NMEA2000 Fingerprinting FTW!

Who are we?

Dean



Who are we?

Anissa



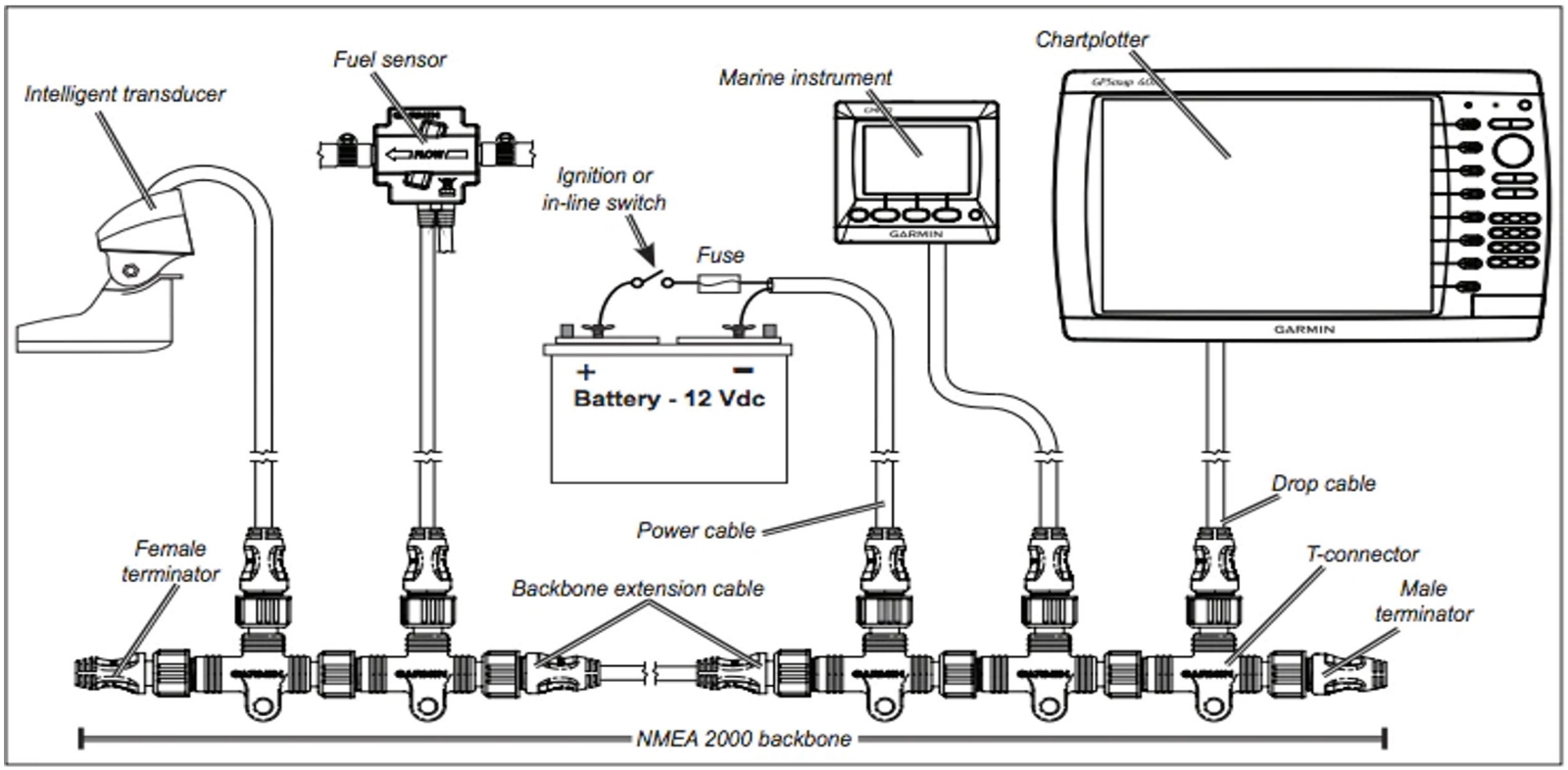
Throwback to DEFCON29...

- Where we presented **OpenBridge**!
  - Our Goals:
    - Make hacking NMEA 2000 and learning about marine electronics easier, cheaper, more inclusive, and more accessible
    - Provide some material for self-study so anyone can start to hack NMEA 2000 without needing to own a boat or know about boats

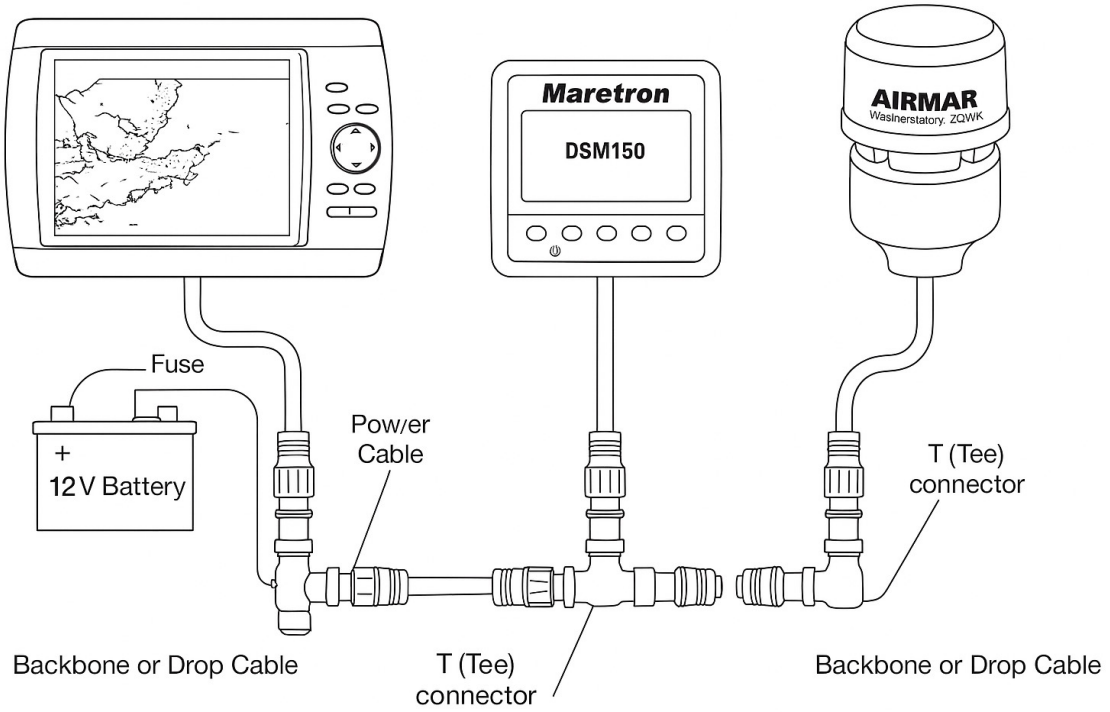
Understanding the Basics

- **National Marine Electronics Association (NMEA)** creates a standardized communication protocol, like **NMEA2000**
- NMEA2000 is based on *Controller Area Network* **(CAN)** protocol
  - Uses **ISO 11783** as a base with Marine Specific, *Parameter Group Numbers* **(PGNs)** to specify data structure
    - CAN uses two wires for robust real-time communication in harsh environments (e.g., boats, forestry equipment, cars, production facilities)
    - NMEA 2000 is compatible with the automotive standard, which is described in SAE J1939 (Automotive Standard).

Standard NMEA 2000 Bus



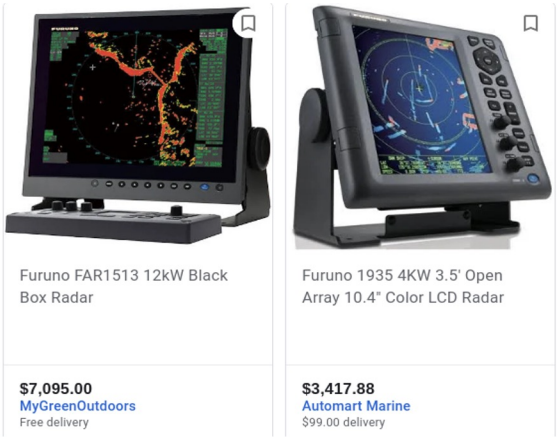
OUR NMEA 2000 Bus



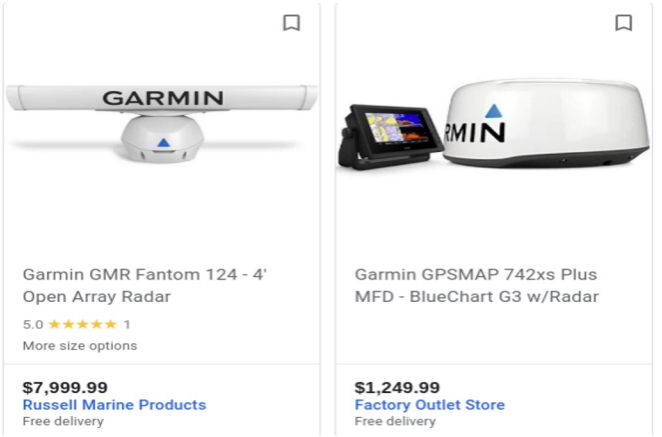
Our NMEA2000 Network (according to ChatGPT…)

Since DEFCON 29…

- NMEA2000 is still a widely used and needed maritime communication protocol with sparse open research
- Research is expensive, confusing, and niche

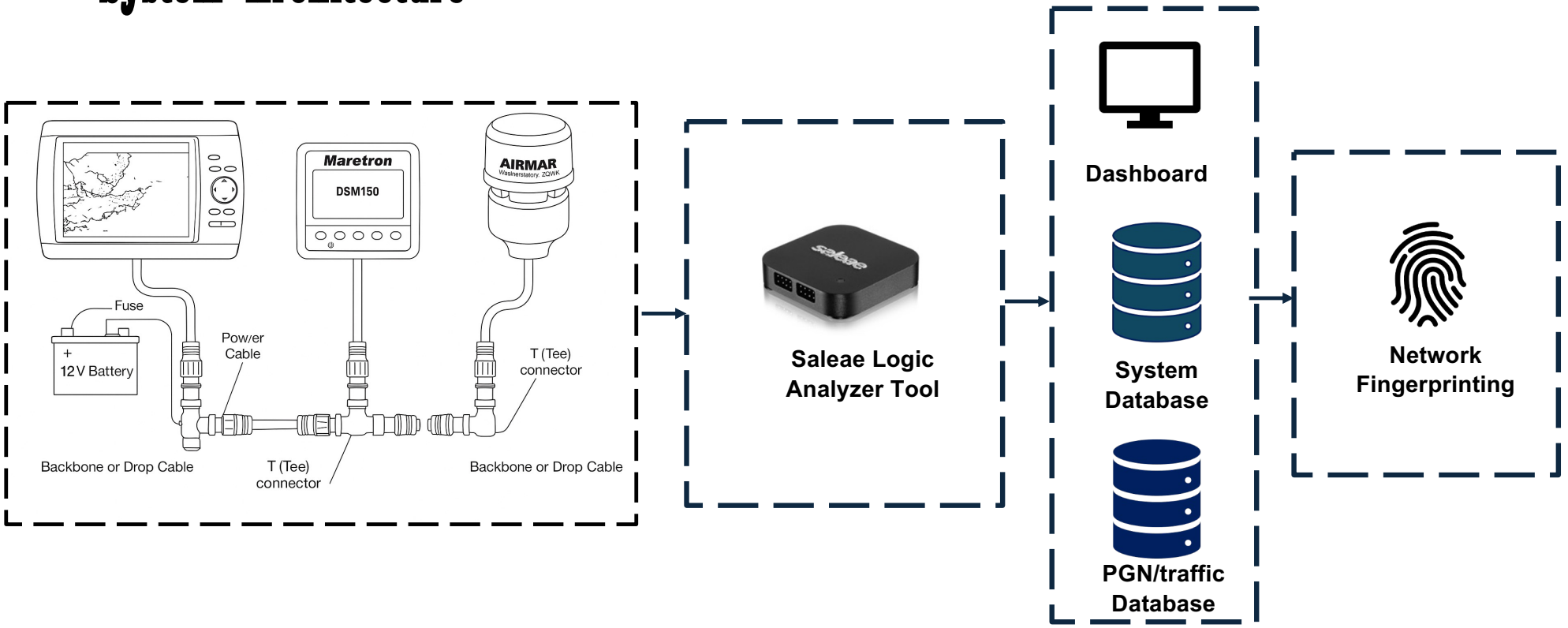


EXPENSIVE!!!

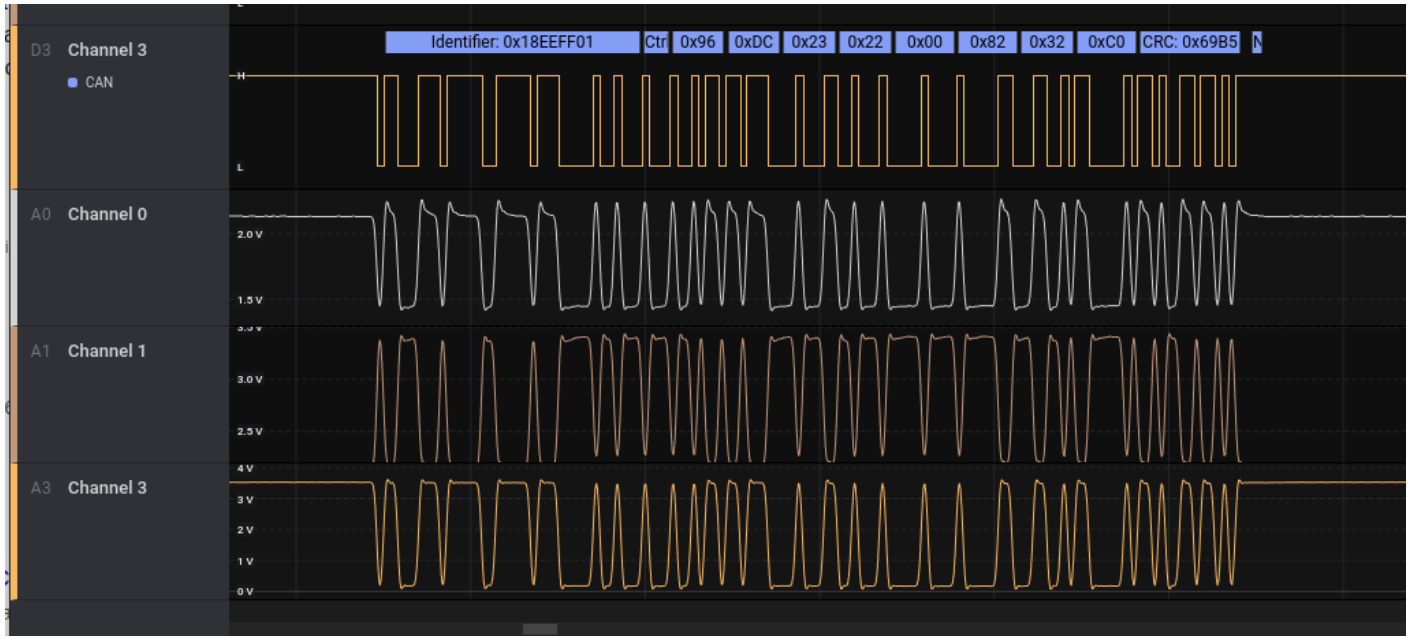


EXPENSIVE!!!

System Architecture



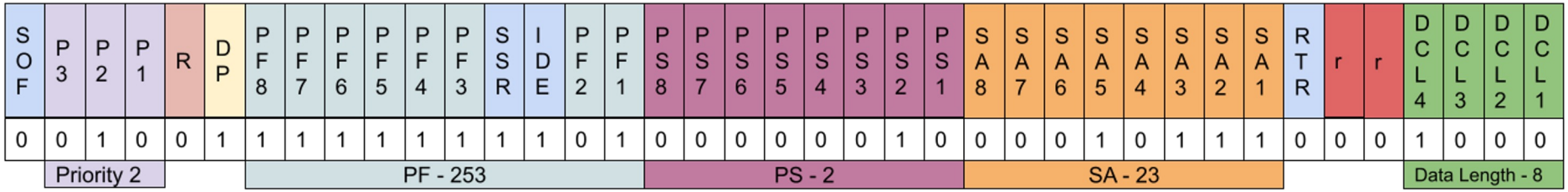
Step 1. Get the frames



CAN Frame on Logic Analyzer

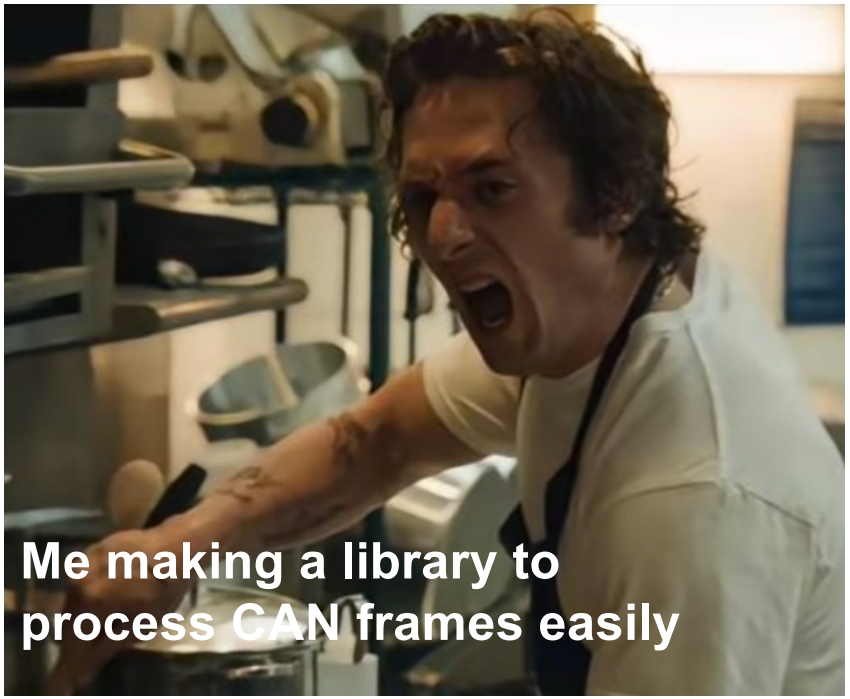
Channel 0 = CAN Lo
Channel 1 = CAN Hi
Channel 3 = CAN Rx

Step 2. Get the frame in Binary



- NMEA 2000 data frame in binary looks like this
- Some parts are more important than others
  - PGN = **R DP PF PS** (information about the frame message)
  - Source Address = **SA** (information about the device transmitting the frame)

CAN Frames to Binary Bits to Readable Messages





Step 3. Get to Calculating!

2. Read CAN Binary – the header is processed

	time	interface	header	size	byte1	byte2	...	byte4	byte5	byte6	byte7	byte8	bin_header
0	(1753987261.056720)	18EEFFB8 -> 00011000111011101111111110111000								82	F0	C0	11000111011101111111110111000
1	(1753987261.302618)	can0	18EFFFB8	[8]	89	98	...	00	05	00	FF	FF	11000111011111111111110111000
2	(1753987261.399770)	can0	18EFFFB8	[8]	89	98	...	00	05	00	FF	FF	11000111011111111111110111000
3	(1753987264.716521)	can0	18EEFF24	[8]	08	A6	...	10	00	B4	A0	C0	11000111011101111111100100100
4	(1753987264.958596)	can0	0DF11924	[8]	00	FF	...	FF	7F	FF	7F	FF	01101111100010001100100100100

3. PGN =

R : [3]
DP : [4]
PF : [5:13]
PS : [21:29]

R	DP	PF	PS
0	0	11101110	11111111

Step 3. Get to Calculating!

4. Clean up, Bit flip, and PGN

R	DP	PF	PS
0	0	11101110	00000000

PGN	PGN_dec
0xee00	60928

5. Source Address = SA : [21:29]

8-Bit value

```
source addresses:
    10111000
```

Step 4. Database Creation

- Known PGN Database

PGN Monitor

Search PGNs...

Instance	Timestamp	PGN	Source Address	Description
195550	2025-02-18 20:41:04.049663	127250	00100100	Vessel Heading
195549	2025-02-18 20:41:04.049061	129026	00100100	COG & SOG, Rapid Update
195548	2025-02-18 20:41:04.048451	129025	00100100	Position, Rapid Update
195547	2025-02-18 20:41:04.047913	127251	00100100	Rate of Turn
195546	2025-02-18 20:41:04.042073	126720	00000000	Seatalk1: Pilot Mode

2	Airmar WeatherStation 200WX	00100100	active
129284	Maretron DSM150	300.94 msg/min	1590
130323	Airmar WeatherStation 200WX	300.91 msg/min	1585

Fingerprinting the Network

- There is currently no standard way to **baseline** an NMEA2000 network
- We propose a deterministic fingerprinting technique that utilizes unique **topological** and **behavioral** knowledge of each network

- Our fingerprint consists of the following equation variables:
  - $\boldsymbol{D} = \{d_1, d_2, \dots, d_n\}$: $set\ of\ known\ devices$
  - $\boldsymbol{P_d} = \{P_{d1}, P_{d2}, \dots, P_{dn}\}$: $set\ of\ known\ PGNs\ sent\ by\ device\ d$
  - $\boldsymbol{\lambda_{dp}}$: $average\ frequency\ \left(\frac{msg}{min}\right)\ at\ which\ device\ d\ sends\ PGN\ p$

Fingerprinting Equation

$$F = \{(d, p, \lambda_{dp})\}_{d \in D, p \in P_d}$$

Where,

- F : *deterministic fingerprint of the network*
- $d \in D$: d *from known set of devices*
- $p \in P_d$: *PGN* p *is from known set of PGNs*
- λ_{dp} : *expected frequency* $\left(\frac{msg}{min}\right)$ *at which device* d *sends PGN* p

Dashboard for Continuous Monitoring

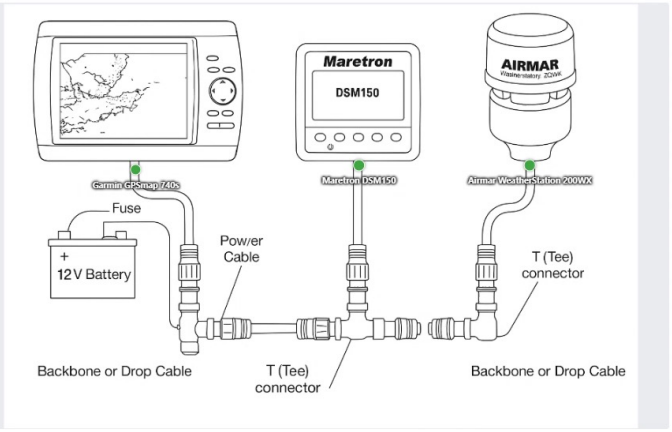
NMEA 2000 Monitoring System Dashboard Anomaly Analysis

Network Control

Capture Data | Process Data

System Map

Status: Normal | Active Devices: 3 | Msgs/sec: 28



Device Inventory

ID	Name	Source-Address	Status
0	Maretron DSM150	00000000	active
1	Garmin GPSmap 740s	10111000	active
2	Airmar WeatherStation 200WX	00100100	active

Page 1 of 1 — Previous | Next

PGN Frequency

PGN	Device Source	Average Frequency	Count
127251	Airmar WeatherStation 200WX	600.15 msg/min	3175
126208	Airmar WeatherStation 200WX	589.05 msg/min	3112
129029	Airmar WeatherStation 200WX	421.27 msg/min	2219
129284	Maretron DSM150	300.94 msg/min	1590
130323	Airmar WeatherStation 200WX	300.91 msg/min	1585

Page 2 of 5 — Previous | Next

PGN Monitor

Search PGNs...

Instance	Timestamp	PGN	Source Address	Description
195550	2025-02-18 20:41:04.049663	127250	00100100	Vessel Heading
195549	2025-02-18 20:41:04.049061	129026	00100100	COG & SOG, Rapid Update
195548	2025-02-18 20:41:04.048451	129025	00100100	Position, Rapid Update
195547	2025-02-18 20:41:04.047913	127251	00100100	Rate of Turn
195546	2025-02-18 20:41:04.042073	126720	00000000	Seatalk1: Pilot Mode

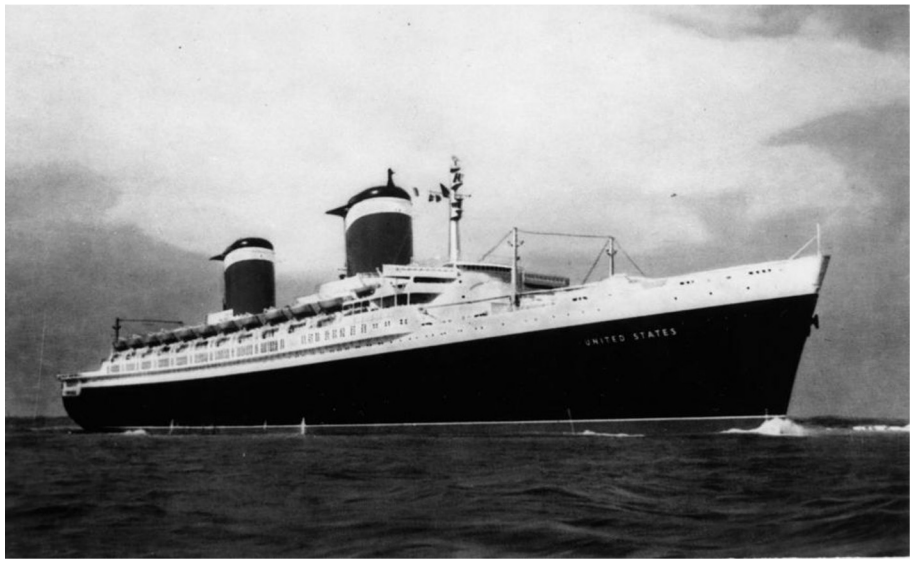
Summary

- **NMEA2000** is a widely used protocol in commercial and military applications.
- Systems are expandable and often differ even within the same class of ship.
- Fingerprinting of the network provides the necessary baseline to measure future work against.



Dean circa DEFCON29

Future Work



- **Investigate** additional fingerprinting techniques using electrical signals to identify unique devices
- Develop an **Anomaly Detection ML** model using the network fingerprint as normal data input
- Develop advanced **filtering & blocking** methods for anomalous traffic with an in-line device

Thank you

Questions?

