TÉCNICO LISBOA

ANTI-DRONE

Detection for Communication Jamming System for Security Forces

Guilherme Martins 106274
Afonso de Mello 107495
Guilherme Luís 106755
Francisco Rodrigues 106695
João Firmino 107485
Rodrigo Sanguino 84342

MEET THE TEAM

Guilherme Martins 106274

Team Leader/Project Manager

Afonso de Mello 107495

R&D Enginner

Guilherme Luís 106755

Systems Analyst

Francisco Rodrigues 106695

Technical Lead

João Firmino 107485

Software Developer

Rodrigo Sanguino 84342

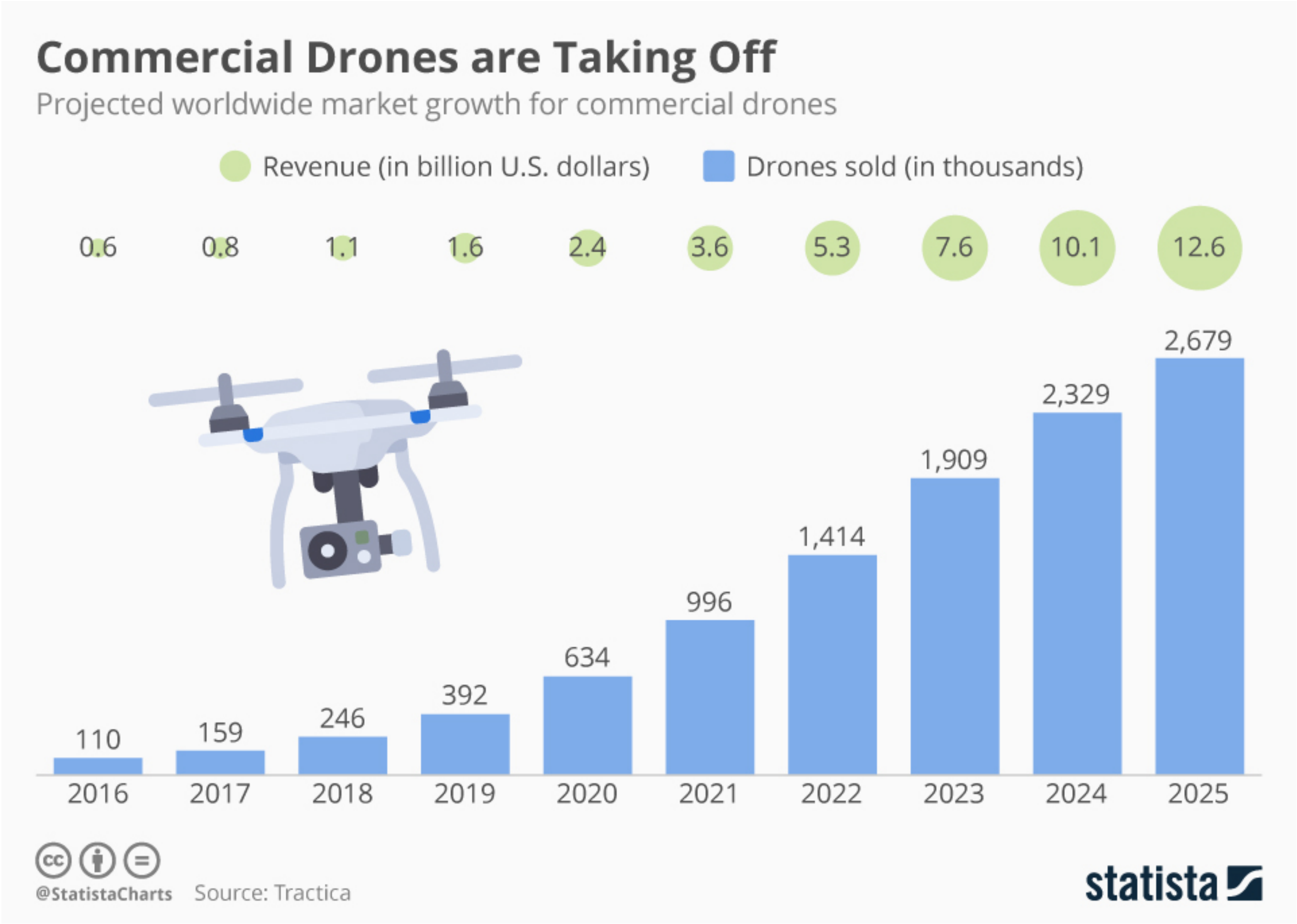
Embedded Systems Engineer

1. ADVISORS AND MENTOR

- Scientific Advisor: Tenente Coronel João Boita
- Scientific Co-advisor: Major Machado; Major Pagaimo
- Coordinator: Prof. João Felício
- Co-coordinator: Prof. Emmanuel Cruzeiro
- Mentor: Prof. João Gonçalves

2. PROBLEM DEFINITION

2. PROBLEM DEFINITION

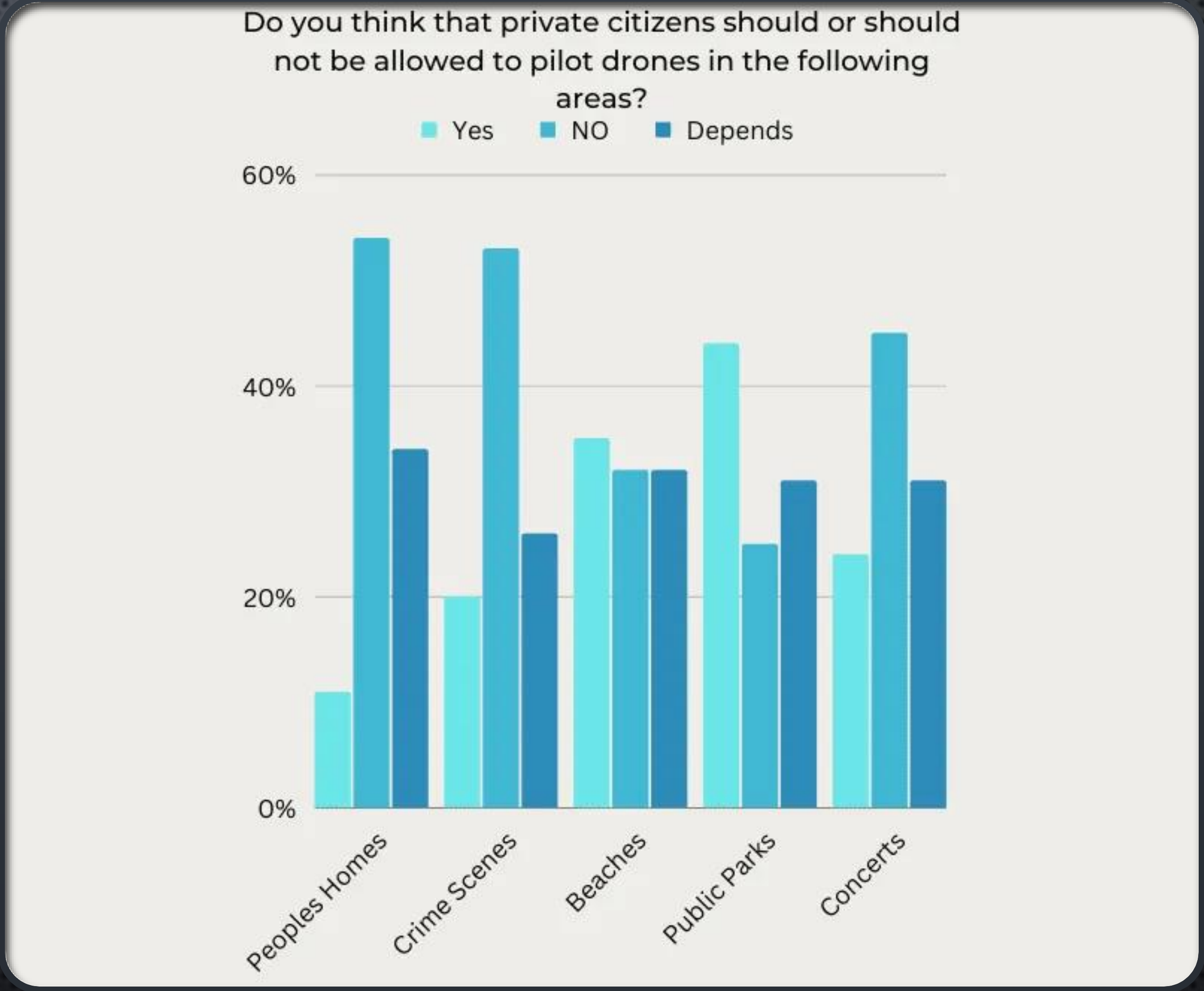


GROWTH OF DRONE USAGE

Drones have gained widespread use for a variety of applications, from recreational flying to industrial uses like surveillance, monitoring, and package delivery.

UNAUTHORIZED SURVEILLANCE OF PRIVATE AREAS

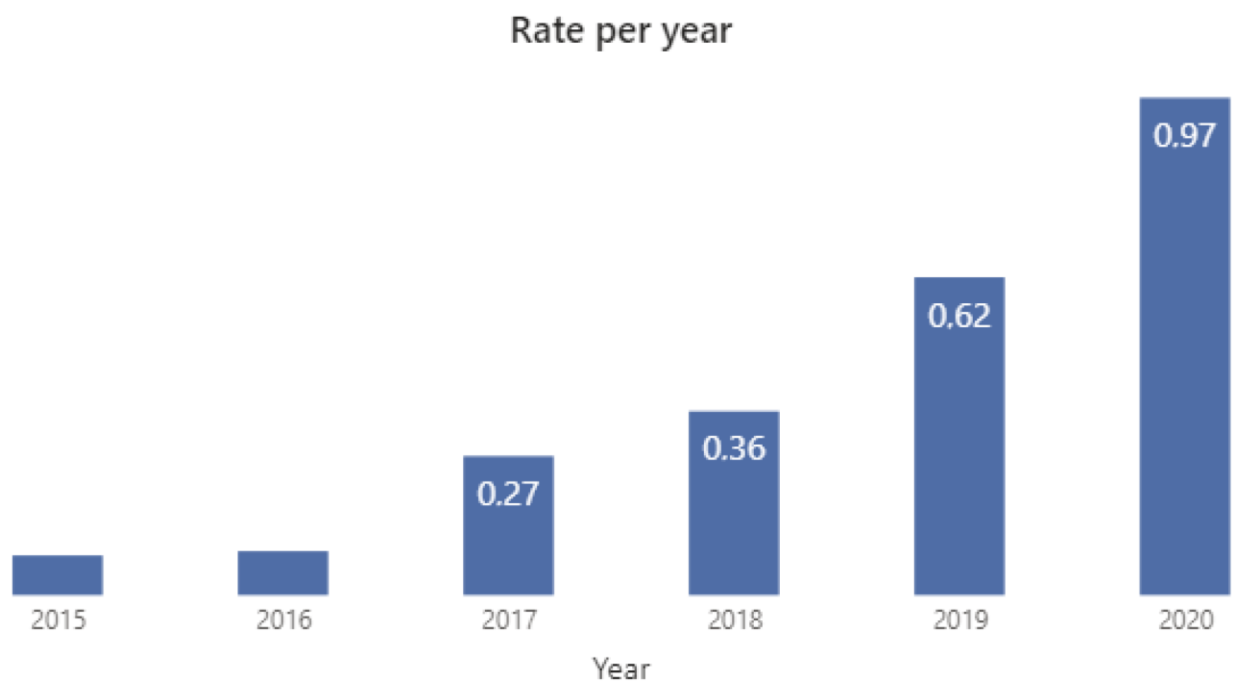
Drones increasing use has also led to significant security concerns. Unauthorized drones, especially those used for illegal surveillance or nefarious purposes, pose a threat to privacy, security, and public safety.



DRONE INTRUSIONS AND SECURITY THREATS

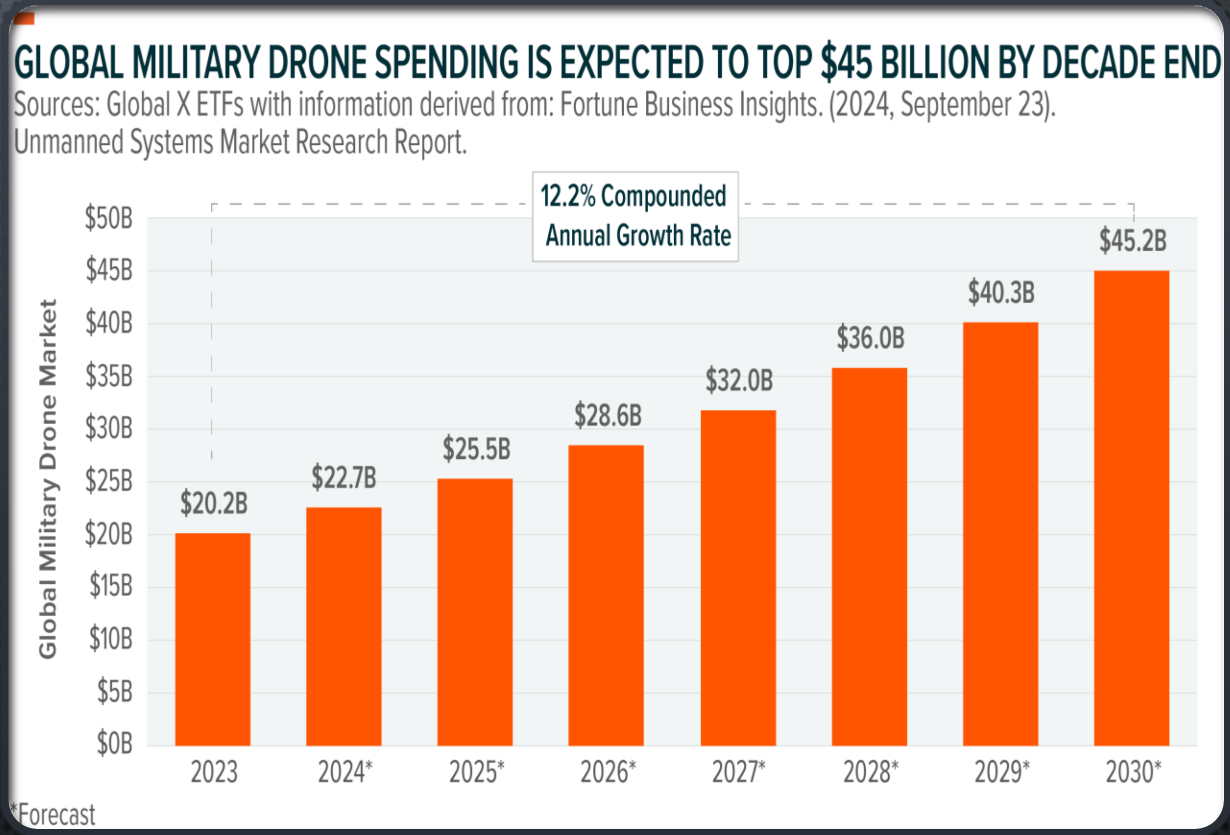
Security forces are often ill-equipped to detect and neutralize these unmanned aerial vehicles (UAVs), which can be difficult to track due to their small size, mobility, and the use of secure communication channels. This makes it challenging to prevent potential risks such as espionage, smuggling, or even terrorist attacks.

Yearly number of drone intrusion in Italian airports per 10,000 airport movements.



2. PROBLEM DEFINITION

The challenge is to develop an innovative system that allows security agencies to detect the presence of unauthorized drones in restricted or sensitive areas. Additionally, the system must be capable of directing interfering signals with the drone’s communication signals, particularly radio-frequency signals, to prevent the drone from transmitting or receiving control commands. This would enable security forces to gain control of the situation and mitigate the potential threat posed by rogue drones. A system that effectively combines detection, tracking, and jamming technologies could be a game-changer in improving national and public security efforts.



3. SOLUTION BENEFICIARIES

3. SOLUTION BENEFICIARIES

Security Agencies

Security forces, military personnel, and border control entities that need to protect restricted or high-risk areas against drone incursions

3. SOLUTION BENEFICIARIES

Governmental institutions

Authorities responsible for overseeing national security, airports, government buildings, and sensitive locations

3. SOLUTION BENEFICIARIES

Private Sector

Organizations and industries concerned with protecting infrastructure, assets, and sensitive data from unauthorized aerial surveillance

THALES

GRUPO EULEN

TEKEVER

Connect Robotics

SwAtter

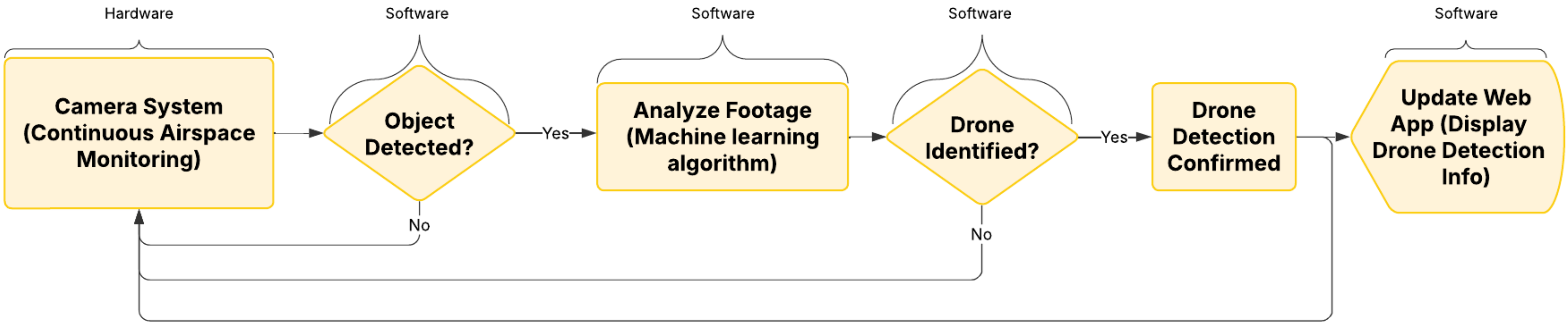
4. TECHNOLOGICAL SOLUTION

Drone Detection Systems: Radar, optical sensors (such as cameras and infrared systems), acoustic sensors and Rf Receivers to visually detect and track drones.

Machine Learning Algorithms: To distinguish drones from other flying objects, such as birds, based on detected video.

Anti-Drone

Detection For Communication Jamming System For Security Forces



4. TECHNOLOGICAL SOLUTION

5. COMPETITORS AND PREVIOUS WORK

Currently, several solutions exist, including manual drone detection using radar systems, acoustic sensors, and optical cameras. Some systems attempt to jam the communication signals of drones, using RF (radio-frequency) jamming to disrupt their control and navigation. However, these solutions tend to have limitations, including short detection ranges, difficulty in distinguishing between authorized and unauthorized drones, and challenges in legally operating RF jammers due to regulatory restrictions in many countries. Some anti-drone solutions also require significant infrastructure investment and integration, making them difficult to deploy on a wide scale. While there are commercial systems available, they are typically expensive, bulky, and may not be easily adaptable to different security needs.

SOME PREVIOUS SOLUTIONS:

NQ Defense ND-BD004

Handheld Anti-Drone Jammer

AARTOS Radar Detection

Drone Radar Detection

Detection Radar IRIS

Drone Radar Detection

6. SOLUTION REQUIREMENTS

As part of this project, we decided to focus on drone detection by implementing a system based on **computer vision**. The core of our solution involves using cameras in continuous operation, which, through **machine learning algorithms**, will analyze the images to determine whether an airborne object is a drone. This approach enables the system to distinguish drones from other flying objects, such as birds or civilian aircraft. To maximize coverage and accuracy, we plan to use either two cameras or a single wide-angle 180° camera to capture the entire field of view.

To enhance usability, we will also develop a web application that allows users to monitor the system's status in real time. This platform will provide a live overview of detected objects, as well as display the total number of drones identified by the system.

If necessary, we may also explore the integration of complementary detection systems, such as radars and acoustic sensors. Additionally, if time permits, we may begin exploring potential techniques to jam the drone’s communication signals as a next step in enhancing the system’s capabilities.

6. SOLUTION REQUIREMENTS

COMPONENTS REQUIRED

Raspberry Pi

Cameras

Arduino Uno

9. TECHNICAL CHALLENGES

Technical challenges in a project refer to the difficulties and obstacles encountered when designing, developing, and implementing a solution. These challenges can arise from hardware limitations, software constraints, integration complexities, scalability issues, or performance optimization. Addressing them often requires innovative problem-solving, rigorous testing, and iterative improvements. Identifying and mitigating these challenges early in the development process is crucial to ensuring a successful outcome. We have identified four main technical challenges:

7. TECHNICAL CHALLENGES

Detection Range

The maximum distance at which the system can accurately detect and identify a drone in each environment. This is a crucial metric for assessing the effectiveness of the detection system

7. TECHNICAL CHALLENGES

False Positive Rate

The rate at which the system incorrectly identifies non-threatening objects as drones. A lower rate indicates a more reliable and accurate detection system

7. TECHNICAL CHALLENGES

Adaptability

↓

The system's ability to handle different types of drones and environments and ensure it is versatile and reliable under different operational conditions

7. TECHNICAL CHALLENGES

Machine Learning Algorithm Training

The main challenge in training a machine learning software to detect drones by video lies in the variability of environmental conditions, the visual similarity between drones and other flying objects, and the need for a large labeled dataset to ensure high accuracy.

8. PARTNERS

- Força Aérea - Expertize
- Thales - Know-How
- Mauser - Components

9. Testing and Validation Metrics

To evaluate the performance of our system, we plan to conduct tests either in a large open field or within a designated area at an Air Force facility, for which we have already obtained authorization. The testing process will be divided into five key stages, each designed to assess a critical aspect of the system's performance:

1. DETECTION ACCURACY AND FALSE POSITIVES RATE

IN THE FIRST STAGE, WE WILL INTRODUCE VARIOUS OBJECTS INTO THE DETECTION AREA, INCLUDING DRONES, BIRDS, AND OTHER AIRBORNE ELEMENTS. BY ANALYZING THE SYSTEM'S RESPONSES, WE WILL VERIFY ITS ABILITY TO ACCURATELY DISTINGUISH DRONES FROM NON-THREATENING OBJECTS. TO CALCULATE THE FALSE POSITIVE RATE, WE WILL COMPARE THE NUMBER OF INCORRECTLY IDENTIFIED OBJECTS WITH THE TOTAL NUMBER OF OBJECTS DETECTED DURING THE TEST. THIS TEST WILL INVOLVE SIMULATING REALISTIC CONDITIONS TO EVALUATE THE SYSTEM'S RELIABILITY AND ENSURE MINIMAL FALSE POSITIVES.

MAX FALSE POSITIVE RATE: 25%

9. Testing and Validation Metrics

2. Detection Range

Next, we will conduct multiple drone flights at varying altitudes and distances to determine the maximum range at which the system can effectively detect a drone. We will document the maximum distance, measured in meters, at which the system correctly identifies the drone. This test is essential for understanding the system's operational limits and ensuring it can be deployed in diverse security scenarios.

Min Range: 2m

3. Drone Compatibility

After that, we will test the system's ability to detect different drone models. This will involve flying drones of various sizes and brands through the detection area to confirm that the system is not limited to specific models. Ensuring broad compatibility will make the system more versatile and effective in real-world applications.

9. Testing and Validation Metrics

4. Latency

A crucial aspect of our system's performance is its response time, or latency, which refers to the time it takes for the system to detect a drone after it has entered the detection area. To assess this, we will measure the time in seconds from when a drone enters the radar's line of sight until the system confirms the detection of the drone. This test will help us understand how quickly the system can react to threats and ensure that there is minimal delay between detection and confirmation, an important factor in real-time security scenarios.

Max Latency: 10s

5. Maximum Number of Drones

Finally, another key test will involve evaluating the system's ability to detect multiple drones simultaneously. In real-world applications, it is likely that multiple drones could be detected at once, and our system must be able to handle such scenarios efficiently. To test this, we will deploy two drones at the same time within the detection area and assess the system's ability to identify both drones simultaneously. This will ensure that the system remains functional and effective even in crowded airspaces, where multiple threats could be present at once.

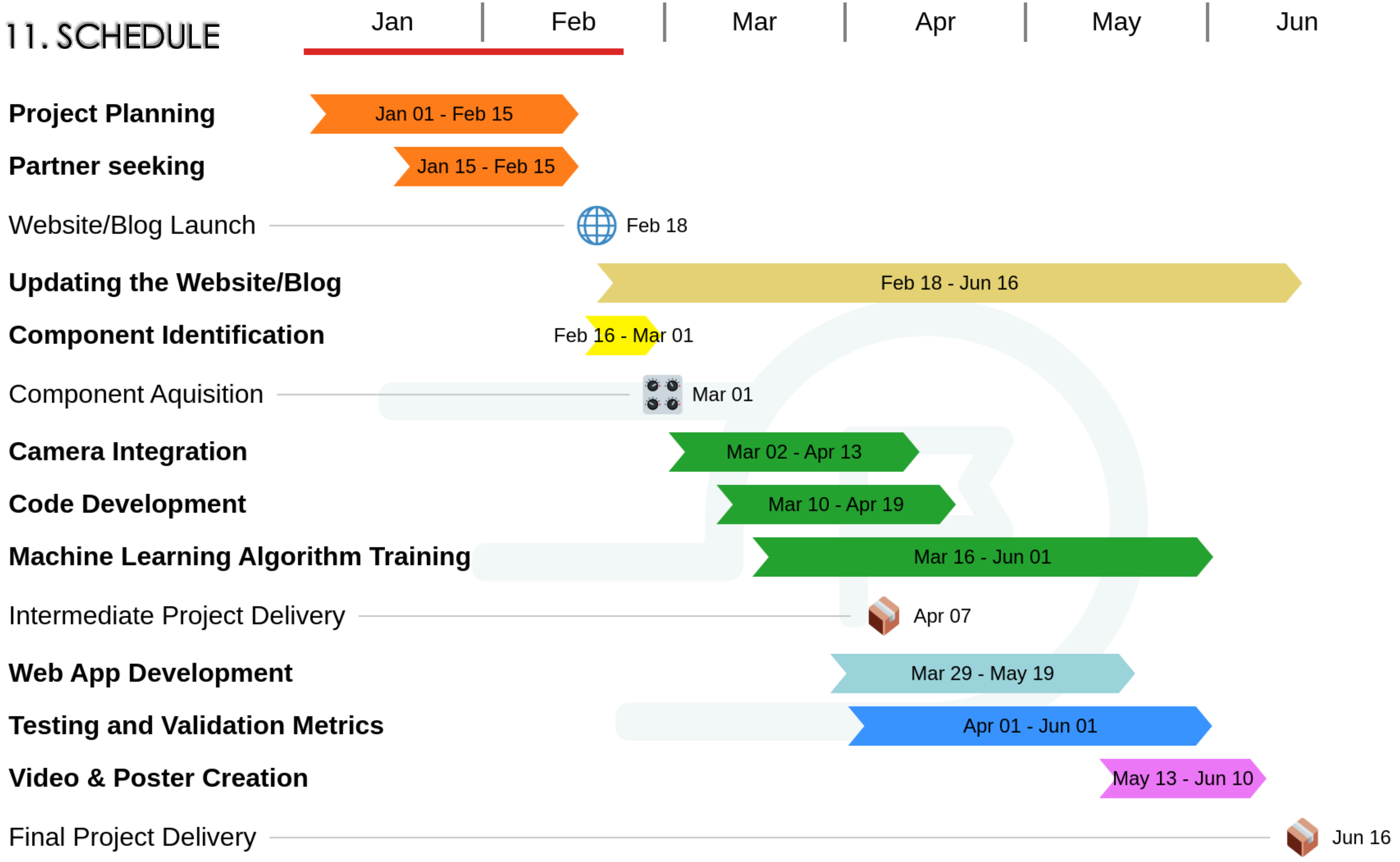
10. DIVISION OF LABOR (I)

Guilherme Martins	Francisco Rodrigues	João Firmino
Management and coordination	Research and initial Study	Research and initial Study
Engagement with Partners	Radar and Arduino Integration	Website Development
Documentation, Video and Poster making	Camera Integration	Code Development
Radar and Arduino Integration	Management	Web-App Development

10. DIVISION OF LABOR (II)

Afonso de Mello	Guilherme Luis	Rodrigo Sanguino
Research and initial Study	Theoretical Analysis	Research and initial Study
Engagement with Partners	Finance	Prototype testing
Radar and Arduino Integration	Testing Analysis	Code Development
Camera Integration		

11. SCHEDULE



Jan
Feb
Mar
Apr
May
Jun
Project Planning
Jan 01 - Feb 15
Partner seeking
Jan 15 - Feb 15
Website/Blog Launch
Feb 18
Updating the Website/Blog
Feb 18 - Jun 16
Component Identification
Feb 16 - Mar 01
Component Aquisition
Mar 01
Camera Integration
Mar 02 - Apr 13
Code Development
Mar 10 - Apr 19
Machine Learning Algorithm Training
Mar 16 - Jun 01
Intermediate Project Delivery
Apr 07
Web App Development
Mar 29 - May 19
Testing and Validation Metrics
Apr 01 - Jun 01
Video & Poster Creation
May 13 - Jun 10
Final Project Delivery
Jun 16