Reverse Engineering Marine Engines:
How to make powerboats do your bidding

Alex Lorman DEFCON 33

Overview of Marine Propulsion

Major Outboard Motor OEMs:

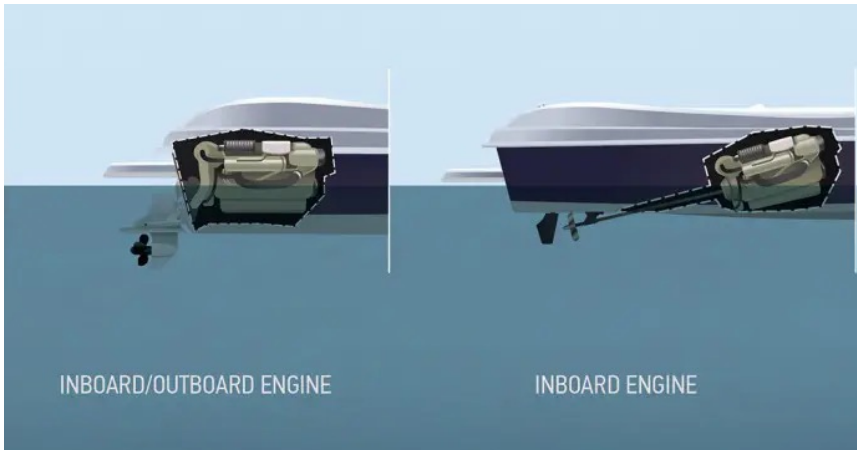
- Mercury (Brunswick)
- Yamaha
- Honda
- Suzuki



Overview of Marine Propulsion

Major Inboard and I/O OEMs:

- Yanmar
- Mercury
- Cummins
- Volvo
- MTU
- Caterpillar



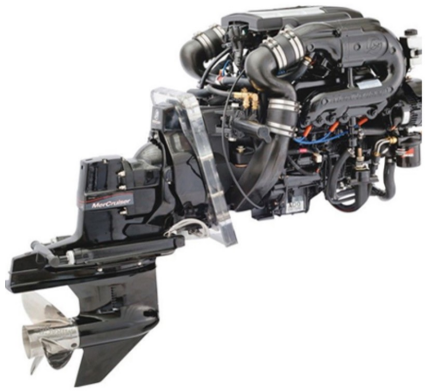
Outboards Motors



- Significant consolidation in the market
- Most OEMs have proprietary systems
- Moving more and more towards fully digital controls including steering
- Companies avoiding legal exposure of more autonomy

Inboard and I/O





- Significantly less sophisticated than outboards
- I/Os tend to have a shared control bus
- Manufacturers are significantly less vertically integrated
- Legacy control systems have existed for some time
- Significantly less commoditized

Existing Control Systems Methods

- Outboards
  - Significantly proprietary engine management
  - Black-box multi-engine and boat-space management
  - Moving all to CAN bus
  - Advanced aids (such as station keeping) are being integrated
  - Sources are from the OEMs themselves



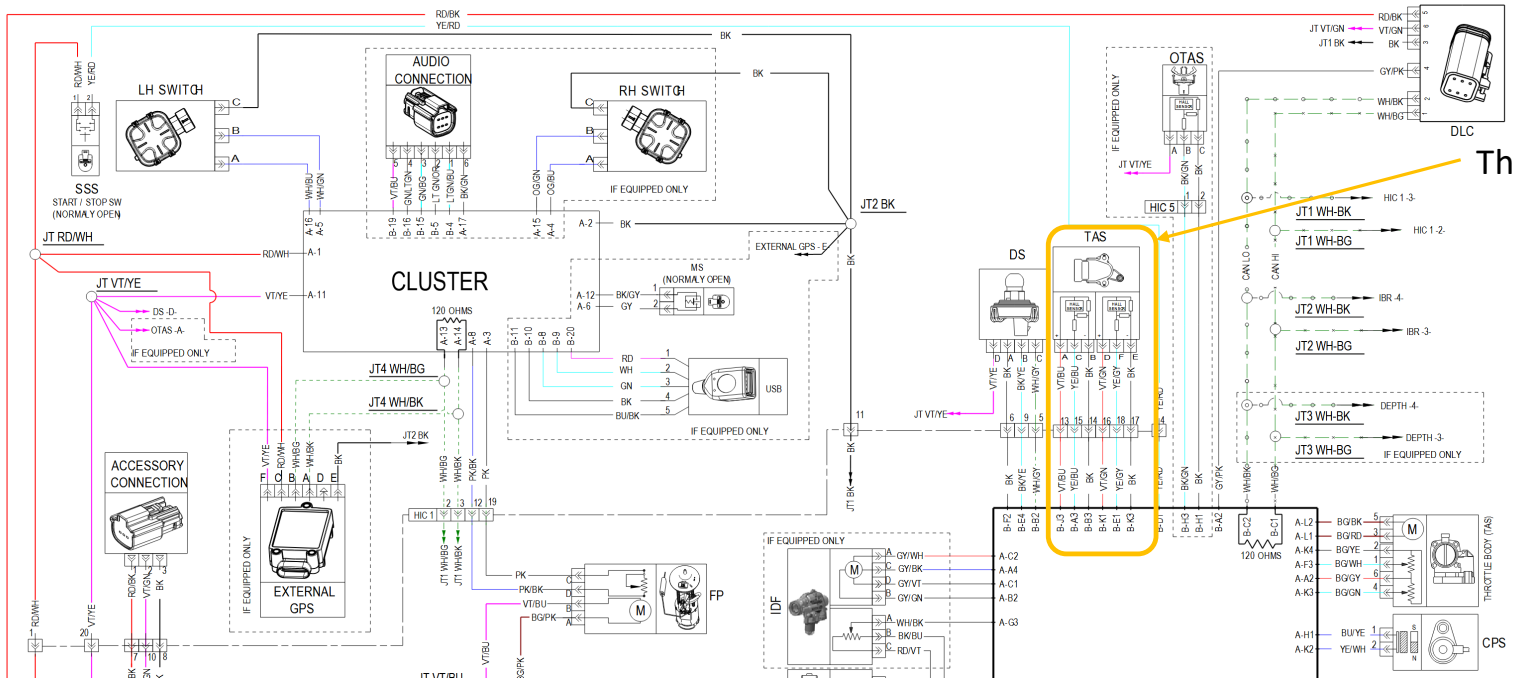
Existing Control Systems Methods

- Inboards
  - Many have modern ECUs for performance emissions
  - Cable driven systems are still common
  - Bolt-on digital systems have been in the market for 15 years
  - Manufacturers of these systems include:
    - Glendinning Controls
    - SeaStar Dometic
    - ZF Micro Commander
    - NHK MEC



Hacking: Jet Skis

- For most systems read the manual first!
- Wiring diagram shows Hall Effect Sensors driving throttle lever



Hacking: Jet Skis

- The rest of the manual tells us how these tone out
- So; to make the ECU think it has throttle and reverse triggers:
- Two DAC outputs per trigger with code to reflect table.
- Use of DACs allows true voltage vs PWM
- Slew rates should be checked before driving (anecdotally, it has been no issue)

BRAKE AND REVERSE LEVER SWITCH (BRLS)

Testing and Specifications

BRLS PINOUT	
PIN	SIGNAL
BRLS-A	5 VDC
BRLS-B	GND
BRLS-C	View signal % in BUDS2
BRLS-D	5VDC
BRLS-E	GND
BRLS-F	View signal % in BUDS2

NOTE: When moving BRLS lever, the BRLS percentage should increase or decrease in a steady linear fashion.

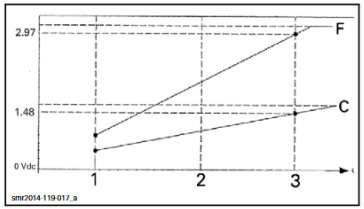
If BUDS2 does not show BRLS percentage moving or if reading is erratic:

- Check for BRLS reference voltage.
- Check for BRLS ground.
- Carry out a continuity test of the wiring between the iBR actuator and the BRLS.

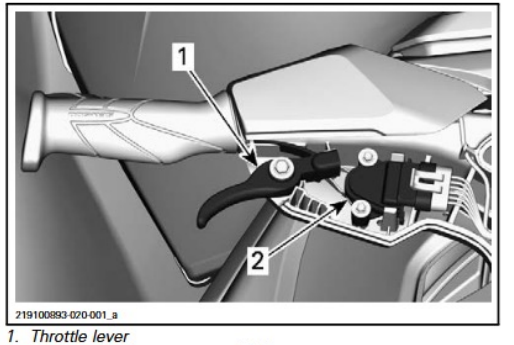
NOTE: When installed on vehicle the BRLS-C Vdc signal should always be half of the BRLS-F Vdc signal when testing with a multimeter.

To test, install Diagnostic harness between steering harness connectors.

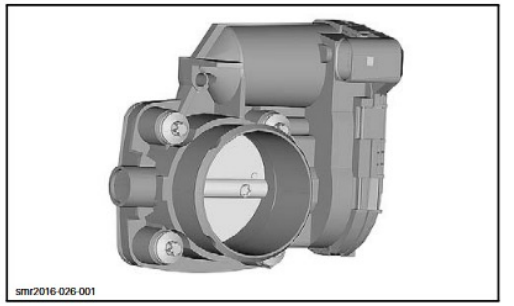
REQUIRED TOOL	
DIAGNOSTIC HARNESS (P/N 529 036 384)	



APPROXIMATE BRLS SIGNAL VOLTAGE CURVE PINS F AND C
1. *BRLS released*
2. *BRLS at 50% pulled*
3. *BRLS fully pulled*



1. *Throttle lever*
2. *Throttle accelerator sensor (TAS)*

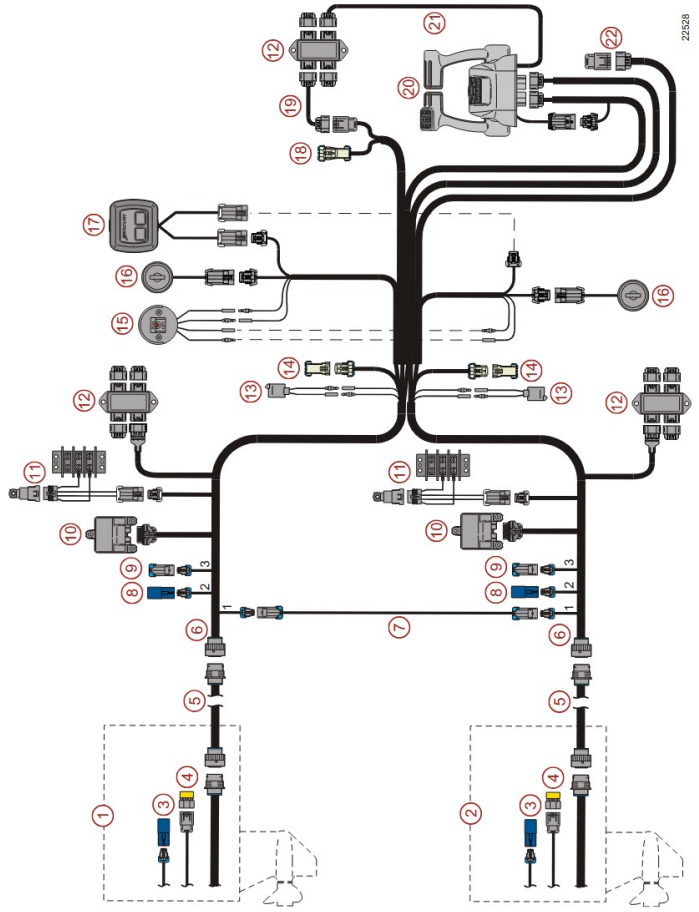


20-PIN CONNECTOR		IDLE POSITION	WIDE OPEN POSITION
PIN		VOLTAGE (VDC)	
13 (VI/BU)	14 (BK)	4.9 - 5.1	
14 (BK)	15 (YL/BU)	0.15 - 0.35	1.4 - 1.6
16 (VI/GN)	17 (BK)	4.9 - 5.1	
17 (BK)	18 (YL/GY)	0.4 - 0.6	2.9 - 3.1

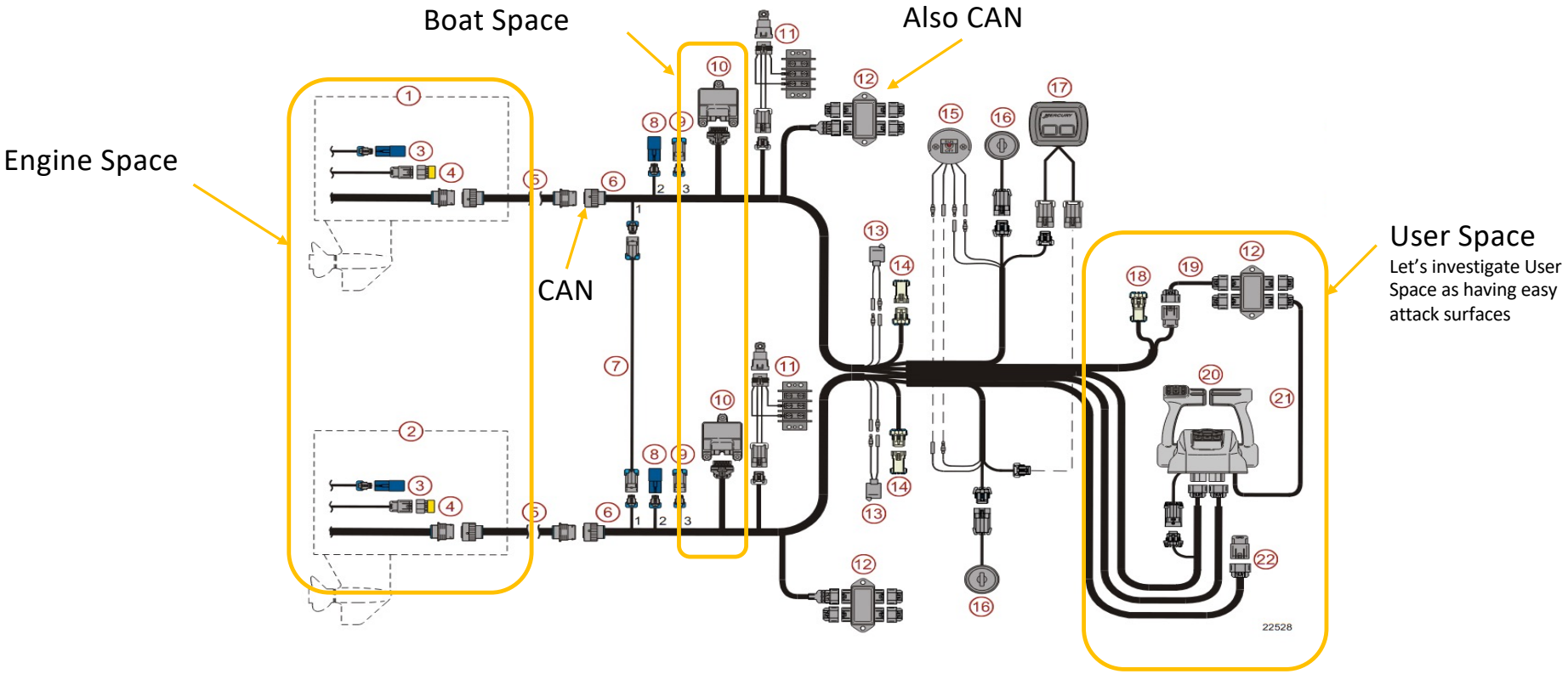
Hacking Mercury DTS

- Significantly more complex architecture
- DTS 1 is Mercury architecture pre ~2022
- DTS 2 is CAN to the helm unit itself
- Multiple engines and multiple “Command Modules”
- Mercury uses at least 2 CAN buses that are not publicly documented.

DTS Dual Engine Single Helm with CAN Trackpad Console Control



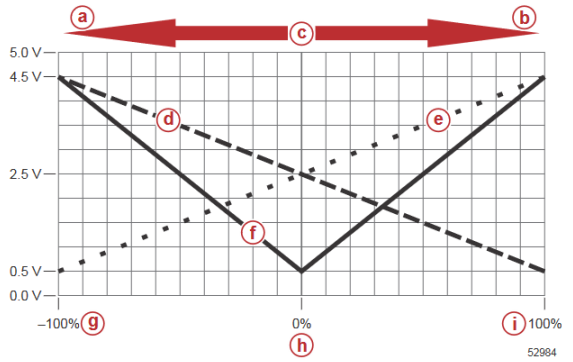
Hacking Mercury DTS



Hacking Mercury DTS

- Again, the manual tells us how to test the throttle levers for function
- This time they're using 3 voltages in tandem.
- To replicate we need 3x DACs and the code to run them
- For DTS 2, open up a throttle binnacle and probe with a scope!

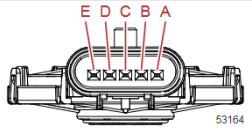
Control Lever Sensor Specifications



Lever Position (Forward +, Reverse –)	Potentiometer Voltages		
	High-Resolution	Decreasing	Increasing
100% (Forward WOT)	4.50 V	0.50 V	4.50 V
50%	2.50 V	1.50 V	3.50 V
0% (Neutral)	0.50 V	2.50 V	2.50 V
–50%	2.50 V	3.50 V	1.50 V
–100% (Reverse WOT)	4.50 V	4.50 V	0.50 V
Sensors vary and are characterized during initialization. All values are approximate.			

Notice that the increasing potentiometer increases in voltage from reverse WOT to forward WOT; the decreasing potentiometer decreases in voltage from reverse WOT to forward WOT; and the high-resolution potentiometer increases in voltage from neutral to both forward or reverse WOT.

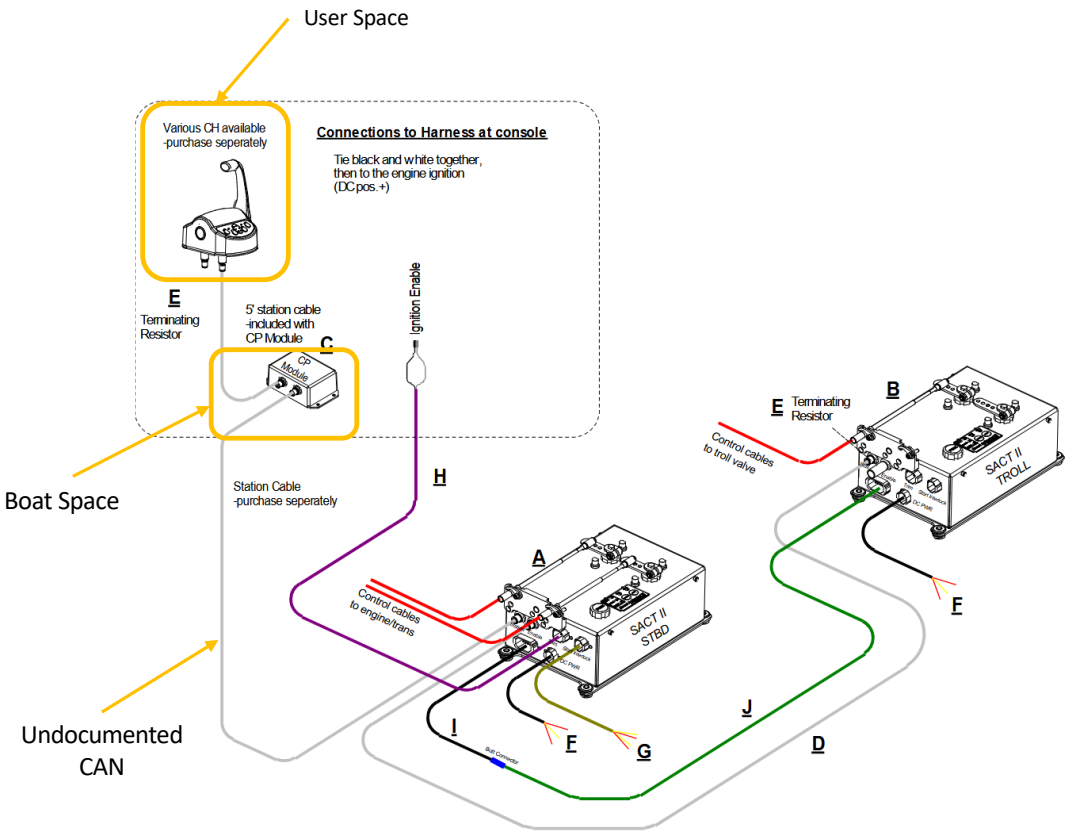
Control Lever Connector Pinout

Component Connector	Pin	Function
	A	Power
	B	Potentiometer 1: High-resolution signal
	C	Potentiometer 3: Increasing signal
	D	Potentiometer 2: Decreasing signal
	E	Ground

 © 2016 Mercury Marine

Hacking Glendinning

- System that uses proprietary CAN to control multiple cable driven engines (either inboard or outboard)
- Taking the helm apart reveals a custom dual output Hall Effect
- Putting this on a scope reveals the signals move with a constant voltage offset



Notable Exceptions

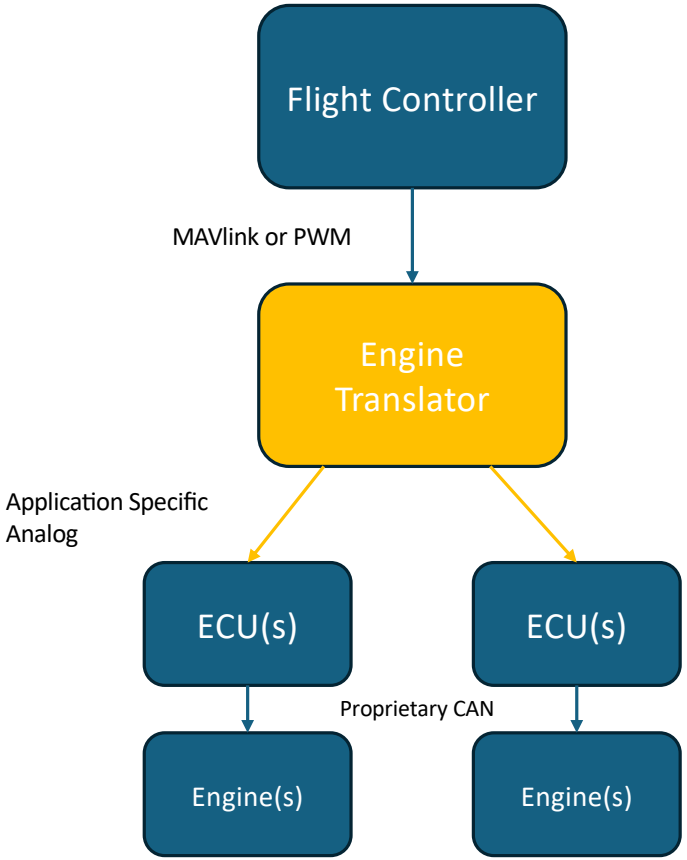




- Torqeedo is well-understood (if finicky) and is included in mainline ArduPilot
- Cox Marine outboards willingly provide a J1939 ICD
- Mercury/Brunswick has been downright hostile to disclosing CAN messages

Interfacing with an Autopilot

- PLCs seem like the obvious solution
  - MAVProxy > MQTT > PLC
  - Basic testing reveals that MQTT options are poorly documented and rate limited
  - PWM input counters are frustrating for PLCs at scale
  - On advanced ones a serial driver could be written
- Custom PCBS
  - Refresh speed is no factor
  - Condensed codebase that is simple to debug
  - Read MAVlink messages over serial or read PWM signals directly
  - Generate analog signals directly



QUESTIONS?

Alex Lorman
alex@alexlorman.com