GALILEO AND EGNOS AS AN ASSET FOR UTM SAFETY AND SECURITY

Adrián Jiménez
everis aerospace and defence, Av. Fuente de la Mora 1, 28050 Madrid, Spain; P: +34 91749 0000; E: uas.team@everis.com

Juan Andrade
Consejo Superior de Investigaciones Científicas, C/ Llorens i Artigas 4-6 08028, Barcelona, Spain; P: +34 93 401 5751; E: cetto@iri.upc.edu

Ivan Tesfai Ogbu,
RINA Consulting; Via Gran S. Bernardo Palazzo R, 20089 Rozzano, Italy; P. +39 02 52876531; E: ivan.tesfai@rina.org

Ioannis Dontas
Aratos Systems; Wilhelmina van Pruisenweg 104, 2595 AN Den Haag, Netherlands; E: idontas@aratos-systems.com

Carlos Capitán
Universidad de Sevilla; Camino de los Descubrimientos, s/n 41092 Sevilla, Spain; E: ccapitan@us.es

Enric Oliveres
everis aerospace and defence, Av. Fuente de la Mora 1, 28050 Madrid, Spain; P: +34 91749 0000; E: enric.oliveres.marin@everis.com

Huamin Jia
Cranfield University, College Rd, Cranfield, Bedford MK43 0AL, UK; P: +44 1234 750111; E: H.Jia@cranfield.ac.uk

Antonis Kostaridis
Satways Ltd, 3 Christou Lada Street, 15233, Halandri Attikis, Greece; P: +30 2106840036; E: a.kostaridis@satways.net

Abstract

GAUSS (Galileo-EGNOS as an Asset for UTM Safety and Security) is a H2020 project[1] that aims at designing and developing high performance positioning systems for drones within the U-Space framework focusing on UAS (Unmanned Aircraft System) VLL (Very Low Level) operations. The key element within GAUSS is the integration and exploitation of Galileo and EGNOS exceptional features in terms of accuracy, integrity and security, which will be key assets for the safety of current and future drone operations. More concretely, high accuracy, authentication, precise timing (among others) are key GNSS (Global Navigation Satellite System) enablers of future integrated drone operations under UTM (UAS Traffic Management) operations, which in Europe will be deployed under U-Space [1].

The U-Space concept helps control, manage and integrate all UAS in the VLL airspace to ensure the security and efficiency of UAS operations. GAUSS will enable not only safe, timely and efficient operations but also coordination among a higher number of RPAS (Remotely Piloted Aircraft System) in the air with the appropriate levels of security, as it will improve anti-jamming and anti-spoofing capabilities through a multi-frequency and multi-constellation approach and Galileo authentication operations.

1 This project receives funding from the EU H2020 Research & Innovation Programme under grant agreement No 776293

The GAUSS system will be validated with two field trials in two different UTM real scenarios (in-land and sea) with the operation of a minimum of four UTM coordinated UAS from different types (fixed and rotary wing), manoeuvrability and EASA (European Aviation Safety Agency) operational categories. The outcome of the project will consist of Galileo-EGNOS based technological solutions to enhance safety and security levels in both, current UAS and future UTM operations. Increased levels of efficiency, reliability, safety, and security in UAS operations are key enabling features to foster the EU UAS regulation, market development and full acceptance by the society.

1. Introduction

The GAUSS solution will develop and validate the following modules in the unmanned aircraft, GCS (Ground Control Station) and UTM service provider systems (see Figure 1):

- GNSS-INS positioning module based on multi-constellation and fusion with on-board sensors.
- GNSS anti-jamming and anti-spoofing security module.
- UTM Coordination module: Identification, permits and flight plan and emergency management.
- UTM Trajectory manager: Generation, validation and coordination of primary and escape/alternate trajectories.
- UTM communications infrastructure (Security module and surveillance broadcast communications).

The project is currently in development phase. The UTM Concept of Operations has been established, relevant use cases and scenarios have been identified and the system requirements have been defined. The work is currently focused on developing the positioning system, ensuring EGNSS signal integrity and security and developing the UTM technologies that will allow the coordination of multiple drone operations. The consortium is coordinated by everis Aerospace and Defense (ES) and includes Rina consulting (IT), the Spanish National Research Council (ES), Aratos Systems (NL), Cranfield University (UK), University of Seville (ES) and Satways Ltd. (GR).

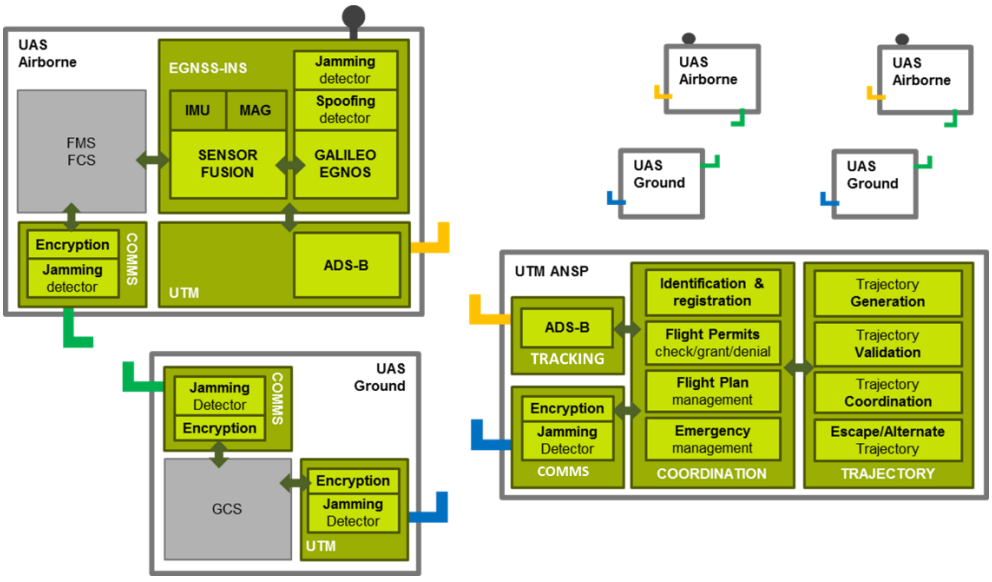

Figure 1: GAUSS system diagram.

The functional architecture is organised so it can create situational awareness for all the actors involved in the distinct stages, as shown in Figure 2. The key capabilities can be expected as follows:

- To define VLL airspace structures for meeting the needs of the U-Space community.
- To configure VLL airspace dynamically according to predicted traffic demand and unforeseen events.

- To accommodate VLL traffic demand, following VLL airspace structures, capacity, operational requirements and procedures.
- To maintain a safe and orderly flow of unmanned traffic depending on the type of unmanned operations and the level of services associated to a given VLL airspace.
- To separate unmanned aircraft from other unmanned and manned aircraft and other hazards such as adverse weather conditions.
- To facilitate the situational awareness to the relevant operational actors in a demand basis, commensurate to the stage of the operation.
- To mitigate the RPA-out-of-control hazards developing into harms for operations - ranging from abnormal to emergency states- by means of taking contingency measures commensurate to the scenario.
- To enable all the above functions by building a technical layer for communications and coordination.

2. Precise Positioning

UTM requires to know precisely the state for every UA in the airspace, i.e. we need to know its position and velocity, both linear and angular. Usually, this kind of vehicles have fast dynamics: fixed-wing UA tend to have fast translation dynamics, while multirotor type can produce aggressive attitude changes. On the one hand, in order to capture these eventual fast dynamics, we need sensors that are able to sample at high rates, e.g. inertial measurement units (IMU), which measures linear acceleration and attitude change rates and can operate at 1 kHz. On the other hand, this kind of sensors cannot observe the full-state we are interested in. The non-observable states are obtained integrating the inertial sensor measurements, which apart from the true state measure it also includes disturbances such as noise or biases. In order to reduce the drift produced by the integration of both the bias and the noise, it is needed to add other sensors to the aircraft so the state becomes fully observable. A good choice when operating robots outdoors is to mount a GNSS receiver, which will give us at least, a global positioning.

Data coming from different sensors will be fused using state estimation techniques. The algorithm used has to be fast enough to process the high rate data streaming produced by the inertial sensors. In the case of the GAUSS project, we use a Graph- SLAM [2] approach. This technique is based on using a graph whose nodes are used to represent poses of the robot at different points in time. The edges between nodes represent movement constraints and are directly linked with the measurements taken by the sensors.

The aim of GAUSS is to test the advantages given by the satellite system Galileo. One of its claims is the positioning accuracy it provides to devices using its satellites. However, the position accuracy computed using GNSS satellites also depends on the techniques used, e.g. there are multiple ways of correcting the biases present in the pseudoranges[2].

Therefore, we will perform a benchmark of different possible ways of computing a position by using GNSS measurements. Eventually, this position will be used in our Graph-SLAM sensor fusion technique in order to assess its validity and accuracy.

Galileo satellite system is the core asset of this project, which means that all the solutions proposed will be constructed around it: Galileo-EGNOS will be tested[3], together with solutions involving Galileo plus others GNSS constellations.

The main idea is to test how Galileo performs using standard positioning techniques presented in [3]. To do so, different positioning scenarios will be tested in order to validate Galileo Satellite System. Thus, both code and carrier measurements will be processed using RTKLIB library.

---

2 It is the pseudo distance between the satellite and the receiver. It contains the prefix pseudo as it is affected by perturbations that modify the true distance, e.g. the ionospheric delay.

3 At the date of this report, Galileo is yet not fully compatible with EGNOSS, even though it will be in the future. Thus, GPS will be used as a substitute of Galileo

The different scenarios first consider the cases of single frequency (L1 band) and double frequency (L1 and L5 bands). For each case, different corrections are applied to the ephemeris, troposphere delay and ionosphere delay. Ephemeris can be defined with Galileo broadcast signal and can also be corrected using both broadcast signal and SBAS (EGNOS in the case of Europe).

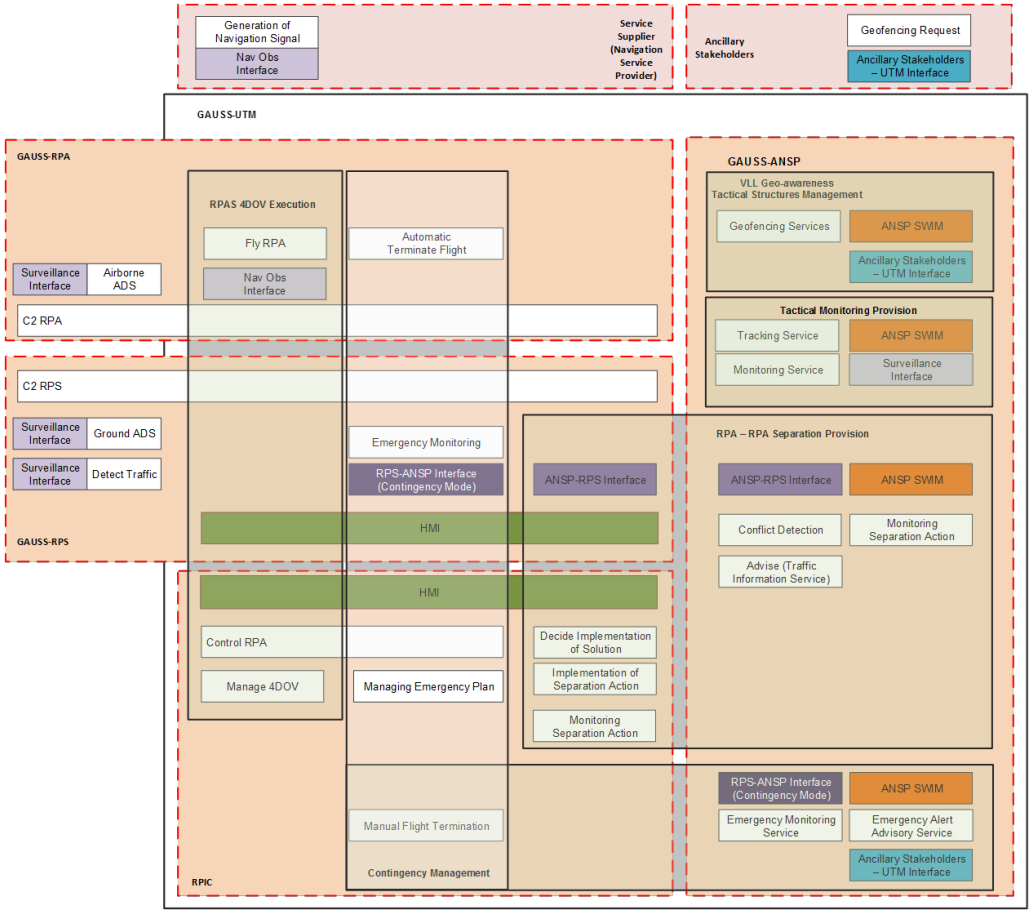

Figure 2: GAUSS Functional Architecture.

Scenario	Frequencies	Ephemeris	Troposphere Correction	Ionosphere Correction
Single frequency, no atmospheric corrections	L1	Broadcast	None	None
Single frequency, broadcast atmospheric corrections	L1	Broadcast	Saastamonien	Broadcast
Single frequency, SBAS corrections	L1	Broadcast + SBAS	SBAS	SBAS
Double frequency, broadcast tropospheric correction	L1+L5	Broadcast	Saastamonien	Ionosphere-free Lineal Combination
Double frequency, SBAS correction	L1+L2	Broadcast + SBAS	SBAS	Ionosphere-free Lineal Combination

Table 1 Table showing the different GNSS positioning scenarios considered in the project.

The simplest method does not consider any correction on the troposphere or ionosphere terms. Then, the broadcast corrections are applied to troposphere (Saastamonien model) and ionosphere delays. SBAS troposphere and ionosphere corrections are also tested. In the case of double frequency, the ionosphere effect will be mitigated using the ionosphere- free linear combination. These scenarios are summarised in Table 1 and their validation and accuracy will be measured using a ground truth receiver correctly positioned.

3. Security module

During flight operations, drones rely on a GNSS system in order to compute its position. This is a great strength, since accuracy of GNSS is sufficient to perform a flight under excellent conditions. However, it could be also a great weakness because the dependency to GNSS is thus considerable. The use of GNSS within this application adds threats to be addressed with a specific threat analysis to cover the weaknesses of the system towards GNSS intentional and unintentional attacks. As reported in [4], the most valuable threat to be considered with the GNSS navigation system is Electromagnetic Interference (EMI). As reported in [5] and [6], EMI can be divided into two main categories: spoofing and jamming.

3.1 Jamming

Jamming is the intentionally disruption of wireless signals through the use of an over-powered signal in the same frequency [7]. GNSS jammers transmit a signal of interference where the carrier is located in the frequency band used for satellite navigation [3]. Jamming occurs in three main forms: broad-band noise, narrow band signal and pulsed signals. Among these, the jammer case can be either sinusoidal or chirped, the latter being the most dangerous one since not easily blanked via receiver filtering (indeed most commercial GNSS receivers already implement the ability to put narrow frequency notch within the receiving chain [8]).

3.2 Spoofing

Compared to the previous technique, spoofing is more complicated to be achieved. Spoofing attack is a transmission of manipulated or simulated GNSS signals. In this kind of attack, the offender can provide false PVT information to the GNSS receiver and deviate the RPA from the flight route. This is true in this context since the signals broadcasted by the offender are powerful enough to dominate the ones of the real GNSS constellation. In a simple spoofing scenario where a trajectory is generated which deviates considerably from the real trajectory, spoofing can usually be detected. In a more sophisticated scenario the spoofed position/ velocity / time solution can to a great extent have the same properties as other independent systems. Spoofing is then difficult to detect [4].

3.3 GNSS Jamming and Spoofing Security Controls

In addition to the already implemented mechanisms in Galileo system (e.g. Navigation Message Authentication, Code Based Authentication, etc.), given the above possible classes of attack on the GNSS signal we identified in literature several types of counter- measures with different level of effectiveness:

- Signal Processing-based techniques: values or trends in parameters like amplitudes, carrier and code phases are stored in order to generate an historical database and looking for GNSS signal anomalies. Another option is to look for distortions in the autocorrelation functions;
- Encryption-based techniques: for these group of mitigation approaches, encryption of spreading codes are employed in order to ensure the authenticity of the signals. Among others, symmetric key encryption, delayed symmetric key (interleaves short segments of a symmetric-keyed Spread Spectrum Security Code, SSSC, with long segment of predictable spreading codes) and asymmetric private/public key (this method is known as Navigation Message Authentication, NMA) can be used. Note that for each of these methods, modification of the satellite signals is required since addition of an encryption layer is needed;

- Drift-based technique: an attack is spotted by analysing the rate of clock drift: if it is larger than the usual drift of the oscillator probably an attack is ongoing. This technique checks changes in clock fix. If external IMU (Inertial Measurement Unit) are available, kinematic constraint can also be exploited calculating estimation of speed, heading and position. For this reason, changes in the receiver position and track are also checked;
- Signal geometry-based technique: GNSS signals are supposed to be sent from a wide set of different angles while spoofed ones can come only from a single point. A multiple receiving GNSS antenna system could calculate the direction of arrival of the navigational signals and discerns spoofing signal. Another way to spot spoofing signal by taking advantage from this technique in a single antenna system on a moving platform is looking for phase shifting consistent with the platform motion.

In order to strengthen security needs in GAUSS applications and to improve robustness and reliability of detection, a suitable solution consists in the implementation of a set of detectors jointly working on the received GNSS signal and looking for signal anomalies. Each detector works on different aspect of the signal and therefore being able to detect different types of attacks. The selected detectors are optimal in the way their joint use provides high probability of detection in the most common operational scenarios where the GNSS signal integrity could be at risk.

4. UTM

In this section, we present details about the different modules of the GAUSS-UTM and the communications infrastructure involved in it (see the GAUSS system diagram in Figure 2). UTM is envisioned as a subset of ATM that is aimed at the safe and efficient management of UAS operations through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions. Such a system would provide UTM through the collaborative integration of humans, information, technology, facilities and services supported by air, ground and/or space-based communications, navigation and surveillance [9] .

4.1 Communications

To accomplish the management of UAS traffic in a UTM environment, communications within GAUSS need to be robust, reliable and have high availability. While not requiring the level of performance expected for operations in controlled airspace using aviation safety spectrum, communications for UTM must nevertheless perform reliably to provide a sufficient level of system safety. To this end, the communications between all systems interacting in the UTM of GAUSS will be developed by using encryption algorithms to ensure integrity and availability. Currently, research analysis of the existing algorithms and their convenience for the UTM has been conducted and the selection of AES 256 algorithm was deemed necessary considering the parameters after a study on the capacity and performance requirements of usual RPAS operations. Thus all considered communication flows will be encrypted using the AES (Advanced Encryption Standard) algorithm [10]. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Based on the communications policy, the technical performance requirements, communications procedures and architectures the communications can be classified in two categories: low data rate communication, such as command signal sending and receiving with relatively small size packets and high data rate communication for payload download and streaming of data.

The solution to be developed will include a hardware approach which is much faster, reliable and well suited to both kind of high bandwidth real time encryption needs and low data rates. The AES 256 algorithm will be integrated into an FPGA-based system which stands for a straightforward process because the data manipulation and transformation performed by the AES algorithm can be easily incorporated into the chips blocks [11]. Crucial parameters such as length of the message, headers as well the communication rates (RPAS to GCS and GCS to UTM) will be adjusted within the AES body with the aim to increase the performance and reliability in the communication. For the encryption/decryption processes in the UTM station a software based approach will be developed.

The designed architecture for the AES to be implemented will consist of three modules: the Communications module, the Encryption module and the Decryption module. All three will be implemented on both the FPGA-based system as well as the processors in the ground stations and UTM stations, and will work without interfering with the currently implemented main system and its functions. By applying such an approach arises the benefit of having an efficient and secure end-to-end communications protocol that can be used for multiple applications regardless of the functions that are performed by the system. Extended research has already been conducted towards the authentication and security through efficient key negotiation. One key aspect within AES proposed solution is the key generation and sharing between systems. The owner of the key will be the UTM ANSP. Each time a RPAS registers with a specific UTM to request permission to operate within certain airspace, and in the case that the UTM ANSP grants this permission, a key is generated and shared through a secure SSL-based virtual private network (VPN) with the RPAS-GCS. This key will be shared between GCS and the RPAS FCS (Flight Control System) by means of a tethered communications, reducing the risk of interception.

4.2 UTM coordination

The GAUSS-UTM coordination is based mainly on the services described in Figure 2. These are e-Registration, e-Identification, Flight Planning management, Monitoring and Emergency Management. Another important UTM service for GAUSS-UTM coordination is the Monitoring service. In the following we are going to define briefly these services.

- *E-Registration* process is a pre-flight requirement; it is mandatory before submitting a flight plan. There are commercial UTM applications which include this functionality. In this sense, we will integrate the GAUSS-UTM with one of them. Otherwise we will consider that the e-Registration process has been fulfilled and the required data will be generated in a database.
- *e-Identification* service allows the localization and identification of a UAS while flying. This identification allows gathering all the information from a registry. The localization of the UAS is sent to the Tracking service as a position report. The e-identificacion service will be implemented in GAUSS using ADS-B and RPA state combination of messages.
- *Flight Planning Management* service receives a flight plan from the operator and provides an approval or rejection answer, depending on the mission, scheduled flights, geofences and regulations. Since it is a pre-flight process it does not fall within GAUSS scope of work. We can manually define flight plans that fulfil the requirements; this flight plans could be stored in the scheduled flights database. This feature is included in most of existing commercial UTM applications, so it might be integrated within GAUSS if the proper API (Application Programming Interface) or SDK (Software Development Kit) is available.
- *Monitoring* service will estimate and calculate potential problems that could appear during a flight. This service will run an independent instance for each flight. We will consider the following events:
    - ✓ Geo-fences: approaching, crossed.
    - ✓ Geo-cage violation.
    - ✓ Potential collision with other RPA: close track, likely collision.
    - ✓ Deviation from plan: time, separation.

  It could also include weather related event, but we consider that this is out of scope in GAUSS. Moreover, this service could be triggered when a mismatch between the flight plan and the actual RPA track occurs. We assume that the Monitoring service is always running for each flight and the information is only forwarded when one of the mentioned events is detected.

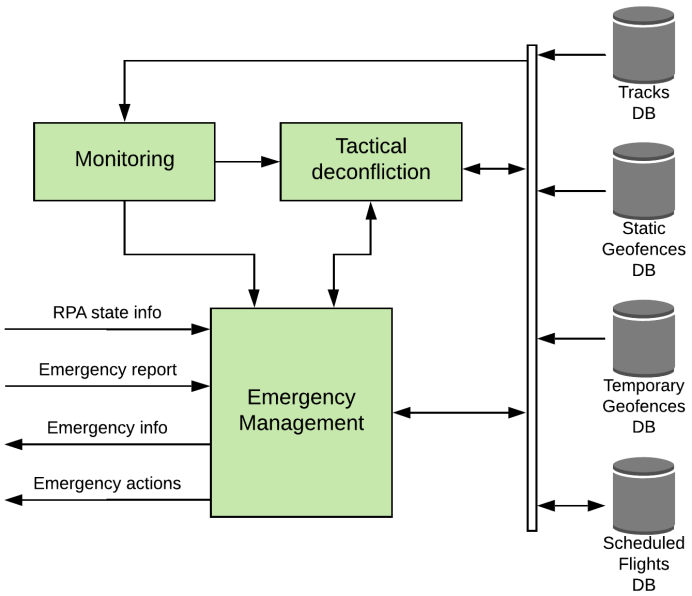

Figure 3: Emergency Management, Monitoring and Tactical Deconfliction U-Space services.

- *Emergency Management* functionality will include three different features (see Figure 3):
  - ✓ Send to *Remote Pilot in Command* (RPIC) emergency information or actions. Emergency information means reporting events that could affect the flight (for example, fly away RPA in close proximity or approaching to jammed GNSS signal area). Emergency actions include manoeuvres to avoid or reduce the effect of these events.
  - ✓ Receive from RPIC emergency reports. Depending on the event, these reports could trigger sending emergency information to other RPAs. Therefore, this service will receive emergency report from flying RPAs and it will also detect emergencies that could arise from an unexpected RPA behaviour (for example, diverting from flight plan). Then decision-making techniques will provide proper actions or trajectories to mitigate the effects of the hazards.
  - ✓ Detection of jamming or spoofing of the GNSS signal together with jamming of C2 link or UTM communications are considered emergency events. This service will receive from each RPA the status information of the communications links (C2 and UTM) and GNSS signal and it will use this information to build a jamming/spoofing map. This map will be part of the decision-making process to submit emergency actions to RPIC

4.3 UTM trajectory management

Management of RPA trajectories in GAUSS is achieved using two different U-space services: Strategic deconfliction and Tactical deconfliction.

- *Strategic deconfliction*. This service (see Figure 4) provides deconfliction assistance to a drone operator before the flight. If a submitted flight plan is not feasible, this service will propose a new flight plan to the operator. Then the operator can accept this new plan or submit a new one. This service is not mandatory in GAUSS, since it is a pre-flight process, but the algorithms implemented for Tactical deconfliction will be used offline for this purpose. As far as we know, none of the existing UTM applications have available this feature at this moment. As shown in Figure 4, this service takes as inputs the geofences (static and temporary), the drone operator database and the scheduled (approved) flight plans. The output is an update of the scheduled flight plans.
- *Tactical deconfliction*. As described in [12], this service provides real-time deconfliction assistance while flying. The service interacts with the Monitoring and the Emergency Management services, as shown in Figure 5, and it is triggered whenever a modification

of the scheduled flight plan is needed due to unexpected events that could compromise the separation from other aircrafts, the violation of a geofence or due to an emergency situation. In GAUSS, the RPA will not receive directly the deconfliction information; this information will be received by the RPIC and he will take the responsibility for rejecting or executing the proposed actions. If the execution is validated by the RPIC, then the proposed actions are forwarded to the RPA.

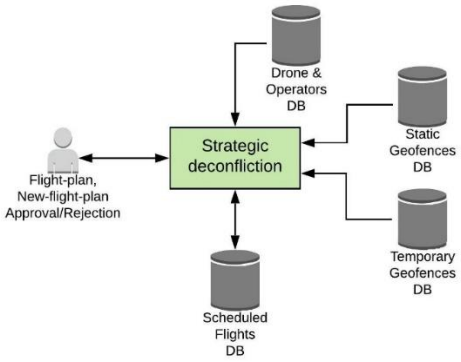

Figure 4: Strategic deconfliction U-Space service

4.4 UTM Web Application

Finally, an interface is needed to visualize flights, statistics, trajectories and geospatial objects (geofences, geocages), emergency information etc. In GAUSS this will be a modular Web application (for desktop and mobile devices) built on React.js and REST Web services and a PostgreSQL/PostGIS backend database. It is a high performance map-cantered application that is also able to communicate in a two way fashion with other commercial UTM solutions via well-defined APIs. Both civil aviation ADS-B and UAS traffic is consumed and displayed in order to assist pilots that choose to embed the web application into their GCS or display it through their smartphone.

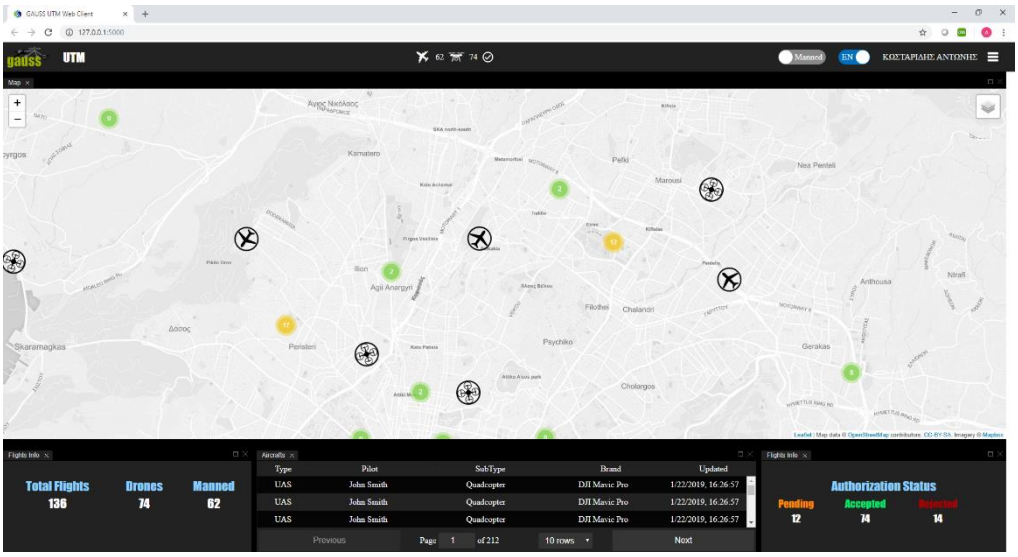

Figure 5: View of the GAUSS UTM Web app

5. Conclusions

The use of RPAS is growing rapidly worldwide and there are several initiatives (public and private funded) working towards ensuring a safe and efficient operation; one of the main concerns in all drone operations is the importance of the positioning information in terms of performance, safety and security. GAUSS addresses this by developing a system able to provide accurate, reliable and secure positioning information. A combination of internal sensors together with multi-

constellation and multi-frequency satellite systems (with Galileo as the core asset) through GraphSLAM algorithms offers a comprehensive solution, able to offer accurate information, where several corrections can be applied (ephemeris, troposphere, ionosphere, etc.). This adjusted signal provides higher robustness against jamming and spoofing. Furthermore, additional techniques can be applied to increase the security levels: signal processing-based, encryption-based, drift-based and signal geometry-based. Data flow through UTM systems may also be vulnerable, this is why such communication should be encrypted; the encryption procedure usually depends on particular system needs (bandwidth, data rates, etc.) and in GAUSS the AES 256 algorithm together with a hardware approach is found to be the fastest and most reliable option. Finally, the safety of drone operations is also highly dependent on the UTM services which should be able to provide coordination and trajectory management of several flights simultaneously. These services were drafted by SESAR (Single European Sky ATM Research) [1] and are in the process of being updated by the CORUS project.

6. References

[1] SESAR Joint Undertaking, “U-space Blueprint,” Bietlot, 2017.

[2] G. Grisetti, R. Kummerle, C. Stachniss, and W. Burgard, "A tutorial on graph-based SLAM," vol. 2, no. 4, pp. 31-43.

[3] J. Sanz Subirana, J.M. Juan Zornoza and M. Hernndez-Pajares, *GNSS Data Processing, Vol.1: Fundamentals and Algorithms.* ESTEC, PO Box 299, 2200 AG Noordwijk, The Netherlands: ESA Communications, 2013.

[4] S. Storm van Leeuwen, "Electromagnetic interference on low cost GPS receivers", National Aerospace Laboratory NLR, NLR-CR-2008-671, 2008.

[5] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," GPS Solutions, vol. 19, pp. 475-487, 2015.

[6] J.T. Curran, M. bavaro, P. Closas, M. Navarro "On the threat of systematic jamming of GNSS," ION GNSS+ Conference, 2016.

[7] A. Graham, *Communications, Radar and Electronic Warfare*, Wiley, 2011

[8] A. Thiel and M. Ammann "Anti-jamming techniques in u-blox GPS receivers," uBlox white paper, GPS-X-090008, 2009.

[9] International Civil Aviation Organization, "Unmanned Aircraft Systems Traffic Management (UTM), A Common Framework with Core Principles for Global Harmonization" 2017.

[10] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Sahamir, "Key recovery attacks of practical complexity on aes-256 variants with up to 10 rounds," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, 2010.

[11] D. S. a. B. SwapnaKumari, "Implementation of aes-256 encryption algorithm on FPGA.," *International Journal of Emerging Engineering Research Technology, Vol. 3, N 4.* p. 104-108, 2015.

[12] SESAR Joint Undertaking (SJU), “European ATM Master Plan: Roadmap for the safe integration of drones into all classes of airspace,” 2018.