

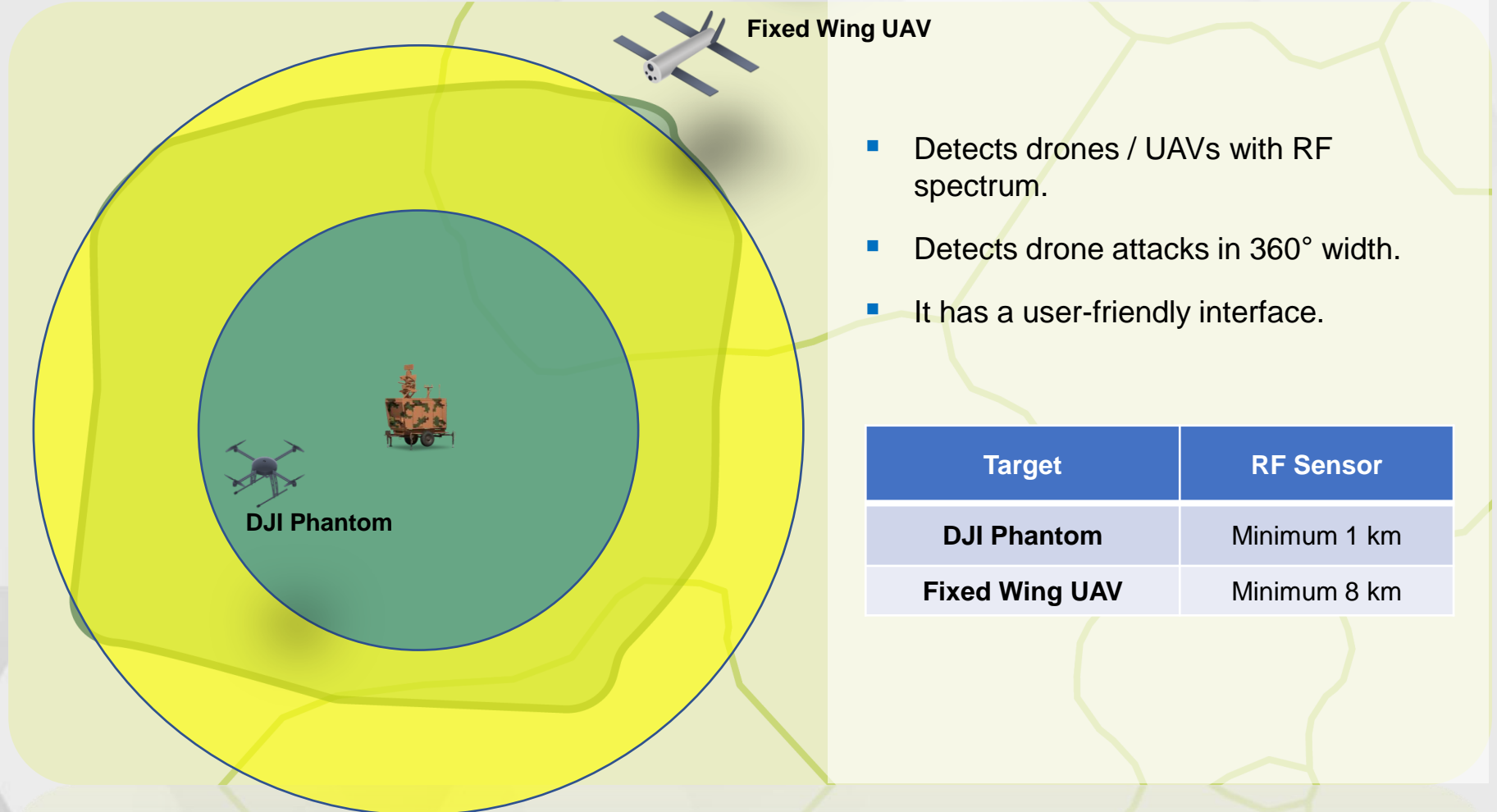


ILTERMIRKAS

Mobile High Power GNSS Spoofing
and ISM Jamming System



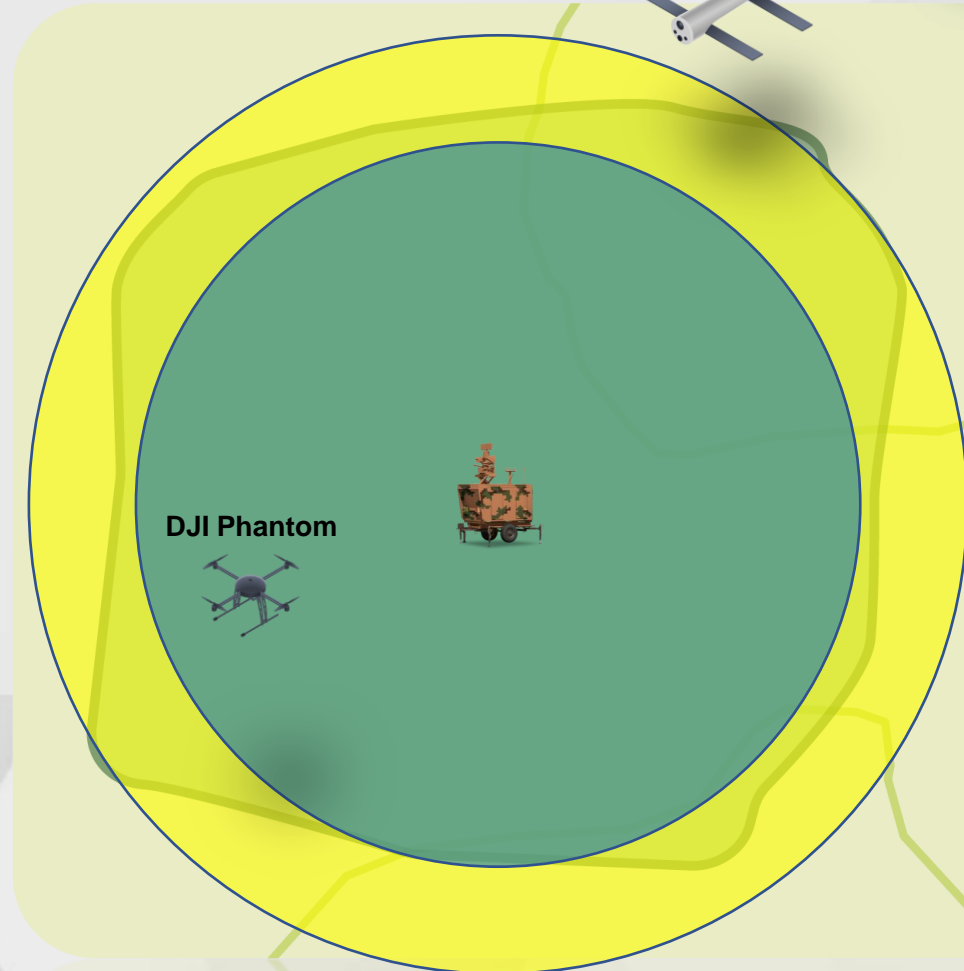
Detection Scenario (RF Sensor)



- Detects drones / UAVs with RF spectrum.
- Detects drone attacks in 360° width.
- It has a user-friendly interface.

Target	RF Sensor
DJI Phantom	Minimum 1 km
Fixed Wing UAV	Minimum 8 km

Detection Scenario (RADAR)



Fixed Wing UAV

- Detects Unmanned Aerial Vehicles / UAVs with RADAR.
- Detects drone attacks in 360° width.
- It has a user-friendly interface.

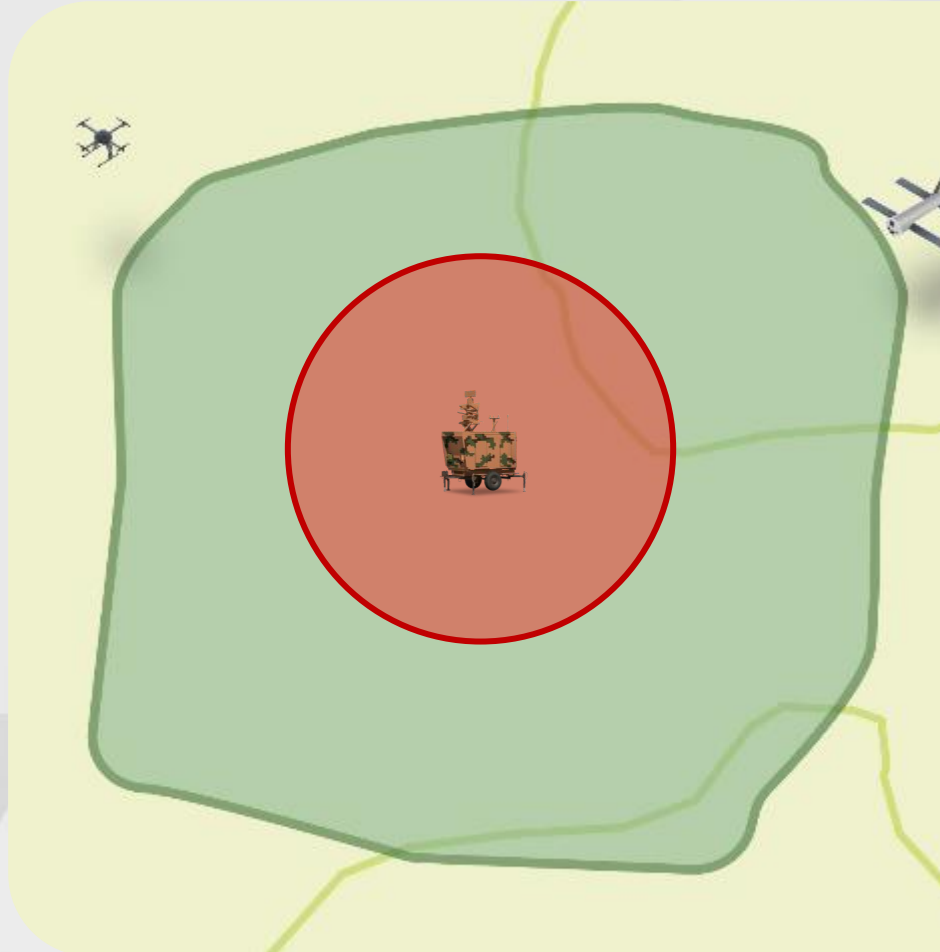
Detection Range	
Micro UAV	5,5 km RCS 0,01 m2
Fixed Wing UAV	10 km RCS 0,1 m2
Mini UAV	10 km on RCS 0,5 m2
Small UAV	15-20 km on RCS 1 m2
Vehicle	15-20 km on RCS \geq 2 m2

Protocol Based Detection System



- **Protocol based detection technology**
- **Passive RF detection**
- **Distinguishing friend and foe according to drone ID**
- **Detection of remote control and drone location info and positioning on the map**
- **Drone information tracking, displaying past track records**
- **Extendible library with AI**
- **Polygon definition on the map (Critical area)**
- **ADS-B Feature**

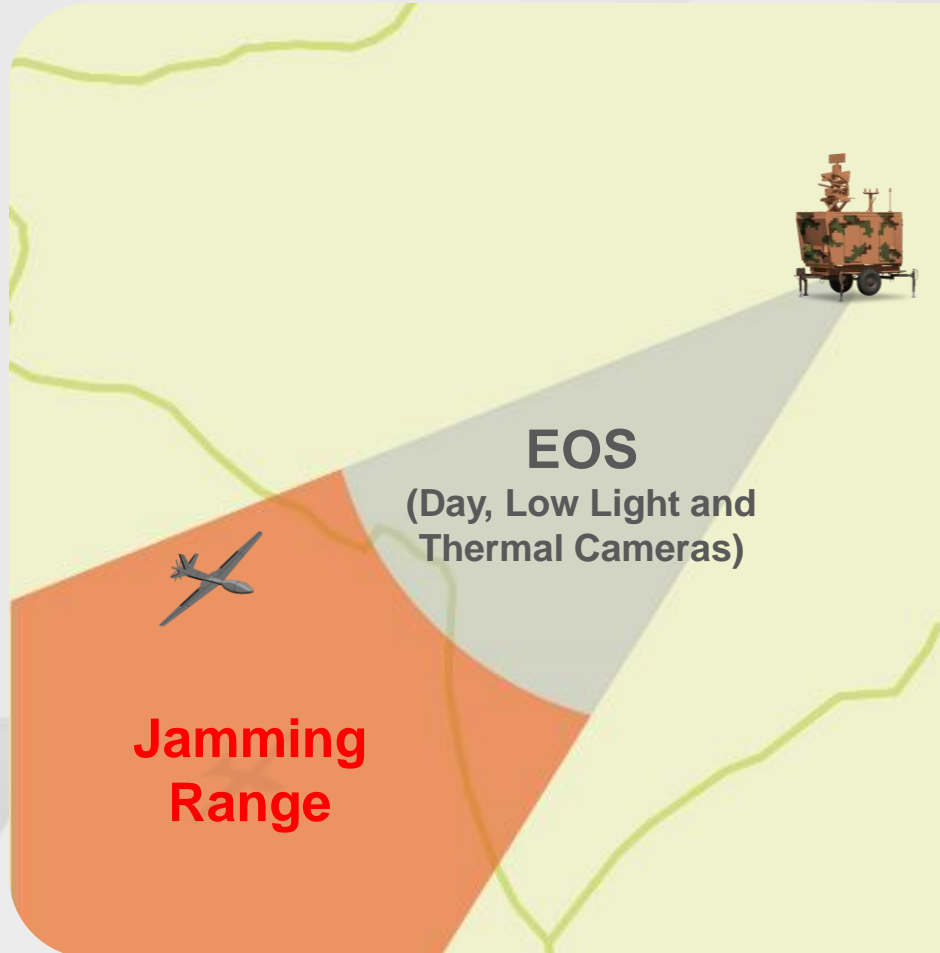
Jamming Scenario (360° Omni Antenna)



- 360° jamming against multiple UAV/drone attacks.
- With its 360° omni antenna, jams GNSS frequency bands up to 10 km.
- 360° jamming on HF and VHF frequencies.

Minimum 1:1 jamming distance	
Remote Controller Distance	Blocking Distance
1500 m	750 m
3000 m	1500 m

Jamming Scenario (Directional Antenna)

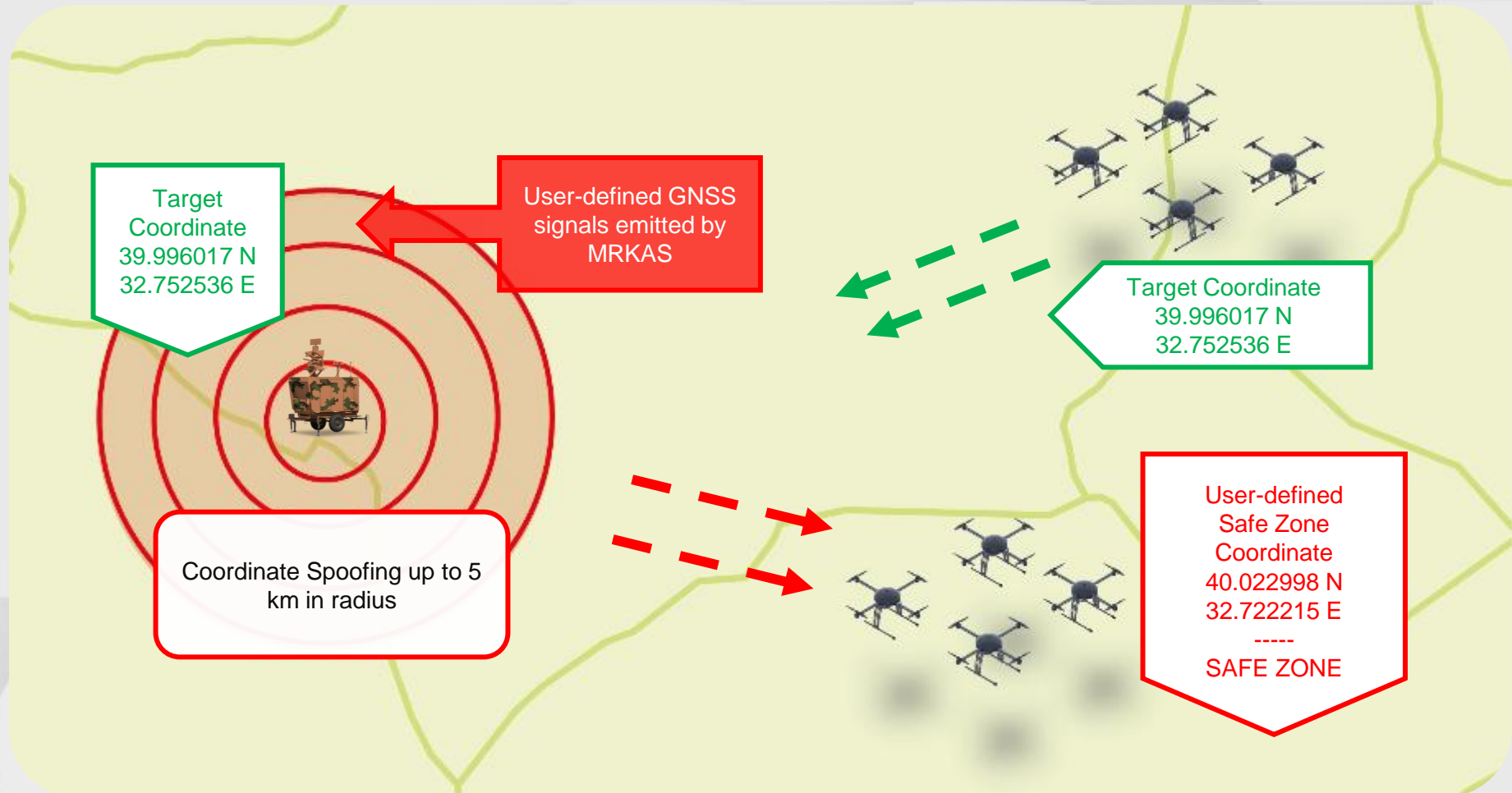


- Jams against long-distance threats in the specified direction.
- In the standard configuration, the RF output power is adjustable up to 4000 Watts with directional antennas, as well as 150 MHz bandwidth jamming anywhere in the SATCOM frequency bands from 10-18 GHz.

Minimum 1:1 jamming distance	
Remote Controller Distance	Blocking Distance
15 km	13.5 km
30 km	27 km

Spoofing (360° Omni Antenna)

- User-defined fake GNSS signals generated to jam autonomous flight threats and remove the threats from the protected area



Spoofing (Directional Antenna)





- User-friendly interface and touch screen
- User authorization
- Wireless connection between command and control center and ILTER
- User-friendly GUI operation
- Detailed log records
- Centralized command and control capability of multiple ILTER systems
- Update with remote connection