Push button.
Receive location.

...

Phil Pemberton -- campGNDd 2020

Congratulations. You're lost.

Setting the scene

You had a lot of fun at campGND last night, but you also had a lot of Bucky.

You woke up in the middle of a field with a map, a radio receiver and a compass.

(You somehow found a traffic cone too)

You have no idea where you are. None of the scenery looks familiar.

Your quest: Figure out where you are, and get back to campGND!

No, you don’t have a GPS receiver.

Nice try ;)

How to find your way

- Radio direction finding:
  - Locate a transmitter based on measuring its location relative to you.
- We can flip this on its head: find your location, provided you know the transmitter's.
- Luckily a few of these are shown on your map...

Triangulation to the rescue!

- **Use a directional receiver to work out your angle to the transmitter**
- **Draw a line on the map**
- **Do the same for another two transmitters**
  - Measure the angle of the transmitter relative to you.
  - Draw a line on the map from the transmitter at that angle.
  - Do the same for a few other transmitters.
  - **The point where these lines intersect is where you are!**

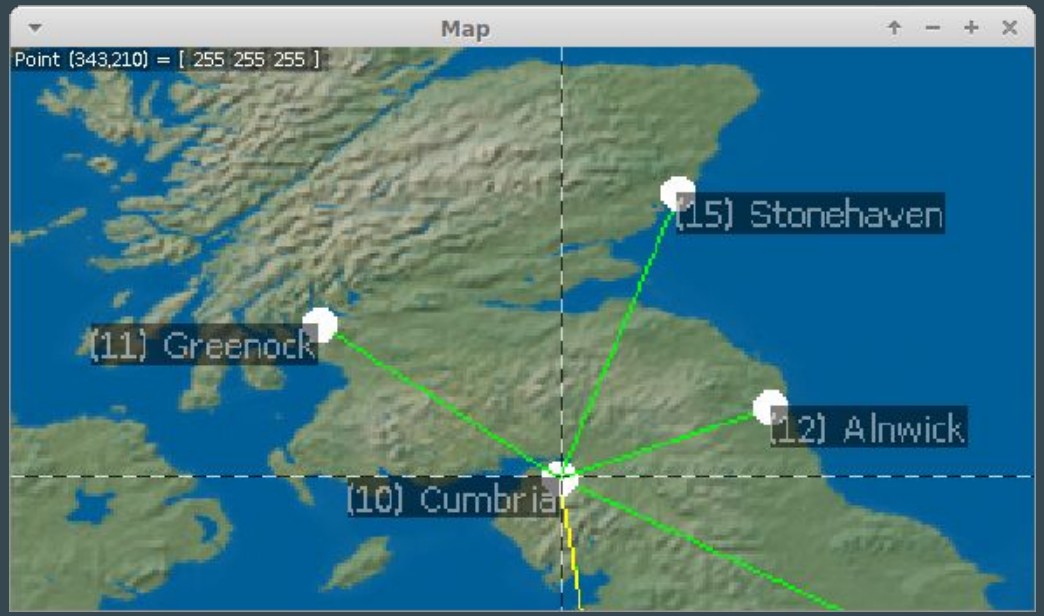
Let’s do that...

- Measure your angle to the transmitter
  - Receiver
  - Directional antenna
  - “Body blocking” can work, with patience

- Draw a line on the map
- Repeat

Here’s one I prepared earlier

Congratulations, you’re in Cumbria!



That was a very roundabout way to set the scene

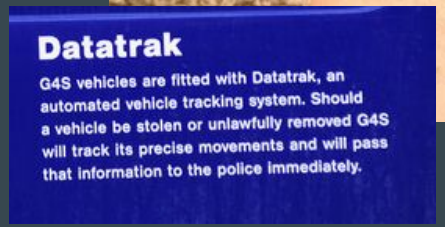
Who am I?

- Phil / @philpem / philpem@philpem.me.uk
- Amateur radio operator (M0OFX)
- Electronics geek, maker, ...

Datatrak Mk.II Locator

- Found this on eBay.
  - “Would you like any more? I have five.”
  - LF+UHF but no radio EPROM
  - Found an antenna and a TrakBak (LF+UHF) unit shortly after

- 3-pin XLR for power, ground and vehicle ignition
- 15-pin digital I/O port (opto-isolated)
- Two RS232 serial ports
  - With a custom pinout (of course)

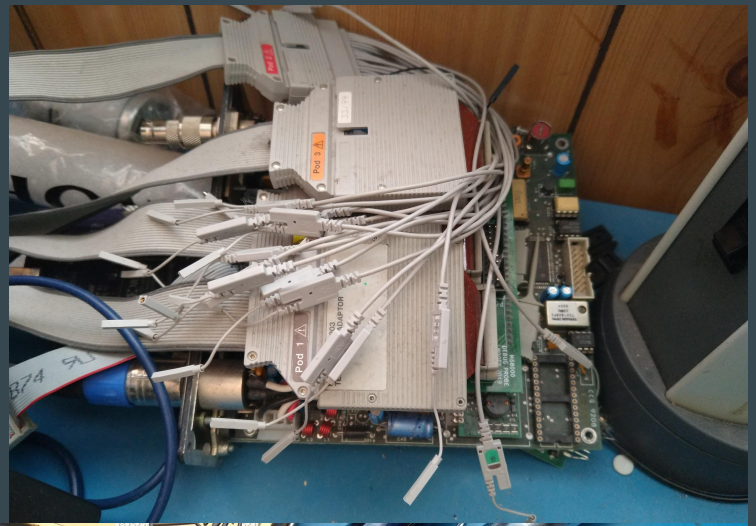


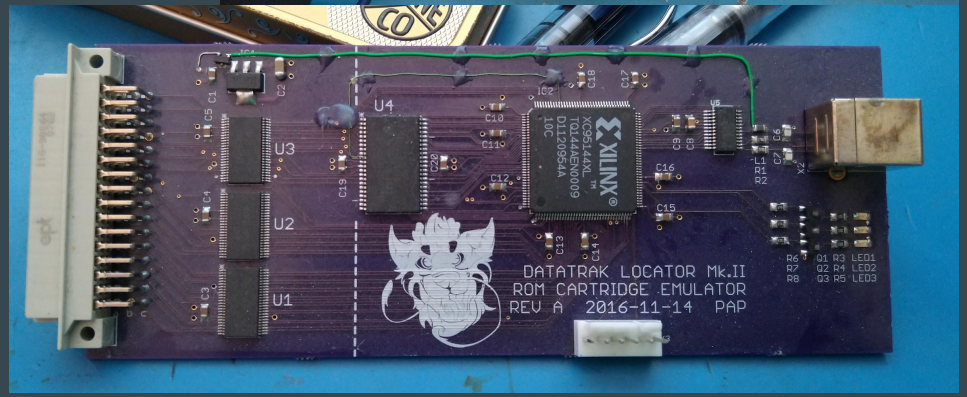
Locator Specs

- 68HC000 processor, 10MHz + custom LF receiver/glue ASIC
  - 128KiB RAM, battery-backed + Plug-in EPROM card (2x1Mbit = 256Kib)
- 80C31 (ROMless 8051) coprocessor, 12MHz
  - 8KiB RAM
  - UHF radio controller - links 68HC000 to UHF radio transmitter
- 68692 Dual UART
- 4kbit serial EEPROM
  - Configuration and unit ID
- Custom RTOS (a little bit UNIX inspired)
  - Has threads, mutexes, message queues
  - Character device support

Reverse engineering

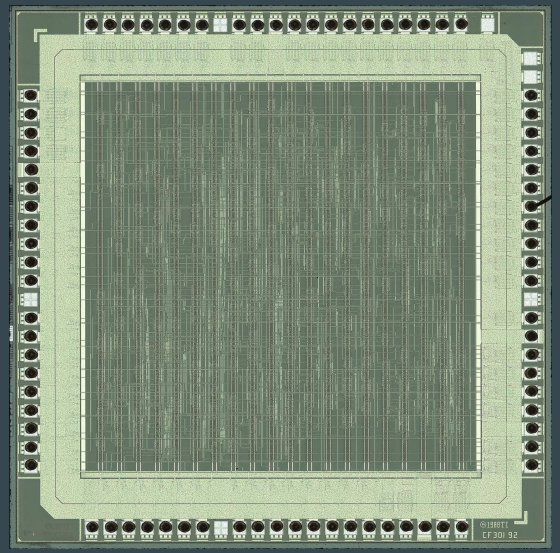
- Dumped the EPROMs
- Reverse-engineered the firmware in Ghidra
  - Custom RTOS
  - Processing is split across threads (tasks)
- Wrote an emulator
  - Doesn't boot
- EPROM emulator + debugger (ROM slot)
  - EPROM emulator, IO port, USB interface
- 68000 probe for HP 16700A logic analyser
  - Can watch instructions, data and code paths
- Used ADI DDS chip + STM32 to generate signals
- Watched what happened

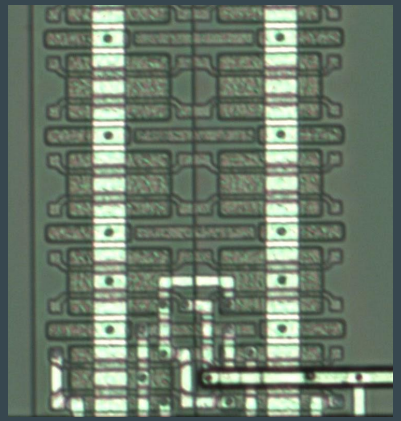




Reverse engineering

- Sacrificed a broken unit
  - Removed components
  - Sanded and scanned the PCB
- Had the ASIC decapped
  - TI gate array, two metal layers.





Datatrak network

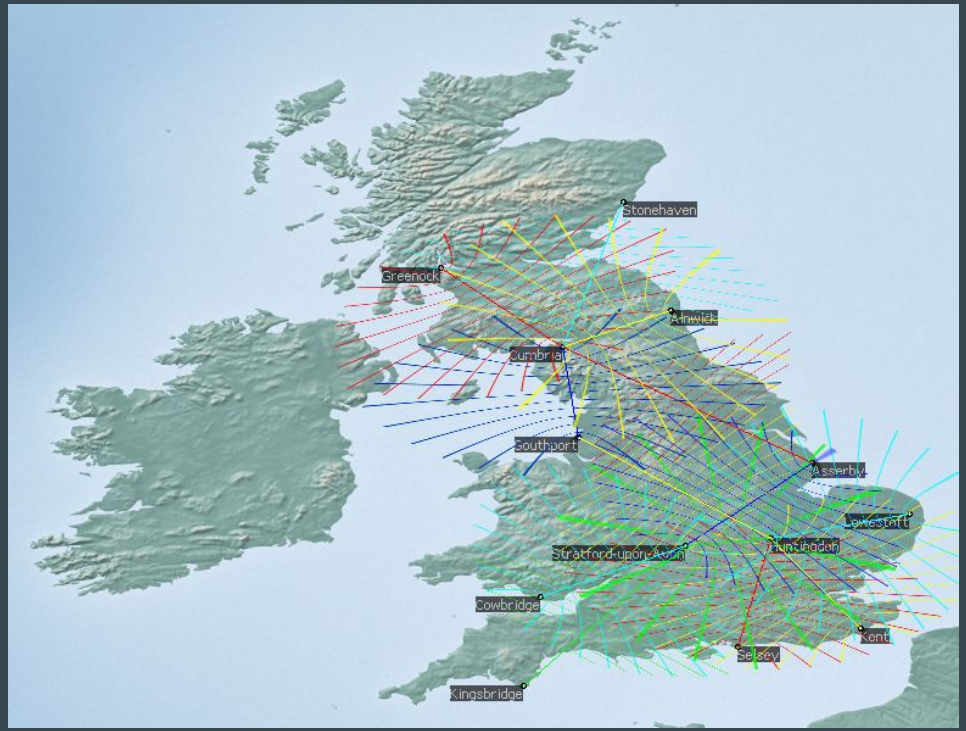
- Land-based navigation network
- Initially UK only but later expanded to Malta, Austria, Netherlands
- Used two long-wave radio channels
  - ~130-140kHz (~13kHz = ~10% spacing)
  - 500Hz channel bandwidth
  - 1.68 seconds cycle time
  - 108 seconds timing sequence
- Hasn't operated since 2011
- Few known recordings of the signal
  - Markus DF6NM (2002)
  - ... and that's about it

Locator, tell us about the network!

- The Locator has debug commands
- A couple of them tell us about the network
  - Transmitter locations
  - Transmitter master/slave relationships
- Here's a pretty map of the network!

Trilateration 2.0: Let's go hyperbolic

- Transmitters are arranged into "chains"
  - 130kHz and 140kHz Chain
- One transmitter is the "master"
  - Generates the Trigger and Clock
- Slaves are assigned Slots in the TDMA block
  - Receives one slot, retransmits in another
  - (This is called **phase mirroring**)
  - Max 24 slots using Interlacing
    - 1..8+9..16, then 1..8+17..24
- Measure relative phase of the signals.



Trilateration 2.0: Coarse positioning

- Notice how the LOPs repeat along the Baselines
- LOPs repeat every half wave
- That means we need a coarse location

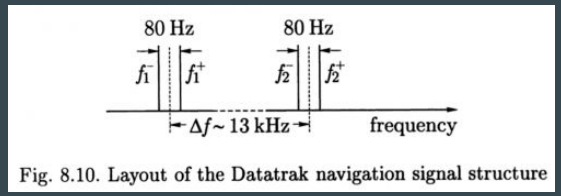
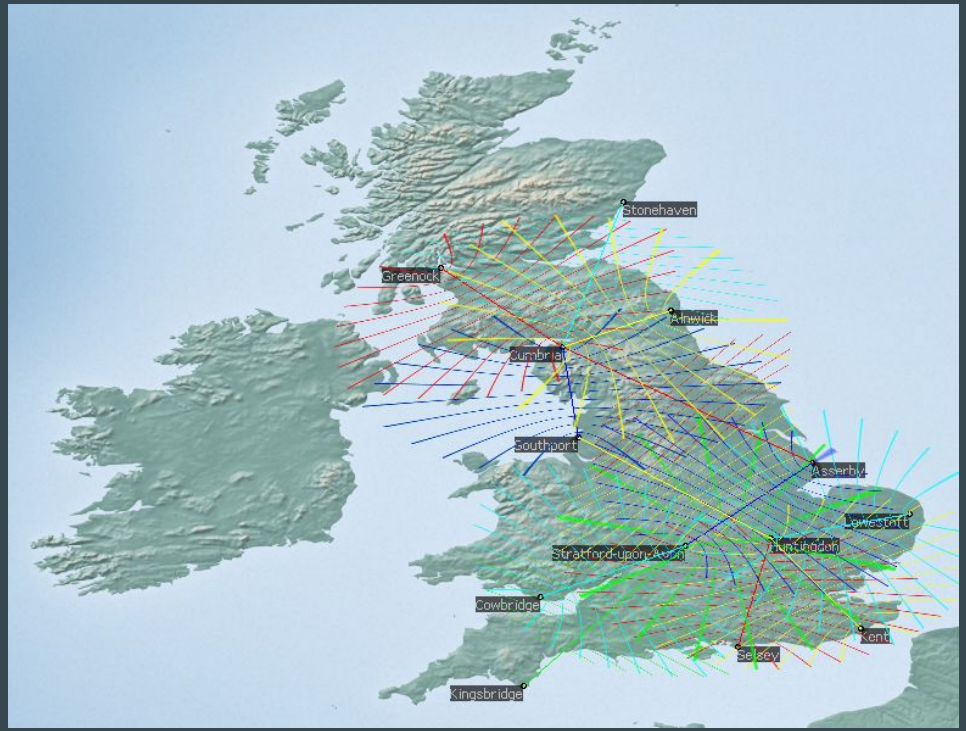
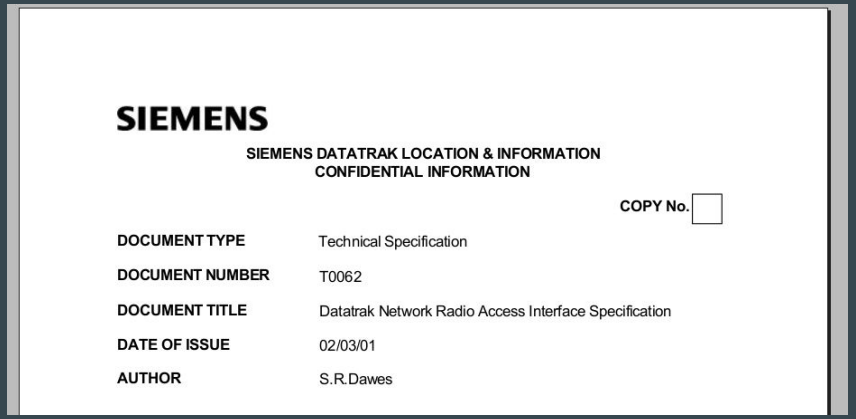


Fig. 8.10. Layout of the Datatrak navigation signal structure



Recent developments

- Abridged network access spec turned up on the Austrian Radio Regulator's website (T0062_3.pdf)
  - LF "redacted for security" but contains lots of data on UHF return channel
  - Glossary explains a lot of the debug messages
- Designed DDS dual-frequency signal generator
  - Still need to build it :(
- More reverse engineering...



SIEMENS

SIEMENS DATATRAK LOCATION & INFORMATION
CONFIDENTIAL INFORMATION

COPY No. ☐

DOCUMENT TYPE	Technical Specification
DOCUMENT NUMBER	T0062
DOCUMENT TITLE	Datatrak Network Radio Access Interface Specification
DATE OF ISSUE	02/03/01
AUTHOR	S.R.Dawes

Thanks!

Slides downloadable from
https://panels.sneptech.io

Twitter @philpem
Email philpem@philpem.me.uk