

# *Przechwytywanie i analiza transmisji radiowych*

*mgr inż. Paweł Koszut*

---

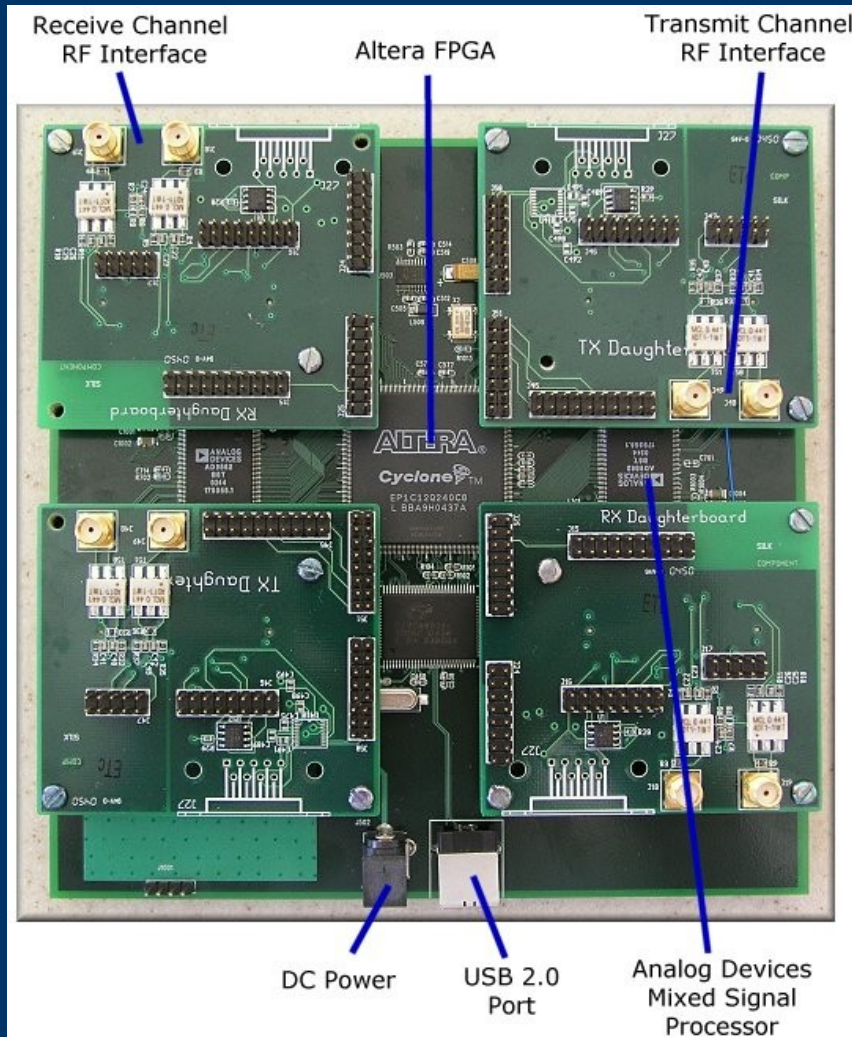
---

# *Plan prezentacji*

- Odbiornik USRP - Universal Software Radio Peripheral
- Zastosowania
- Odbiór transmisji GSM



# USRP - Universal Software Radio Peripheral

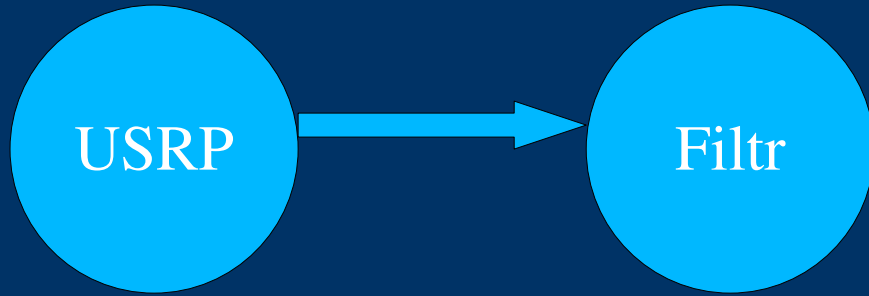


- Odbiornik SDR
- Interfejs USB 2.0
- Przenoszone pasmo 6 MHz
- Open-hardware
- Współpraca z GNU Radio

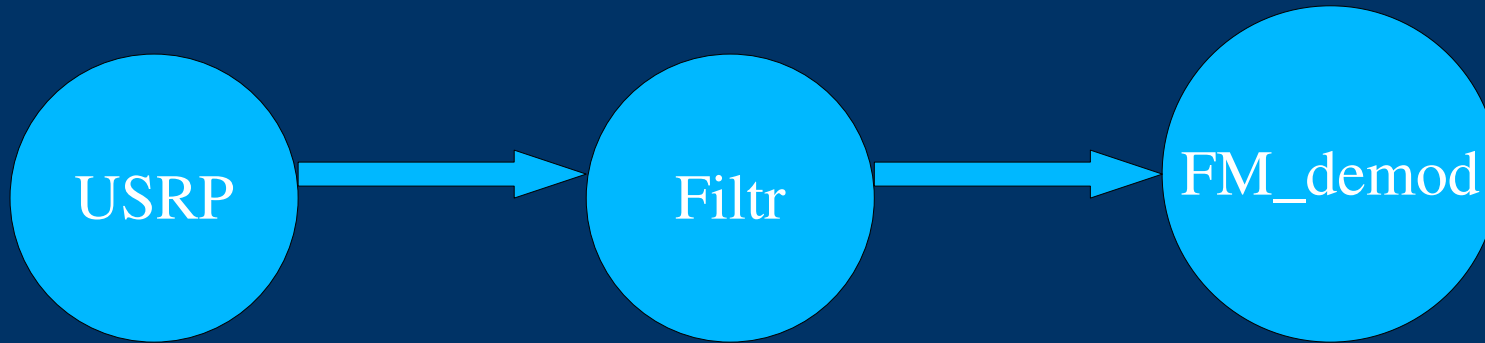
# *GNU Radio*



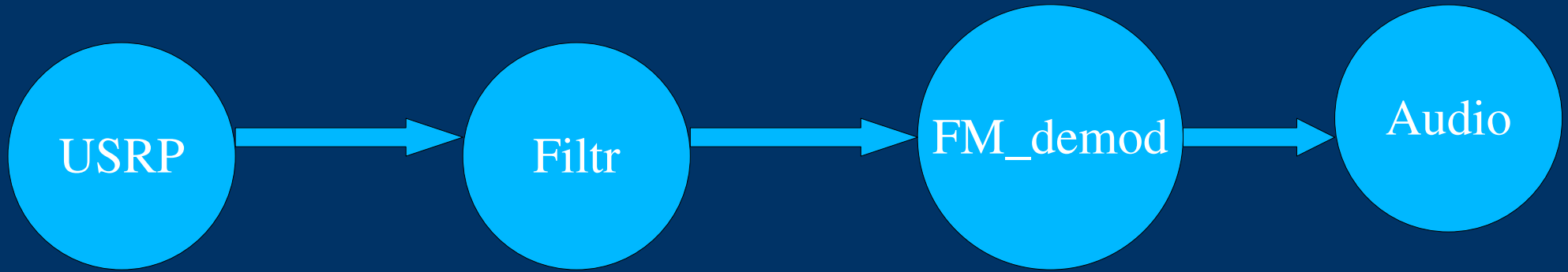
# *GNU Radio*



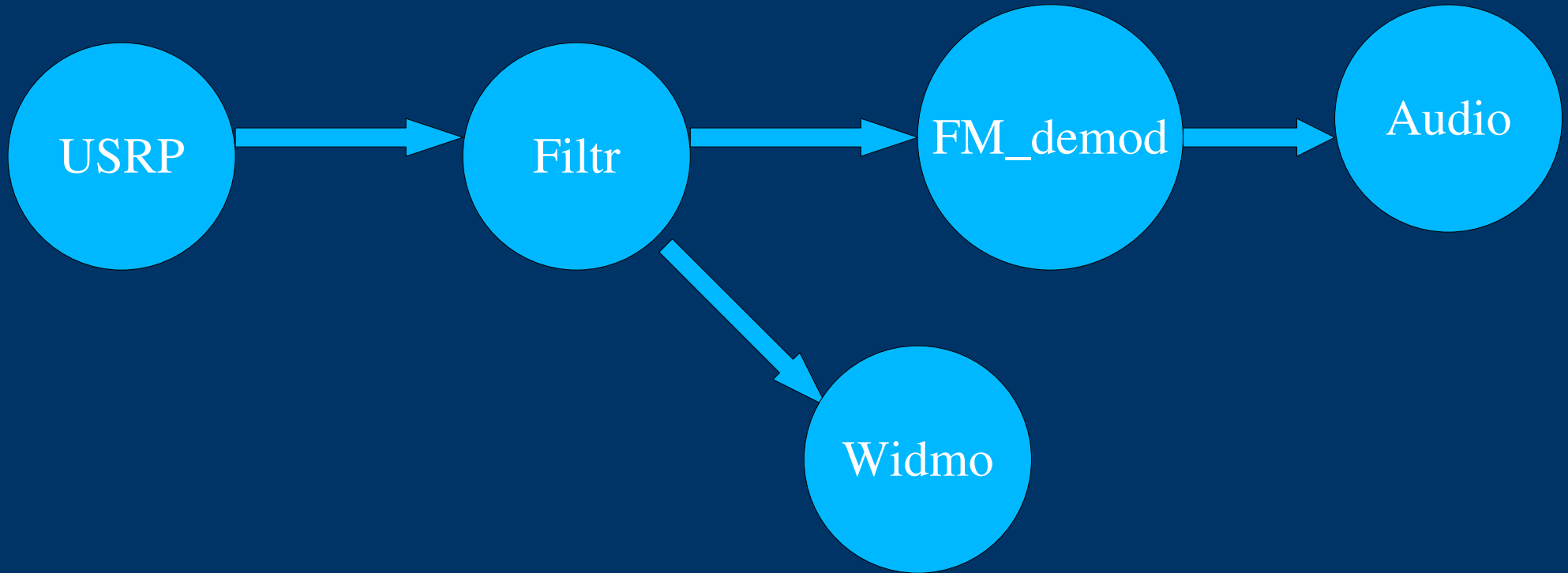
# *GNU Radio*



# *GNU Radio*



# *GNU Radio*



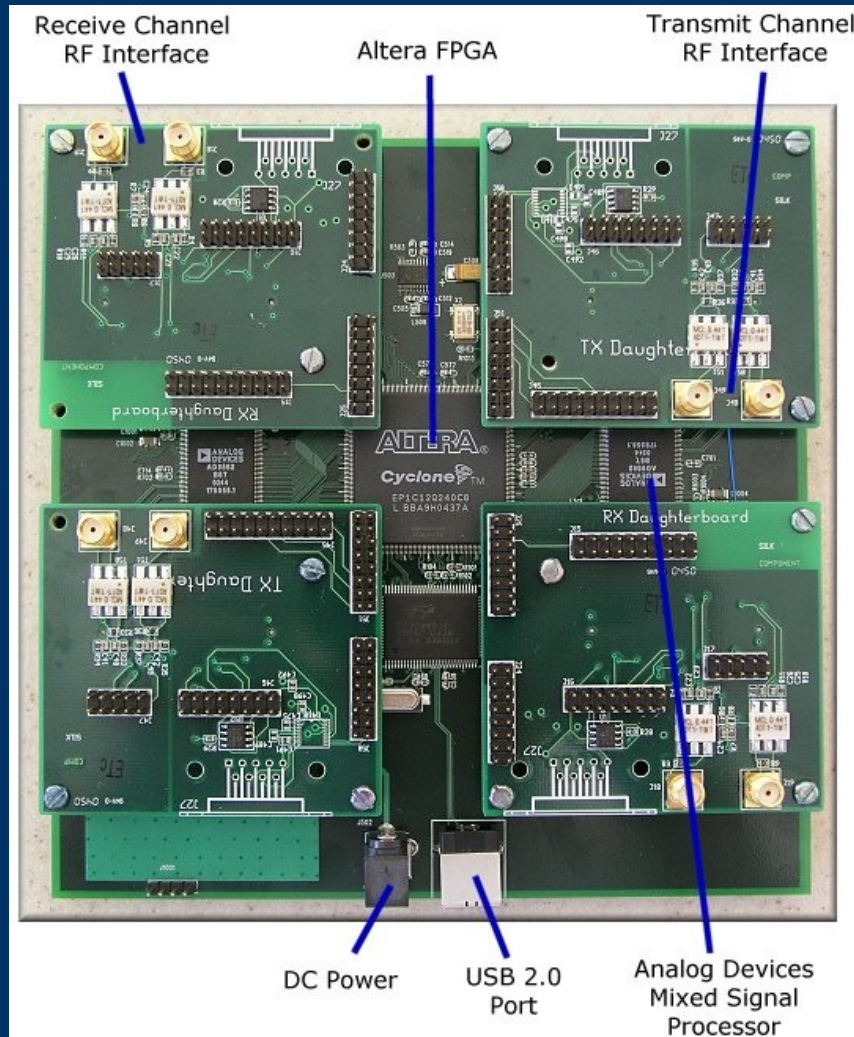


# *USRP - zastosowania*

- odbiornik radiowy
- karta telewizyjna
- GPS
- bezprzewodowa karta sieciowa
- bluetooth

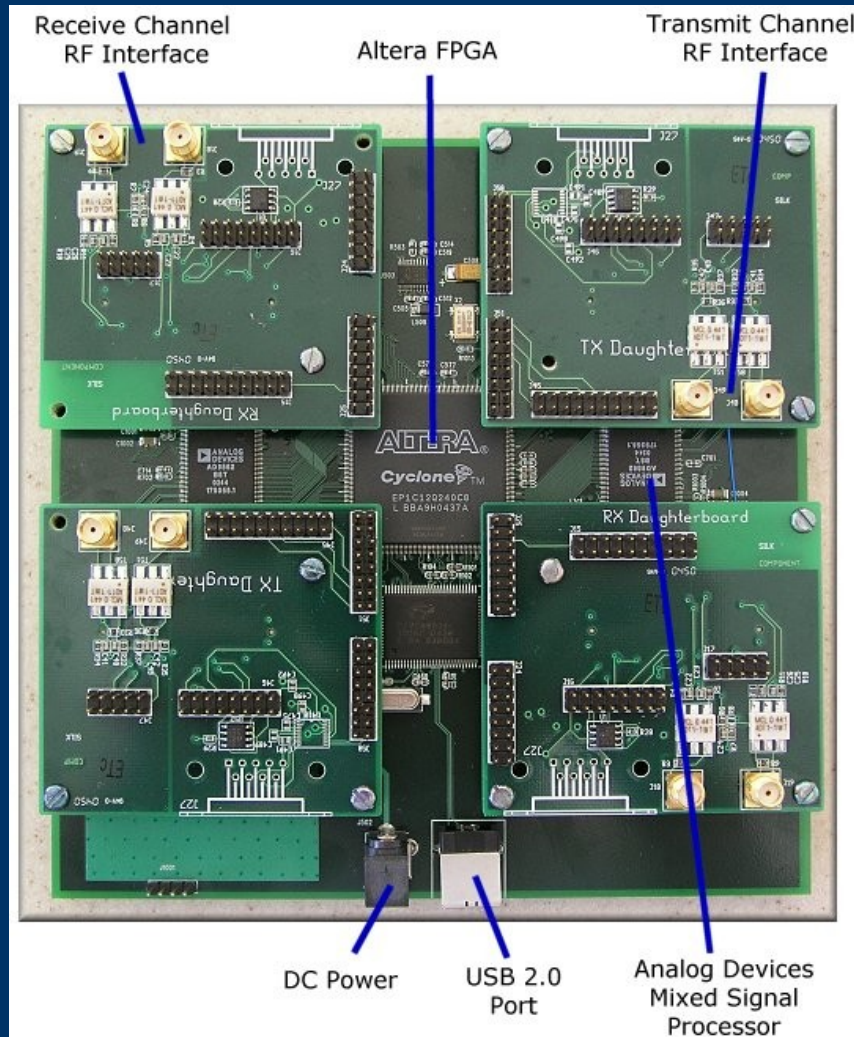


# USRP - Universal Software Radio Peripheral



- DC to 30 MHz receiver
- DC to 30 MHz transmitter
- 1 MHz to 250 MHz receiver
- 1 MHz to 250 MHz transmitter
- 50 to 860 MHz receiver
- 800 MHz to 2.4 GHz receiver
- 400-500 MHz transceiver
- 750-1050 MHz transceiver (including cell and ISM bands)
- 1150-1450 MHz transceiver
- 1.5-2.1 GHz transceiver (including PCS bands)
- 2.3-2.9 GHz transceiver (including ISM band)

# USRP - Universal Software Radio Peripheral



- DC to 30 MHz receiver
- DC to 30 MHz transmitter
- 1 MHz to 250 MHz receiver
- 1 MHz to 250 MHz transmitter
- 50 to 860 MHz receiver
- 800 MHz to 2.4 GHz receiver
- 400-500 MHz transceiver
- 750-1050 MHz transceiver (including cell and ISM bands)
- 1150-1450 MHz transceiver
- 1.5-2.1 GHz transceiver (including PCS bands)
- 2.3-2.9 GHz transceiver (including ISM band)

*GSM*



# GSM



## GSM-900

890 MHz – 915 MHz

stacje bazowe + 45 MHz

czyli 935-960 MHz

## GSM-1800

1710 MHz – 1785 MHz

stacje bazowe + 95 MHz

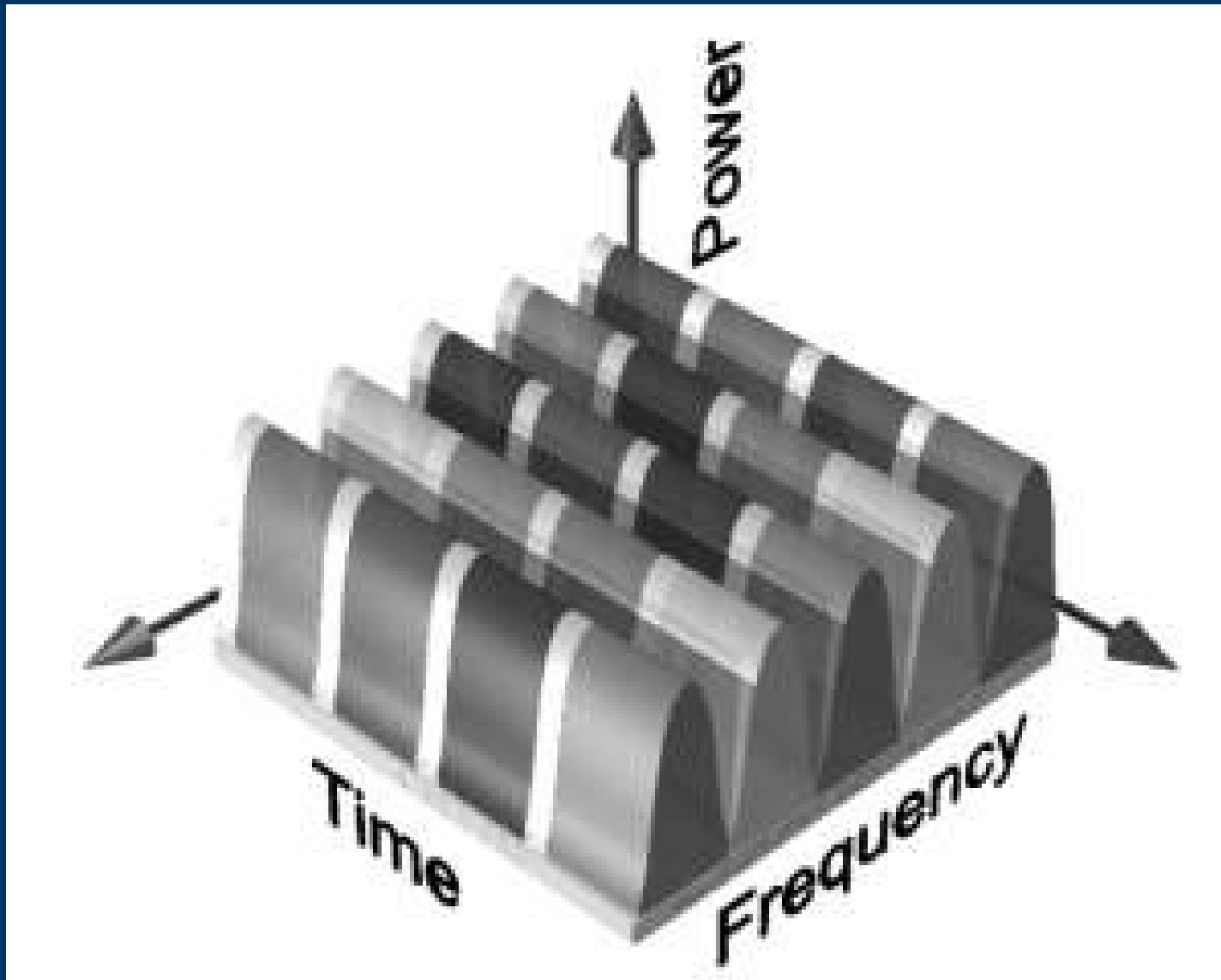
1805 MHz – 1880 MHz

# GSM

- FDMA/TDMA



# *GSM - FDMA/TDMA*



***GSM***

***– obejrzymy przy pomocy USRP***





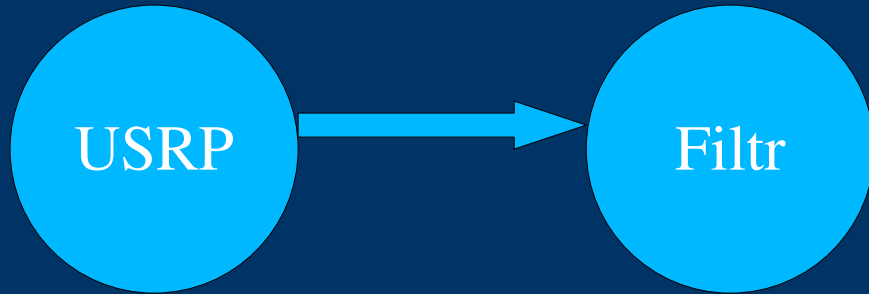
# *GSM – GNU Radio*



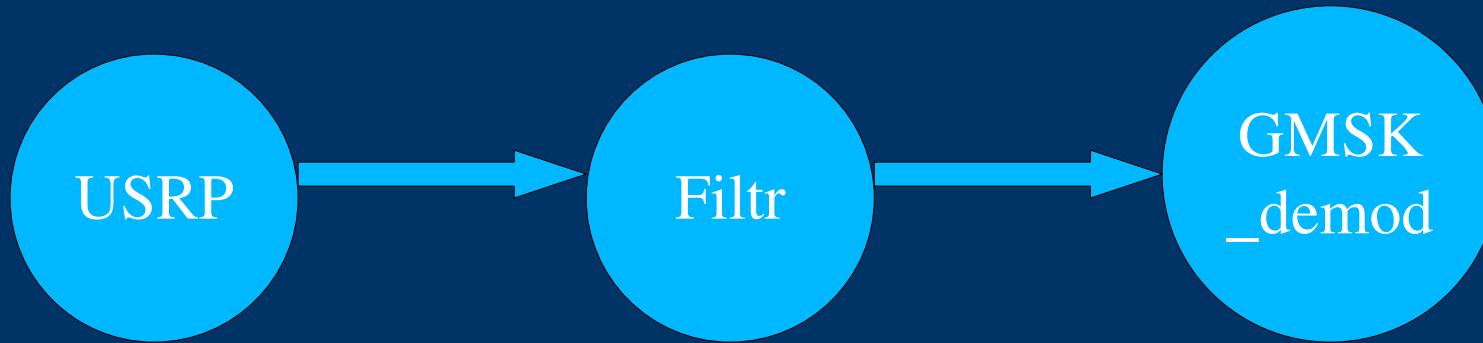
# *GSM – GNU Radio*



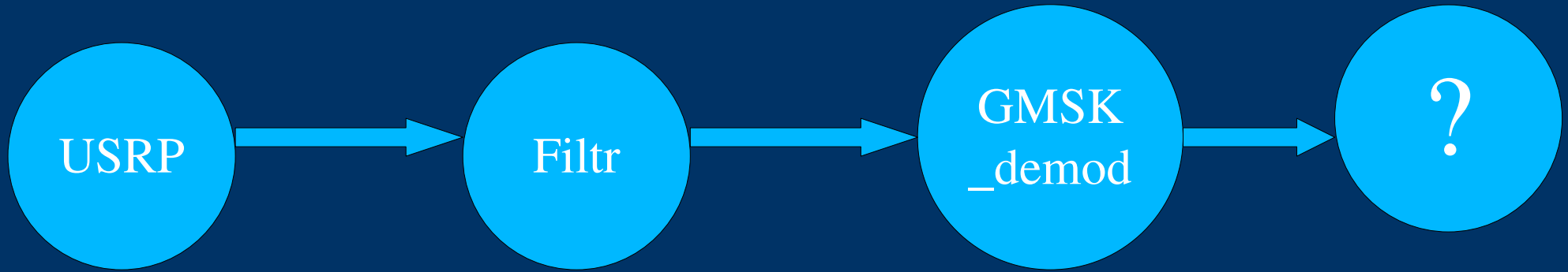
# *GSM – GNU Radio*



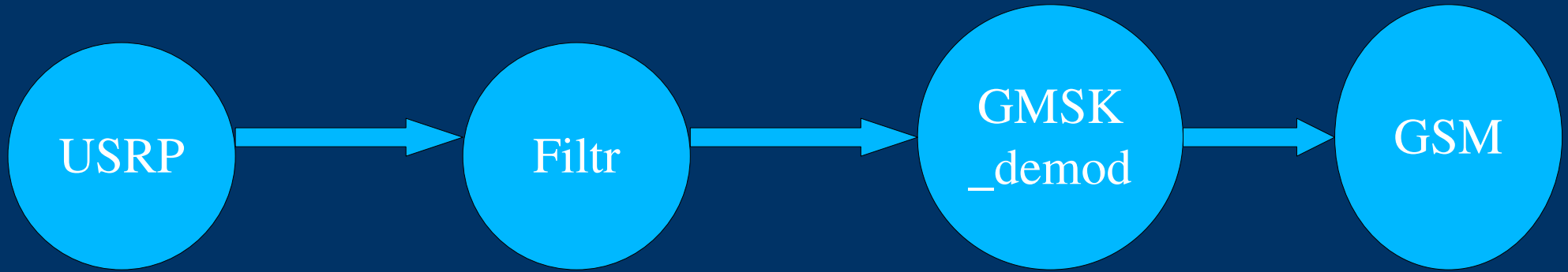
# *GSM – GNU Radio*



# *GSM – GNU Radio*



# *GSM – GNU Radio*



# *Co dalej ?*

- Analiza transmisji nieszyfrowanych
- Przechwycenie kanału TCH
- Kryptoanaliza A5/2, A5/1, oraz ataki aktywne
- Dekoder mowy



# *GSM Interceptor*





# ***GSM Interceptor***



***CENA: \$420 000***

Dziękuję za uwagę

