allocortech inc.

Comet E-Stop and FTS Operators Manual

600-0049-000

Revision G

Nov 2025

440 N Commerce Ave
Waynesboro, VA 22980

https://allocor.tech

Table of Contents

Version History

Revision	Changes
A	Initial Draft

B	Updated allocortech's physical address
	Renaming from AIR and GND to Vehicle and Operator
	Added information about new commands
	Added descriptions about telemetry and faults
	Added diagrams and explanatory text about the possible software states and transitions.
	
	Based on Comet FTS Repository Hash:
	`8591d449994321ec91d39b2235c6972902ac423c`
	With allocore Repository Hash:
	`7a5933ea54b79e3952b453e6bfac7533ca993fcc`

C	Corrected erroneous CAN IDs Added information about the `set_telem_timing` and `set_eth_telem_ip` commands.
D	Added Teleop functionality section
E	Documentating version 3.1 functionality
F	Clarifying software update tools and options
G	Added information about 3SO state machine Documented the `set_buzzer` configuration option Clarified support for Diode+Zener coil suppression

Introduction

The allocortech inc. Comet is a remote safety system capable of operating as a vehicle's emergency stop (E-Stop) or Flight Termination System (FTS). The system is composed of a vehicle unit[1] and a small number[2] of operator units[3].

The Comet system is designed to prevent single faults from causing an uncommanded positive voltage on the output pins, but is not designed to guarantee a positive output in the face of a single fault. When operated as an E-Stop, the software will emit a positive output as a ‘run’ signal, and short the output as ‘stop’. When operated as a FTS, a positive output should be interpreted as ‘terminate’.

FTS are commonly used when testing new air vehicle concepts, particularly at larger scales at which a “runaway” vehicle could cause significant harm to people, animals or property. To prevent vehicles traveling outside designated test areas, a multitude of failsafes are used, frequently including separate, remote operated/controlled systems such as the Comet. Having a separate system with a ground element allows operators, range safety personnel or other oversight entities to have a means of terminating testing if onboard systems fail to respond or unaccounted for events occur on the test range (such as unscheduled intrusions in the test area (people or animals). These systems must have very high reliability to function when needed and the Comet is one such system.

Similarly the Comet can be used as an E-stop for other vehicles in which the actions imparted by using the Comet may just induce limited capability, slowing a vehicle down, making it idle, return home or any number of operations that do not “terminate” the vehicle or its functionality.

The Comet vehicle unit can be factory configured with any combination of voted or non voted voltage or current outputs. In current mode, the Comet is able to fire up to a 5A pyrotechnic charge. It is up to the operator how best to implement these actions to assure appropriate termination of the vehicle as desired. Example implementations include cutting propulsion power (either by turning off motor controllers, pyro cutting power cables, turning off battery outputs, etc.), unpowering other control systems, forcing control surfaces to hard over positions, deploying drogue chutes, etc. Vehicle integrators and operators should consider which means will most reliably and robustly impart the desired outcome for the vehicle and conduct appropriate analysis to understand post termination outcomes (such as the radius of glide slope in reference to test range borders).

Each Comet unit provides auxiliary CAN or 10/100 Ethernet communication channels for telemetry and redundant termination commands. Additionally a single RS-232 port is available, which is normally used for console access but could be repurposed to communicate with something like a GPS or IMU.

[1] The vehicle unit is sometimes referred to as the Air unit for historical reasons.
[2] 900 MHz FTS firmware allows 2 simultaneous operator RF units. All other FTS firmware only allows a single operator RF unit. E-Stop firmware on all bands only allow a single operator unit regardless of transmission path. For the FTS firmware, additional operator units can be supported with changes to the reporting rates and RF link latency.
[3] The operator unit is sometimes referred to as the Ground or Remote unit for historical reasons.

Scope of this Document

This document covers the software configuration and operation of the Comet Vehicle and Operator units in a nominal Flight Termination System configuration. Allocortech allows end users to customize the software that runs on each unit and therefore some aspects of the operation of the unit may differ between serial numbers. Further, although allocortech has a standard communications protocol for the Ethernet and CAN interfaces for internal test purposes, this is very likely different per vehicle integration.

For information about the electrical and mechanical aspects of the devices, including any installation guidelines, see document 601-0049-000 Comet E-Stop and FTS Mechanical ICD.

Hardware Revision Information

Mark II versions of the Comet introduce an onboard GPS and dual IMU which can be used for autonomous actions such as geofencing, leashing operation to a radius around the operator unit, detection of impacts, and limited reversionary control. The onboard GPS however was not brought out to the enclosure.

Mark III versions of the Comet added an internal TVS diode to protect the SAFE MOSFET, which required the addition of a “contactor or relay” factory option which would remove it in the case that a fast contactor limiting circuit is present externally. Additionally the GPS antenna is now brought to the enclosure.

List of Abbreviations

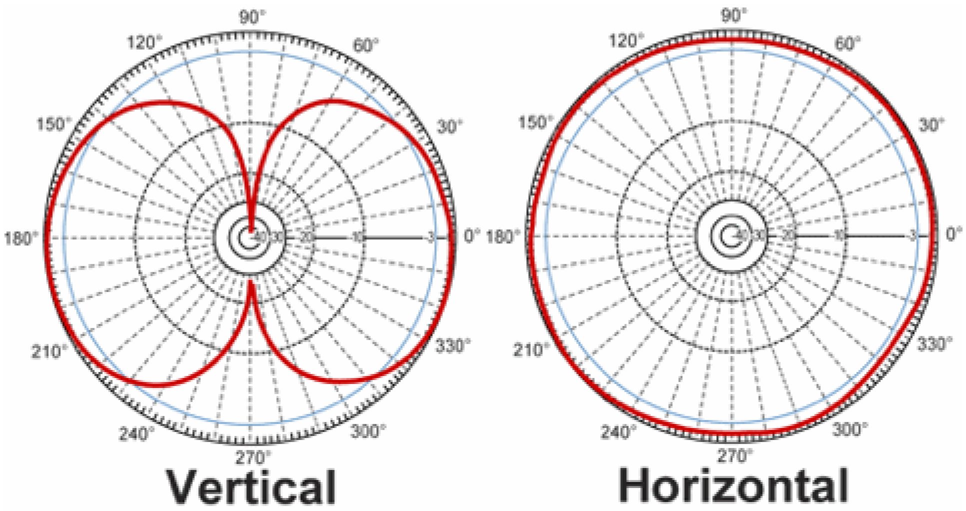
BIT	Built in Test
CAN	Controller Area Network (an arbitrated 2 wire network protocol)
CBIT	Continuous Built-in Test
E-Stop	Emergency Stop
FMEA	Failure Modes and Effects Analysis
FTS	Flight Termination System
FTS-AIR	Flight Termination System - Airborne Unit (now known as the vehicle unit)
FTS-GND	Flight Termination System - Ground Unit (now known as the operator unit)
GPS	Global Positioning System
ICD	Interface Control Document
IMU	Inertial Measurement Unit (rate of turn gyroscopes and accelerometers)
MCU	Microcontroller
ms	Milli-seconds
PBIT	Power-on Built in Test
PCB(A)	Printed circuit board (assembly)
RF	Radio frequency
RP-SMA	Reverse polarity sub-miniture connector A
RS-232	A 2 wire point to point communications protocol utilizing -5 to +5V signaling
RSSI	Received Signal Strength Indicator
TNC	Threaded Neill–Concelman radio frequency connector
TTL	Transistor/transistor logic, a low voltage electrical standard
UART	Universal asynchronous receiver and transmitter
YAPP	Yet Another Packet Protocol (allocortech's in house streaming protocol)

References

Allocortech 601-0049-000	Comet E-Stop and FTS Physical ICD
Allocortech 600-0061-000	Comet - 400 MHz RF Configuration
Allocortech 600-0065-000	Comet - 869 MHz Unit Commissioning
Microhard Application Note	*The Diagnostics Channel Protocol, Model P900* Revision 1.04
RTCA DO-160G	Environmental Conditions and Test Procedures for Airborne Equipment
STMicroelectronics AN3155	USART protocol used in the STM32 bootloader

Radio Operation

The FTS radio link, in its recommended configuration, uses linearly polarized omnidirectional rubber duck antennas. These antennas have a strong overhead null and function best when antennas are parallel to each other.



Example quarter wave antenna radiation pattern.
90 degrees vertical is through the tip of the antenna.

For best operation, ensure a clear line of sight to the Vehicle unit antenna. Note that obstructions near to the line of sight path may still significantly interfere with signal quality due to Fresnel zone and multipath effects.

Antenna Separation

To satisfy FCC RF exposure requirements for mobile transmitting devices, the operator must maintain a minimum separation distance, determined by the frequency and antenna gain, between themselves and the antenna during operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

These FCC limits are detailed in 47 CFR § 2.1091 for mobile devices (vehicles or other non permanent structures) and 47 CFR § 2.1093 for portable operations in close proximity to persons. In general, the maximum 6 minute average power density for the vehicle is 1.33 mW / cm^2 and the maximum 30 minute average power density for the operator is 0.27 mW / cm^2.

Microhard has provided the following table for **400 MHz operation:**

	Impedance (ohms)	Antenna Gain (dBi)	Minimum Separation Distance (cm)
Minimum Gain	50	0	39
Maximum Gain	50	18	305

Microhard has provided the following information for **869 / 900 MHz operation:** Maintain a minimum separation distance of at least 23cm.

Antenna Isolation

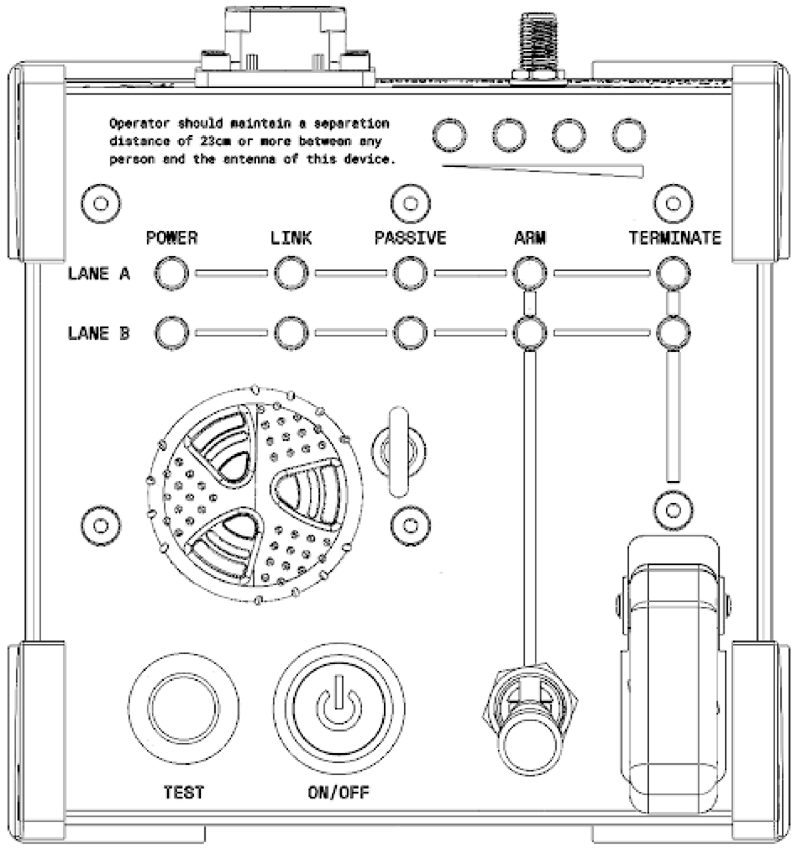
On the Vehicle unit, both the RF and GPS antenna shields are isolated from the chassis but are connected to the digital ground. To prevent unwanted loops, the ground patch on the hull and any hull penetrations either need to be isolated themselves, or a shield DC block must be used.

Antenna Isolation

Comet does not include any lightning or transient voltage suppression on the RF lines. If such protection is required it must be added externally.

Operator Unit

Operational Summary



As a quick summary of the operation of the Comet Operator Unit through termination:

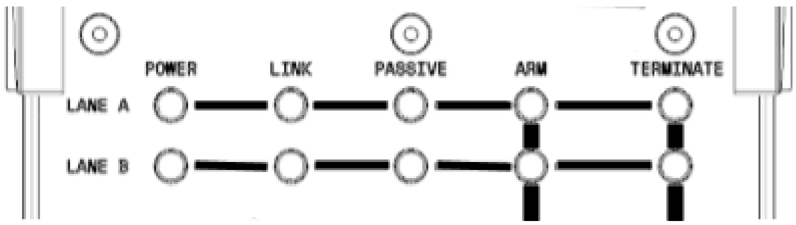
1. Press the power button, the LED ring will illuminate Green or Red (indicating low battery)
2. The Power and Passive LEDs for each lane will illuminate solid
3. The Link LED will illuminate either Solid (good link) or Blinking (link not yet established)
4. With a solidly illuminated Link LED, actuating the ARM switch will:
    a. Solidly illuminate the Arm LED and extinguish the Passive LED
    b. Cause the buzzer to emit a warbling tone
5. Actuating the terminate switch will blink the Terminate LED until Vehicle unit confirmation of termination, at which point it will solidly illuminate.
6. Actuating the Terminate and Arm switches back to the off position will result in the Terminate LED and either the Arm or Passive LED blinking. If the Vehicle unit is allowed to disengage Terminate, then once the command is acknowledged, the Operator unit will solidly illuminate the Arm or Passive LED.
   Note: The buzzer only sounds when the Operator unit Arm or Terminate switches are actuated and does not reflect the acknowledged state of the Vehicle unit.

Indicators

In general, LEDs are only illuminated for positive acknowledgment. A lack of illumination should be taken as an indication of failure.

There are two independent lanes inside of the Comet Operator unit, and each lane controls its own set of Power, Link, Passive, Arm, and Terminate LEDs. These lanes and their association are marked with black horizontal lines across the face of the unit.

Black vertical lines visually connect the Arm and Terminate LEDs with their respective switches.



Link

Solidly Illuminated	The vehicle unit has acknowledged at least one command in the timeout period[4].
Blinking	No message from the Vehicle unit has been recently received

Passive, Arm, and Terminate

Solidly Illuminated	Vehicle and this Operator unit are in the same state. This implies an active Link and acknowledgement of commands from the Vehicle.
Single Blinking LED	This Operator unit is in the indicated state, but does not have link or acknowledgement from the Vehicle unit.
Multiple Blinking LEDs	Vehicle and this Operator unit are in different states.
Extinguished	If other Passive, Arm, and Terminate LEDs are illuminated, neither Vehicle or this Operator unit are in this state. Otherwise the state of the system is unknown.

Note: If the Terminate switch is actuated before the Arm switch, the unit will remain in the Passive state and the LED indications will reflect that (solid if the Operator unit is also Passive, and blinking if otherwise.)

Note: If the unit is powered with the Arm switch already actuated, it will not progress out of its power on-built in test. In this case, the Power indicators will be illuminated and the buzzer will sound, but no other indicators will be illuminated.

Note: In the case where the Operator unit has terminally failed its built-in test, all the state LEDs for the failing lane will be extinguished.

---

[4] The command timeout period can be configured using the `set_command_timeout` command.

Power

Solidly Illuminated	The processor for the respective lane is working normally.
Blinking	The processor for the respective lane has not booted, is not configured, or has otherwise had a terminal failure.

RSSI - Radio Received Signal Strength Indication

There are four RSSI LEDs controlled by the Lane A processor reflective of information received from the radio about the quality of link between the Operator and Vehicle units. These LEDs behave slightly differently depending on if an auxiliary link is configured or not.

Radio Link Only:

LEDs will illuminate from left to right as the signal strength improves.

# of LEDs Illuminated	RSSI (dBm)	Approximate SNR (dB)	Estimated Distance to Vehicle (km) 900 MHz
1	-90 to -80	20	22 to 8
2	-80 to -75	30	8 to 5
3	-75 to -70	35	5 to 2.5
4	Better than -70	40	Less than 2.5

Auxiliary Link Configured:

If an auxiliary link is configured:

- The left most LED will illuminate if the RF link is active
- The right most LED will illuminate if the Auxilliary link is active
- The middle two LEDs illuminate:

# of LEDs Illuminated	RSSI (dBm)
2	Better than -85
3	Better than -75

Buzzer

The buzzer will sound when either lane detects its Arm or Terminate switch actuated into the active state. This is true regardless of which switch was actuated first.

On/Off

Solid Green	Unit has more than 30 minutes of estimated battery life remaining.
Solid Red	Unit has less than 30 minutes of estimated battery life remaining.

Battery Charging

There is a Lithium-ion battery inside the Operator unit that needs to be recharged routinely. Vin0 is the connection to charge the battery via a dedicated battery-charger adapter. Vin1 is for the optional external power. The unit does not need to be on in order to charge. However, the specifics of the battery and charging differ between revisions of the hardware which are detailed below.

Charging Hardware

Mark I Units
The Vin0 input must be powered with an external 6S CC/CV charger limited to no more than 25.2V and 2.5A.

Mark II+ Units
The Vin0 input is connected to a 8~60V absolute maximum (28V nominal) 40W buck/boost converter to charge the battery.

Battery Part Number

Mark I, some II, and all III+ operator units include a BatterySpace CU-N105R pack, which is a 6 cell 2.6Ah Lithium-ion battery with included over and under discharge protection. The specific battery cells are LG ICR18650B4 B4 rated for discharge between -20 and 60 °C; and for charge between 0 and 45 °C.

Low serial number Mark II operator units include a BatterySpace PR-CU-R972 pack, which is a 6 cell 2.6Ah Lithium-ion battery with included over and under discharge protection. The specific battery cells are Molicel INR-18650-P28A rated for discharge between -40 and 60 °C; and for charge between 0 and 60 °C.

Battery Lifetime

To extend battery service lifetime, care should be taken to ensure that the battery remains within the 20% to 80% state of charge window when storing the unit for long periods of time.

The state of charge of the battery can be monitored via three means:

- The On/Off button will turn red when the battery has less than 30 minutes of runtime remaining.
- Pressing the test button four times in rapid succession will cause the unit to enter brightness adjustment mode, which will also indicate the battery state of charge in the RSSI LEDs where each illuminated LED indicates at least 20% state of charge.
- Monitoring the telemetry of the Lane A processor, only this processor has the ability to see the battery input voltage.

With normal use, the battery should last more than 8 hours at 20°C. The Comet Operator unit should always be operated between -20°C and 60°C and to maximize battery life should be stored and charged at room temperature and out of direct sunlight.

Alternative Modes

Several alternative operating modes for test and maintenance of the Operator unit are available via the Test button.

Functional Test Mode

Any time the Operator unit is in Passive mode, where neither the Arm or Terminate switch is actuated, the unit may be functionally tested by the operator by pressing the Test button. The unit will remain in this mode while any switch is in the actuated state.

In this mode all indicators will present with the following pattern:

Power, Link, and Passive LEDs	Solidly illuminated
RSSI LEDs	Solidly illuminated
Arm and Terminated LEDs	Blinking if the associated switch is not actuated, solid otherwise
On/Off Switch	Alternating between Red and Green
Buzzer	Audible

Brightness Adjust Mode

If the test button is pressed four times in three seconds, the unit will enter brightness adjustment mode where the panel illumination can be modified and persist until the unit is power cycled. In this mode, further presses of the test button will cycle through the available brightness settings.

This mode will also display slightly more granular information about the battery state of charge.

The unit will return to Passive mode if no further presses of the test button are detected in a three second time window and if the Arm and Terminate switches are not actuated.

In this mode all indicators will present with the following pattern:

Power LEDs	Solidly illuminated
RSSI LEDs	Each lit LED indicates at least an additional 20% battery state of charge (e.g. 0 LEDs lit implies less than 20% SoC, 2 LEDs lit implies at least 40% SoC)
On/Off Switch	Alternating between Red and Green
All other LEDs	Blinking
Buzzer	Silent

Adjusting Panel Brightness

The brightness of the Comet Operator panel is controlled by Lane B and can be adjusted in one of two ways:

Temporarily Adjusting Brightness
In the field, the operator can set the panel brightness until the next unit reset by pressing the test button three times in rapid succession to enter Brightness Adjust Mode as discussed in the Alternative Modes section.

Persistently Adjusting Brightness
A persistent change to the unit's panel brightness can be made with the `backlight` command using the command console on Lane B. Backlight intensity is adjustable from 1 to 10 as the single argument to this command, and the setting will need to be saved using the `write_cfg` command to take persistent effect.

More information on the command console is available in the System Setup section.

Adjusting Annunciator Volume

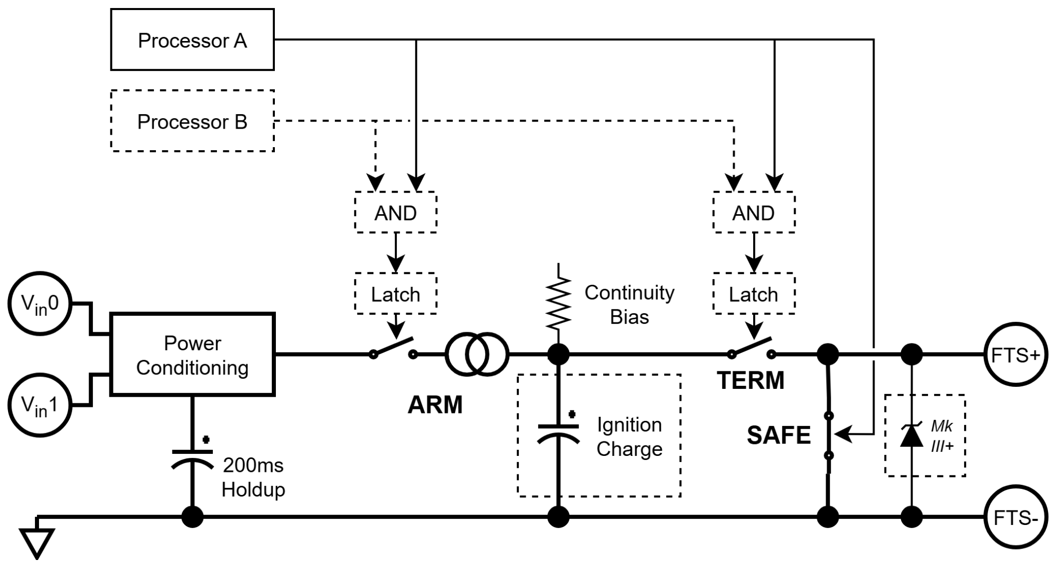
The speaker on the front panel of the Operator unit has a rotating shutter capable of 10dB of attenuation between the fully open and fully closed positions. The operator can adjust this shutter at any time and test the resulting volume change using the Test button.

More control over the range of volume is available via an adjustable trim pot located between the 4 pin battery connector and 2 pin speaker connector on the indicator printed circuit board. This trim pot is user accessible by removing only the back panel of the Operator unit.

Vehicle Unit

Theory of Operation

The Vehicle unit has two independent termination lanes (consisting of a microprocessor, Arm, Terminate, and Safety switches) with power regulation and holdup being shared between the two lanes.



Power flow and voting schematic of a single output (one of two.) Dashed lines indicate an optional component or voting signal from the companion lane available as hardware configuration options.

In the event of power failure on a single power input, the unit will seamlessly switch to sourcing all power from the redundant power input. Failure of an internal power supply may result in the entire unit becoming non-functional although it will not result in an inadvertent termination.

Hardware Options for Output

Voting – If the system integrator wishes to have redundancy inside the unit, then the hardware can be configured to require both processors to assert before the output can transition.

Latching – To protect against hardware or software glitches after termination has been achieved, a hardware latching circuit can be installed.

Output Protection (Mark III+) – To protect the output stage from flyback or other voltage surges, Mark III+ units have a 48V TVS diode installed. This option should not be installed if Comet is driving an external contactor with coil suppression, instead an external series diode should be installed.

Ignition Charge – The ARM switch will limit the continuous output current, but pyrotechnic ignitors and large contactors can require large instantaneous make currents. This can be achieved as a hardware option by the installation of a 680µF capacitor. This should not be installed for digital outputs as it adversely affects the holdup time.

Termination After Loss of Power

Units configured for digital termination output with the signal coming from the voltage bus after the voltage clamp and hold up capacitor are capable of providing a 50mA termination signal with decaying voltage (from the input down to about 12V) for approximately 200ms. In this case, the termination signal and unit power are sourced from the same hold up capacitor and so the signal will no longer be applied to the output once the unit shuts down due to low voltage. If the voltage later recovers, although the unit will reboot, it is unlikely that it will have had the energy to retain the hardware latched termination command.

Units configured for pyrotechnic operation are unable to terminate after loss of power as there is no method to transfer charge from the hold up capacitor to the ignition charge capacitors. Customers needing pyrotechnic termination after power failure are advised to monitor the input voltage rails or flight conditions and Arm the Vehicle unit prematurely so that sufficient charge is available if needed.

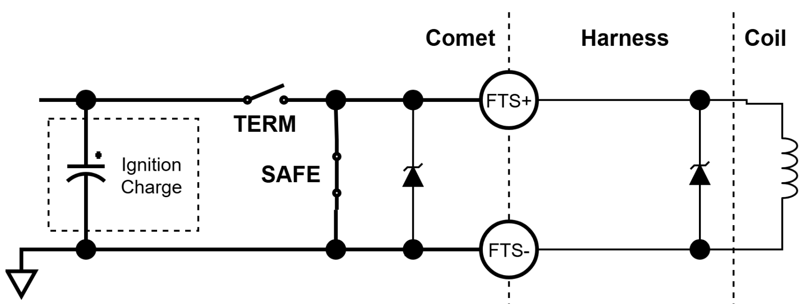
Driving Contactors

If the output of the Comet is used to drive a contactor or other large relay then it is common that the back EMF developed as the output is deasserted is used to quickly drive the physical contacts apart. Unfortunately this back EMF can and will damage the output stage of the Comet if steps are not taken to address it.

In response to units being damaged due to transient voltages, Mark III+ units are equipped with internal TVS diodes. However, these diodes **should not** be used as the primary means of coil suppression.

Parallel Diode Coil Suppression

A reverse biased diode placed across (in parallel with) the coil contacts will allow recirculating current with a small loop as the coil voltage collapses.



However, the integrator should take note that the presence of this recirculating current can cause issues with contact welding due to non linear interactions between the contactor armature spring and coil field[5].

[5] TE reports in Application Note 13C3264 “Coil Suppression Can Reduce Relay Life” that the collapsing field can actually cause the armature to bounce.

Zener + Diode Coil Suppression

To promote fast opening of the contacts, a back to back signal/zener diode is sometimes used to delay starting to recirculate current. Unfortunately, **Comet does not presently support this type of coil suppression** because the SAFE switch is actually a MOSFET with an integrated body diode that will still allow coil current to flow. If the integrator chooses to use this type of coil; an external parallel diode coil suppressor must still be installed in order to protect the Comet (and thus will circumvent the system inside the contactor.)

As a Flight Termination System

Once the Vehicle unit has received a valid termination command from the Operator unit, it will close the ARM switch, allow the ignition charge capacitor to charge, open the SAFE switch, and then close the TERM switch. The unit will relay the termination command via Ethernet or CAN to the rest of the vehicle upon receipt of the command without waiting for the ARM, TERM, and SAFE switches to be in the terminate state.

As an E-Stop

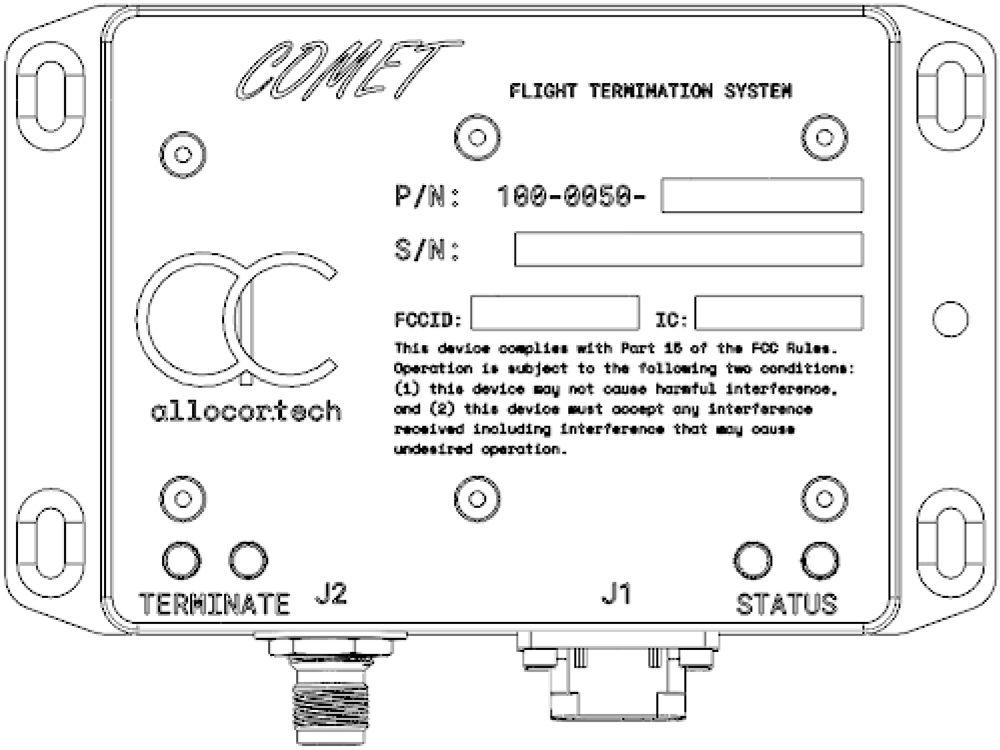
Allocortech intends to issue a more in-depth operators manual for use of Comet an as E-Stop once the reference software has been finalized. Customers wishing to use the Comet as an E-Stop are welcome to inquire and to inform allocortech of their specific requirements. As a general concept however:

The vehicle unit starts with the output disabled and shorted to ground. Once a connection to the operator unit is established, and if all operator units are commanding ‘run’, the vehicle unit will open the SAFE switch and close the ARM and TERM switches to provide a positive ‘run’ signal. The vehicle unit will continuously evaluate if it is safe to continue operating and if it is not, it will open the ARM and TERM switches and close the SAFE switch to provide a ‘stop’ signal.

Standard integrations as an E-Stop would include using the output to…

- Close a power contactor in the ‘run’ state, where removal of power would cause the contactor to open.
- Keep a motor or wheel brake open allowing motion while power is provided.
- Provide a digital signal to downstream motor controllers where a high voltage or a small current loop indicates ‘run’, and the absence of voltage or current indicates ‘stop’.

Indications



Each lane of the Comet Vehicle unit independently controls a Terminate and a Status LED.

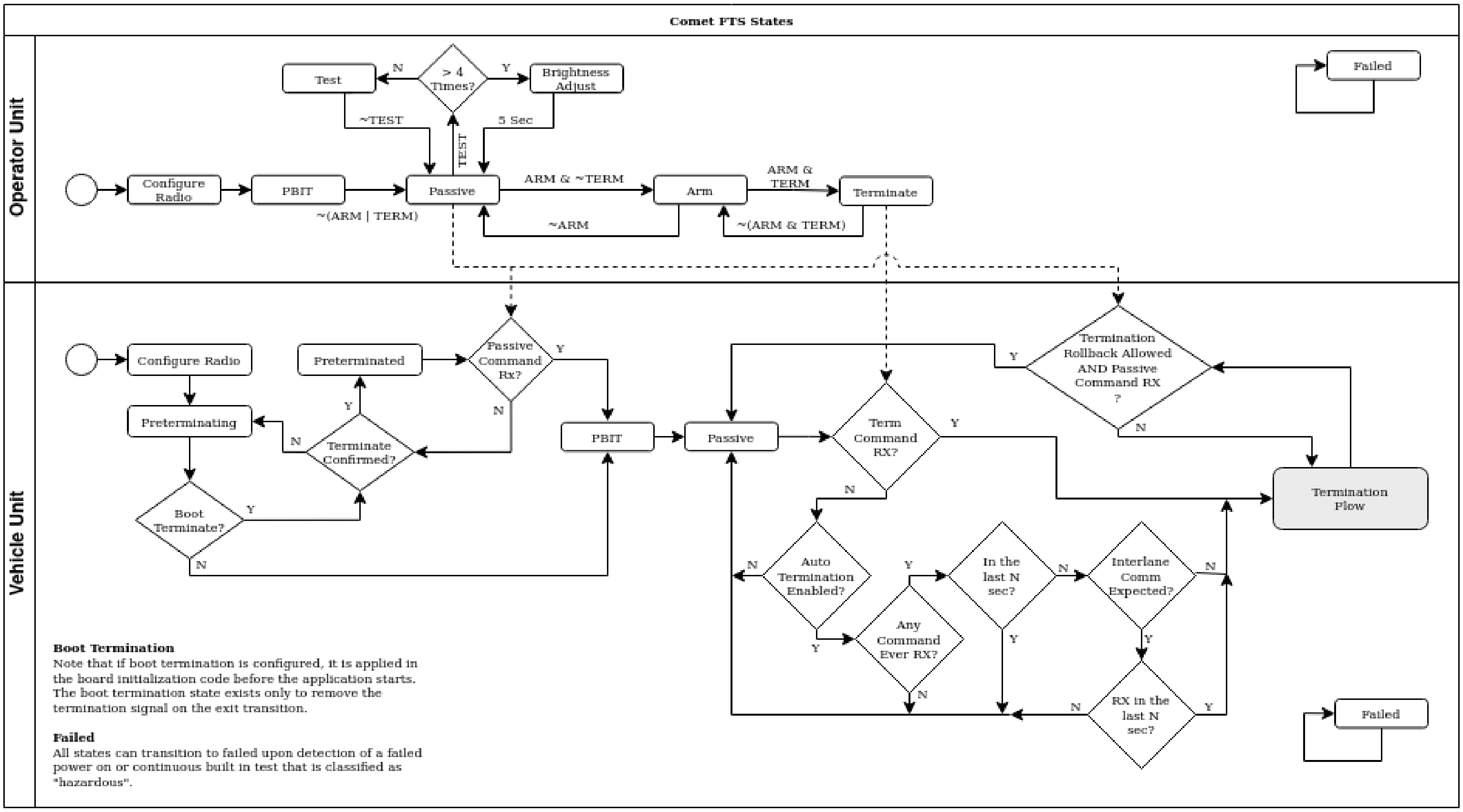
Status

Solidly Illuminated	Vehicle unit is in contact with at least one Operator unit.
Blinking	Vehicle unit is either not in contact with an Operator unit, or the unit has failed its built-in test (in which case Terminate will also be blinking.)

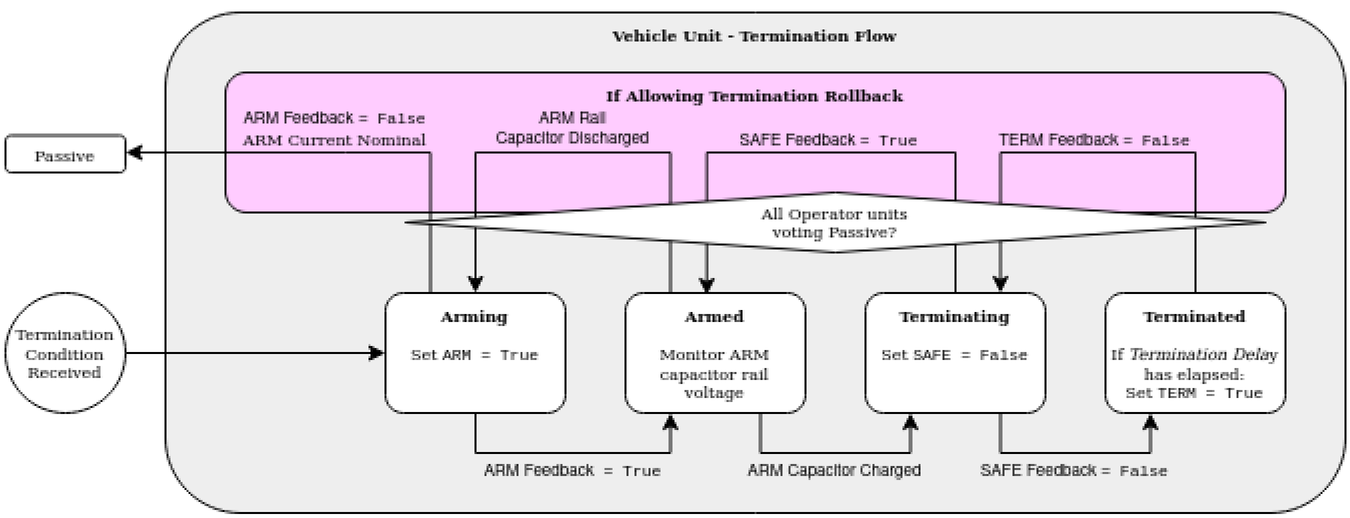
Terminate

Solidly Illuminated	Vehicle unit termination output is live.
Blinking	Vehicle unit is performing or has failed its self test, or is preparing to terminate.
Off	Vehicle is in the Passive state and has passed the self test

Software States and Transitions



Software states of both the Vehicle and Operator units, with command interactions between the two systems shown with a dotted line. State transitions are shown with solid lines.



Vehicle unit termination flow states diagram - broken out of the main software states diagram for clarity due to the complicating option of allowing Termination Rollback and return to the Passive state.

Operator Unit States

Configure Radio

Comet lane A queries the radio for its present configuration, lane B proceeds through to PBIT.

If lane A determines that the radio's present configuration does not match that expected for the vehicle and software configuration, it will attempt to place the radio into its internal AT mode[6] and send the correct configuration via AT and diagnostic commands.

Note: Lane A may stall in this state indefinitely if the Vehicle unit is in range and transmitting as the radio has difficulty accepting the AT configuration commands while simultaneously accepting radio traffic.

PBIT

Both lanes perform various checks on the state of the hardware as determined by the FMEA performed at hardware design time. Failure of any PBIT check, or any critical failure of a CBIT check will result in the unit transitioning to the failed state.

Note: Comet will not transition out of the PBIT state if any switch is in the asserted position.

Passive

Operator unit is ready to receive user input via switches. Comet protocol link will be established with the Vehicle unit, and will be voting Passive.

Test

LED and Switch test state, enter by pressing the Test button. In this state the Lane will transmit Passive to the Vehicle unit, and illuminate all of its LEDs. If the switch corresponding to an LED is not asserted, the LED will blink on and off, otherwise it will illuminate solidly.

Lane A will flash the power button Red and Green.

Comet will exit this state and return to Passive once all the switches are returned to the deasserted state.

Comet will proceed to the Brightness Adjust state if the test button is pressed several times rapidly in succession.

Brightness Adjust

Lane A will display the battery state of charge on the RSSI LEDs.

Lane B will cycle through the available brightness levels with every additional push of the Test switch.

After several seconds without additional input, Comet will return to the Test state.

---

[6] For more information on the radio modes and configuration, see the Diagnosing the Radio Link section.

Arm

When the user asserts the ARM switch, the Operator unit will vote for the Vehicle unit to proceed into the Armed state.

If the ARM switch is deasserted, the unit will proceed back into the Passive state.

Terminate

From the Arm state, if the user asserts the TERM switch, the Operator unit will vote for the Vehicle unit to proceed into the Terminated state.

Note: If the user de-asserts the ARM switch before the TERM switch, the unit will remain in the Terminate state.

Failed

If any continuous built in check fails in a manner that is considered hazardous, the unit will proceed to this state and will vote for the Vehicle unit to remain Passive.

This state may only be exited with a power cycle of the Operator unit.

Vehicle Unit States

Configure Radio

Comet lane A queries the radio for its present configuration, lane B proceeds through to PBIT.

If lane A determines that the radio's present configuration does not match that expected for the vehicle and software configuration, it will attempt to place the radio in AT mode and send the correct configuration via AT and diagnostic commands.

Preterminating

If the *boot time termination* option is configured, the Vehicle unit will assert the ARM and TERM outputs and de-assert the SAFE output. If the allocortech bootloader is installed, the unit will already have these outputs set.

The unit will proceed to PBIT after a short delay if the boot time termination option is not set, or if at least one Operator unit is in contact with the Vehicle unit and if all connected Operator units are voting Passive. The delay allows the filtered measured unit power to return to the nominal level seen during Passive; otherwise the PBIT routine will fail.

Otherwise, it will proceed to the Preterminated state if all the ARM, TERM, and SAFE feedbacks reflect the commanded state.

Note: This state happens prior to PBIT because otherwise the termination output will glitch as the PBIT routine tests the voting and termination logic.

Preterminated

The unit has determined that the ARM, TERM, and SAFE feedback are consistent with commanding "Terminated".

The unit will return to the Preterminating state if at least one Operator unit is in contact with the Vehicle unit and if all connected Operator units are voting Passive; or if the ARM, TERM, or SAFE feedbacks fail to be consistent with the "Terminated" command.

Note: Boot Time Termination and *Termination Rollback* are separate features, however a unit configured with boot time termination will likely wish to also enable termination rollback in order to counteract situations related to Operator units connecting as Passive and then commanding Terminate - for example if the Vehicle unit is powered before an Operator unit, or if multiple Operator units are present and the one unit commanding Terminate drops link for more than the lost link timeout.

PBIT

Both lanes perform various checks on the state of the hardware as determined by the FMEA performed at hardware design time. Failure of any PBIT check, or any critical failure of a CBIT check will result in the unit transitioning to the failed state.

Some implied Lane coordination happens in this state as units that are hardware configured to vote on the ARM and TERM outputs must both vote simultaneously. This coordination happens in the time domain under the assumption that both lanes started roughly at the same time.

However, PBIT will be skipped if the lane detects that it was reset from something other than a cold boot which should prevent problems if the lane were to restart in the air.

Passive

The lane is waiting for commands from an Operator unit and the termination output is verified to be safe.

This state will automatically transition to Arming if *Lost Link Terminate* is active and if the Operator links have been lost. Otherwise it will only transition to Arming if commanded by an Operator unit.

Arming

The Lane is preparing to terminate by closing the ARM switch and waiting until the ARM rail capacitor has been charged. If no capacitor has been installed, we still progress through this state but there is no hardware imposed delay because the voltage will rise nearly instantaneously.

Armed

The ARM rail is near the input voltage, and if commanded to terminate by the Operator unit or configuration, the lane will open the SAFE switch and transition to Terminating.

Terminating

If the SAFE switch has been verified to be open, the lane will continue to the Terminated state.

Terminated

If *Termination Delay* has been configured, this state will wait the configured time before releasing the TERM output for the corresponding termination output. This is important for units that are configured to vote.

Note: Due to *Termination Delay*, the lane may report to be in the Terminate state before the Terminate output is live. This may result in a false indication to the operator until the configured termination delay expires. This known errata exists in part because Comet wants to notify external entities via telemetry that a valid termination command has been received and that those external units should take any necessary action.

Failed

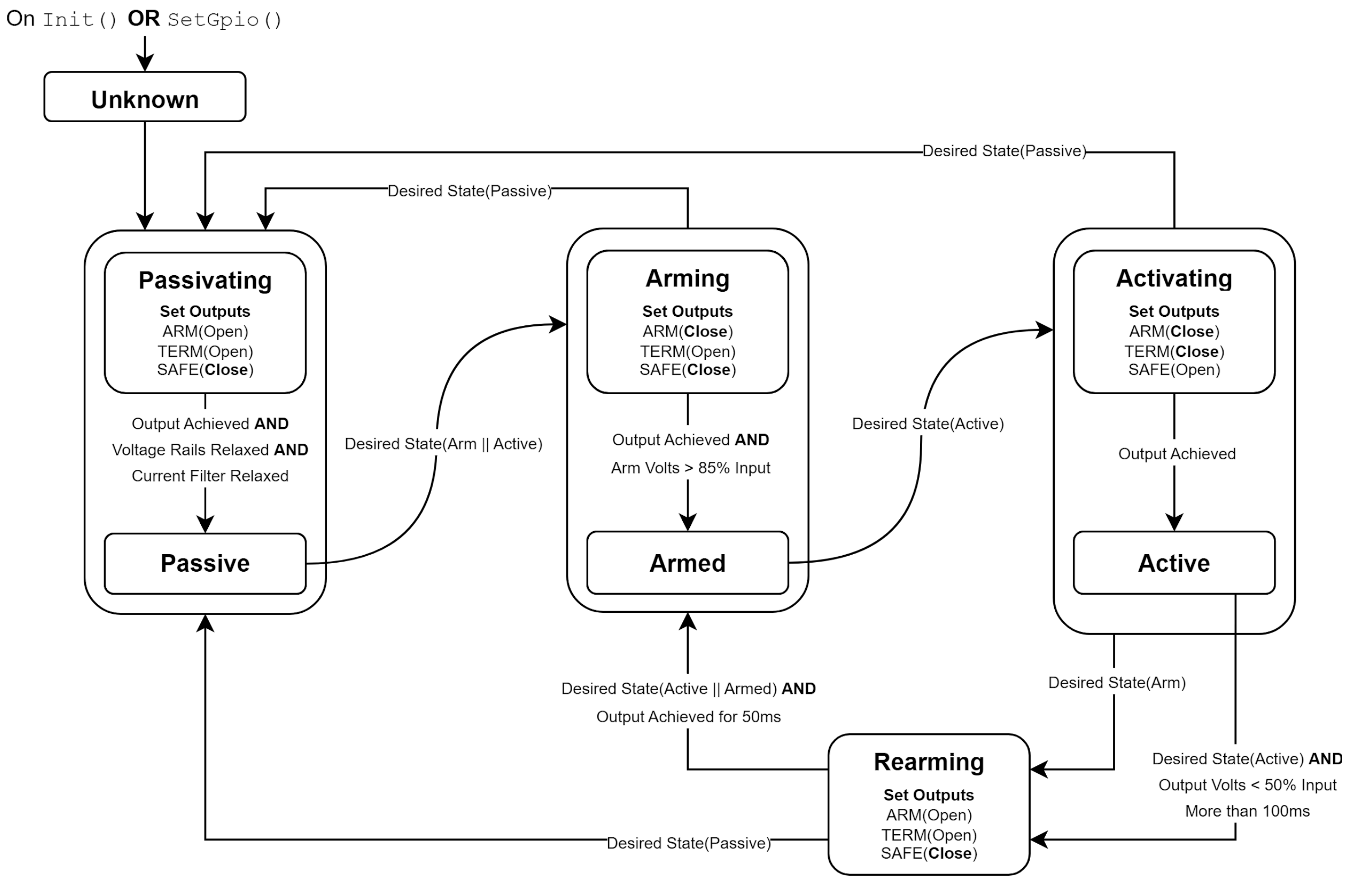
If any continuous built-in check fails in a manner that is considered hazardous, the unit will proceed to this state and attempt to make the termination output safe.

However, in this state the termination output should be considered active, or that it could become active, and additional steps should be taken by the user to ensure that the vehicle is actually in a safe condition before continuing work.

This state may only be exited with a power cycle of the Vehicle unit.

Output State Machine

The broader application state machines will coordinate with an inner state "3 State Output" state machine to safely transition between active and passive output states.



The 3SO states roughly correspond to the application states; but if, for example, the `set_active_in_arm` option is used, then the 3SO will be asked to transition to Active while Comet is in the Arming/Armed states.

Available Telemetry

By default, Comet emits telemetry in allocortech's native YAPP (Yet Another Packet Protocol) format. The protocol is similar to many packet formatting protocols, and includes a header, packet payload and a CRC for data integrity checks. This document will not go through all of the details of the protocol, but a basic Ethernet message is broadly constructed as follows.

Header						Payload	CRC
SYNC[2]	Seq[1]	CTL[1]	ID[4]	Size[2]	RSVD[2]	*Size* Bytes	32-bit CRC

Messages sent over CAN are similar, but are chunked and aspects of the ID and sequence numbers are incorporated into the CAN ID. For more information about how CAN YAPP works, please contact allocortech.

`SYNC`: Synchronization header of "`YP`"

`Seq:` Sequence number, increments for every newly created message under the given ID

`CTL:` Control byte, always 0 for Comet

`ID:` YAPP message identifier. Comet IDs are 11 bits with

```
[   CLASS    ] [   ID   ] [ BOX ] [ LANE ]
 10        9   8       4  3    1     0
```

The message IDs given for each message below embed the message class.

`Size:` Size of Payload in bytes

`RSVD:` Reserved bytes for future use

`CRC:` YAPP message payloads are protected with the Koopman Hamming distance 6 order 32 (aka `CRC-32K/6.4`) cyclic redundancy check. This CRC has a polynomial of `0x1'32c0'0699`, is computed with a starting value of `0xFFFF'FFFF,` and does not invert the output.

In the tables below, most types are described as if they were C standard types, and all types in YAPP are defined to be little endian. Some amount of protocol compression is allowed for floating point types, and is identified by `<min, max>` after the type name and width. When a data type is compressed, there are 5 reserved values:

`Not a Number`	`max`	All signaling and none signaling IEEE 754 values
`Positive Infinity`	`max - 1`	Special case of out of range high
`Negative Infinity`	`max - 2`	Special case of out of range low
`Out of Range High`	`max - 3`	Initial value was greater than `max` (but not infinity)
`Out of Range Low`	`max - 4`	Initial value was less than `min` (but not infinity)

As an example, `float16 <-10.0, 5.0>` would map the following values:

```
-10.0    -> 0 counts
0.0      -> 43,687 counts
5.0      -> 65,530 counts
NaN      -> 65,535 counts
```

Structure Definitions

Comet Vehicle State (Enum)

Operating states of the Comet Vehicle unit.

Name	Value	Description
Config Radio	`0x00`	Unit has just powered up and is ensuring the radio is configured.
Preterminating	`0x0A`	Unit has booted, and if configured to terminate at boot will confirm that and proceed to the preterminated state. Otherwise it will proceed to the PBIT state.
Preterminated	`0x0D`	Unit has booted, and has confirmed that it is in the terminated state, but is waiting for a Passive command from a ground unit to proceed.
PBIT	`0x11`	Unit has just powered up and is performing power on self tests.
Passive	`0x22`	Unit has passed self tests and is waiting for Operator commands.
Arming	`0x33`	Unit has received the Arm or Terminate command and is preparing to terminate.
Armed	`0x44`	Unit has received the Arm command and is ready to terminate.
Terminating	`0x55`	Unit has received the Terminate command and is preparing to terminate.
Terminated	`0x66`	Unit has terminated.
Failed	`0x77`	Unit has failed a built in test routine, is no longer safe to operate, and will not attempt to respond to Operator unit commands. Not all faults result in this state, some recoverable or non-critical faults will merely prevent the state from progressing forward.

Comet Operator State (Enum)

Operating states of the Comet Operator unit.

Name	Value	Description
Config Radio	`0x00`	Unit has just powered up and is ensuring the radio is configured.
PBIT	`0x11`	Unit has just powered up and is performing power on self tests.
Passive	`0x22`	Unit has passed self tests and is waiting for user interaction.
Armed	`0x33`	Unit has seen a transition on the ARM switch from Passive to Active and TERM is Passive.
Terminating	`0x44`	Unit has seen a transition on the TERM switch from Passive to Active while Armed and is commanding the Vehicle unit to terminate.
Testing	`0x55`	Unit push to test button is Active.
Failed	`0x66`	Unit has failed a built in test routine.
Config LED PWM	`0x77`	Operator is changing the display brightness (by pressing the test button)

Comet Common Faults (Bitfield)

Faults that are common to both the Vehicle and Operator units.

Name	Bit	Description
Radio Event Early	1	Radio event (Lane A: DCD, Lane B: TDMS) happened earlier than expected. Possible RF Link overutilization.
Radio Event Late	2	Radio event (Lane A: DCD, Lane B: TDMS) happened later than expected. Possible latency guarantee violation.
Radio Link RSSI Low	3	Indicates that the RSSI of either the Vehicle or Operator side is lower than the lowest RSSI LED illumination setpoint (`kRssiLedLevels[0]`.)
Radio Management Timeout	4	Updates on the radio management link have not happened in more than XXX seconds.
Logic Volts	5	One or more of the low voltage rails reads out of specification.
Cross Link Timeout	6	No traffic has been seen on the cross link UART for XXX seconds.
Temperature	7	One or more of the temperature sensors reads out of specification.
Radio Link SNR Low	8	Indicates that the signal to noise ratio is lower than 20dBm
CPU Usage	9	One or more of the monitored threads is using more than the expected amount of CPU.
Stack Usage	10	One or more of the monitored threads is using more than the expected amount of stack.
PBIT Timeout	11	Power on built in tests took too long to complete and were skipped.
Return Current Low	12	The return current appears too low compared to the input current, indicative of a potential broken return wire.
Excessive Current Draw	13	Measured input current is excessively high for the current operating mode.
Logic Overvoltage Protection	14	Over-voltage protection monitoring on the 3.3V rail is out of specification.
Backfeeding Current	15	Excessive negative current has been detected implying that the input power diodes may be compromised and thus the unit may be back feeding one lane to another.
Radio RF Volts	16	Normally we expect to feed the radio around 3.5V; but if this reads outside of that range something has gone wrong. Typically this is indicative of bad matching between the radio and its antenna.

Comet Vehicle Faults (Bitfield)

Faults that are specific to the Vehicle unit.

Name	Bit	Description
ARM Rail Bias	1	When not ARMed, the bias voltage reads out of specification.
ARM Rail Charge Timeout	2	While ARMing, it took too long for the ARM rail to reach the input voltage.
TERM Rail Bias	3	When not terminating, the termination rail reads high (not SAFE.)
GPIO Loopback	4	The digital loopback between the ARM and TERM GPIO controllers is not reading back values correctly. This means they may be misconfigured, or communication with the controllers may be suffering from some form of fault.
ARM Overvoltage Protection	5	The over-voltage lockout protection on the ARM switch reads out of specification.
Radio Link Timeout	6	No Operator unit message has arrived on the RF link in XXX milliseconds.
Input Volts	7	The monitored input voltage rail (before the diode OR) is out of specification.
ARM Charge Failure	8	The squib capacitor installed on the ARM rail does not match expected capacitance
Input Holdup Failure	9	The input holdup capacitor has failed PBIT testing.
ARM State Invalid	10	Digital ARM signal feedback is not in the commanded state.
TERM State Invalid	11	Digital TERM signal feedback is not in the commanded state.
SAFE State Invalid	12	Digital SAFE signal feedback is not in the commanded state.
ARM Rail Current	13	When not terminating, the ARM rail current reads out of range. (Excessive leakage indicating component failure.)
PBIT Skipped	14	PBIT was not run due to the type of reset condition performed.
Lost Link Terminate Warning	15	Indication that the Comet will terminate due to lost link unless a valid ground command is received soon.
Auxiliary Link Timeout	16	No Operator unit message has arrived on the auxiliary link in XXX milliseconds.

Comet Operator Faults (Bitfield)

Faults that are specific to the Operator unit.

Name	Bit	Description
Radio Link Failure	1	Indicates that the unit has not received a message from Vehicle unit with its `kRssiValidFlag` bit set in more than `kAirGndMsgTimeout` seconds.
Battery Voltage Low	2	Battery has less than 30 minutes of charge remaining
Auxiliary Link Failure	3	No Vehicle unit message has arrived on the auxiliary link in XXX milliseconds.
TDMA Sync Late	4	The unit has not seen a TDMA sync pulse in some time. This can cause lost link on lane B.
Reserved	5~16	-

Common Status (Structure)

This structure is reported by both the Vehicle and Operator units as part of their unique status messages.

Data Type	Name	Units	Description
`float32`	V_{In} Positive	Amps	Positive and negative leg current sense readings at the point they enter the logic board. Notionally used for detecting broken wires or sneak current paths if a negative reading is near zero, or if the inflows do not equal the outflows. Lane A reads $V_{In}[0]$ (aka operator unit battery), Lane B reads $V_{In}[1]$ (aka operator unit auxiliary.)
`float32`	V_{In} Negative	Amps	
`float32`	V_{In}	Volts	Positive leg voltage reading at the input to the logic board. Lane A reads $V_{In}[0]$, Lane B reads $V_{In}[1]$.
`float32`	V_{In} OR	Volts	Input voltage reading of the common bus after the diode OR circuit.
`float32`	$V_{PS,In}$	Volts	Input voltage reading of the common bus after the overvoltage protection circuit.
`float32`	$PSU_{5.0}$	Volts	Logic bus voltage monitor: 5.0V
`float32`	$PSU_{4.0}$	Volts	Logic bus voltage monitor: 4.0V (Analog bias)
`float32`	$PSU_{3.5}$	Volts	Logic bus voltage monitor: 3.5V (Radio RF)
`float32`	$PSU_{3.3}$	Volts	Logic bus voltage monitor: 3.3V (Logic)
`float32`	$PSU_{0.5}$	Volts	Logic bus voltage monitor: 0.5V (Analog bias)
`float32`	$PSU_{-5.0}$	Volts	Logic bus voltage monitor: 5.0V (Termination bias)
`float16 <0, 0.6>`	Overvolt Input	Volts	Lane A only, 3.3V rail over-voltage lockout tap at I_{in} clamp
`float32`	Logic PCBA Temperature	°C	Lane A: Top side, measured near power conditioning circuitry. Lane B: Top side, measured near the radio heat sink.
`float32`	CPU Temperature	°C	Lane CPU die temperature
`uint32`	Number of Flash ECC Single Faults	-	
`uint32`	Number of RAM ECC Single Faults	-	
`float8 <0, 100>`	Total CPU Usage	%	
`float8 <0, 100>`	App Thread CPU Usage	%	
`float8 <0, 100>`	Telemetry Thread CPU Usage	%	
`float8 <0, 100>`	lwIP Thread CPU Usage	%	
`float16 <0, 100>`	App Thread Stack Usage	%	
`float16 <0, 100>`	Telemetry Thread Stack Usage	%	

Data Type	Name	Units	Description
`float16 <0, 100>`	lwIP Thread Stack Usage	%	
`uint16`	Common Faults	-	Bitfield, see the Comet Common Faults (Bitfield) table for more information.
`float16 <-1.0, 8.0>`	V_{In} Positive (Filtered)	Amps	Filtered versions of V_{In} Positive and V_{In} Negative, mostly for cross lane power measurement purposes.
`float16 <-1.0, 8.0>`	V_{In} Negative (Filtered)	Amps	

Message Definitions

Vehicle Unit Status

YAPP Message ID: `0x61X, where X is <3 bits box ID> <1 bit lane ID>`
Default Period: 10 ms
Size: 163 bytes

Data Type	Name	Units	Description
`int64`	Timestamp	ns	Local time on the Vehicle unit when this message was prepared.
`uint8[2]`	Operator to Vehicle State Command	-	Command received from each Operator unit.
`int8[2]`	Operator to Vehicle RSSI	dBm	Received signal strength as reported by the Vehicle unit radio for each of the Operator units.
`bool[2]`	Operator to Vehicle Link Up	-	True if the Vehicle unit considers the command from each Operator unit valid.
`int64[2]`	Operator to Vehicle Last RF Message Timestamp	ns	Time of last received valid RF message.
`uint8`	Vehicle Unit State	-	See Comet Vehicle State (Enumeration) table
`float16 <0, 60>`	ARM Rail	Volts	Voltage of the rail between the ARM and TERM MOSFETs.
`float16 <0, 30>`	ARM Rail	Amps	Current flowing through the ARM MOSFET.
`float16 <0, 60>`	TERM Rail	Volts	Voltage after the TERM MOSFET, applied to the downstream unit.
`float16 <0, 2>`	Logic Overvoltage Monitor	Volts	Both lanes, 3.3V rail over-voltage lockout tap at ARM switch.
`bool`	ARM Feedback	-	Readback of the ARM signal from the GPIO expander feedback.
`bool`	TERM Feedback	-	Readback of the TERM signal from the GPIO expander feedback.
`bool`	SAFE Feedback	-	Readback of the SAFE signal from the GPIO expander feedback.
`uint16`	Vehicle Faults	-	See Comet Vehicle Faults (Bitfield) table.
`structure`	Common Status	-	See Common Status (Structure) table.
`int64[2]`	Operator to Vehicle Last Auxiliary Message Timestamp	ns	Time of last received valid auxiliary message.
`uint8_t`	RF TX Max	-	Bitfield indicating which operator units are allowed to transmit.
`bool[2]`	Operator to Vehicle RF Link Up	-	True if the Vehicle has recently received messages from the operator over the RF link
`bool[2]`	Operator to Vehicle Aux Link Up	-	True if the Vehicle has recently received messages from the operator over the Aux link

Operator Unit Status

YAPP Message ID: `0x62X, where X is <3 bits box ID> <1 bit lane ID>`
Default Period: 10 ms
Size: 141 bytes

Data Type	Name	Units	Description
`int64`	Timestamp	ns	Local time on the Operator unit when this message was prepared.
`uint8`	Operator Unit State		See Comet Operator State (Enumeration) table
`uint8`	Reflected Vehicle State		Last received Vehicle unit state.
`int64`	Vehicle to Operator Unit Last RF Message Timestamp	ns	Time of last received valid RF message (directly via the radio.)
`bool`	Test Switch State		Debounced reading of the Test switch.
`bool`	Arm Switch State		Debounced reading of the Arm switch.
`bool`	Terminate Switch State		Debounced reading of the Terminate switch.
`float8 <0, 100>`	Battery SoC	%	Battery capacity remaining percentage based on Open Circuit Voltage lookup table.
`int64`	Estimated Battery Time Remaining	ns	Estimated amount of time remaining before battery is drained.
`int8`	Vehicle to Operator Unit RSSI	dBm	Received signal strength as reported by the Operator radio for the Vehicle unit.
`uint16`	Operator Unit Faults		See Comet Operator Faults (Bitfield) table.
`int8[2]`	Reflected Operator to Vehicle RSSI	dBm	Received signal strength as reported by the Vehicle radio for each of the Operator units.
`bool[2]`	Reflected Operator to Vehicle RF Link Up		Indication from Vehicle unit if it is receiving valid packets from a given Operator unit via the RF link.
`structure`	Common Status		See Common Status (Structure) table.
`int64`	Vehicle to Operator Last Auxiliary Message Timestamp	ns	Time of last received valid RF message (via the aux channel.)
`bool[2]`	Reflected Vehicle to Operator Unit Auxiliary Link Up		Indication from Vehicle unit if it is receiving valid packets from a given Operator unit via the auxiliary link.

Radio Statistics

These radio statistics are routinely collected by Lane A over the diagnostic link. Descriptions, where available, are either taken from the Microhard Application Note *The Diagnostics Channel Protocol, Model P900* Revision 1.04, or amended based on field experience.

YAPP Message ID: `0x63X, where X is <3 bits box ID> <1 bit, always 0>`
Default Period: 30 ms
Size: 134 bytes

Data Type	Name	Units	Description
`int64`	Timestamp	ns	Unit time data was collected.
`float`	Radio Temperature	°C	Parameter 55, offset of 55°C subtracted
`int8`	RSSI Average	dBm	Parameter 60 (Vehicle unit), Parameter 61 (Operator unit)
`int8`	Noise Average	dBm	Parameter 62 (Vehicle unit), Parameter 63 (Operator unit)
`float`	Voltage	Volts	Parameter 118, converted from mV
`uint32`	Payload Bytes RX	-	Fields gathered from parameter 97.
`uint32`	Bytes RX	-	
`uint32`	Payload Bytes TX	-	
`uint32`	Bytes TX	-	
`uint32`	Error Correction Count	-	
`uint32`	Packets Dropped due to Memory	-	
`uint32`	RX Packets Dropped due to Age	-	
`uint32`	Packets TX	-	
`uint32`	Packets RX	-	
`uint32`	CRC Errors	-	
`uint32`	Synchronization Lost Events	-	
`uint32`	Synchronization Count	-	
`uint32`	Number of Packets with Errors	-	
`uint32`	Packets Dropped due to Payload CRC Errors	-	
`uint32`	RX Packets Dropped due to Age	-	
`uint32`	MAC TX Busy Time Total	ms	
`uint32`	MAC TX ACK Expected	-	
`uint32`	MAC TX ACK Missed	-	
`uint32`	Number of CTS Events	-	
`uint32`	Number of RTS Events	-	

Data Type	Name	Units	Description
`uint32`	Number of Packets Dropped due to Routing	-	
`uint32`	Count of Invalidated Routes	-	
`uint32`	Receiver Busy Events	-	
`uint32`	Channel Access Time	-	
`uint32`	Channel Access Counter	-	

Radio Channel Information

Comet Lane A routinely asks the Radio for information about the hopping channels.

YAPP Message ID: `0x64X, where X is <3 bits box ID> <1 bit, always 0>`
Default Period: 100 ms
Size: 422 bytes

Data Type	Name	Units	Description
`int64`	Timestamp		
`uint8`	Hop Mode		`0:` HopOnPattern `1:` HopOnFrequencyTable `2:` HopOnChannel `3:` HopOnFrequency
`uint16`	Test Channel	-	
`uint8`	Pattern Length	-	Number of populated channel data structures (remainder contain random data from the radio)
`uint16`	Minimum Channel #	-	Lowest channel number in the hopping pattern.
`uint16`	Maximum Channel #	-	Highest channel number in the hopping pattern.
`uint16`	Channel Space	kHz	Inter-channel spacing
`uint32`	Start Frequency	kHz	Hopping start frequency (channel number base.)
`uint16[64]`	Channel #	-	Channel number index for the following data set.
`int8[64]`	Channel RSSI Average	dBm	Channel RSSI average, over the last N hops.
`int8[64]`	Channel Noise Max	dBm	Maximum channel noise level, over the last N hops.
`int8[64]`	Channel Noise Minimum	dBm	Minimum channel noise level, over the last N hops.
`int8[64]`	Channel Noise Average	dBm	Average channel noise level, over the last N hops.

Aux Channel Messages

Both the Vehicle to Operator and Operator to Vehicle messages are contained as a fixed length opaque data blob in a YAPP frame.

Vehicle to Operator

YAPP Message ID: `0x41X, where X is <3 bits, always 0> <1 bit lane ID>`
Default Period: 250 ms
Size: 48 bytes (as YAPP, 32 bytes on RF link)

Operator to Vehicle

YAPP Message ID: `0x40X, where X is <3 bits box ID> <1 bit lane ID>`
Default Period: 33ms
Size: 42 bytes (as YAPP, 26 bytes on RF link)

System Setup

Connecting via RS-232 Serial Port

A Lane multiplexed RS232 port is present on the J1 connector. Selecting the Lane to talk to is accomplished by toggling pin 8 (MCU Select) on J1 where a short to GND indicates Lane A and a 5V signal indicates Lane B. It is most convenient to the operator if the MCU Select pin is connected to the RS232 cable's RTS pin for programmatic operation.

The default application listens on this port at 500kbps with 8 data bits, no parity bit, and 1 stop bit. (This is also the configuration of the JTAG UART.)

Once connected, pressing enter should bring up a command shell. The most useful general purpose commands may be:

`help` — Print the list of known commands and a brief description of what each command does.

`reset` — Performs a soft reset of the Lane processor. Will not reset the other Lane. Can be used with the following optional arguments:

- `reset bootloader` — Boot into the bootloader slot if something like the `comet_bootyloader_app` is installed
- `reset bootrom` — Boot into the STM32 built in bootloader in order to flash with the `stm32flash` tool.

`version` — Displays the compile time version statistics of the running application and of the bootloader, if installed. The reported Git SHA will be truncated to 4 hexadecimal digits if the application was built from a dirty git repository.

`state` — If the Comet application is running, this will display information about the state of the lane CPU, the RF link, and any active faults.

On the vehicle unit specifically, the `Term Chain` line which looks like:

```
Term Chain: <ARM Volts> <ARM Amps> <TERM Volts> <3.3V Voltage Check>
                     (<ARM Feedback> <TERM Feedback> <SAFE Feedback>)
```

Displays the voltage on the rail between the ARM and TERM switches, the rail charging current, the voltage on the output pin, and a diagnostic voltage at the monitoring circuit which will suicide the unit if it looks like the 3.3V rail has shorted to 5V or any other rail.

The feedback indications show the voted state of each output switch.

For more in-depth general debugging, here are some other commonly used general commands:

`adc`	Print the status of all analog inputs to the Lane.
`canstat`	Display statistics about the CAN buses, such as their operating mode and error counters.
`cpuusage`	Prints a summary percentage of all the CPU usage, including interrupt service routines.
`gpio`	Print the status, or modify the value of, all the GPIO pins connected to the Lane. Note that GPIO pins controlled by the application will likely immediately switch back as the application thread asserts most state on every application loop iteration.
`heap_info`	Display information about the dynamically allocated memory, note that `sram3` is an independently managed pool by the `lwIP` embedded networking library and statistics about this pool are not available.
`mem`	Read or modify arbitrary memory locations on the processor.
`top`	Display detailed statistics about all threads in the system, including stack usage.
`uartstat`	Display statistics about the UART devices.

Working with Non-Volatile Storage

The last sector of each Lane processor flash is dedicated to storing the application configuration. End users are welcome to add additional configuration keys, but this manual only details those commands present in the standard configuration.

In general, each console command, if given without arguments, will print the current configuration. If given with arguments, changes are saved to RAM and not written to the flash until the `write_cfg` command is issued. Changes are generally not applied to the running application until the unit is power cycled or `reset`.

`write_cfg`	Commit the configuration stored in RAM into the internal non-volatile Flash.
`read_cfg`	Read the configuration stored in Flash into RAM.
`erase_cfg`	Erase the configuration stored in non-volatile Flash.
`print_cfg`	Print to the console the text of all the configuration commands.

Mark II Comet FTS include both a large NAND EEPROM for logging, a 1-wire serial EEPROM for manufacturing information, and a method to connect to an additional 1-wire serial EEPROM in the harness. As of the writing of this document, the Comet FTS application does not make use of these flashes and no shell commands exist to interact with or modify them.

Commissioning Units

Each complete Comet Flight Termination System, consisting of 1 Vehicle unit and up to 2 Operator units, is uniquely specified using a common vehicle ID and Lane specific cryptographic signing keys. Each unit in the system is identified with a unit ID, where the Vehicle unit is always 0.

Note that the limitation of 2 Operator units per FTS is a soft limitation, but altering this limit will require changes to either the radio protocol, or the message transmission frequency. Therefore, the Operator unit IDs, in a nominal configuration, will be either 1 or 2.

Additionally note that the vehicle ID and the Lane A signing key feed into the radio network ID which additionally specifies the radio channel hopping pattern. Unique vehicle IDs are required to differentiate telemetry sources in shared telemetry networks, and unique lane keys are required to prevent message forgery from third party adversaries and to prevent message confusion between lanes.

Unique Lane keys can be generated on device using the built in hardware random number generator using the `gen_key` command.

Once a key has been generated, the units may be paired using the `commission` command which takes 3 arguments, in order: the vehicle id (from 0 to 7), the unit ID (0 if Vehicle, 1 or 2 if Operator), and the cryptographic signing key. Running the `commission` command without arguments will print the current pairing settings and a hash of the key.

The `commission` command must be run on both Lanes as configuration is not shared between Lanes. Note that the Lane key should be different between the two Lanes, but all Lanes in the pairing should share the same key.

Once the `commission` command has been run, save the configuration to non volatile storage using the `write_cfg` command.

`commission`	Set the units pairing information, e.g
	`commission <vehicle ID> <unit ID> <lane key>`
	
	To print all pairing information, including the lane key:
	`commission true`

`gen_key`	Generate a random lane key to pass to the commission command

Ethernet Network Settings

The Ethernet stack on the Comet is capable of 10/100 Mbps full duplex communication with a MAC address generated from the CPUs unique ID. As this is effectively a random, albeit static, MAC address that is not allocated by the IEEE, the locally administered address bit is set. At this time it is not possible to set the MAC address of the interface using the console.

It is however possible to set the IP address to either a static IPv4 address, or to instruct the unit to request an address via DHCPv4. Do this with the `set_ip_config` command.

`set_ip_config`	`off`	Disable networking on this Lane
	`dhcp`	Obtain a dynamic IPv4 address via request to the DHCP server
	`static`	Using three arguments set the IP address, network mask, and gateway. For example: `set_ip_config static 192.168.0.2 255.255.255.0 0.0.0.0`

Normally telemetry is emitted via UDP to the broadcast address on port 10,000 but this can be customized with the `set_eth_telem_ip` command.

```
set_eth_telem_ip <destination IPv4 address> <destination UDP port>
```

Controller Area Network Settings

The Comet FTS has a CAN-FD link per Lane, although the pins are only exposed on the J1 connector if the hardware option of Lane A Ethernet, Dual Lane CAN was selected at hardware build time. Configure the baud rates and FD mode using the `set_can_config` command.

`set_can_config`

`off`	Disable CAN on this Lane
Single argument	Set the nominal CAN bitrate and disable CAN-FD
Two arguments	Set the nominal and the FD bitrates

Telemetry Customization

By default Comet will emit telemetry on both the CAN and ethernet interfaces, and with all messages. The `set_telem_timing` command allows the user to customize what messages are sent on what interfaces at a customizable rate.

```
set_telem_timing <interface> <message> <period (ms)> <offset (ms)>
```

`interface`	Either `can` or `eth` (for ethernet.)
`message`	One of `status`, `rf`, or `rfchan.` See the message definitions in the sections above for more information about each message type.
`period`	The emission rate of the message in milliseconds, must be a multiple of 10ms.
`offset`	Move the message, in a multiple of 10ms, within its configured period.

For example, if a user wanted to emit via Ethernet the radio statistics message every second, but at a 250ms offset (e.g. sending at 0.25, 1.25, 2.25, etc) then the command would be:

```
set_telem_timing eth rf 1000 250
```

RF Command Path

Comet Lane A controls the RF link and timing. Lane B sends messages through the crosslane UART to Lane A to forward over the appropriate link in a single conjoined Lane A/B message. This message conjoining does mean that the loss of Lane A results in a loss of Lane B's ability to terminate.

Vehicle Lane A steers timing across all joined units and, with use of the RF mask, controls which Operator units are allowed to transmit over RF. Units are always allowed to transmit over the Aux link and will do so even if connection to the Vehicle unit is lost.

The varying amount of bandwidth available in the various radio types results in different default RF message rates, but the actual rate can be set using the `set_rf_command_path` command which has the following defaults:

Band	Epoch Period	Vehicle		Operator		
		Divider	Burst Count	Divider	Burst Count	Scheduler
400 MHz	50 ms	10 (2 Hz)	N/A	1	3	Triggered
869 MHz		20 (1 Hz)	N/A	1	1	Triggered
900 MHz		5 (4 Hz)	N/A	2 (10 Hz)	N/A	Periodic

Comet Vehicle and 900 MHz Operator always operate under a periodic transmit scheduler where the RF message is always sent at the rate specified by the divider (the clock will tick at 50ms, this is known as an RF epoch.) For 400 and 869 MHz units, the Operator unit will send some number of messages (the `Burst` count) separated by `50ms × Divider` every time the unit receives a Vehicle unit RF message.

```
set_rf_command_path <TX period divider> [TX burst count]
               TX Divider        Divisor for the RF Epoch clock (50ms)
               TX Burst          How many messages to send per trigger event
```

On 400 MHz units, due to bandwidth limitations and the need to explicitly schedule transmit slots, only a single Operator unit is allowed to be active on the RF link.[7] However, failover between operator units is allowed by using the `set_rf_policy` command which allows the Vehicle unit to switch which specific Operator units to transmit on request.

```
set_rf_command_path
   <max operators> <max simultaneous> <hysteresis ms> <change period ms>

   Max Operators                  Total number of operators in link (must start at ID 1)
   Max Simultaneous               How many are allowed to transmit simultaneously
   Hysteresis MilliSeconds        How long to stay with a given operator unit after link
                                  timeout.
   Change Period MilliSeconds     How long to allow an operator unit to attach before
                                  selecting the next potential unit.
```

[7] This is a software limitation.

Auxiliary Command Path

Comet can send and receive commands over Ethernet in order to provide link diversity over some other communications system. The normal RF packets are encapsulated into YAPP frames and then sent via UDP to an IP address (which can be the broadcast address) and port of the end user's choosing. Although the normal timeout and expiry[8] rules apply, to reduce bandwidth the auxiliary link can send messages at a reduced rate of the users choosing.

When operating with an auxiliary command path, both the Vehicle and Operator units will indicate a link if either the primary RF link or the auxiliary path is valid. The RSSI lights on the Operator unit, however, will only reflect the signal strength of the primary link. To aid in operator awareness and for logging, the `RadioLinkTimeout` and `AuxLinkTimeout` faults as well as the `XXX_rf_time` and `XXX_aux_time` telemetry values help to discriminate the two links. The `status` command on both unit types will display similar information to that in telemetry to aid in real time debugging.

It is best practice to separate Comet's from each other by port in order to avoid adding unnecessary overhead into the network stack of the Comet, but if multiple vehicles end up in the same stream then the vehicle ID and lane key are used to discriminate between messages.

Comet can send Aux messages to up to 8 endpoints with customizable rates for each (this accommodates scenarios where there might be simultaneous high bandwidth cellular and low bandwidth satellite links.)

```
set_aux_command_path
    false                                Disable all Aux links
    tx <tx udp port>                     Set the common transmit to UDP port
    rx <rx udp port>                     Set the common receive on UDP port
    <idx> false                          Disable the specific Aux link index (0 thru 7
    <idx> [ipv4=<tx ipv4>] [div=<rf divider>]
                                         Set the specific Aux link index properties, transmit IP
                                         and RF divider (multiple of the RF epoch.) The
                                         transmit IP can be a broadcast or multicast address.
```

To simulate a loss of RF link to verify the behavior of the auxiliary command path, the `radio_tx_ctrl` command may be used on each lane to prevent that lane from sending on the RF link. Therefore, any messages received by the opposing lane must have come through the auxiliary link. This command is temporary and will reset to standard behavior on the next boot.

[8] Messages will be rejected by a unit if the received sequence number is not monotonically increasing. However, if a sufficient number of messages are received in a row, the unit assumes the counter unit has restarted and will accept the new sequence number start point. Additionally a message will be rejected by the Vehicle unit if the reflected sequence number was not sent by the Vehicle unit in the last 10 seconds. These provisions prevent delayed and out of order messages from taking effect.

Command Timeout

A link (RF and Aux) will be considered timed out after the time period specified via `set_command_timeout` has elapsed since the last valid message was received. By default the timeout is set to 1.5 seconds.

Evidence around tuning of the command timeout can be obtained using the `link_rtt` command which shows the observed delay of a particular link

Termination Behavioral Tweaks

Several modifications to how the Vehicle unit terminates are available which can aid in integration, ground operations, or autonomous actions in marginal link cases.

`set_allow_termination_rollback <true | false>`

Allow the Operator unit to command a reversion to the Passive state from `Armed` or `Terminated`. This is only effective if the hardware configuration was chosen at build time to be non-latching.

`set_lost_link_terminate_timeout <time in milliseconds>`

If set to a non zero value, the Comet will terminate autonomously if any Operator link (primary or auxiliary) has previously been active, and if all links to all Operator units have been lost for at least the configured time period.

Although the configuration resolution is in milliseconds, the achievable precision is only as good as the application loop period, which is 10 ms.

`set_output_delay <output A or B> <delay in microseconds>`

Add an additional delay to when the termination output will become active once the unit is in the `Terminated` state. This can help stage behavior between the A and B terminated outputs. For example the A output might disable the motors immediately, and the B output might fire a ballistic parachute 30 seconds later. This would be configured on both units by:

```
set_output_delay A 0
set_output_delay B 30000000
```

`set_terminate_at_boot <true | false>`

If set to `true`, as soon as possible in the board support package, the lane will open SAFE and close ARM and TERM. If voting is selected in the hardware configuration, the lane will vote for both outputs to be terminated.

No output delay will be applied, even if set_output_delay is set to a non zero value.

If an allocortech bootloader is installed and was compiled against the Comet platform, this feature is supported from bootloader boot and will be glitch free while handing off into the application.

`set_active_in_arm <bool A> <bool B>`

Allow a particular output to assert in the ARM state, this can be used by the integrator/operator command things like a soft termination or to prepare the vehicle for a full termination event.

Lane Cross-Connect

There is a UART that connects lane A and B internal to the Comet which is used to share system state (RF and telemetry messages.) Because of this, each lane can forward each other's telemetry if needed.

`set_cross_connect ethernet`
: Will cause that lane to emit telemetry from the other lane on the Ethernet link.

Low Voltage Operation

Although the Comet has been qualified for low voltage operation to 18V, and can operate as low as 12V, the built in tests will complain if the voltage appears to be abnormal. To circumvent a nuisance fault, the integrator should set the minimum expected operating volts.

`set_min_op_volts <volts>`
: Set the minimum expected operating volts (e.g. the threshold for the `InputVolts` fault.

Buzzer Behavioural Tweaks

The buzzer on the operator unit supports several options to change when and how it annunciates.

`set_buzzer <flag> <true | false>`
: Where the following flags are supported

- `buzz_on_arm_active`
  Continuously sound buzzer if ARM switch is asserted (FTS Only)
- `buzz_on_term_active`
  Continuously sound buzzer if TERM switch is asserted (FTS Only)
- `buzz_on_run`
  Briefly sound buzzer if transitioning from STOP to RUN or TELE-OP (E-Stop only.)
- `chirp_on_low_rssi`
  Chirp if low RSSI fault is active
- `chirp_on_link_failure`
  Chirp if both RF and Aux links have timed out
- `chirp_on_low_battery`
  Chirp if the low battery fault is active
- `chirp_on_failure`
  Chirp if this lane or the corresponding vehicle unit lane are failed

Diagnosing the Radio Link

NOTE: Comet requires all units in a link to share the same software version (unless the `rf_sync` debug option is enabled.)

There are several built-in console commands available for diagnosing and debugging problems with the radio link. These are

`radio_diag`
: This command will print Comet radio protocol information such as number of received and corrupted frames; and on Lane A will print information gathered from the radio over its Diagnostic Link.

`radio_shell`
: Lane A is capable of stopping the Comet application and allowing an operator, through the FTS shell, to interact directly with the radio's data port. The radio shell is specific to the serial port the operator is interacting with:
RS232, the command is `radio_shell RS232`
JTAG, the command is `radio_shell JTAG`

  In either case, once the shell has been established, whatever the operator types into the console will be forwarded to the radio. To exit this mode, the operator should type `exit` or power cycle the unit.

  To interact with the radio's built-in text configuration menu, wait 1 second without any traffic and then type `+++`. For more information on the capabilities of the Microhard radio's options, see the Microhard P Series Operating Manual.

`set_debug rf_sync true`
: The radio link between units is usually protected by a software version specific synchronization header. If units have software versions built from different git repository commits, then they will normally not synchronize. This behavior can be changed by setting the rf_sync debug flag to `true` which will set the radio synchronization value to `0x1234`.

`radio_version`
: Prints the version of software running on the radio module.

Software Updates

File Names and Formats

As a general rule

- Files with the `.bin` suffix are the raw binary images that should be loaded onto the target with some bootloading application (STM32Cube, stm32prog, bootyloader.)
- Files with the `.relo` suffix are intended to be loaded alongside the Allocortech bootloader (e.g. the Allocortech bootloader loads these binary files.)
- Files without extension or with the `.elf` suffix are ELF format applications. These are not necessarily compiled for the host computer, instead they may be the embedded binary with debug symbols.

Filename	**Built For**
`comet_gui_app`	Linux

Diagnostic utility capable of decoding and logging all Comet telemetry from both the Operator and Vehicle units. With the correct arguments and an external Microhard radio it can also emulate an Operator or Vehicle unit.

`comet_fts_app`	Comet

Embedded application with the Flight Termination personality. Should be loaded onto both lanes of the Operator and Vehicle units. Supports multiple operator units at once.

`comet_estop_app`	Comet

Embedded application with the E-Stop personality. Should be loaded onto both lanes of the Operator and Vehicle units. Only supports a single operator unit.

`comet_bootyloader_app`	Linux

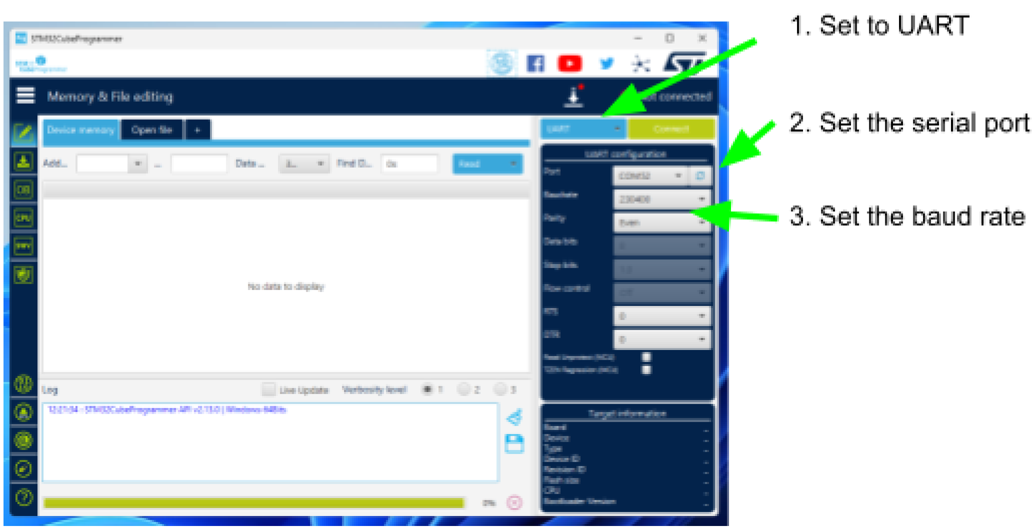
Allocortech bootloader, which is compatible with the `yubnub_app` and can be used to load the Comet software over Ethernet or CAN. Note that the .relo version of this application can be used to update the bootloader itself (e.g. load the bootloader into the application slot, boot into that, and then have `yubnub_app` flash the bootloader slot.)

STM32 Boot ROM - `STM32CubeProgrammer` Tool

The software on the Comet FTS can be updated via the RS232 or CAN ports using using the STM32CubeProgrammer tool from ST, obtainable from https://www.st.com/en/development-tools/stm32cubeprog.html.

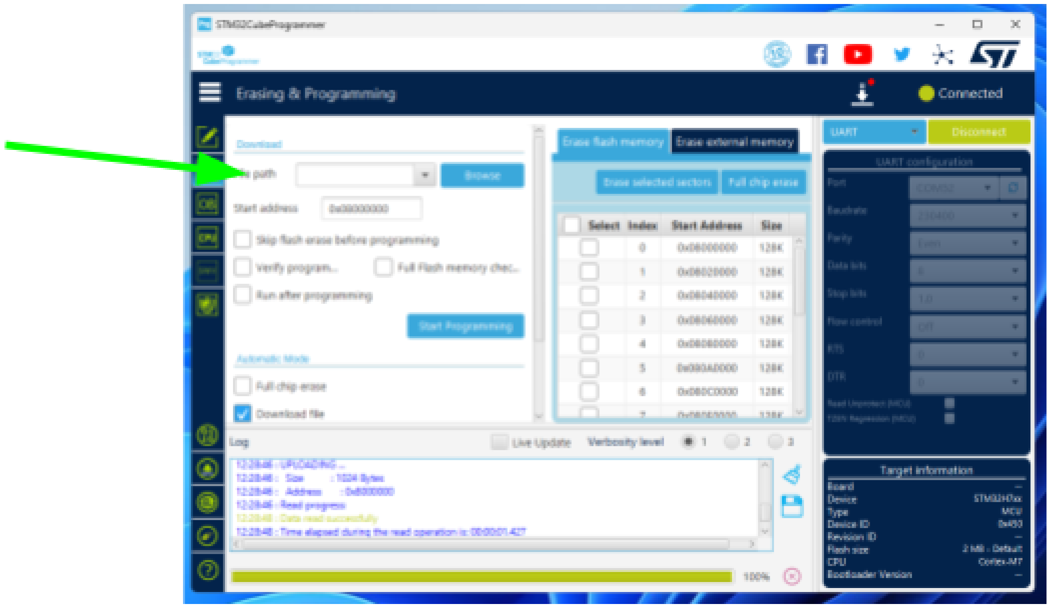
To use this tool (to load via RS232)

1. Place the Comet into ST bootload mode by
    a. Remove power from the Comet
    b. Short the BOOT pin to ground (if using the development harness, press and hold the “boot recovery” switch.)
    c. Apply power to the Comet (it should draw about 40mA at 28V)
    d. Release the BOOT pin
2. Configure the tool to connect to Lane A by setting
    a. … the programmer mode to UART
    b. … the correct UART / COM Port (it’s likely the only one present besides COM1)
    c. … the baud rate to 230,400



3. Connect the tool to Lane A by pressing the green “Connect” button.
   The text in the upper right corner should change from “Disconnected” to “Connected”

4. Change to “Erasing & Programming” mode by clicking on the second icon down on the left hand side.



5. Select Browse and find the correct file, typically either `comet_estop_app.bin` or `comet_fts_app.bin`.
6. Set the “Start address” to `0x08000000`
7. Press the “Start Programming” button
    a. ... wait until complete
    b. The log should emit something like:

```
12:34:07 : Memory Programming ...
12:34:07 : Opening and parsing file: comet_estop_app.bin
12:34:07 :   File            : comet_estop_app.bin
12:34:07 :   Size            : 365.35 KB
12:34:07 :   Address         : 0x08000000
12:34:07 : Erasing memory corresponding to segment 0:
12:34:07 : Erasing internal memory sectors [2 4]
12:34:14 : Download in Progress:
12:35:24 : File download complete
12:35:24 : Time elapsed during download operation: 00:01:16.671
```

8. Now program Lane B by
    a. Pressing the “Disconnect” button in the upper right corner
    b. Set “RTS” to 1 in the UART configuration pane
    c. Press “Connect”
    d. Press the “Start Programming” button
        i. ... wait until complete
9. Disconnect and cycle power

STM32 Boot ROM - `stm32flash` Tool

The software on the Comet FTS can be updated via the RS232 port using the STM32 UART Bootloader protocol detailed in ST application note AN3155. For users convenience, allocortech bundles a tool, installable via the `allocortech/mk/scripts/stm32flash_install.sh` script from the repository root, that speaks this protocol and is capable of manipulating the RTS pin to toggle between lanes.

To flash either Lane's processor it is first necessary to place the unit into bootloader mode. This is accomplished by shorting to ground pin 3 (bootloader recovery) on J1 and power cycling the unit.

The operator should then select which Lane they want to flash using pin 8 (MCU Select) on J1 where a short to GND indicates Lane A and a 3.3V signal indicates Lane B (there is an internal pull up to 3.3V.) It is most convenient to the operator if the MCU Select pin is connected to the RS232 cable's RTS pin for programmatic manipulation.

Example Commands:

```
/opt/allocortech/bin/stm32flash -b 230400 \
      -w build/comet_fts/fts/comet/release/comet_fts_app.bin \
      -i -rts -e15 <serial port>
/opt/allocortech/bin/stm32flash -b 230400 \
      -w build/comet_fts/fts/comet/release/comet_fts_app.bin \
      -i rts -e15 <serial port>
```

Allocortech Bootloader - `yubnub` Tool

allocortech has a precomposed bootloader which understands various aspects of the Comet configuration, such as the Ethernet network configuration, CAN bus configuration, and boot time termination. It can also help to prevent issues by verifying the application binary image before booting it.

Once loaded, the allocortech provided bootloader, `comet_bootyloader_app`, can be interacted with using the standard `yubnub` tool.

Initial Flashing:

```
/opt/allocortech/bin/stm32flash -b 230400 \
      -w build/comet_fts/yaploader/comet/release/comet_bootyloader_app.bin \
      -i -rts -e15 <serial port>
/opt/allocortech/bin/stm32flash -b 230400 \
      -w build/comet_fts/yaploader/comet/release/comet_bootyloader_app.bin \
      -i rts -e15 <serial port>
```

Flashing Comet Application using YubNub:

```
build/allocortech/booty/host/host/release/yubnub_app -i ethernet -n <ip address> \
      -f build/comet_fts/fts/comet/release/comet_fts_app.relo.bin -a 256k -e 1M -w \
      -d internal -s 1024
```

Avoiding the Configuration Area

Regardless of how the application is loaded onto Comet, it is important to avoid erasing the configuration area at the end of flash which is 1 sector in length (or 128k.) This is why the `stm32flash` tool is provided with the `-e15` argument (erase the first 15 sectors, leaving the last one untouched) and why the `yubnub_app` is given `-a 256k -e 1M` (erase 1M of flash after the first 256k which is where the bootloader lives.)

Verification of Loaded Image

The running software version can be queried using the serial console by using the `version` command.

Linux Notes

To avoid needing to run tools as the superuser (under `sudo`,) ensure that your user is in the `dialout` group or the appropriate group specified in the `udev` rules for your distribution. For example:

```
$ groups
example-user dialout cdrom sudo plugdev
```

You can check what group is required for your distribution by checking the permissions on the serial devices like so:

```
$ ls -alh /dev/ttyUSB*
crw-rw---- 1 root dialout 188, 0 Sep 10 10:36 /dev/ttyUSB0
crw-rw-rw- 1 root dialout 188, 1 Sep 10 10:36 /dev/ttyUSB1
```

If you are not already part of the dialout group, but have administrative permissions, you can add yourself with

```
$ sudo usermod -a -G dialout <username>
```

It is also usually convenient to work with attached serial devices by ID as this is a stable mapping. If using the development harness with integrated cable, the name will be something like `/dev/serial/by-id/usb-FTDI_USB-RS232_Cable_FT03A5EU-if00-port0`

You can discover the attached USB serial devices on your computer by running a list command:

```
$ ls -l /dev/serial/by-id
```

Custom User Software

If additional functionality is desired or if the existing functionality needs to be tweaked, please reach send an email to `info@allocor.tech` for information on our software development kits and contracting services.

Comet Mark II introduces several pieces of hardware (IMUs, GPS, and a large embedded flash) specifically designed for use cases beyond the basic “receive command from operator, emit simple signal.”

Using the Comet GUI Tool

The Comet GUI tool can be used to monitor the state of the unit and log telemetry. It can be invoked with the following command, specialized as needed:

```
$ ./comet_gui_app \
      --personality estop \
      --udp 10000 \
      --box 0 \
      --logdir ./directory
```

When connected to Ethernet, Comet will by default broadcast telemetry to the local subnet on UDP port 10,000 but this can be customized using the `set_eth_telem_ip` command.

The Vehicle unit is always box 0. The Operator unit will be 1 or 2, but can be confirmed by running the commission command on the unit.

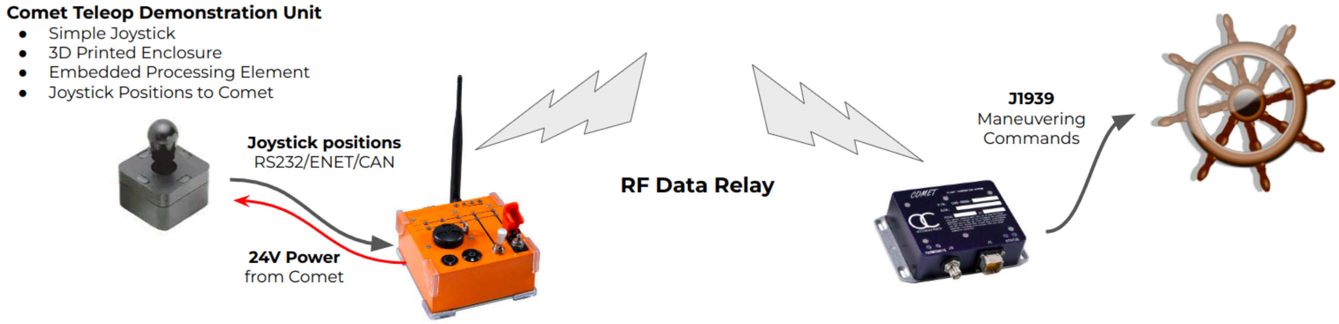
Comet Teleop Functionality

The following section outlines new functionality that has recently been implemented and demonstrated using the Comet system. The operator unit is paired with a joystick and used in a “Teleop” mode to take over basic command and control functions of an Autonomous Surface Vessel.

Please contact allocortech directly if interested in this use case to obtain a more detailed briefing on this functionality and to discuss implementation specifics.

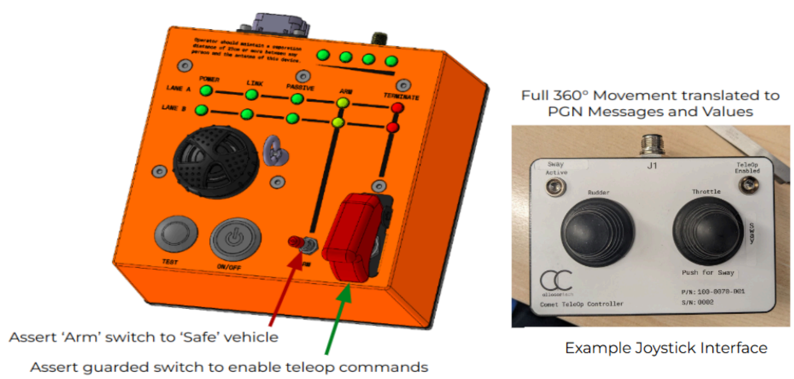
System Description

The Teleoperations (‘teleop’) concept (shown below) is intended to be extremely simple to demonstrate Comet’s ability to relay primitive commands that can be used to maneuver the vessel.



Teleoperations via Comet RF link

If the Comet Teleop Demonstration Unit is not connected, the Comet system will operate in its normal mode. However, the custom firmware delivered will implement the added capability of manual takeover of the vehicle when it is “Safe.” The basic CONOPS targeted to achieve this are shown below.



Teleoperations Demo CONOPS

Once in this mode, the joystick positions will result in specific PGN values being sent to the vehicle. The PGN values and mapping to the Joysticks can be set by allocortech prior to delivery. Mapping/remapping after delivery is possible with a purchased allocore SDK license to manipulate the source code and generate new firmware.