SECMAR

Secure digitalisation for sustainable maritime transport

Cyber – physical security in Drone Management

Program: Interreg South Baltic

Project goal: To develop and launch a cross-border digital innovation hub for enabling business development and innovation in the field of maritime informatics and cyber security

Work Package: 6
WP Leader: PP4 Blekinge Institute of Technology

Authors:

Lawrence Henesey, Ph.D.	Phone+46 454 38 5902
Department/Unit: Department of Computer Science	Email **larry.henesey@bth.se**
Title: Universitetslektor	
Alexandr Silonosov	Phone+46 **455 38 5855**
Department/Unit: Department of Computer Science	**Email aiv@bth.se**
Title: Projektassistent	
Maryam Rezaei	Phone+46732099195
Department/Unit: Department of Computer Science	**Email maryam.rezaei@bth.se**
Title: Projektassistent	

Address
Blekinge Institute of Technology / Blekinge Tekniska Högskola,
Biblioteksgatan 4, S-37440, Karlshamn, Sweden

Version: v.1

Date: December 04, 2021

Submission Date: December 30, 2021

Other Attachments:

1.Drone market review.
2. 2021-08-15_SECMAR_BTH_Final Results. Drone Automation testbed

"The contents of this paper are the sole responsibility of the author[s] and can in no way be taken to reflect the views of the European Union, the Managing Authority or the Joint Secretariat of the Interreg South Baltic Programme 2014-2020 "

Document status		Document confidentiality	
X	working document		WP and task leaders
	to be reviewed	X	internal use only (direct partners only), distribution RESTRICTED
	proposal		entire project partnership (direct + associated partners)
	final		target groups (key target – 200 SMEs from the blue and green targeted sectors)
	released		public in large, public distribution

Table of Contents

List of Figures

List of Tables

Abstract

The emergence of unmanned aerial vehicles (also referred to as drones) has transformed the digital landscape of surveillance and environmental monitoring, especially in cargo terminals where such was previously accomplished with static video monitoring systems. Moreover, the adoption of autonomous drones flights has further led to the diverse of IoT systems interconnectivity, which has introduced many cyber security concerns. Drone management is concrete and a conceptual platform where key players in the digital transformation and society join in a conversation about the role and impact of autonomous systems and machine learning.

Drone solutions provide an easy-to-use programmable drone testbed to experiment with novel drone applications and explore cybersecurity-related use cases. High-resolution & high-zoom thermal and optical imagery allows for confident decision-making.

This research has been conducted to set up a testbed for autonomous flights, collect data and test the level of cyber-physical security during drone's autonomous flights.

Acknowledgment

This report in hand stands for a compilation of data, its analysis, gradual update, and finalization in the frame of the SECMAR – Secure Digitalisation for Sustainable Maritime Transport, part-financed by the programme from the European Regional Development Fund (EDRF). Agreement on the Technical Assistance project STHB.06.01.00-22-0002/16

Representing the project partner PP4 – Blekinge Institute of Technology, herewith we would like to express gratitude to the partners, industry experts and various company representatives for their contribution in the frame of provided information

The contents of this paper are the sole responsibility of the author[s] and can in no way be taken to reflect the views of the European Union, the Managing Authority, or the Joint Secretariat of the Interreg South Baltic Programme 2014-2020.

1. Introduction

As part of the SECMAR Project, a pilot was introduced in which the proposal was to investigate on how Drones and Drone management could be employed in improving Maritime Cyber Security with an emphasis to the South Baltic region. Several contacts were made and discussions with a port in Sweden led to using the Port of Ystad as a test site. As there has been several delays in acquiring the equipment and software due to mostly the effects of Covid-19 this proposal had to be reevaluated. The reevaluated proposal has been on assessing the technologies and tools for conducting such a pilot in which Drones would be employed. For example, we have evaluated the choice of technology from Drone industry, the challenges in conducting such experiments when working in pilot projects, and identifying case studies that would be the most interesting for the field. Finally, a survey of the “state of the art” was performed to update our understanding of what is available in the market and research published in this new and exciting area. In the scientific literature, drones, usually referred to as UAVs (Unmanned Aerial Vehicles) [1], are getting more common, bringing positive and negative effects. The possibilities with UAVs expand for an array of different uses and industries as other technologies develop. However, the explosive increase in production to meet the rising demand has allowed various security weaknesses/vulnerabilities to enter their systems[2].

Drone solutions are popular these days as the eye in the sky from the security providers To provide Intelligent flight automation, collect, analyze and share data in real-time. We can see a significant increase in using drones for industrial goals as automation or compliance use cases.

Area inspection (like fences damages, water pollutions, quay fenders), video surveillance, object detection, accounting, and maps update are some of the critical use cases in port digitalization by applying drone solutions.

Drone route mission control by SaaS is autonomous and easy to operate. It has the pre-planned routes and starts the flight by pressing the fly button simply.

There are more capabilities in Enterprise drones in comparison with consumer's drones such as:

- More qualifications: load weight (8kg), flight time (1h), distance
- Camera with thermal sensor, infrared
- On-board API: Edge-computing, extra control over the drone.
- Add-ons: Beacon, Speaker, Spotlight
- More security features: encryption, password protection

2. Scope and problem statement

Digital workplace emergence increases the feature of applied technologies. There is a need to identify the best features and levels and use them efficiently to reach the project goal. Recently, drone solutions have become a commercially available technology, affordable to the wider public. Many research projects have already investigated their use in swarms and collaboration with other autonomously operating cyber-physical systems [3][4][5] and studies [6].

Classical real-time video surveillance systems (CCTV) cannot entirely meet todays' requirements in complex industrial environments such as Ports: Changing infrastructure with dynamic surveillance targets, more sophisticated monitoring is needed to identify air quality, pollutions, monitor water area and to inspect of conditions (damages) of port infrastructure, assets, and terminal yard sites.

This project investigates the cyber security challenges with Drones / IoT nowadays in the maritime industry. Regarding these challenges, some questions can be raised.

- Do we ready for valid autonomous flights?
- Required security vs. advertised security
- Do we control data privacy?
- Do we understand lifecycle (inventory, updates, disposal)?
- Do we have an incident response plan?

The Following features were identified while studying Drone Automation solutions with use cases in maritime industry:

- Ability to organize a protected and secured parking slot with drone charging ability;
- Drone precision landing on a charging pad;
- Ability to manage drones and flight routes via online dashboard by using a class of solutions: Drone management as a Service;
- Ability to periodically deliver aerial images of a specific trail in industrial territory to recognize and detect a specific event, misbehavior, or pattern.

3. Project Goals:

The target area of this project is considering possible drone use cases in ports. As the first use case, we can mention Area Inspections such as fences damages, water pollutions, quay fenders. The second drone use case in a port can be Video Surveillance, and the third one is Digitalization in terms of object detection and accounting or maps updating. Drone automated charging, Drone-In-a-Box – docking stations, and Drone route mission control by SaaS are good practices to evaluate the proposed drone automation solutions.
The significant goals of the project are considered as the following list:

- Understanding elements of drone automation system
- Share compliance and regulations impacts
- Perform threat modeling exercise
- Understand cyber-security defense level and required security controls
- Share security requirements awareness

The experimental setup of this project is testing the level of cyber-physical security during drone's autonomous flights with a dynamically created flight path over a quay area using predefined flight routes. The goals will help to understand:

- Secure communication with control center

- Secure delivery of flight path.
- Aerial photos and video privacy
- System capabilities for drone self-return and landing in case of miss-configured flight path or missed connection with control center.

4. UAV Operation

To describe how drone management can provide cyber and physical security in the maritime industry in the context of state of the art, we aimed to explore and analyze the current process, practices, and use cases in other industries. In this section, the literature relevant to drones in the industry environment from various areas have been reviewed to find the different capabilities of drones.

Operating UAVs poses several challenges, such as testing and simulating swarms of UAVs and training operators, which generally require expensive simulators [7] because the conditions under which UAVs operate are different from conventional piloted aircraft [8]. However, the environment in which UAVs operate poses a concern, independent of the environment; a traffic management approach is required for operating many devices in an airspace.
Furthermore, there are other concerns regarding the operation of these devices such as security and privacy[9].

4.1 Environmental challenges

Weather conditions such as rain, wind, humidity and terrain characteristics raises some environmental challenges. [10].
Experiments have shown [11] that the power consumption may depend significantly more on environmental conditions such as side winds [7]. Using multiple UAVs in unknown scenarios requires fast and adaptive path planning to avoid collisions and ensure optimal travel times for the devices. A self-adapting multi-object evolution algorithm is proposed to facilitate UAV path planning [12]. Simultaneous localization and mapping-based real-time tracking can be used when GPS signals cannot be used reliably or are unavailable[13]. Generally speaking, the choice of device and hardware will be influenced by the environment the device is intended to operate in. The more specialized an application is, the operational requirements regarding the environment, and it is essential to define the specifications of environmental conditions in the first step.

4.2 UAV Traffic Management

In order to managing the airspace when large numbers of UAVs are operating in the same theatre, ref [14] investigates platooning for UAV swarms and proposes an approach that can handle massive fleets and manages device malfunctioning or intrusion well. In [15], multiple device types addressing the Travelling Salesman Problem (TSP) in the context of measuring/surveilling an area are considered. Suppose UAVs are to be allowed to operate within urban areas. In that case, for handling the increasing traffic in an airspace there is a need to use a cloud-based system for city-wide unmanned air traffic management, for collision avoidance are proposed in [16].

4.3 Compliance Issues

Drone's use and availability is spreading considerably faster than awareness about potential concerns or legislative frameworks to address these concerns[17]. Shortly different countries will probably continue to impose additional regulations regarding the use of UAVs [18], [9], and those regulations may be subject to frequent change. The use of UAVs in public airspace causes several technical and societal concerns and challenges[19]. Currently, there are few certainties regarding the legal regulations for drones since, as is frequently the case with new technologies. Their rapid adoption outpaces legal, policy, and social ability to cope with issues regarding privacy and interference with well-established commercial air space[20]. It should be noted, though, that different regulations may apply to the usage of UAVs for emergency or disaster scenarios [18]. [21] is provided a survey to investigate security, privacy, and safety aspects associated with the use of civilian drones in the national airspace.

4.4 Privacy and Data Security

The increasing number of devices in operation poses threats to people, property, and privacy rights [21]. In [17], the authors analyze the risk drones can pose for privacy and data protection and [19] surveys aspects of cybersecurity, privacy, and public safety in the context of drones in future smart cities. In [22], the use of UAVs to augment the sensing capability of a smart city is proposed. Still, the authors suggest a data broker to provide a secure communication to share the data across the subscribers and smart objects[23] but as mentioned above, the legal situation is currently changing quickly.

5 Market review

As a part of this work, we have investigated the different capabilities of drones in the maritime industry and how they help provide cyber security. We have collected the prominent use cases of drones, and the elements have been offered or produced by various companies worldwide. The scope is industrial use cases based on some search phrases:

- Intelligent drone solutions
- Enterprise drone solutions
- Drone automation solutions
- Drone-in-a-box solutions
- Drone cyber security

5.1 Different use cases

We are influenced by attending the webinars, such as Lorenz drones, to identify the practical use cases improving cyber security strength. Here is the list of possible capabilities and features of drone technologies in the conducted market review:

- Inspecting the quay walls and the sea defense revetments at the port.
- Survey: Drones acquired the data and used it in conjunction with previously-collected bathymetric data. It offers a holistic view of the condition of the port – both above and below the waterline. As an example, maybe the port's construction was completed some years ago and there have been maybe noticeable changes in the condition of some of the assets.
- Autonomously monitoring, inspection, data collection and analysis, emergency responses, remote assistance.
- Drone management and automation

5.2 Drone solutions comparison matrix

During the market review we have identified the state-of-the-art business solutions and necessary element of drone automation system which are: Drone, Remote control device, Appliance or software, Web service and automated Charging technology. The most latest products marketed as "Drone in a Box solutions" contains all these elements. During the review we have identified three groups of vendors. Group 1 focus on automated charging solutions only. Vendors from group 2 focus on drone management as a service type of products that is usually offered as a web site and software for smartphone or computer available by subscription. Vendors from group number 3 produces drones itself, remote control device with software. Table 1 indicates the results of market review and availability of mentioned elements have been offered or produced by a variety of vendors.

Manufacturer Name	Drone	Remote control	Appliance	Web service	Charger
Lorenz			✓	✓	
Terra Drone		✓	✓	✓(cloud-based 3D-model)	
Action Drone	✓	✓			
Airoboticsdrones	✓	✓	✓	✓	✓
Dronesolutionservices				✓	
Azure Drones	✓	✓	✓	✓	✓
Measure			✓	✓	
Drone Base			✓	✓	

PERCEPTO	✓	✓	✓	✓	✓
DCI Drones	✓	✓			
Planck Aerosystems		✓	✓	✓	
inspired flight	✓				
Flyability	✓	✓ Elios Controller MSDS, Ground Control System(GSC)	✓	Cockpit App	
Voliro	✓	✓			
Skydio	✓	✓			
IDiployer					✓
Hextronics					✓
Shenzhen Heisha Technology					✓
DJI	✓	✓	✓	✓	
Skycharge					✓
FlytNow			✓	✓	

Table 1: Market analisys. (Source; Results – Drone market review, 2021)

The results obtained from market review provided understanding of what are necessary elements and building blocks of drone automation system.

6 Drone automation testbed

The experimental setup of this project is testing the level of cyber-physical security during drone's autonomous flights with a dynamically created flight path over a port terminal and quay area. Figure 1 represents an experimental layout for drone automation system with the port terminal, the layout includes drone, automated charge station, and flight routes provided by drone management service.

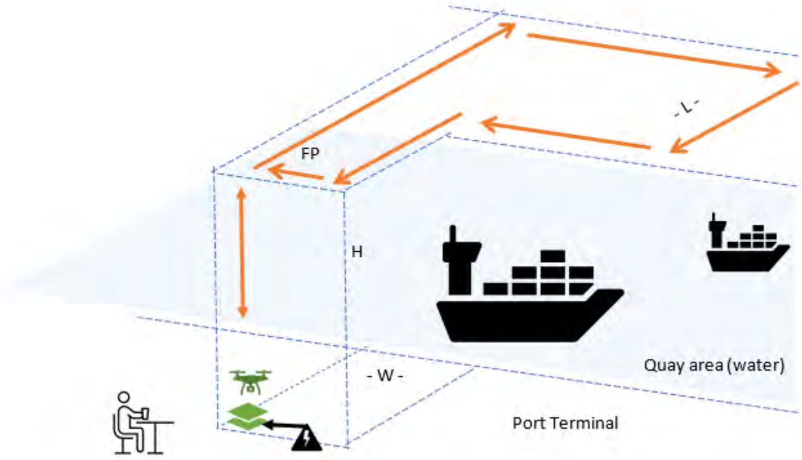


Figure 1: Drone flights testbed in Port quay area. H, W, L – height, width, and length of flight path (FP). (Source: Final Results – Drone Automation Testbed, 2021)

The pilot project conducted with the participation of multiple vendors yielded many results and contributed to the generation of knowledge and sharing regarding to improved digitalization operations by incorporating prototyping approach. Using the results of market review, we have identified essential elements of any drone automation system which includes: automated charging, on-board control appliance, and web-based service of SaaS type that serves as data storage, aerial images processing unit and flight route management for operator. Figure 2 demonstrates the architecture and main elements of proposed automation system as follows: drone landing plate with integrated charger (L), drone appliance (A) that controls drone by using native remote control hardware module (RC), Drone fleet management web service (M) that store, process, and display results of drone operations and captured data via web site.

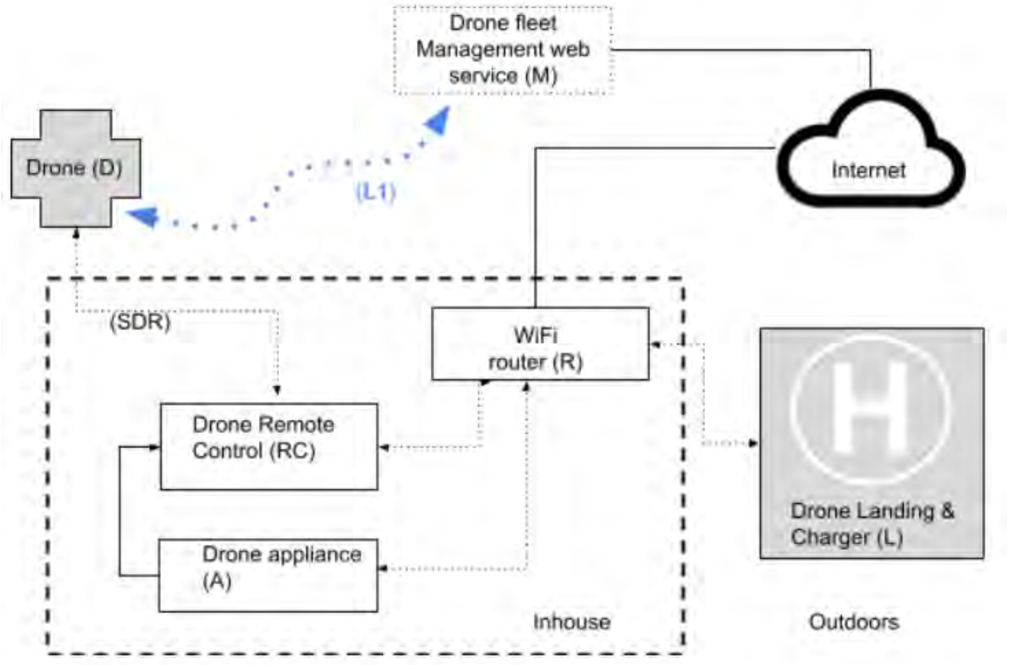

Drone fleet Management web service (M)
Drone (D)
(L1)
Internet
(SDR)
WiFi router (R)
Drone Remote Control (RC)
Drone appliance (A)
Drone Landing & Charger (L)
Inhouse
Outdoors

Figure 2: Drone testbed architecture (Source: Final Results – Drone Automation Testbed, 2021)

Usually Appliance (A) presented by smartphone device (Google or iOS) with specially designed software program provided by web service vendor.

The principle of drone automation is provided with the following steps: Drone start to charge the battery as soon as it lands on landing plate (L), appliance (A) periodically check on the drone's charge level and retrieve flight tasks from the web service (M). The operator can check for the drone's status, create new flight tasks, observe for new aerial images or supervise live video stream from the drone camera by using web interface of web service (M) in any web browser application. As the new information about drone tasks is delivered to appliance (A) it instructs remote control (RC) and Drone (D) to perform take-off and perform the flight according to the route retrieved from web service (M). Remote Control (RC) have a direct, real-time communication with the drone by using Software Defined Radio (SDR) wireless communication technology. The purpose of the drone appliance is to support logical communication channel (L1) between drone and web service and thus operator and business users. The proposed architecture presented on Figure 1 highlights that some of the components resides within the port physical facilities i.e., inside the building (inhouse) and connected via regular networking equipment such as WIFI router (R) that is in turn connected to internet. The Charge station (L) is situated outside the building and connected to the inhouse network by using WIFI router (R) or regular, wired LAN router. The experimental setup of this project is testing the level of cyber-physical security during drone's autonomous flights.

6.1 Cyber-security threat analysis

To ensure proper cyber security level during drone automation project development and lifecycle, alongside conducting risk management, one of the first steps should be Threat Modeling.

Threat modeling is the process that improves software and system security by identifying and rating the potential threats and vulnerabilities that various components of your system may have. The main purpose is to fix security issues before cyber-criminals take advantage of them. The process is then followed by defining countermeasures which will prevent those same threats and exploits likely to put your system at risk. This allows to address threats with the appropriate solutions in a logical order, starting with the ones which present the greatest risk. It is important to start this process on early stages of project development lifecycle to avoid significant changes in the system after potential threats or weaknesses will be identified while understanding and refining system architecture.

In the following sub-chapters, we will analyze all three components of the testbed with the purpose to identify all assets in the proposed architecture, make decomposition of software components, identify data flow and entry points, highlight trust boundaries and possible privileged modes. At the end of the chapter threat modelling table will be presented.

Drone and systems provided by manufacturer

Most of the drone manufacturers maintains the registry of produced drones. This registry includes ownership information and software status of the drone. Drone vendor (DJI) provides software program to register and activate the drone before the first-time usage. The activation procedure includes to create password account that is used to store information about the drone on vendor web service.

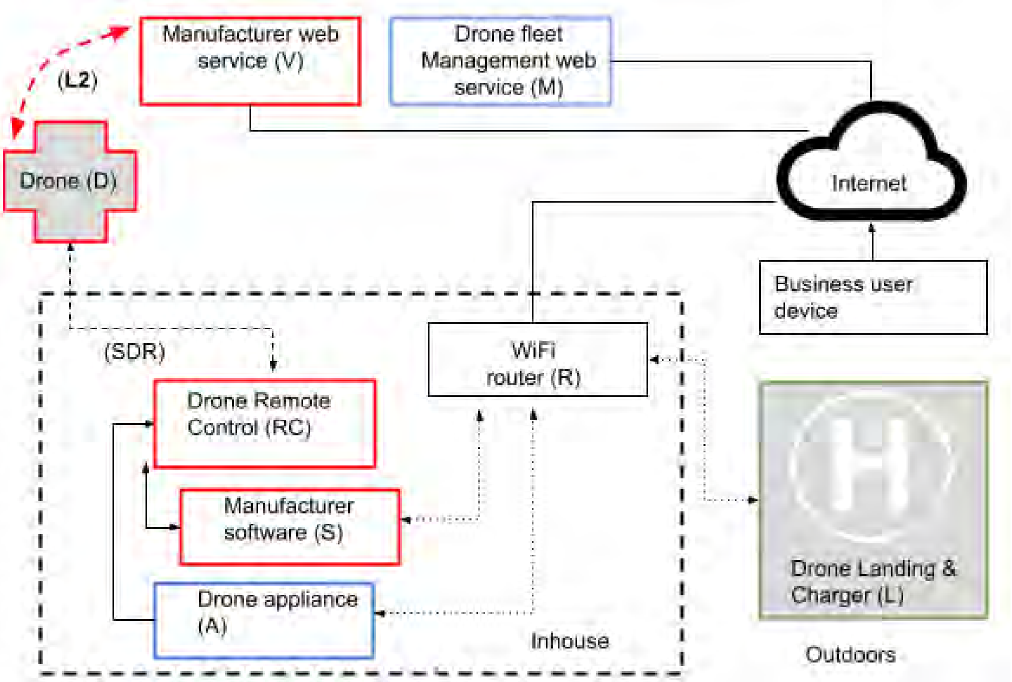
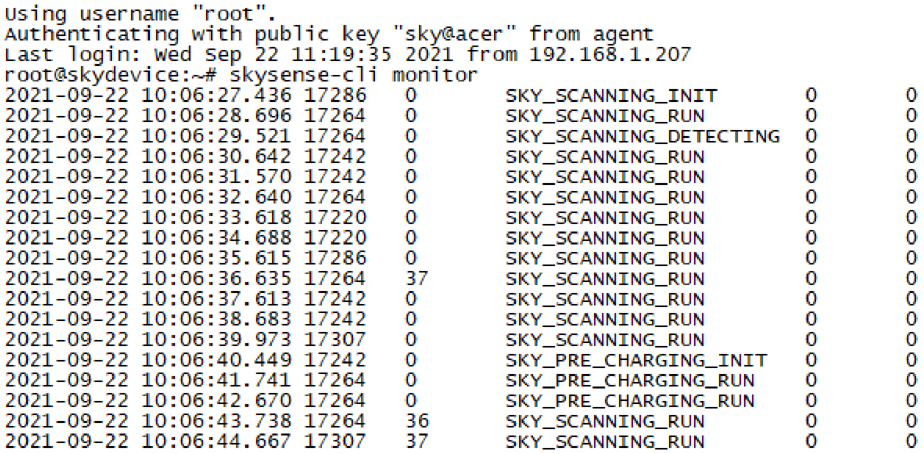

Manufacturer web service (V)
Drone fleet Management web service (M)
(L2)
Drone (D)
Internet
Business user device
(SDR)
WiFi router (R)
Drone Remote Control (RC)
Manufacturer software (S)
Drone appliance (A)
Inhouse
Drone Landing & Charger (L)
Outdoors

Figure 3: Additional elements provided by Drone vendor . Red, Blue, Green color: components of the same vendor. (Source: Final Results – Drone Automation Testbed, 2021)

Figure 3 shows in red color the elements that belongs to the same drone manufacturer that also needs to be used and configured to setup and use automated operations. Web service (V) and software (S) provided by drone manufacture are new elements added the initial architecture in Figure 1. These new elements also should be considered in cyber security risk assessment. Security assessment of DJI drones software available in the internet [24] (https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html, https://www.auvsi.org/sites/default/files/DHS%20report.pdf) shows that there a number of concern and finding was made regards the DJI vendor that may pose a certain threat to the system like: confidentiality loss and control take over.

Outdoor charging pad

The charging pad is an IoT device with the Linux based system installed inside and software program that control the following charging procedures: detect the time moment when drone contact with the charging plate, turn on charging voltage element, control charging process and provide API for the external requests. The API for external request includes REST API and provided by internal web service application. Figure 4 demonstrate that root privileges is provided to the system user to monitor charging status with the ‘skysense-cli’ software.

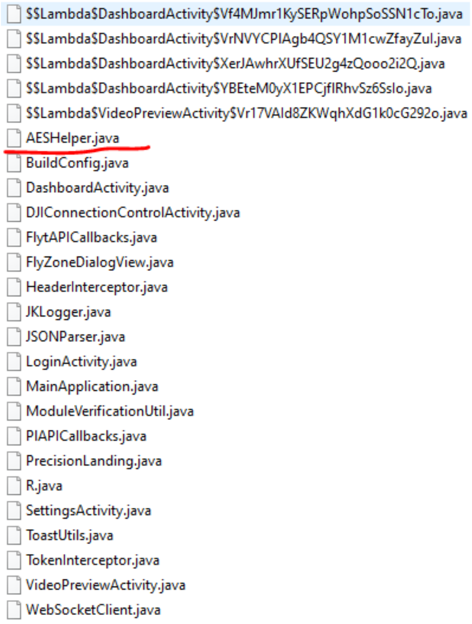


```
Using username "root".
Authenticating with public key "sky@acer" from agent
Last login: Wed Sep 22 11:19:35 2021 from 192.168.1.207
root@skydevice:~# skysense-cli monitor
2021-09-22 10:06:27.436 17286   0       SKY_SCANNING_INIT       0       0
2021-09-22 10:06:28.696 17264   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:29.521 17264   0       SKY_SCANNING_DETECTING  0       0
2021-09-22 10:06:30.642 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:31.570 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:32.640 17264   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:33.618 17220   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:34.688 17220   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:35.615 17286   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:36.635 17264   37      SKY_SCANNING_RUN        0       0
2021-09-22 10:06:37.613 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:38.683 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:39.973 17307   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:40.449 17242   0       SKY_PRE_CHARGING_INIT   0       0
2021-09-22 10:06:41.741 17264   0       SKY_PRE_CHARGING_RUN    0       0
2021-09-22 10:06:42.670 17264   0       SKY_PRE_CHARGING_RUN    0       0
2021-09-22 10:06:43.738 17264   36      SKY_SCANNING_RUN        0       0
2021-09-22 10:06:44.667 17307   37      SKY_SCANNING_RUN        0       0
```

Figure 4: Example of output in Charge station (L) software program skysense-cli . (Source: Final Results – Drone Automation Testbed, 2021)

Drone Management Appliance and web service

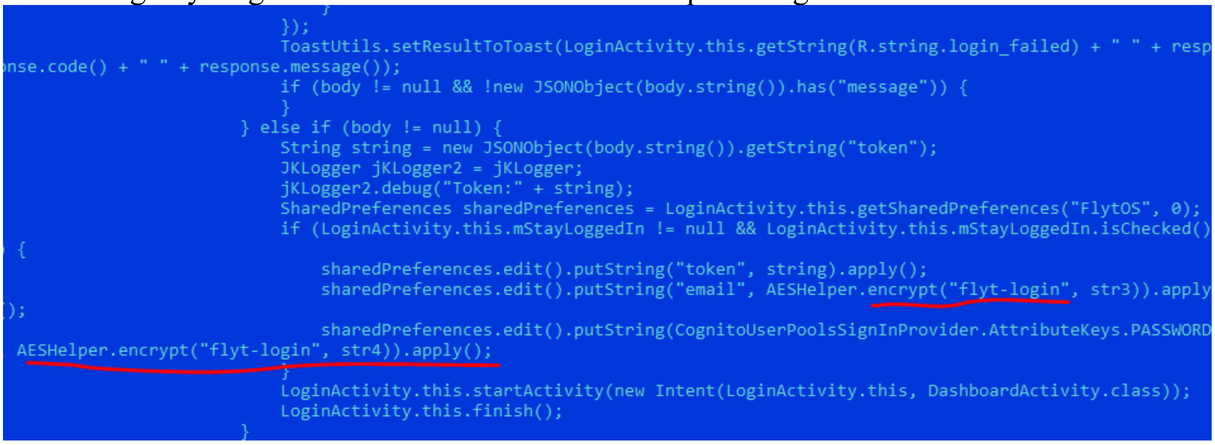
Web service and Drone appliance provided by FlyNow.com vendor. Web service provides REST API to retrieve drone information, subscription status, flight route and parameters. Drone appliance represented by software program for Android OS and standalone IoT device with Android OS. Both application uses various REST requests like https://my.flytbase.com/accounts/login/v2/, https://my.flytbase.com/api/ at web service.
To understand the availability of security mechanisms and strength of encryption protocol between the web service (M) and appliance(A) we have performed de-compilation of software package with a Apktool and Jadx software applications. Figure 5 shows the presence of AESHelper.java file within the internal components.



```
$$Lambda$DashboardActivity$Vf4MJmr1KySERpWohpSoSSN1cTo.java
$$Lambda$DashboardActivity$VrNVYCPIAgb4QSY1M1cwZfayZul.java
$$Lambda$DashboardActivity$XerJAwhrXUfSEU2g4zQooo2i2Q.java
$$Lambda$DashboardActivity$YBEteM0yX1EPCjflRhvSz6Sslo.java
$$Lambda$VideoPreviewActivity$Vr17VAld8ZKWqhXdG1k0cG292o.java
AESHelper.java
BuildConfig.java
DashboardActivity.java
DJIConnectionControlActivity.java
FlytAPICallbacks.java
FlyZoneDialogView.java
HeaderInterceptor.java
JKLogger.java
JSONParser.java
LoginActivity.java
MainApplication.java
ModuleVerificationUtil.java
PIAPICallbacks.java
PrecisionLanding.java
R.java
SettingsActivity.java
ToastUtils.java
TokenInterceptor.java
VideoPreviewActivity.java
WebSocketClient.java
```

Figure 5: Internal structure of software program in Drone Appliance (A) with underlined data encryption code. (Source: Final Results – Drone Automation Testbed, 2021)

AESHelper file contains only encryption functions that implement data encryption\decryption by using "AES/CBC/PKCS7Padding" schema with 256 bit encryption key generated by hashing provided string with "SHA-256" hash algorithm. The software uses encryption\decryption functions to save account login in encrypted form. Application does not encrypt any information that is retrieved or sent from or to the web service. User account credentials stored in local device in encrypted form by using static encryption key generated from string “flyt-login” as demonstrated on code sample in Figure 6.



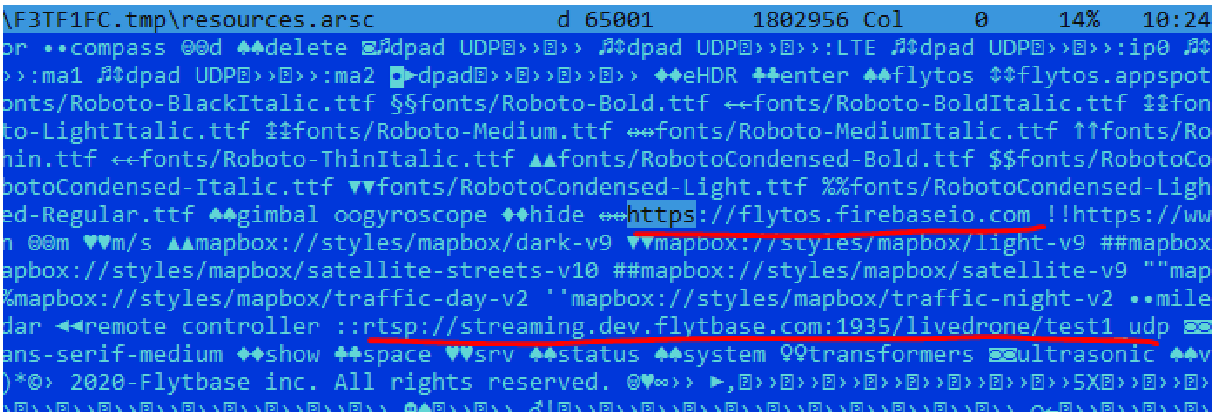
```
                           });
                           ToastUtils.setResultToToast(LoginActivity.this.getString(R.string.login_failed) + " " + resp
onse.code() + " " + response.message());
                           if (body != null && !new JSONObject(body.string()).has("message")) {
                           }
                       } else if (body != null) {
                           String string = new JSONObject(body.string()).getString("token");
                           JKLogger jKLogger2 = jKLogger;
                           jKLogger2.debug("Token:" + string);
                           SharedPreferences sharedPreferences = LoginActivity.this.getSharedPreferences("FlytOS", 0);
                           if (LoginActivity.this.mStayLoggedIn != null && LoginActivity.this.mStayLoggedIn.isChecked()
 {

                               sharedPreferences.edit().putString("token", string).apply();
                               sharedPreferences.edit().putString("email", AESHelper.encrypt("flyt-login", str3)).apply
);

                               sharedPreferences.edit().putString(CognitoUserPoolsSignInProvider.AttributeKeys.PASSWORD
 AESHelper.encrypt("flyt-login", str4)).apply();
                           }
                           LoginActivity.this.startActivity(new Intent(LoginActivity.this, DashboardActivity.class));
                           LoginActivity.this.finish();
                       }
```

Figure 6: Using data encryption with static encryption key generated from ‚flyt-login‘ string. (Source: Final Results – Drone Automation Testbed, 2021)

The application also relies only to underlying Operating System capabilities to mitigate man-in-the middle attack or web service spoofing. Software package also contain information about development environment “dev.flytbase.com:9000” as shown in strings file resources.arsc on Figure 7



```
\F3TF1FC.tmp\resources.arsc                    d 65001         1802956 Col      0      14%    10:24
or ••compass @@d ♠♠delete ◙♫dpad UDP⍰››⍰›› ♫↕dpad UDP⍰››⍰››:LTE ♫↕dpad UDP⍰››⍰››:ip0 ♫↕
››:ma1 ♫↕dpad UDP⍰››⍰››:ma2 ◘►dpad⍰››⍰››⍰››⍰›› ♦♦eHDR ♣♣enter ♠♠flytos ↕↕flytos.appspot
onts/Roboto-BlackItalic.ttf §§fonts/Roboto-Bold.ttf ←←fonts/Roboto-BoldItalic.ttf ↨↨fon
to-LightItalic.ttf ↨↨fonts/Roboto-Medium.ttf ↔↔fonts/Roboto-MediumItalic.ttf ↑↑fonts/Ro
hin.ttf ←←fonts/Roboto-ThinItalic.ttf ▲▲fonts/RobotoCondensed-Bold.ttf $$fonts/RobotoCo
botoCondensed-Italic.ttf ▼▼fonts/RobotoCondensed-Light.ttf %%fonts/RobotoCondensed-Ligh
ed-Regular.ttf ♠♠gimbal oogyroscope ♦♦hide ↔↔https://flytos.firebaseio.com !!https://ww
n @@m ♥♥m/s ▲▲mapbox://styles/mapbox/dark-v9 ▼▼mapbox://styles/mapbox/light-v9 ##mapbox
apbox://styles/mapbox/satellite-streets-v10 ##mapbox://styles/mapbox/satellite-v9 ""map
%mapbox://styles/mapbox/traffic-day-v2 ''mapbox://styles/mapbox/traffic-night-v2 ••mile
dar ◄◄remote controller ::rtsp://streaming.dev.flytbase.com:1935/livedrone/test1 udp ◙◙
ans-serif-medium ♦♦show ♣♣space ♥♥srv ♠♠status ♠♠system ♀♀transformers ◙◙ultrasonic ♠♠v
)*©› 2020-Flytbase inc. All rights reserved. @♥∞›› ►,⍰››⍰››⍰››⍰››⍰››⍰››⍰››⍰››5X⍰››⍰››⍰›
```

Figure 7: Internal string resources of Drone Appliance (A) with underlined API URL end-points. (Source: Final Results – Drone Automation Testbed, 2021)

Business user device

The system setup requires user to create an account at FlytNow.com. Later login credentials will be used by a variety of users, referred as business user, to access Drone management dashboard online at FlytNow.com web site that preserves shared access scenario as regular web site. It means any computer where login credential will be used needs to be on account for threat model, since in case of malware attack the login credentials and web site cookies will be copied by malware i.e. stolen with the purpose of unauthorized access. Later cyber criminals may extract aerial images from the FlytNow.com storage or change drone flight route with the purpose to retrieve more aerial images of industrial territory of the port.

Threat categorization

In this chapter we provide threat categories with corresponding examples to each identified threat and asset so that threats can be systematically identified in the proposed architecture in a structured and repeatable manner. To assign categories for each asset we use STRIDE method. STRIDE is an acronym for the following categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. To structure the threat assignment, we elaborated Data Flow diagram for all identified assets presented in Figure 8.

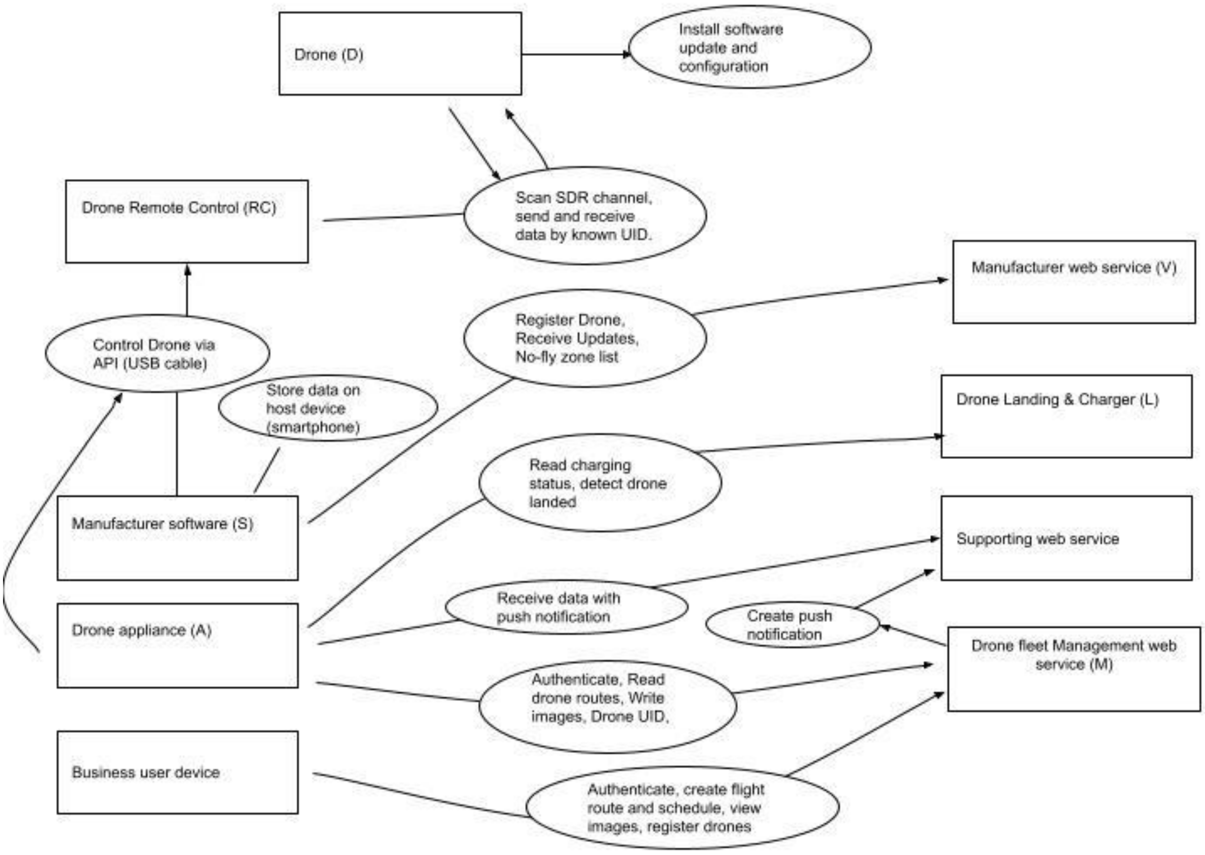

Drone (D)
Install software update and configuration
Drone Remote Control (RC)
Scan SDR channel, send and receive data by known UID.
Manufacturer web service (V)
Control Drone via API (USB cable)
Register Drone, Receive Updates, No-fly zone list
Store data on host device (smartphone)
Drone Landing & Charger (L)
Read charging status, detect drone landed
Manufacturer software (S)
Supporting web service
Drone appliance (A)
Receive data with push notification
Create push notification
Drone fleet Management web service (M)
Authenticate, Read drone routes, Write images, Drone UID,
Business user device
Authenticate, create flight route and schedule, view images, register drones

Figure 8: Data flow for proposed architecture. (Source: Final Results – Drone Automation Testbed, 2021)

A categorization, according to STRIDE, represent the following threats:
Spoofing - attack by using weak identity validation.
Tampering - attack on integrity of the data or communication.
Repudiation - threats that mainly goes by human factor with business logic or elevated operations misuse by privileged users.
Information disclosure - attack on confidentiality.
Denial of service - attack on availability.
Escalation of privileges - credentials leak or authorization misuse.
Table 1 shows the STRIDE matrix for the asset inventory in proposed architecture.

Asset	**S**	**T**	**R**	**I**	**D**	**E**
Drone (D)	X	X		X	X	X
Remote Control (RC)		X			X	
Software (S)				X		X

Appliance (A)	X			X		X
Drone management web service (M)	X	X	X	X	X	X
Manufacturer web service (V)	X	X	X	X	X	X
Charge station (L)				X	X	X
Business user workstation (W)	X		X	X		

Table 2: Threat categorization for asset inventory. (Source; Results – Drone Automation Testbed, 2021)

Security controls and defense tools

According to table 1, drone (D) may be affected by “S“T“I”D”E” threats. Where “T” and “I” can be a drone system intrusion or unauthorized access. Most enterprise drones have password protection mechanism. To enhance the security of the drone and this data, operators are required to enter a password each time they activate the drone, use remote controller or access the drone onboard storage via software. This provides aerial images confidentiality, even if the drone is lost or physically compromised.

DJI’s newest enterprise drones uses SDR protocol with data encrypted using the leading AES-256 standard, ensuring critical information exchanged between the drone and its remote control is protected against other SDR devices in the area. However, DJI also offers Periscope product that allows to take control over any DJI drone, it means that Remote Control (RC) and Drone (D) systems may have manufacturers backdoors[1] that may be re-used by cyber criminals, represented as “T” and “D” threats. Such backdoors represent great threat to entire system since it is designed to bypass known security controls.

To protect confidentiality “I” and “T” for Software (S) and Appliance (A) components it is possible to install integrity antivirus on mobile device where (S) will be installed or Intrusion detection software in the Network. Also, periodic vulnerability scan may be used. To protect Availability “D” we can employ solutions like CloudFlare and system resources monitoring software to prevent intermediate system malfunction. To eliminate (E) a two-factor authentication can be used to protect access to web site control panel at (V) and (M) systems.

7 Conclusion

The security aspect of drones can keep the facilities secure through high-end gathering data capabilities and secure data transmission. In summary, the use of threat modeling tools and asset inventory method in proceeding with the pilot project yielded many positive outcomes. The results of cyber security STRIDE analysis were used by the port management to confirm the implementation of security controls. As a decision support, the security review of each

[1] An undocumented way of gaining access to a computer system

system components gave confidence to the port managers in the security posture of drone automation system depending on security features of suppliers and its products. The security aspect of drone management system is able to keep the facilities secure through high-end gathering data capabilities and secure data transmission. To create a fully autonomous solution, a wide range of systems can be configured with complementary technologies, such as autonomous charging stations, software, and cloud SaaS service.

The next steps of the project could be to incorporate multiple redundant systems, which are fail-safe to mitigate risk around critical infrastructure of cargo terminal. The main lessons learned was to keep a certain range of defense rules, tools and procedures configured with complementary technologies in IT infrastructure. According the cyber-security standards such as ISO-27001, such defense strategy should be reflected in organization Cyber-security policy document and kept applied in periodical manner. Another lesson was to develop a resilience or continuity plan in case of successfully cyber-attack, due to unpredictable nature of vulnerabilities of any nested components. According to public information available at CVE[2] database, hundreds or software and hardware vulnerabilities discovered each month and cyber criminals start exploiting them on the next day. This raises a third lesson to integrate Threat Intelligence service into the organization business processes. This will allow organization to properly respond to discovered vulnerabilities, for example update software, install new security tools or shutdown affected hardware for some time until a patch, update or mitigation will be available by the vendor. This can help to archive the better safety and privacy when using autonomous UAVs systems.

8 References

[1] L. Mejias, J. P. Diguet, C. Dezan, D. Campbell, J. Kok, and G. Coppin, "Embedded computation architectures for autonomy in unmanned aircraft systems (Uas)," *Sensors (Switzerland)*, vol. 21, no. 4, pp. 1–33, 2021, doi: 10.3390/s21041115.

[2] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," *J. Def. Model. Simul.*, vol. 13, no. 3, pp. 331–342, 2016, doi: 10.1177/1548512915617252.

[3] C. Coopmans, "Architecture requirements for ethical, accurate, and resilient unmanned aerial personal remote sensing," *2014 Int. Conf. Unmanned Aircr. Syst. ICUAS 2014 - Conf. Proc.*, pp. 1–8, 2014, doi: 10.1109/ICUAS.2014.6842233.

[4] R. T. Ogan, "Integration of manned and unmanned aircraft systems into U.S. airspace," *Conf. Proc. - IEEE SOUTHEASTCON*, pp. 4–7, 2014, doi: 10.1109/SECON.2014.6950681.

[5] W. J. Broad, "Published by : American Association for the Advancement of Science The U . S . Flight from Pilotless Planes," vol. 213, no. 4504, pp. 188–190, 1981.

[6] H. Shakhatreh *et al.*, "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019, doi: 10.1109/ACCESS.2019.2909530.

[2] https://cve.mitre.org/

[7] V. Rodriguez-Fernandez, H. D. Menendez, and D. Camacho, “Design and development of a lightweight multi-UAV simulator,” *Proc. - 2015 IEEE 2nd Int. Conf. Cybern. CYBCONF 2015*, pp. 255–260, 2015, doi: 10.1109/CYBConf.2015.7175942.

[8] W. Khawaja, I. Guvenc, and D. Matolak, “UWB channel sounding and modeling for UAV air-to-ground propagation channels,” *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, 2016, doi: 10.1109/GLOCOM.2016.7842372.

[9] J. Boubeta-Puig, E. Moguel, F. Sanchez-Figueroa, J. Hernandez, and J. Carlos Preciado, “An Autonomous UAV Architecture for Remote Sensing and Intelligent Decision-making,” *IEEE Internet Comput.*, vol. 22, no. 3, pp. 6–15, 2018, doi: 10.1109/MIC.2018.032501511.

[10] A. Mora, S. Vemprala, A. Carrio, and S. Saripalli, “Flight performance assessment of land surveying trajectories for multiple UAV platforms,” *2015 Work. Res. Educ. Dev. Unmanned Aer. Syst. RED-UAS 2015*, pp. 1–7, 2016, doi: 10.1109/RED-UAS.2015.7440984.

[11] N. Neji and T. Mostfa, “Communication technology for unmanned aerial vehicles: A qualitative assessment and application to Precision Agriculture,” *2019 Int. Conf. Unmanned Aircr. Syst. ICUAS 2019*, pp. 848–855, 2019, doi: 10.1109/ICUAS.2019.8797879.

[12] Y. Liu, R. Lv, X. Guan, and J. Zeng, “Path planning for unmanned aerial vehicle under geo-fencing and minimum safe separation constraints,” *Proc. World Congr. Intell. Control Autom.*, vol. 2016-Septe, no. 4, pp. 28–31, 2016, doi: 10.1109/WCICA.2016.7578482.

[13] N. M. Thamrin *et al.*, “Simultaneous localization and mapping based real-Time inter-row tree tracking technique for unmanned aerial vehicle,” *Proc. - 2012 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2012*, pp. 322–327, 2012, doi: 10.1109/ICCSCE.2012.6487164.

[14] M. Chen, Q. Hu, C. Mackin, J. F. Fisac, and C. J. Tomlin, “Safe platooning of unmanned aerial vehicles via reachability,” *Proc. IEEE Conf. Decis. Control*, vol. 54rd IEEE, no. Cdc, pp. 4695–4701, 2015, doi: 10.1109/CDC.2015.7402951.

[15] P. Tokekar, J. Vander Hook, D. Mulla, and V. Isler, “Sensor Planning for a Symbiotic UAV and UGV System for Precision Agriculture,” *IEEE Trans. Robot.*, vol. 32, no. 6, pp. 1498–1511, 2016, doi: 10.1109/TRO.2016.2603528.

[16] A. G. Foina, R. Sengupta, P. Lerchi, Z. Liu, and C. Krainer, “Drones in smart cities: Overcoming barriers through air traffic control research,” *2015 Work. Res. Educ. Dev. Unmanned Aer. Syst. RED-UAS 2015*, pp. 351–359, 2016, doi: 10.1109/RED-UAS.2015.7441027.

[17] C. Pauner, I. Kamara, and J. Viguri, “Drones. Current challenges and standardisation solutions in the field of privacy and data protection,” *Proc. 2015 ITU Kaleidosc. Trust Inf. Soc. K-2015 - Acad. Conf.*, vol. 8, no. October 1995, 2016, doi: 10.1109/Kaleidoscope.2015.7383633.

[18] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, “Help from the Sky: Leveraging UAVs for Disaster Management,” *IEEE Pervasive Comput.*, vol. 16, no. 1, pp. 24–32, 2017, doi: 10.1109/MPRV.2017.11.

[19] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, “Drones for smart cities: Issues in cybersecurity, privacy, and public safety,” in *2016 International*

Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 216–221, doi: 10.1109/IWCMC.2016.7577060.

[20] J. P. G. Sterbenz, “Drones in the Smart City and IoT,” pp. 3–3, 2016, doi: 10.1145/2935620.2949659.

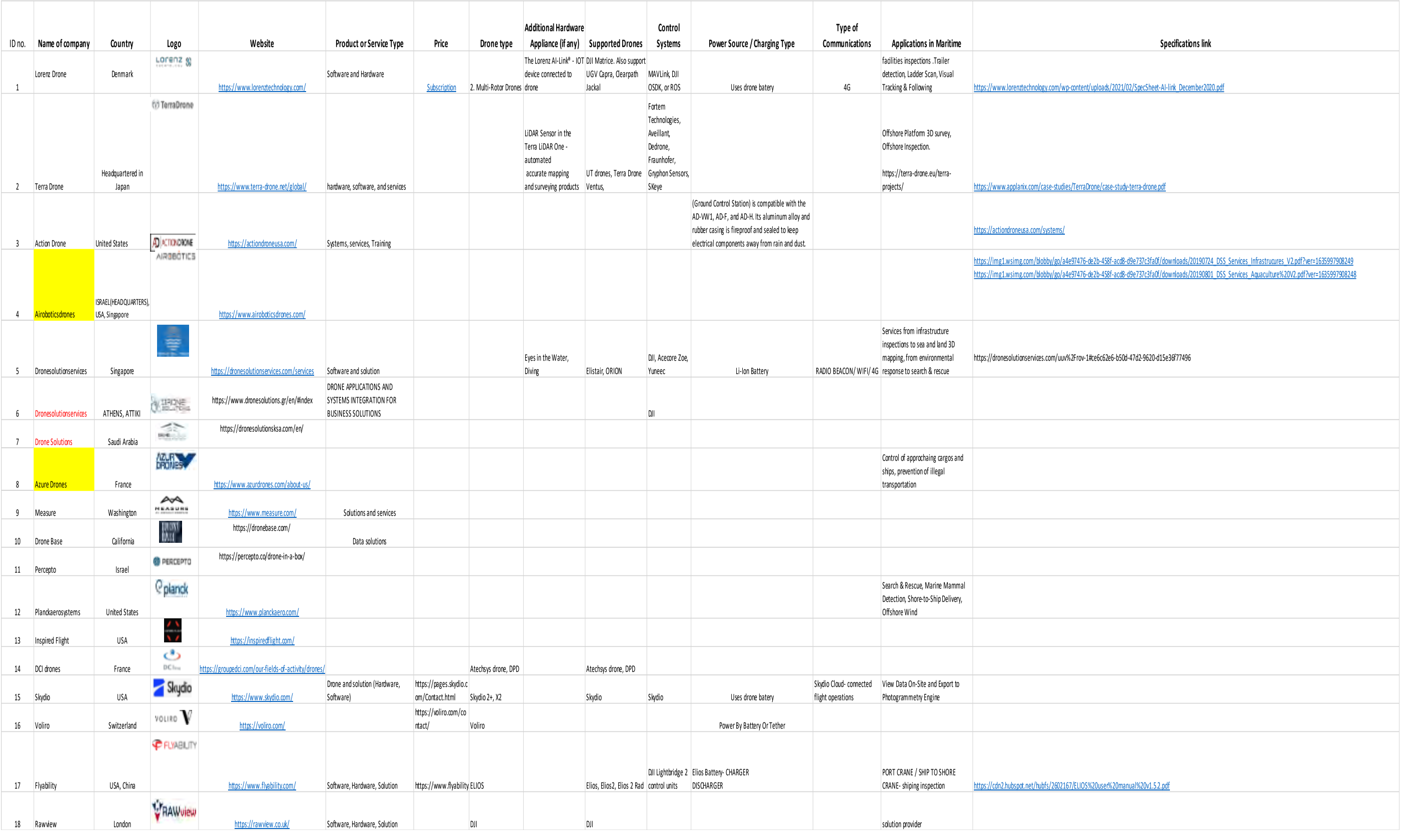
[21] R. Altawy and A. M. Youssef, “Security, privacy, and safety aspects of civilian drones: A survey,” *ACM Trans. Cyber-Physical Syst.*, vol. 1, no. 2, pp. 1–25, 2017, doi: 10.1145/3001836.

[22] A. Shariat, A. Tizghadam, and A. Leon-Garcia, “An ICN-based publish-subscribe platform to deliver UAV service in smart cities,” *Proc. - IEEE INFOCOM*, vol. 2016-Septe, pp. 698–703, 2016, doi: 10.1109/INFCOMW.2016.7562167.

[23] J. Won, S. H. Seo, and E. Bertino, “A secure communication protocol for drones and smart objects,” *ASIACCS 2015 - Proc. 10th ACM Symp. Information, Comput. Commun. Secur.*, pp. 249–260, 2015, doi: 10.1145/2714576.2714616

[24] Andrew Shelley,Addressing Security Concerns with Chinese Dronesand DJI Products, https://www.academia.edu/43142234/Addressing_Security_Concerns_with_Chinese_Drones_and_DJI_Products

Attachment Drone market review. Drone industry scan.



ID no.	Name of company	Country	Logo	Website	Product or Service Type	Price	Drone type	Additional Hardware Appliance (if any)	Supported Drones	Control Systems	Power Source / Charging Type	Type of Communications	Applications in Maritime	Specifications link
1	Lorenz Drone	Denmark		https://www.lorenztechnology.com/	Software and Hardware	Subscription	2. Multi-Rotor Drones	The Lorenz AI-Link® - IOT device connected to drone	DJI Matrice. Also support UGV Capra, Clearpath Jackal	MAVLink, DJI OSDK, or ROS	Uses drone batery	4G	facilities inspections .Trailer detection, Ladder Scan, Visual Tracking & Following	https://www.lorenztechnology.com/wp-content/uploads/2021/02/SpecSheet-AI-link_December2020.pdf
2	Terra Drone	Headquartered in Japan		https://www.terra-drone.net/global/	hardware, software, and services			LiDAR Sensor in the Terra LiDAR One - automated accurate mapping and surveying products	UT drones, Terra Drone Ventus,	Fortem Technologies, Aveillant, Dedrone, Fraunhofer, Gryphon Sensors, SKeye			Offshore Platform 3D survey, Offshore Inspection. https://terra-drone.eu/terra-projects/	https://www.applanix.com/case-studies/TerraDrone/case-study-terra-drone.pdf
3	Action Drone	United States		https://actiondroneusa.com/	Systems, services, Training						(Ground Control Station) is compatible with the AD-VW1, AD-F, and AD-H. Its aluminum alloy and rubber casing is fireproof and sealed to keep electrical components away from rain and dust.			https://actiondroneusa.com/systems/
4	Airoboticsdrones	ISRAEL(HEADQUARTERS), USA, Singapore		https://www.airoboticsdrones.com/										https://img1.wsimg.com/blobby/go/a4e97476-de2b-458f-acd8-d9e737c3fa0f/downloads/20190724_DSS_Services_Infrastrucures_V2.pdf?ver=1635997908249 https://img1.wsimg.com/blobby/go/a4e97476-de2b-458f-acd8-d9e737c3fa0f/downloads/20190801_DSS_Services_Aquaculture%20V2.pdf?ver=1635997908248
5	Dronesolutionservices	Singapore		https://dronesolutionservices.com/services	Software and solution			Eyes in the Water, Diving	Elistair, ORION	DJI, Acecore Zoe, Yuneec	Li-Ion Battery	RADIO BEACON/ WIFI/ 4G	Services from infrastructure inspections to sea and land 3D mapping, from environmental response to search & rescue	https://dronesolutionservices.com/uuv%2Frov-1#ce6c62e6-b50d-47d2-9620-d15e36f77496
6	Dronesolutionservices	ATHENS, ATTIKI		https://www.dronesolutions.gr/en/#index	DRONE APPLICATIONS AND SYSTEMS INTEGRATION FOR BUSINESS SOLUTIONS					DJI				
7	Drone Solutions	Saudi Arabia		https://dronesolutionsksa.com/en/										
8	Azure Drones	France		https://www.azurdrones.com/about-us/									Control of approchaing cargos and ships, prevention of illegal transportation	
9	Measure	Washington		https://www.measure.com/	Solutions and services									
10	Drone Base	California		https://dronebase.com/	Data solutions									
11	Percepto	Israel		https://percepto.co/drone-in-a-box/										
12	Planckaerosystems	United States		https://www.planckaero.com/									Search & Rescue, Marine Mammal Detection, Shore-to-Ship Delivery, Offshore Wind	
13	Inspired Flight	USA		https://inspiredflight.com/										
14	DCI drones	France		https://groupedci.com/our-fields-of-activity/drones/			Atechsys drone, DPD		Atechsys drone, DPD					
15	Skydio	USA		https://www.skydio.com/	Drone and solution (Hardware, Software)	https://pages.skydio.com/Contact.html	Skydio 2+, X2		Skydio	Skydio	Uses drone batery	Skydio Cloud- connected flight operations	View Data On-Site and Export to Photogrammetry Engine	
16	Voliro	Switzerland		https://voliro.com/		https://voliro.com/contact/	Voliro				Power By Battery Or Tether			
17	Flyability	USA, China		https://www.flyability.com/	Software, Hardware, Solution	https://www.flyability	ELIOS		Elios, Elios2, Elios 2 Rad	DJI Lightbridge 2 control units	Elios Battery- CHARGER DISCHARGER		PORT CRANE / SHIP TO SHORE CRANE- shiping inspection	https://cdn2.hubspot.net/hubfs/2602167/ELIOS%20user%20manual%20v1.5.2.pdf
18	Rawview	London		https://rawview.co.uk/	Software, Hardware, Solution		DJI		DJI				solution provider	

Final Results – Drone Automation Testbed

Date: 15 August 2021.

Authors:

Lawrence Henesey, larry.henesey@bth.se

Alexandr Silonosov, aiv@bth.se

Maryam Rezaei, maryam.rezaei@bth.se

Drone testbed - experimental area setup for autonomous flights.

Drone Management System project for SECMAR Project.

Author: Alexandr Silonosov, aiv@bth.se, Lawrence Henesey larry.henesey@bth.se, Blekinge Tekniska Hogskolan

The aim is to test cyber-security aspects of autonomous drone operations during flights by dynamically created paths over a quay area with the purpose of ship visual monitoring.

Testbed #1

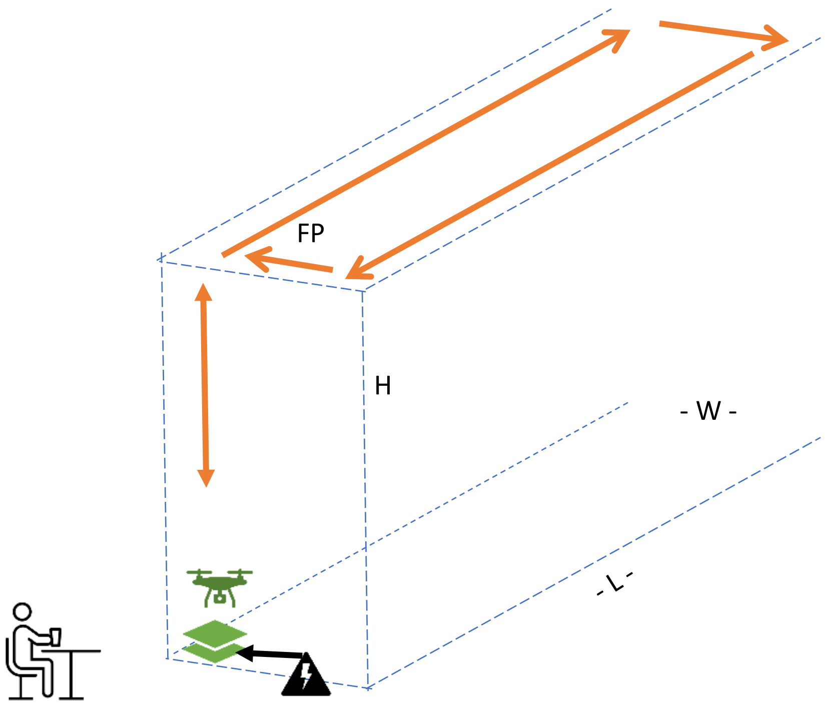


Figure 1. Drone flight testbed. H, W, L – height, width and length of flight path (FP).

We need to organize a special testbed environment before we run a series of test flights in autonomous mode (without operator intervention), i.e., programmed autopilot with a pre-defined flight path.
The goal of experiment is to test the necessary level of autonomous drone operations, including cyber-physical safet: test auto-charge device, drone control center connection by using online SaaS. Test flight path (FP) delivery via the online control center. Test drone self-checkup, return, and landing in case of miss-configured flight path or missed connection with a control center.

Requirements:

1. H – 40 meter, W – 10(5) meters, L – 50(100) meters, FP – 40+5(10)+50(100) * 2 meters
2. Operator room, with power supply and window facing to FP area for visual contact.
3. An open air place with a power supply for the drone charge station (2 * 2 meters), is used as a drone launch (takeoff).
4. No people sitting in FP area (some occasional pedestrians is OK)

Testbed #2

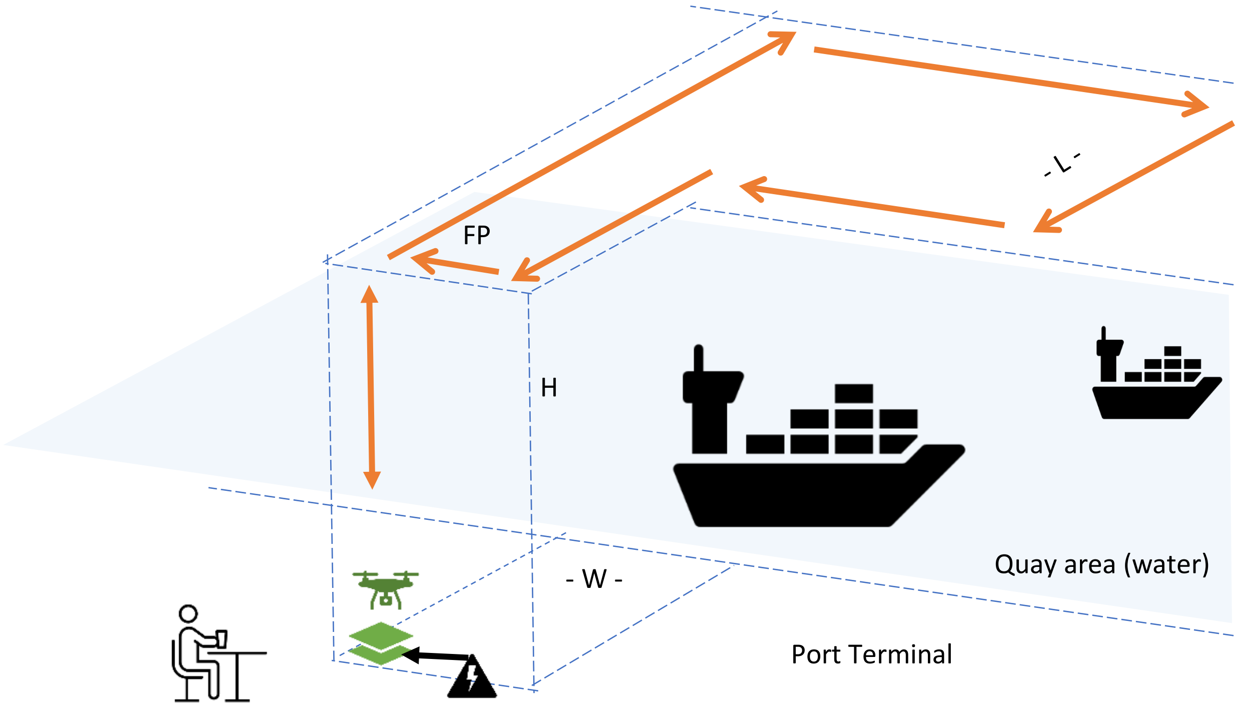


Figure 2. Drone flights testbed in Port quay area. H, W, L – height, width and length of flight path (FP).

The goal of testbed #2 is to test the necessary level of cyber-security during autonomous drone operations with a dynamically created flight path over a quay area, by using AIS data provider. Test dynamic creating of flight path and with secure delivery to the drone. Test ship aerial-photo capture and secure photo storage and delivery to control center. Test drone self checkup, return and landing in case of miss-configured flight path or missed connection with control center under quay area.

Requirements:

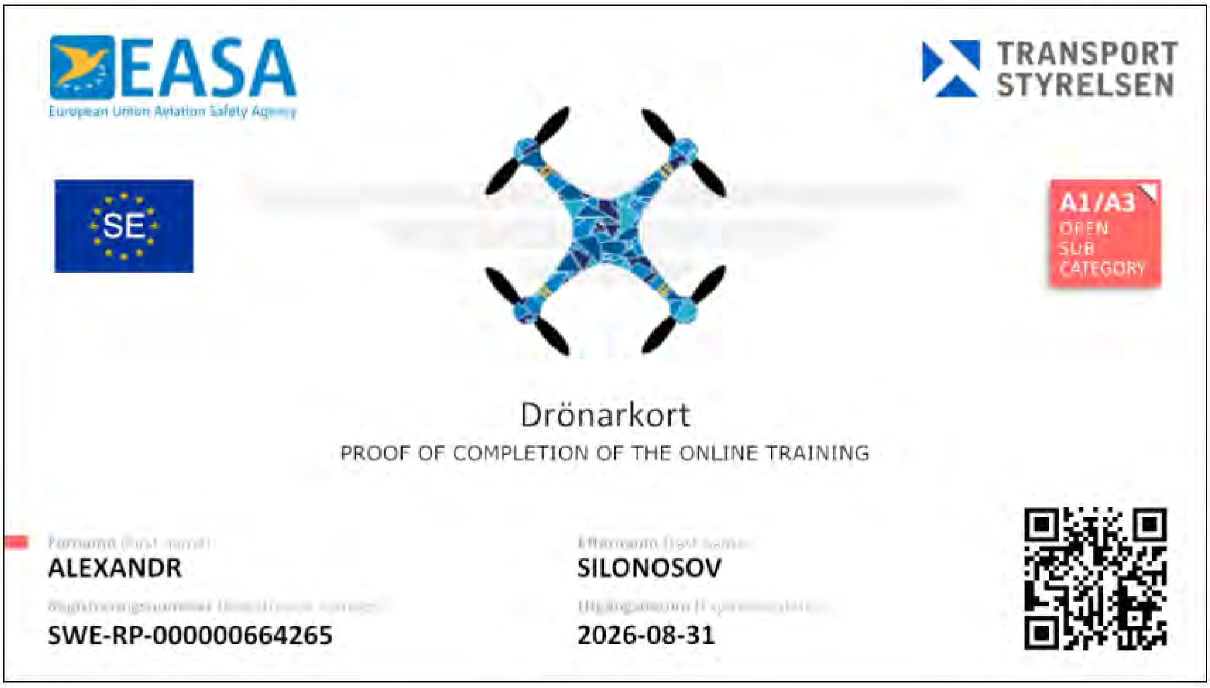
1. H – 80 meters, W – 50 meters, L – 500 meters, FP – 80+50+500 * 2 meters
2. Operator room, with power supply and window facing to FP corridor.
3. An open air place with a power supply for the drone charge station (2 * 2 meters), is used as a drone launch (takeoff).
4. Flight Path under quay area intersecting ship arrival/departure route.

References:

Afanasov, Mikhail, et al. "FlyZone: A testbed for experimenting with aerial drone applications." *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*. 2019.

Al-Radaideh, A., Al-Jarrah, M. A., & Jhemi, A. (2010, April). UAV Testbed building and development for research purposes at the American University of Sharjah. In *7th International Symposium on Mechatronics and its Applications* (pp. 1-7). IEEE.

Drone operator license:



EASA
European Union Aviation Safety Agency

SE

TRANSPORT
STYRELSEN

A1/A3
OPEN
SUB
CATEGORY

Drönarkort
PROOF OF COMPLETION OF THE ONLINE TRAINING

Förnamn (First name)
ALEXANDR

Efternamn (Last name)
SILONOSOV

Registreringsnummer (Registration number)
SWE-RP-000000664265

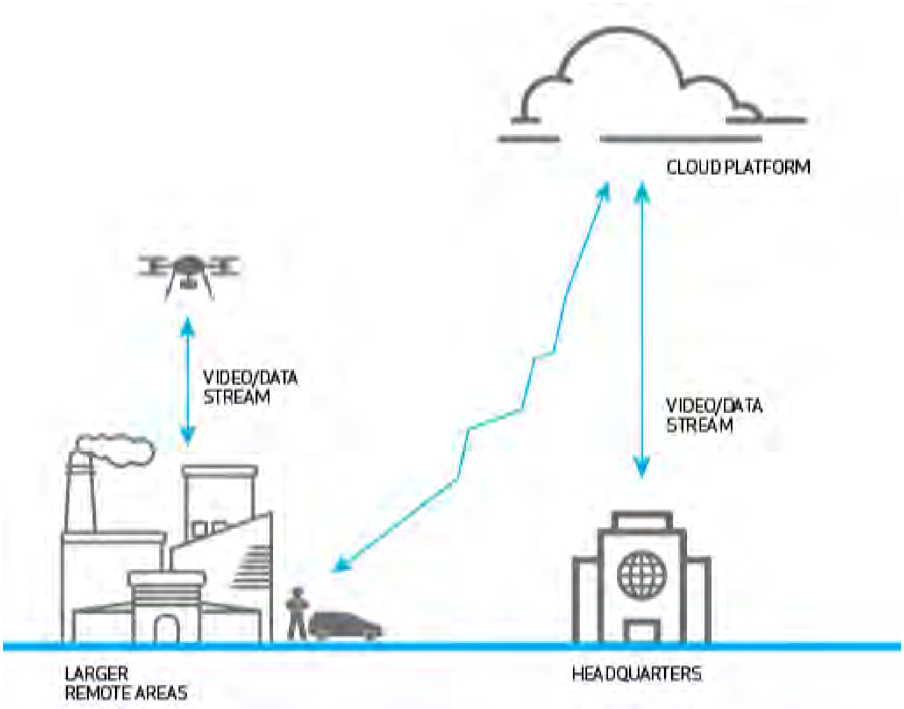
Utgångsdatum (Expiration date)
2026-08-31

Beslut om operatörs-ID. Transportstyrelsens beslut. Transportstyrelsen beviljar ansökan om registrering i operatörsregistret och tilldelar Alexandr Silonosov följande operatörs-ID: SWEd0u8at2akr7uj

Registreringen gäller från och med 2021-08-10.

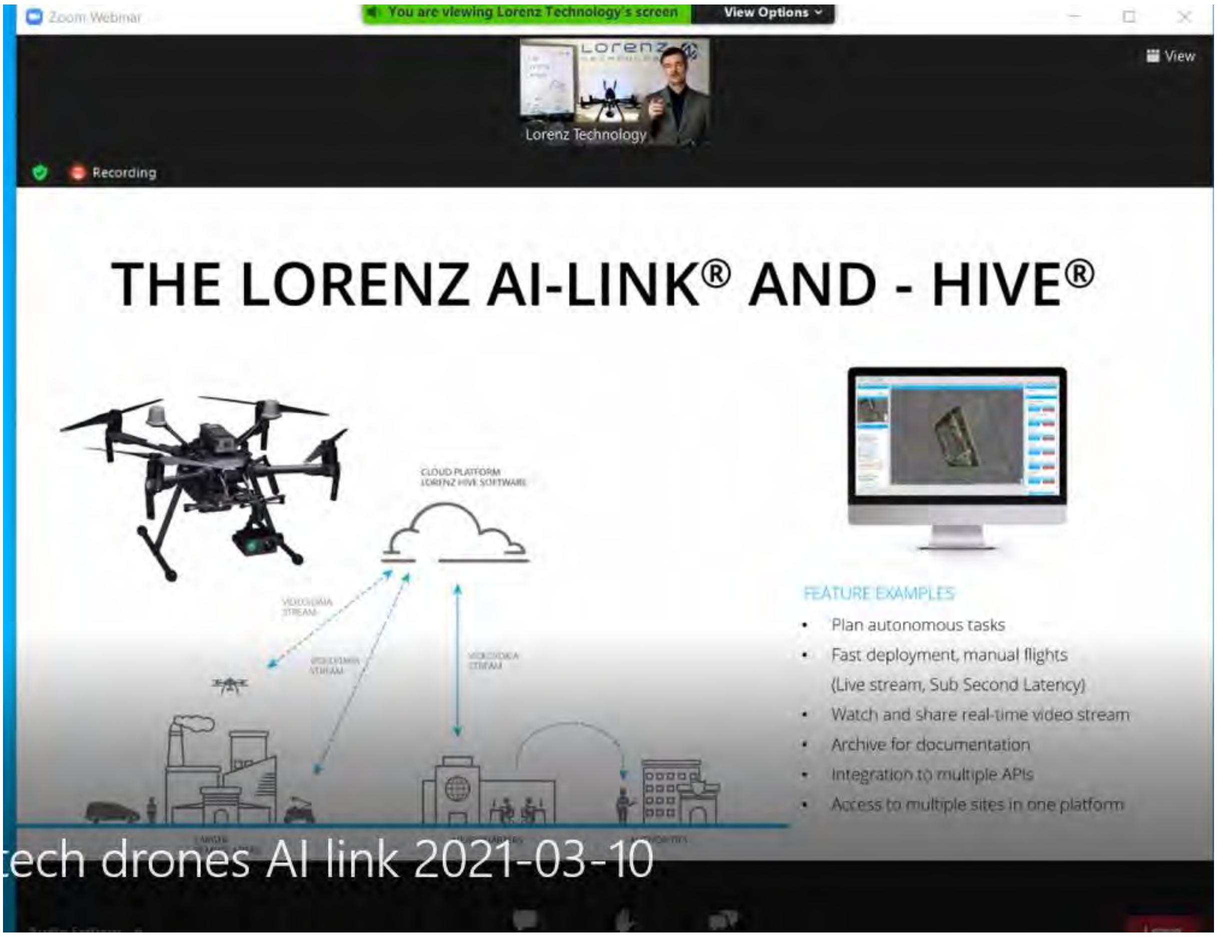
Webinars materials

lorenztechnology.com



On-board API: Edge-computing, extra control over the drone, Drone Hardware Appliance

Webinar 2021-01-28

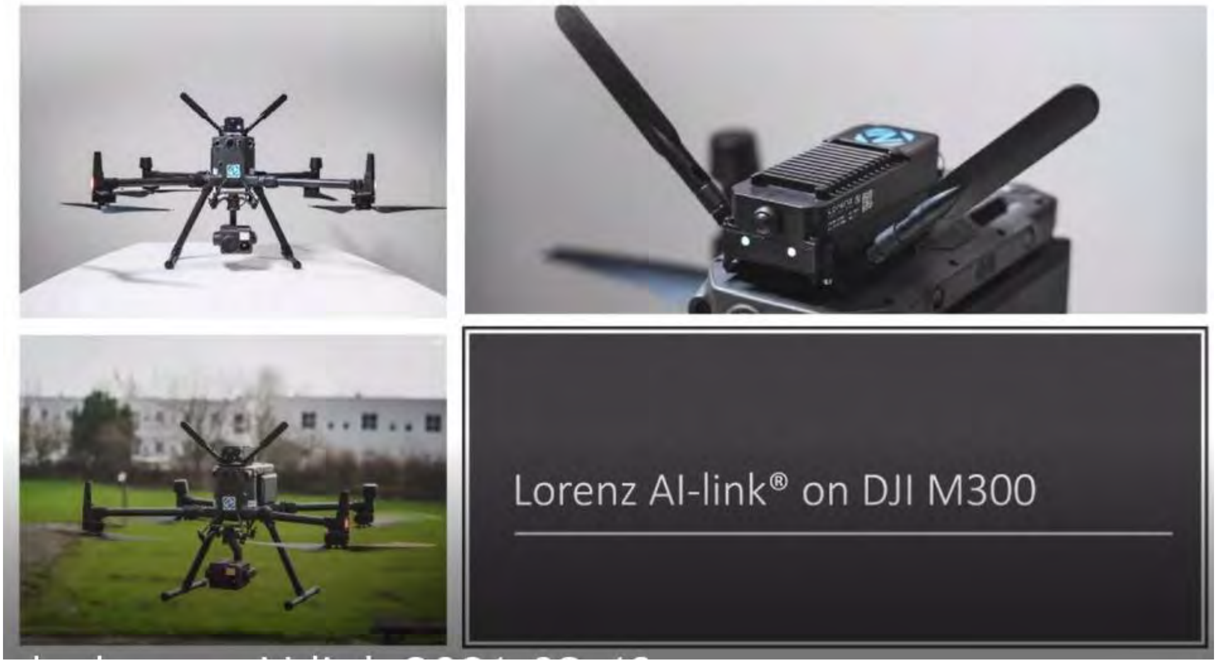


THE LORENZ AI-LINK® AND - HIVE®

FEATURE EXAMPLES

- Plan autonomous tasks
- Fast deployment, manual flights (Live stream, Sub Second Latency)
- Watch and share real-time video stream
- Archive for documentation
- Integration to multiple APIs
- Access to multiple sites in one platform

ech drones AI link 2021-03-10



Lorenz AI-link® on DJI M300

SOLUTION STEP TWO – **ADDED SERVICES**

Facility Management

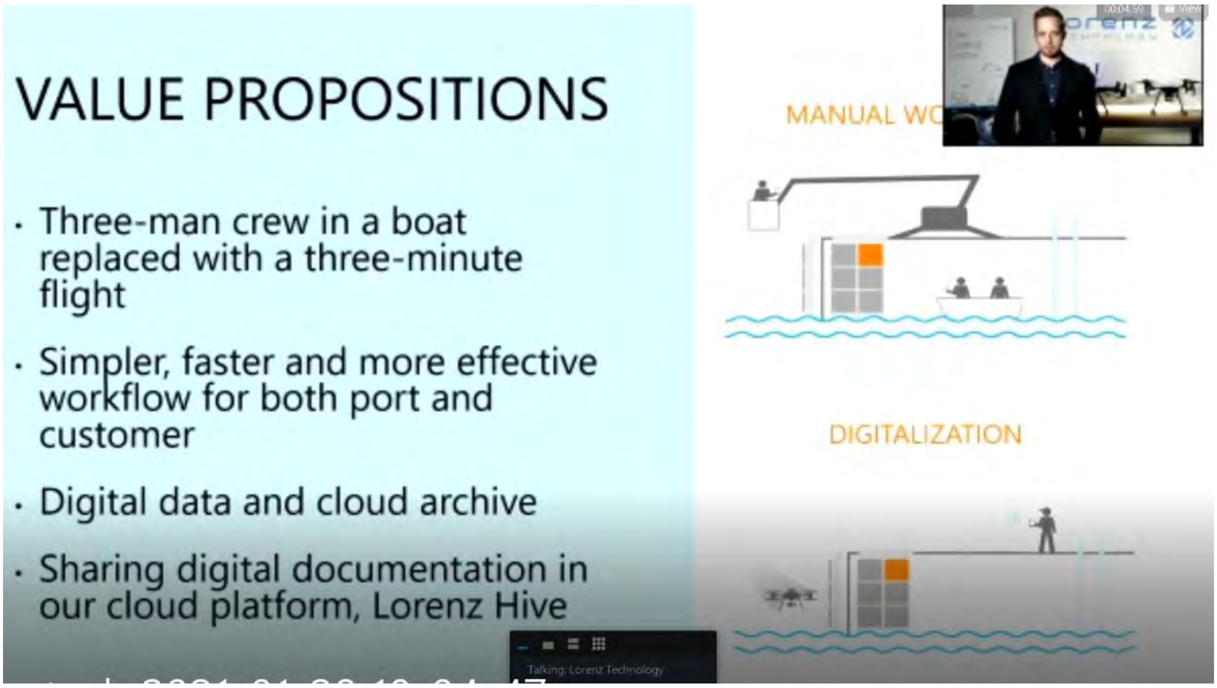
Surveillance and updated maps

USE CASE INSPIRATION

USE CASE - THE DIGITAL PORT

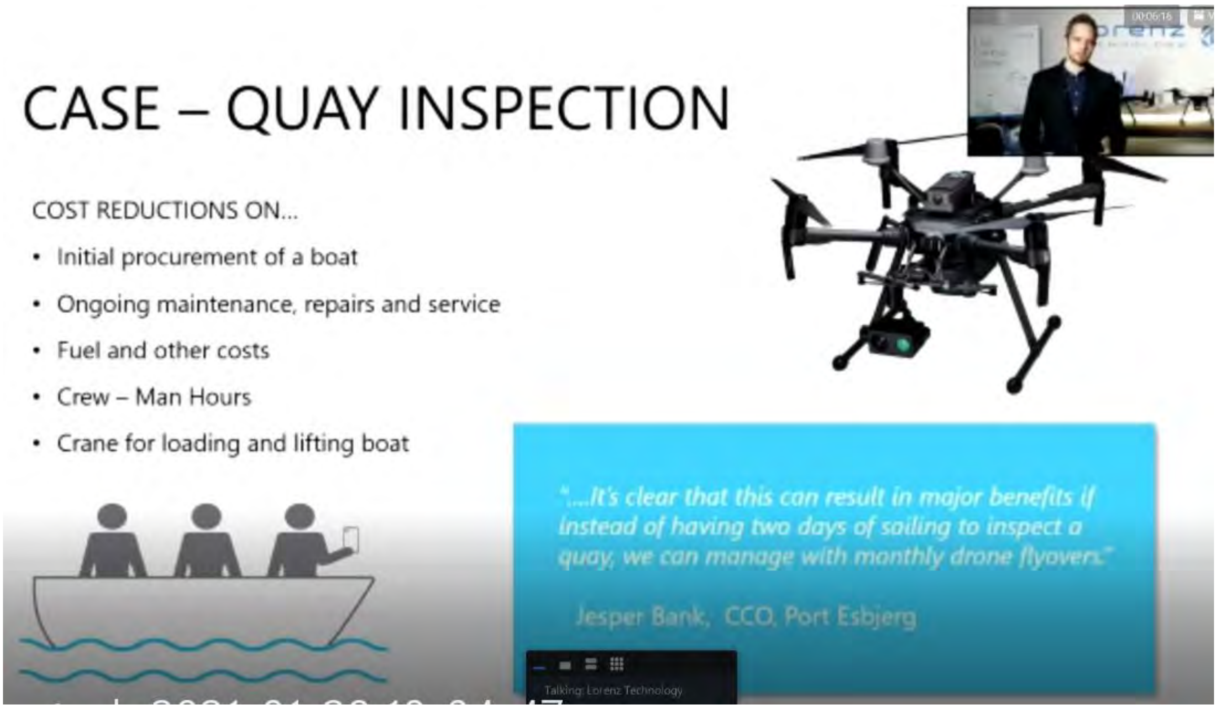
- Quay inspection
- Incidents (AdHoc)
- Area mapping
- Road inspection
- Building inspection
- sediment tracking
- Lighthouse and buoy inspection
- Fence inspection

Webinar 2021-03-10



VALUE PROPOSITIONS

- Three-man crew in a boat replaced with a three-minute flight
- Simpler, faster and more effective workflow for both port and customer
- Digital data and cloud archive
- Sharing digital documentation in our cloud platform, Lorenz Hive



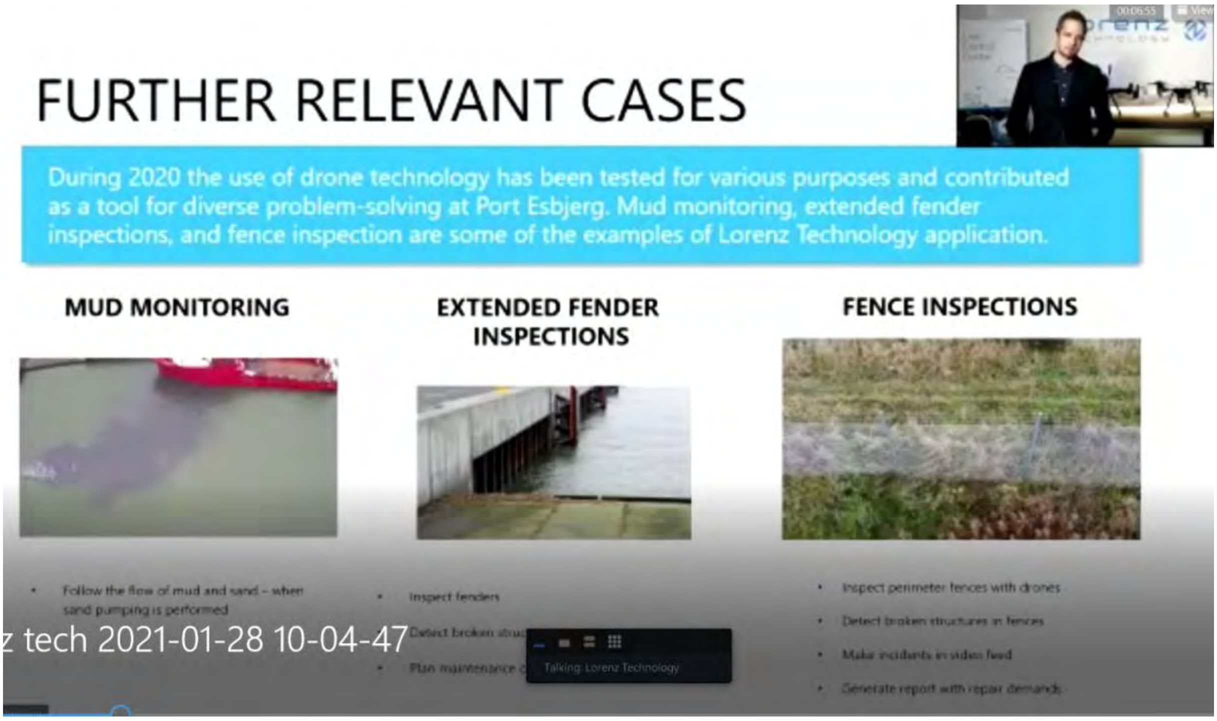
CASE – QUAY INSPECTION

COST REDUCTIONS ON...

- Initial procurement of a boat
- Ongoing maintenance, repairs and service
- Fuel and other costs
- Crew – Man Hours
- Crane for loading and lifting boat

"...It's clear that this can result in major benefits if instead of having two days of sailing to inspect a quay, we can manage with monthly drone flyovers."

Jesper Bank, CCO, Port Esbjerg



FURTHER RELEVANT CASES

During 2020 the use of drone technology has been tested for various purposes and contributed as a tool for diverse problem-solving at Port Esbjerg. Mud monitoring, extended fender inspections, and fence inspection are some of the examples of Lorenz Technology application.

MUD MONITORING

- Follow the flow of mud and sand – when sand pumping is performed

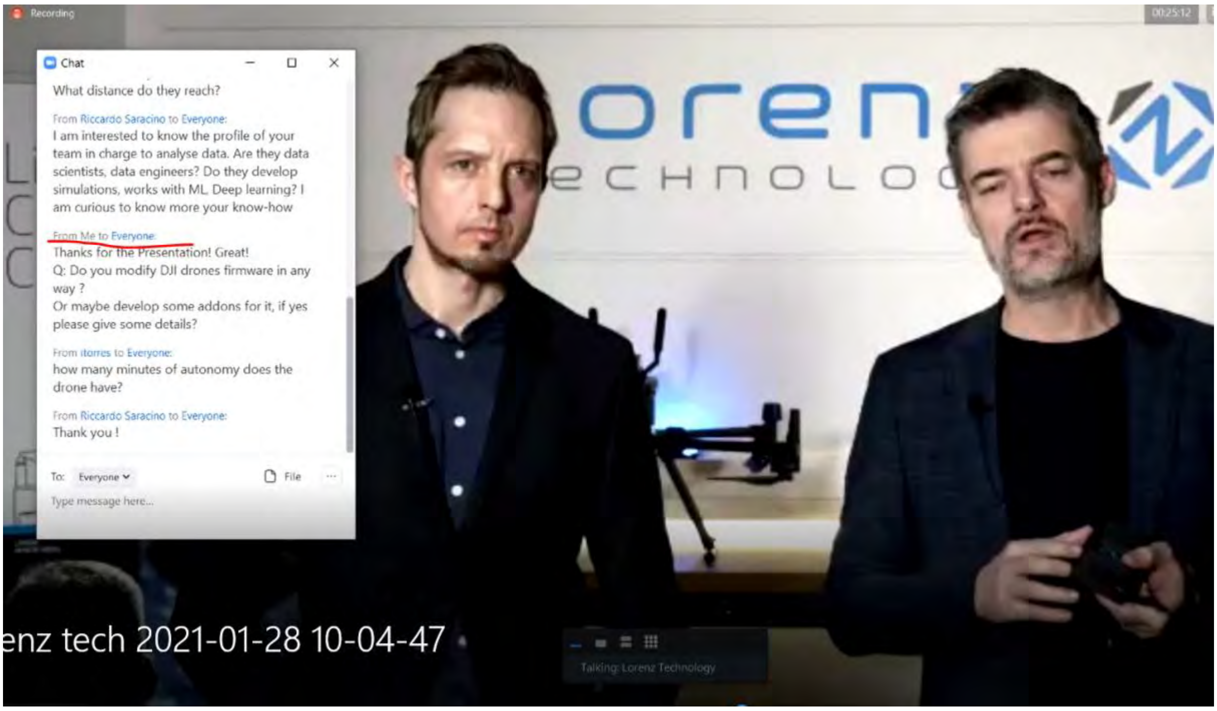
EXTENDED FENDER INSPECTIONS

- Inspect fenders
- Detect broken struc
- Plan maintenance c

FENCE INSPECTIONS

- Inspect perimeter fences with drones
- Detect broken structures in fences
- Make incidents in video feed
- Generate report with repair demands

BTH Asking questiona in Zoom seminar -



Chat

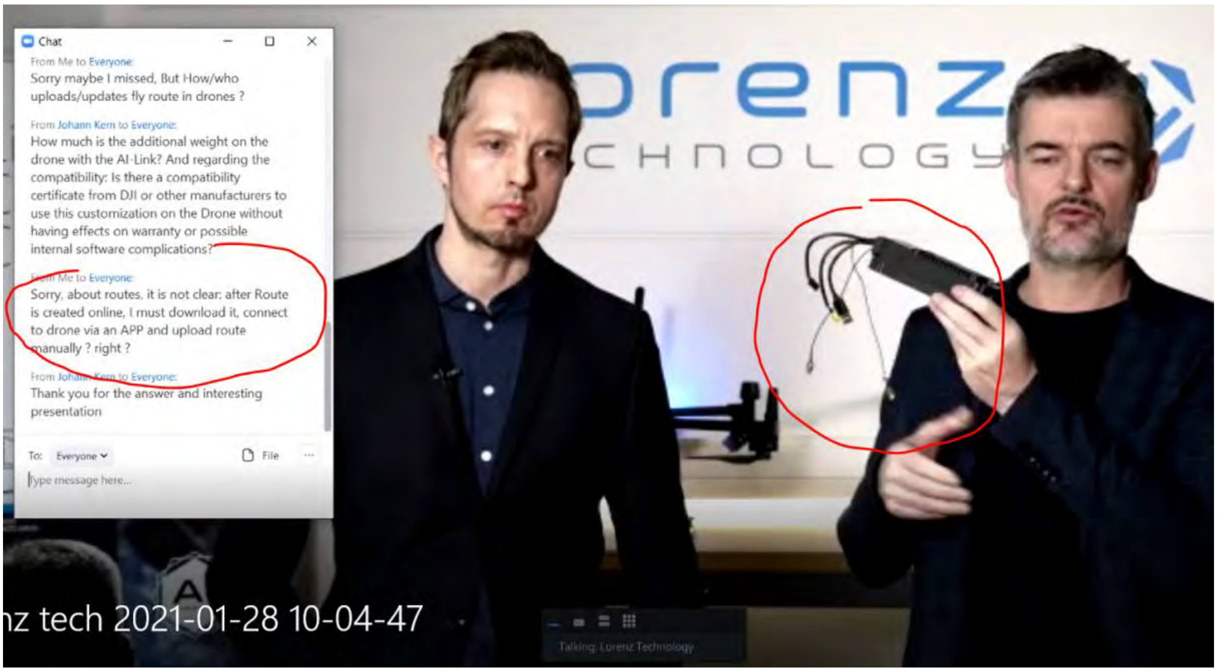
What distance do they reach?

From Riccardo Saracino to Everyone:
I am interested to know the profile of your team in charge to analyse data. Are they data scientists, data engineers? Do they develop simulations, works with ML Deep learning? I am curious to know more your know-how

From Me to Everyone:
Thanks for the Presentation! Great!
Q: Do you modify DJI drones firmware in any way ?
Or maybe develop some addons for it, if yes please give some details?

From itorres to Everyone:
how many minutes of autonomy does the drone have?

From Riccardo Saracino to Everyone:
Thank you !



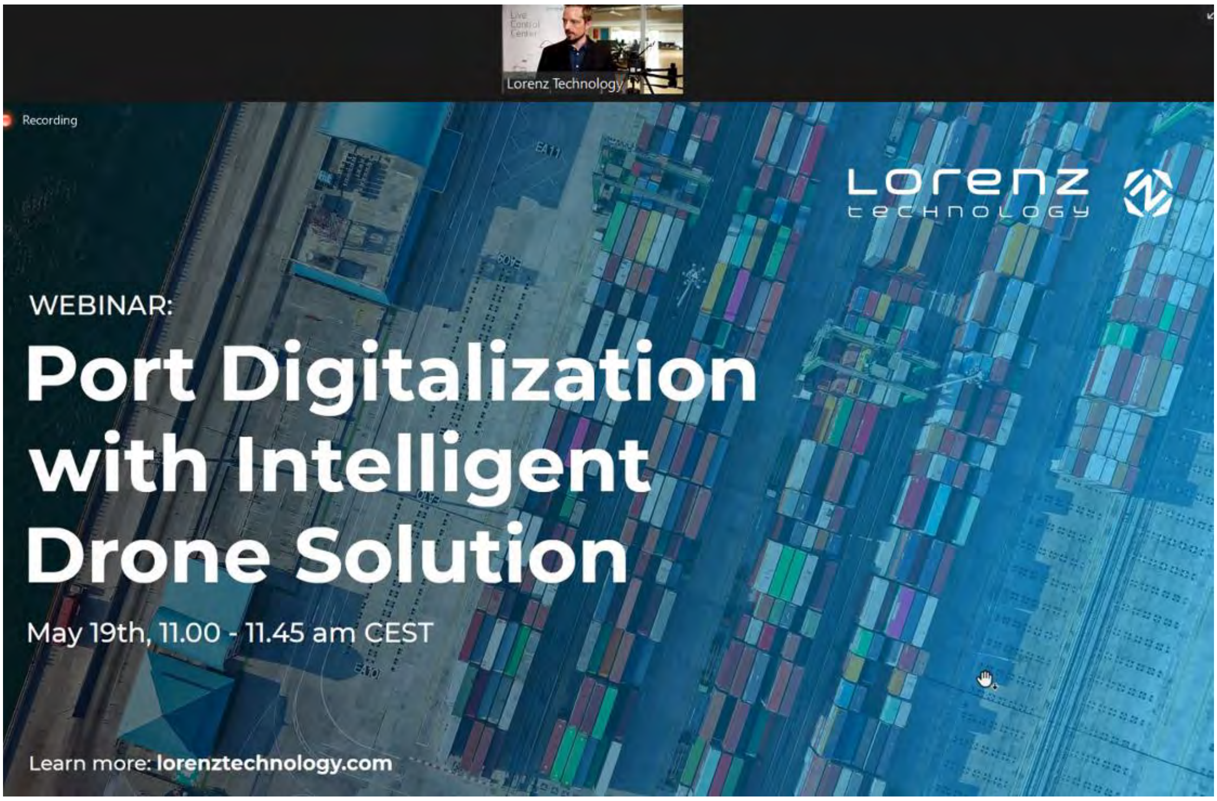
From Me to Everyone:
Sorry maybe I missed, But How/who uploads/updates fly route in drones ?

From Johann Kern to Everyone:
How much is the additional weight on the drone with the AI-Link? And regarding the compatibility: Is there a compatibility certificate from DJI or other manufacturers to use this customization on the Drone without having effects on warranty or possible internal software complications?

From Me to Everyone:
Sorry, about routes, it is not clear: after Route is created online, I must download it, connect to drone via an APP and upload route manually ? right ?

From Johann Kern to Everyone:
Thank you for the answer and interesting presentation

Webinarr Lorez May 2021

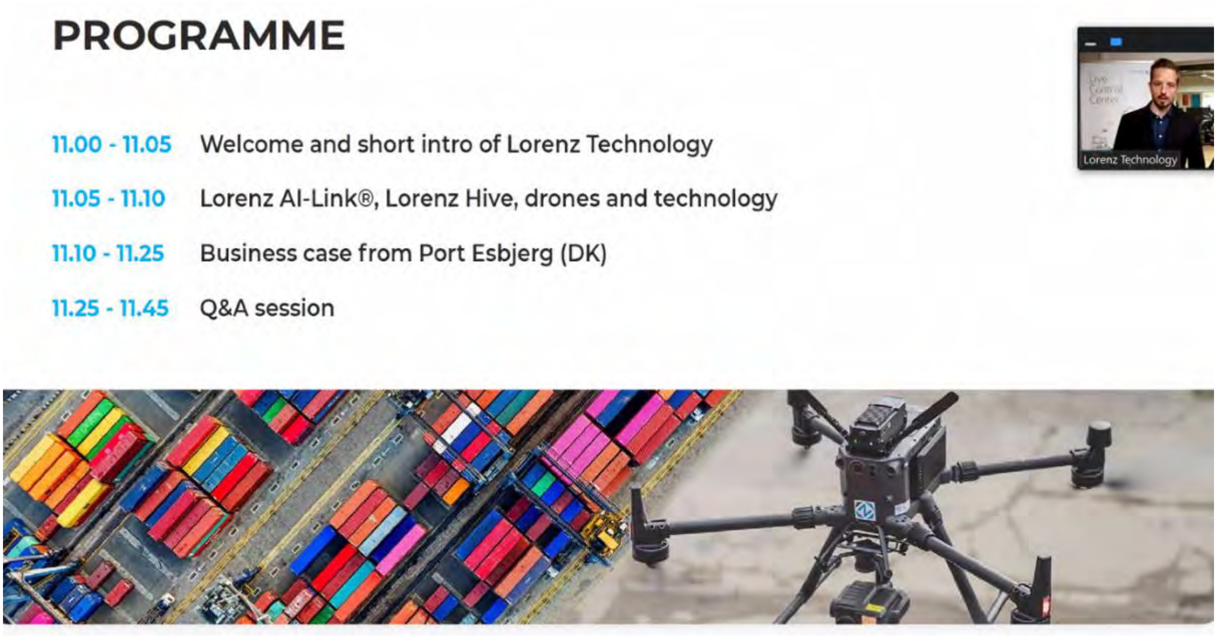


WEBINAR:

Port Digitalization with Intelligent Drone Solution

May 19th, 11.00 - 11.45 am CEST

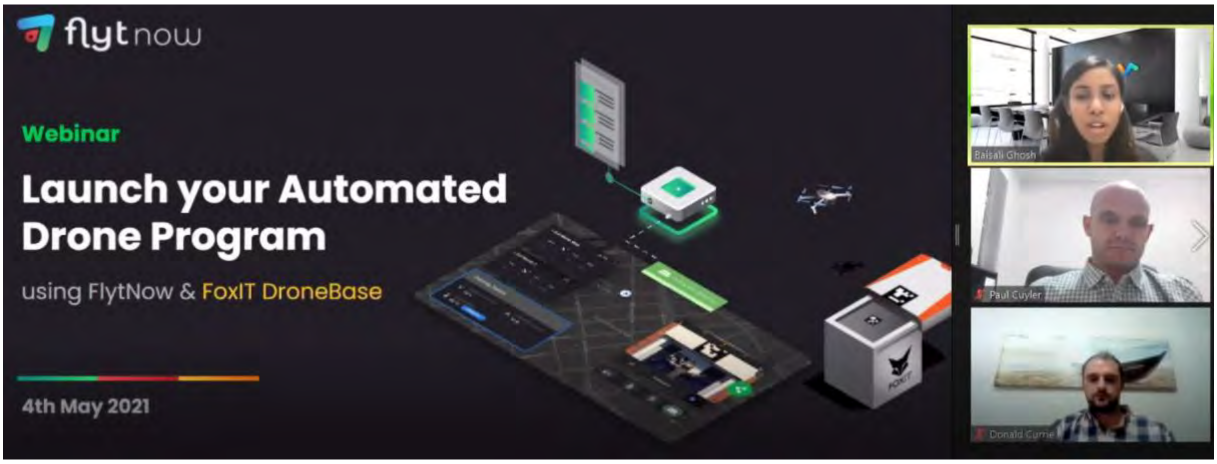
Learn more: **lorenztechnology.com**



PROGRAMME

11.00 - 11.05	Welcome and short intro of Lorenz Technology
11.05 - 11.10	Lorenz AI-Link®, Lorenz Hive, drones and technology
11.10 - 11.25	Business case from Port Esbjerg (DK)
11.25 - 11.45	Q&A session

FlytNow / FlytBase webinars



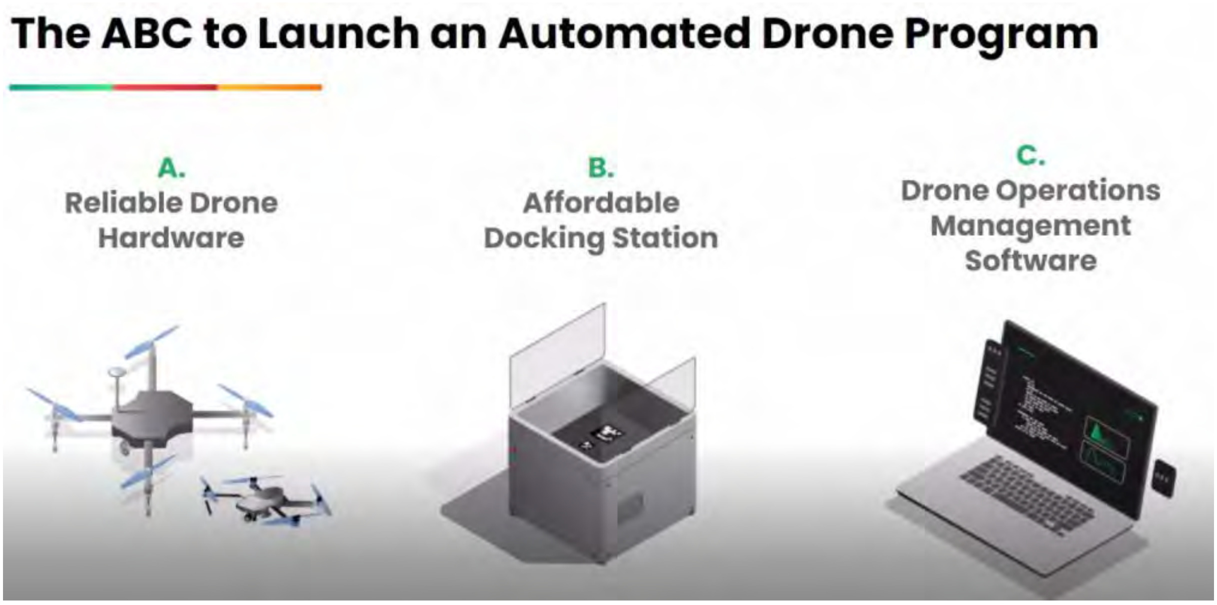
flytnow

Webinar

Launch your Automated Drone Program

using FlytNow & FoxIT DroneBase

4th May 2021

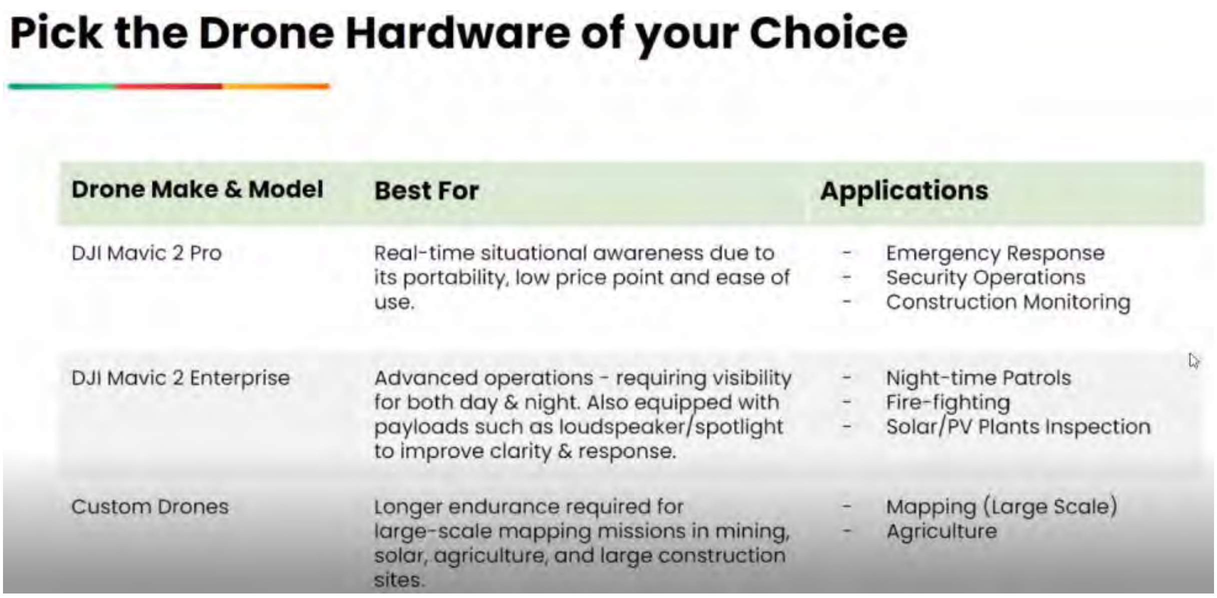


The ABC to Launch an Automated Drone Program

A.
Reliable Drone Hardware

B.
Affordable Docking Station

C.
Drone Operations Management Software



Pick the Drone Hardware of your Choice

Drone Make & Model	Best For	Applications
DJI Mavic 2 Pro	Real-time situational awareness due to its portability, low price point and ease of use.	- Emergency Response - Security Operations - Construction Monitoring
DJI Mavic 2 Enterprise	Advanced operations - requiring visibility for both day & night. Also equipped with payloads such as loudspeaker/spotlight to improve clarity & response.	- Night-time Patrols - Fire-fighting - Solar/PV Plants Inspection
Custom Drones	Longer endurance required for large-scale mapping missions in mining, solar, agriculture, and large construction sites.	- Mapping (Large Scale) - Agriculture

FoxIT Autonomous Drone Base Station

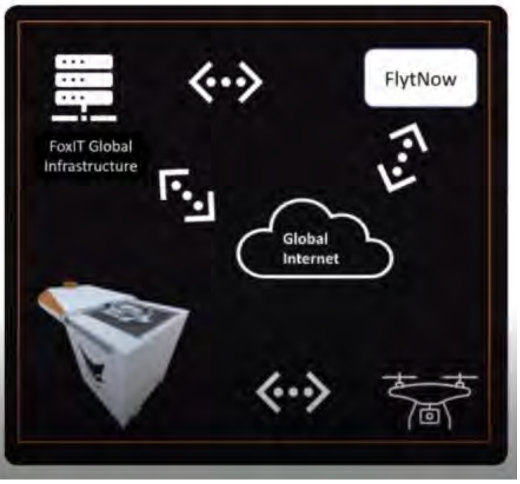
FoxIT Response Unit (RFU110)

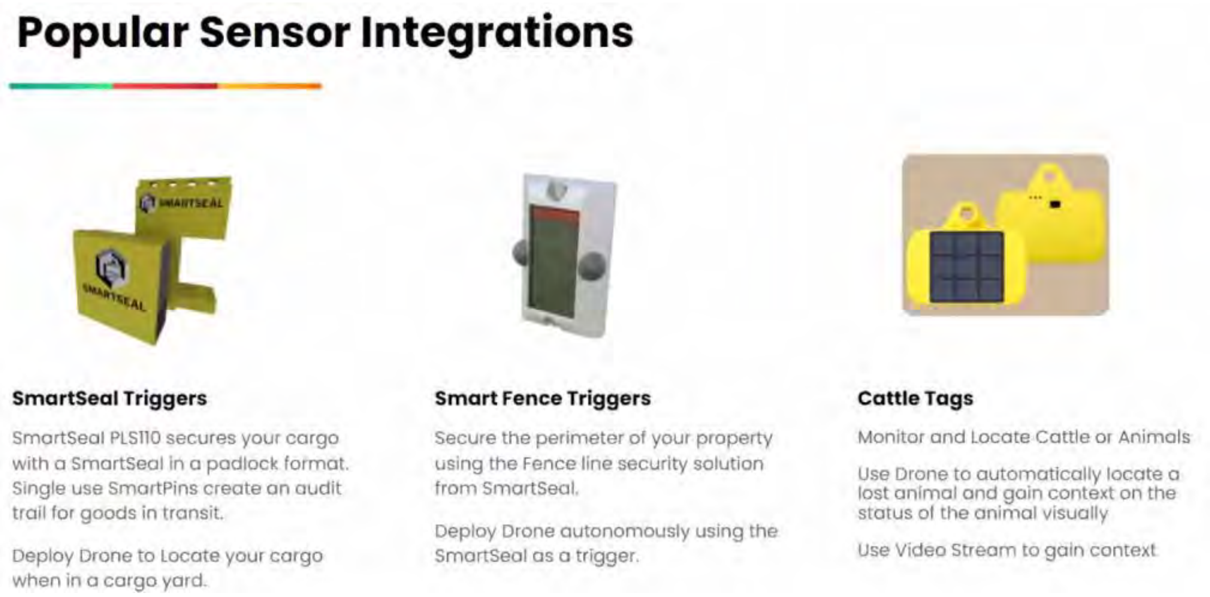
- Automated Drone Charging
- Automated Deployment and Precision Landing
- Native FlytNow integration built-in
- Built for rugged terrain (high heat environments)
- Anti-Theft System
- 12 months warranty and support (with options to extend)
- Estimated delivery of 3 months from date of order

FOXIT
FOXIT

Network Architecture

- FoxIT infrastructure is designed and engineered to be secure, fast, reliable and private.
- Each FoxIT Response Unit has a dedicated connection to our global infrastructure which allows for easy and secure communication between your drone, the FoxIT Response and almost any business application.
- FlytNow comes standard with all FoxIT Response units. A true plug n play solution for autonomous droning
- The FoxIT Response Unit uses any standard ethernet connection to gain access and supports full remote access from anywhere in the world using our secure global network





Popular Sensor Integrations

SmartSeal Triggers

SmartSeal PLS110 secures your cargo with a SmartSeal in a padlock format. Single use SmartPins create an audit trail for goods in transit.

Deploy Drone to Locate your cargo when in a cargo yard.

Smart Fence Triggers

Secure the perimeter of your property using the Fence line security solution from SmartSeal.

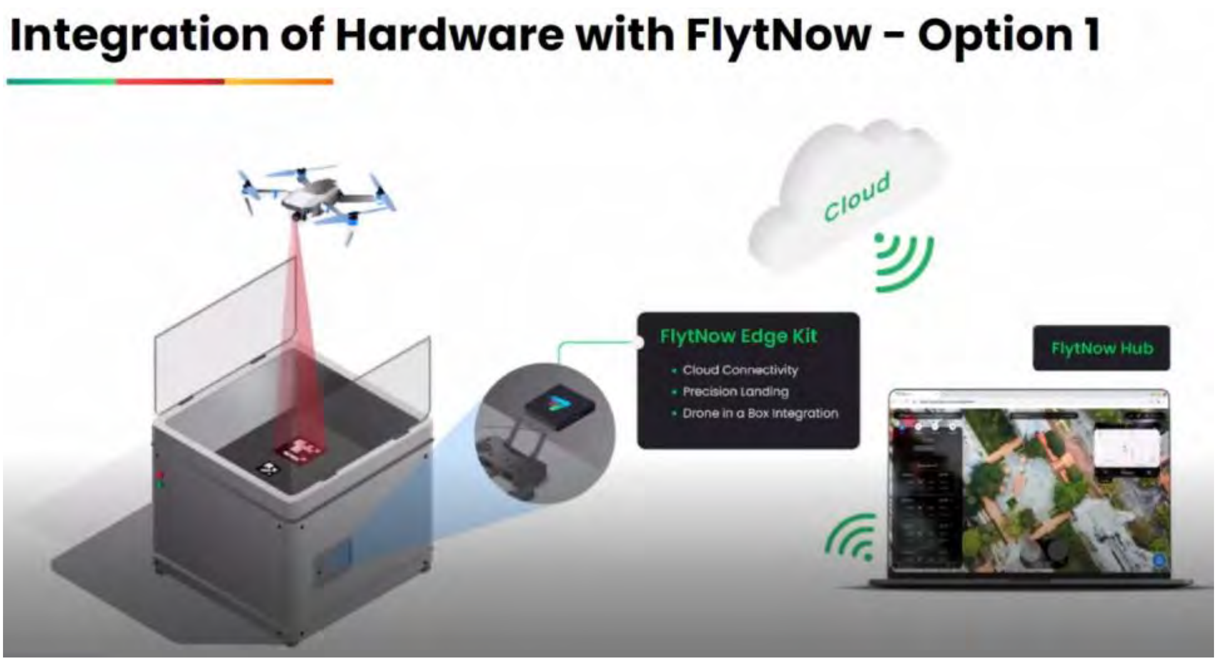
Deploy Drone autonomously using the SmartSeal as a trigger.

Cattle Tags

Monitor and Locate Cattle or Animals

Use Drone to automatically locate a lost animal and gain context on the status of the animal visually

Use Video Stream to gain context



Integration of Hardware with FlytNow - Option 1

FlytNow Edge Kit

- Cloud Connectivity
- Precision Landing
- Drone in a Box Integration

Drone-in-a-Box solutions

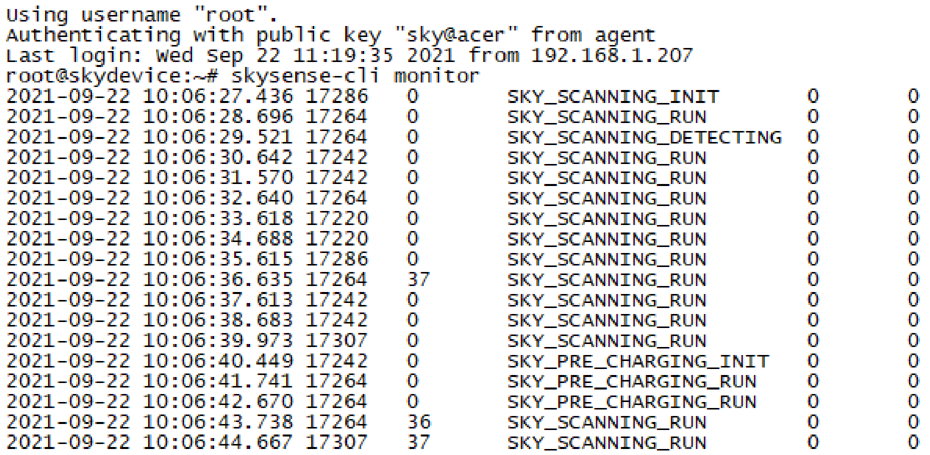
SkyCharge charging pad:

Please find the user's manual here: https://support.skycharge.de/docs/indoor-charging-pad

The installation guide of your Mavic kit can be found here: https://support.skycharge.de/docs/mavic-indoor

Attached you will find the API keys and the API documentation can be found here: https://support.skycharge.de/docs/api

SSH session to SkyCharge unit:



```
Using username "root".
Authenticating with public key "sky@acer" from agent
Last login: Wed Sep 22 11:19:35 2021 from 192.168.1.207
root@skydevice:~# skysense-cli monitor
2021-09-22 10:06:27.436 17286   0       SKY_SCANNING_INIT       0       0
2021-09-22 10:06:28.696 17264   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:29.521 17264   0       SKY_SCANNING_DETECTING  0       0
2021-09-22 10:06:30.642 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:31.570 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:32.640 17264   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:33.618 17220   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:34.688 17220   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:35.615 17286   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:36.635 17264   37      SKY_SCANNING_RUN        0       0
2021-09-22 10:06:37.613 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:38.683 17242   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:39.973 17307   0       SKY_SCANNING_RUN        0       0
2021-09-22 10:06:40.449 17242   0       SKY_PRE_CHARGING_INIT   0       0
2021-09-22 10:06:41.741 17264   0       SKY_PRE_CHARGING_RUN    0       0
2021-09-22 10:06:42.670 17264   0       SKY_PRE_CHARGING_RUN    0       0
2021-09-22 10:06:43.738 17264   36      SKY_SCANNING_RUN        0       0
2021-09-22 10:06:44.667 17307   37      SKY_SCANNING_RUN        0       0
```

Drone cyber security . SDR.

Open transmission on 2.5 GHz 5.7 GHz band . SDR with IP stack, SSL?

HackRF radio transceiver for 50$ to read Software Defined Radios channels.

HackRF One BUNDLE4
Metal case, Include TCXO Module Inside
3 Kinds of Antenna / 1PCS FM filter
HACKRF ONE
Filter
GSM/3G/4G
PiSwords
2.4G/5.8G

Vendor backdoors: DJI Aeroscope.

FlytNow – Drone Management as a Service web application .

FlytNow Auto+ Starter Kit Setup

FlytNow Auto+ Starter Kit Setup comes with a pre-installed FlytNow Edge application. The user does not have to download or install any modules or applications separately.

FlytNow Auto+ Starter Kit Connections

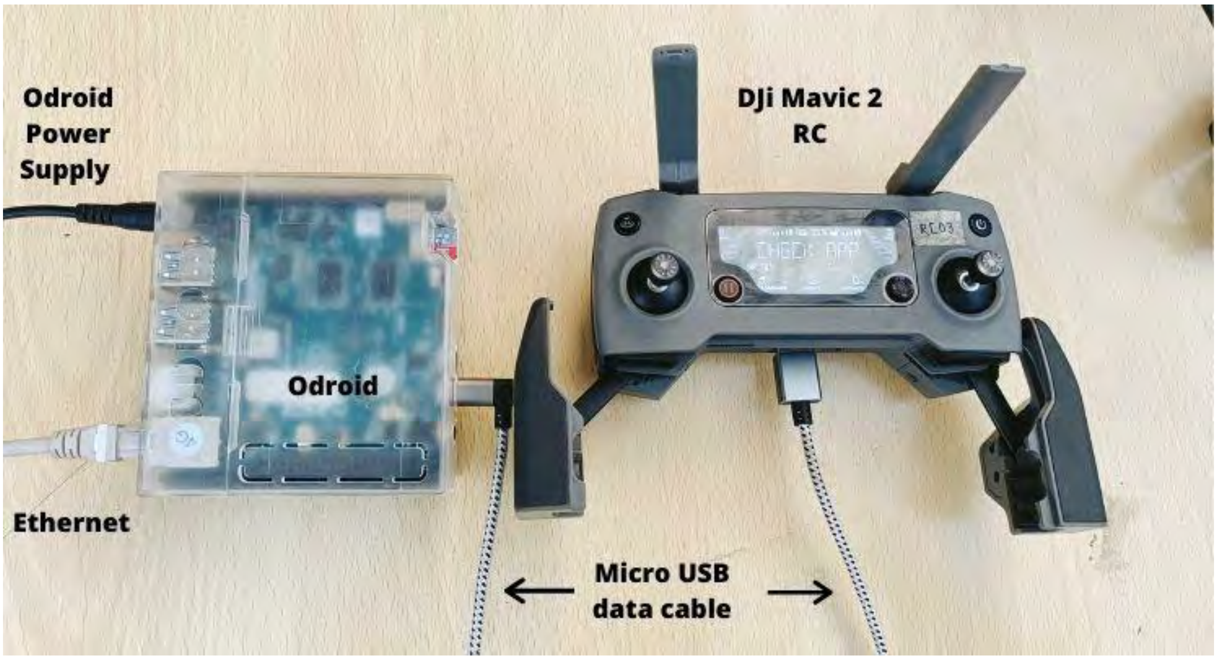
Follow these instructions to connect your DJI drone to the cloud using the FlytNow Edge application.

Connect the SBC (Odroid) to the internet via the ethernet cable.

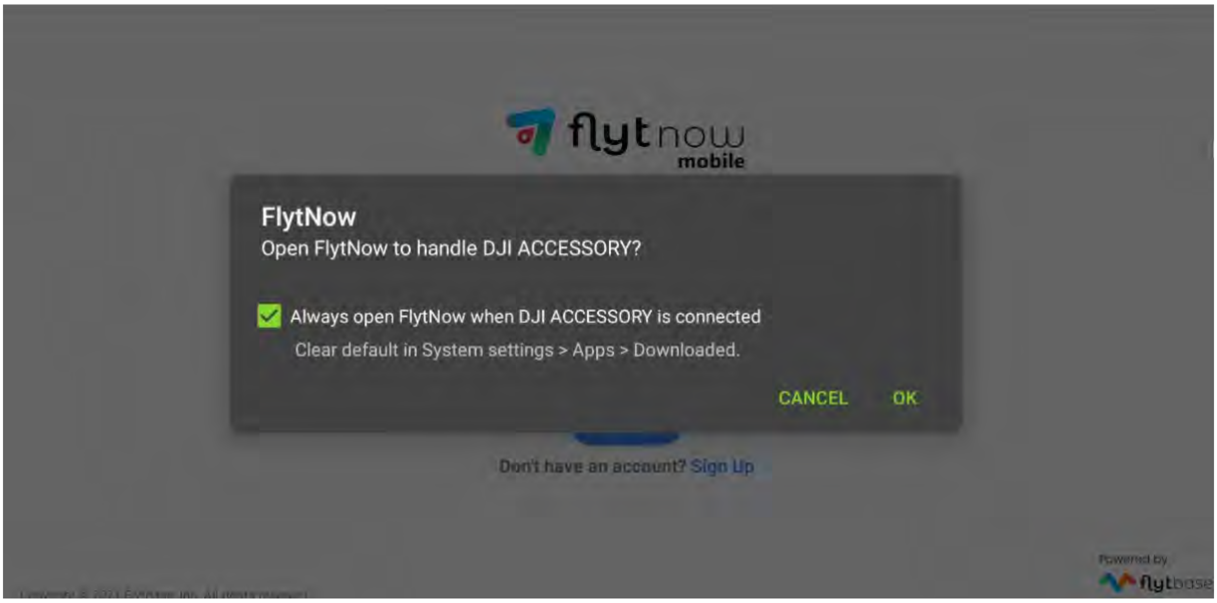
Connect Odroid to an HDMI screen, keyboard and mosue and power it up by connecting the power cable.

Connect the DJI RC to Odroid N2+ via the USB cable.

Now power up the system by connecting the power cable.



https://www.youtube.com/watch?v=MoZvSU9O0WA



flytnow mobile

FlytNow

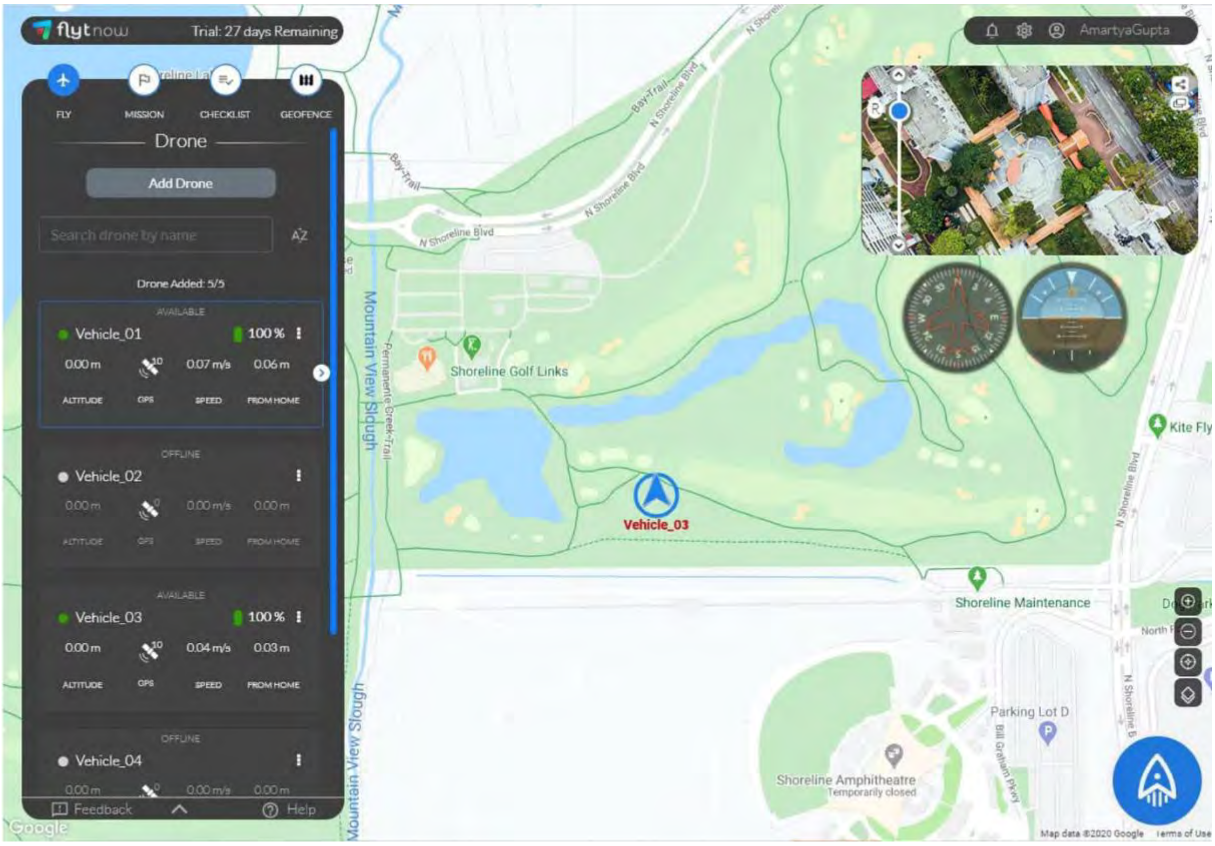
Open FlytNow to handle DJI ACCESSORY?

☑ Always open FlytNow when DJI ACCESSORY is connected

Clear default in System settings > Apps > Downloaded.

CANCEL OK

Don't have an account? Sign Up



flytnow Trial: 27 days Remaining

FLY MISSION CHECKLIST GEOFENCE

Drone

Add Drone

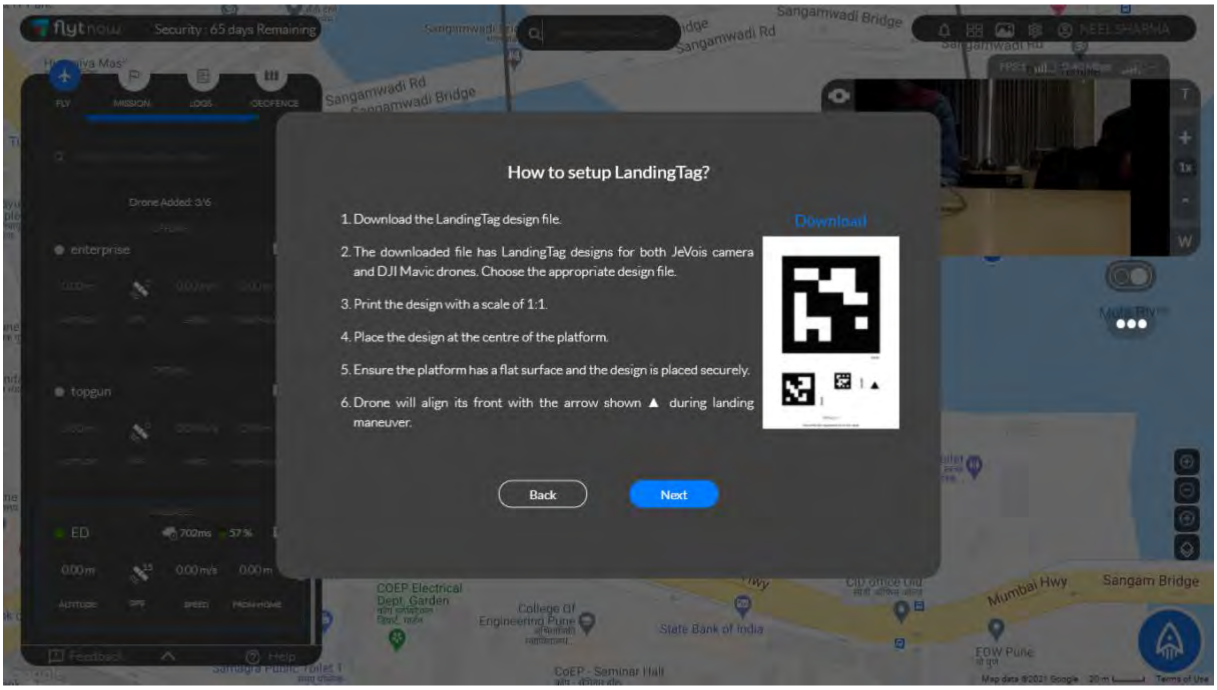
Search drone by name

Drone Added: 5/5

AVAILABLE			
● Vehicle_01		100 %	
0.00 m	10	0.07 m/s	0.06 m
ALTITUDE	GPS	SPEED	FROM HOME
OFFLINE			
● Vehicle_02			
0.00 m		0.00 m/s	0.00 m
ALTITUDE	GPS	SPEED	FROM HOME
AVAILABLE			
● Vehicle_03		100 %	
0.00 m	10	0.04 m/s	0.03 m
ALTITUDE	GPS	SPEED	FROM HOME
OFFLINE			
● Vehicle_04			
0.00 m	0	0.00 m/s	0.00 m

Feedback Help

Presision landing setup:

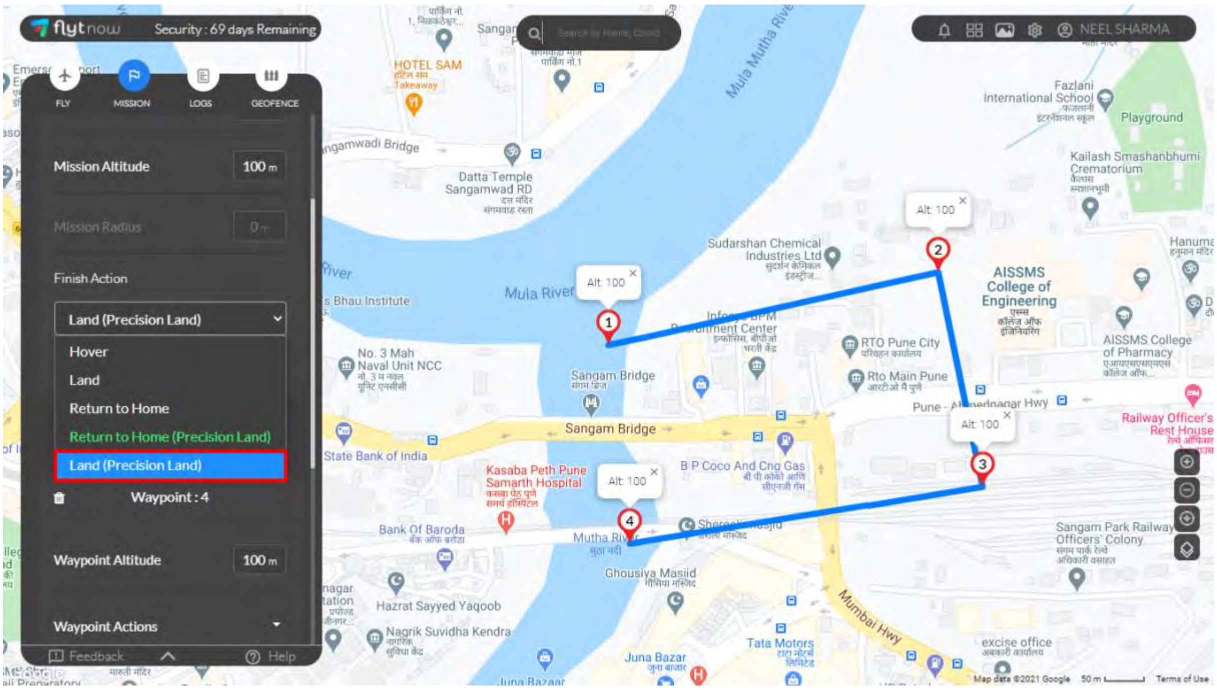


How to setup LandingTag?

1. Download the LandingTag design file. Download
2. The downloaded file has LandingTag designs for both JeVois camera and DJI Mavic drones. Choose the appropriate design file.
3. Print the design with a scale of 1:1.
4. Place the design at the centre of the platform.
5. Ensure the platform has a flat surface and the design is placed securely.
6. Drone will align its front with the arrow shown ▲ during landing maneuver.

Back Next

Precision landing action at the end of flight:



Mission Altitude 100 m

Mission Radius 0 m

Finish Action

Land (Precision Land)

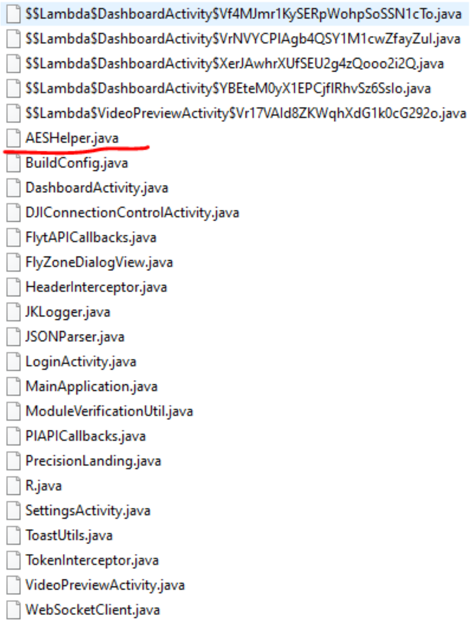
- Hover
- Land
- Return to Home
- Return to Home (Precision Land)
- Land (Precision Land)

Waypoint : 4

Waypoint Altitude 100 m

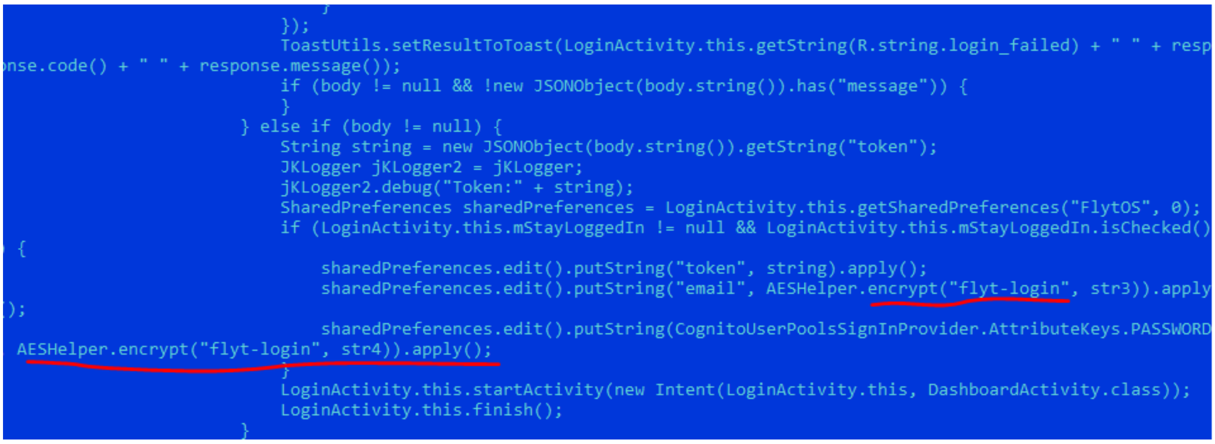
Waypoint Actions

FlyNow Android app source code analisys



$$Lambda$DashboardActivity$Vf4MJmr1KySERpWohpSoSSN1cTo.java
$$Lambda$DashboardActivity$VrNVYCPIAgb4QSY1M1cwZfayZul.java
$$Lambda$DashboardActivity$XerJAwhrXUfSEU2g4zQooo2i2Q.java
$$Lambda$DashboardActivity$YBEteM0yX1EPCjfIRhvSz6Sslo.java
$$Lambda$VideoPreviewActivity$Vr17VAId8ZKWqhXdG1k0cG292o.java
AESHelper.java
BuildConfig.java
DashboardActivity.java
DJIConnectionControlActivity.java
FlytAPICallbacks.java
FlyZoneDialogView.java
HeaderInterceptor.java
JKLogger.java
JSONParser.java
LoginActivity.java
MainApplication.java
ModuleVerificationUtil.java
PIAPICallbacks.java
PrecisionLanding.java
R.java
SettingsActivity.java
ToastUtils.java
TokenInterceptor.java
VideoPreviewActivity.java
WebSocketClient.java

Encryption code usage

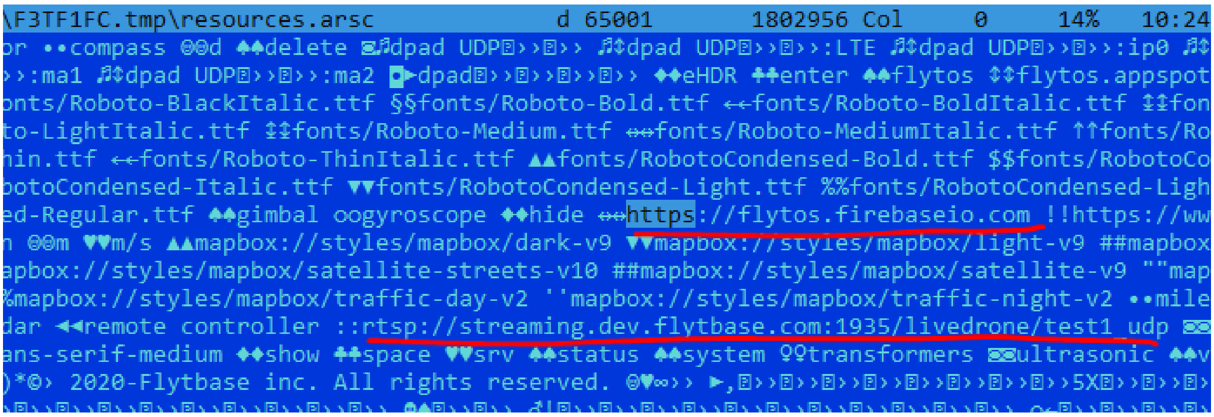


```
                            });
                            ToastUtils.setResultToToast(LoginActivity.this.getString(R.string.login_failed) + " " + resp
onse.code() + " " + response.message());
                            if (body != null && !new JSONObject(body.string()).has("message")) {
                            }
                        } else if (body != null) {
                            String string = new JSONObject(body.string()).getString("token");
                            JKLogger jKLogger2 = jKLogger;
                            jKLogger2.debug("Token:" + string);
                            SharedPreferences sharedPreferences = LoginActivity.this.getSharedPreferences("FlytOS", 0);
                            if (LoginActivity.this.mStayLoggedIn != null && LoginActivity.this.mStayLoggedIn.isChecked()
 {

                                sharedPreferences.edit().putString("token", string).apply();
                                sharedPreferences.edit().putString("email", AESHelper.encrypt("flyt-login", str3)).apply
);

                                sharedPreferences.edit().putString(CognitoUserPoolsSignInProvider.AttributeKeys.PASSWORD
 AESHelper.encrypt("flyt-login", str4)).apply();
                            }
                            LoginActivity.this.startActivity(new Intent(LoginActivity.this, DashboardActivity.class));
                            LoginActivity.this.finish();
                        }
```

String search in source code:



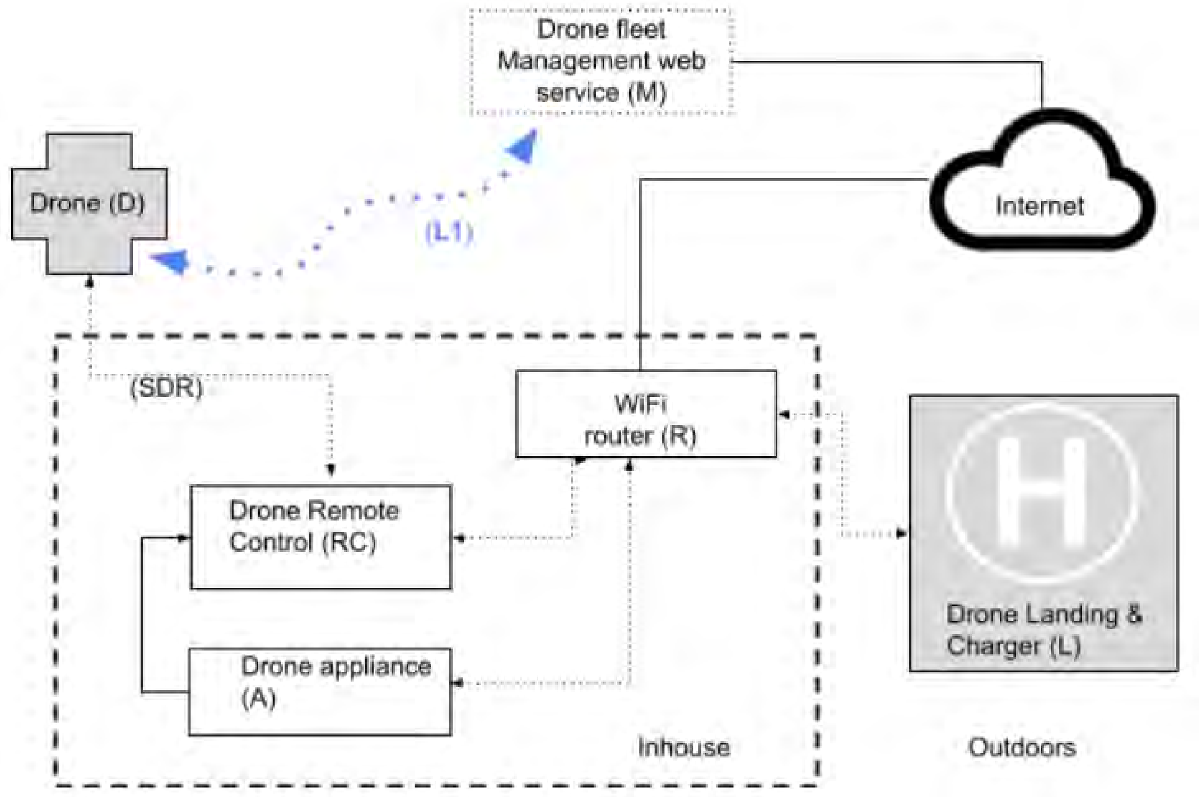
```
\F3TF1FC.tmp\resources.arsc                     d 65001         1802956 Col       0       14%     10:24
or ••compass ©©d ♠♠delete ◙♫dpad UDP⍰››⍰›› ♫⇕dpad UDP⍰››⍰››:LTE ♫⇕dpad UDP⍰››⍰››:ip0 ♫⇕
››:ma1 ♫⇕dpad UDP⍰››⍰››:ma2 ◘►dpad⍰››⍰››⍰››⍰›› ♦♦eHDR ♣♣enter ♠♠flytos ⇕⇕flytos.appspot
onts/Roboto-BlackItalic.ttf §§fonts/Roboto-Bold.ttf ←←fonts/Roboto-BoldItalic.ttf ↨↨fon
to-LightItalic.ttf ↨↨fonts/Roboto-Medium.ttf ↔↔fonts/Roboto-MediumItalic.ttf ↑↑fonts/Ro
hin.ttf ←←fonts/Roboto-ThinItalic.ttf ▲▲fonts/RobotoCondensed-Bold.ttf $$fonts/RobotoCo
botoCondensed-Italic.ttf ▼▼fonts/RobotoCondensed-Light.ttf %%fonts/RobotoCondensed-Ligh
ed-Regular.ttf ♠♠gimbal ○○gyroscope ♦♦hide ↔↔https://flytos.firebaseio.com !!https://ww
n ©©m ♥♥m/s ▲▲mapbox://styles/mapbox/dark-v9 ▼▼mapbox://styles/mapbox/light-v9 ##mapbox
apbox://styles/mapbox/satellite-streets-v10 ##mapbox://styles/mapbox/satellite-v9 ""map
%mapbox://styles/mapbox/traffic-day-v2 ''mapbox://styles/mapbox/traffic-night-v2 ••mile
dar ◄◄remote controller ::rtsp://streaming.dev.flytbase.com:1935/livedrone/test1_udp ◙◙
ans-serif-medium ♦♦show ♣♣space ♥♥srv ♠♠status ♠♠system ♀♀transformers ◙◙ultrasonic ♠♠v
)*©› 2020-Flytbase inc. All rights reserved. ©♥∞›› ►,⍰››⍰››⍰››⍰››⍰››⍰››⍰››⍰››5X⍰››⍰››⍰›
```

Drone Management System. Security analisys

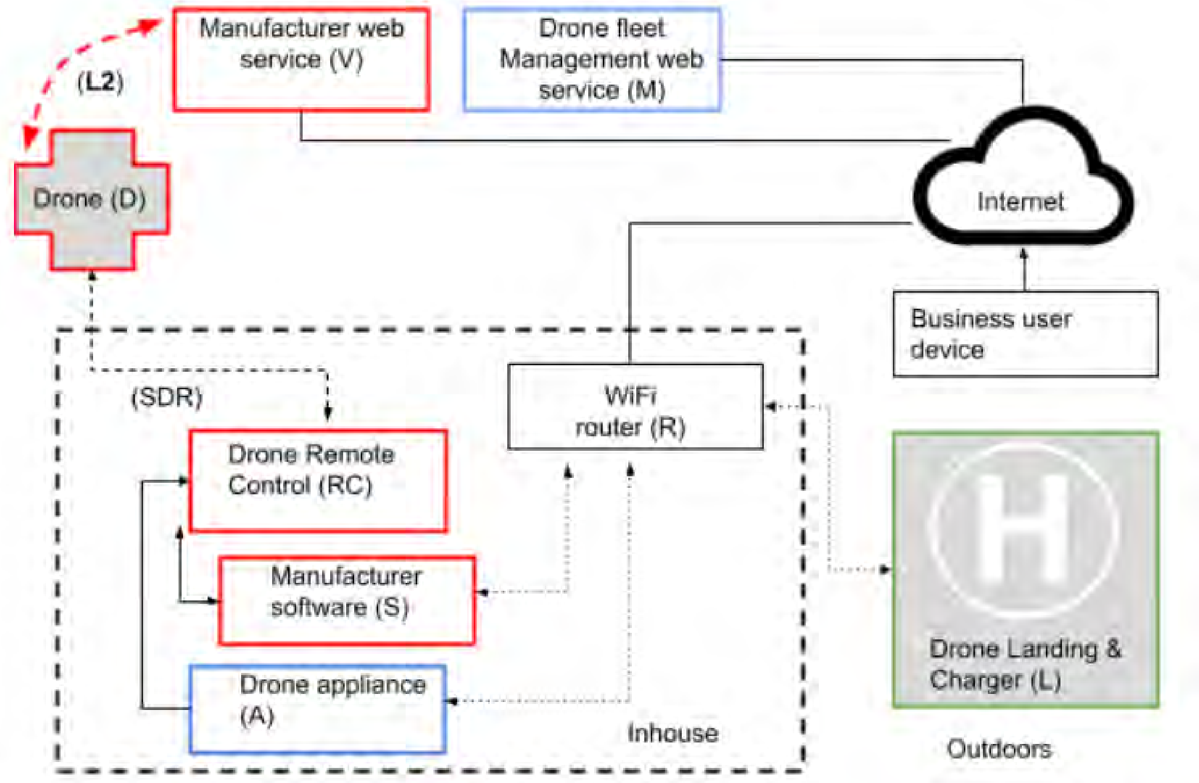
System components and STRIDE

Asset	**S**	**T**	**R**	**I**	**D**	**E**
Drone (D)	X	X		X	X	X
Remote Control (RC)		X			X	
Software (S)				X		X
Appliance (A)	X			X		X
Drone management web service (M)	X	X	X	X	X	X
Manufacturer web service (V)	X	X	X	X	X	X
Charge station (L)				X	X	X
Business user workstation (W)	X		X	X		

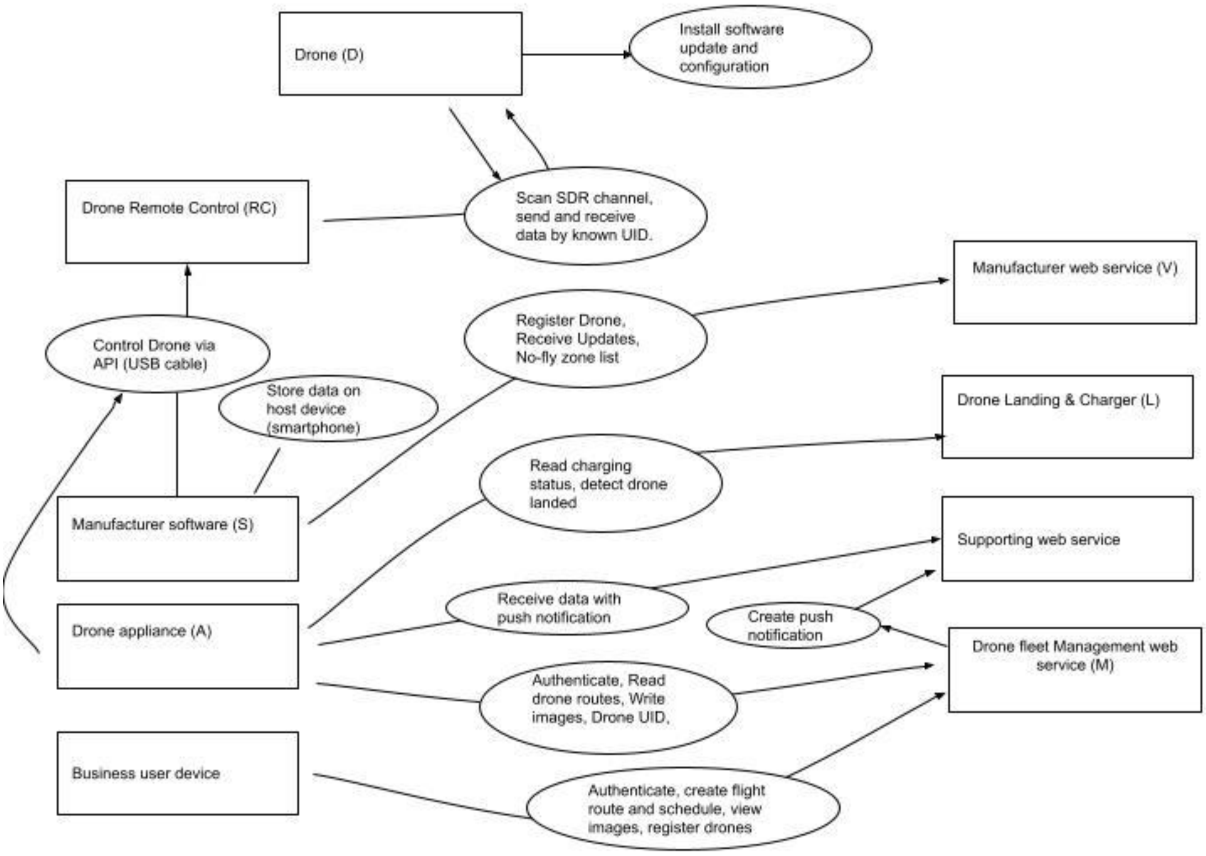
Architecture diagram


Drone fleet Management web service (M)
Drone (D)
(L1)
Internet
(SDR)
WiFi router (R)
Drone Remote Control (RC)
Drone appliance (A)
Drone Landing & Charger (L)
Inhouse
Outdoors

Data Flow diagram:


Manufacturer web service (V)
Drone fleet Management web service (M)
(L2)
Drone (D)
Internet
Business user device
(SDR)
WiFi router (R)
Drone Remote Control (RC)
Manufacturer software (S)
Drone appliance (A)
Drone Landing & Charger (L)
Inhouse
Outdoors

Use cases diagram :


Drone (D)
Install software update and configuration
Drone Remote Control (RC)
Scan SDR channel, send and receive data by known UID.
Manufacturer web service (V)
Register Drone, Receive Updates, No-fly zone list
Control Drone via API (USB cable)
Store data on host device (smartphone)
Drone Landing & Charger (L)
Read charging status, detect drone landed
Manufacturer software (S)
Supporting web service
Receive data with push notification
Create push notification
Drone appliance (A)
Drone fleet Management web service (M)
Authenticate, Read drone routes, Write images, Drone UID,
Business user device
Authenticate, create flight route and schedule, view images, register drones