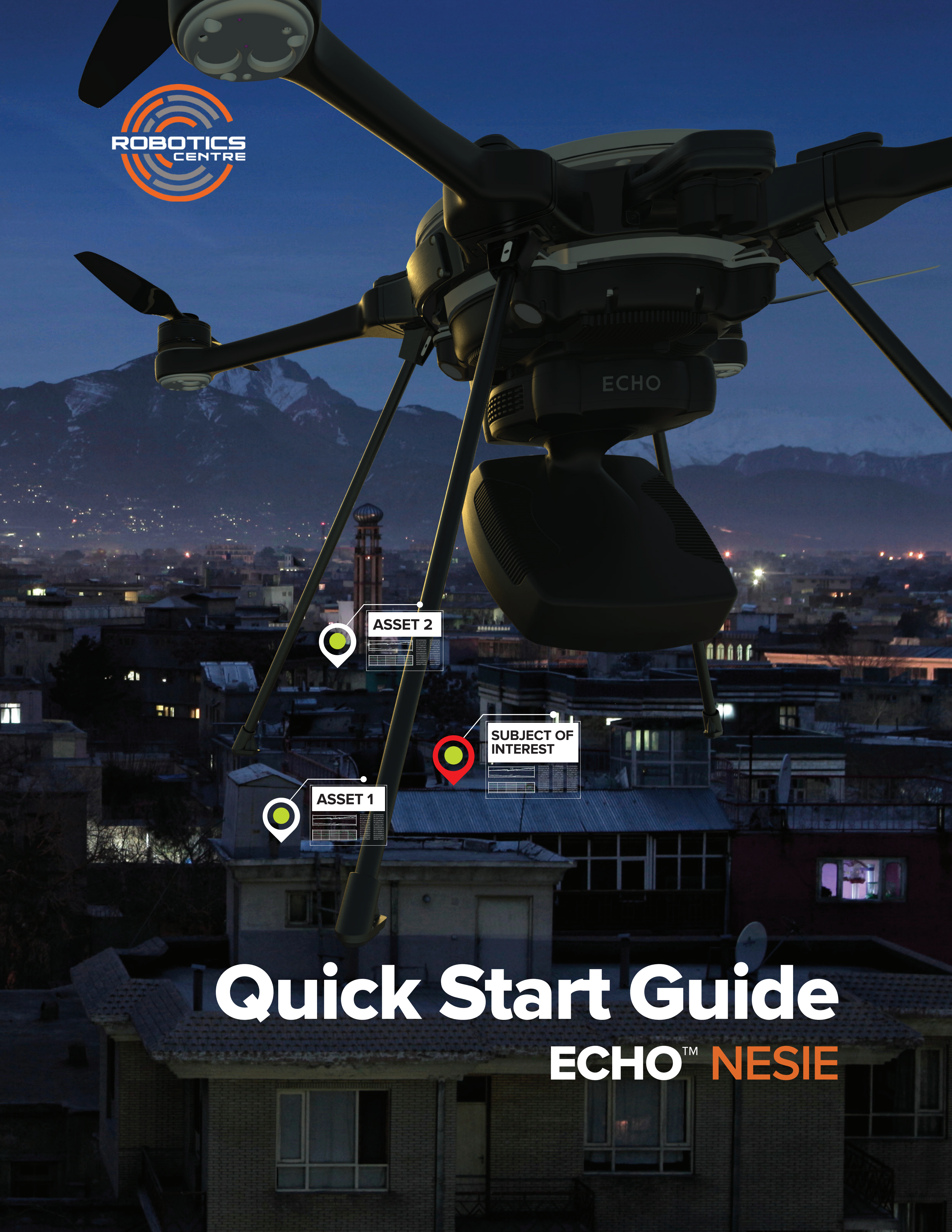
ROBOTICS CENTRE



Quick Start Guide

ECHO™ NESIE

Robotics Centre
225 Marché Way, Suite 205
Ottawa, Ontario K1S 5J3
Canada

robotics-centre.com
support@robotics-centre.com

RC-QSG-ECHO-NESIEen-FLIR-SR-1.0.0-001

Manufacturer’s disclaimers

- The content in this manual, and all other collateral documents, is subject to change at the manufacturer’s sole discretion.
- The software and hardware are subject to change due to the manufacturer’s continuous development process.
- The manufacturer shall not be liable for any damages, losses, costs, or expenses, direct, indirect or incidental, consequential or special, arising out of, or related to the use of this content or the products described herein including failure to heed warnings or cautions.
- You are solely and personally responsible for your conduct and control while operating this equipment and any consequences as a result.

Symbols and conventions

This manual uses the following symbols and conventions:

📖 *This symbol indicates a note with recommendations from the manufacturer.*

✓ *This symbol indicates a helpful tip or recommendation that can enhance the performance of the aircraft or software.*

☰ *This symbol indicates tasks that you must perform before completing the procedure described.*

! *This symbol indicates a caution or warning. For safety purposes, always follow the instructions described.*

□ *Throughout this document RED BOXES are used to highlight or draw attention to sections of the user interface. These boxes are for illustrative purposes only and will not be seen on the operational user interface.*

GLOSSARY

dB – Decibel. A relative unit of measurement corresponding to one tenth of a bel. It is used to express the ratio of one value of a power or root-power quantity to another, on a logarithmic scale.

dBm – A decibel-based unit of power referenced to 1 mW.

DM – Degrees, Minutes.

DMS – Degrees, Minutes, Seconds.

GPS – Global Positioning System. A commonly used satellite-based radio-navigation system owned by the United States government.

GSM – Global System for Mobile Communications. A standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols used in digital cellular networks. Often referred to as 2G.

IMEI – International Mobile Equipment Identity. A unique 16-digit number used to identify mobile devices. It contains a manufacturer code, model number, and serial number.

IMSI – International Mobile Subscriber Identity. A unique 16-digit number that identifies each user of a cellular network. Held on the SIM card, it contains country, network, and subscriber information. After initial registration, the actual IMSI is not used by the network which instead uses a TMSI.

LTE – Long-Term Evolution. A fourth-generation mobile cellular system for networks based on the GSM and UMTS standard. Often referred to as 4G.

m – Metres; used as a measurement of distance.

MGRS – Military Grid Reference System. A military system for defining a unique point on the Earth.

RSSI – Relative Received Signal Strength Indication (measured in dBm).

Rx – Receive antenna.

SMS – Short Message Service. A messaging system available on most cellular devices.

TA – Timing Advance. A value corresponding to the length of time a signal takes to reach the ECHO from a mobile phone.

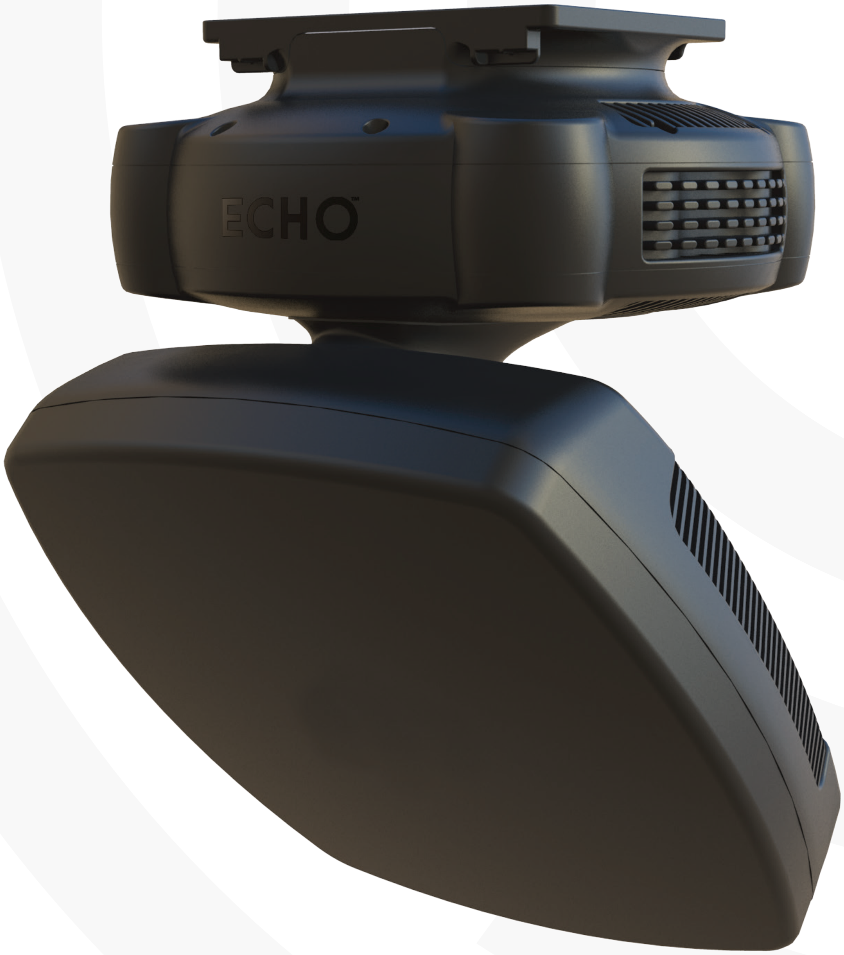
Tx – Transmit antenna.

UMTS – Universal Mobile Telecommunications Service. A third generation mobile cellular system for networks based on the GSM standard. Often referred to as 3G.

UTM – Universal Transverse Mercator. A coordinate system dividing the world into sixty north-south zones, each six degrees of longitude wide.

CONTENTS

OVERVIEW



Introduction

The ECHO NESIE is a mobile phone identification, geolocation, and interrogation payload that is compatible with the FLIR SkyRanger R70 and R80D SkyRaider platforms. The payload is designed to gather cellular intelligence, locate cellular devices, and influence mobile phones in a number of ways.

Through Smith Myers NESIE (Network Emulation, Simulation and Interrogation Equipment) Software, ECHO NESIE performs this task by emulating a genuine mobile phone cell site/base station, and communicates with the mobile phone in the same manner as a genuine mobile phone network. Only authorised government agencies are permitted to use this software. The data collected from this software is maintained in the database of the ECHO NESIE system.

ECHO NESIE can be used as a stand-alone system or in combination with other Smith Myers supported platforms, and does not require the presence of a cellular network.

When using the ECHO, Robotics Centre recommends using the legs that are most appropriate for the payload. After assembling the aircraft and mounting the payload, ensure that there is enough clearance below the payload such that it will be clear of obstacles on landing.

This guide provides only the information that is specific to using the ECHO NESIE payload.

Before flying the aircraft with the ECHO payload, be sure that you are familiar with the information and procedures described in the FLIR Pilot Operating Manual for your aircraft as well as the Smith Myers NESIE User Guide. Ensure that your aircraft is using system software version 5.1.1 (or higher) and that the Robotics Centre ECHO CNX plugin has been installed as part of the FLIR Mission Control Station. If the aircraft is using an older software version, the plugin may not function properly. The ECHO payload cannot operate with older versions of the software.

The ECHO NESIE has the capability of transmitting on frequencies with the potential to interfere with aircraft communications and operation. It is strongly suggested that the operator familiarise themselves with frequencies used by the aircraft and adapt ECHO NESIE transmissions accordingly.

Contact Robotics Centre Support

If you are a current customer, visit **https://www.robotics-centre.com/customers**

Email the support team at **support@robotics-centre.com**

ECHO SOFTWARE

ECHO CNX™

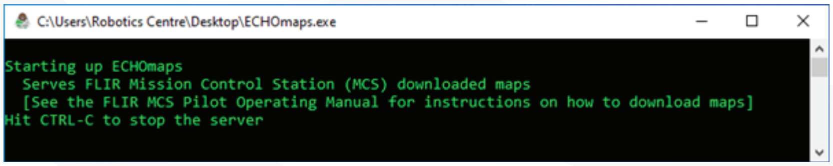
ECHO CNX is a plugin designed for the FLIR Mission Control Station (MCS) to provide the pilot with enhanced target discovery, acquisition, and geolocation capabilities during ECHO missions.

Before launching the FLIR MCS application, be sure that you have placed the ECHO CNX jar file into the dedicated MCS plugin directory "\Users\<CurrentUserName>\FLIR_MCS\Plugins"

ECHOmaps™

ECHOmaps is a standalone application providing a local map tile server for the Smith Myers NESIE web client. The application utilises FLIR MCS downloaded maps as its map tile source.

Before launching the NESIE web client, be sure that you have already launched the ECHOmaps application and downloaded maps using the FLIR MCS. The application can be launched simply by double clicking the respective executable file. No installation is required. The application only serves map tiles to the device it has been executed on.

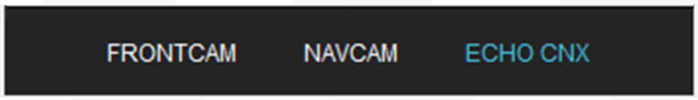


```
Starting up ECHOmaps
  Serves FLIR Mission Control Station (MCS) downloaded maps
  [See the FLIR MCS Pilot Operating Manual for instructions on how to download maps]
Hit CTRL-C to stop the server
```

USING THE ECHO NESIE

Switch to the ECHO CNX View

The aircraft comes with built-in cameras, including four downward-facing navigation cameras (NAVCAM) and a forward EO/IR camera (FRONTCAM), which are viewable in the primary video panel. Attaching the ECHO payload will add a third view (ECHO CNX) to the primary video panel.



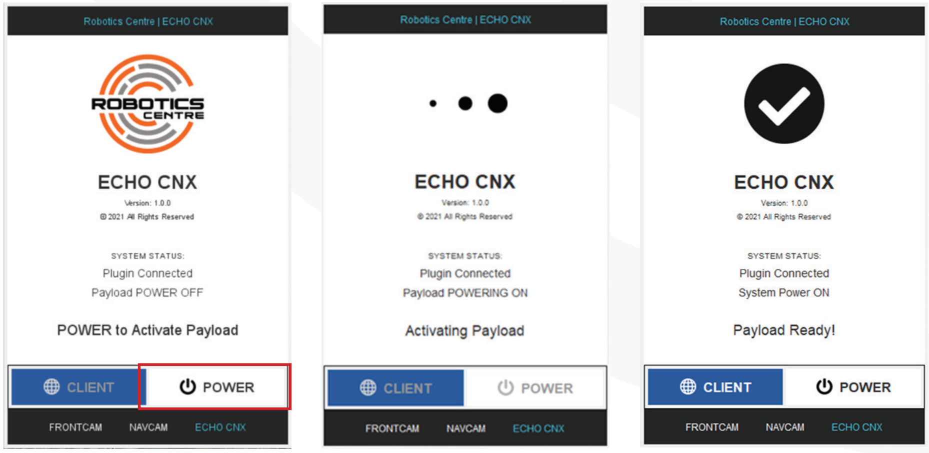
In the primary video panel, to switch to the ECHO payload, tap ECHO CNX.

Power ON/OFF the ECHO

With the ECHO attached to the aircraft the following view appears and the ECHO is ready to be powered on.

To avoid damage to the ECHO, always ensure all antennas are connected prior to powering on.

To power on the ECHO click the power button and confirm the power on request. The ECHO will then power on and enter a booting state.



ECHO CNX
Version: 1.0.0
©2021 All Rights Reserved
SYSTEM STATUS:
Plugin Connected
Payload POWER OFF
POWER to Activate Payload

ECHO CNX
Version: 1.0.0
© 2021 All Rights Reserved
SYSTEM STATUS:
Plugin Connected
Payload POWERING ON
Activating Payload

ECHO CNX
Version: 1.0.0
© 2021 All Rights Reserved
SYSTEM STATUS:
Plugin Connected
System Power ON
Payload Ready!

Once the ECHO has successfully booted, a confirmation screen will appear and transition into the pilot user interface.

Booting the ECHO may take up to 60 seconds.

The same approach is used to shut down/power off the system.

Shutting down the ECHO may take up to 30 seconds.

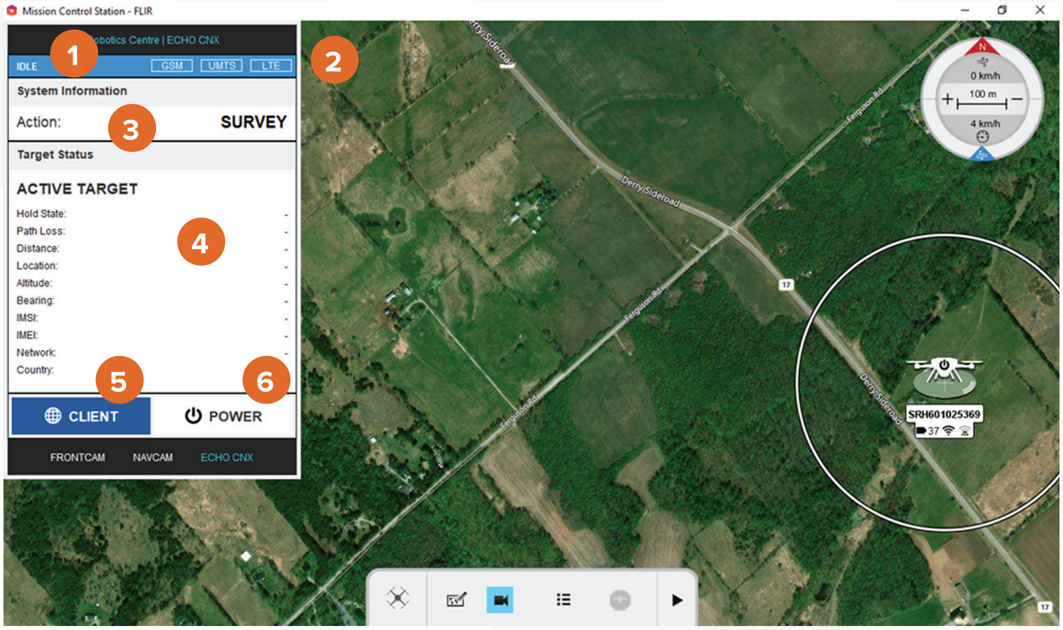
To avoid data corruption, always power off the ECHO before powering off the aircraft or disconnecting the payload from the aircraft.

Pilot User Interface Overview

The main screen of ECHO CNX is the pilot user interface, designed to provide insight into the current operation of the ECHO NESIE and assist the aircraft pilot with handset discovery, acquisition, and geolocation.

Prior to utilizing ECHO CNX, Robotics Centre recommends operating personnel to have been trained in the use of the Smith Myers NESIE software. As such, the reader is assumed to have a working knowledge of NESIE operations and actions, which will only be discussed at a high level in this quick start guide.

The pilot interface is composed of the following components:



Mission Control Station - FLIR

Robotics Centre | ECHO CNX

IDLE

System Information

Action: SURVEY

Target Status

ACTIVE TARGET

Hold State: -
Path Loss: -
Distance: -
Location: -
Altitude: -
Bearing: -
IMSI: -
IMEI: -
Network: -
Country:

1 System State

Idle – The normal colour of the header bar is blue. This is the colour shown when the system is 'idle', i.e. neither transmitting nor scanning.

Scanning – The header bar is shown in purple whenever the system is conducting a network scan.

Transmitting – The header bar is shown in green whenever the system is transmitting.

2 Technology

The technology that the system is currently using to conduct a network scan or transmitting on will be highlighted. The technology will rotate through GSM, UMTS, and LTE.

3 Action

Action is the current operational function of the system. Actions are introduced in the following section.

4 Target Status

If a target phone has been located, target information will populate the target status pane.

Active Target – The active target text will be replaced by the name of the target as saved by the operator. If the target is not named, the target IMSI/IMEI will be displayed.

Hold State – When a target is in a hold state, the system has automatically moved the target to a traffic channel where it is holding the target. This is necessary for geolocation. Hold states are

- HELD: the target is in a successful hold.
- FOUND: the target has been found, but is not in a successful hold.
- LOST: the target has been lost.
- ABANDONNED: attempts to hold the target have been abandoned.

Path Loss – The strength of the signal in dB from the target when detected. Path Loss is a continuous calculation of the difference between the measured Received (Rx) Signal Strength Indicator (RSSI) for the named mobile and the Transmit (Tx) power reported by that mobile: **Rx RSSI – MS Tx POWER**

When the system loses contact with the mobile phone, an infinite (or extremely large) path loss is assumed.

As a general rule, the closer the aircraft is to the named mobile the lower the path loss will be.

If the aircraft was in close proximity to the mobile phone and had clear line of sight, the path loss would be at its lowest. It can be a good indicator that the named mobile is not in line of sight when the aircraft is in close proximity to the named mobile but the path loss is still high.

For example: Measured range to named mobile is low, but path loss is still very high (>120dB). This could indicate that the named mobile signal is being reduced by obstructions. For example, the named mobile may be in the next valley, behind a dense wooded area or inside a building.

Distance – The distance to the target as calculated (estimated or GPS).

Location – The latitude/longitude of a target location fix. When a target is being held on GSM, the system continually attempts to retrieve a GPS location from the target. If the handheld is compliant (and the command works on its first attempt), it will take approximately 10–15 seconds to retrieve the GPS results. If successful, the Target GPS Latitude and Longitude will be displayed. If a GPS position cannot be extracted, estimated values will be shown instead.

> *Location coordinates will be displayed in the format selected in the FLIR Mission Control Station. Supported formats are Deg, DM, DMS, UTM, and MGRS.*

Altitude – The altitude of the target as calculated (estimated or GPS).

Bearing – The bearing to the target as calculated (estimated or GPS).

IMSI – The target IMSI.

IMEI – The target IMEI.

Network – The network name based on the network code being utilized.

Country – The country name based on the country code being utilized.

5 Client Button

Clicking this button will open a default browser to the NESIE web client.

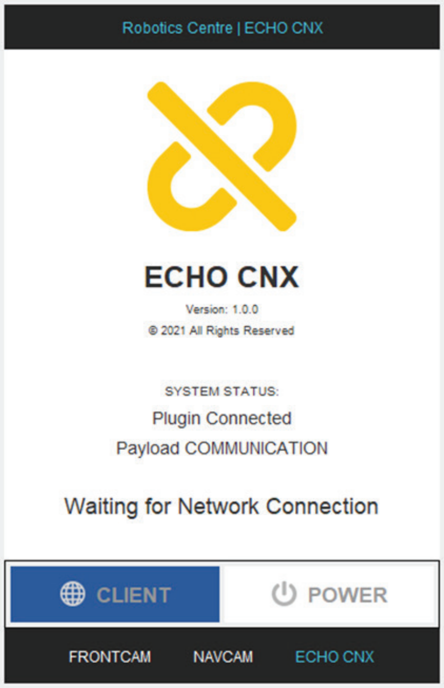
6 Power Button

Button to power on/boot and power off/shut down the payload. (See the Power ON/ OFF the ECHO Section)

> *The Client and Power Buttons are enabled when appropriate and disabled when not. For example, the Client Button is disabled when the payload is not powered on.*

In the case where ECHO CNX is waiting for, or loses, connection with the ECHO payload, a connection loss screen will appear. If connection is lost, ensure proper network connection between the aircraft and the device running ECHO CNX, and that the ECHO payload is properly seated on the aircraft.

> *On payload attachment, the connection loss screen will appear until the network is up on the ECHO (~15 seconds).*



Robotics Centre | ECHO CNX

ECHO CNX

Version: 1.0.0

© 2021 All Rights Reserved

SYSTEM STATUS:

Plugin Connected

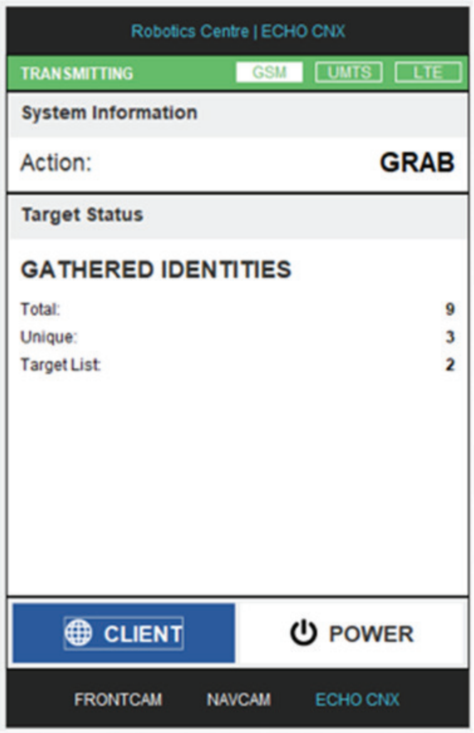
Payload COMMUNICATION

Waiting for Network Connection

ECHO NESIE Actions

Grab – Grab is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – before rejecting them back to the real network. Displayed in the Target Status window are the gathered identities broken down into

- *Total:* The total number of grab interactions (a single handheld may be grabbed more than once).
- *Unique:* The number of unique identities grabbed.
- *Target List:* Of the unique identities, the number appearing in the target list.



System Information

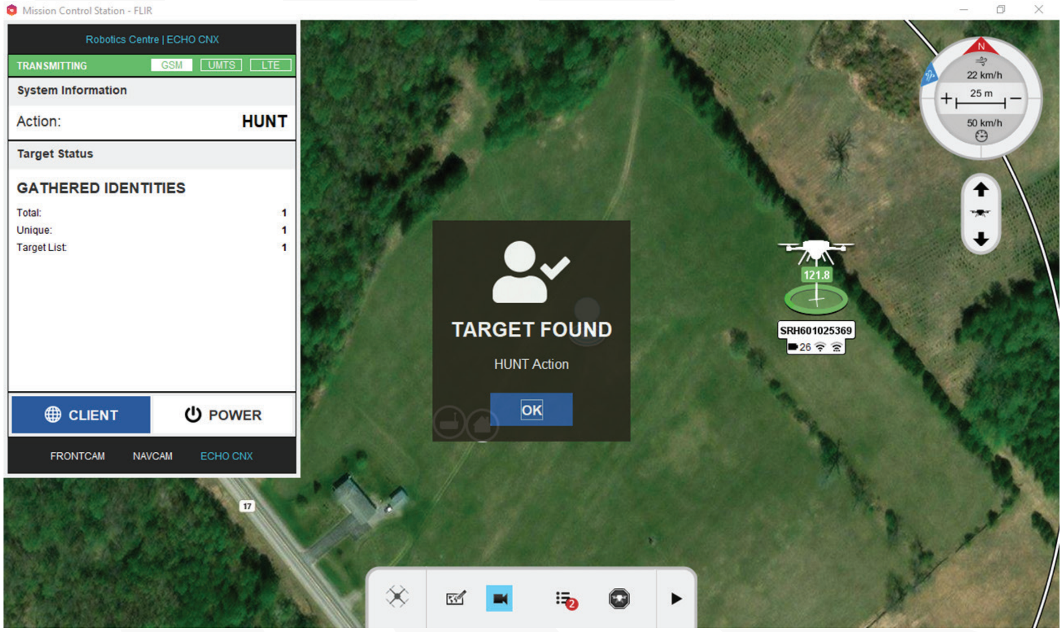
Action: GRAB

Target Status

GATHERED IDENTITIES

Total:	9
Unique:	3
Target List:	2

Hunt – Hunt is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for one or multiple target identities, before rejecting them back to the real network. A visual alert will be used to notify the operator to the presence of a target.


Mission Control Station - FLIR

Robotics Centre | ECHO CNX

TRANSMITTING

System Information

Action: HUNT

Target Status

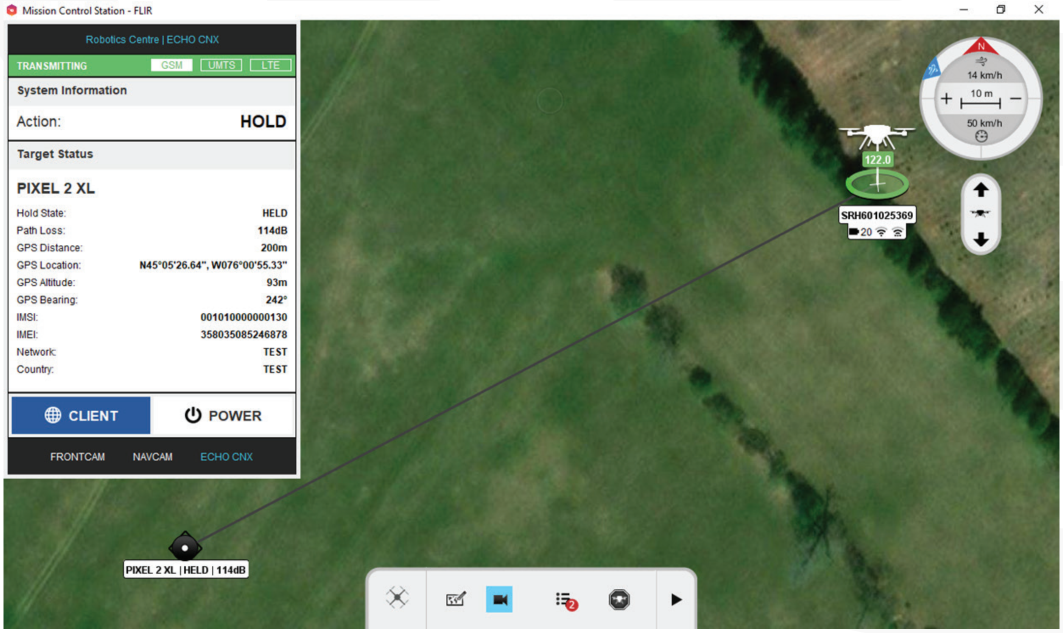
GATHERED IDENTITIES

Total:	1
Unique:	1
Target List:	1

TARGET FOUND

HUNT Action

Hold – Hold is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for the first target identity. The target cellular device is moved onto a designated traffic channel and put into a Hold (Silent Call) state.


Mission Control Station - FLIR

Robotics Centre | ECHO CNX

TRANSMITTING

System Information

Action: HOLD

Target Status

PIXEL 2 XL

Hold State:	HELD
Path Loss:	114dB
GPS Distance:	200m
GPS Location:	N45°05'26.64", W076°00'55.33"
GPS Altitude:	93m
GPS Bearing:	242°
IMSI:	001010000000130
IMEI:	358035085246878
Network:	TEST
Country:	TEST

PIXEL 2 XL | HELD | 114dB

Deny – Deny is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for one or multiple target identities. When the required identities are seen, they will be registered onto the NESIE base transceiver station and denied access to the real network. Any identities not required will be rejected back to the real network and not affected.

Disable – Disable is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for one or multiple target identities. When the required identities are seen, they will be sent a disable code. This disable code will temporarily disable the handset and deny it access to the real network. Any identities not required will be rejected back to the real network and not affected.

Broadcast SMS – Broadcast SMS is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for one or multiple target identities. When the required identities are seen, they will be registered onto the NESIE base transceiver station and denied access to the real network. Upon registration on the NESIE network, an SMS will be broadcast (sent) to the cellular devices. Any identities not required will be rejected back to the real network and not affected.

Redirect – Redirect is the is the process of transmitting pseudo base transceiver stations in order to gather the IMEIs and IMSIs from all the cellular devices in the area – looking for one or multiple target identities. When the required identities are seen, they will be sent a technology redirect message (e.g. go from 4G to 2G, go from 3G to 2G).

Redirection allows the user to bring a target handheld to a desired technology for exploit. This requires a multi-channel approach (i.e. one to redirect and another to grab). This can be achieved with two or more single channel ECHOs working together.

Geo-Locating a Target

Whenever a HOLD operation is carried out and a device is successfully held, the ECHO NESIE system will automatically attempt to extract the GPS location from the handset. It takes approximately 15 seconds for this process to be completed and, if successful, the Latitude and Longitude of the target handset will be displayed on the user interface.

> ✓ *Not all phones will comply with a command sent by the ECHO NESIE system to return their GPS position. It depends on the make, model, software installed and sometimes the GPS chip fitted in the cellular device.*

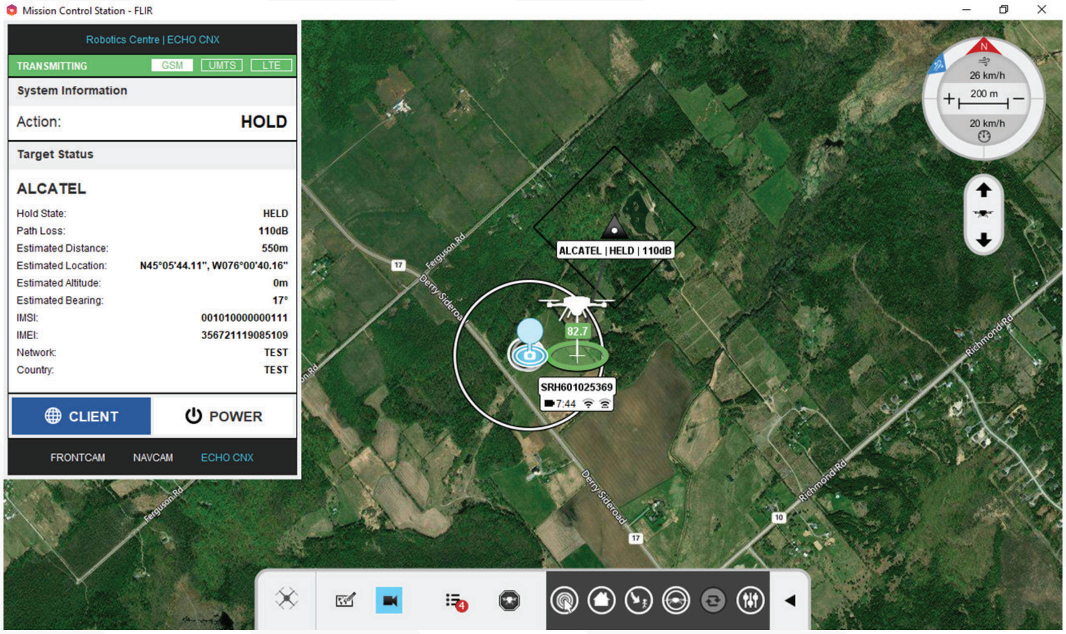
> *To enable ECHO NESIE to control a handset and extract the GPS data, the handset must be moved onto a GSM channel. This allows the system to circumnavigate the security controls in the UMTS and LTE protocols.*

Should GPS extraction not be successful, ECHO NESIE uses the native (2G, 3G or 4G) protocol to measure the distance from its own location to the handset. The further ECHO moves, the more measurements will be calculated and the more accurate the location of the target will be.

> ✓ *The ECHO system should be moved in an arc or L-shape to aid the calculations and firm up the position fix. The estimated location may initially switch left and right but, as the ECHO NESIE system moves in an arc or L-shape, the switching location will settle as the fix firms up.*

Map Display and Error Bounding

Initially, the error bounding calculated by the ECHO NESIE system may be represented by a large square. This indicates that there is a large error in the calculated position. This square will shrink as the possible error decreases.



Mission Control Station - FLIR

Robotics Centre | ECHO CNX

TRANSMITTING GSM UMTS LTE

System Information

Action: HOLD

Target Status

ALCATEL

Hold State: HELD
Path Loss: 110dB
Estimated Distance: 550m
Estimated Location: N45°05'44.11", W076°00'40.16"
Estimated Altitude: 0m
Estimated Bearing: 17°
IMSI: 001010000000111
IMEI: 356721119085109
Network: TEST
Country: TEST

There are two types of geolocation icons:

● *(Circle) GPS Derived*

▲ *(Triangle) TA (Timing Advance) derived*

The colour of the geolocation icon will change depending on the geolocation state

Active	The target mobile is being held and located.
Registered	The target mobile has been registered but is not currently being located.
Lost	The last calculated location of the target mobile before the signal was lost by the system.

ACCESSING SMITH MYERS WEB CLIENTS

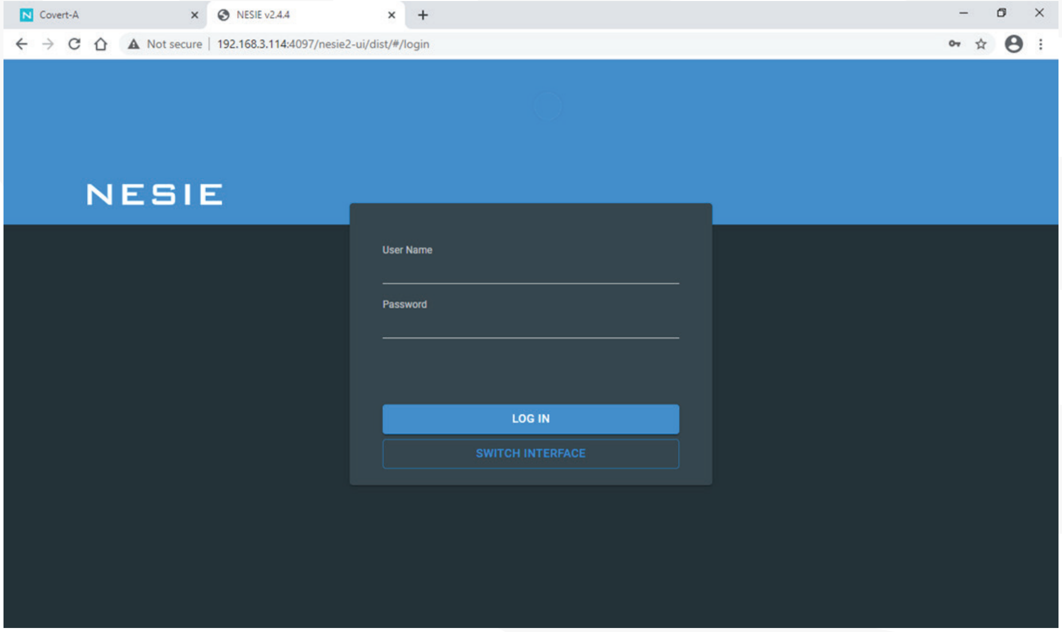
All Smith Myers web clients can be accessed by any device connected to the aircraft network made available through the aircraft base station. The base station and its antennas provide a long-distance communication link between a device and the aircraft.

The ECHO payload has been assigned a series of ports associated with the IP address of the aircraft.

NESIE Web Client

The NESIE web client can be accessed through a dedicated port 4097 with the addition of the following resource path *http://aircraftip:4097/nesie2-ui/*

If the aircraft IP address is 192.168.3.113, then the corresponding URL would be http://192.168.3.113:4097/nesie2-ui/



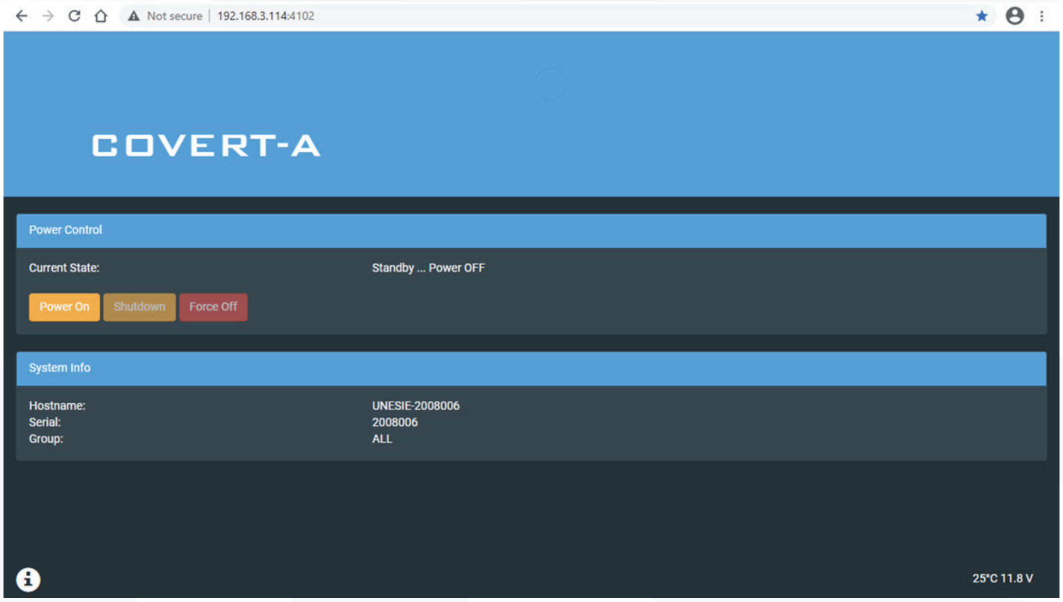
Power Control Web Client

The Power Control web client can be accessed through a dedicated port 4102 (*http://AIRCRAFTIP:4102/*). Unlike the NESIE web client, the Power Control web client is available as soon as the ECHO payload is attached, regardless of whether the payload is powered on or not.

If the aircraft IP address is 192.168.3.113, then the corresponding URL would be http://192.168.3.113:4102/

The Power Control web client provides monitoring information on the COVERT-A category ECHO payload such as status, power, temperature, and more. In addition, the client allows for power on/off control as well as a ‘force off’ button for a payload hard reset.

The ‘force off’ button is to be used in a troubleshooting scenario only, e.g. an unresponsive payload, such that data corruption may occur.



Power Control

Current State: Standby ... Power OFF

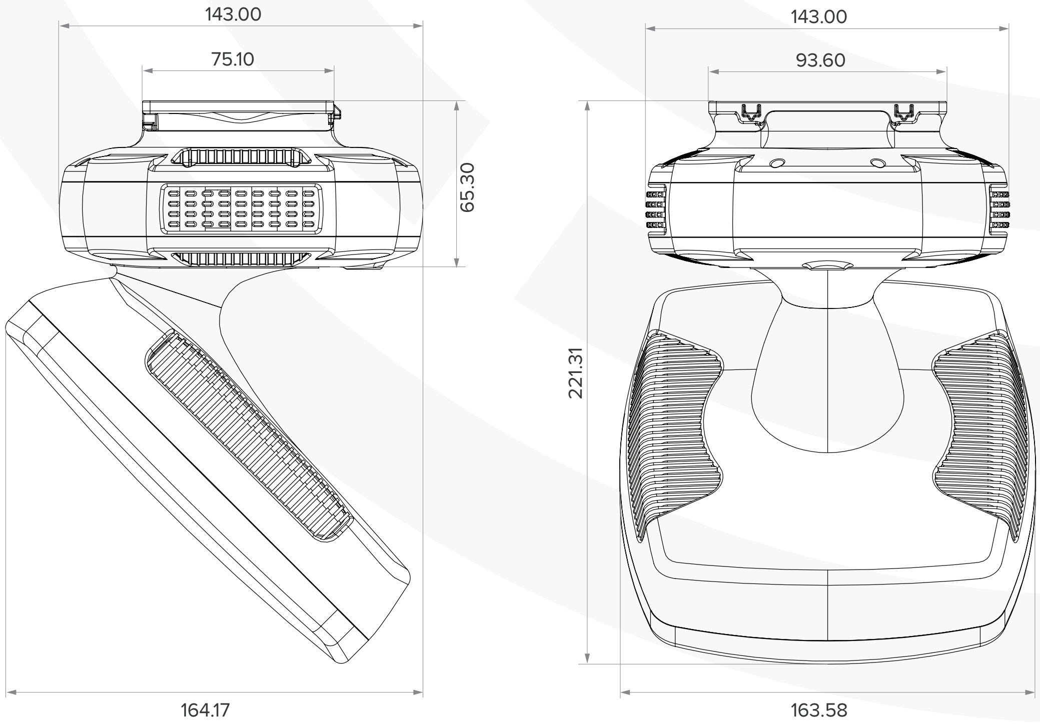
System Info

Hostname: UNESIE-2008006
Serial: 2008006
Group: ALL

25°C 11.8 V

SPECIFICATIONS

Category	Details
Weight	1.04kg (2.29lbs)
Dimensions	163.58 (W) x 164.17 (L) x 221.31mm (H)
Output Power	120mW (peak)
Operating System	LINUX
Internal Memory	32GB
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Spectrum Coverage	Worldwide cellular bands (20MHz-3.5GHz) GSM: 900, 1800, 850, 1900 UMTS: 850, 900, 1700, 1800, 2100 LTE: 700, 800, 850, 900, 1700, 1800, 1900,2100, 2300, 2600


143.00
75.10
65.30
164.17
143.00
93.60
221.31
163.58