Embedded Selforganizing Systems (Vol 5. No 1. 2018) (pp. 17-25)

Embedded Selforganizing Systems

Issue Topic: "Unmanned Aerial Systems and Its Application"

Timing and Navigation in UAVs: Synchronization of UAV Swarms and Testing GPS Error Effects on GNSS Reception

Karen von Hünerbein
Lange-Electronic GmbH
E-mail: KvH@lange-electronic.com

Werner Lange
Lange-Electronic GmbH
E-mail: WL@lange-electronic.com

Abstract[1] — Precise timing and precise location information are provided by Global Navigation Satellite Systems (GNSS) and play a crucial role in the positioning, navigation and data acquisition of most Unmanned Aerial Vehicles (UAV) and in various flight operations and tasks, e.g. time-stamping and geo-referencing of data and images, return home, avoidance of obstacles and geo-fencing. Some of these critical operations have implications for the safety of the UAV, the surrounding environment and health and safety of people.

Thus, it is important to ensure correct function of the navigation and the timing, under a wide variety of circumstances and in the presence of GNSS threats and GNSS signal denials. The performance of timing and navigation based on GPS/GNSS can be tested and verified in a controlled and repeatable way in the laboratory with different types of test equipment. We will introduce a wide range of potential threats to GNSS Positioning, navigation and timing and an overview of different test methods. In addition, we are presenting a method for time synchronization of drones to enable safe swarm and follow flights in UAVs.

Keywords—GNSS simulation, interference monitoring, GNSS error effects, synchronization, precise timing

I. INTRODUCTION

One of the major sources for precise timing and precise location information are the signals of Global Navigation Satellite Systems (GNSS). They also play a crucial role in the positioning, navigation and data acquisition of most Unmanned Aerial Vehicles (UAV), with many different applications in UAVs: time-stamping and geo-referencing of collected data and images, synchronization of swarm flying and follow-me flights, determination of position and attitude in-flight, flight trajectory by following a pre-defined number of waypoints, mission planning, return home automatically without external control, avoidance of obstacles and geo-fencing [1,13].

Some of these critical operations have implications for the safety of the UAV, the surrounding environment and health and safety of people, for example UAVs threatening to bring down aircrafts at airports, which are no-fly zones for UAVs. The appropriate GNSS based function to avoid this is geo-fencing. Another example is obstacle avoidance to prevent collisions and damages for both the UAV and the obstacle, e.g. anything from a windowpane, tree, human being, to a power line.

In order to ensure health and safety it is thus important to guarantee correct function of navigation and the timing, under a wide variety of circumstances, and in different signal environments. There can be signal disturbances, such as obscurations by buildings or reflected GNSS signals, called multipath. The performance of the timing and the navigation based on GPS/GNSS can be tested and verified in a controlled and repeatable way in the laboratory with different types of test equipment. We will give an introduction to and summary of a wide range of potential threats to GNSS positioning, navigation and timing, as described previously by ourselves and other authors, and test-setups for testing them in UAVs. The test set-ups serve to illustrate state of the art GNSS test methods for UAVs. In addition, we, as timing experts, are proposing a method for time synchronization of UAVs to enable safe swarm and follow flights in UAVs.

GNSS Vulnerabilities

GPS/GNSS signals are vulnerable, because they "arrive at the surface of the Earth with a very low signal power of -120 to -130 dBm, so low that it is usually buried inside the thermal noise. The GPS/GNSS signals are thus easy to interfere with by

other signals in the same band of moderate strengths, and vulnerable to different types of effects, including atmospheric disturbances, multipath and malicious spoofing. Other signals in the same band can be unintentional interference, jammers and spoofers." [2a]

Interfering radio signals in the L-band can be emitted and generated unintentionally, e.g. by defect devices or intermodulation effects of several RF transmitters, or different transmitter antennas installed on top of roofs of large sea vessels for a variety purposes, e.g. for mobile satellite communication and RADAR.

Intentional interference is caused by jammers, which are devices designed with the purpose to disrupt GNSS signals. They produce stronger RF signals in the same RF band, and simply overwhelm the GPS receiver by sheer noise [3]. When a receiver is disrupted by a jammer, it is clear to the receiver and to the user that there is a signal problem. Jamming is not a highly selective process and can affect numerous unintended targets [11]. Several test campaigns in Europe in the last 2 years suggest that the amount of jamming events has increased in recent years, e.g. by the widespread use of "privacy devices" generating intentional interference to GPS signals to prevent vehicle tracking, with a high density on highways [5,8].

Spoofing on the other hand is a hidden attack misleading the receiver with erroneous information, to make it believe it has different position, velocity or time than it actually has. In this case, it is not clear to the receiver and the user, that there is a signal problem. Spoofing has been observed rarely so far, once f.i. at the Mexican US border for drug smuggling, but demonstrated to work in experimental field tests. [7]

Multipath consists of reflections of the GNSS signals from metal or glass planes or smooth water surfaces, for instance reflections of GNSS signals on large sea vessels from the metal parts on board or from freight train iron parts on marshalling yards. In the case of multipath, the reflections are usually weaker and delayed with respect to the direct Line of Sight (LOS) signal.

Atmospheric disturbances are caused by ions and particles in the ionosphere and troposphere and can delay, refract, attenuate and phase shift the GNSS RF signals, which will either affect the accuracy of the positioning and timing and/or the acquisition and tracking of the signals.

All these effects can impair or deny GNSS based positioning, navigation and timing. Jamming and strong atmospheric disturbances cause lower carrier to noise ratio of tracked satellites and eventually loss of tracked satellites [5]. Multipath can lead to a decrease in accuracy of the position fix, as the receiver sometimes uses the reflected signals for the calculation instead of the line of sight ones. And the effect of spoofing are wrong position, navigation and timing results: a position or time deviating from the true one."

"Jamming can be detected due to the strong power of the signals. Spoofing can be detected, because the spoofing signals differ from the real ones by" [2]

- greater variation of signal strength, especially if the distance between the spoofer transmitter and the GNSS receiver changes a lot in the course of time as would be expected in a drone moving along its trajectory and a spoofer on a ground-based transmitter
- spoofing signals result in more overall transmitted GNSS RF power
- spoofing signals arrive from different angles than the RF signals of the GNSS satellites and all spoofed signals are arriving from only one direction, if sent by only one transmit antenna near the ground, in any case it would be close to impossible to mimic all the different angles of GNSS satellites signals even with airborne spoofing vehicles.
- All satellites are received twice – double signals
- Difference between L1 and L2
- Spoofed GNSS signals yield conflicting information with other on board sensors (if present)

Thus spoofing and jamming signals can be detected with different detection algorithms [4], integrated into a receiver, or with special antenna arrays [12], capable of detecting the angle of arrivals of signals [13, 24], or with additional sensors integrated in the sensor hardware portfolio of the UAV. For other methods to mitigate jamming see [2, 4, 5].

In case of multipath, there are several signals for the same satellite, but in contrast to a spoofer, they arrive from various directions, they are weaker in signal power than the LOS signals and they contain exactly the same information in the navigation message as the other signals. During an in depth analysis with a Software Defined Receiver they can be distinguished.

In addition, GNSS system errors have been observed several times in recent years. This means that the GPS or GLONASS satellites broadcasted erroneous information, such as a wrong UTC timing offset or a completely incorrect Almanac. In January 2016, there was a GPS anomaly during decommissioning of a GPS satellite, when several satellites transmitted an incorrect UTC timing offset, of -13.7 µsec [8], causing GPS timing receivers to output wrong timing information with the effect that a TV network in Europe stopped operation for several hours. [9].

Another accident happened on 2nd April 2014: there was an incorrect upload of ephemerides to all GLONASS Satellites, equivalent to a complete loss of the GLONASS system for more than 10 hours. Only two weeks later, eight GLONASS satellites were malfunctioning for 30 min [10].

II. IMPORTANCE OF TESTING

In order to maintain correct navigation and timing, it is important that the receiver algorithm has functions to detect and cope with such events. These functions need to be tested to guarantee continued operation, even in case of external error sources. When improving software algorithms or installing other countermeasures, systems need to be retested to verify and quantify and the improvement.

The easiest way is a live sky test with live GNSS signals outside buildings. Field-tests of UAVs and their GNSS navigation and flight control units are a good start for testing, but also time-consuming and expensive. In addition, all GNSS

signals vary a lot with time, as the GNSS satellites are moving fast in their orbits. They also vary with weather, 3 D Terrain and different disruptive factors, as described above. Thus, the tests under live-sky conditions can only convey part of the picture and do not allow for controlled and repeatable testing.

Moreover, live sky tests are not possible in many special situations, e.g. in the case of geo-fencing. If a drone must not fly in the area of an airport, the test of the geo-fencing function cannot be carried out on-site, e.g. Frankfurt airport. One possibility for testing it is to artificially generate the respective signal environment consistent with the desired location and run the test elsewhere, preferably in a laboratory.

More systematic testing can be performed in the laboratory repeatability and under controlled conditions, at different locations around the Earth, with different signals types and error effects and satellite constellations. In addition, a lot more tests can be run in the laboratory, than in the field. More tests improve the results and give a chance to fully assess the strengths and weaknesses of the GNSS navigation and flight control unit [15].

Testing in the lab can save a lot of time and will improve the overall reliability and functionality of the GNSS based navigation unit and answer questions like: Where is the best place for the antenna on the airframe? Can the vehicle still calculate its own position accurately, if flying at high latitudes, e.g. in Scandinavia, where there are fewer or no satellites overhead, "Can the UAV quickly regain its intended position if blown off course by the wind? Can the UAV recognize and compensate for multipath signals, reflected off water surfaces and tall buildings?" Does the UAV comply with public and legal regulations like altitude restrictions and no-fly zones? [14]

III. Test Methods

Many different test systems are available, e.g. interference detection and monitoring systems, GNSS RF signal generators, interference signal generators, and Record & Replay Systems for GNSS signals.

Interference detection and monitoring systems [16], allow non-stop monitoring 24 h and 7 days a week of GNSS and interference signals on different L-bands and automatic detection and classification of interference. The severity of the interference events is analysed. The severity is the degree of degradation inflicted on GNSS reception and position accuracy. Moreover, snapshots of the jamming signals are stored and can be converted to test cases, which are later replayed in the laboratory, for systematic testing, by an interference simulator.

A GNSS simulator generates realistic GPS/GNSS radio frequency signals (RF) designed to be as representative as possible of the signals that would actually be incident at the antenna of a GNSS receiver in the real world at any given time and date, with many different vehicle trajectories, obscuration environments, landscapes and buildings and different error effects, e.g. satellite orbit errors, strong attenuation of RF signals, or atmospheric effects [17].

Using an interference simulator allows to generate Radio Frequency Interference events with different waveforms, frequencies, duration and signal strengths. Both the GNSS signal environment and the interference can be combined and applied simultaneously to the Device under Test in order to check its ability to cope with the interference.

A record and replay system samples the GNSS signal environment at L-Band and stores the down sampled, digitized GNSS signal internally at intermediate frequency (IF). Later the stored GNSS signals can be up converted again and be replayed in the laboratory with minimum loss. The advantage is that the complete and realistic GNSS signal environment is stored during a UAV test flight, including all multipath, interference and other error effects. Recordings can be replayed as many times as needed and thus provide full repeatability.

IV. Interference Detector

One example of an Interference detector is the Spirent GSS200D [16]: The DETECTOR constantly monitors the live GPS and Galileo RF signal environment at L1 at +/- 8 MHz around Centre Frequency (CF) and the GLONASS L1 RF signal environment at L1 at +/- 4.5 MHz, in a signal power range of -95 dBm to -25 dBm. An alternative model includes the GPS/Galileo L5 band at +/- 10 MHz, in a signal power range of -126.5 to – 38 dB. "It detects jamming events, classifies the impact of a jamming event, characterizes the waveform and type of interference, notifies the user via E-Mail about serious events and stores snapshots of spectrum and spectrogram. The DETECTOR is a detector and an analyser, analysing the jamming signals frequency properties, signal strengths and potential impact on a GPS receiver. In addition, the snapshots can be converted into test cases for a GNSS and interference simulator system, enabling repeated and controlled testing of real jamming events in the laboratory." [2, 5, 16]

The access to the jamming event data is enabled via a web based service: all events are sent to a central webserver via internet, allowing the user to access an overview over all events listed in a table on a web portal. This can be either the Spirent web portal PT Cloud or a user specific private network. The web portal table allows viewing of the spectrum and spectrogram snapshots. The online table grants an easy access to the data and a fast impression about the amount and severity of jamming events at the test location of the active DETECTOR or even at several test locations, without a need for the user to manually sort and look through a huge amount of recorded data and without extensive computations. In addition to the online table there are analysis and visualization tools enabling monitoring over time and in-depth trend analysis [2, 16].

Data contain start time, date, ID (identification number), and duration of the event, signal type e.g. single tone or CDMA (Code Division Multiple Access), signal strength, and severity of the event.

"The detection function is accomplished using a fusion of complementary pre- and post-correlation techniques. The detection fusion algorithm is patented. Pre-correlation

algorithms make use of the digital signals at baseband or intermediate frequency (IF) which are available in the software receiver in the GSS200D. The post-correlation algorithms use measurements, which are typically available as outputs from a standard GNSS receiver, such as signal to noise rations (SNR), numbers of satellites tracked, automatic gain control (AGC) parameters and satellite geometry information." [2]

After the first level signal classification at the GSS200D Detector Probe hardware, the captured interference event is then transferred to the server for further characterization.

The classification approach used assigns a threat level severity metric to the event. [16].

This system allows to:

- Monitor multi-frequency, on GPS and GALILEO L1 and L5 (E5a), including all major Satellite Based Augmentation Systems SBAS (WAAS, EGNOS, MSAS, GAGAN, SDCM) [23]
- Gather Quantified information on frequency, type and severity of RF interference threats
- Automatic RFI event detections and alerts based on levels defined by the:
  - United Nations International Civil Aviation Organization (ICAO) Annex 10 for GPS L1
  - The European Organisation for Civil Aviation Equipment (EUROCAE) Galileo MOPS for GPS L5 (or GALILEO E5a) [23]
- Enables correlation between observed performance issues and the threats that caused them
- Confirm that a particular installation is contaminated/ uncontaminated by RF interference, raising an alert if there is a detected event.
- Use collected data to derive a list of accurate resilience requirements
- Differentiate non-intentional interference from jamming
- Distinguish different jammers or identify multiple detections of the same jammers
- Support the development of effective counter-measures
- Identify DME and TACAN signals
- The ability to replay and resynthesize RFI: Used in conjunction with the interference generator GSS7725 and the automatization software PT Test Bench, the detector can help with testing GNSS receiver, system or application performance. This enables informed decision making on mitigation and hardening strategies to improve robustness and integrity. " [16]

V. GNSS SIMULATORS

Simulation has been a standard test method for testing GNSS (Global Navigation Satellite Systems) receivers for a long time. This test method is based on the artificial generation of realistic RF (radio frequency) signals on different signal channels as representative as possible of the signals that would normally arrive at the antenna of a GNSS receiver in the real world at any given time and date [17]. These signals are emulated with the correct frequency, modulation, Pseudo Random Noise (PRN) codes, navigation message and Doppler Effect. At the same time, they model vehicle and satellite motion, atmospheric and other effects, causing the receiver to actually navigate according to the parameters of the test scenario [17, 18, 19].

One of the major advantages of a simulator is that the user can freely chose location, time and date of the simulation, so that scenarios from all over the world can be tested without moving the receiver out of the lab. A signal generator offers full control over satellite signals, amount of satellites present, the health status of each satellite, error effects at the signal level and in the atmosphere [17, 18, 19]. Satellite signals can be switched on and off, and attenuated or amplified. Satellite clock and orbit errors can be introduced. Orbital deviations by application of an offset to the pseudorange, are especially suitable for Receiver Autonomous Integrity Monitoring (RAIM) testing.

Simulators can also provide correction data for GPS/GNSS pseudoranges, when higher accuracy than 2-15 m is required for positioning and geo-referencing in the cm range. A higher accuracy is necessary for survey grade-applications such as photogrammetry, dropping biological pest control (eggs of predators) or spraying fertilizers on agricultural fields. One such technique is Real Time Kinematic, where a mobile reference station transmits correction data to a rover receiver over the air. It is based on carrier-based ranging and provides ranges and positions that are much more precise than those available through code-based positioning [20]. Correction data are also provided by national CORS Networks (Continuously Operating Reference Station), with fixed stationary reference stations, which continuously monitor all GNSS satellites and gather integrity information and pseudorange corrections for their specific location. These data can lead to a significant improvement of the accuracy and integrity of the position fixes up to 200 km from the reference station. "Rovers determine their position using algorithms that incorporate ambiguity resolution and differential correction. Like DGNSS (Differential GNSS), the position accuracy achievable by the rover depends on, among other things, its distance from the base station (referred to as the "baseline") and the accuracy of the differential corrections. Corrections are as accurate as the known location of the base station and the quality of the base station's satellite observations. Site selection is important for minimizing environmental effects such as interference and multipath, as is the quality of the base station and rover receivers and antennas." [Citation from Novatel, 20]. RTK is a method for real-time correction. There are also methods for post-processing data to achieve the high accuracy, if it is not needed in the field, such as Post processed Kinematic, allowing for more convenient calculation in the lab.

Another source of correction data are broadcasts from special geostationary satellites. These systems are called Satellite Based Augmentation Systems (SBAS), some provide data in the public domain free of charge [e.g. EGNOS the European Geostationary Overlay Service] [24], others are commercial systems, e.g. Starfire [25].

High quality simulators are capable of generating several different types of correction data as provided by publically available SBAS, CORS and RTK stations in the correct format consistent with the GNSS signal environment and simulated location of the device under test. Here we show different possibilities of test-setups for a drone navigation unit with a simulator, depending on the accuracy level required.

For testing normal accuracy levels of 2-15 m, the uncorrected GPS/GNSS RF signals from the simulator are sufficient as shown in the left side of figure 1. This test only requires one set of signals via one RF output. Initially the GNSS RF signals from a high quality simulator are "too good" to be true. They are very pure and accurate and do not reflect the live sky conditions. Thus, the Device Under Test will usually show better results with a simulator than outside in the real world. In order to be more realistic, atmospheric delays, disturbances, and antenna patterns need to be introduced, and further environmental effects.

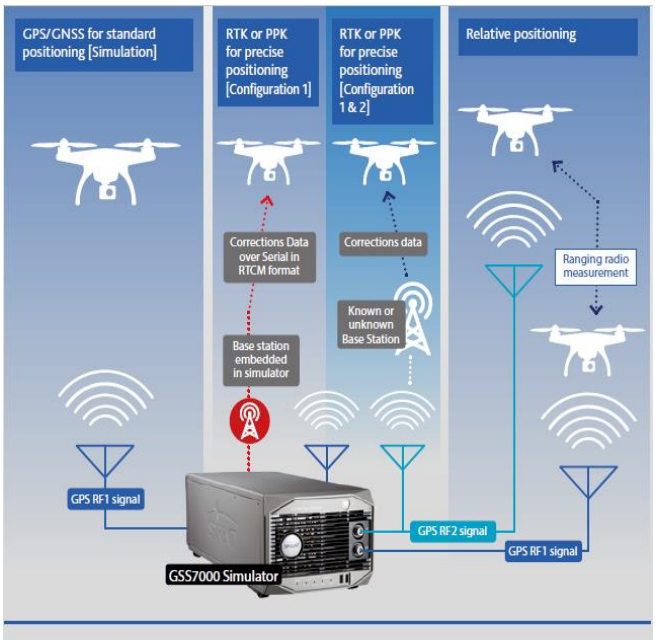

Figure 1: Test Setups with a GNSS simulator [1]

In PPK, the correction data are not immediately applied to the position, navigation and timing fix, but later after the return of the UAV. With this method, it is sufficient to log the RTCM correction data during the simulation and apply them later to the acquired pseudo-ranges and positions.

A second possibility to output the correction data of the reference station is by antenna over the air via second RF Output to be retransmitted. In this case, amplification of the RF signals is required, because the RF signals are strongly attenuated by the air near the antenna.

For a simulation with two UAV`s, which need to be aware of their relative position to each other, a GNSS signals simulator can output the correct signal environment via two RF outputs. The signal environment is slightly different for each of the UAVs, and thus needs to be generated separately and specifically for each of the two flying aerial vehicles, according their specific location, trajectory and vehicle dynamics.

With a GNSS signal simulator there is also the possibility for a HIL, Hardware in the loop, simulation (figure 2). A UAV trajectory simulator can calculate and modify the trajectory in real-time during the simulation run, feed the new positions to the simulator, which converts it into corresponding, coherent GNSS signals and transmits them to the Navigation Unit of the UAV, which in turn feeds back its calculated position to the UAV trajectory simulator. The UAV simulator is very similar to standard flight simulators.

VI. Interference Generators

Interference signal generators emulate jamming and interference signals. The purchase and operation of GPS /GNSS jammers is illegal in many different countries. However, it is possible to legally generate interference signals with an interference generator, e.g. a vector signal generator. It allow the user to directly inject the interference signals into the Device under test via cable and avoid the RF entering the surrounding environment. The interference generator can be combined with a GNSS signal generator and controlled by one software and its Graphical User Interface. This enables controlled simulation of both signal types together: the desirable GNSS signals and the undesirable interference signals, adding the possibility to modify the interference signals, set and modify the onset and end, signal strength and waveform. The interference signal can be attenuated or amplified step wise to allow for systematic sensitivity tests.

One such system is the Spirent GSS7725 Interference Generator, which allows the playback of real detected events or custom RF Interference Sources. "Interference signals can be generated from I/Q data files provided from real detected events, such as from a Spirent Detector [21]. The interference generator is controlled via Ethernet with a host controller which, when combined with a Spirent Simulator … allows seamless control of both GNSS and interference signals to be combined and generated …. The interference signals are in the form of canned I/Q files converted to RF interference signals with a 3 dB bandwidth up to 25 MHz A selection of these signals are available from predefined test scenarios for GNSS vulnerabilities and threats." Moreover, specific I/Q files can be generated. The interference source follows the trajectory of the simulated vehicle" [21, 22].

VII. Record and Replay Systems

In recent years, Record and Replay of GNSS signals has been established as an alternative method to simulation, with signals being received and captured in a static or dynamic measurement like a test drive, then converted to IF and stored on a hard disk, and later replayed in the lab after up-conversion from the IF back to the RF signals. [17].

The advantages are that the recordings can fully capture real signal environments with complex errors including obscuration and multiple reflections, called multipath. Multiple test drives or flights at difficult locations, with a known GPS/GNSS reception problem, can be captured and used for tests, with no need to revisit the real location. The replay tests are fully repeatable, as the same signal environment is reproduced during each replay, at the same time and date [26].

On the other hand, there is virtually no control over the signals and the error conditions in the recording, except that some attenuation can be applied. Contrary to GNSS simulators, time and date of the test flight cannot be changed, nor the amount of satellite signals present in the recording, nor the signal parameters and the navigation message.

For every new location or date, a new test recording is required. The recorded error conditions captured in the recording are usually unknown, unless the user has additional information about special conditions from external sources, like space weather reports. Test drives and recordings are easy and cost effective for stationary receivers and land vehicle based receiver, and possible for UAVs, and allow Software and Hardware testing including system trials, algorithm studies and iterative algorithm development, interference and jamming recording and monitoring. Tests are possible on UAVs capable of carrying a payload of 2.2 kg or more. See test-setup in figure 2.

One example of a record and replay system is the Spirent GSS6450. The record replay system GSS6450 is a portable unit with a weight of 2.2 kg. It is capable of recording 4 GNSS bands simultaneously at all L-band frequencies, including IRNSS (Indian Regional Navigation Satellite System), SBAS, Inmarsat based correction services, QZSS (Quasi Zenith Satellite System), B3, and Galileo E6, in short it will record all major GNSS bands via 1 RF input port. The latest version of the GSS6450 is capable of recording signals in the GNSS, WIFI and LTE band, simultaneously, via three RF input ports. During recording, the RF signals, are down converted, digitized and stored at IF and can later be faithfully replayed with minor losses of 1-2 dB. During playback, the IF signal is recreated and then up-converted to RF at the relevant GNSS frequency using the same built-in oven controlled local oscillator (OCXO) as used to record the data for minimum phase noise." [6]. RF signals can be recorded at 4, 8 or 16 bit for quantization and at 10, 30, 50, 60 MHz and 80 MHz bandwidth. There are throughput limitations at 8 and 16 bits and at 50, 60 and 80 MHz bandwidth, limiting the amount of channels that can be recorded simultaneously to 1-2. [6]. The GSS6450 contains an OCXO for record and playback for high frequency stability [2]. The advantages of a higher bit depth, e.g. 16 bit, are a reduction of loss in C/No during quantization and a higher dynamic range of signals recorded.

In addition the RPS GSS6450 contains an L1 only GPS/GNSS receiver, integrated together with an internal LINUX controller, allowing to cross check visible satellites and carrier to noise levels. NMEA data from the internal GNSS receiver can be stored to file [6]. Additional Recording of external data, such as CAN bus data and IMU data, is possible via serial ports and data is stored inside the GNSS file, so that it can be replayed synchronously. Up to eight synchronous inputs can be stored. Recording of four different video streams parallel to GNSS signals is also possible, and the video signals can be replayed within 0.5 sec of the GNSS signals.

In figure 2, a test setup for UAV applications can be seen: a UAV trajectory and GNSS signal environment can either be recorded by simulating them with a GNSS signal simulator and injecting the RF into the RF Input Port of the Record and Replay System, or a UAV carries the Record and Replay System as a payload, due to the low weight of the GSS6450 of 2.2 kg. In this case, the GPS/GNSS signal environment is recorded in flight along the UAV's trajectory.

If differential corrections are needed, a stationary Record and Replay system (RPS) can serve as a reference station together with a geodetic GNSS receiver. The Record and Replay system records the GNSS signals on the ground, while the geodetic GNSS receiver calculates the corrections, which are then transmitted to the device under test [20]. In RTK tests with a previous model with two stationary RPS and a baseline of 2 km, the accuracy of positions was less than 8 mm difference to the truth-value in latitude and longitude and about 13 mm in height. [20].

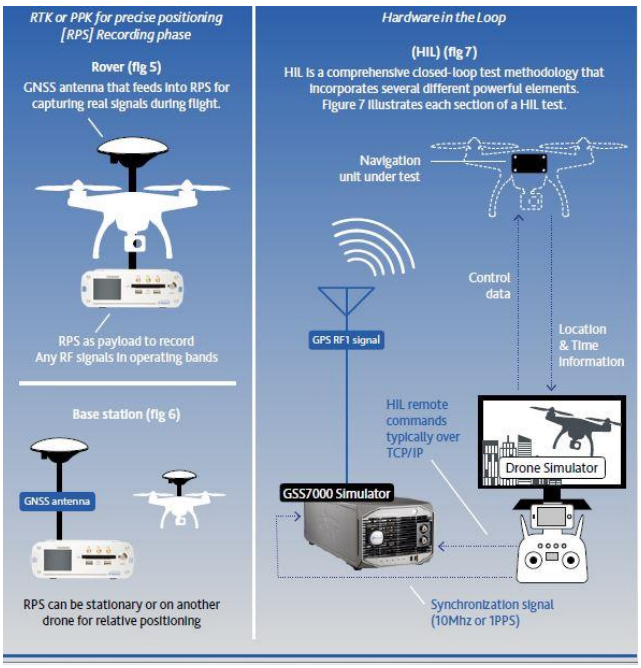

Figure 2: Record and Replay System and HIL [14]

VIII. Use Cases

Simulators and RPS (Record and Replay):

A Chinese manufacturer of commercial UAVs for precision aerial surveying, wanted to test the performance of their UAV

GNSS receivers. Using a high-end research and development R&D simulator, they were able to model a wide range of real-world conditions.

The particular focus was on how well the receiver would cope with high winds, multipath effects, atmospheric interference, signal obscuration, and the vibration and tilting of the UAV in flight. The high-end research and development simulator was able to simulate all of these conditions to characterise the performance of the receiver. In addition, this company is also using a Record and Replay System to record and replay live test flight data in the lab, greatly reducing the amount of additional test flights. [14]

Simulator and Engineering Test Services:

A US company wanted to apply for an FAA certification for their UAVs and asked for help with conversion of DO 229 test cases into simulator scenarios, to prove that their UAV GNSS receiver could be compliant to the aviation MOPS (Minimum Operational Performance Standard) in aviation standard DO-229. Simulator tests were used to help them prove air-trustworthiness of their UAV GNSS system. Simulator scenario generation and testing of the GNSS receiver part were outsourced to experienced test engineers and carried out with a combination of a GPS/GNSS simulator and interference simulator as described above.

Tests included are:

Scenario	Constel-lations	Interfe-rence	Description
1	GPS + SBAS	No	Received messages can be decoded properly. Calcu-late the loss rate of messages over 6 hours.
2	GPS	No	Detect an error in the root square semi-major axis (A1/2) parameter of the ephemeris transmitted by a satellite.
3	GPS	No	Introduce a pseudorange step error (m) in a satellite signal. Check that the receiver can exclude quickly the satellite from the navigation solution.
4	GPS	No	Similar to above, for a pseudorange ramp error (m/s), then check that the receiver can exclude quickly the satellite from the navigation solution.
Scenario	Constel-lations	Interfe-rence	Description
5	GPS	Yes	Valid Horizontal Protection Level (HPL) and position error within a certain threshold under the pre-sence of interference for a moving receiver.
6	GPS	No	How quickly the receiver can re-acquire the signal of a satellite.
7	GPS + SBAS	No	How quickly the receiver can re-acquire the signal of an SBAS satellite.
8	GPS	Yes	Ability to exclude a satellite with high Interfe-rence-to-Signal Power (I/S) ratio
9	GPS + SBAS	Yes	Ability to maintain robust pseudorange measurements under interference condi-tions (at various frequency test points).

Table 1 DO 229 Example test cases [personal communication, Kimon Voutsis, Spirent]

Interference monitoring:

DETECTORs cannot be used directly for testing interference. They are mainly used to monitor the signal environments continually for longer periods. Such monitoring field measurements have been performed in many locations around Europe. One 2 week field test near a German Autobahn and near a small airport demonstrated 238 interference events, spread out quite evenly over the 2 weeks, with 34 high priority events [5], having a strong impact on C/No of GNSS signals and numbers of tracked satellites in a professional GNSS receiver installed at the same site. [5].

DETECTORs can contribute to testing interference, because they acquire signal snapshots, as spectrum and spectrogram, which can be converted into test files, to be replayed by a professional interference signal generator (see above), enabling laboratory testing of real life interference events. In this way, more realistic, repeatable testing of real jamming threats becomes possible.

IX. Timing and Synchronization in a UAV Swarm

UAVs flying in a swarm are used for strategic and highly professional operations. They need to be steered in synchronized action, so that they do not collide with each other and external structures, thus they need to be synchronized in time and space. In order to synchronize UAVs flying in a swarm, all UAVs need be on the same time-scale with a high accuracy of timing information. One way to do this is, when all members of the swarm are equipped with the same type of GPS/GNSS receiver, and with a high quality oscillator (e.g. Oven Controlled Oscillator OCXO) with a drift of 0.002 ns/s or with a slightly less stable more lightweight TCXO (Temperature Controlled Oscillator) with a drift of 200 ns/s. In addition, the UAVs need at least one communication link to a central server and communication station, which

monitors and controls their movements, via telemetry commands.

Almost all professional UAVs are equipped with a GPS/GNSS receiver, integrated into their on-board flight control system. The receivers are able to calculate a time with very good accuracy from the GNSS signals: standard receivers achieve a normal timing accuracy in the range of about 100 ns, resulting from a calculation of a position and timing fix (PNT fix), which does not drift. In order to synchronize the drones in a swarm, it is sufficient to transmit the resulting times of each UAV to a central processing server and record the messages. The normal timing accuracy of a GPS/GNSS receiver is in the range of about 100 ns. However, the computer chips with a LINUX operating system embedded in the navigation and control unit only support timing accuracies of 100 – 200 µsec. Thus, the accuracy available by the GPS/GNSS receiver cannot be fully used. A drone flying at 10-20 m/sec (36-72 km/h), would move only 0.02 mm in 1000 ns, and will move only 2-4 mm in 100-200 µsec. If the position of all drones in a swarm is known at the beginning of the swarm flight, with a sufficient accuracy of a few cm, the small timing differences of GPS/GNSS time cannot cause any major conflicts in their flight trajectories.

The OCXOs (or TCXOs) of all drones will be synchronized by the GPS/GNSS time at the initial phase of the flight, and serve as a backup in case of lack of GPS/GNSS signals. This process takes about 4 minutes. After a synchronization phase, the OCXOs (or TCXOs) are independent of the GPS/GNSS time and thus able to provide precise timing on their own for several minutes, even if GPS/GNSS fails due to errors and vulnerabilities (see above). Whenever GPS/GNSS signals are available, the precise time from the PNT fix will serve as correction for the OCXO, at regular intervals throughout the flight of the UAV, and thus maintain precise time in each UAV.

In this way, synchronization of UAV timing and position is achieved in a first step and synchronization is maintained during the flight. In a second step, control of their joint actions is managed by the central control server, which will send manoeuvre control commands tagged with a timestamp to ensure that the commands are carried out simultaneously by all UAVs in the swarm. The manoeuvre control commands could also be sent out to take immediate effect, provided that the swarm members are flying close by each other within 500 m, else there will be a propagation delay of the transmitted command signals, causing a certain offset in the arrival at the UAVs command receiver, also causing lack of synchronization in the motion, if uncompensated for. As all the positions of all the UAVs are available and known at the central control server, an offset can be included in the timestamp of the action and manoeuvre commands to compensate the propagation delay due to different distances of the UAVs to the control centre.

The greatest problem for the swarm could occur in case of loss of communication path to the central server. In this case the UAV's should have an on-board program with a predefined security manoeuvre, e.g. a "return to home" trajectory, enabling each member of the swarm returning to its initial homing position.

In order to implement the synchronization functionality, normal COTS timing systems and standard timing GNSS receivers are fully adequate. We assume that drones for swarms will be used for professional applications, e.g. surveillance of an area and have a sufficient size to be able to easily carry both the additional OCXO (weight about 8 g) or TCXO (with a weight of 1-2 g), and the Telemetry and command unit, receiving the commands from the central control server. The precision of this timing solution, GPS/GNSS time, which does not drift, combined with a local OCXO, which does drift, but is always available, is far better than the level necessary for navigation and manoeuvre control. At the same time, this timing precision is a great advantage for data acquisition and data transmission.

X. Conclusion

As GNSS positioning, navigation and timing are crucial for most UAVs in flight and for many different UAV applications, it is important to test the performance of GNSS based flight controllers of UAVs.

In this paper, we give an overview of different types of GNSS errors and vulnerabilities, such as interference, spoofing, multipath and GNSS system errors. We also introduce different methods to monitor and generate interference signals, and emulate or replay complete GNSS signal environments including diverse errors and interferences with high fidelity and close to reality. These emulated or replayed signals can be used in the laboratory for controlled and repeatable testing. Different test setups are possible, and have been used manifold in real-life field tests and laboratory tests. We present three examples of such field and laboratory test campaigns. In addition, we introduce a method to combine GNSS timing results with an OCXO (TCXO) for precise synchronization of timing and motion in a swarm of UAVs.

XI. Acknowledgements

We are grateful to Kimon Voutsis, from Spirent Communications, for contributing real-life examples of test cases and Clive de la Fuente, INS, for results of RTK measurements with the GSS6425 and GSS6450 RPS.

References

[1] Spirent, "Improving PNT for Smarter Drones" *MCD00383 Drone Test eBook Issue 1-00 0817 NEW, 2016*

[2] K. v. Huenerbein, W. Lange, " Monitoring of the interference environment on large vehicles with a network of highly accurate record and replay systems synchronised by a very precise timing unit", *European Navigation Conference, Lausanne, Switzerland, 9th -12th May,2017*

[3] K. Hünerbein, W. Lange "Real Life Evidence for Spoofing and Jamming of GNSS Receivers", *Conf. Proc. of CerGal, DGON Conference, Darmstadt, Germany, 7th-8th July ,2015*.

[4] U. Bestmann, M. Steen, P. Hecker, A. Konovaltsev, M. Heckler, F. Kneissl, "Aviation Applications: Hybrid Navigation

Techniques and Safety of Life Requirements, Part 1" *Inside GNSS, June 2010,* pp. 64-72.

[5] M. Stanisak, K. Hünerbein, U. Bestmann, W. Lange, "Measured GNSS Jamming Events at German Motorways", *Proc. of POSNAV ITS, DGON Conference, Berlin, Germany,5th-6th July, 2016*.

[6] Spirent Communications, "Spirent GSS6450 Multi-frequency Record & Playback System", *Datasheet with Product Specification: MS3098 Issue 2-02 March 2017.*

[7] D. Shephard, J. Bhatti, T. Humphreys, "Drone Hack: Spoofing Attack Demonstration On a Civilian Unmanned Aerial Vehicle", *GPS World, vol.23(8), Aug 2012,* pp. 30-33.

[8] D. A. Divis "GPS Glitch Caused Outages, Fueled Arguments for Backup". *Inside GNSS, News. 29th Jan 2016. http://insidegnss.com/ gps-glitch-caused-outages-fueled-arguments-for-backup/*

[9] Editor of GPS World "GLONASS Fumbles Forward - Two April Disruptions Furnish Fodder for Multi-GNSS Receivers and Alternative PNT" *GPS World May, Vol 25(5), 2014,* p. 16.

[10] G. Gibbons "Satellite Outages afflict GLONASS", *Inside GNSS, Editor's News Update May/June 2014, Vol 9(3)*

[11] M. Jones, "The Civilian Battlefield", *Inside GNSS, March/April 2011, vol. 6, no. 2, pp. 40-49.*

[12] M Cuntz, A. Konovaltsev, A. Hornbostel, E. Schnittler, A. Dreher, "GALANT – Galileo Antenna and Receiver Demonstrator for Safety Critical Applications", *European Microwave Week. European Microwave Association. EuMW, 2007, München, Deutschland*

[13] Spirent Communications, "An Introduction to Testing Navigation and Positioning Performance in Drones, UAS and UAVs" *E-Book, 2016*

[14] Spirent Communications, "How to Construct a GPS/GNSS Test Plan -- A guide for engineers integrating GPS / GNSS capabilities into new devices", *E-Book, 2015, https:// www.spirent.com/Assets/EB/EB_How-to-Construct-GPS-GNSS-Test-Plan*

[15] Spirent Communications, "GSS200D GNSS Interference DETECTOR." *Datasheet with Product Specification. MS3103 Issue 2-00, March 2017*

[16] K. Huenerbein, W Lange "Testing of GNSS Receivers with Recorded and Replayed Signals of Multiple Constellations",, *Conference Proceedings of DGON Conference CERGAL, 8th-9th, July 2014, Dresden, Germany,*

[17] E. Vinande, B. Weinstein, T. Chu, and D Akos, " GNSS Receiver Evaluation, Record-and Replay Test Methods", *GPS World , Jan 2010, vol. 21(1),* pp. 28-33

[18] J. Pottle "System Health". *GPS World, May 2012, vol.23 (5),* p. 13

[19] J. Sickle, "GPS for Land Surveyors". *Book.* 3rd edition, Taylor and Francis Group, *2008*

[20] C. Fuente, "GSS6425 Multi-Frequency Record\playback - 50MHz RTK Results", *Presentation, 2016.*

[21] Spirent Communications, "GSS7725 Interference Generator", *MS7725 Datasheet with Product Specification, Issue 1-00 March 2017*

[22] Spirent Communications, " GNSS Vulnerability – Interference Effect mitigation Testing", *Application Note, DAN030, Issue 1-00, 2018*

[23] Spirent Communications " "Better Understand and Protect Against GNSS Interference in Civil Aviation", *E-Book, MCD00379 Issue 1-00, 2017*

[24] U. Celestino et al. "Expanding EGNOS Horizons in North Africa and the Middle East", *Inside GNSS March/April 2015, vol. 10(2)* , pp. 44-52

[25] T. Sharpe, R Hatch, F. Nelson. "John Deere's Starfire System: WADGPS for Precision Argriculture", *2006, https://web.archive.org/web/20060711194114/http://www.navcomtech.com/docs/StarFireSystem.pdf*

[26] K. v. Huenerbein, W. Lange, " Monitoring of the interference environment on large vehicles", *Coordinates,col XIII(9), Sep 2017,* pp. 34-39