Reverse engineering Quasar
Introduction

• Guns donated from the Quasar centre in Whitstable.
• Late 1980’s hardware (still working fine, but with some obvious limitations)
• Attempting to reverse engineer the system to build compatible devices (other guns but also turrets, etc.)
Components

• Three main components in a Quasar system:
  • Guns – given to players to shoot each other!
  • Energisers – send the setup codes to the guns at the start of each game
    • In some game modes players need to return to these mid-game to recharge on shots / lives.
  • Bases – In some game modes, shooting the enemy base gives more points.
Communication

• Laser is just for show!

• Devices use IR to communicate, but very different to standard “TV Remote” protocols:
  • 28.8Khz carrier frequency (almost everything else is 38Khz).
  • 2404 baud RS232 over IR.
    • Works surprisingly well in practice – IR LED is on for 1, off for 0.
  • Start and stop bits are reversed...
Start and stop bits are reversed...?!

• It doesn’t matter what the start and stop bits are, as long as they are:
  • Opposite to each other
  • The start bit is opposite to the idle state (otherwise the start bit will never be received, it will be treated as idle).
• In this case, the second of these requirements isn’t met – the start bit is the same as the idle state.
• The protocol works around this by sending a full 0 byte before each transmission, pulling the line low so the start bit (high) will then be recognised.
• This means we can use a hardware UART to receive (with a NOT gate), but sending has to be bit-banged.
Protocol decoding

• Whitstable provided us with the 2.4 version of the protocol.
• Protocol in use on the guns we have is 2.7 - which meant a certain amount of reverse engineering was required (they inconsiderately changed a load of bits!)
• Most of the reverse engineering was done with a oscilloscope running a simple logic analyser, sitting behind a 28Khz IR receiver.
• The start-stop bit problem was found by comparing printouts of waveforms and decoding by eye & hand.
Current status

• The complete protocol has been reverse engineered and we are currently building a “gun on a board” that emulates the original - but uses far fewer (and modern) components!

• When “gun on a board” is done, aiming to print (or mould) some newer, smaller gun casings and build some PCBs to make our own compatible system.
Future ideas

• Mentioned earlier that the 1980’s system has some limitations...
  • Most notable is no live scoring. Score only updates when players visit an energiser, which may be never!
  • WiFi could solve this cheaply (especially with the ESP8266 chips), gun we’re building is easily extensible so these components can be added easily in future.
  • Guns could have small OLED screens displaying positions of other players in a larger field via GPS
  • Different game modes – playing area could be defined by GPS co-ordinates and get smaller as time progresses...
  • Turrets, mines, “extra life” packs, etc. are all relatively easy to implement.
  • Open to other suggestions!
Questions?