# SOFTWARE-DEFINED RADIOS

Collaboration space, Alexandria, VA

SEPTEMBER 2018

WHAT IS AN SDR?

- A radio system that features a Radio Frequency (RF) front-end that is defined in software, rather than traditional hardware (analog circuits).

- Are used to convert radio signals to digital bits of information.

- Analog-to-Digital Converters (ADC) and Digital-to-Analog Converters (DAC) are some of the most important components.

- Field Programmable Gate Arrays (FPGAs) and Radio Frequency Integrated Circuits (RFICs), or a combination of the two, are the most popular types of SDRs.

- Universal Software Radio Peripheral (USRP) is a highly popular brand: https://www.ettus.com/
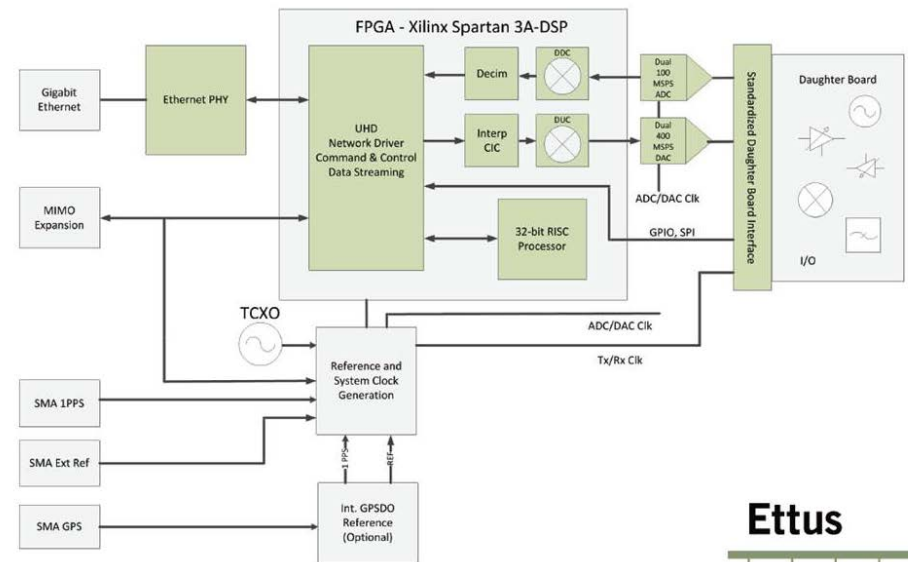
HOW TO USE AN SDR - HARDWARE

- An external computer is typically used to process the bits of information produced by the SDR.

- Ethernet or USB are the physical connection methods used to connect to the device and an associated driver must be installed on the computer to allow it to be recognized.
  - USRP devices use the Universal Hardware Driver (UHD): https://www.ettus.com/sdr-software/detail/usrp-hardware-driver

- The bits of information are typically at a high data rate (called the Sample Rate), which usually require a decently powerfully computer to process.

HOW TO USE AN SDR - SOFTWARE

- Once you connect an SDR to the computer, you need to do something with the data.
  - You either transfer data to the SDR (TX) or receive data from the SDR (RX).
- Usually an SDR program is used to make this task easier, such as GNU Radio: https://www.gnuradio.org/
- GNU Radio is a Digital Signal Processing (DSP) library that facilitates the processing of samples of data to produce either an input or an output.
- Tutorials and Instructions can be found on the main wiki page: https://wiki.gnuradio.org/index.php/Main_Page
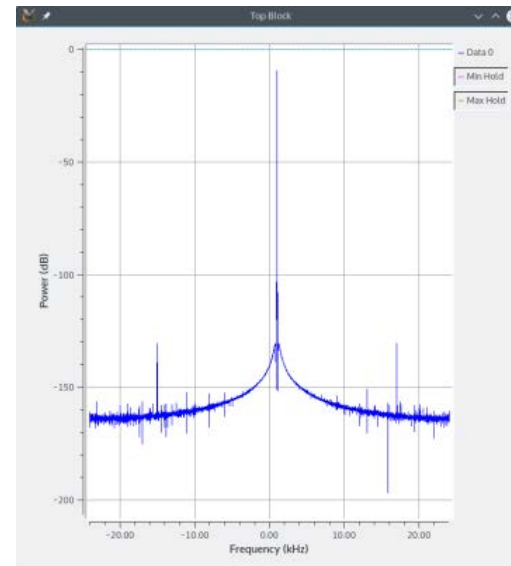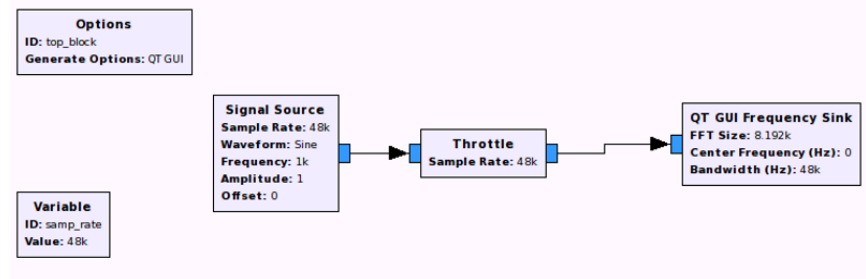
DIGITAL SIGNAL PROCESSING

- ADC / DAC
  - Voltage to binary mapping

- Signal Sampling Theorem
  - $fs \geq 2\ fm$
  - Aliasing

- Digital Filtering
  - Finite Impulse Response (FIR)
  - Infinite Impulse Response (IIR)
  - IIRs usually are more efficient in their implementation, but FIRs are easier to design.
  - FIRs are designed with taps (or a coefficient/delay pair).

- Fast Fourier Transform (FFT)
  - Used for transforming a signal from the time domain to the frequency domain.
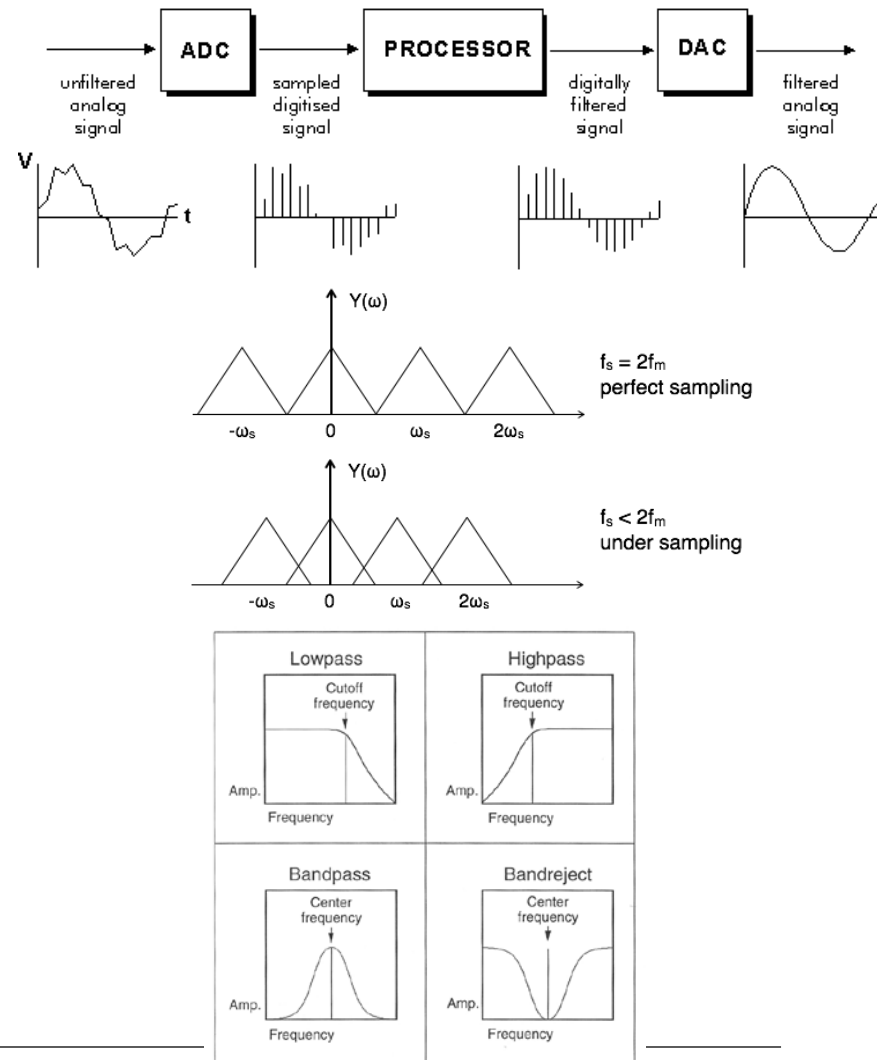
MARITIME COMMUNICATIONS

- Both TRUDI's have several different RF communication protocols active.

- Digital Selective Calling (DSC)
  - https://en.wikipedia.org/wiki/Digital_selective_calling
  - "Text messaging" for maritime vessels, primarily used for digital Distress messages.
  - Uses Audio Frequency Shift Keying at 1200 sym/s modulation (AFSK1200).
  - An SDR can be used to create spoofed messages.

- Very-high Frequency (VHF) Radio
  - https://en.wikipedia.org/wiki/Marine_VHF_radio
  - Voice communications for verbal calling and emergency announcements.
  - Uses Amplitude Modulation (AM).
  - An SDR can be used to jam any of the Marine VHF channels.

- Automatic Identification System (AIS)
  - https://en.wikipedia.org/wiki/Automatic_identification_system
  - Automatic tracking system used on ships to monitor the whereabouts of other commercial or military vessels.
  - Use of existing libraries on GitHub such as gr-ais: https://github.com/bistromath/gr-ais and gr-aistx: https://github.com/trendmicro/ais/tree/master/gr-aistx
  - An SDR can be used to spoof vessels which do not exist physically, but show up on the AIS plotters.