

SIGN4L

D-PROTECT

ATTACKS DISABLED. DEFENCE SECURED.



ADVANCED RF AND GNSS JAMMING SOLUTION

The Drone-Protect (D-Protect) System is an advanced RF and GNSS jamming solution with spoofing designed specifically for drone control. With its powerful capabilities, this system provides effective countermeasures against unauthorized drones, ensuring enhanced security and control in sensitive areas.

SPECIFICATIONS

KEY FEATURES

- Jams full range of GNSS spectrum
- Jams drone's command & control channels
- Spoofs commercial GNSS spectrum to protect a specified area of interest
- Combination of jamming and spoofing capability for maximum coverage range
- Typical jamming range for unprotected GNSS platform is up to 10km
- Typical jamming range for command-and-control channels is 2:1 from drone's remote control

COMPONENTS

- Optional Indoor equipment installed in 19-inch equipment rack.
- Outdoor directional antennas installed on a motorized pedestal.
- Optional 3600 omni-directional antennas instead of the directional ones with reduced performance.

Integrated Rack System	L mm	W mm	H mm	W kg
C2 Server	800	470	45	13.5
Network Switch	360	485	45	4
Power Supply Unit	580	480	135	12.5
Jamming/Spoofing Block	600	480	170	35.5
20U Rack	-	-	-	-

Antennas	L mm	W mm	H mm	W kg
PT Head	206	320	380	23.0
GNSS Antenna (Option)	-	94	57	1.0
Directional antenna (Qty 2)	-	106	332	2.3
Directional antenna	-	450	770	3.7
Antennas Total				~ 30

*Depending OEM Sensor performance.

*Using directional antennas

HARDWARE

Operational Bandwidth	400 to 6000 MHz
GNSS Spoofing Frequency	GPS L1C/A, L2C, Glonass L1OF, L2OF
Total PA output power	Up to 350W CW
RF Jamming and Spoofing PA Output power	Jamming: up to 100W from 400-1000MHz Jamming/Spoofing: up to 100W from 1000-2000MHz Jamming: up to 100W from 2000-3000MHz Jamming: up to 50W from 3000-6000MHz
Jamming Signal Source	Field programmable gate array (FPGA)
Jammer Type	Active Jammer
Exciter sweep time	≤ 1.8 micro-sec
Jammer Total power control step	≤ 2 dB
Power Consumption (Peak)	≤ 5kW excludes 3rd party equipment
Connectivity to Command & Control	Ethernet interface
Antenna	High gain directional antennas
Safety	Alarms for VSWR and temperature
Environmental	Design to meet MIL-STD 810G

SOFTWARE

Remote Control Unit	C-UAS C2 application
Exciter controller	Ability to activate/deactivate specific frequency bands
Jammer Power mute per bands	GUI allows the user to mute specific bands before activation
Jammer Power mute for all bands together	GUI allows the user to mute all bands instantaneously
Safety measures	Alarms for VSWR and temperature
Health monitor	System status (Initializing, standby, transmitting)
Selectable jamming threats	400 to 6000 MHz
Ephemeris data	Live update obtained from system location
Update desired spoof location	User defined spoof location
Pan and tilt control via C2 software	Pan the antennas in ±180 degrees Tilt the antennas between 0 to +80 degrees

DEPENDENCIES

- Antennas must have clear line of sight to the jammed/spoofed target
- Cable length between cabinet and antenna is assumed to be no more than 5 metres (for performance purposes)
- The spoofer requires fresh ephemeris data to properly work
- C2 must interface closely with the radar system supplied by the end user
- For best result, accurate position of the target must be provided by the radar to the spoofer (within 300-meter accuracy).
- C2 integration with new 3rd party radar or other sensors, will be costed separately on time & material basis

*All specifications provided herein are indicative values and figures, and there may be reasonable deviation from the same.

*The environmental conditions stated above apply to the V-Protect systems' main components only.