applied sciences

Article

A Proposal for Decentralized and Secured Data Collection from Unmanned Aerial Vehicles in Livestock Monitoring with Blockchain and IPFS

Julio César Úbeda Ortega [1], Jesús Rodríguez-Molina [1,*], Margarita Martínez-Núñez [2] and Juan Garbajosa [3]

[1] Department of Telematics and Electronics Engineering, Universidad Politécnica de Madrid, 28040 Madrid, Spain
[2] Department of Organization Engineering, Business Administration and Statistics, Universidad Politécnica de Madrid, 28040 Madrid, Spain
[3] Higher Technical School of Engineering of Information Systems, Universidad Politécnica de Madrid, 28040 Madrid, Spain
* Correspondence: jesus.rodriguezm@upm.es; Tel.: +34-910673350

Featured Application: The presented work makes significant contributions towards setting the technologies, both in terms of hardware and software, required for the usage of Unmanned Aerial Vehicles in livestock monitoring in a secure, decentralized manner. Thus, secure livestock management, animal behaviour data collection or cattle tracking throughout a specific period are but a few of the applications that the proposed system can support.

Abstract: Livestock monitoring often requires human supervision to guide farm animals to a specific point and the displacement of workers to the places where these animals are, which is likely to be several kilometers away, thus resulting in a repetitive task that requires a significant amount of time and demands the usage of land vehicles capable of moving swiftly through the countryside. In addition to that, data collection about animal behaviour with such procedures is often insufficient and cannot be shared in a secure enough manner. This paper describes how Using Unmanned Aerial Vehicles (UAVs) tailored for this kind of task, when combined with other protocols and software technologies, can provide a useful to mitigate these issues. To prove this end, a functional prototype has been designed, built and tested, offering the operator accurate monitoring of farm facilities and animals. Additionally, security has been conceived as a cornerstone of the presented system from the very beginning. Not only the communication protocols used for this purpose have built-in security layers, but also InterPlanetary File System (IPFS) and blockchain have been used as the technologies that enhance data storage among peers in a network.

Keywords: Unmanned Aerial Vehicle; Smart Farming; InterPlanetary File System; blockchain

check for updates

Citation: Ortega, J.C.Ú.; Rodríguez-Molina, J.; Martínez-Núñez, M.; Garbajosa, J. A Proposal for Decentralized and Secured Data Collection from Unmanned Aerial Vehicles in Livestock Monitoring with Blockchain and IPFS. *Appl. Sci.* **2023**, *13*, 471. https://doi.org/10.3390/app13010471

Academic Editor: Roberto Romaniello

Received: 31 October 2022
Revised: 16 December 2022
Accepted: 27 December 2022
Published: 29 December 2022

1. Introduction

Smart Farming is an activity that comes with a plethora of different definitions and differentiations. It has been described as "*a farm management concept that may use Internet of Things (IoT) to overcome the current challenges of food production*" [1] and it is also mentioned how "*Farming and how farmers work is changing, the use of Information and Communications Technology (ICT) together with the increased use of the Internet of Things (IoT) is developing a concept that is called Smart Farming*" [2]. In the end, Smart Farming refers to the technification both in terms of hardware and software of the human activities related to the obtention of foodstuffs, so that agricultural production can be improved while keeping it a sustainable activity that will not deplete resources (energy, water, etc.) in an irrecuperable manner. Many of the works done to enhance agricultural production involve the usage of different hardware and software technologies, ranging from blockchain-based deployments ([3]) to the usage of semantics ([4]) and Cyber-Physical Systems [5]. Using such developments should not come as a surprise, as they involve several technologies (sensors, actuators, manned and unmanned vehicles) of proven usefulness in activities like measuring, monitoring, and acting during prolonged periods of time.

There are several technological hardware and software solutions that can be used in this regard. One of the most prominent is Unmanned Aerial Vehicles (UAVs), popularly referred to as drones. They can serve purposes that have been defined as in "The four Ds": *Dull* (repetitive, mundane tasks that demand a significant amount of similar sets of movements without any elaborated procedure behind), *Dirty* (tasks that imply high levels of pollution that might be unpleasant or hazardous to humans), *Dangerous* (operations that have an inherent risk in their execution for humans, to the point that they might be fatal depending on the conditions where they take place) and *Dear* (as in tasks that are of expensive nature that might be aided by the usage of robotics in general and UAVs in particular). Many UAVs work in deployments that are at least matching one of these purposes, especially when data must be transferred throughout heterogeneous, decentralized Cyber-Physical Systems as shown in [5]. However, while Smart Farming is one of these areas [6], the usage of UAVs in this application domain is still limited and there are no established criteria on their utilization, thus resulting in an underusage of resources that could potentially provide significant savings in time and funds for certain activities, while obtaining data of high accuracy and reliability over time about livestock behaviour or foodstuffs production.

Security is another feature of critical importance that must be considered in any deployment that involves Cyber-Physical Systems (CPSs) and/or IoT (Internet of Things)-related technologies, especially in open environments with devices vulnerable to be hijacked, such as UAVs [7]. Despite the security features that HTTP Secure (HTTPS) or Transport Layer Security (TLS) can offer, security is often overlooked. We believe that one main aspect of security is that it should be integrated into the design and development of any solution from the very beginning rather than as an afterthought. Consequently, security-enabled components must be integrated into UAV-based systems to be deployed, regardless of the activities expected to be performed by it. Therefore, security must be present in every hardware and software component used to receive and/or transmit data so that cybersecurity threats are reduced to a minimum and attacks end up being ineffective. As it will be described in this paper, there are several elements that must be secured in CPS deployed in open environments, such as radio communications, electronical components and any storage means used to store information, especially when data are saved outside the UAV. Another reason to include security in this kind of developments is providing support material for quality certifications. Being able to certify that the agricultural products come from livestock that was well taken care of can be an asset that will provide a competitive edge to the producer over other competitors that do not have this kind of certification. One example is the Animal Welfare certification provided by institutions belonging to the Welfare Quality network [8]. This certificate is obtained by means of "*audits that are based on the direct observation of the animal itself, by assessing 4 principles: good feeding, good housing, good health and appropriate behaviour. Within these four principles, 12 measurable animal welfare criteria have been identified that complement each other.*" [9]. Having a tool that will provide information about the welfare of the animals in the shape of pictures, video recordings or timestamped content with Distributed Ledger Technology (DLT) or distributed data storage like Interplanetary File System (IPFS) can be very useful, as it will aid in the assessment of how cattle is being treated.

This manuscript provides a framework on the requirements to be considered when creating a system that makes use of UAVs with the purpose of monitoring livestock able to move throughout open spaces. This is the way cattle are held in a great number of larger exploitations all around the world, as it is usually more consistent with the idea of performing traditional cattle raising activities in a sustainable manner. In addition to that, it offers information about how to do it under major security parameters that must be taken into account for the system to be viable in a real environment, so that neither the UAV will malfunction as a result of a cyberattack, nor the data collected can be altered once it has been stored.

1.1. Contributions of the Paper

It is the opinion of the authors that the manuscript that is presented here has made several contributions to the existing Sate of the Art on how to use UAVs in a secure framework when monitoring livestock. These contributions are as follows:

1. A study on the State of the Art regarding the existing solutions for UAV usage in livestock monitoring oriented to Smart Farming. In this way, not only a collection of related works about this topic has been made available, but also the main open issues that have been found are present as well.
2. A specific list of requirements, both for hardware and software components, with regard to how to deploy a UAV in a secure manner whenever it is needed to do so. Therefore, UAVs can either be built from scratch with the specific purpose of cattle monitoring or purchased with the requirements needed to perform monitoring and surveying missions satisfactorily. It must be born in mind that there are several aspects like communications bandwidth, operational distance or data transmission rates that have to be specified for the better performance of a UAV in this application domain.
3. A security threat analysis on how to create a secure framework for UAV livestock monitoring applications. As mentioned, cybersecurity must be considered from the very beginning when deploying a system in the application domain of Smart Farming. Combining the security analysis with the requirements one, an accurate and effective livestock monitoring UAV can be developed.
4. An actual implementation and testing of the proposed framework under the formulated UAV requirements. Thus, the theoretical concepts that are described previously can be put to practice and assessed under a real-world scenario. Not only hardware components for the UAV have been considered, but also the software components (blockchain, IPFS) and protocols (TLS, HTTPS) that are decisively assisting the security capabilities.

1.2. Paper Structure

This paper is organized as follows: an introduction with the most prominent elements about the manuscript (namely, a UAV-based secure framework for the deployment of hardware capable of collecting data about livestock monitoring) has already been presented. Section 2 deals with the related works that have been found with regard to the presented topic. Open issues in the studied solution have been described as well. Section 3 describes the requirement analysis that must be performed to present a solution according to the objectives (data obtention via secure livestock monitoring with a UAV) and requirements (hardware, software and security) that have been mentioned before. The components used for the hardware and software parts of the deployment are thoroughly described, especially with regard to data transmission via wireless communications, their storage via IPFS network, and the blockchain used for data storage. Section 4 is about the testing activities carried out, as well as the discussion on the results that have been reached from them. Section 5 includes the conclusions and future works foreseen for the immediate future. Finally, author contributions, acknowledgments and bibliographical references have been included in the manuscript.

2. Related Works

The materials found about the usage of UAVs show how there is a significant interest in using UAVs in this application domain. Unfortunately, the developments of the solutions proposed tend to have several issues when they must be applied to a real-world scenario.

2.1. Study of the State of the Art

It is mentioned in [10] how an algorithm can be used to distribute a set of UAVs in an open space to maximize the area covered by a group of UAVs. The authors of the paper rely on GPS collars used by individual cattle to advertise their position, which is transmitted to the UAVs. Afterwards, a standard K-Means clustering algorithm is used to determine the optimal distribution of the UAVs deployed in the countryside. This paper justifies the usefulness of utilizing a plethora of UAVs to monitor cattle and how a standard K-Means clustering algorithm can be utilized for such purpose, but its scope is different from the one that is sought in this manuscript, as area coverage rather than security is the main topic of the reviewed manuscript.

Liu et al. [11] describe on their own manuscript an application consisting of a real-time mobile system for cattle tracking that makes use of video captured from a UAV. In this case, the authors explore the advantages of using UAVs in large spaces when requested by legislative reasons. They carry on by explaining the framework that has been used to create an iOS application able to send commands to a UAV from the manufacturer DJI, which in turn is capturing videos and images across the pasture. These data are sent afterwards to a server where processing (segmentation and counting) is performed on them. Overall, the authors' work is impressive in the sense that a mobile application has been built with the capability of sending data to a Deep Learning-capable server where data processing can be done, but due to a different scope sought it offers little information about what security measurements are taking place, or what kind of features are expected from the drones used.

Furthermore, Jung et al. [12] have performed research activities in determining how to round up several animals by using UAVs. The authors of this paper described how they make use of UAVs that mimic the noise perform by predators so that livestock can be gathered and guided into their pen as fast as possible. After introducing how UAV technology has improved to the point that it is possible to use this unmanned vehicle in the application domain of Smart Farming, the authors describe a mission scenario where a group of UAVs give chase to four animals with GPS collar tags attached to them. MATLAB/Simulink models are used for simulations on the strategies that should be followed by the UAVs. Overall, this piece of research focus on objectives that resemble the ones that we described in our own manuscript, but the results obtained are based on simulations rather than testing with actual cattle, whereas our solution considers the latter as well. Additionally, and as it happens in most of the other cases, security is not prominently considered in the research.

It is also described in [13] how Long-Range Wide-Area Network communications (LoRaWAN) can be used to monitor large scale livestock as an activity to perform in rural farms. The authors regard LoRaWAN as one technology that enables the development of the Internet of Drones [14] and carry on describing how a farm-oriented holistic monitoring system can be built with the usage of UAVs, LoRaWAN, Low-Power Wide-Area Networks (LPWANs) and other IoT-related technologies. They also display the main components of the modified LoRaWAN multi-channel gateway produced to make possible the different communications among the integrated parts of the heterogeneous system used for the monitoring activities. The authors, though, have a scope that is different from the one put forward in the manuscript, as their main target is the monitoring water supply in and consumption by livestock, rather than the components required for the monitoring of the livestock themselves. Security is another feature that has not been included or developed in the manuscript either.

Another piece of research with equivalent goals is the one presented in [15] where large animals-specifically, groups of yaks- are monitored via UAVs with an hourly spatial distribution. To obtain data about yak individual movement and behavior, the yak herd was watched from 5 to 8 days every month in a grazing area of 48.5 hectares. A DJI Phantom 3 UAV was used to take photographs, which were used for data analysis. Results showed that there was no significant difference between ground-counting and UAV-based methods for yak herds, thus providing a relatively cost-effective and noninvasive monitoring tool for large cattle. Unfortunately, these activities did not involve the development from scratch of a tailored solution for the objective of the presented research, nor security or the development of a secure infrastructure was a development goal sought or conceived from the very beginning.

Mulero-Pázmány et al. [16] have performed research operations on how to use UAVs as a tool to complement biologging (that is to say, getting precise knowledge about spatial distribution of animals) in spatial ecology studies, especially with regard to the forecasting of animal distribution patterns. In this sense, the authors of this manuscript make use of Unmanned Aerial Systems (UASs) to monitor several individual animals within the Doñana Nature Reserve with GPS collars for them. Afterwards, the UAS registered data is compared to predicted spatial patterns; results offer similar spatial distributions for both cases. Sampling sizes, data features (accuracy, diversity and frequency) or impact are mentioned as parameters that strongly influence experiments of this kind. This reviewed paper proves again that UAVs are a reliable and useful way to gather information about animals scattered in an open field. However, as it was mentioned in other research works, this paper is not oriented towards the enhancement of UASs with security components, nor there is any reference on how to build a tailored solution from scratch for improved animal monitoring. Finally, the scope of this manuscript is different from ours, as it is aiming towards monitoring GPS-traceable animals by means of a glider-like UAV, whereas we make use of a quadcopter and expand the usage of the UAV beyond animal monitoring,

Al-Thani et al. [17] put forward their own developments for sheep livestock monitoring. The authors describe how they have chosen a quadcopter as the most suitable option for cattle monitoring, since it does not require a runaway for takeoff and landing. It is mentioned how the ArduPilot Mega (APM) is used as the flight controller, which reflects some of the choices that have been done for our own solution. A Raspberry Pi processor and a camera are used as part of the UAV as well. Once the UAV is deployed, it is used to collect data processed afterwards for animal detection and counting. When all is said and done, this paper shows that a UAV built from scratch with off-the-shelf components is viable for livestock monitoring, but it makes no reference on how to secure the data or how to create a framework or system beyond the UAV itself, focusing rather on the data processing procedures.

Another piece of research can be found in the study of video cameras to assess feeding behavior of Raramuri Criollo cows [18]. In this piece of work, researchers were most interested in whether the UAV sounds and presence would altern in any way the feeding patterns of the cows (something that is also considered in our own research activities). To assess this, an experiment with two groups of non-lactating cows, where they were fed with and without the presence of UAV noise, was conducted. According to the authors, pilot tests showed no difference in feeding behavior between UAV-naïve and UAV-adapted cows, proving that UAV can be good tools for cattle monitoring. However, the presented piece of research does not provide information about UAV features or security frameworks.

In addition to this, resources like aerial images from Google Earth can be used for effective monitoring, in the way that has been depicted in [19]. The authors suggest that a Flying Ad Hoc Network (FANET) outfitted with image sensors can come in handy whenever extensive monitoring activities must be performed, as well as other tasks like spotting trespassing hunters, illegal farming activities or controlling herd-related operations. To this purpose, a deployment scheme is built where a FANET network monitors a large area of the countryside while collecting data and preserving coverage time and interconnections as optimal as possible, along with a task-sharing protocol among the UAVs that are part of the FANET. Due to a different scope from the one presented in our manuscript, the paper does not provide enough information about other features UAVs should have or how they can be used under a security framework, while our proposal takes these aspects into account and can be used with a collection of UAVs as well.

Pablo Chamoso and other researchers describe in [20] how UAVs can be used for animal counting and monitoring via artificial vision. In this case, a Convolutional Neural

Network (CNN) is used for cattle counting purposes to detect livestock scattered in the field. The technology used and the system created for these goals prove to be effective, but this piece of research is focused on data visualization techniques rather than the UAV technologies for secure data transmission and storage (aside from the camera used in the UAV itself).

William Andrew et al. [21] put forward their own deployment for visual localization and individual identification of Holstein Friesian cattle via Deep Learning. As it happens in other regions of the world, identification and traceability of cattle has become mandatory due to the kind of legislation enforced. In this case, a R-CNN (Regions with CNN features) adaptation of a network published as part of other already existing network architecture proposals has been used for the purpose of locating and detecting Friesian cows. A Video-based Long-term Recurrent Convolutional Network (LRCN) technique has been used for individual identification. Overall, this piece of work mimics the ones presented before that make use of Deep Learning for localization and identification of cattle, but as it happened before, it is oriented towards different goals than the ones put forward in this manuscript. A similar approach can be observed in [22], where LCRN and Long Short-Term Memory (LSTM) technologies are used for the same kind of purposes.

Furthermore, it is also shown in [23] how UAVs can be used to measure spatial proximity, a parameter of major importance when defining social structure, dyadic relationships or grazing and maternal behavior among cattle. UAVs were used to monitor both the location of the individual members of the herd and the identity of cow-calf pairs. To perform the required research, cattle became acclimatized to the UAVs, a procedure that lasted 3 days until cattle got fully adjusted to the presence of the UAVs. An additional period of 4 days was used to collect proximity data. Results showed that cow-calf distance was of around 40 m during daytime and more than 80 m during the evening. These research activities prove that UAVs can be used for measurement purposes whenever a significant degree of accuracy is required, but these activities do not cover other aspects like the security of the information transferred or the components of UAVs that must be settled.

Other pieces of literature are oriented towards researching a specific part of the livestock monitoring procedures. For example, D. B. Mamehgol Yousefi et al. [24] have performed a review on the Use of Deep Learning in Precision Livestock Detection and Localization Using Unmanned Aerial Vehicles. This and other presented research works show how Deep Learning is a very useful tool for cattle detection or counting, but they refer to an area different from the one covered in this paper, which is oriented towards hardware and software components for a UAV monitoring system and how they are used within a secure framework. Literature about cattle detection and counting is rather profuse, with solutions ranging from using the You Only Look Once (YOLO) algorithm for real-time object detection [25] to UAVs equipped with thermal cameras to monitor animal populations [26]. However, most of these research works are focused on how to use Machine Learning and/or Artificial Intelligence to count or identify cattle, rather than how to use security as a cross-layer solution at every possible communication level.

When all is said and done, all these solutions provide some advantages on the works done that offer usefulness and an improvement on the existing state of the art in using UAVs for Smart Farming or cattle monitoring purposes. However, as far as tailoring a tool for cattle monitoring and enhancing it with cybersecurity features is concerned, most of the solutions studied have flaws that have yet to be solved. This is so because these research works only stress the importance of counting and recognizing livestock and, generally speaking, how to identify it and post-process data so that there can be an individual assessment. However, research on developing tailored UAVs for the purpose of livestock monitoring, along with considering the real needs of farmers and how security must be integrated in new developments, are largely missing aims.

2.2. Open Issues

There are several open issues that have been found in the reviewed literature that are yet to be properly solved with regard to the main topics and ideas that have been put forward in this manuscript. Table 1 highlights the pros and cons for each of the studied solutions.

Table 1. Advantages and disadvantages of the studied UAV solutions.

Authors	Advantages	Disadvantages
[10]	Usage of algorithms to determine accurate livestock positions.	Security, or tailoring a UAV for the scope of the paper is not considered.
[11]	Profuse data processing used, usage of mobile application.	No security considered. Different scope from the one put forward in our paper.
[12]	UAVs used for livestock guidance. Movement modeling.	No security is taken into account in the paper. No usage of specific UAV.
[13]	IoT-based, reliable deployment of technologies.	No security is evaluated in the paper. UAV as a closed solution.
[15]	Real-world development oriented to cattle monitoring in the countryside.	No security considerations. Commercial UAV rather than tailored solution.
[16]	Usage of Unmanned Aerial Systems for cattle monitoring in the countryside.	No security considerations in the paper. No usage of tailored UAV.
[17]	UAV built from scratch with the purpose of livestock monitoring.	No information about how to secure data or how to create a secure infrastructure.
[18]	Experiments proving that UAVs can be used for livestock monitoring.	Secure framework or UAV building are out of the scope of the paper.
[19]	Development of the concept of a Flying Ad hoc Network for livestock monitoring.	No security framework is taken into consideration. No specific UAV building.
[20]	Usage of Convolutional Neural Network (CNN) for cattle counting purposes	Scope of the manuscript does not consider security frameworks or UAV tailoring
[21]	Usage of Deep Learning for visual localization and individual identification	UAV preparation for livestock monitoring is not considered. No security.
[23]	UAVs are used for measurement of specific parameter (spatial proximity)	Security components have not been described, nor any kind of framework.

In a more general manner, the open issues found are as follows:

1. Lack of focus on cybersecurity implementation. Security features usually come as an afterthought rather than having them embedded in the development of the solution from the very beginning. In most of cases of the reviewed literature they are given negligible importance, whereas in some others cybersecurity is nonexistent as a feature. This might create major issues when monitoring cattle or performing Smart Farming activities, as the collected data can be tampered with easily, whereas other pieces of information (what kind of protocols must be used for data transmission, which components are vulnerable to cyberattacks, etc.) are missing.
2. Lack of UAV tailoring for the purpose of cattle monitoring. Rather than having one or a collection of UAVs specifically prepared for the purpose of monitoring cattle (something that demands specific components that can be used for data transmission, UAV control or information security) commercial models have been used for the most part to perform the missions. While this might work in some cases, there are others where, due to the communications range or the information flows, using purely

multi-purpose commercial UAVs might present issues that could limit the usefulness of such solution.

3. Lack of description in hardware and software component interweaving and integration. Partially because of the previous open issue, most of the components used in the deployments performed are taken for granted and there is very limited research on how to build hardware and software parts with the specific purpose of cattle monitoring adapted to the actual needs of farmers. In addition to that, cybersecurity features are still largely missing.

Considering the open issues that have been found in the reviewed literature, it has been deemed desirable that the following contributions, already explained in Section 1.2 of paper, are made:

1. A thorough study on the requirements to build such a solution is performed. This has been done according to questions asked to farm staff regarding their own specific needs in cattle monitoring, how they can be solved with the use of UAVs and what has been studied in the State of the Art.
2. Usage of cybersecurity components whenever there is a need for data transmissions so that efforts to exploit weaknesses become futile.
3. Implementation and testing of a UAV-based tool that will meet all the requirements and security characteristics that must be integrated in the system.

Furthermore, it is at this point that the existing literature related to this topic has been reviewed when a hypothesis can be formulated: *can a UAVs-based framework be used to monitoring livestock so that data can be collected and can be kept in a secure way?* Next sections explain how this hypothesis has been answered by means of a theoretical model, its implementation and how it has been tested.

3. Prototype Description and Implementation

The system put forward in this manuscript comes with several advantages compared to the reviewed literature, as it can be inferred from the contributions that were described in Section 1.1. These advantages are as follows:

1. Cybersecurity implementations. In most of the reviewed proposals cybersecurity has not been considered as a serious requirement at any stage of the development, even when sensitive information about living beings or locations was collected. Our proposal integrates specific security solutions derived from the components that have been chosen to build the required subsystems and how they have been integrated.
2. Tailored development. Many of the proposals that have been described do not consider the specific needs of the environment of smart farming (distances from one place to another, easiness to repair damaged components, First Person View or FPV of cattle, enhanced radio control subsystem, etc.). As it will be explained in further sections of the paper, the subsystems that our proposal consists of are built according to the feedback obtained by farmers that work with sheep and the foodstuffs derived from them, so the proposed system is also making use of the information obtained from experts in this area of knowledge.
3. Subsystems built for integration. In most of the reviewed proposals, there is no clear information of the components used to build the UAV (partially since most of them offer commercial, closed solutions from manufacturers) or any other systems that are used in a supportive role. We have described not only such subsystems, but also have explained each of the components used to build them internally, so the technological foundations of the presented CPS are crystal clear.

The advantages that this proposal offers compared to the reviewed literature has been depicted in Table 2. The technologies used to obtain an advantage over the existing literature have been made explicit in the rightmost column of this table.

Table 2. Advantages of the proposed system compared to the open issues identified.

Open Issue	Proposed Solution	Means Used for the Solution
Lack of focus on cybersecurity implementation	Incorporating components and protocols with security capabilities	Usage of security-enabled wireless communication protocols, blockchain and IPFS for data distribution
Lack of UAV tailoring for the purpose of cattle monitoring	Building the UAV used from scratch according to the application domain needs.	Usage of components that enable FPV within the range of kilometers
Lack of description in hardware and software component interweaving and integration	Usage of components that can be described without difficulty	Description of the subsystems and the components that have been implemented/mounted to create them.

In addition to Table 2, Table 3 shows a comparative analysis on the advantages that our proposed solution offers when compared to the ones that have been reviewed in Section 2. It must be noted that some of the previously reviewed solutions fall out of the scope of the paper, and others might be directed towards other kind of goals.

Table 3. Comparative analysis of the solution advantages.

State of the Art Proposal	Disadvantages	Proposed Solution
[10]	Security, or tailoring a UAV for the scope of the paper is not considered.	Tailored UAV and security measures added from design and protocol usage.
[11]	No security considered. Different scope from the one put forward in our paper.	Security measures added from design and protocol usage.
[12]	No security is taken into account in the paper. No usage of specific UAV.	Specific UAV and security measures added from design and protocol usage.
[13]	No security is evaluated in the paper. UAV as a closed solution.	Tailored UAV and security measures added from design and protocol usage.
[15]	No security considerations. Commercial UAV rather than tailored solution.	Tailored UAV and security measures added from design and protocol usage.
[16]	No security considerations in the paper. No usage of tailored UAV.	Tailored UAV and security measures added from design and protocol usage.
[17]	No information about how to secure data or how to create a secure infrastructure.	Data about hardware and software components enhanced with security.
[18]	Secure framework or UAV building are out of the scope of the paper.	Tailored UAV and security measures added from design and protocol usage.
[19]	No security framework is taken into consideration. No specific UAV building.	Tailored UAV and security measures added from design and protocol usage.
[20]	Scope of the manuscript does not consider security frameworks or UAV tailoring	Tailored UAV and security measures added from design and protocol usage
[21]	UAV preparation for livestock monitoring is not considered. No security.	Tailored UAV and security measures added from design and protocol usage.
[23]	Security components have not been described, nor any kind of framework.	Security measures added from design and protocol usage.

Overall, this section has been built with the purpose of showing what kind of requirements are needed to build a specific solution that makes use of a UAV for cattle monitoring under a secure, decentralized framework for data sharing.

3.1. Theoretical Model for the Proposal

Considering the know-how and experience of the authors of this manuscript, a theoretical model has been built according to what could be expected for a system capable of providing improved features compared to what had been found in the reviewed literature. Each of the authors has made their own contribution on what components are to be utilized in order to guarantee that the proposed system offers distinctive advantages over the existing ones. It must be born in mind that, to an extent, requirement analysis can also be regarded as part of the theoretical model. It is based on the following principles:

1. Security. The system should be secured, and security should be at the center of its conception from the beginning.
2. Tailored UAV. The usage of a specific UAV that can face the required needs of the application domain has to be considered.
3. Distribution. The system must have some degree of distribution to ensure that information is not kept in a single, centralized location that might be more vulnerable to cyberattacks.
4. Immutability. Data that have been obtained from the monitoring of animals and other usages must not be altered once they have been saved and shared throughout the system.
5. Data collection. The system will collect data from the activities it is performing for information further analysis.
6. Data availability. The data that have been collected should be available even in case the location saving them has any issue guaranteeing that they can be offered at any time.
7. Information representation. The information that has been collected should be visible for any party interested in the system.
8. System constrains. The system developed for the purpose of this manuscript should consider several constrains related to the budget and usability of the system (both of them must be reasonable).

The main components and layout of the theoretical model conceived for this proposal have been further represented in Figure 1. It is believed by the authors of this manuscript that this theoretical model, consisting of the formulated principles and how they are combined fulfills the criteria that are wanted in them:

1. The theoretical model has significance: it is strictly related to the application domain where the presented theoretical model has a purpose.
2. It has internal consistency: it does not fall into contradictions related to components, their interactions, or their requirements, even during the implementation and testing stages.
3. The model offers parsimony: the components used can be justified from a functional and non-functional requirements point of view and it can be easily explained what kinds of components have been used and their purpose.
4. It makes testability possible: it has been involved in building a prototype that has been tested throughout several experiments.
5. The theoretical model has empirical adequacy: it considers principles in the performance of the UAV and data sharing that exist outside the phenomenon the model describes, such as gravity and time delays in data transfers.
6. It has pragmatic adequacy: it is useful to solve problems that have been found as part of practical works, as it is reflected on the advantages that the proposed system offers compared to the existing literature.

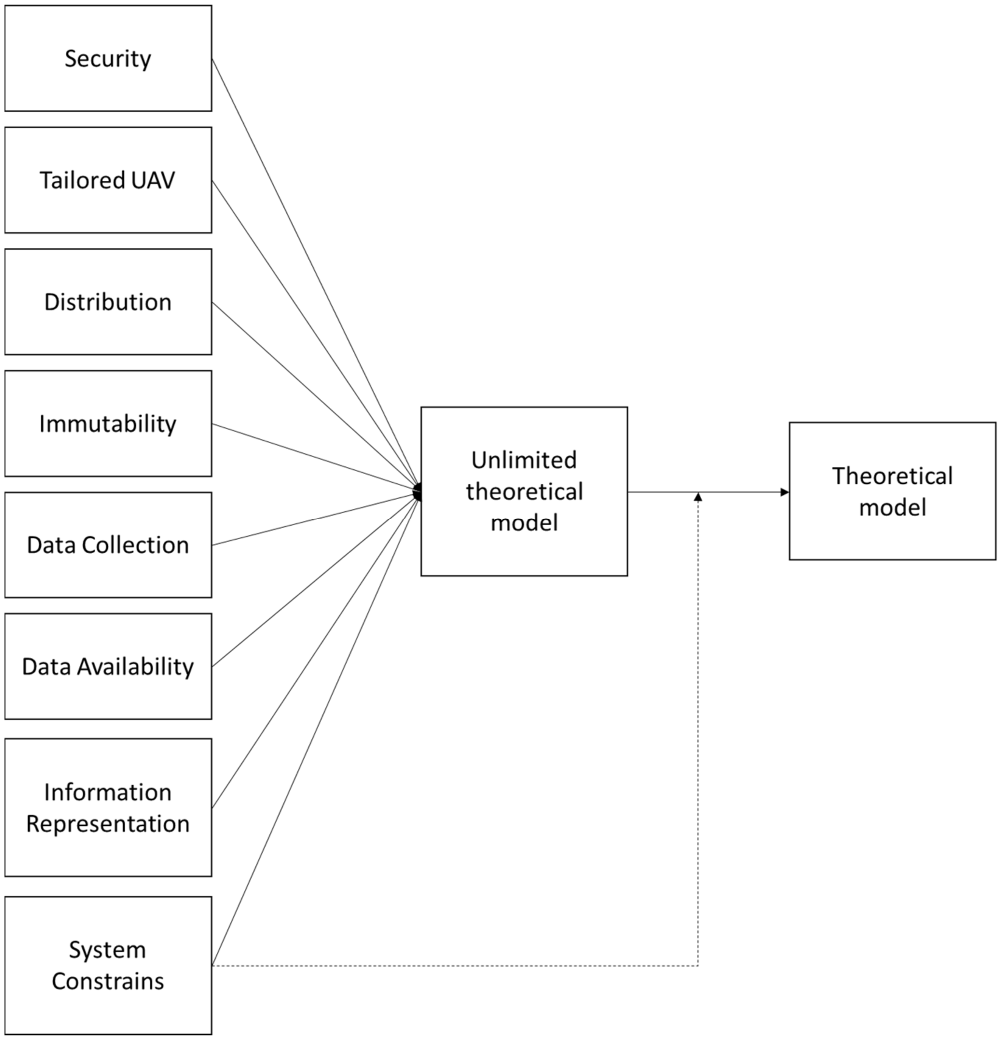


Figure 1. Theoretical model for the system proposal.

3.2. Requirement Analysis

One of the main challenges found in he reviewed literature was the fact that the UAVs used for livestock monitoring were not specifically conceived for this purpose. While they are capable on their own to perform most of the functionalities expected from them, there are several facts that have not been taken into account and may result into issues:

1. Security is a must in the UAV. The components that make the UAV should have as many security features as needed, so that its usage will not result into any kind of cyberattack becoming successful and either luring the UAV away from their owners or damaging the hardware components used for its normal operating. This makes the idea of building a UAV from scratch more attractive, as it is possible to have a better knowledge of the security embedded in each of the components.
2. Security is a must in the deployed subsystems. Not only the UAV must be secured, but also the infrastructure used to secure the data delivery and transfer. To accomplish this purpose, there are several actions that can be taken: to begin with, the data storage infrastructure can become decentralized, so that it becomes obvious when one of the parties is trying to modify the data with malicious intentions. With such an infrastructure, integrity of the information uploaded (images, video) can be guaranteed and farmers can display the location and characteristics of the livestock whenever they are grazing, along with identifying potential predators o rother threats.
3. Range for monitoring. Wireless communication protocols have features related to signal power, range and data transmission, which also impose restrictions on what

power a UAV needs to perform its functionalities and might come in conflict with using a UAV as simple as possible. Using a UAV with limited capabilities for the purpose shown in this manuscript might be desirable due to two reasons: budget (a simpler, more basic UAV will be cheaper to deploy and will required not too skilled workforce) and legislation (current legislation might be too restrictive for small or medium-small UAVs, but more lenient on smaller UAVs, which will make them easier and faster to use in the latter case).

4. Mission autonomy. Energy for UAV movements and communications is drawn from a built-in battery that requires being recharged before it comes to depletion. With not enough battery energy, the UAV purpose might become jeopardized if flight autonomy is too small, thus forcing to either having a recharging infrastructure in the location where monitoring is taking place, or to make short-timed monitoring missions that might miss some of the animal actions.
5. Closed, regular commercial solutions are harder to fix in the countryside. While already built solutions are easier to maneuver as a UAV pilot and offer a level of quality that more oriented Do-It-Yourself developments cannot compete with, its closed nature makes it more difficult to repair in case the UAV results damaged from operating with it. It must be born in mind that livestock monitoring might take place in remote locations (as it has been reviewed in the literature shown in the previous section), so having to take the UAV to an official maintenance service branch might be challenging for the kind of missions that are performed. This, in turn, will likely force farmers to own more than one UAV as a closed solution, thus resulting in extra budgetary needs. Building a UAV from scratch solves that issue to an extent, as there are others related to security and legislation that might appear.
6. Animal behaviour can be challenging. Due to the behaviour of animals when monitored with an alien, unknown element that seems to behave in an unsettling manner (high-pitched noises, hovering), livestock tends to become uneasy and even frightened around UAVs at first, to become indifferent once they have adapted to the UAV presence afterwards. This might result in behaviour issues when having cattle coexisting with the UAV, as they could behave in unwanted manners either if they are being monitored or the UAV is being used to guide them to a specific point.
7. Legislation effectively encourages simpler UAVs. Legislation tends to be restrictive for end users to utilize UAVs, especially when these are large or complex, so simpler models that adapt poorly to the purpose described in this manuscript might be used instead. This pattern might create challenges for UAV utilization even in open, non-inhabited areas, especially if a tailored one is built, as its features might be mixed between more than one UAV class.
8. Information sharing procedures must be enhanced for the purpose of creating a secure, reliable system. If the data provided by the UAV is to be shared among interested parties with the idea of providing all the information in a transparent manner, procedures and tools used from the point of view of data sharing must be an improvement over what is used in the reviewed literature.

All these facts were corroborated in interviews held with staff working in the primary sector that the authors of this manuscript contacted to test the hypothesis that was formulated before. During these actions, it was confirmed that:

1. Using UAVs would provide an advantage for workers in agricultural exploitations as far as livestock monitoring is concerned. Specifically, it would allow farm workers to disengage partially or completely from activities like (a) cattle monitoring to check whether animals are in a suitable position for grazing and away from predators or hunting grounds, (b) cattle guidance towards specific locations where livestock can be kept in safe locations and (c) information gathering about individual animals with conditions that make them special (pregnancies, wounds, etc.). This would enable farm workers to perform other tasks (facilities maintenance, indoor animals cleaning and preparation, etc.) while the UAV is taking care of livestock outside.

2. UAV flight capabilities would come in extremely handy when the livestock is away from the place where farm workers would be performing other tasks (not only in farm installations but also on the countryside), as UAVs can negate any irregularity or difficulty on the terrain where cattle is and can fly at a steady pace that often outruns ground vehicles like automobiles or vans, which can move fast but are dependent on ground accessibility, gravel and/or dirt roads and previously existing paths to get to their destination.
3. Information security was a matter of interest, since videos and images collected can be used to prove that animals have been well treated, have grazed in good conditions and their general well-being is compliant with the currently enforced legislation. The technology behind it was overall nonimportant for the farm staff, although there was a degree of curiosity about it. Likewise, the possibility of reliably sharing information with parties that will provide any kind of benefit or perk (good practices certification, assurance of premium quality in agricultural output) is considered a desirable feature as well.
4. While UAV autonomy is a major concern, it is not as critical as to become a deal breaker for the usage of such autonomous vehicles. Several examples were described, and it was claimed by the farm staff interviewed that a total of 5–6 min was required to conduct a herd of sheep from their grazing location back to a sheepfold in the premises that were used for testing the solution. In that case and similar ones, a flight autonomy of 15 or more minutes should be sufficient to perform missions in a reliable manner.
5. UAV maneuverability was strongly regarded as a necessary feature since it is required to counter sudden strokes of wind or any condition that would send the UAV in a control loss state. Sturdiness (for short-term damage) and durability (for long-term one) were also positively evaluated.
6. An emergency stop feature was desirable, as it would allow to immediately stop any misbehavior that the UAV might experience. This is a characteristic that is included in the overwhelming majority of commercial and built-in UAVS, so applying it to this application domain does not represent a problem.
7. Bad weather conditions are mentioned as a major limitation of the proposed system. While testing and deployment of the whole proposed solution was done in a Spanish location with temperate and not too rainy climate (and in this context, UAVs can be used during a wide range of days), it might not be the case in other locations.

Consequently, a collection of requirements was elaborated. It must be born in mind that requirements have been separated between functional and non-functional: functional requirements refer to the behavior to be expected when the UAV is used and what purposes it has, whereas non-functional requirements will set boundaries to the functionalities that the UAV will perform and what specific properties they have. Table 4 shows the functional requirements that have been inferred from the issues that have been described previously in this subsection.

As for the non-functional requirements, they have also been represented in Table 5. Note that although security is mentioned as a must-have for communications, protocols and standards used do not have to be explicitly mentioned, as there is a plethora of available options to use.

Considering the requirement analysis performed, based both in the reviewed literature and the information that has been obtained on the ground from farm workers, there are enough data on how to implement a UAV-based solution that will fulfil the hypothesis formulated for this manuscript.

Table 4. List of the UAV functional requirements.

Requirement Number	Description	Purpose
Functional Requirement 1 (FR1)	The UAV will FLY over cattle with as little disturbance as possible.	Basic functionality expected for cattle monitoring.
Functional Requirement 2 (FR2)	The UAV will HOVER over cattle with as little disturbance as possible.	Basic functionality expected for cattle monitoring.
Functional Requirement 3 (FR3)	The UAV will perform missions in a GUIDED manner.	Ability to monitor cattle as the main task.
Functional Requirement 4 (FR4)	The UAV will perform missions in an AUTONOMOUS manner.	Ability to ease the farmer from constant monitoring tasks.
Functional Requirement 5 (FR5)	The UAV will transmit information as REAL-TIME DATA.	Instant information about livestock movement and location can be obtained.
Functional Requirement 6 (FR6)	The UAV will STORE DATA as part of the information collected.	Ability to have data saved for future processing and/or knowledge inference
Functional Requirement 7 (FR7)	Data will be SHARED among relevant parties participating in the system	Ability to share information among different entities in a reliable, trustless manner

Table 5. List of the UAV non-functional requirements, as obtained from studied literature and questions formulated to farmers.

Requirement Number	Description	Purpose
Non-Functional Requirement 1 (NFR1)	Security measures must be present in the UAV hardware.	The UAV must not be hijacked or tampered with in any way.
Non-Functional Requirement 2 (NFR2)	Security measures must be present in the software.	The data collected from the UAV must not be tampered with in any way.
Non-Functional Requirement 3 (NFR3)	Communications range must be of at least 5 milometers long.	The UAV must be able to fly through the countryside with no restraint for monitoring.
Non-Functional Requirement 4 (NFR4)	Mission length must be of at least 15 min.	The UAV must have enough battery autonomy to perform monitoring missions.
Non-Functional Requirement 5 (NFR5)	UAV must have components that can be repaired in situ.	The UAV must be repaired without significant aid from outside monitoring space.
Non-Functional Requirement 6 (NFR6)	UAV and missions must be compliant with current legislation.	The UAV deployment and data gathering must respect existing legislation.
Non-Functional Requirement 7 (NFR7)	Data must be shareable among interested parties in a reliable manner	Information will be provided in a transparent way to any party providing perks
Non-Functional Requirement 8 (NFR8)	Data must be transferred in a secure manner through the system	Hardware and software components used will provide security measures

3.3. Prototyping of Hardware Components

As far as hardware components are concerned, the UAV that has been built as a livestock monitoring tool has two fundamental subsystems.

The first of the subsystems is a Command Ground Station (CGS) that, for convenience in receiving information and sending commands, must be located next to the flight operator.

The CGS can be built with a computer capable of running a mission planner software [27] and a display connected to a 5.8 GHz analog video receiver. Through this base station, the operator will have detailed telemetry of the aircraft, without requiring a too steep learning curve. Telemetry information will display data to help the operator with any decision making during the flight in case the flight is guided (so the operator is effectively maneuvering the UAV). Some of these data are (a) the position of the aircraft, (b) its altitude or (c) the State of Charge (SOC) of the battery. The base station will also enable the operator to program a series of alerts whenever telemetry values are abnormal (i.e., programming the return of the UAV to the takeoff point when the battery level is low). In addition to this, the display and analog video receiver provide the UAV operator with visual imaging of the terrain the aircraft is flying over, which are pivotal to carry out monitoring and grazing of livestock. This image is transmitted through a video system integrated in the UAV that will be described in the next section.

Aside from the base station, which is mandatory to send and receive data, the actual UAV components used to build it up must be considered as well, so that a UAV that is compliant with the requirements previously formulated can be used. Such components are as follows:

1. Frame F450 [28]: this frame is one of the most popular in UAV prototyping. Its main advantages are its light weight, its resistance to impacts and its ease of repair, which are of great usefulness for the application domain formulated in this paper. Furthermore, its size makes it a suitable option for assembling modular UAVs since it has more than enough room for the integration of many components. The material from which it is made of is reinforced plastic and its low cost are added values that make it the best option.
2. Navio2 controller [29]: the flight controller is the component in charge of ensuring that all the other ones that make up the UAV will work properly. Together with the Raspberry Pi 3B [30] on which it is integrated, the controller governs the modular systems integrated in the aircraft (that is to say, autonomous stabilization, GNSS navigation, flight by waypoints or displacement points, failsafe systems or rear door for greater security, camera control, UAV manual control functions). The Raspberry Pi 3B is also an extremely useful tool for hardware integration, as it offers several interfaces (four Universal Serial Bus -USB- ports, one High-Definition Multimedia Interface -HDMI- interface and, more importantly, a 40-pin extended General Purpose Input/Output) that can be used to connect any hardware component required. Overall, the flight controller used offers a series of features that come in handy for the purpose of this demonstrator. The Global Navigation Satellite System (GNSS) receiver provided by Navio2 is compatible with various positioning systems, such as the American GPS [31], Russian GLONASS [32] and European Galileo [33]. One of the reasons why this controller was selected is that its GPS chip is compatible with the GNSS European civil positioning system. As far as the purpose of this system proposal is concerned, Galileo offers several advantages: it is a free and open service, it offers greater positioning accuracy (explicitly described as Galileo High Accuracy Service or HAS [34]) and, more importantly for the purpose of this manuscript, it offers a higher level of security for data encryption that are not present in the other GPS solutions. Galileo also offers a high precision, fully encrypted service freely available for government-authorized users [35], which is equivalent to the one that GPS offers as military P(Y) or M code.
3. Video transmission subsystem: the designed aircraft has an integrated analog video system that offers the operator a first-person view of the drone’s flight (which is referred to as First Person View or FPV). This feature will provide the pilot with a precise view of the UAV state at every moment of the mission that is taking place. For the implementation of this system, a series of hardware components are required. As mentioned, an analog video camera is needed, which is integrated on board the UAV and provides images with enough quality for the operator so that they can orient

themselves on the terrain over which the UAV is flying. Additionally, an analog video transmitter is required, which receives the signal captured by the camera and transmits it to the ground base station that has a receiver synchronized with the transmitter and connected to a screen. Due to the importance of this subsystem, it has been further divided onto four different hardware components:

a. FPV camera (25 × 25 mm 1200TVL CMOS 3.6 mm) [36]: the FPV camera is a small analog video camera placed on the UAV. Its main function is to offer the pilot a real-time image of the position and the environment where the aircraft is located. The video quality must be good enough to allow the operator to maneuver with and steer the vehicle. This component is directly connected to the video transmitter through a bus that feeds the component with power and in turn transmits the signal of the captured image.

b. Video Transmitter AKK-FX2-Dominator 250 mW [37]: it is a component responsible for transmitting the signal it receives from the FPV camera to the receiving CGS. This video transmitter must broadcast a signal with enough power to be received within the radius of action of the flight plan, thus preventing the operator from losing visual reference to the position of the vehicle. Due to the nature of the proposed system, a long-range analog video transmitter has been chosen (the distances handled in the grazing and monitoring of sheep must be considered here). Specifically, this video transmitter offers a range slightly greater than four kilometers as long as it is used with omnidirectional antennas. Taking into account its characteristics and the fact that the area where it will be used does not have major obstacles that could cause interference, it becomes rather suitable for the purpose of this manuscript. Since it is transmitting significant amounts of data, this component will heat up considerably, so it should be placed in a space where it is ventilated during the flight. This video transmitter works combined with the antenna that will be described in the next subsection, due to the need to transfer the collected images to the module expected to send the data out of the UAV. As it will be explained later, both this video transmitter and the antenna it works with make use of the 802.11 ac wireless standard that transmits data at 5.8 GHz.

c. VTX Antenna AKK 5dBi 5.8 GHz FPV [38]: this antenna is a component connected to the video transmitter. Its main function is the conversion of the electrical waves of the video signal into electromagnetic waves that the ground station will receive. In this case, an omnidirectional antenna with Right Hand Circular Polarization (RHCP) has been used, which implies that the receiver of the CGS must have an antenna polarized in the same way. An omnidirectional antenna will be used because it is the one that offers the greatest range for the transmission of video signals and therefore allows the operator to take the aircraft further from the ground station. For the usage of the 5.8 GHz band, the standard 802.11 ac has been used, which offers better security capabilities than other transmission systems due to including support for 256 bit AES keys and the Galois Counter Mode Protocol (GCMP) encryption protocol, which is more efficient and performs better when compared to Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). In addition to that, a) the 5 GHz band is much less cluttered with traffic than the 2.4 GHz one, so data transmissions are more efficient and easier to deal with and b) Protocol Data Units (PDUs) have been further optimized (according to the Amendment 4 of the standard [39] "*CCMP-128 processing expands the original MPDU size by 16 octets, 8 octets for the CCMP Header field and 8 octets for the MIC field. CCMP-256 processing expands the original MPDU size by 24 octets, 8 octets for the CCMP Header field, and 16 octets for the MIC field.*").

d. FPV goggles (Eachine EV800D) [40]: FPV goggles integrate several components that allow the operator to have visual information about what can be watched from the position of the UAV. Firstly, they incorporate a receiver for the video signal transmitted by it. This receiver transforms the received electromagnetic signal into an analog video signal. Furthermore, this model of glasses uses a 5.8 GHz diversity receiver (this means that it incorporates two types of antennas: one linear and one omnidirectional, polarized in the same direction as the video transmitter antenna that is on board the UAV). Receiver diversity technology is developed to minimize the effect of multipath cancellation and extend the useful operating range of the system. The receiver can tune up to 40 channels to avoid interference with the signal from other vehicles transmitting data. Adding to the video receiver, the glasses also incorporate a screen where the operator can see the image taken by the camera and transmitted in real time with minimal delay. This makes possible not only to see what the UAV camera is transmitting, but also enables the operator to know the location of the UAV and have a visual reference of its surroundings to be able to maneuver properly.

When designing the video transmission subsystem for the deployment that has been put forward, it was necessary to research what components could meet the minimum requirements formulated for the UAV. The main challenge to be faced was maintaining image quality at a distance range beyond two kilometers. The chosen AKK receiver has a theoretical range of four kilometers (although it is usually dependent on the conditions of the environment where it is used) so it was deemed as valid for the location where the deployment tests were to be done. The quality of the image offered enables the operator to orient themselves in the air and manage the aircraft in a timely manner.

4. Radio control subsystem: like the video system, the UAV radio control management system must be adapted to the needs of the project. The system is basically made up of three main components: firstly, the transmitter by which the pilot can control the UAV; secondly, the radio control transmitter module connected to the transmitter, and finally, the radio control receiver on board the UAV. The transmitting and receiving modules must be connected and synchronized through a process called “binding”. This process only needs to be done once during initial aircraft setup. The receiver that goes on board the drone is responsible for transmitting the signal received from the station to the Navio2 controller. The list of components that has been used for this purpose is as follows:

    a. Station: Taranis QX7 [41], this station offers numerous possibilities due to the following facts: (a) it integrates an internal RC module that works with the Pulse-position modulation (PPM) and Serial Universal Serial Bus (SBUS) protocols (it also incorporates a port to connect external modules that work in different frequencies and with different radio control communications protocols), (b) it implements OpenTX [42], an open-source firmware for radio control transmitters that is highly configurable and incorporates many more features than usually found in traditional radios (also, daily feedback from its users ensures the continued stability and quality of the firmware), (c) it has numerous configurable switches to activate Pulse Width Modulation (PWM) channels and (d) it can work integrated into the UAV, such as the choice of flight mode.

    b. Radio Controller (RC) Transmitter Module: TBS-Micro Transmitter Crossfire V2 [43]. The transmitter manufacturer is specialized in the design of radio-controlled components for long-range use. The communications protocol that it usually uses is CrossFire (CRSF), which is developed by the manufacturer itself (TBS) and its main advantage is a faster cycle time and bidirectional communications, enabling data such as telemetry to be included in the data flow without the need to use additional ports. Since the controller used is not compatible with the CRSF communications protocol, the one used will be Pulse Position Modulation PPM, which is the protocol recommended by the manufacturer of the flight controller. Its main advantage is that only one signal cable is needed to receive the radio control channels (channels 8 to 16). A PPM signal is nothing more than a series of PWM signals transmitted through the same cable one after the other. The transmitter module has a built-in T-shaped antenna. These types of antennas are used for the transmission of medium and long wavelength signals.

c. RC receiver (on board the UAV): CrossFire Nano Rx [44]. It is a small-sized receiver of great usefulness due to its small size, in addition to the robustness and range it offers. The normal course of action would be for it to implement the TBS Crossfire (CRSF) protocol, but given the impossibility of doing so, it is also compatible with PPM. The radio control receiver has another T-shaped antenna that will be placed on one of the legs of the drone.

5. Rotors: the rotors that have been selected for the prototype are the MN2212 18 model from the manufacturer T-Motor. They are specific for UAVs used to travel long distances and usable in, at least, medium sized-UAVs. In case of this UAV, the rotors have 920 KV (KV refers to the constant revolutions of a rotor per Volt, that is to say, the revolutions per minute that the rotor offers when 1 Volt of voltage is applied). While its maximum speed is not as high as what racing drone motors can offer, it is torquier and will lift the UAV with ease. Additionally, motors with a lower KV have a smoother ride.
6. ESC (Electronic Speed Control): a speed variator or electronic power controller has as its fundamental purpose to vary the speed of an electric motor, along with the direction of rotation. Typically, the UAV controller sends a PWM signal to the ESC with variations of 1 to 2 ms. If the value is 1 ms, the motor will be stopped. If it is 1.5 ms it will be at half power and at 2 ms it will be at 100% power. For the implementation of the requirement-compliant UAV, four variators of 30 Amperes each have been chosen. There are several ESC features that must be considered, like the maximum current that an ESC can deliver to the motor, the size of the propellers, the number of battery cells or the type of motor that is being used in the UAV.
7. Finder: while it is an accessory not essential for the operation of the aircraft, it can be very useful for the operator when an UAV has an accident (i.e., the UAV falls into an area with high vegetation and becomes difficult to locate). In the environment where the deployment will be made there are areas with cereals, tall grass, bushes, etc. Therefore, it will be necessary to integrate the finder in our aircraft. This finder is connected to one of the PWM channels that the Navio2 has and is activated through a switch in the transmitter. The chosen Finder is the JHE42B S model [44]; it has an extra battery that gives it a few minutes of duration if the UAV battery runs out of power. It is also possible to use the sound emitted by its buzzer to guide the sheep in the desired direction, although they may ignore it once they get used to it.
8. Battery: the battery mounted by the aircraft must have enough autonomy for the UAV to travel to the desired area and be able to make the return trip. The deployment that has been performed works with relatively long distances (2–3 km), so a battery with a higher capacity than those regularly used is required. The choice made is a LiPo battery (Lithium Polymer). This type of battery has been selected due to its energy storage capacity, in addition to the fact that it offers a high discharge rate, something very necessary for multi-rotors. The battery has 4 cells of 3.7 Volts each, so its nominal voltage is 14.8 Volts. It has a discharge capacity of 25 C and a capacity of 6750 milliamperes, enough to cover the distances used in the deployment for testing purposes. Cs of a LiPo battery refer to the rate of discharge. It stands for the capacity of a battery, usually measured in Ampere hours or Ah. The higher the C of a battery, the shorter its life and the higher the speed it can achieve. In this case, being 25 C, there is a balance between battery life and the maximum speed that the aircraft can reach. It has been estimated that, considering the other parts of the UAV, this battery would have a duration of about twenty-one minutes. Due to the feedback received by the farm workers where tests took place, it has been regarded as enough for the

aircraft to perform reconnaissance and herd-gathering missions. Considering that the UAV can travel at an average speed of 30 km per hour, during the battery life duration it could travel up to about 10 km without the risk of running out of energy. Based on the data shown, it can be concluded that the chosen battery satisfies the requirements of the project.

9. As for the Radio Control System of the aircraft, it offers the possibility of PPM or SBUS protocol and has 14 fully configurable PWM channels for the implementation of different modules. In addition, it has other ports and a high-sensitivity barometer that allows the UAV to be positioned with high accuracy.

With all the features considered for the hardware parts of the proposed system, it can be claimed that the components integrated in this prototype are contributing to the fulfillment of the functional and non-functional requirements that were formulated in the previous section in Tables 4 and 5. Table 6 shows how this is done. Note that there are several not applicable requirements, as they are more software oriented. Nevertheless, they will be satisfied by the software components of the system.

Table 6. Fulfillment of some functional and non-functional requirements with the UAV.

Requirement Number	Description	Fulfillment
Functional Requirement 1 (FR1)	The UAV will FLY over cattle with as little disturbance as possible.	Frame, Controller, Motors, RC components, ESCs, Battery
Functional Requirement 2 (FR2)	The UAV will HOVER over cattle with as little disturbance as possible.	Frame, Controller, Motors, RC components, ESCs, Battery
Functional Requirement 3 (FR3)	The UAV will perform missions in a GUIDED manner.	Frame, Controller, Motors, RC components, Radio Control Systems, ESCs, Battery
Functional Requirement 4 (FR4)	The UAV will perform missions in an AUTONOMOUS manner.	Frame, Controller, Motors, RC components, Radio Control Systems, ESCs, Finder, Battery
Functional Requirement 5 (FR5)	The UAV will transmit information as REAL-TIME DATA.	Frame, Controller, Motors, RC components, Video Transmission System, Radio Control Systems, ESCs, Finder, Battery
Functional Requirement 6 (FR6)	The UAV will STORE DATA as part of the information collected.	Not Applicable. Fulfilled by IPFS and blockchain nodes
Non-Functional Requirement 1 (NFR1)	Security measures must be present in the UAV hardware.	Controller, RC components, Video Transmission System, Radio Control Systems
Non-Functional Requirement 2 (NFR2)	Security measures must be present in the software.	Not Applicable. Fulfilled by IPFS and blockchain nodes
Non-Functional Requirement 3 (NFR3)	Communications range must be of at least 5 milometers long.	RC components, Video Transmission System, Radio Control Systems
Non-Functional Requirement 4 (NFR4)	Mission length must be of at least 15 min.	Battery
Non-Functional Requirement 5 (NFR5)	UAV must have components that can be repaired in situ.	Frame, Controller, Motors, RC components, Radio Control Systems, ESCs, Battery
Non-Functional Requirement 6 (NFR6)	UAV and missions must be compliant with current legislation.	Frame, Controller, Motors, RC components, Radio Control Systems, ESCs, Battery

The components used for hardware prototyping can also be seen in Figure 2.

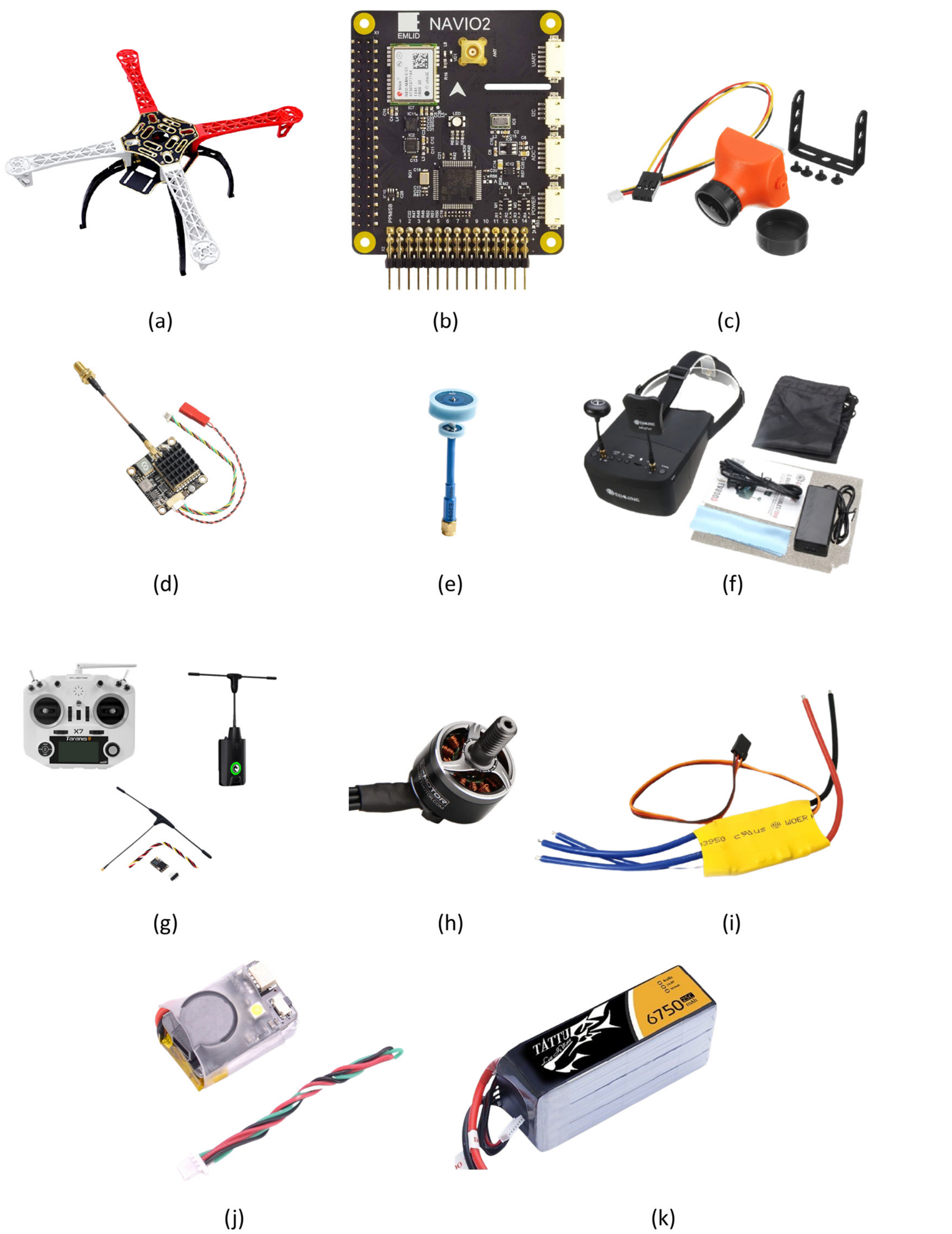


Figure 2. UAV individual components.

It must be noted that the components represented in Figure 2 are placed in the same order as described in the manuscript: (a) Frame F450, (b) Navio2 controller, (c) FPV camera from the video transmission subsystem, (d) Video Transmisor AKK from the radio control subsystem, (e) Antena RHCP 5, 8 GHz, (f) FPV Goggles Eachine EV800D, (g) RC System, (h) rotor MN2212, (i) ESC, (j) Finder JHE42B S and (k) battery.

3.4. Prototyping of Software Components

If location is taken into account, there are four kinds of software that have to be taken into account to work with each other: (a) the UAV itself that has been tailored for the purpose of the presented research, (b) the CGS where commands are run whenever there is a mission that has to be carried out, (c) the IPFS decentralized network where images are being uploaded and shared with the users participating in the system and (d) the blockchain used for data storage and sharing among the parties interested in having the information from the monitoring activities that are carried out with the UAV. Therefore, the description of the prototyping of the software components is based on what has been developed in these three parts of the system. These components and their interactions are represented in Figure 3.

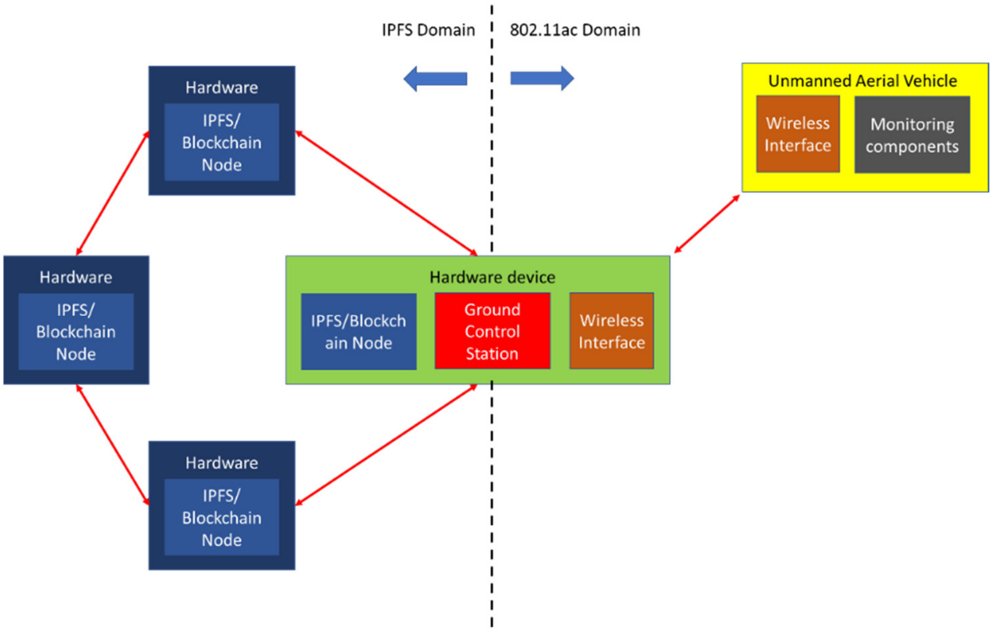


Figure 3. Software components use in the proposed system.

The elements that have been included in Figure 3 can be further represented to reflect what will be found in a less abstract manner. This representation is the one that has been included in Figure 4. It can be seen here the appearance of the UAV tailored for the project, along with the appearance of the laptop that, once it had the suitable software installed, became the CGS. The addition of the required software for the CGS to become a blockchain/IPFS network has also been represented. All these elements are further described in the following subsections of the paper.

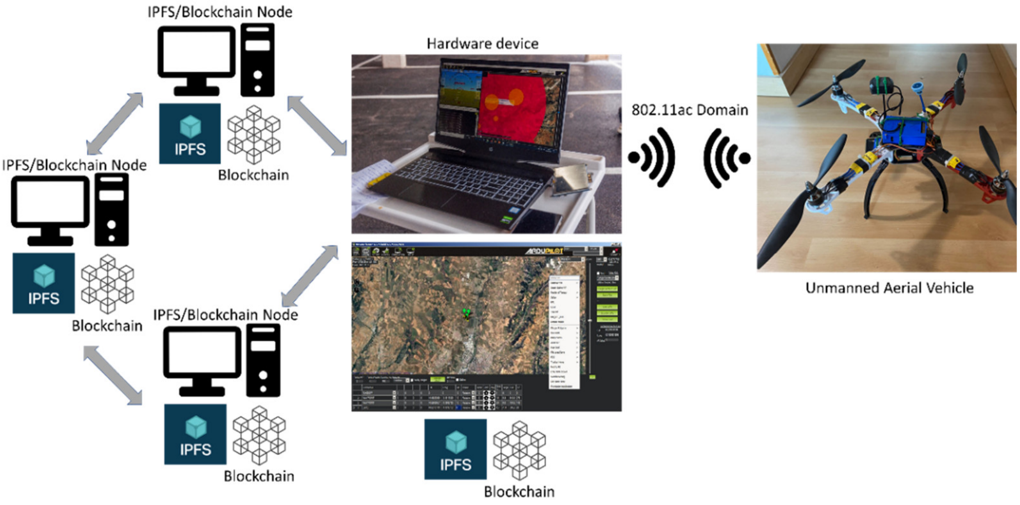


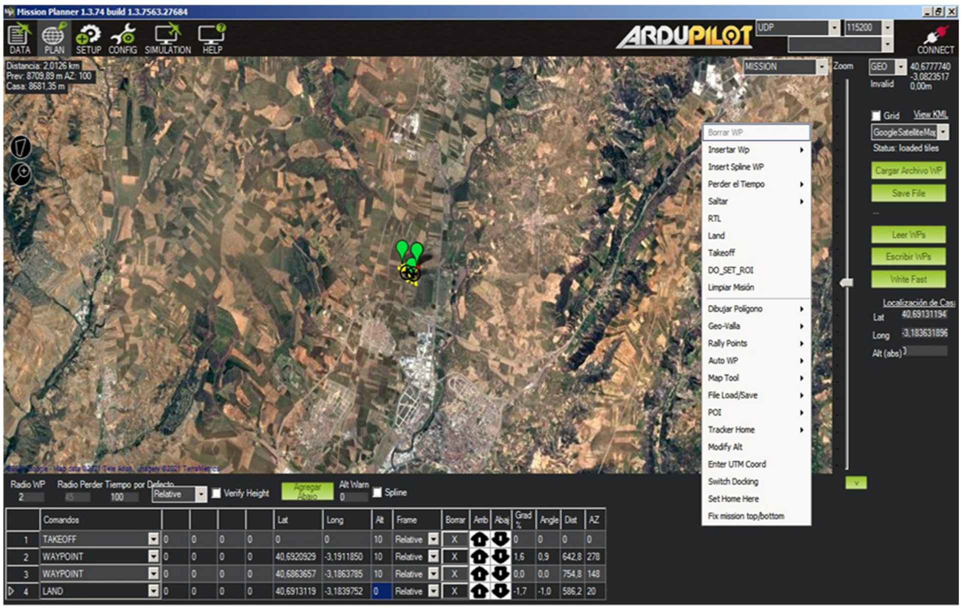
Figure 4. Representation of the proposed system.

3.4.1. Command Ground Station Software Prototyping

To have all the facilities required to run a laptop/Personal Computer hardware behaving like a CGS, the Mission Planner software must be installed first. This is a software used for planning UAV flights to last for a specific amount of time and point out what locations or intermediate coordinates should be visited. This is a program created by Michael Oborne [45] that turns a computer into a complete CGS. It effectively implements all the necessary functionalities for the ArduPilot open-source program described above and thus has been integrated in the built UAV for handling it and performing flights autonomously. While it is only compatible with the Windows Operating System, the Mission Planner program offers as main advantage the possibility to use it as a tool for the configuration of the technical parameters of the vehicle, as well as an aid for the dynamic control of autonomous missions. Some of the features that Mission Planner implements are as follows:

a. Creation of routes for autonomous missions.
b. Creation of geofences using Google Maps, Open Street Maps or customized WMS (Web Map Services).
c. Selecting commands for the mission through its Graphical User Interface (GUI).
d. Downloading .log files with mission records for later analysis.
e. Configuration of the settings for the auto piloting of the vehicle.
f. Interface with a flight simulator for the creation of a complete software in the loop UAV simulator.
g. Execution of SITL simulation on different frameworks for all ArduPilot vehicles.

The appearance of the Mission Planner software can be seen in Figure 5.



Mission Planner 1.3.74 build 1.3.7563.27684

Distancia: 2,0126 km
Prev: 8709,89 m AZ: 100
Casa: 8681,35 m

GEO 40,6777740 -3,0823517 Invalid 0,00m

Status: loaded tiles

Localización de Cas:
Lat 40,69131194
Long -3,183631896
Alt (abs)

Radio WP 2 Radio Perder Tiempo por Defecto 45 100 Relative □ Verify Height Alt Warn 0 □ Spline

	Comandos					Lat	Long	Alt	Frame	Borrar	Arrib	Abaj	Grad %	Angle	Dist	AZ
1	TAKEOFF	0	0	0	0	0	0	10	Relative	X	⬆	⬇	0	0	0	0
2	WAYPOINT	0	0	0	0	40,6920929	-3,1911850	10	Relative	X	⬆	⬇	1,6	0,9	642,8	278
3	WAYPOINT	0	0	0	0	40,6863657	-3,1863785	10	Relative	X	⬆	⬇	0,0	0,0	754,8	148
▷ 4	LAND	0	0	0	0	40,6913119	-3,1839752	0	Relative	X	⬆	⬇	-1,7	-1,0	586,2	20

Figure 5. Example of Graphical User Interface provided by ArduPilot.

In the deployment proposal carried out, a large part of the functionalities offered by this software are used, with the most important ones being the first two (a. and b.) due to the following reasons:

a. The creation of routes for autonomous missions is one of the functions implemented by the program that is most useful for the system proposal described in this manuscript. With this function, the operator of the aircraft can plan a fully autonomous flight by configuring numerous parameters such as the route to be followed by the aircraft, the altitude to be carried at all times or the actions to be carried out in an unforeseen event. With this, the farm staff can schedule reconnaissance flights to check that the herd is in the place where it should be, that there is water in the drinkers, etc. Another possibility is carrying out reconnaissance routes to look for possible dangers in the pasture, such as the presence of feral animals that can prey on the livestock, or an area with better conditions for the cattle. By means of the GUI offered by the Mission Planner software, the instructions are configured with the parameters that the UAV must follow during the flight. Some examples of parameters that must be configured would be (a) the height to which the aircraft must rise on takeoff, (b) the "waypoints" or route points that it must follow or (c) the speed at which it must move, (d) the point where it must land. The parameters mentioned are the most basic that a flight plan must contain. However, there are many more configurable parameters when establishing a flight plan.

b. The other functionality that should be highlighted in the program is its general GUI, which allows the configuration of many parameters such as the station and everything related to it (channels, switches), the adjustment of the speed of the motors, telemetry settings, etc. In addition to that, it also has a window where all the telemetry parameters that can be useful for the handling of the UAV by the operator are shown.

Finally, it is worth mentioning that through the GUI of the Mission Planner software it is possible to carry out a series of actions related to the handling and management of the UAV. Although some of these actions can also be carried out through the transmitter, there are others that can only be executed from the software. It should be noted that during the flight the UAV is always connected to the CGS, so that there will be dual control of the vehicle (by means of both the broadcaster and the CGS). Different flight modes, request to return to the marked landing point, emergency stops of the engines or restart of one mission are several choices possible.

The overall appearance of the CGS used for testing purposes after the installation of the required software is as represented in Figure 6.

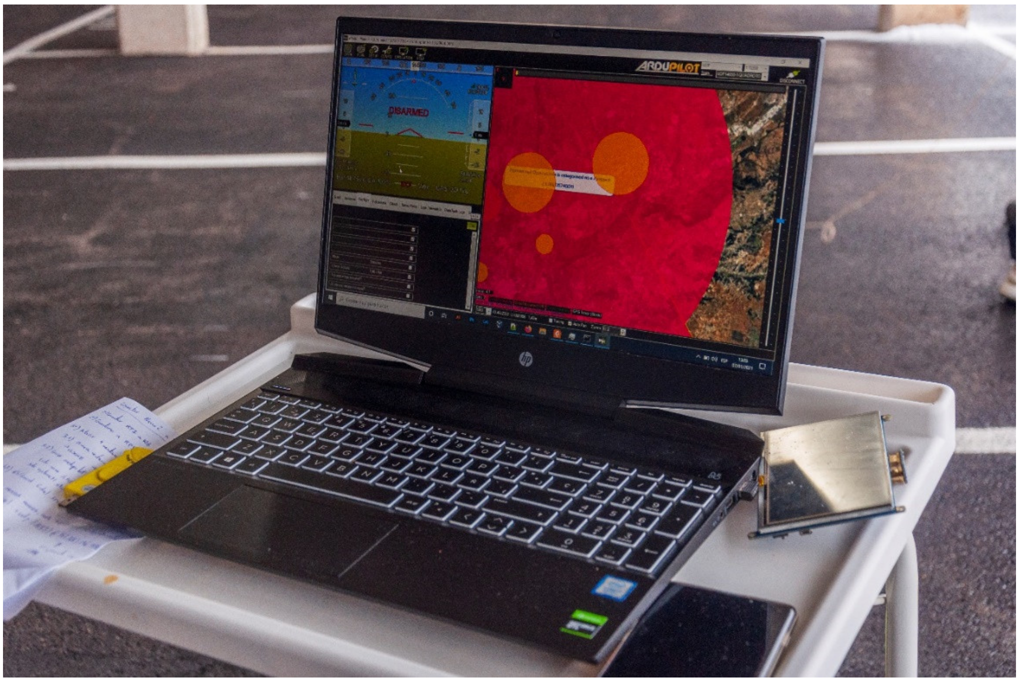
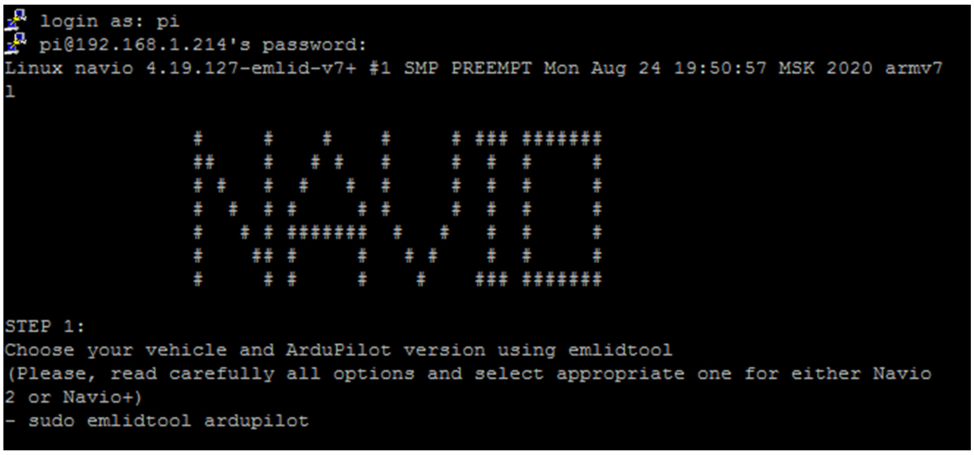


Figure 6. Laptop used as CGS during testing.

3.4.2. UAV Software Prototyping

The first software of major importance to consider for the development of the UAV prototype is ArduPilot [46]. ArduPilot is an open-source, firmware-based project that performs the information processing functions required by the vehicle that makes use of them. Additionally, due to the MAVLink protocol [47], the UAV offers two-way telemetry in real-time. MAVLink (Micro Air Vehicle Link) is a protocol for communication with small, unmanned vehicles. It is designed as a "header-only" message classification library. It can be used to transmit the orientation of the vehicle, its position or speed. In addition to MAVLink, the Project implements the ROS system (Robot Operating System) through MAVROS. ROS is a framework for software development used in robots that provides the functionality of an operating system in a heterogeneous cluster. This system is licensed under BSD (Berkeley Software Distribution), so it can be used openly and freely. MAVROS is defined as an extensible communication node for ROS with a proxy for ground control stations. The ArduPilot software, on the other hand, works directly on a Raspberry Pi 2, 3 or 4 with Navio2 (the autopilot program can work directly on the Raspberry Pi as well). In this Project, a Raspberry Pi 3 Model B was used, which used Raspbian as the Operating System to work with ArduPilot. This software is not only free, but also has a large amount of teaching material, as well as ongoing projects. Its appearance once it was launched has been displayed in Figure 7. Note that neither the UAV nor the Raspberry Pi have any screen to display information; the latter must be connected to a monitor for data visualization.



```
login as: pi
pi@192.168.1.214's password:
Linux navio 4.19.127-emlid-v7+ #1 SMP PREEMPT Mon Aug 24 19:50:57 MSK 2020 armv7
l

                #     #    #    #     # ### #######
                ##    #   # #   #     #  #  #     #
                # #   #  #   #  #     #  #  #     #
                #  #  # #     # #     #  #  #     #
                #   # # #######  #   #   #  #     #
                #    ## #     #   # #    #  #     #
                #     # #     #    #    ### #######

STEP 1:
Choose your vehicle and ArduPilot version using emlidtool
(Please, read carefully all options and select appropriate one for either Navio
2 or Navio+)
- sudo emlidtool ardupilot
```

Figure 7. Launch of ArduPilot through the Navio2 controller.

The second software of major importance used is OpenTX, the open-source firmware used by radio transmitters and implemented in the radio control station. To use it, it is necessary to install it in the station via a microSD card. One of the main advantages of this firmware is that the controls, switches and potentiometers of the transmitter are highly configurable by means of the "LUA scripts" which are text files not part of the firmware, yet they allow the customization of the mentioned components.

The third and last major piece of software that will be described in this section is the TBS (the chosen Radio Controller transmitter module, as described before) Agent. It is used for the configuration and update of the radio control transmitter module, as well as the nano receiver integrated in the UAV. It is only necessary to connect the transmitter to the computer through the Universal Serial Bus interface (USB) and follow the steps indicated by the TBS Agent program.

3.4.3. IPFS Prototyping

IPFS must be mentioned as one pivotal part of the system that has been built with the idea of providing a secure and decentralized framework for data analysis and storage. As it was mentioned before, InterPlanetary File System (IPFS) is defined by its creators as "*a distributed system for storing and accessing files, websites, applications, and data*." [48]. It was first developed by Juan Benet, and its progress in implementation works carries on as an open-source project. There are two major elements to consider beyond the sentence mentioned in [48]:

1. The information or contents are sought via a web request pointing at the contents themselves rather than their location. That is to say, the HTTPS request used to obtain

the resource provides the very resource itself, rather than the location (folder, directory, etc.) where it would be located. This is done so by identifying the content with a hash function output that becomes embedded in the Uniform Resource Identifier (URI) used for content requests. Therefore, every URI becomes naturally different, as every piece of content has a different hash output.

2. The nature of the web request (or as it will be shown, requests) perform to obtain the resource is different from the client/server regular one. IPFS relies on a decentralized storage of information, where there are several IPFS nodes (which can be any IPFS-enabled computer, as the demand for computational resources is relatively low) that can provide the requested piece of information. Once the resource has been obtained, it becomes available in the network for other users as well, so the resource will be shared among them rather than just obtained after the request has been completed. It is claimed that, in this way, not only resources are shared among the different parties for an easier access and increased availability of files, but also the computer used for downloading those files collaborates in distributing them, as it makes the files available to the network while keeping the anonymity of the users behind the IPFS nodes.

Therefore, there are two main features typical of IPFS: (a) content addressing via embedding hash outputs in the HTTPS requests and (b) decentralization of information availability. Theoretically, it is claimed by [48] that this latter feature should provide several advantages over traditional client/server requests: it will make the web more resilient (as files are available in several computers, even there is a major issue with the one that made them public in the network), it can fight censorship in a more effective manner (shutting down a single web site with is content becomes useless, as the content can be reproduced from other IPFS nodes, and closing all of them can be an impossible task if the information becomes widespread enough) and it can increase the performance of the web, in case connectivity at the physical level is limited (like mirrors providing content, nearby nodes can be easier to reach and data can be gathered from them in an easier way). IPFS works as a Peer-to-Peer (P2P) storage network, with IPFS nodes acting as peers providing access to information and/or storing it. The network will typically locate the requested resource with the content identifier rather than its location in a file system. In addition to this (referred to as *unique identification* via *content addressing*), there are two more technological fundamental principles of pivotal importance in IPFS: content linking via Directed Acyclic Graphs (DAGs, used for giving a unique identifier via a hash of the node's contents) and content discovery via Distributed Hash Tables (DHTs, used to find which peers are hosting the content that has been requested).

Thus, in the context of the proposed system, the usage of IPFS is justified by the possibility to offer a decentralized manner to store information related to the data collected by the UAV that will be saved in a JSON-formatted file once these data have been encased in the blockchain the system is built into. The files then will be distributed among the peers that belong to the IPFS network they take part in. Since those files (a) contain blockchain-related information and (b) become distributed among each of the IPFS participants, each of the IPFS nodes effectively becomes a blockchain node. In this way, IPFS provides an additional layer of improvements related to security and distribution, due to the following facts:

1. It provides replicas of the information collected by the system, both included in the blockchain (as explained before, the data collected is stored as JSON objects in files keeping a blockchain-based structure like the one described in the next subsection and in Section 4) and, in case they are left out, as files to be shared in the IPFS network.
2. Eliminates the need to create a specific system server and having to keep it up and running at every moment so that availability of the content is guaranteed. Since information is saved in every IPFS node, it will be available even if just one of the IPFS nodes is still online and can be reached.
3. It makes more difficult to alter the information stored, since not only any data tampering will be noticed whenever the blockchain data validation is taking place, but also

because it would have to be changed in each of the IPFS/blockchain nodes that share the data, which would require a very significant effort in terms of time, funds, and computational resources.

As it can be seen, IPFS provides significant usefulness in the context of livestock monitoring, especially when the animals will be used for as part of commercial purposes (i.e., meat, dairy or wool production) and information about their activities, feeding grounds and location can come in handy for regulators. Files containing information about the cattle are available for all the participants in the system, enhancing transparency with regard to cattle care and grazing habits, and even if the node that provided them to the IPFS network in the first place becomes unavailable, they can still be used by the other participants in the system that downloaded them. Therefore, IPFS was included as one of the main software components in the UAV-based system that is put forward in this manuscript.

3.4.4. Blockchain Prototyping

Lastly, blockchain was also included in the development of the solution, as another layer that would provide additional security and decentralization in information treatment. There are several reasons that justify adding blockchain to the development that is presented here:

1. It can be used for transparency in data for any required third-party assessment. The data collected by the UAV will be formatted so that they can be placed in a string of characters with any other piece of useful content that do not have multimedia capabilities, such as timestamps. As far as the development works shown here are concerned, images were formatted to Base64 so they could be included as characters. This image formatting is reversible, so images can be formatted back to their original data format if required.
2. It can store several kinds of multimedia information. As for the implementation works included here, images have been formatted to be included in the blockchain, but there is no reason not to include other multimedia information, such as video recordings. The underlying IPFS infrastructure can be used to share them as if it was any other kind of data, and so do all the other lower communication layers.
3. If used in the way is put forward in this proposal, blockchain does not demand a large quantity of resources, neither for energy nor storage. In the system that is proposed here, every block in the custom-made blockchain is used to store a single piece of information collected by the UAV. However, these blocks are shared as JSON files by means of the underlying IPFS network, rather than using any public blockchain platform or crypto-enabled network (such as Ethereum), so they do not require any gas for data transfers among the nodes. No funds or any kind of money is used in this system proposal to be transferred either, so money transfers do not need to be taken into consideration. Validation of the blockchain is done locally considering all the previously added content, as each of the IPFS nodes works as a blockchain node as well.
4. Due to the features previously mentioned, blockchain can be used as a support for good practices certification. As explained before and depending on the requirements from each institution, the information stored in blockchain can be used to prove that cattle is grazing in areas with good access for grass and water, along with any other visible feature in the animals themselves. Typical features of blockchain prevent an effective way of tampering with the information and, should it be tried, it would become rapidly noticeable due to the properties of the hash function used for block summary.

In a more specific way, blockchain provides distribution (there is no central authority making decisions; the most important operations in the blockchain-validation of the transactions taking place and creation of new blocks containing such transactions- are performed by the nodes participating in the system), redundancy (the exact same information is available for all the nodes that participate in the system, except for the very first moment that a new block containing transactions is spread among the participant nodes), transparency (widespread availability of the data for every node makes it very difficult to hide away information), immutability (once transactions have been included in the blockchain there is no way to pull them back, event if any kind of mistake is made in the data destination) and consensus (an algorithm is used to define what algorithm is used to define what kind of way will be use to agree on what is regarded as the truth). In the context of this proposed deployment, blockchain has been used to provide the features typical of it to the information that is collected by means of the following actions:

1. Distribution has been made possible with the underlying IPFS data networking system, which can be used to share any file related to the transactions stored in the blockchain.
2. Redundancy is also supported by IPFS, as there will be several nodes (or repositories) with the same shared information.
3. Considering what redundancy can offer in the previous point, transparency comes as another feature that can be provided for any kind of assessment of the information about farming offered in images and other multimedia.
4. Immutability will make extremely unlikely to alter in any way the multimedia data collected by the UAV once it has been deployed in the countryside.
5. The consensus algorithm used for this deployment is Proof of Work (PoW). While there are some issues about PoW and its energy demand (mining a new block usually requires a significant number of computational capabilities and, therefore, a high amount of energy is demanded for this procedure), that power consumption is acceptable in the application domain where tests have been carried out.

Finally, it must be considered how blockchain increases in a significant manner the security of the overall proposed system.

1. Redundancy will ensure that all participants in the IPFS network have the same information (that is to say, the same collection of images and timestamps), so any attempt made by just one of them to alter the information will involve making major changes in the whole blockchain (since due to the properties of the chained hash outputs and their verification, changing one will demand either controlling all the blocks deployed afterwards or changing all the hashes until the genesis block), which might require enough resources that outnumber all the other participants in the system with the PoW consensus algorithm used in this development, thus resulting in a significant need for energy and funds to perform such a change.
2. Immutability is also a blockchain feature that comes to the benefit of the proposed system. Since changing any hash output is extremely difficult, information that has been included in the customized blockchain about the monitored animals will remain the same, so any claim that is done by farmers or certification authorities can be backed with the data that has been saved.
3. The consensus algorithm required to make any addition to the blockchain demands that these changes are validated (by checking the provided versus the calculated hash outputs for each and every block) by all the members of the blockchain/IPFS network. As mentioned, this will give away any individual attempt to change any data on the customized blockchain.

As described, blockchain allows to share timestamped data with unique hash outputs that cannot be altered without having the other participants noticing about the tampered data, as the validation operation performed by each of the nodes in the blockchain will reveal that the information transmitted is not valid. In our deployment, the information regarding what data present in the blockchain is formatted as JSON files in IPFS nodes. Therefore, the IPFS nodes that share the files with the blockchain data effectively become blockchain nodes as well, as they are sharing the information stored in a blockchain at a specific moment. In this way, the system provides an additional layer of decentralization that at the same time is built on top of IPFS (which is the system used to share the files) it can effectively share the information provided by the files that contain the chain of blocks with information related to the system. Note that the IPFS nodes are free to decide whether to share the blockchain data files or not, so in this context blockchain depends on the IPFS infrastructure to become as widespread as possible.

3.5. Security Threat Analysis

As it has been previously mentioned, security is a feature of critical importance in this proposal, which distinguishes it from the ones studied in the existing literature within the application domain of this manuscript. For this purpose, a security analysis has been carried out, so that not only the main threats for the whole system are known, but also their location and how these threats could disrupt it. The main source of cybersecurity threats and the possibility for attacks comes from the facts that the UAV must receive commands in a remote manner (which implies an interchange of data according with the communication protocols used) and data received from the UAV will have to be stored at some location (even if the location is part of a decentralized subsystem). Consequently, wireless communications between the CGS and the UAV, the infrastructure for data storage itself and any other communication between the infrastructure for data storage and the UAV are locations where cybersecurity-based attacks could take place. These threats can be countered by guaranteeing that any system built based on CPS components will provide a collection of security characteristics that is characterized in the following manner:

1. Confidentiality. It is expected that the data that has been collected from the UAV will not be accessible by any unwanted party during the transfer procedures, so that they will not become exposed (as described in [5]). However, any party that has a genuine interest in the information (i.e., farm supervisor, foodstuff quality inspectors, consumers that demand it) will be granted access to this information whenever they request to have it.
2. Integrity. Data is expected to be stored in the exact same way that it was collected from the application domain where it was, so that information that can be inferred from those data is legit and not based on false assumptions. While confidentiality is a valuable feature in the system put forward in this manuscript, data integrity is of critical importance, as it will be used by several parties of very significant importance for the farm (supervisors, owners, quality organisms, information verifiers) and the cattle present in it.
3. Authentication. It is a security characteristic aimed to provide some form of valid identification that will be revoked, if needed, if any issue takes place. Failure to provide a proper identification should result in negative consequences for the spurious user.
4. Availability. This feature is related to the capability of a system to keep itself, or its features, accessible for end users without any unexpected issue, such as the ones that would be found whenever a Denial of Service (DOS) or Distributed Denial of Service (DDOS) attack are taking place. For the context of our proposal, it is the capability to keep the collected information available.

As far as the works presented in this manuscript are concerned, the most important security features are Integrity (since information will be shared among all the participants of an IPFS-based network, either from accessing the stored files or via the blockchain implementation that has been carried out) and Availability (information collected from the UAV will be displayed for all the participants in the network). In addition to this, hardware agents in the de facto CPS that this proposal consists of must be taken into consideration, so that their role in the system and the vulnerabilities they carry with them can be countered. These agents are (a) the UAV that is used in this proposal for data collection and transmission on the one hand (specifically, images and videos) and surveillance and monitoring flights on the other hand (that, as has been previously mentioned, can be either guided with an operator or autonomous), (b) the CGS (which in the deployment that has been developed for the manuscript is a laptop with all the required hardware and software components) and (c) the IPFS network that will be used to share the information and, by doing so, providing security-related features. It must be noted that the laptop used as CGS will also have an IPFS node running with it, so it will be used for both purposes at the same time. Once the hardware-based agents that make the deployment have been described, attention must be put on the boundaries among them so that limits among the components will define what kind of weaknesses can be exploited. There are two boundaries to consider in this case, as they are separating the three agents previously mentioned:

1. The one between the IPFS network and the CGS. It separates the IPFS nodes which, in the end, are also based on hardware elements, from the CGS elements used to upload missions to the UAV and/or control it during flights. It must be noted that, due to the dual nature of the hardware used in the deployment, the boundary that separates both parts of the deployment effectively goes through the hardware use for CGS and IPFS network.
2. The one between the CGS and the UAV. These two elements are separate entities that will communicate through the wireless 802.11 ac protocol, so that boundary separating the agent and the data traffic that goes through it must be born in mind. Unlike the previous one, the boundaries between these agents are physical and create a separation between the hardware elements of the system.
3. In addition to this, the blockchain network must be included in the security solution to be designed. The presence of such a subsystem proves to be an asset, as it is possible to share the data about the different pieces of information that have been added to the IPFS files included as part of the testing activities with an additional level of security derived from the hash outputs used to characterize each block (since PoW is being used as the consensus algorithm, any tried alteration will demand changing not only the hash output of the block where data is tried to be modified, but also the ones from any other block mined afterwards, requiring an amount of computational power hard to have by any regular user).

Finally, the data storage adds another infrastructure element that will have to be taken care of, as the information obtained (that, as mentioned before, will consist mainly of the pictures and videos collected by the camera installed in the UAV). All these considerations have been included in Figure 8. It encases in a graphical way the security threat analysis that has been done to be aware of the potential vulnerabilities or possibilities for an attacker to get into the system. It can be seen how two different boundaries have been set in the system that separate the three domains created by the subsystems:

1. The UAV subsystem faces threats related to UAV data tampering and UAV hijacking, which will either result in false data being transferred or damaging and/or losing the UAV. The UAV makes use of a wireless interface that is used in this context to send commands from the CGS and acknowledge their reception from the UAV back to the CGS, so security measures must be taken in the wireless interface
2. The CGS has two network data ports that, since they are used for receiving and transmitting data, can be exploited by a spurious party to enter the system. One port is the wireless interface that connects to the UAV, whereas the other is connected to the TCP/IP network that is used to connect the IPFS/blockchain capabilities that the CGS has as a node from these networks to its other distributed peers.
3. The IPFS/blockchain nodes represent a fully distributed network that operates under a peer-to-peer paradigm. Consequently, they are prone to cyberattacks typical of distributed systems, like the already explained DOS and DDOS, as well as any other attack that works by faking access credentials or tampering information files data into corrupting the content or showing something different from what was obtained from the UAV.

Once all the agents present in the system have been described, along with their boundaries and what actions can be prone to having cyberattacks on them, a summary of these issues must be made. For that purpose, Table 7 shows the main security threats faced by the system developed and how they are tackled to avoid unwanted results.

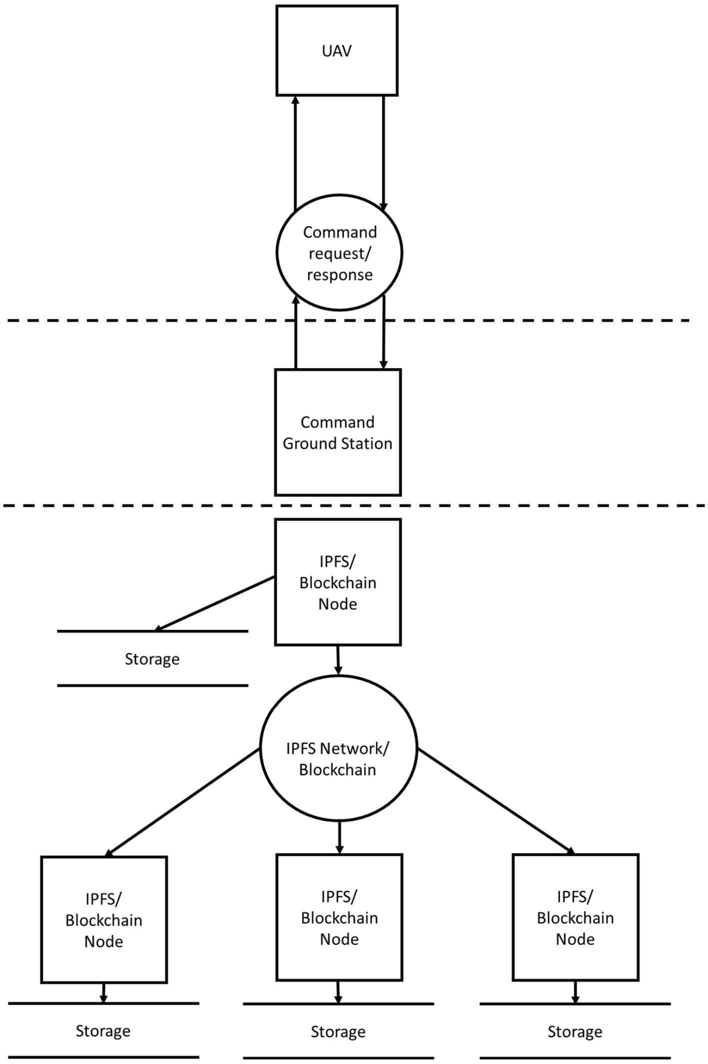


Figure 8. Security threat analysis for the proposed system.

Table 7. Security threats in the system and how to counter them.

Security Threat	Countermeasure
Command monitoring	Data encrypted by means of the wireless communication of choice
Command spoofing	Data encrypted by means of the wireless communication of choice
Denial of Service	Distributed data storage. Encrypted wireless communications.
Distributed Denial of Service	Distributed data storage. Encrypted wireless communications
Data Tampering	Distributed data storage
UAV hijacking	Secured wireless connection. Security in previous data flow stages
CGS credentials exposure	Credentials periodic update. Strengthening mechanisms for providing credentials

As it has been formulated, there are several security threats faced by the proposed framework. Nevertheless, it is also shown how these threats can be solved:

1. Command monitoring: it refers to the capacity of a spurious third party to obtain information about the commands that are being sent to the UAV, or how information

is being downloaded for the participants in the system in case this spurious party can exploit it to its advantage. It is countered in the proposed system by using the encryption capabilities that the 802.11 ac network provides.

2. Command spoofing: it is referred to the capability of a spurious party to send commands to the UAV without any permission or notification, so that the UAV will perform the actions requested by the spurious party rather than the legitimate ones. The most significant threat about this attack is that the UAV is taken away by the spurious party. Fortunately, it can be countered with the encryption capabilities that are used in the 802.11 ac wireless protocol.
3. Denial of Service: in this case, the spurious party will prevent legitimate users from operating the UAV and/or retrieving the information (pictures and videos) collected by means of it. There are two ways that the proposed solution can be used to counter this threat. On the one hand, the wireless protocol used for communications makes use of encrypted capabilities that will enable a higher level of security to the system. On the other hand, having data stored in a decentralized manner will make possible that it is available even if one of the legitime parties that is sharing it comes under attack. Such advantage is typical of distributed systems that enable data redundancy of some kind.
4. Distributed Denial of Service: its effects are the same as with the regular Denial of Service attack, but it is performed in a distributed, more sophisticated manner, as it is executed by a plethora of spurious parties (or a single one attacking from different machines) in a network. The countermeasures applied to the previous system are valid for this attack as well.
5. Data tampering: it refers to the possibility of altering the stored information about the livestock collected by the UAV and kept by the IPFS network that contains the blockchain files that store the information collected by the UAV used for monitoring purposes. This latter subsystem is the one that prevents effective data tampering: once the information is saved onto the network, it is done so with a unique hash number (an output that works as a piece of information characterizing the content of an image) and a timestamp, with both becoming embedded to the data provided. Since the hash number results from applying a hash function to the data, any change on the image or video collected will alter the hash number/output, thus resulting in a hash number/output different from the one that the other participants of the network have, so it will become rapidly evident who the spurious party is. In addition to this, it must be considered that IPFS uses a series of identifiers to guarantee that the data provided neither has been changed, nor the party that first provided it has changed its identification by any means. The IPFS peer identifier ensures that the identification of the node is used to know what user uploaded the files shared with all the other nodes. Additionally, the IPFS hash-based identifiers for the uploaded files provide another unique way of identifying the files in a way that resembles the presented in the blockchain part, so any change in such hash will be noticed by all the other parties sharing that information.
6. UAV hijacking. It could happen that a spurious party gets into the system and manages to alter the UAV normal flight. Since this attack is located at the very end of the system (there is no other subsystem beyond the UAV, nor the UAV connects to any subsystem except for the purpose of taking actions based on the commands that have been received) any security flaw in the wireless interface used to control it or in any previous stage (i.e., credentials to access the CGS got leaked, as it will be mentioned in the next point) can be responsible for the success of this cyberattack. To prevent this, the best action that can be carried out is making use of a secure wireless connection between the CGS and the UAV. In our implementation of the proposed system, this has been done with the built security capabilities provided by the 802.11 ac wireless protocol used for command and data transfer between the CGS and the UAV.

7. CGS credentials exposure. If access to the CGS is obtained by an illegitimate user, they will have complete access to one of the most prominent elements of the system and most of the other security measures will become useless. To prevent this, credentials must be created following several guidelines, which include updating those credentials periodically or making them stronger by applying hash functions or cryptography features on them.

Considering all the hardware and software components present in the system, security in this manuscript has been deployed as shown in Figure 9. It can be noted how there are security capabilities at almost every level of communications, as shown below:

1. The wireless, physical interface is based on 802.11 ac, which provides data encryption capabilities that secure communications when real-time commands are transmitted to the UAV, or images are transmitted from it.
2. At the transport layer, Transport Layer Security (TLS) protocol can be offered as an additional security solution where the transport layer that transfers segments through the network becomes secure as well. Besides, HTTPS requires the usage of TLS for its own functionalities, so its usage is little less than mandatory in this context: with a TLS certificate, HTTPS can encrypt web requests and responses (which becomes especially useful when requesting information to the IPFS network) that can be digitally signed.
3. Security protocols provided at the application level before reaching the IPFS network has also been offered by means of using HTTP Secure (HTTPS) as the application layer protocol, which will enable further securitization of communications when working combined with TLS.
4. The IPFS network provides a level of decentralization that, in addition to storing information in a decentralized manner, provides a hash number and a timestamp that characterizes every new whole piece of data.
5. Blockchain files stored in the IPFS nodes ensure that the collected information is also provided an additional hash that, instead of just identifying each of the data, can effectively link the pieces of data as they are collected by the UAV, thus not only characterizing each of them, but also creating a time-ordered list of information that, due to the usage of consensus algorithms, cannot be modified without knowledge by the blockchain nodes (and by proxy, the IPFS network).

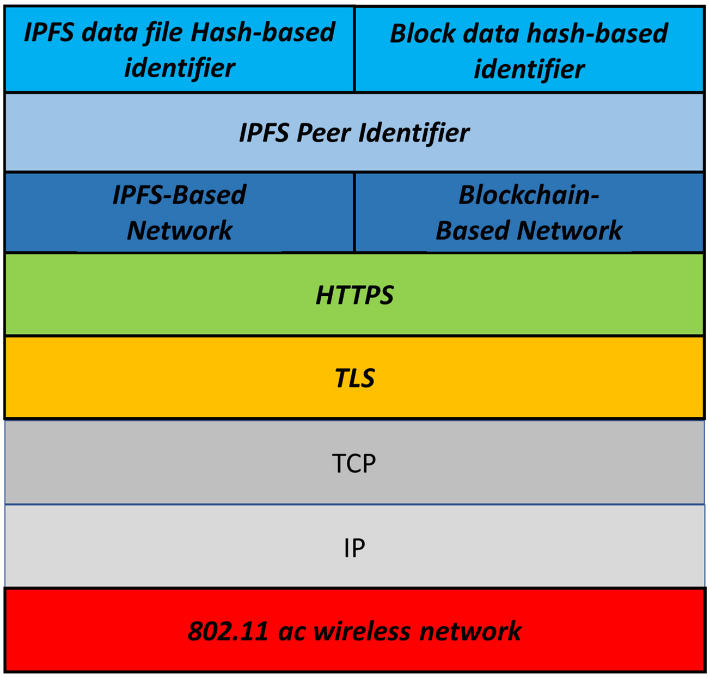

IPFS data file Hash-based identifier
Block data hash-based identifier
IPFS Peer Identifier
IPFS-Based Network
Blockchain-Based Network
HTTPS
TLS
TCP
IP
802.11 ac wireless network

Figure 9. System layers. Security-enhanced ones are highlighted.

It must be taken into consideration that due to the plethora of security measures that has been taken from using the suitable features from each of the communication protocols (HTTPS, TLS, 802.11 ac) and the distribution capabilities of the two main tools used at the data level (blockchain, IPFS), the security mechanisms that are put forward in the proposal are part of the characteristics used in those developments, rather than any program codified ad hoc. This latter aspect offers an advantage to the users of the system, who can replicate a high security level by just mirroring the components present in this proposal, instead of having to develop any new code.

3.6. Assembly of the Prototype System

As described before, it was required that the UAV had a GNSS signal reception system, so a choice had to be made between a controller with an integrated GNSS signal reception system or integrating one that would always indicate the position of the UAV to the operator. In this case, the first option was chosen since, besides being more efficient for it to be integrated into the controller due to space and aerodynamics, it was also more efficient for communications bandwidth between the base station and the controller. As already explained in chapter 3, the controller chosen for the project has been the Navio2, which is characterized as a HAT (Hardware Attached Top) for the Raspberry Pi board used to integrate the hardware components. It must be noted that Navio2 that has several precision sensors, as well as an integrated GNSS signal reception circuit.

The Operating System installed on the Raspberry Pi is a preconfigured distribution of Raspbian, which is the recommended Operating System for Raspberry based on a Debian GNU/Linux distribution [49]. To install it, it is only necessary to download the preconfigured image from the Navio Emlid tools website and install the microSD card that will later be inserted in the Raspberry Pi. Once the installation process of the operating system has been completed, it was necessary to edit the *wpa_supplicant.conf* file (which is in the/boot directory) to configure the Wi-Fi network where the ground control station must be found for subsequent communication with the aircraft (in this case, the UAV). Once the Raspberry Pi was connected to a Wi-Fi network, it was also possible to connect to it through the Secure Shell protocol (SSH) so that the configuration of the UAV will be completed.

Afterwards, the UAV was assembled by mounting the components described in the third chapter. Figure 10 displays the result of the UAV with all its components fully assembled. The blue box located in the center of the UAV is the Navio2 controller; the GPS antenna (black) and the video transmitter antenna (blue) can be seen as well.

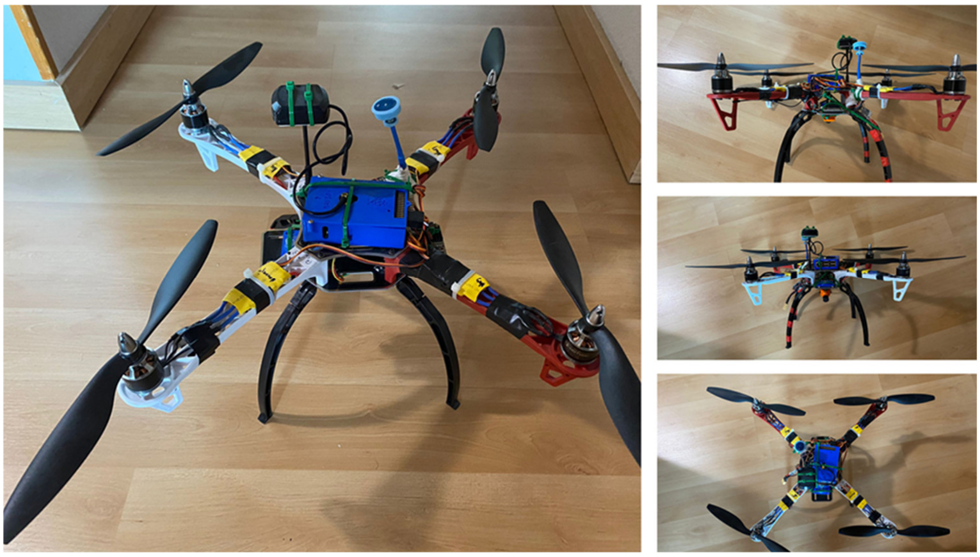


Figure 10. Assembled UAV.

The UAV is now ready to be configured through the Mission Planner software. However, to perform this task, there must be a Wi-Fi network to which both the Raspberry Pi of the UAV and the CGS that runs the software are connected. To configure the UAV, the battery must be added to the UAV by the port enabled for it once the connection to the Wi-Fi network of both the Raspberry Pi and the CGS has been established. From this point, the Raspberry Pi Operating System will boot and the Arducopter software will start. The first step that must be carried out is the process of "binding" (pairing) or establishing a connection between the radio control transmitter and the receiver on board the aircraft. Here, a communication channel between the transmitter and the UAV is created the first time that communications between both entities are set (it is only necessary to do it in the initial configuration since in future occasions the connection will be established automatically) by updating the transmitter to the latest version of the OpenTX software, as this it is necessary to connect the transmitter to the computer via the USB cable. Prior to this step, the latest version of OpenTX Companion software must have been installed on the computer. Once all the necessary software has been installed, the station must be turned on in bootloader mode.

After switching on the transmitter in bootloader mode, it must be connected to the computer via the USB cable. Afterwards, the following procedures must be carried out according to the hardware built specifically for the purpose of this system:

1. The Radio Controller module must be configured. To do so, the software used in such controller might have to be updated. This is required in case there are new functionalities that improve the usefulness of the Radio Controller itself.
2. Once this procedure is complete, the pairing process (binding) between the receiver and the transmitter must be completed. This will be done by adjusting any required parameters on the Radio Controller (maximum power output, frequency, etc.).
3. When the connection process between the transmitter and the receiver has been successfully established, the flight mode will be configured. These flight modes are configured through the Mission Planner software from the CGS and are activated and deactivated from the transmitter.
4. It will also be necessary to make the correct configuration of the radio control channels to carry out proper handling of the UAV. To do so, it is necessary to connect the battery to the aircraft and connect to the Raspberry Pi through the SSH protocol.
5. Afterwards, the different components of the UAV can be calibrated. In this regard, we proceed with the calibration of the accelerometer. This component is integrated in the controller and is responsible for providing information on the forces that work against the UAV flight (wind, gravity, etc.) to keep it always stabilized. It must be connected to the CGS and place the aircraft in the positions indicated by the Mission Planner software.
6. The UAV compass must be calibrated right afterwards. This component is also integrated in the controller and allows the aircraft to know in which direction it is pointing. To carry out this process it is necessary to take the UAV and rotate it 360 degrees around all axes.
7. Next, the radio transmitter is calibrated. It is necessary to ensure that all the transmitter controls respond correctly and that their transmitted signal level corresponds exactly to that received by the UAV. It is needed to configure throttle, pitch, yaw, roll maneuvers and a switch to select flight modes.
8. The final step required in the UAV setup is to select the flight modes to use. The Mission Planner software has 25 flight modes, of which 6 are used. The flight modes are assigned to one or more of the channels that the transmitter has and are selected through the position of the switch. The flight modes used are as follows:
    a. Stabilize: This flight mode is used most of the time. It allows the operator to fly over a surface keeping the UAV in a stable position during flight.

b. RTL (Return to Launch): When this flight mode is activated, the UAV automatically returns to the point where it took off and lands. It is very useful for when the operator wants the UAV to return to the base.

c. Auto: used to perform predefined missions through the software (usually, autonomous missions).

d. Land: It reduces progressively the UAV altitude to ground level. It is used to land the UAV.

e. Brake: used to perform an emergency stop. In the event of an unexpected event or accident, it stops the UAV motors.

Once the configuration of the components and parameters of the aircraft has been completed, the tests and missions can be undertaken.

4. Testing and Result Discussion

In this section, the testing operations that were performed to know the suitability of the developed system have been displayed. The UAV was deployed in an agrarian exploitation where a group of sheep had to be monitored, so that (a) their grazing habits and locations would become better known, (b) the farm staff were able to see the whole group of animals at the same time from an aerial perspective and (c) the UAV could, to an extent, guide the sheep towards a specific location. While this last objective was achieved, it must be noted that the reviewed literature has proven that after flying the UAV for several times, animals will get used to its presence and will not move away from it significantly unless they are frightened into doing so, which is to be avoided for animal welfare reasons.

4.1. Preliminary Testing

Before deploying the UAV where the sheep were located, a series of tests had to be carried out to assess (a) the general assembly of the prototype (especially any component that might had been not properly mounted) and (b) the flying capabilities of the prototype. It was decided that the first flight test should be conducted in a closed environment with enough space to be able to lift the UAV approximately one meter off the ground. With this test it could be assessed whether the placement of the motors and propellers is correct. Should any mistake had been made, the UAV would typically flip over before it was able to properly take off and stabilize itself on air. It is very important that during the configuration of the flight mode and the channels of the transmitter, a control switch is assigned to the "emergency stop" function. This function will halt the rotation of all the motors instantly and will bring the UAV to the ground in case it flies beyond the properly set boundaries of the mission due to external circumstances (usually related to weather conditions). During flight tests, this function made possible avoiding major accidents in the event of an unforeseen event. To test the correct operation of this emergency stop, it is enough with arming the UAV, activating the emergency stop and checking whether rotors are truly stopping when requested.

Once the motor and propeller tests have been successful and the correct operation of the emergency stop of the motors had been verified, the first outdoor flight was made. Due to the dimensions and weight of the UAV that has been assembled, it was not possible to fly it just anywhere, as current regulations regarding aviation safety in the demonstrator location had to be observed. In addition to this, operators required a Remotely Piloted Aircraft System (RPAS) pilot certificate issued by a competent authority. The most important considerations to take into account when carrying out this flight outdoors were: (a) making sure that the location where the test was located was far from any population, (b) that this location was a place where it is not explicitly prohibited to fly a RPAS (due to proximity to an airport, military base, etc.) and that there was no group of people under the area where the tests were going to be carried out so as not to compromise anyone's safety. The first test that was carried out outside consisted of a manually operated UAV flight to become familiar with the response of the UAV to the controls. It was possible to observe that the flight was stable and precise. In addition, the humming sound emitted by the aircraft's own engines while it is in the air was expected to be loud enough to cause the desired movement of the herd of sheep intended to be directed. The operator always had visual contact with the UAV; the maximum horizontal distance reached was approximately 150 m.

After performing the manual flight test, a simple autonomous flight test was performed. In this case, and to prevent any unwanted issues, the pilot had the ability to recover the control of the UAV at any time during the flight. For this test a simple flight plan was prepared consisting of the following actions:

1. Takeoff from point A and lift to 10 m high.
2. Displacement in a straight line of 15 m to a point B.
3. Wait 5 s at point B.
4. Return to point A.
5. Landing.

This second flight test had an unexpected ending, when the UAV began its descent before reaching point A due to a planning error. Having carried out the test in a rural environment with an irregular surface, when the supports touched the ground, there was a loss of stability that caused the UAV to land in an unwanted manner, to the point that it flipped over. This showed that rural operations with UAVs can face challenges unseen in other areas where human presence has modified the environment and created flat surfaces (i.e., open parking lots, asphalt, or pavement tiles).

The final flight test carried out was a manual flight, which was fully successful despite having several tall trees as obstacles. Again, this test taught the testing team a lesson about when to use guided or autonomous flights when they are required. It was observed that the movement of the UAV was agile and responded perfectly to the operator orders, with a stable flight and without any loss of control. In this occasion, both takeoff and landing were carried out smoothly.

4.2. System Deployment in the Real Scenario

Further tests were done in the main farm exploitation expected to make use of the developed system. The objectives with these tests were (a) assessing the interaction between the UAV and the cattle, (b) saving information from the performed flights and missions and (c) storing the data in a IPFS node to have the information in a decentralized repository. For the first objective, UAV missions were performed to monitor livestock and have an accurate idea of their interaction. The location to perform such an operation was a farming exploitation at the *pedanía* of Alpedroches in Spain. *Pedanía* is a Spanish term that defines an "*entity with a territorial scope inferior to the municipality that lacks legal personality and that constitutes a form of decentralized organization of the municipality for the administration of separate population groups*" [50]. This usually involves having several *pedanías* managed by a single townhall (located in a bigger village or a town) to minimize rural management costs and assigning budget in rural areas in the most efficient manner. Therefore, Alpedroches can be considered as an example of *La España Vaciada*, which refers to the towns and locations that have become devoid of people, with especial intensity in the rural Spain. As such, only 2 people are censed to permanently live in this location, which are the farm owners of the exploitation where the tests for this system were carried out. Therefore, having technological solutions that can be used by only a few people (as mentioned, requiring a small amount of manpower and a relatively flat learning curve) is of great usefulness in this context. Sheep livestock is common in the area; it is used as a source of several products (lamb meat, wool, milk, cheese) so it is a significant part of the local economy of the land. Thus, the importance of having tools that make easier assessing the possibility of obtaining certifications is of major importance to assess the quality of the resulting goods and foodstuffs from cattle. It is in this context where information obtained from the UAV and transferred to a IPFS node comes of major importance, as it can be used as support material to assess what kind of grasses were eaten by the sheep or what kind of natural environment they were bred in.

The location of Alpedroches and the exploitation where tests were performed can be seen in Figure 11. The total surface of the location used for testing was of 300 hectares, which is average considering the kind of animals used and their needs for space and grazing. Two folds are used at the left side and the right side of the exploitation are used to keep the sheep inside when sheep must stay put. The layout of the testing location comes in as very useful for UAV flight and data collection, as it provides a large area to have cattle without any restrictions in movement, while at the same time the retrieved information can be stored and shared with the available wireless communication protocols and standards described in the prototype section.

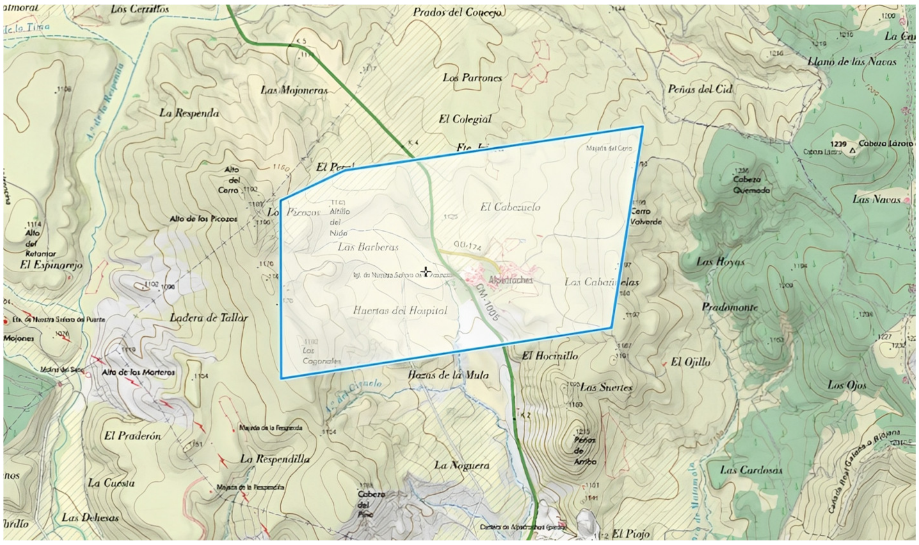


Figure 11. Location and extension of the testing location.

A first flight of approximately 10 min duration was made. During this test, it was possible to monitor the sheep from a significant distance (according to the idea of having the system for cattle monitoring) and to make several tests about driving the herd in a desired direction (which specifically aimed at the formulated objective of assessing the interaction between the UAV and the cattle). During the flight, it was possible to monitor the cattle farm from one end to the other several times, proving that control of the entire farm could be maintained with the use of the prototype. Tests regarding moving the herd by making use of the UAV showed that it is possible to steer the sheep in the desired direction (as it was already shown in the reviewed literature). It was also proven how one of the great advantages of using UAVs for livestock monitoring is the speed with which it is possible to reach the location of the herd. Indeed, it took the UAV just under a minute to cover the required distance, which according to the farm staff would have taken from ten to fifteen minutes. In addition to that, it was very advantageous to use the UAV to collect visual data from the herd of sheep (thus fulfilling the objective b) about saving information from the performed flights and missions). It can be observed in Figure 12 how it is possible to monitor cattle and have a clear control of the position and the actions that the sheep are carrying out.

If required, the operator has the possibility of approaching the herd and directing it in the desired direction (thus effectively using the UAV as a sheepdog) by standing behind the sheep herd and moving the UAV as if it was "pushing" the animals. This is represented in Figure 13, where it can be seen how the UAV approaches the herd with the aim of driving it back to the stables. Not only the proximity of the device to the herd can be spotted, but also it shows how the sheep react favorably and move in the same direction as the drone.

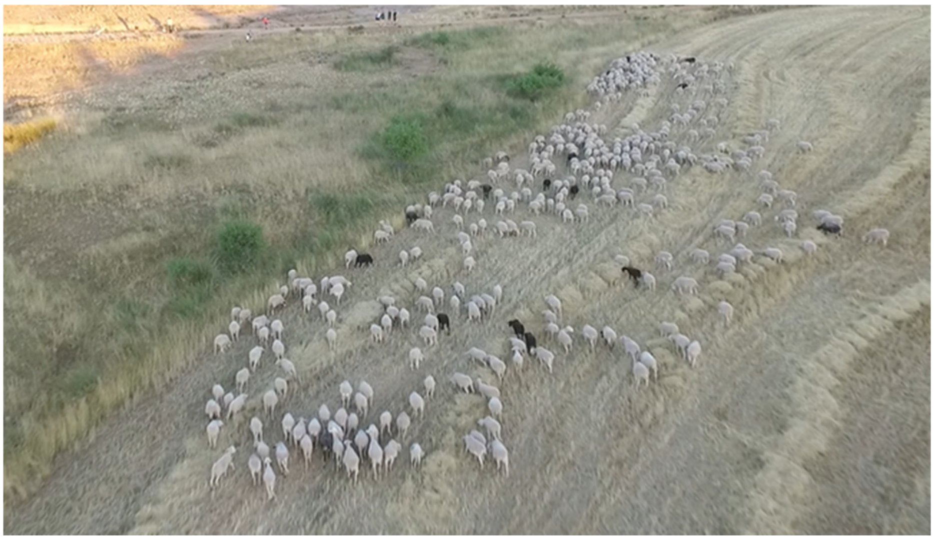


Figure 12. Cattle monitoring via UAV.

Further flights were carried out where it became evident that a UAV can be used to obtain information about the herd of sheep. However, there were still two more experiments to perform. The first one was making those data available via IPFS network, whereas the other was transferring those data into the built blockchain. To have an IPFS node, it was required to download the software facilities as shown in the official web site and, as long as there is an Internet Protocol-based network connectivity and the installation had no issues, a node would become operational with all the required features for file sharing at the data level working properly.

Figure 13. Close view of the sheep herd.

As far as the blockchain development is concerned, there were several elements that were included in each of the blocks:

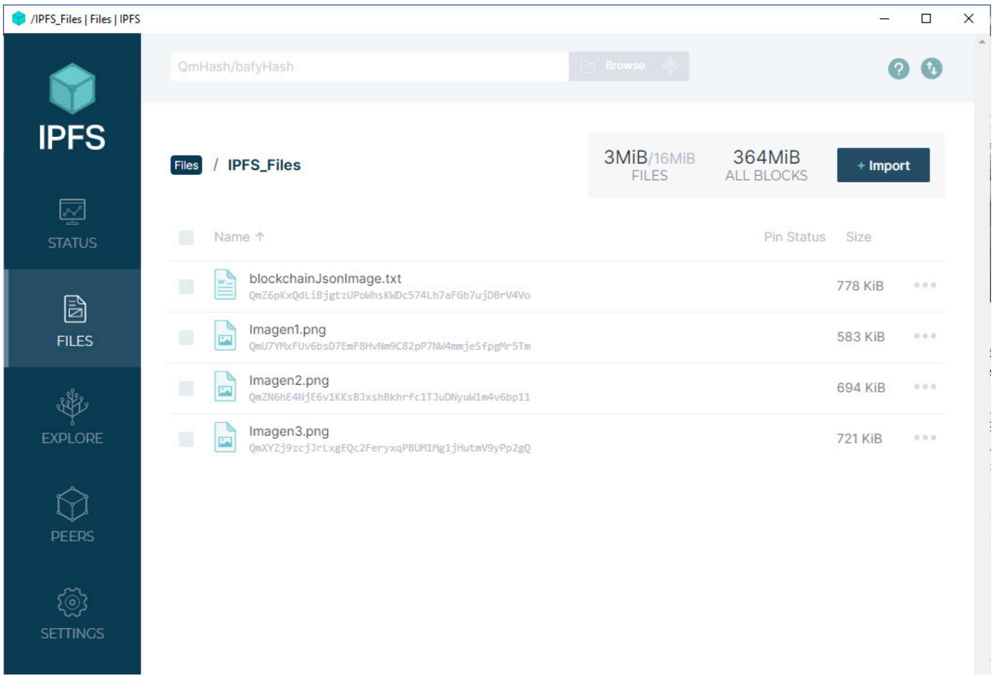
1. Current block hash: it identified in a unique manner the data that had been included in the system. It can be regarded as the result of applying a hash function on several pieces of information (usually, current block data, a nonce number, the previous block hash, and timestamps as input data).
2. Previous block hash: it was used as part of the data utilized as input to calculate the hash of the current block, thus chaining together each of the blocks that contain data.

3. Data: These were the actual information collected by the UAV. Typically, it will consist of some multimedia information that will be formatted so that it can be added to the blockchain as text. In the tests that were carried out the codification chosen was Base64, so images were converted into a string of characters that was added to the block. When required, this codification can be reversed, and the image is back to its original format and appearance.
4. Timestamp: it was a piece of information useful to know when data were included in the blockchain.
5. Nonce: it is an acronym of "*number used only once*" used to guarantee that there will not be two similar hash outputs in the blockchain.

To improve portability and shareability of the information (thus taking advantage of the IPFS data network running just below the blockchain from a layered point of view) the blockchain information was stored as files shared throughout the IPFS network. As explained before, the main motivation to have blockchain in this deployment is providing an extra layer of security and distribution, which adds up to the one provided by IPFS. Since the computers used to store the IPFS-related facilities are also hosting blockchain data shared among all the participants, those computers become blockchain nodes as well.

An example of the appearance of the IPFS node once information has been uploaded onto that server has been displayed in Figure 14. The node has several tabs that aid understanding the different elements present in an IPFS network:

1. Status: this tab is used to visualize information about bandwidth usage over time and network traffic during a specific period.
2. Files: used to show the files that have been uploaded onto the node, along with what characteristics has each of them, like the IPFS link to access it or its identifying hash.
3. Explore: used to see the Merkle tree resulting from the application of the InterPlanetary Linked Data.
4. Peers: it is useful to explore the number of users present in the IPFS network where the information is being uploaded.
5. Setting: this tab is used for the IPFS node system settings, such as the public gateway used for data requests or the file pinning so it will not be garbage-collected.



Name ↑	Pin Status	Size
blockchainJsonImage.txt QmZ6pKxQdLiBjgtzUPoWhsKWDc574Lh7aFGb7ujDBrV4Vo		778 KiB
Imagen1.png QmU7YMxFUv6bsD7EmF8HvNm9C82pP7NW4mmjeSfpgMr5Tm		583 KiB
Imagen2.png QmZN6hE4NjE6v1KKsBJxshBkhrfc1TJuDNyuW1m4v6bp11		694 KiB
Imagen3.png QmXYZj9zcjJrLxgEQc2FeryxqP8UM1Mg1jHutmV9yPp2gQ		721 KiB

Figure 14. Appearance of the dashboard in the IPFS node.

The four files that have been included in Figure 14, which are part of the testing activities carried out, can be accessed via IPFS public gateways. Due to the decentralized nature of IPFS, each of the nodes that make part of the network are servers themselves that share the available information among the peers that are part of the IPFS network. The public gateway that has been chosen to visualize the data is ipfs.io, so the four files that have been included as a test in this node will be accessed with the following Uniform Resource Identifiers (URIs):

Monitoring cattle from the distance once (Figure 12):
https://ipfs.io/ipfs/QmU7YMxFUv6bsD7EmF8HvNm9C82pP7NW4mmjeSfpgMr5Tm
Monitoring cattle from the distance twice:
https://ipfs.io/ipfs/QmZN6hE4NjE6v1KKsBJxshBkhrfc1TJuDNyuW1m4v6bp11
Monitoring cattle at a close distance: (Figure 13):
https://ipfs.io/ipfs/QmXYZj9zcjJrLxgEQc2FeryxqP8UM1Mg1jHutmV9yPp2gQ
Figure 12 formatted to Base64 and included in blockchain data:
https://ipfs.io/ipfs/QmZ6pKxQdLiBjgtzUPoWhsKWDc574Lh7aFGb7ujDBrV4Vo

From the previous examples, the last one must be further discussed due to the objectives of the manuscript. As it can be seen in the piece that has been included below (the previous link shows that the Base64 formatted image is too long to fit it in this manuscript) it contains the information parts (hash, previous hash, data, timestamp and nonce) described before. Note that the image has been inserted right after the first block that has "Genesis" as data and "0" as the previous hash (since there is no previous hash to take the hash from).

```
[
{
"hash":
"36b81a86281783aa06ad46b269b11a57fe39c784f17888ffcb0a5674399e4bd6",
"previousHash": "0",
"data": "Genesis",
"timeStamp": 1662373905696,
"nonce": 0
},
{
"hash":
"2817df1646973ecbc25ee620357f9a7a4ca595b13aaad862ac42d614ce94ac23",
"previousHash":
"431695e2c33be553bb6faef3c9470764bcb4b11d12978ad7d91e9b9ccc8e701a",
"data": "data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAocA
[ . . . ]
BJRU5ErkJggg\u003d\u003d",
"timeStamp": 1662373905728,
"nonce": 0
}
]
```

Therefore, it is proven that IPFS can be used to share not only multimedia information, but also blockchain-based data that will aid in the assessment of how livestock has been raised in any exploitation.

4.3. Result Discussion

Since IPFS works in a decentralized manner, one feature that must be considered is that the performance of the IPFS network is related to the number of peers that are sharing the files in such network. Consequently, the more popular a specific content is (especially when they are related to viral multimedia pieces) the more likely it is to become shared immediately. Since the uploaded files were not of significant public interest, it took a while until they became available for all the peers in the network. One way that this can be mitigated to an extent is by making use of gateway caching, which will enable several public gateways to provide access to the information that is being provided by an IPFS node. In the case of this manuscript, a Public Gateway Cache website [51] was used for this purpose. After caching the information via this web site, the data was easy to access in an almost immediate manner. As for the experimental analysis, and as it has been previously described, there were several experiments that were run:

1. UAV flight over flat terrain: this experiment was performed to test the performance of the UAV that had been built from the scratch with the purpose of checking how good its flying abilities were. It was expected that the UAV would fly with ease and no issues. Results matched the expectations.
2. UAV flight over hilly/rocky terrain: this experiment was performed to know how different terrain conditions would affect the UAV flight, or if any change would take place at all. While flight itself was fine, the UAV flipped over when landing had to be taken (this resulted in no damage for the UAV). More careful planning for landing was performed afterwards.
3. UAV flight over cattle: the flight of the UAV was tested to know to what extent the system built with FPV equipment, along with the UAV, would work for cattle monitoring when the UAV flies at a certain altitude above the animals. They worked as expected with no issue. Due to altitude flight, animals were oblivious to the existence of the hovering UAV in this experiment.
4. UAV shepherd-like flight: this experiment was carried out with the purpose of gathering the sheep scattered in the countryside, in a functionality that would mimic what a shepherd dog would do. There were some previous ideas about what to expect from this experiment due to the reviewed literature, so it was believed that the cattle would behave in way comparable to how they would behave with an actual shepherd. This expectation was indeed confirmed by the field tests: the UAV would push the sheep around so that they became a compact herd that could be rounded up and guided with ease.
5. Data collection from UAV: the experiment described shows that information could be obtained from the UAV, and it would be relevant enough. Since images of the gathered sheep and their location were obtained, expectations regarding this experiment were regarded as fulfilled.
6. Data sharing via blockchain: this experiment had as target the information that had been collected from the UAV, as it was expected to include it in a blockchain tailored for this proposal that would enhance its availability. Once the images were converted to Base64 text, there were no issues adding the to the tailored blockchain that was developed for the project.
7. Data sharing via IPFS: the experiment involved sharing he data that had been integrated in the blockchain as JSON-formatted files among the participants of the IPFS network. Although it was possible to perform this action, the public caching website described in [51] was used to enhance data availability.

These experiments have been further summarized in Table 8.

It is the opinion of the authors of the paper that the hypothesis that was presented in Section 2 (“*can a UAVs-based framework be used to monitoring livestock so that data can be collected and can be kept in a secure way?*”) has been answered positively, as it has been proven that the UAV can be used to monitor cattle with significant precision, and the data collected from have been gathered and shared in a secure way via a system that made use of a theoretical model that was implemented and tested in real world conditions. From the point of view of the hypothesis, a prototype was designed and implemented as described in Section 3 (which fulfills the requirements formulated in such section) and the testing activities performed in Section 4 prove that, judging from the usual functionalities expected by farmers, the described system has been validated.

Table 8. Experiments performed and comparison between expected and obtained results.

Experiment Performed	Expected Result	Obtained Result. Deviations
UAV flight over flat terrain.	Flight where UAV will show its performance.	Regular flight where UAV behaved accordingly.
UAV flight over hilly/rocky terrain.	Flight where UAV will show its performance.	Regular UAV flight, but it had unsatisfactory landing.
UAV flight over cattle.	Flight where the UAV will be used to monitor cattle from a certain altitude.	Regular flight where UAV behaved accordingly.
UAV shepherd-like flight.	Flight where the UAV will be used to group cattle.	Cattle and UAV behaved accordingly. Likely to reduce effectiveness over time.
Data collection from UAV.	Images obtained from the UAV flight.	Images obtained from the UAV flight.
Data sharing via blockchain.	Data will be incorporated onto a tailored blockchain.	Data was incorporated onto a tailored blockchain.
Data sharing via IPFS.	Data will be shared among IPFS network participants.	Data was added to the IPFS network. Caching information was used.

5. Conclusions and Future Works

Overall, the tests carried out in the farm were deemed as satisfactory. When the herd of sheep was monitored, information about their whereabouts from a remote location was gathered in a reliable manner. These advantages enabled farmers and farm staff to save a significant amount of time because they could take visual control of the situation in a few minutes. Should they have performed these actions in a traditional way, they would have needed to move from one point to another either on foot or by using vehicles (thus, the proposed system helps in both saving fuel by not having to physically move and avoiding the emission of greenhouse gases into the atmosphere), so this also translates into economic and environmental savings for farmers and farm staff. The fact that the animals reacted in the desired way to the stimulus produced by the UAV when they were in the countryside was also of most interest. It must be noted, though, that sheep usually move all together without breaking the unity of the herd, which makes handling the whole a more doable task. Other animals of more individualistic nature (bulls, horses) are likely to be harder to track.

From our point of view, there are several innovations that have been performed because of the research and development work done in this manuscript. They are strongly linked to the contributions that the paper offers, along with the design, implementation, and testing work:

1. Tailored UAV and FPV systems. Rather than using a commercial solution or some hardware reused from a different project, an UAV specifically built for the purpose shown in this manuscript has been described from two different points of view: (a) on the one hand, the information compiled from professional staff working in cattle monitoring and guiding throughout the countryside and (b) the studied State of the Art and its remaining open issues. With these two contributions a list of functional and non-functional requirements was developed, both for the UAV and the other subsystems of the developed solution, that provided guidelines and boundaries for the kind of UAV to be used, especially in terms of the radio transmission equipment (which had to be suited to the distances and needs of the farmers, so they could monitor the animals from a distance ranging in kilometers) and the FPV equipment to be used in visualizations (i.e., what kind of goggles to use). To the best of our knowledge, there is no other research work that offers this kind of solution based on requirements obtained both from previous research work and interviews from end users in this application domain.

2. Usage of blockchain for UAV information storage. Blockchain as a way to store multimedia information collected from UAVs in a distributed manner is, at the moment of composing this manuscript in the application domain of agriculture, a technology that has not been used to a significant extent. It provides features that are desirable for end users at farms, like data redundancy, immutability transparency that are hard to provide combined in a reliable manner. It has been previously justified, along with the other used technologies, why the addition of blockchain is a suitable idea, and how it can provide benefits to any farmer looking to prove that their cattle have been well-treated, the same way that blockchain is used in developments related to the production of foodstuffs in the supply chain and other manufacturing procedures.
3. Usage of IPFS for information sharing at the data level. In order to enhance security and availability of the data shown, an infrastructure to share the files containing blockchain information has been provided, so that once the information added is verified and validated (which is done by the consensus algorithm used in the blockchain development) can be shared among a plethora of participants in a fully decentralized manner and without requiring any centralized repository that would question the legitimacy of the decentralization of the system (if the information provided is kept in a repository controlled by a single party, regardless of what kind of data structure is used to save the information). Usage of IPFS is unknown to us in the context that this manuscript describes.
4. Lastly, this list of functional and non-functional requirements (as depicted in Tables 4 and 5 and developed in Table 6) establishes a starting point for similar deployments that can be reused for application domains that are comparable to the one that has been presented here. The advantage of having this list to give design and implementation for hardware and software components should not be underestimated.

It was also proven that through the image offered to the operator by the camera on board the UAV, it is possible to control the facilities of the livestock farm and its status. For example, a farmer can see if the animals have water in the drinkers and food in the feeders. Controlling the state of the salt stones scattered on the farm used by the animals to get additional minerals can be done by using the UAV as well. Finally, using IPFS/blockchain as the means of information storage is useful to provide timestamped information that, with the consensus algorithm used, would require the spurious party to modify such a significant number of blocks that it could not go unnoticed, thus providing another tool for the assessment of cattle living conditions that ensures that the provided multimedia information is authentic and legitimate.

Although the tests had favorable results, there are still some challenges that could be proposed as future works. In the first place and considering the reviewed literature, the animals will diminish their reaction to this stimulus after a prolonged exposure; while that would be good for purely monitoring activities (they will behave in a more natural way) it will make harder controlling the herd by just using the UAV. Another of the challenges to consider is the difficulty that the UAV operator may have to face when trying to handle it in weather conditions that are not as favorable as those of the days on which the tests were carried out. Although using a regular UAV during rain is generally discouraged, it would be necessary to study how the wind or fast temperature changes can affect the flight, and up to what speed of sudden drifts of wind the UAV can maintain its stability.

While IPFS provides an additional layer to make data tampering or alteration more difficult, its dependence on the number of online peers to be effective is still an issue. Although this problem can be solved to an extent in short term (caching files with tools as the already presented Public Gateway Cacher) the most suitable long-term solution is the increase of the number of peers so that files will become easier to access, which is challenging to obtain with the implication of one mere node. As far as this application domain is concerned, the upload of material of high popularity and potential fast shareability is usually not possible, as the images, video and files provided are related to research and Smart Farming, which fall short in comparison with other multimedia content (music, videos, etc.).

Author Contributions: J.C.Ú.O. made major contributions in the development and testing of the UAV, as well as farm staff interviews in the location where the system was tested. J.R.-M. contributed to this manuscript in the IPFS development and the reviewed literature on this topic. M.M.-N. and J.G. by providing the functional and non-functional requirements required for the prototype after considering the open issues and needs for farmers in the testing area. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that has been included as IPFS files can be found here: Monitoring cattle from the distance once (Figure 12): https://ipfs.io/ipfs/QmU7YMxFUv6bsD7EmF8HvNm9C82pP7NW4mmjeSfpgMr5Tm; Monitoring cattle from the distance twice: https://ipfs.io/ipfs/QmZN6hE4NjE6v1KKsBJxshBkhrfc1TJuDNyuW1m4v6bp11; Monitoring cattle at a close distance: (Figure 13): https://ipfs.io/ipfs/QmXYZj9zcjJrLxgEQc2FeryxqP8UM1Mg1jHutmV9yPp2gQ; Figure 12 formatted to Base64 and included in blockchain data: https://ipfs.io/ipfs/QmZ6pKxQdLiBjgtzUPoWhsKWDc574Lh7aFGb7ujDBrV4Vo (all accessed on 26 December 2022).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Navarro, E.; Costa, N.; Pereira, A. A Systematic Review of IoT Solutions for Smart Farming. *Sensors* **2020**, *20*, 4231. [CrossRef] [PubMed]
2. Barreto, E.; Amaral, A. Smart Farming: Cyber Security Challenges. In Proceedings of the International Conference on Intelligent Systems (IS), Crete, Greece, 5–7 May 2018; pp. 870–876. [CrossRef]
3. Lamela, M.P.; Rodríguez-Molina, J.; Martínez-Núñez, M.; Garbajosa, J. A Blockchain-Based Decentralized Marketplace for Trustworthy Trade in Developing Countries. *IEEE Access* **2022**, *10*, 79100–79123. [CrossRef]
4. Díaz, V.H.M.; Martínez, J.-F.; Cuerva, A.; Rodríguez-Molina, J.; Rubio, G.; Jara, A. Semantic as an Interoperability Enabler in Internet of Things. In *Internet Things: Converging Technologies for Smart Environments and Integrated Ecosystems*; River Publishers: Gistrup, Denmark, 2013; Chapter Nine; Volume 1, pp. 315–342.
5. Rodríguez-Molina, J.; Corpas, B.; Hirsch, C.; Castillejo, P. SEDIBLOFRA: A Blockchain-Based, Secure Framework for Remote Data Transfer in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 121385–121404. [CrossRef]
6. Zhang, C.; Xiao, L.; Zheng, X.; Rui, L. FengHuoLun: A Federated Learning based Edge Computing Platform for Cyber-Physical Systems. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Austin, TX, USA, 23–27 March 2020; pp. 1–4. [CrossRef]
7. Abro, G.E.M.; Zulkifli, S.A.B.M.; Masood, R.J.; Asirvadam, V.S.; Laouti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones* **2022**, *6*, 284. [CrossRef]
8. Welfare Quality Network Web Site. Available online: http://www.welfarequality.net/en-us/home/ (accessed on 26 October 2022).
9. AENOR (Asociación Española de Normalización y Certificación). Animal Welfare in Livestock and Slaughterhouse Operations. Available online: https://www.en.aenor.com/certificacion/alimentacion/bienestar-explotaciones-ganaderas-mataderos (accessed on 26 October 2022).
10. Xiaohui, L.; Xing, L. Use of Unmanned aerial vehicles for livestock monitoring based on streaming K-means clustering. In Proceedings of the 6th IFAC Conference on Sensing, Control and Automation Technologies for Agriculture AGRICONTROL, Sydney, Australia, 4–6 December 2019; Volume 52, pp. 324–329. [CrossRef]
11. Liu, C.; Jian, Z.; Xie, M.; Cheng, I. A Real-Time Mobile Application for Cattle Tracking using Video Captured from a Drone. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–6. [CrossRef]
12. Jung, S.; Ariyur, K.B. Strategic Cattle Roundup using Multiple Quadrotor UAVs. *Int. J. Aeronaut. Space Sci.* **2017**, *6*, 315–326. [CrossRef]
13. Behjati, M.; Mohd Noh, A.B.; Alobaidy, H.A.H.; Zulkifley, M.A.; Nordin, R.; Abdullah, N.F. LoRa Communications as an Enabler for Internet of Drones towards Large-Scale Livestock Monitoring in Rural Farms. *Sensors* **2021**, *21*, 5044. [CrossRef] [PubMed]
14. Abdelmaboud, A. The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. *Sensors* **2021**, *21*, 5718. [CrossRef] [PubMed]
15. Sun, Y.; Shuhua, Y.; Fujiang, H.; Dongwen, L.; Junqi, H.; Zhaoye, Z. Quantifying the Dynamics of Livestock Distribution by Unmanned Aerial Vehicles (UAVs): A Case Study of Yak Grazing at the Household Scale. *Rangel. Ecol. Manag.* **2020**, *73*, 642–648. [CrossRef]

16. Mulero-Pázmány, M.; Barasona, J.A.; Acebedo, P.; Vicente, J. Unmanned Aircraft Systems complement biologging in spatial ecology studies. *Ecol. Evol.* **2015**, *5*, 4808–4818. [CrossRef] [PubMed]
17. Al-Thani, N.; Albuainain, A.; Alnaimi, F.; Zorba, N. Drones for Sheep Livestock Monitoring. In Proceedings of the IEEE 20th Mediterranean Electrotechnical Conference (MELECON), Palermo, Italy, 16–18 June 2020; pp. 672–676. [CrossRef]
18. Nyamuryekung'e, S.; Cibils, A.; Estell, R.; Gonzalez, A. Use of a UAV-Mounted Video Camera to Assess Feeding Behavior of Raramuri Criollo Cows. In Proceedings of the10th International Rangeland Congress, Saskatoon, SK, Canada, 16–22 July 2016.
19. Alanezi, M.A.; Sadiq, B.O.; Sha'aban, Y.A.; Bouchekara, H.R.E.H. Livestock Management on Grazing Field: A FANET Based Approach. *Appl. Sci.* **2022**, *12*, 6654. [CrossRef]
20. Chamoso, P.; Raveane, W.; Parra, V.; González, A. UAVs Applied to the Counting and Monitoring of Animals. In *Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2014; Volume 291. [CrossRef]
21. Andrew, W.; Greatwood, C.; Burghardt, T. Visual Localisation and Individual Identification of Holstein Friesian Cattle via Deep Learning. In Proceedings of the IEEE International Conference on Computer Vision Workshops (ICCVW), Venice, Italy, 22–29 October 2017; pp. 2850–2859. [CrossRef]
22. Andrew, W.; Greatwood, C.; Burghardt, T. Aerial Animal Biometrics: Individual Friesian Cattle Recovery and Visual Identification via an Autonomous UAV with Onboard Deep Inference. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 3–8 November 2019; pp. 237–243. [CrossRef]
23. Mufford, J.T.; Hill, D.J.; Flood, N.J.; Church, J.S. Use of unmanned aerial vehicles (UAVs) and photogrammetric image analysis to quantify spatial proximity in beef cattle. *J. Unmanned Veh. Syst.* **2019**, *7*, 194–206. [CrossRef]
24. Mamehgol Yousefi, D.B.; Mohd Rafie, A.S.; Al-Haddad, S.A.R.; Azrad, S. A Systematic Literature Review on the Use of Deep Learning in Precision Livestock Detection and Localization Using Unmanned Aerial Vehicles. *IEEE Access* **2022**, *10*, 80071–80091. [CrossRef]
25. Yan, B.; Li, J.; Yang, Z.; Zhang, X.; Hao, X. AIE-YOLO: Auxiliary Information Enhanced YOLO for Small Object Detection. *Sensors* **2022**, *22*, 8221. [CrossRef] [PubMed]
26. Longmore, S.; Collins, R.; Pfeifer, S.; Fox, S.; Mulero-Pázmány, M.; Bezombes, F.; Goodwind, A.; Ovelar, M.; Knapen, J.; Wich, S. Adapting astronomical source detection software to help detect animals in thermal images obtained by unmanned aerial systems. *Int. J. Remote Sens.* **2017**, *38*, 8–10. [CrossRef]
27. Mission Planner Home—Mission Planner Documentation. 2021. Available online: https://ardupilot.org/planner/docs/mission-planner-overview.html (accessed on 14 December 2021).
28. F450 Integrated 4 Axis Quadcopter Frame PCB for Flamewheel F450, Multicopter. 2022. Available online: https://www.multicoptero.com/es/tienda-on-line/drones-dji/dji-f450-f550/ (accessed on 24 February 2022).
29. Navio2: Autopilot HAT for Raspberry Pi. Powered by ArduPilot and ROS. Available online: https://navio2.emlid.com/ (accessed on 27 October 2022).
30. Raspberry PI 3B Datasheet. Available online: https://www.alliedelec.com/m/d/4252b1ecd92888dbb9d8a39b536e7bf2.pdf (accessed on 27 October 2022).
31. GPS: The Global Positioning System. Available online: https://www.gps.gov/ (accessed on 27 October 2022).
32. About GLONASS. Available online: https://www.glonass-iac.ru/en/about_glonass/ (accessed on 27 October 2022).
33. GALILEO | European Global Navigation Satellite System. Available online: https://galileognss.eu/ (accessed on 27 October 2022).
34. Galileo High Accuracy Service (HAS). Available online: https://www.gsc-europa.eu/galileo/services/galileo-high-accuracy-service-has (accessed on 27 October 2022).
35. Galileo Public Regulated Service (PRS). Available online: https://www.euspa.europa.eu/european-space/galileo/services/prs (accessed on 27 October 2022).
36. 25 × 25 mm 1200TVL CMOS 2.1 mm 2.5 mm 2.8 mm 3.6 mm 130/120 Degree FPV Camera 16:9 PAL NTSC 5V-12V for FPV Racing Drones DIY Parts. Available online: https://www.amazon.co.uk/25X25mm-1200TVL-2-1mm-Degree-Camera/dp/B0B5SHLP52 (accessed on 27 October 2022).
37. 2000 mW VTX FX2-Dominator. Available online: https://www.akktek.com/fx2-dominator.html (accessed on 27 October 2022).
38. AKK LR2 5.8G 5DBi RHCP FPV High Gain Four Leaf Clover Antenna for TX/RX SMA Male Antenna. Available online: https://www.amazon.com/-/es/cuatro-tr%C3%A9bol-Tr%C3%A9bol-Antena-Ganancia/dp/B01M35T3Q3?language=en_US (accessed on 27 October 2022).
39. 802.11ac Encryption Upgrade. Available online: https://framebyframewifi.net/2016/08/02/802-11ac-encryption-upgrade/ (accessed on 27 October 2022).
40. EV800D FPV Goggles with DVR 5.8G 40CH 5 Inch 800 × 480 Diversity Video Headset Build in 3.7 V 2000 mAh Battery. Available online: https://www.amazon.com/Goggles-800x480-Diversity-Headset-2000mAh/dp/B08ZXQW67F (accessed on 27 October 2022).
41. FrSky Taranis Q X7 2.4 Ghz 24CH ACCESS. Available online: https://rc-innovations.es/shop/Frsky-Taranis-Q-X7-access-2-4ghz-24ch-negra#attr=7145 (accessed on 27 October 2022).
42. Welcome to OpenTX. Available online: http://www.open-tx.org/ (accessed on 27 October 2022).
43. TBS-Micro Transmitter Crossfire V2. Available online: https://maxterdrone.com/es/modulos-de-radio/703-tbs-crossfire-micro-tx-0741587433040.html (accessed on 27 October 2022).

44. CrossFire Nano Rx. Available online: https://maxterdrone.com/es/receptores/749-tbs-crossfire-nano-rx-se-0741587426158.html (accessed on 27 October 2022).
45. Mission Planner Home. Available online: https://ardupilot.org/planner/ (accessed on 28 October 2022).
46. ArduPilot—Versatile, Trusted, Open. Available online: https://ardupilot.org/ (accessed on 28 October 2022).
47. Introduction—MAVLink Developer Guide. Available online: https://mavlink.io/en/ (accessed on 28 October 2022).
48. What is IPFS? Available online: https://docs.ipfs.tech/concepts/what-is-ipfs/ (accessed on 28 October 2022).
49. Operating System Images. Available online: https://www.raspberrypi.com/software/operating-systems/ (accessed on 28 October 2022).
50. Diccionario Panhispánico del Español Jurídico (Spanish). Available online: https://dpej.rae.es/lema/pedan%C3%ADa (accessed on 28 October 2022).
51. Public Gateway Cache Website for IPFS. Available online: https://natoboram.gitlab.io/public-gateway-cacher/ (accessed on 28 October 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.