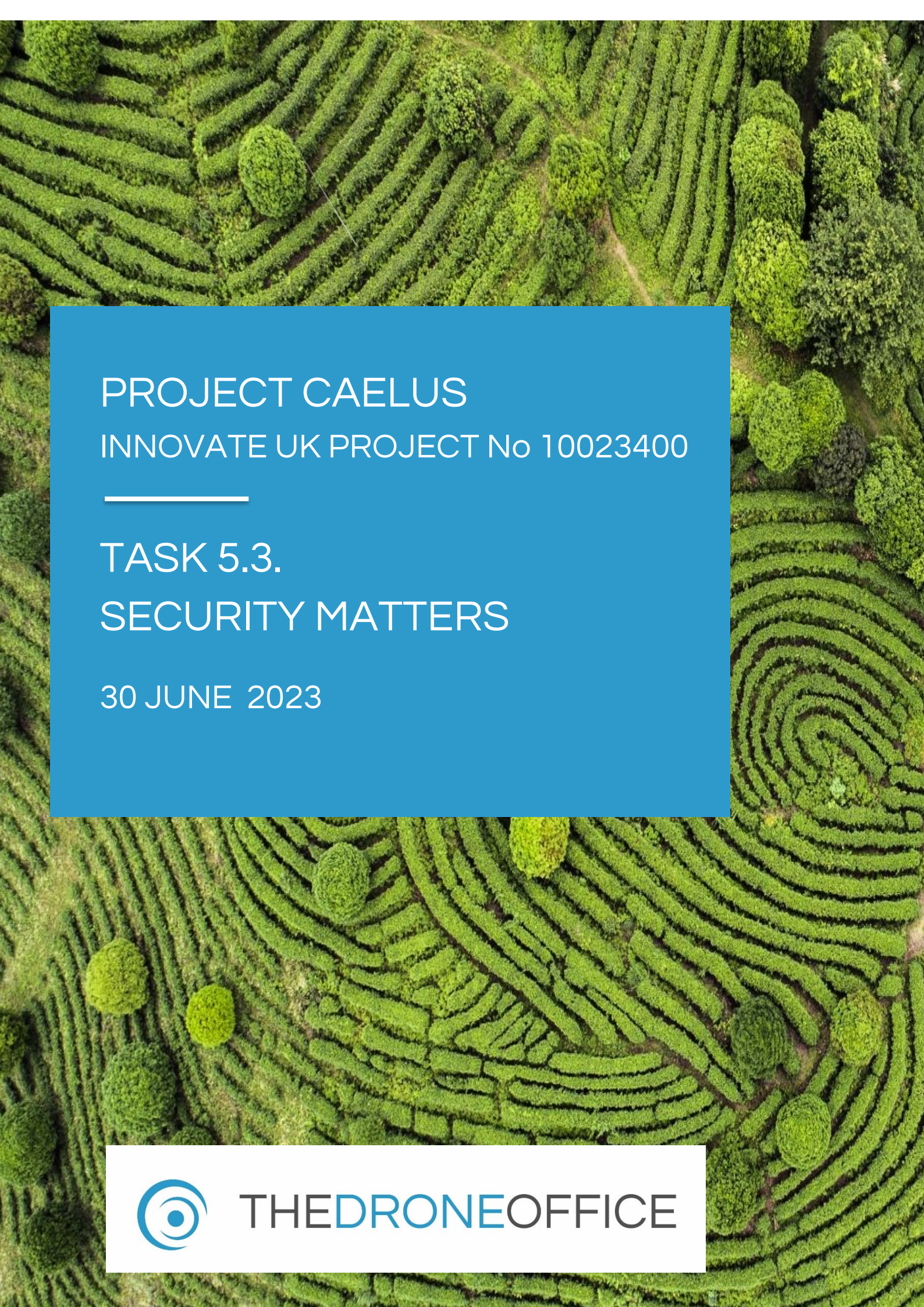


PROJECT CAELUS

INNOVATE UK PROJECT No 10023400

TASK 5.3.
SECURITY MATTERS

30 JUNE 2023

THEDRONEOFFICE

ALL INFORMATION HAS BEEN MADE AVAILABLE ON THE CAELUS COMMONPLACE WEBPAGE

WWW.CAELUS.COMMONPLACE.IS

Table of Contents

I. REGISTRATION

DID YOU KNOW?
YOU MUST FIRST REGISTER BEFORE FLYING MOST DRONES

REGISTRATION: DRONE FLYER ID AND OPERATOR ID

Mandatory registration is applicable to all drones in the UK. The only exception is for drones lighter than 250 grams that are either toys or do not have a camera.

For example, the DJI Mini weighs less than 250g (249g) but has a camera, therefore you must register.

That way, each drone actually has an identifiable Operator ID label and a verifiable pilot behind it in the first place.

There are in fact two separate registration requirements:

- The remote pilot, equivalent to the pilot in the cockpit in commercial aviation, must first pass an online theory test and get a **flyer ID.** The remote pilot is responsible for flying safely and legally when actually piloting the drone.
- The person or organisation responsible for the drone, equivalent to the airline company in commercial aviation, must also register for an **operator ID**.

The operator must:

- make sure that only people with a valid flyer ID use their drone.
- label their drones with their operator ID.

The online theory test to get a Flyer ID covers the very basics and helps users understand how to fly in a sufficiently low risk environment, depending on the drone you pilot. More complex flying, for example closer to people, require additional training and pilot competencies.

For more information, check the Civil Aviation Authority web pages on The Drone Code.

It is against the law to fly a drone without having the required IDs. People can be fined for breaking the law when flying. In the most serious cases, they could be sent to prison.

II. TRACKING TECHNOLOGIES

TRACKING TECHNOLOGIES LIKE REMOTE-ID OR NETWORK-ID WOULD PROVIDE ASSURANCES THAT THE DRONES OPERATING NEARBY ARE LEGAL AND SAFE.

SUMMARY

Tracking technologies forming the first steps of "Unified or Unmanned Traffic Management UTM" will give a real-time map of which drones are flying in a particular area.

One way of performing that real-time tracking is called "Remote ID", or "digital license plate" for drones. The drone provides real-time information during the flight so that it can be tracked and identified – like a "Find My" app on a smartphone. Anonymized ID information would be accessible to the public. More detailed information would be transmitted to the Unified or Unmanned Traffic Management system to create that real-time flying map and ensure the safety and efficiency of flying operations.

Tracking technologies such as remote ID serve several purposes: privacy, security, facilitating law enforcement, and it is a building block for advanced operations such as Unified or Unmanned Traffic Management UTM. More importantly, Remote ID helps increase public trust in drone operations by providing assurances that the drones operating nearby are legal and safe. Some countries follow different approaches and use different terms when they are referring to remote ID for security purposes, vs tracking technology for UTM. Both purposes are combined for ease of read in this article.

Remote ID is on its way both in the USA and in Europe for end 2023/2024.

UNDERSTANDING REMOTE IDENTIFICATION, OR "REMOTE ID"

What is Remote ID? The "digital license plate" for drones.

Remote ID is often referred to as a "digital license plate" for drones. It is a functionality on the drone that provides real-time flight information about the drone and its remote pilot's location. It is similar to "Find My" on a smartphone, except that people could track and identify (via an anonymous ID, no actual name or contact details disclosed of course) drones flying in their immediate surroundings.

Why would we need Remote ID? Primarily for privacy, security, facilitating law enforcement.

Drone usage has been increasing dramatically over the last few years and helps increase the efficiency and productivity of many industries. However, these new innovations bring new concerns for the public.

For example, some may worry about whether the drone flying nearby is being controlled by malicious actors, others may be frightened that these machines could be used to spy on their activities, how could the police forces or even people know that the drone they see is operating legally?

"Remote ID is designed to provide greater security, accountability, and safety of drone operations, where a drone will be required to transmit real time information such as a unique serial number and location, enabling it to be tracked. It has the potential to support authorities such as the aviation authority to allow for safer flying, and with law enforcement to allow for threat

mitigation and traceability for enforcement by being able to identify a drone, its associated location, altitude and potentially its control station location and take-off point."

Why would we need Remote ID? To help increase public trust in drone operations by providing assurances that the drones operating nearby are legal and safe.

Many local authorities have been confused regarding whether they should or should not authorise drone flights on their land. How could they know what to do? They certainly are not experts in aviation regulations, cannot possibly keep up with their evolutions, and having a tool such as Remote Identification available to authorities, and possibly to citizens, would greatly alleviate their concerns. Many are not aware that drone flights are already regulated by the Civil Aviation Authority when it comes to safety, i.e., not endangering people and assets on the ground. Having knowledge of this regulator and implementing Remote ID should help greatly.

Why would we need Remote ID? It is also a building block for more advanced operations.

Remote ID is necessary to address aviation safety and security issues regarding UAS operations in our airspace and is an essential building block toward safely allowing more complex UAS operations.

WHAT IS HAPPENING IN THE USA?

> **In the USA, Remote ID should become effective in December 2022 for drone manufacturers, and September 2023 for drone operators. Our understanding is that it will apply to all drones (except for sub 250grams drones flown for recreational purposes in model aircraft club environment, and federal agencies), and that the public could access anonymous identification number to then share with the relevant authority for check.**

If you want to know more, please read the Federal Aviation Authority FAA's website pages on Remote ID.

The FAA's Notice of Proposed Rulemaking (NPRM) on Remote Identification of Unmanned Aircraft Systems was first published on December 31, 2019. Thousands of comments were made, resulting in amendments and delays.

The effective date of Remote ID compliance for drone makers has been pushed back to December 16, 2022. All drone pilots required to register their UAS must operate their aircraft in accordance with the final rule on remote ID beginning September 16, 2023, which gives drone owners time to upgrade their aircraft.

Will it apply to all drones?

The FAA remote ID regulations apply to nearly all drones, with exceptions for (a) drones under 0.25kg that are used for recreational purposes only and under the safety guidelines of an FAA-recognized Community Based Organization like model aircraft club, and (b) for the U.S. Department of Defence or other federal agencies.

What information will be broadcast?

Whether using a Standard Remote ID Drone or a remote ID broadcast module, nearly all of the message elements are the same and they must be broadcast from take-off to shut down.

A Standard Remote ID Drone must broadcast by radio frequency, i.e., Wifi or Bluetooth the following message elements:

- A unique identifier for the drone. Operators of a Standard Remote ID Drone may choose whether to use the drone's serial number or a session ID (an alternative form of identification discussed below that provides additional privacy to the operator) as the unique identifier;
- An indication of the drone's latitude, longitude, geometric altitude, and velocity;
- An indication of the control station's latitude, longitude, and geometric altitude;

- A time mark; and
- An emergency status indication.

Who can access the information?

Only authorized parties such as law enforcement will be able to see personal information about the remote drone ID, but the public will be able to see the identification number labelled on the drone, which can then be cross-referenced with the FAA database to find the owner.

How does/will Remote ID work?

In the USA, there are three ways drone pilots can meet the identification requirements of the remote ID rule:

- Operate a Standard Remote ID Drone that broadcasts identification and location information of the drone and control station. A Standard Remote ID Drone is one that is produced with built-in remote ID broadcast capabilities.
- Operate a drone with a remote ID broadcast module giving the drone's identification, location, and take-off information. A broadcast module is a device that can be attached to a drone, or a feature (such as a software upgrade) integrated with the drone. Persons operating a drone with a remote ID broadcast module must be able to see their drone at all times during flight.
- Operate without remote ID equipment, but only at specific FAA-recognized identification areas (FRIAs) maintained by community-based organizations or educational institutions. FRIAs are the only locations unmanned aircraft (drones and radio-controlled model airplanes) may operate without broadcasting remote ID message elements.

Can existing drones be retrofitted?

Yes, a broadcast module can be attached to existing drones, or a software upgrade can provide adequate retrofit functionalities to existing drones.

WHAT'S HAPPENING IN EUROPE?

In Europe, Direct Remote ID, or "DRI," is a compulsory functionality for all drones class-marked C1 and above – but not for Class C0 sub 250grams., nor tethered C3, nor C4 model aircraft. Class marking drones should now be implemented starting January 2024. The public can access anonymous identification number (as well as the location of the drone pilot?) to then share with the relevant authority for check.

The effective implementation of Remote ID is dependent on the more global process of approving Class-marked drones so that they become available for sale on the market. Like in the USA, the key manufacturers have already developed Direct Remote ID functionalities.

Drones with a class identification label (i.e. C0, C1, C2, C3, C4) are expected to become commercially available by end of 2022. The transition period has been extended to 31 December 2023. Starting from 1 January 2024 operations in the open category must be conducted either with a drone bearing a C0 to C4 class identification label, or being privately built or even without class identification label but only if purchased before 31 December 2023.

For reference, in Europe, the Delegated Regulation (EU) 2019/945 lays down the requirements for the design and manufacture of unmanned aircraft systems ('UAS') intended to be operated under the rules and conditions defined in Implementing Regulation (EU) 2019/947 and of remote identification add-ons. It also defines the type of UAS whose design, production and maintenance shall be subject to certification. The regulation provides for class marking of drones.

Will it apply to all drones?

Direct Remote ID is a requested feature for all drones from class C1 (more than 250g) and above, with the following exemptions:

- Class 0 drones that weigh less than 250 grams (including payload).
- Class 3 drones with a tether of less than 50 meters and 25g total weight including payload. These must be fully electrically powered and have geo-awareness functionality and features with alerts for low batteries.
- Class 4 drones that weigh less than 25kg and have no automatic control functions aside from flight stabilization (i.e., model aircraft).

What information will be broadcast?

The UA or Unmanned aircraft or drone must have a direct remote identification that:

(a) allows the upload of the UAS operator registration number provided by the registration system. The system shall perform a consistency check verifying the integrity of the full string provided to the UAS operator at the time of registration. In case of inconsistency, the UAS shall emit an error message to the UAS operator;

(b) ensures, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, in a way that it can be received directly by existing mobile devices within the broadcasting range, of at least the following data:

- the UAS operator registration number and the verification code provided by the Member State;
- the unique serial number of the UA;
- the time stamp, the geographical position of the UA and its height above the surface or take-off point;
- the route course measured clockwise from true north and ground speed of the UA;
- the geographical position of the remote pilot or, if not available, the take-off point; and
- an indication of the emergency status of the UAS;

(c) reduces the ability of tampering the functionality of the direct remote identification system.

If the UA or drone is equipped with a network remote identification system or a direct remote identification add-on, the information broadcast is equivalent.

Will the localisation of the drone pilot, or at least his/her ground station be tracked?

Yes, the drone pilot's position, or more precisely his/her ground control station will be broadcasted.

Can existing drones be retrofitted?

Yes, drones may comply with Direct Remote ID requirements either with a built-in broadcast functionality or an add-on module that satisfies EASA requirements.

Who can access the information?

Anybody in the public via an app on their mobile phones can, as long as they are close enough to the drone to receive its remote ID broadcasting. Operator's registration data and personal data (name, address etc) are kept by the authority in a database not accessible to the public.

We are not sure whether the public can access only a subset of information broadcasted like the operator registration number, or if the public could also access the pilot location (or the take-off position of the drone).

WHAT WILL HAPPEN IN THE UK?

The UK is focusing on Electronic Conspicuity as the key tracking terminology and technologies. The main objective is to develop the first set of functionalities offered by the "Unmanned Traffic Management" services to make sure drones and other aircrafts avoid one another in the sky. There may be a consultation on remote ID implementation in the UK during 2023, or maybe later to capture the lessons learnt from the USA and Europe.

REFERENCES

[1] https://www.pwc.co.uk/intelligent-digital/drones/skies-without-limits-2022.pdf

[2] Public dialogue on drone use in the UK Moving Britain Ahead. (2016). [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579550/drones-uk-public-dialogue.pdf [Accessed 5 Oct. 2022].

[3] Belwafi, K., Alkadi, R., Alameri, S.A., Hamadi, H.A. and Shoufan, A. (2022). Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey. *IEEE Access*, 10, pp.87577–87601. doi:10.1109/access.2022.3199909. [Accessed 5 Oct. 2022]

[4] Faa.gov. (2019). *UAS Remote Identification | Federal Aviation Administration*. [online] Available at: https://www.faa.gov/uas/getting_started/remote_id. [Accessed 5 Oct. 2022]

[5] DEPARTMENT OF TRANSPORTATION. (2020). *Remote Identification of Unmanned Aircraft | Federal Aviation Administration.* [Docket No.: FAA-2019-1100; Amdt. Nos. 1-75, 11-63, 47-31, 48-3, 89-1, 91-361, and 107-7] [Accessed 5 Oct. 2022]

[6] www.caa.co.uk. (n.d.). *Register to fly a drone or model aircraft | Civil Aviation Authority*. [online] Available at: https://www.caa.co.uk/consumers/remotely-piloted-aircraft/register-to-fly-a-drone-or-model-aircraft/. [Accessed 5 Oct. 2022]

[7] DJI Official. (2022). *DJI's Top Drone Models Approved for FAA's Remote ID Mandate*. [online] Available at: https://www.dji.com/newsroom/news/dji-top-drone-models-approved-faa-remote-id [Accessed 6 Oct. 2022].

[8] Tabbara, R. (n.d.). *How to activate Remote ID on Parrot drones*. [online] www.911security.com. Available at: https://www.911security.com/blog/how-to-activate-remote-id-on-parrot-drones [Accessed 6 Oct. 2022].

[9] AeroPing - Drone Defence. (n.d.). *Drone Defence*. [online] Available at: https://www.dronedefence.co.uk/aeroping/ [Accessed 8 Oct. 2022].

[10] Thales Group. (n.d.). *ScaleFlyt Remote ID: Identification & tracking for safe drone operations*. [online] Available at: https://www.thalesgroup.com/en/markets/aerospace/drone-solutions/scaleflyt-remote-id-identification-tracking-safe-drone-operations [Accessed 6 Oct. 2022].

III. SECURITY OF TRACKING TECHNOLOGIES: INTERVIEW WITH JAMES DUNTHORNE, NEURON INNOVATIONS

https://youtu.be/OZPm9sVczTg

TRANSCRIPT

Anne-Lise Scaillierez: Good afternoon, James, and thank you for having this conversation with us. Now, James, can you tell us a bit more about yourself and Neuron Innovations?

James Dunthorne: Hi there. Yes, thanks Anne-Lise. I'm James, James Dunthorne, I'm CEO of Neuron Innovations. So, my background is in aeronautical engineering. We build technology that provides surveillance and tracking services to drone operators, airports and other community users who need secure and trustable aviation data. I've been in the industry, been flying drones for about 11 years, done some really cool projects that I'm not allowed to talk about unfortunately. All the best projects you're never allowed to talk about. But yeah, that's probably me in a nutshell.

Anne-Lise Scaillierez: Alright, very good. Thank you so much for this overview. So, you know, to be frank, you were on my top list of experts that I wanted to engage with when it comes to discussing security matters - one of the concerns that were raised by the public in general public surveys. So, I think for today, if that's alright with you, we are going to talk about tracking technologies and how it helps enhancing security of use of drones, but also how, like in any technology, there may be some risks and how we are going to mitigate them. So maybe if that's alright with you can you explain to us, in simple terms, what we mean by the tracking technologies?

James Dunthorne: Yeah, sure. So surveillance and tracking is the idea of being able to see where things are in the sky. Whether that's a drone or an aircraft, traditionally it's always been crewed aircraft, whether that's your airliners or general aviation aircraft that are sort of going on hobby flights, but it's the idea of being able to locate them in 3D space and in time and that information can be used for a range of purposes, whether it's planning, whether its safety or trying to keep them from crashing into each other. There's a range of different technologies that you can use - ADSB is probably the most common form of surveillance, but there's all sorts of others including things such as flan, which is what the glider community use. When we're talking about surveillance and tracking technologies, what we're talking about is the suite of different technologies that allow you to track the position and time of where these aircraft and drones are.

Anne-Lise Scaillierez: Thanks, James. So it's really good to know that there are technologies that help us provide a real time map of aircraft in the sky, whether there are drones or whether there are conventional aircraft or helicopters. Now these technologies, do you think that they have some security vulnerabilities that should be considered as well?

James Dunthorne: Yeah, well, a lot of these technologies are quite old. ADSB is many decades old, and it wasn't really designed to be in this new world we live in with drones. So, one of the problems is, because it's not an encrypted and protected technology, you can essentially fake signals so pretending there are aircraft in the sky when there aren't. Obviously when you're using this information for navigation purposes this could cause a problem because you could see something up ahead of you that isn't actually there. This could be used by cybercriminals or

attackers to do things if there wasn't a solution to that. So that's probably one area that that obviously needs to be addressed. The second area is, who's actually sending this information? Obviously if people are spoofing or faking data within this ecosystem, then where does that data come from in the first place and how do we know which aircraft are which? We need to know from a drone perspective. You got people flying in from the ground and so obviously we need to understand who these people are who are in charge of those vehicles. Otherwise, if they're doing something that they're not meant to be doing that could cause a big problem. So, these are probably the two areas where I would say are the biggest areas from a security perspective.

Anne-Lise Scaillierez: Alright, understood. Those security vulnerabilities, to call it this way, apply to both drones and non-drones or other aircraft because these technologies are on board other aircrafts today. So, I mean, looking at the complete ecosystem then - can you let us know how neuron innovations help solve that problem.

James Dunthorne: Yeah, sure, so the problem of which I talked about around fake data or spoofing information this can be solved, and has been solved in the past, by air traffic control by using multiple devices. What you can do is actually calculate the time when the signal was received from multiple devices and use that to triangulate the position or figure out using clever mathematics where that aircraft is in real space. You can then check that against the reported position and see if they marry up with each other. If they don't then there's a high probability that that aircraft isn't a real aircraft and so we can use that (commonly called multi-lateration for those who are interested in the technology) technique to essentially remove the problem, or certainly reduce it to something that's almost inconceivable.

The other area I would say that we can solve some of these problems is through authentication. So, when you're accepting data into this ecosystem, you can sign those data packets essentially, which allow you to work out who was sending that information, who was requesting that information, and that's really important for basically data provenance, so understanding who was responsible. If someone did do anything that they weren't meant to, we can at least trace it back to who it was - essentially a passport and ID card that says okay it was this person who did that. And this is really important when it comes to sort of accountability.

On the issue with knowing which drones are where, each of these devices that are put on the aircraft have to be associated with essentially like an electronic number plate like you would have on a car, but a call sign which gets associated with the specific aircraft. That call sign like your car number plate is registered to a specific person and so by putting this device in the aircraft, we can associate that particular aircraft to a particular person, which when it gets detected by the sensors on the ground that detect the location of that aircraft gives us a trace all the way back to the person who's flying the aircraft so it creates essentially a chain of custody right from the person registering their aircraft, right the way through to that data being received, we now know exactly who that person is flying the drone or the aircraft.

Anne-Lise Scaillierez: Well, that's brilliant. I think it's really good to know that those security measures are in place and that there is technology available and thriving here in the UK to support those new developments. So, James, I'd like to thank you very much. If it's OK If we get some questions from the audience, are you happy that we share your contact details with our audience?

James Dunthorne: Certainly, no problem and you can find out a little bit more on Neuron.world or on our app, our tracking app, which is 4dsky.com.

Anne-Lise Scaillierez: Brilliant. Thank you, James.

James Dunthorne: Thank you.

IV. SECURITY OF GNSS/GPS: WHAT IF A DRONE'S GNSS/GPS SIGNAL IS LOST OR JAMMED?

Drone = UAS, Unmanned or Uncrewed Aircraft System = Remotely Piloted Aircraft System, RPAS

SUMMARY

Most drones use GNSS/GPS, meaning Global Navigation Satellite System, to determine their precise location, navigate, and follow their automated flight paths.

Interference in satellite signals from other electronic devices is becoming a growing issue, not only for drones, and not only due to malicious intent!

A degraded GNSS/GPS signal, or the loss of signal during a flight, can start for many reasons, mainly interferences from the environment. It is a known vulnerability, and it is therefore mitigated and managed. Mitigation and safety measures may include the redundancy of sources of positioning data with inertial sensors onboard, automatic fail-safe modes such as Return to Home, anti-jamming equipment. Some drones on the market are specifically conceived to navigate in a GNSS/GPS denied environment, such as indoor inspections, using onboard camera and sensor-based situational awareness for obstacle avoidance – some drones are combining both sensor-based situational awareness and GNSS-based navigation.

WHAT IS GNSS? DIFFERENCE BETWEEN GPS AND GNSS?

Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location. By definition, GNSS provides global coverage.

Examples of Global Navigation Satellite Systems, or GNSS, include:

- USA's GPS
- Europe's GALILEO
- Russia's GLONASS
- China's BEIDOU

You will know GNSS from mobile devices like phones, where apps like google maps or "Find My" use your geo-position to help you reach your destination or orientate yourself.

WHY DO MOST DRONES NEED GNSS/GPS INPUT?

Most drones rely on GNSS to determine their precise location and navigate.

Of course, smaller drones such as toys do not need satellite-based navigation: the remote flyer can simply pilot his/her drone, like a car toy with a remote control.

For professional applications however, precise navigation, and precise geo-tagging of the data collected is often required. For more advanced operations such as long-range automated flights, satellite-based navigation system is the norm. It is overall cost-effective, accurate and reliable.

Can a drone lose its GNSS signal?

Unintentional interferences

Interferences, obstacles, and loss of satellite signal is becoming an increasing issue, but not only for drones! Satellites' signals coming from their orbit at around 20 000km are in a way competing

with many signals on our busy and connected planet earth. There can be a lot of "noise" around the receiver, and there can be a lot of obstacles between the satellites and the receiver.

For example, a drone can lose its GNSS signal when operating:

- Indoor – unlike mobile phone signals, satellite signals do not go through walls
- in an area with lots of obstacles such as buildings, trees, bridges, structures… all forming potential obstacles to GNSS reception
- close to electric power lines or other electric or electronic devices, or metallic structures that may create signal interferences.

Intentional interferences, jamming, spoofing.

Satellite signals may also be interrupted or jammed or spoofed intentionally, as illustrated in other GNSS/GPS applications.

For example, some truck drivers may use a GPS jammer, readily available online at a modest price, to jam their trucks' GPS trackers, so that their company may not be aware of all their whereabouts. Some employees may consider the same when using their company cars outside of business hours.

Also, did you know that a number of options are openly described on the internet to fake your mobile phone's GPS position and collect more points at Pokémon Go?

WHAT HAPPENS IF A DRONE LOSES ITS GNSS SIGNAL?

A degraded GNSS/GPS signal, or the loss of signal during a flight, for whatever reason and starting by interferences from the environment, is a known vulnerability. It is therefore mitigated and managed. Mitigation measures and safety responses include for example:

- Redundancy of sources of positioning data, for example with inertial sensors onboard
- Fail-safe modes automatically triggered by the loss of GNSS signal, without the need for human input. Typically, drones on the market would perform one of three things: return to home (RTH), hover on the spot, or land, or a combination of those.
    - "Return to Home" RTH is the most typical solution used in the industry and simply means that if the GNSS signal is lost and can't be recovered, the drone will automatically reverse (whether this is straight away or after a set amount of time) and go back to the home point where the flight started, or to a pre-determined safe landing point. This will also activate when the battery charge is running low.
    - Paired with the RTH function are the landing protection mechanisms. The drone has sensors and gyros onboard so that it will first hover then find a safe area to land without risking contact with uneven terrain or other objects e.g., rocky terrain or forested areas – or people of course.
- Anti-jamming equipment onboard. There are various solutions to the jamming threat available on the market, providing anti-jamming protection to drones in many scenarios, from low-cost jammers to high-power ground jammers.

WHAT ABOUT DRONES OPERATING IN A GNSS/GPS-DENIED ENVIRONMENT?

Although it is industry standard to use GNSS, many companies are now utilising drones to carry out tasks in GNSS denied environment such as power plants, underground tunnels, or warehouses. These drones are designed specifically for indoor environment and use on-board sensors, camera-based visual situation awareness, to detect their immediate surroundings and avoid collisions while providing reference points. Already we see on the market drones that

combine GNSS-based navigation and enhanced situational awareness based on sensors onboard, for collision avoidance.

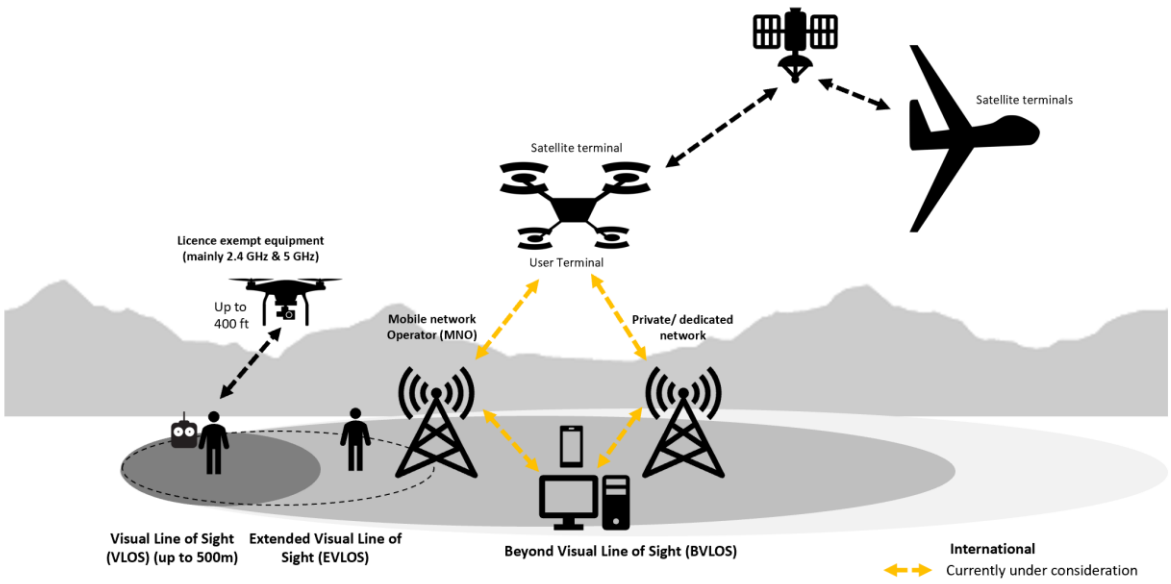
V. SECURITY OF C2 LINK: WHAT IF A DRONE'S COMMAND AND CONTROL C2 COMMUNICATION LINK IS LOST OR JAMMED?

SUMMARY

- Most drones on the market today are operated within close distance of the Remote Pilot, using a direct radio link like model aircrafts for Control and Command. These radio links are vulnerable to interferences, starting with unintentional interferences (terrain, buildings…) and drones have procedures in case of loss of communications link.
- For longer distance drone operations in kilometres, the most appropriate communication links are 4G 5G mobile networks and satellite communications networks. These networks have developed cybersecurity strategies and standards to support multi-billion end-user industries, and drone connectivity will benefit of it. In the UK, OFCOM, the communication regulator, issued in December 2022 its decision to set up a mobile and satellite communications onboard equipment licence for UAS.

WHAT IS A C2 COMMUNICATION LINK?

C2 means "Command and Control" link. It is the communication link between the drone in the air and the Control Unit on the ground that the Remote Pilot uses to control the UAS and give his/her commands to the aircraft.



Source: OFCOM, June 2022

To operate a UAS, a radio link is or will be needed to perform the key C2 functions as well as other tasks, such as:

- Relaying of payload data – for data and video to be sent from the UAS to the remote pilot/operator;
- Electronic Conspicuity – technology to make other airspace users aware of the UAS's location and flight path;
- Detect and Avoid – the capability for the UAS to avoid objects or other aircraft to a level at least equivalent to the 'see and avoid' principle in crewed aviation; and
- Communications, navigation, and surveillance – depending on the airspace in which the UAS is being flown and also on the capability of other systems on the UAS, Air Traffic Controllers may need to maintain oversight and control of the flight.

WHAT KIND OF RADIO LINK IS, OR WILL BE, USED BETWEEN THE DRONE AND THE GROUND?

Today for most drones: a direct radio link, like a model aircraft

Most drones commercially available today use direct radio links, like model aircrafts. Typically, these devices either use the 35 MHz frequency band (designated for airborne model control) or the 2.4 GHz and 5 GHz frequency bands (using Wi-Fi or other low power radio network technologies).

Now and for drone operations with a range in kms: 4G 5G mobile and satellite networks

A direct radio link has its limits, starting with range: 3-5km max for most drones on the market, up to 20km range for higher range system.

Also, the direct radio link can be impacted or lost in case of obstacles, like houses, terrain, or sometimes even trees.

As a result, as the operational range of UAS flights is increasing, a radio link or Wi-Fi link is not suitable and does not provide the necessary coverage.

The two leading solutions that meet the coverage needs of long-distance drone operations are the use of satellite and/or mobile networks.

OFCOM, the UK's communications regulator, has issued its decision in December 2022 to "introduce a new UAS Operator Radio licence to authorise the use of radio equipment on drones. The authorisation of this equipment is an enabler for drones to be operated beyond visual line of sight (BVLOS). The licence authorises a range of equipment that an operator may choose to use or be required to carry by the Civil Aviation Authority (CAA). The UAS Operator Radio licence will:

- Cover all drones a company or individual operates in the UK and territorial waters but does not cover international flights.
- Have an indefinite duration, subject to payment of an annual licence fee of £75.
- Authorise a range of specific radio equipment that may be needed for future drone operations, including beacons and safety equipment that may be mandated by the CAA. The list of equipment will be kept under review and, subject to consultation, will be updated to reflect changes in technology or the overarching air safety framework.
- **Permit the use of satellite and mobile technologies while requiring the specific agreement of the network operator(s).** No transmission will be permitted in the 2.6 GHz band.

This licence does not replace the current licence exemption regime for low power 2.4 GHz and 5 GHz equipment which most drones on the market currently fall under. "

Source: OFCOM "*Spectrum for Unmanned Aircraft Systems (UAS): Approach to authorising the use of radio equipment on UAS*", December 2022.

WHAT IS THE IMPACT IN TERMS OF SECURITY?

Direct radio links like Wi-Fi are vulnerable, they can be impacted by unintentional interferences, such as interference from other signals in the airspace, harsh weather conditions, buildings. They can also be subject to intentional interferences from malicious actors.

4G/5G mobile networks and satellite networks are used in a broad array of end-user industries, including mobile online banking. Of course, both types of networks are prime targets for cybercriminals. However, industries have developed cybersecurity strategies and standards to securely support a large array of multi-billion or trillion client industries, and drone connectivity will benefit from that umbrella.

STILL, WHAT HAPPENS IF A DRONE LOSES ITS C2 LINK?

The loss of a C2 link could result in the pilot no longer being able to manage the aircraft's flight. This is a known vulnerability of current radio links and as such there are methods in place to mitigate and manage the drone in the event this happens, with some examples being:

- Redundancy of communication links
- Fail-safe modes automatically triggered by the loss of C2 signal, without the need for human input. Typically, drones on the market would perform one of three things: return to home (RTH), hover on the spot, or land, or a combination of those.
    - "Return to Home" RTH is the most typical solution used in the industry and simply means that if the C2 link is lost and can't be recovered, the drone will automatically reverse (whether this is straight away or after a set amount of time) and go back to the home point where the flight started, or to a pre-determined safe landing point. This will also activate when the battery charge is running low.
    - Paired with the RTH function are the landing protection mechanisms. The drone has sensors and gyros onboard so that it will first hover then find a safe area to land without risking contact with uneven terrain or other objects e.g., rocky terrain or forested areas – or people of course.
- Anti-jamming equipment onboard.

Ofcom Statement: Spectrum for Unmanned Aircraft Systems (UAS). Ofcom drone statement, December 2022

VI. SECURITY OF C2 LINK: INTERVIEW WITH ANDREW THOMAS, CELLNEX

https://youtu.be/-xhgKu9B9ho

TRANSCRIPT

Anne-Lise: Good morning, Andrew.

Andrew: Good morning, Anne-Lise.

Anne-Lise: Thank you for joining us for this discussion around security matters as part of Project Caelus. First, Andrew, can I ask yourself to introduce yourself and introduce Cellnex?

Andrew: Yeah, my name is Andrew Thomas. I'm the Head of Innovation for Cellnex UK. Cellnex is an infrastructure provider to UKs telecoms industry. If you look around and see a cell tower with antennas on, that is most likely to be provided by Cellnex. So, we provide Network Solutions for the major mobile phone operators. We also provide private networks for use in industry.

Anne-Lise: Currently there are many drones on the market commercially available and they are essentially operated within visual line of sight, meaning that the pilot commands the device using a direct radio link like a model aircraft or maybe a Wi-Fi. But as part of Project Callus, we will be dealing with a completely different type of animal because the idea is to develop a logistics network for the NHS so we are referring to systems that can travel over long distances. So now that I've explained the background to this conversation, Andrew, can you let us know the type of communication link that will be used in Calais between the ground station and the drones?

Andrew: OK, so the drones for Caelus will be flown beyond visual line of sight, which means that you need a controller to manage its flying. Project Callus will be using a mixture of satellite comms, very remote rural locations and we'll be using a 4G LTE network in urban environments that are out and about in city and where there's good mobile phone coverage and we'll also be using a 5G network within the airport when the drone is landed in in a busy, controlled environment.

Anne-Lise: So, you're referring to communications networks that are available for phones, actually. Can you let us know the difference in terms of security and cyber security between a regular direct radio link or Wi-Fi and a communications network?

Andrew: OK, so if we're discussing a 4G communications network, this is the same network that all consumers mobile phones connect to. The network is secured by the communications link between the drone and the ground station which is all encrypted. We provide a SIM card like you do for normal mobile phone to the drone. We know the id of that SIM card and that's how you

guarantee security through the network. I mean 4G LTE is planned to be used by the UK emergency services, so you know, we know it's inherently secure for these sorts of locations and these sorts of applications.

Anne-Lise: So, what you're saying is that with the systems that will be used as part of Caelus, the radio link will benefit from the regular communications networks that are available to smartphones and it's a completely different profile. We hear of people's concerns that the communication link could be hacked or spoofed or jammed or whatever - do you have in hand any form of statistics on that kind of attack on the mobile network?

Andrew: There have been stories about how SIM cards can be hacked. These have only ever happened in very, very controlled conditions in labs. Yes, it is possible using a supercomputer and maybe new generations of computer to decrypt the channel but this isn't something that happens in day-to-day operations, so I'm not aware of any 4G LTE network being hacked. You can't spoof the SIM card. Hacking on mobile phones is more about calling the person up and pretending to be somebody else or having these fraud messages - "Hi Mum, it's me". That's the sort of fraud that happens on mobile phone networks, but directly against the equipment itself is very, very and it's very, very complex, very, very difficult and out of the realms of normal practise.

Anne-Lise: So, you are a regulated industry, you provide communications to millions of people. And as we all know, 3G-4G networks are used around the globe and they benefit from a significant amount of R&D and oversight from regulators. So, I guess it's fair to say that we are on a different planet in terms of security of the communication link between simple direct radio link as it is today in commercially available consumer type of drones and what will be operated as part of Caelus for the long-range travel and operations.

Andrew: Absolutely. The SIM card is encrypted. The whole solution is designed with security in mind. I remember many years ago working in a lab with security agencies, testing the security, doing penetration testing, looking at how these networks worked and for these sorts of applications they are absolutely secure.

Anne-Lise: Andrew, one last question. There will actually be 2 links between the remote control or the ground station and the drones. One will be the 3G-4G-5G networks that you will be providing. The other one is satellite communication using the satellite networks as it exists today, I know that you are not into satellite comms networks, but would you concur that we are also on a different planet in terms of security level for regular sat comms versus a direct radio link as is commercially available on consumer drones?

Andrew: Absolutely. So, drones are used in for information gathering. the US military uses them to fly, and they're flown basically with sat-coms communication. So absolutely, again, it's very secure. There are known ground stations, they're secure. The equipment on the device is provided by, you know, a secure organisation. I don't know a huge amount about sat coms, but absolutely right, it's the same principles that it's regulated, the ground stations where the information receives from the satellite is secure. So again, it's a completely different level of security from a normal communication between a drone controller and a drone.

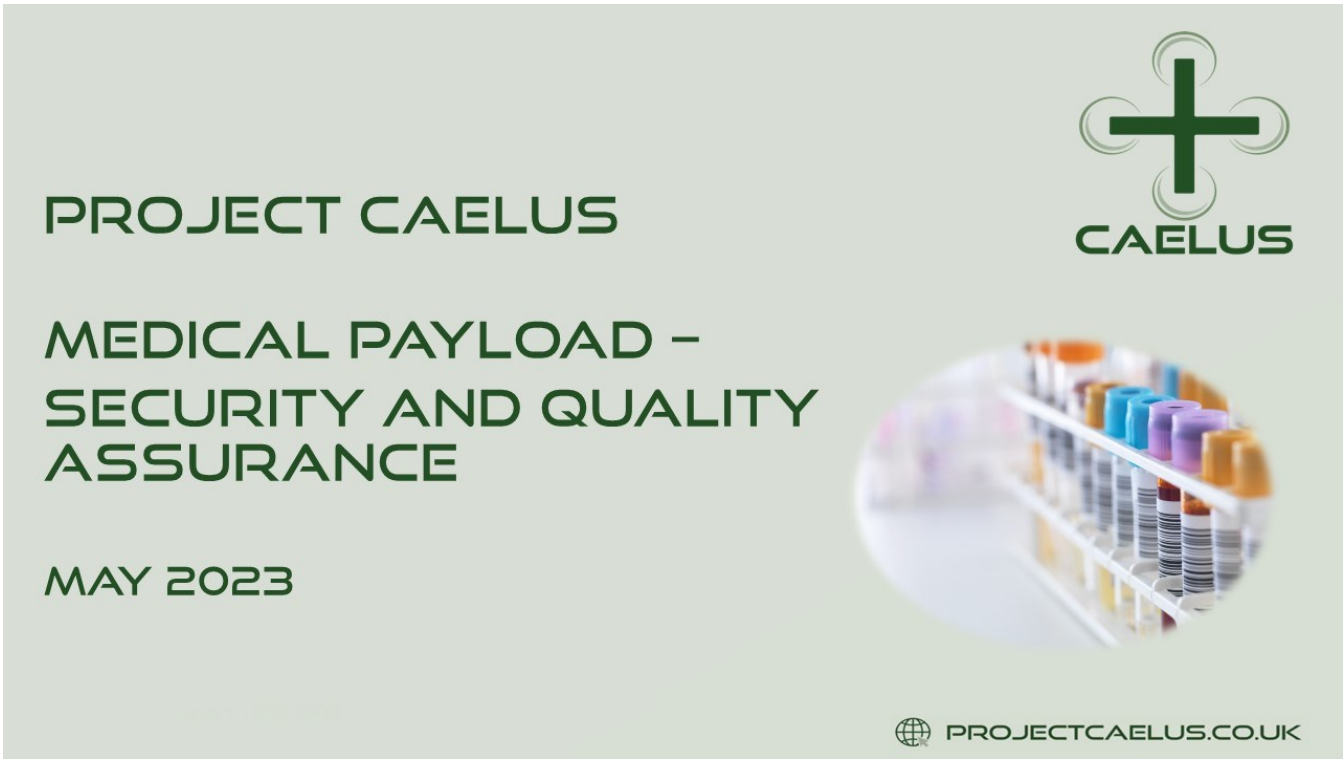
Anne-Lise: All right. OK. Thank you very much, Andrew.

Andrew: No problems at all.

VII. MEDICAL PAYLOAD QUALITY ASSURANCE: INTERVIEW WITH RICHARD MERCHANT, DGP INTELSIUS

HTTPS://YOUTU.BE/OCX7ZXUB3NS

SLIDEDECK



ABOUT DGP INTELSIUS

CAELUS

25 YEARS EXPERIENCE
In the design, supply and manufacture of market leading sample transport and temperature-controlled solutions

TEMPERATURE CONTROLLED PACKAGING (TCP)
Solutions designed to keep the contents (payload) within a specific temperature range

SAMPLE TRANSPORT PACKAGING (STP)
Solutions designed to safely and compliantly transport patient samples for analysis

BEST IN CLASS SERVICES
Technical, design and fulfilment services alongside ongoing customer support

INTELSIUS™ A DGP COMPANY

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 2

ABOUT THE DRONE OFFICE

CAELUS

Drones in Medical Logistics - White Paper

Inter-medical sites drone delivery - Standard OperatingProcedures

Model CAA Ops Manual Chapter for Medical dangerous goods transport by drone

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 3

INTRODUCTION

Logistics by drone will be another form of transport, and like any other mode of transport, it will comply with the regulations and best practices applicable in healthcare.

We should even strive to improve compliance and quality assurance with technology.

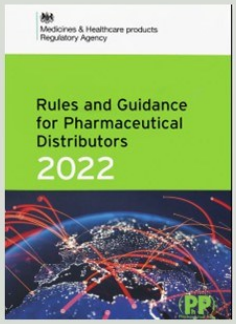
The following pages provide an overview of the key regulations identified, how, to the best of our knowledge, they would apply to drone logistics, and how we are addressing medical payload security and quality assurance.

Engagement and feedback welcome!

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 4

RULES FOR THE TRANSPORT AND DISTRIBUTION OF MEDICINES AND MEDICAL PRODUCTS



The **Good Distribution Practices**, or **GDP**, is a Code of Standards to ensure that security , quality and efficacy of medicines is maintained in transit to patients.

In the United Kingdom, the **Medicines and Healthcare Products Regulatory Agency**, the **MHRA**, is the executive agency of the Department of Health and Social Care, or DHSC, responsible for ensuring that medicines and medical devices work and are acceptably safe.

The MHRA implements those guidelines through its **publications** the "**Orange Book**" and the "**Green Book**".

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 5

KEY REQUIREMENTS IN THE GOOD DISTRIBUTION PRACTICES, OR "GDP"

CAELUS

Regardless of the mode of transport, it should be possible to demonstrate that the medicines have not been exposed to conditions that may compromise their quality and integrity.

- Personnel training on GDP requirements
- Documentation as part of quality system
- GDP applicable to outsourced activities
- Containers, packaging, labelling
- Positive identification of Receiver - Chain of control
- Traceability
- Anti-tampering, prevention of falsified medicines introduction
- Temperature monitoring
- Suitability of Vehicle and Container

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 6

DANGEROUS GOODS

CAELUS

Dangerous Goods are **materials identified and classified as hazardous within the UN model regulations.**

Several transported goods across hospitals are classified as Dangerous Goods.

The risk is not necessarily to the patient, but to handlers, the public and/or the environment.

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 7

EXAMPLES OF DANGEROUS GOODS

Toxic Substances Class 6.1, such as **cytotoxic medicines for cancer treatment. UN1851** Medicines, liquid, toxic, n.o.s. **UN3249** Medicines, solid, toxic, n.o.s.

Infectious Substance Class 6.2, **materials expected to contain pathogens**. Category A **UN2900** and **UN2814** Infectious Substances, or Category B **UN3373** Biological Substances, such as **blood samples for analysis.**

Lithium-ion batteries packed with equipment **UN3481** or **Lithium-metal** batteries with equipment **UN3091** such as defibrillators

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 8

RULES FOR THE TRANSPORT BY AIR OF DANGEROUS GOODS "DGR"

The transport of Dangerous Goods is **regulated on a global basis**.

The UN model regulations are used by the **International Civil Aviation Organization** ICAO to develop their "Technical Instructions for the Safe Transport of Dangerous Goods by Air".

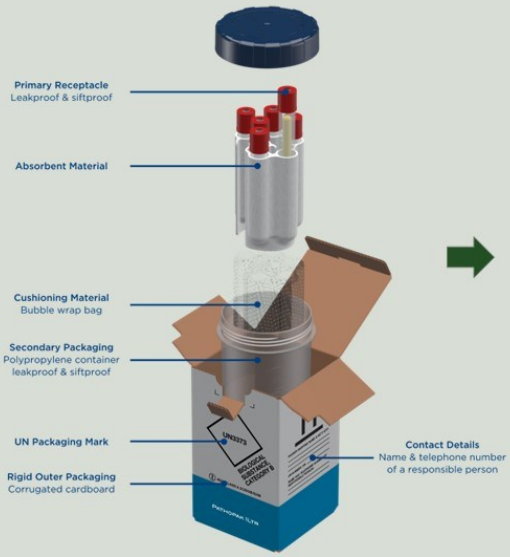
The International Air Transport Association IATA Dangerous Goods regulations contains the ICAO TI + additional requirements. That book is called the DGR.

Transporting Dangerous Goods by air requires a specific approval by the UK Civil Aviation Authority, the CAA.

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 9

KEY REQUIREMENTS WHEN TRANSPORTING DANGEROUS GOODS



- Marks, labels recognizable by the public
- UN specification packaging that can contain any leaks in case of fall or accident
- Personnel training on the DGR, handling requirements, recognition of non-declared DG
- Acceptance checklist, loading and offloading procedures
- Inspection of package
- Written documentation
- Procedure for emergency situations
- DG Standard Operating Procedures

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 10

HOW WILL CAELUS ADDRESS MEDICAL PAYLOAD SECURITY SPECIFICS?

Consortium partners DGP Intelsius will develop a **temperature controlled packaging solution capable of transporting medicines, blood samples and other treatments**:

- Real time data logging to access temperature information during transit.
- Insulated locking case that is unlocked remotely or through online application to ensure auditable chain of custody.
- Temperature control for 2 to 8°C, 15 to 25°C and -25 to -15°C temperature ranges.
- Online portal to track shipments and access temperature reporting.

Disclaimer: this overview is correct to the best of our knowledge. If you identify inaccuracies or would like to comment, please email us at: hello@projectcaelus.uk

p. 11

Other key regulations / Best Practices we should consider?

Key Concerns we should specifically address?

Any questions, recommendations?

www.caelus.commonplace.is

12

TRANSCRIPT

Anne-Lise: Welcome everyone and thanks for joining this discussion on medical payload, security, and Quality assurance as part of Project Caelus. Just to remind everybody, Project CAELUS is a research project part funded by Innovate UK. CAELUS stands for Care and Equity, Logistics, UAS, Scotland and the aim of our research project is to investigate and demonstrate the benefits and the challenges of implementing a logistics network, using aerial drones, for the NHS and more broadly for the healthcare services.

As part of our research programme, we have had some discussions with medical teams as well as some surveys of the general public in terms of the key benefits and concerns that they have. One of the concerns is about the medical payload. How do we know that the medicine transported by drone will be fit for purpose at the receiving end? How do we know that the medicine received is the one that was meant to be booked? How do we know that the payload has not been tampered with in between? So, in this interview we will try and answer some of these questions together with Richard.

First, Richard, can you tell us a bit more about Intelsius and yourself?

Richard: I can, yes. Thanks for inviting me along today. I'm Richard Merchant. I'm the product development and engineering manager at Intelsius. Intelsius is a healthcare packaging company supplying life sciences and particularly the distribution of pathology samples as well as finished and investigative medicinal products. Intelsius have been around for 25 years and started in the BSE crisis in 1998 and we've built globally over that time to develop a portfolio of sample transport packaging covering class 6.2 dangerous goods along with temperature control packaging for medicines basically. We're based in the UK as our headquarters as well as having global sites across US, India, Ireland, Germany, and Malaysia.

Anne-Lise: Good. Thank you, Richard. And let me introduce you to The Drone Office. My name is Anne-Lise Scaillierez, I'm a partner at The Drone Office. I started investigating the requirements of transporting medical products by drones back in 2019 with an international pathology lab company. We continued working on that topic as part of other research projects funded by Innovate UK. First with AiResponse, where we developed standard operating procedures for inter-medical sites drone delivery. The second project was INMED where we looked into further details on the requirements to get approval from the authorities to transport dangerous goods by drones.

As a way of introduction to this discussion, maybe we can share the philosophy that is driving us. In a sense, we consider that logistics by drone will be a form of transport like any other form of transport. And as a result, it will comply with all the regulations and best practises that are currently applicable in healthcare and healthcare logistics. And we would even say that we should strive to improve compliance and improve quality assurance with the use of new technologies.

So, with Richard in the next 10 minutes and going through the next slides, we will provide an overview of the key regulations identified for drone logistics and we will share with you the best of our knowledge in terms of how we can respond to those requirements using drones. Now

obviously this is a field of innovation, so engagement and feedback is very much welcome. You can respond or post comments on the commonplace platform. You can also use the e-mail address hello@projectcaelus.uk to offer comments or feedback.

So, Richard, can you walk us through the rules that apply to the transport and distribution of medicines?

Richard: Yes, so, to make sure that the efficacy of a drug is still maintained throughout any distribution network, we've got to monitor that payload. And the reason why we monitor that payload is that we need to report to people like the Medicines Healthcare Products Regulatory Agency or the MHRA about how the materials have been moved about within any sort of network. So that could be from distribution hub to dispensing pharmacy, or that could be anywhere within the logistics network. There's a set of rules: irrespective of the mode of transport, we are able to demonstrate that the medicines haven't been exposed to conditions which are outside of the requirements of the drugs, we've got to make sure that the products integrity is maintained throughout.

We can do that in numerous ways but usually that's making sure that we've got a qualified packaging system, making sure that we're monitoring internal external temperatures as well as tracing those shipments, making sure nobody's interfered with it and making sure that there's a series of SOPs or operations manual which people are following to ensure that each shipment is done correctly.

Anne-Lise: OK, so that was for medicines and maybe now I will mention the notion of dangerous goods and how it applies in the context of logistics for the healthcare system. So first, what is dangerous goods? Dangerous goods are materials that are identified as such under the UN model regulations. The UN (United Nations) have issued model regulations back in the 1950s and they have identified and classified all the different materials that could present a danger. The danger here is not so much in reference to the patient, but more in reference to the handlers, the public or the environment. What if that substance is exposed for example to the handlers? Or exposing the public in case of a, I don't know, in case of a crash for example.

So, if we look at the different dangerous goods that could be transported for applications in the healthcare industry, there are maybe three main categories.

The first one would be the toxic substances class 6.1, because the number of medicines, whether they are liquid or toxic, could be classified as the two numbers UN1851 or UN3249. This for example would apply to some cytotoxic medicines for cancer treatment. Another bucket of dangerous goods that we can see in user cases in the medical environment are classified as infectious Substance class 6.2. This would be blood samples for example, because unless and until they are tested, we don't know whether there could be a pathology within the blood sample. Therefore, if in doubt they are classified as dangerous goods. The third bucket of dangerous goods that could be transported are the lithium batteries. We all know that we have lithium batteries pretty much everywhere in our lives - smartphones, PCs, but also in medical equipment starting with defibrillators. Therefore, it's one of the key categories that we have to consider when we look at the types of dangerous goods that could be part of medical payload using drones.

Now that we've described what could be the dangerous goods on board the drones, the regulations applicable: they are what we call the DGR standing for the Dangerous Goods Regulations. They are a set of rules developed by IATA, which is the International Association of Transport Operators. So crewed aviation, manned aviation. They've been developed over

decades, and they would apply, the general philosophy would apply in the same manner to drones being transported by air. It's important to note that transporting dangerous goods by air is subject to a specific approval by the aviation authorities in the UK. That authority is called the CAA.

Now Richard, can you walk us through how you address those requirements starting with the dangerous goods for example,

Richard: Yes, so for pathology samples we're looking at class 6.2 and the packaging that's involved there. It follows a very basic sort of three-layer packaging principle. So, our primary or first layer of packaging is the receptacle, so our tube, our 30-mil universal gets packed into what's known as a secondary. So, in this instance here that's our patho pack one litre bottle and that bottle needs to be sort of leak proof as well as make sure that we can withstand pressure differentials and then external packaging. This is our third layer and that needs to have relevant information printed on it.

This is a category A box so on there we have a UN number printed. We also have the relevant markings and labelling for the system and then also people like responsible persons, contact details, recipient, sender as well as a list of contents that needs to be included there. Under IATA Packaging systems for UN3373 need to undergo drop testing from 1.2 metres and packaging for class or category A materials, they're dropped from 9 metres as well as undertaking some stack and puncture testing. So that's sort of our packaging for pathology samples, similarly for packaging for the device that's containing batteries they'll need to go through their testing, as well as those for class 6.1 toxic materials, but all in a similar manner.

OK, so I guess the final question is how's CAELUS is going to meet all of these requirements which we've spoken about. First and foremost, we want to make sure that this packaging is secure and so we've got a locking device within the packaging. We also want to make sure that the temperatures within there are being monitored. We've got some onboard temperature monitoring capabilities. So that will take an internal temperature as well as an external temperature. So, we'll now know how the external temperature affects the insides of the packaging and the payload temperatures. We'll also have different ways of making sure that the product payload is kept at the correct temperatures, so different medicines and different blood products need to be maintained at different temperatures. So, 2 to 8, 15 to 25 and minus 25 to minus 15. We've got all the coolants and the necessary materials and knowledge to make sure that that's maintained as well as making sure that that box is insulated because what we don't want to do is let the external temperature affect the internal temperature of the packaging.

Then finally we've spoken about the temperature and all the rest of it – what we want to do is make sure that this is sort of future facing with the technology and the devices transmitting the information wirelessly. You'll have a tracking portal where you can actually see what the temperature is on board the drone whilst in flight as well as then generate the relevant quality reports that come out at the end of it for auditing and to make sure that the people that were mentioned at the start of the presentation, the MHRA, are happy with how we are moving materials in our drone network.

Anne-Lise: Thanks, Richard. Brilliant. You know, it's a really good to have that comprehensive overview of the requirements that will be applicable to the transporting of medicines and medical payload by drones.

Watch our discussion on medical payload and quality assurance with Richard Merchant at DGP Intelsius

Logistics by drone will be a form of transport like any other form of transport. In our discussion, we will share our understanding of regulations and best practices that would apply to the transport of medicines and medical products. We focus in particular on Good Distribution Practices, and the safe transport of dangerous goods by air. Richard walks us through the packaging solutions to meet those requirements.

https://youtu.be/OCx7zxub3Ns

By Robert Burns and Anne-Lise Scaillierez.


THEDRONEOFFICE