exceptional permissions regarding these bans on operation. The responsible authority is the aviation authority of the state where the drone operation will take place.
8. Drones with a payload of more than 0,25 kg are shall bear a fireproof badge identifying the name and the address of the drone's owner.

Copyright law, press law and privacy law

The operation of drones for the purpose of media production needs to comply with the usual requirements regarding copyright law, press law as well as privacy and other personality rights that journalists need to observe in production.

Due to the range of drones and the possibility to penetrate very private personal areas, DW staff is obliged to always operate drones with a high level of sensitivity and responsibility.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Copyright law in particular

One particularity of copyright law requires special attention: The filming of buildings or monuments that are protected by copyright can be permitted,

- if the building/monument can be considered as a "minor accessory" of the image/video that is not focused on and only depicted "on occasion";
- if the building/monument is depicted for the purpose of reporting current news affairs;
- if the media production is specifically dealing with and referring to this building/monument so that the depiction can be based on the "right of citation".

If none of these requirements are fulfilled, images/videos of protected buildings/monuments can also be based on the so-called *freedom of panorama*. According to the freedom of panorama, it is permissible to reproduce, distribute and make available to the public works located permanently in public roads and ways or in public open spaces. In the case of buildings, this authorisation shall only extend to the façade. The important restriction is that this privilege only refers to the view of the building/monument that is accessible for everyone (so-called "passer-by perspective"). Other perspectives, such as the filming of a building/monument that is protected by copyright law from the roof of a neighbouring house, from a crane or a camera drone generally requires the approval by the copyright owner (normally the architect).It is also important to note that the *freedom of panorama* privilege varies from country to country. French copyright law for instance, does not allow for professional and profit-driven usage of videos/images of protected buildings/monuments. These national restrictions and particularities need to be researched and taken into account when planning the production.

Insurances

Drone owners are obliged to take out third party liability insurance. A private liability insurance is not sufficient. Each drone that was acquired by DW needs to be insured via the DW legal department before usage. This insurance requires the following information:

Manufacturer:	e.g. DJI
Type:	e.g. Mavic Pro
Maximum payload:	e.g. 1,5 kg

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Serial number: please read off the drone itself.

Drone flights in practice

Lead pilot

It is of outmost importance to regulate responsibilities of all persons who are involved in DW productions with drones. The "Lead pilot" is entitled to make the final decision in any given circumstances. The Lead pilot is responsible for checking whether the drone is ready to fly, e.g. that official flight permissions have been issued and that the drone itself is technically fit to fly. The Lead pilot also supervises the flight of the drone itself. Editorial staff is responsible for making content decisions (e.g. what to film when and how) but the Lead pilot is entitled to make the final decision on all flight operations. His/her main task is to guarantee the safety of all involved production staff as well as of third parties. It is subject to the Lead pilot's own discretion whether - in case of any risks - the production needs to be stopped temporarily or cancelled altogether.

Production planning

Editorial staff is responsible for choosing the topic, the location and all storytelling aspects regarding the production. Editorial staff will also check whether the shooting location is in or close to a no-fly-zone any whether any other (legal) restrictions need to be observed (e.g. high-voltage power lines, windmills or similar facilities).

Editorial staff initiates the application for the necessary permissions and approvals. In particular, it is **always** necessary to obtain the approval of the owner of the plots from where the drone takes off and where it lands. The same refers to the plots of residential areas that the drone is supposed to fly over.

Editorial staff is also responsible for obtaining the necessary permissions from the aviation authorities if the production is supposed to take place in flight-restricted areas or no-fly-zones:
https://www.drohnen.de/12114/aufstiegsgenehmigung-beantragen-infos-und-links-zu-luftfahrtbehoerden/
The following map might prove useful for examining the chosen flight area:
https://map2fly.flynex.de/

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

It is recommended to involve the Lead pilot in the selection and the assessment of the shooting location, in the production planning and the examination of flight restrictions and other legal aspects as soon as possible.

Note: Permissions from aviation authorities and other institutions generally require a processing time of up to two weeks.

Immediate flight preparation

The Lead pilot is responsible for the immediate flight preparation. On the basis of the following checklist, the Lead pilot will examine whether the drone(s) and the involved pilots are fit to fly. He/she will also check specific flight requirements as well as all other aspects that are relevant for the safety of the operation.

Before departure

Topic	Action point
Batteries (drone)	Charge
Batteries (remote control)	Charge
Propellers	Check bayonet fittings
Drone frame	Check and tighten screws if necessary
Motor mount	Check and tighten screws if necessary
Emergency protocols	Check return to home functionality
iPhone/iPad (DJI)	Charge and update Apps.
Firmware	Check update

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Camera (mounting)	Check and tighten screws if necessary
Camera (batteries)	Charge
Camera (memory card)	Check, erase and format if necessary
Camera lenses	Check and clean
Drone equipment case	Check content (e.g. spare parts, replacement batteries, cables)
Airspace	Check airspace map for no-fly-zones and other important aspects
Weather	Check weather forecast
Video	Check resolution, framerate and camera settings

On location

The Lead pilot will start flight preparations on location only after having verified that the necessary permissions have been granted.

Topic	Action point
Weather	Check actual weather conditions on location
Wind	Check wind direction and velocity
Airspace	Examine airspace visually for any risks and dangers

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

RC connection	Check RC connection
Drone fit to fly	Final check of drone
Satellite connection	Check connection with at least 8 satellites
Sensors	Activate sensors (or deactivate in case of a 360° production); clean sensors if necessary.
Remote control	Check master/slave coupling
Batteries	Mount and check coupling
Gimbal	Remove cover and release clamp
Propellers	Mount and check
Return to Home	Check environment and set up RTH
Gimbal-Responsiveness	Check and set up
Take of zone	Ensure safety distance of involved staff and third parties
Emergency protocol, loss of contact	Check RTH set-up
Memory cards	Insert
RC display	Check for error messages (e.g. regarding compass calibration).

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Flight operation

Normal flight

Topic	Action point
Stable hovering	Check RC levers and manoeuvrability; land immediately in case of problems.
Faulty navigation	Land and re-calibrate compass
Camera	Check camera manoeuvrability
Flight mode	Change flight modes only when drone is hovering
Batteries	Lead pilot frequently checks charging status
Flight parameters	Lead pilot permanently checks flight data and parameters (e.g. altitude)
Empty batteries (Alarm)	Immediate return to home
Change batteries	Lead pilot changes batteries
Landing	Keep landing zone clear, no landing on sloping terrain

Emergency measures during flight

Topic	Action point
Weather change	In case of sudden weather deterioration (rain, thunderstorms, hail) immediate return to home.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Loss of connection	Turn remote control off and on; · If connection is re-established, land drone immediately; · If connection is not re-established, check whether "Return-to-home" functionality is activated; · Remove batteries immediately after landing.
Drone out of sight	· Lead pilot informs all involved parties that drone is outside the visual line of sight; · Lead pilot tries to reverse and fly back; · If drone cannot be spotted, the Lead pilot will activate „Return-to-home" button.
Loss of engine power	· Lead pilot informs all involved parties; · Lead pilot tries to land drone immediately in a safe area.

After the flight

Topic	Action point
Batteries	Remove batteries
Remote control	Switch off and remove battery
Engine control	Check whether engine is overheated
Camera	Switch off
Memory cards	Remove and store safely
Propellers	Check for damages

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.

Frame	Check for damages
Gimbal	Check for damages
Flight records	Store Flight records
Logbook	Fill in flight data and special occurrences, especially emergency measures.

Note: The "Operations Manual" provided by the Drone Journalism Lab of the College of Journalism and Mass Communications at the University of Nebraska-Lincoln was the basis for these checklists.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No *731667*.