Wireless Systems Security

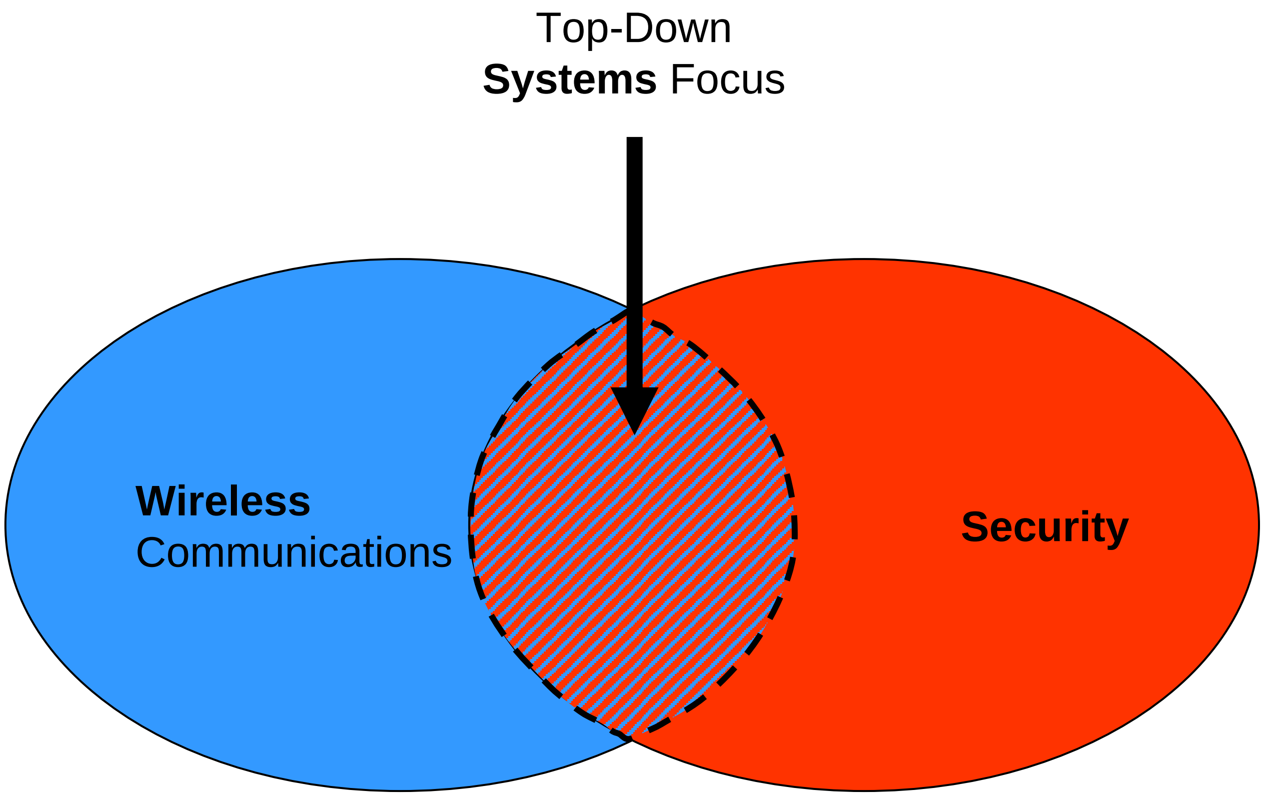
EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

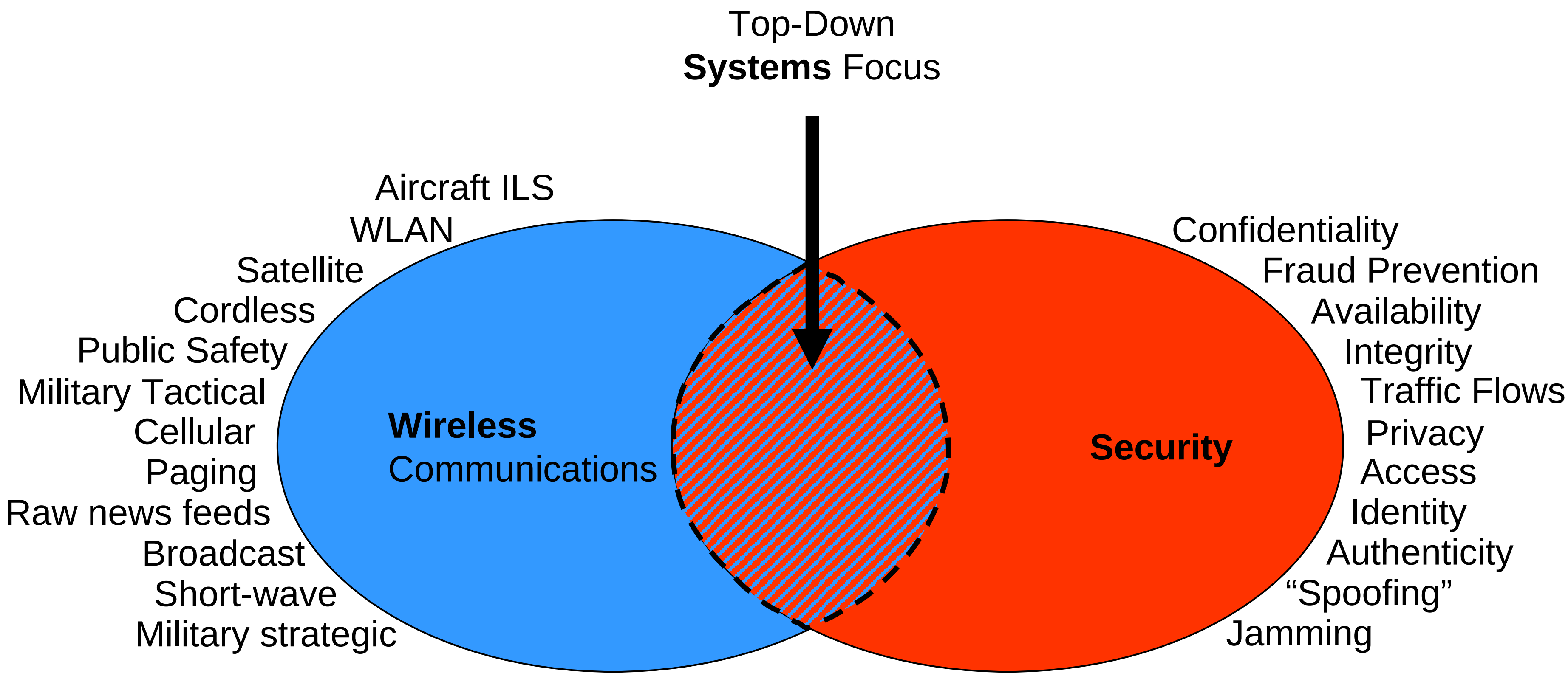
Week 1

Basic considerations in Wireless Systems

Wireless Systems Security

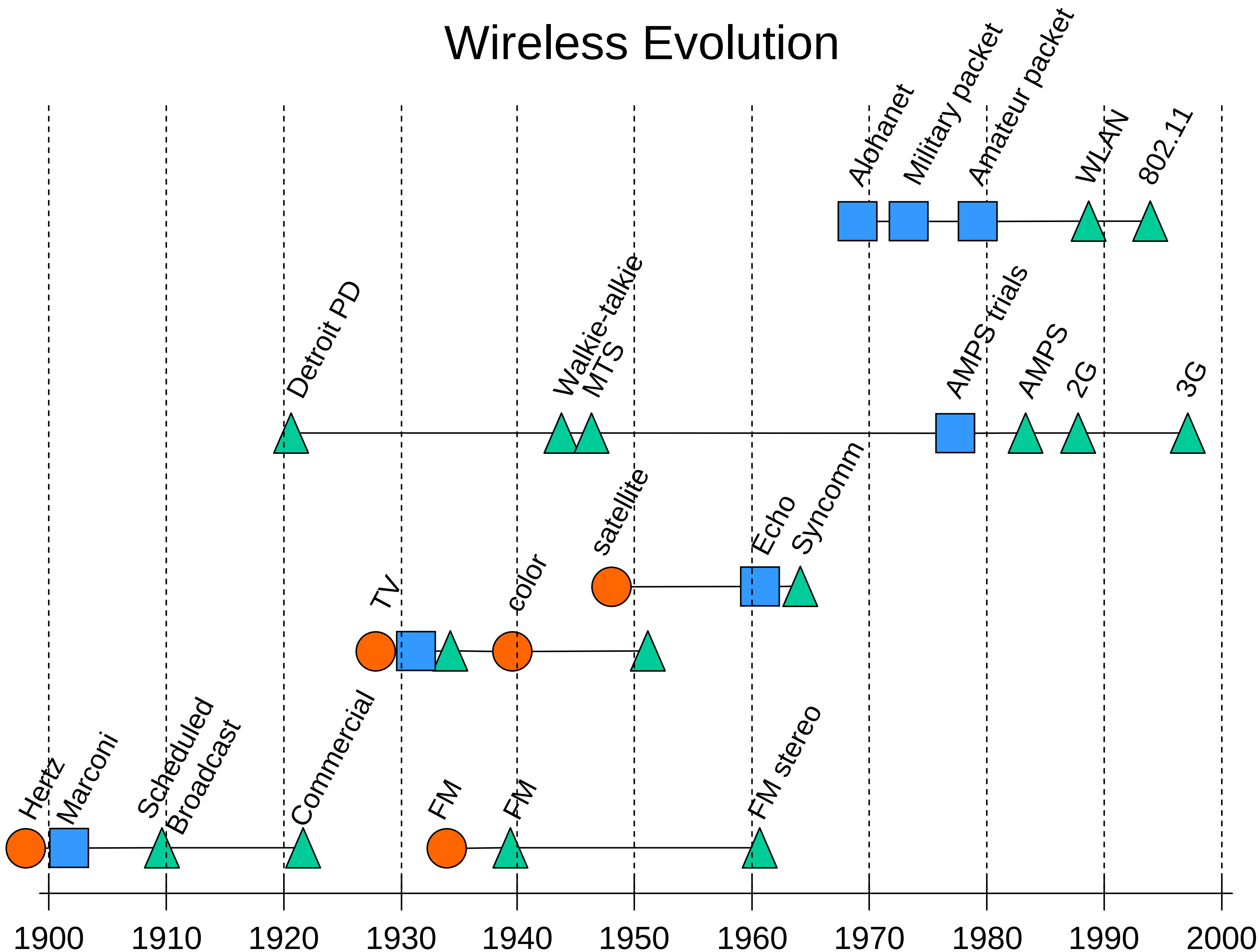


Wireless Systems Security

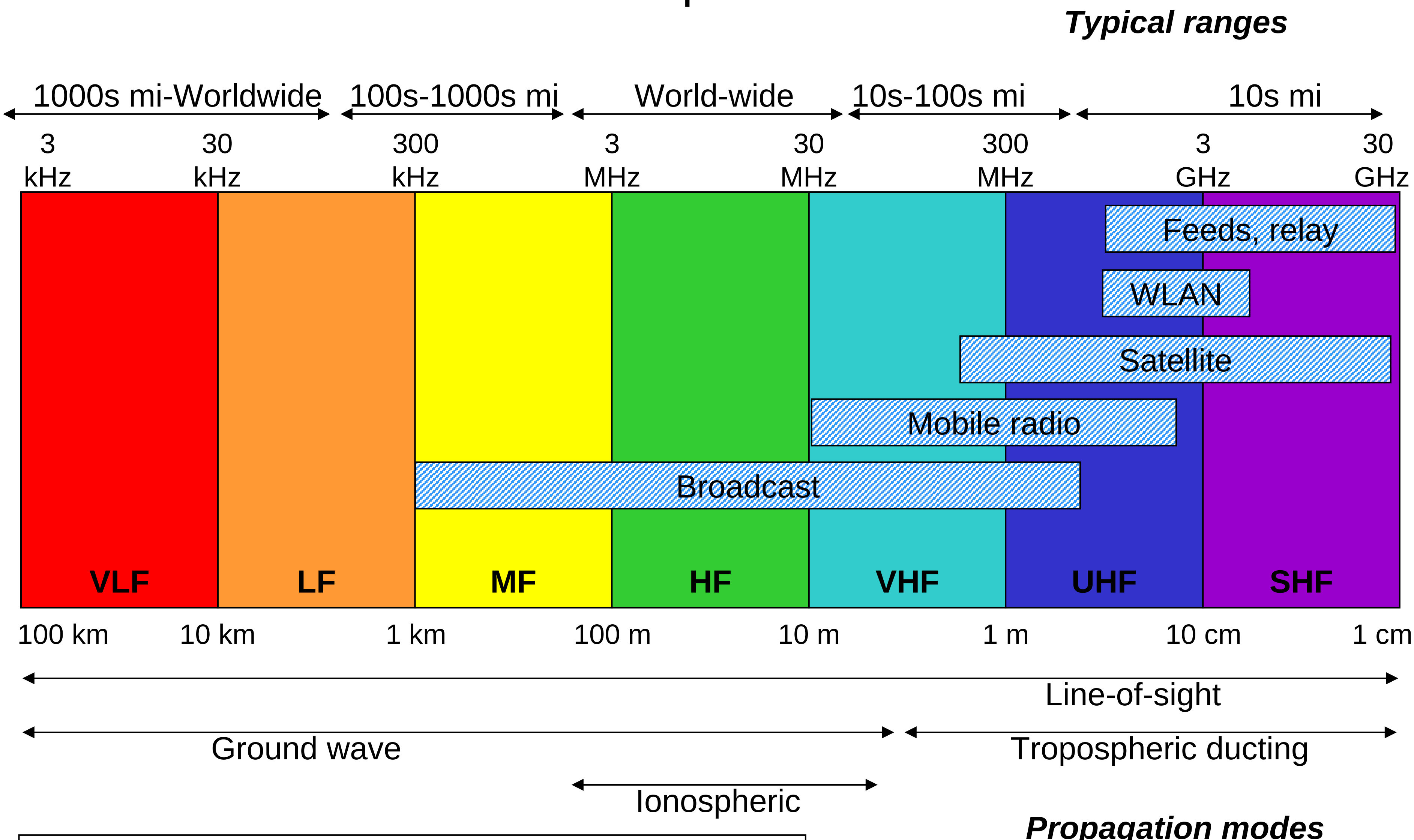


Wireless Communications Topics

Wireless Evolution

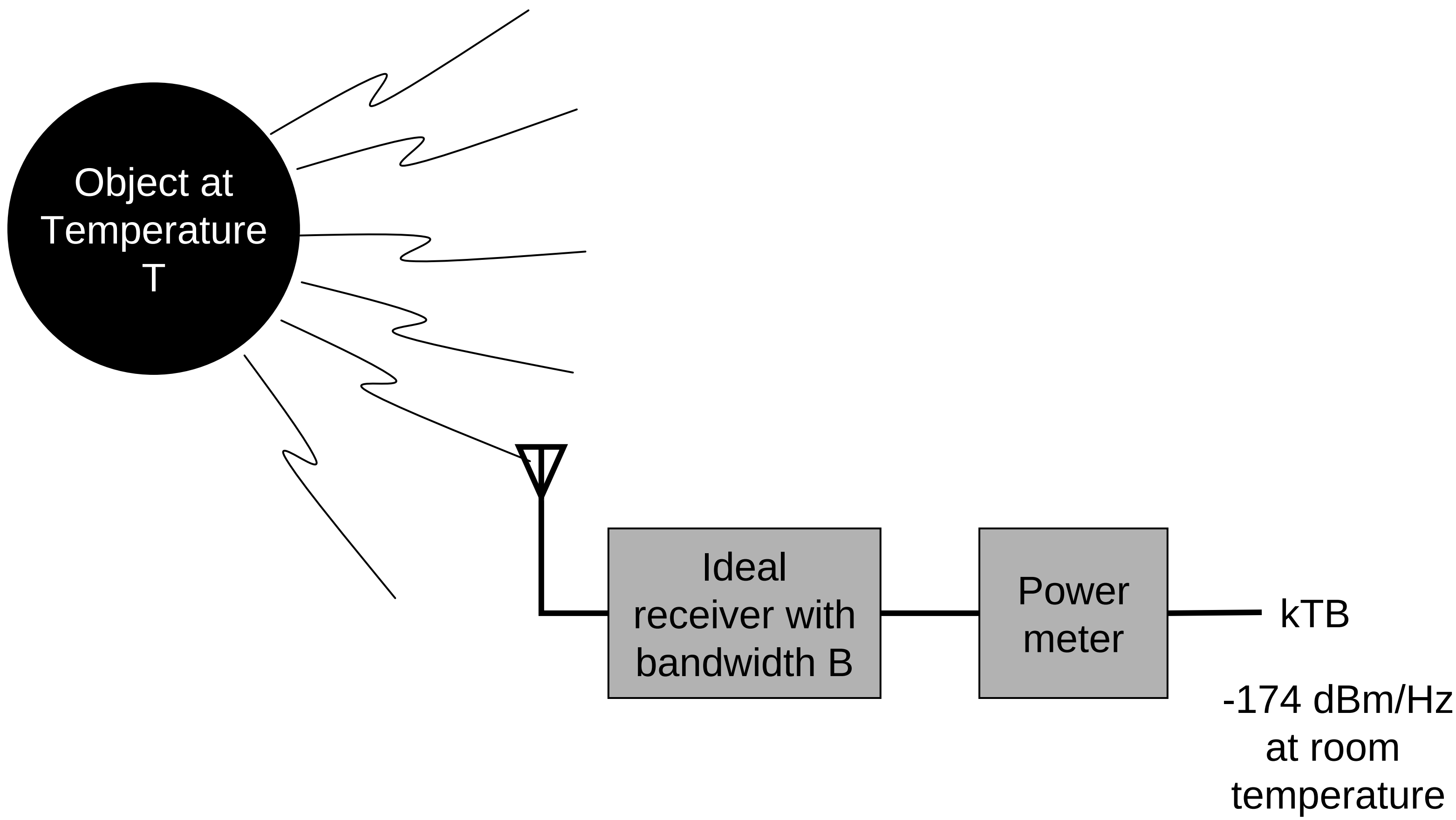


RF Spectrum



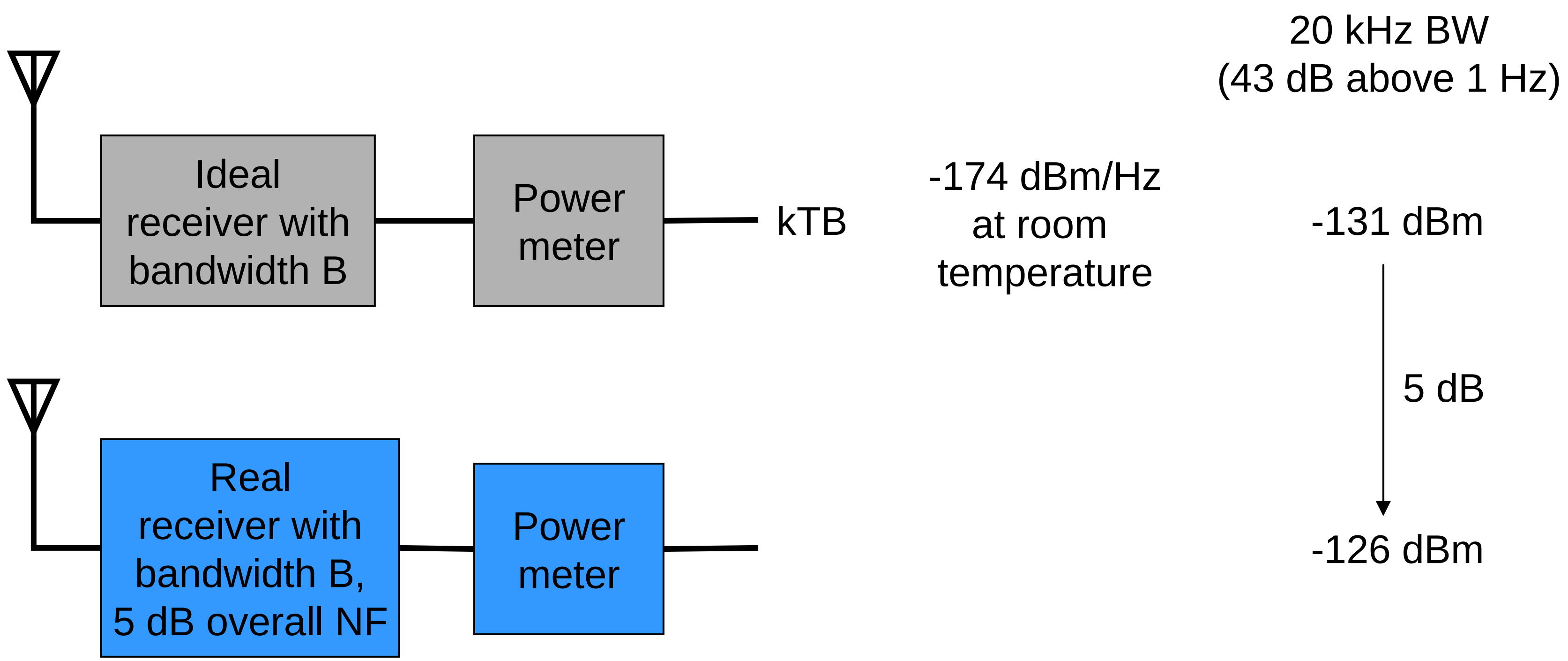
See http://www.ntia.doc.gov/osmhome/allochrt.pdf for full details (1996)
Or http://www.jsc.mil/images/speccht.jpg for the military view

Thermal Noise



Noise Figure

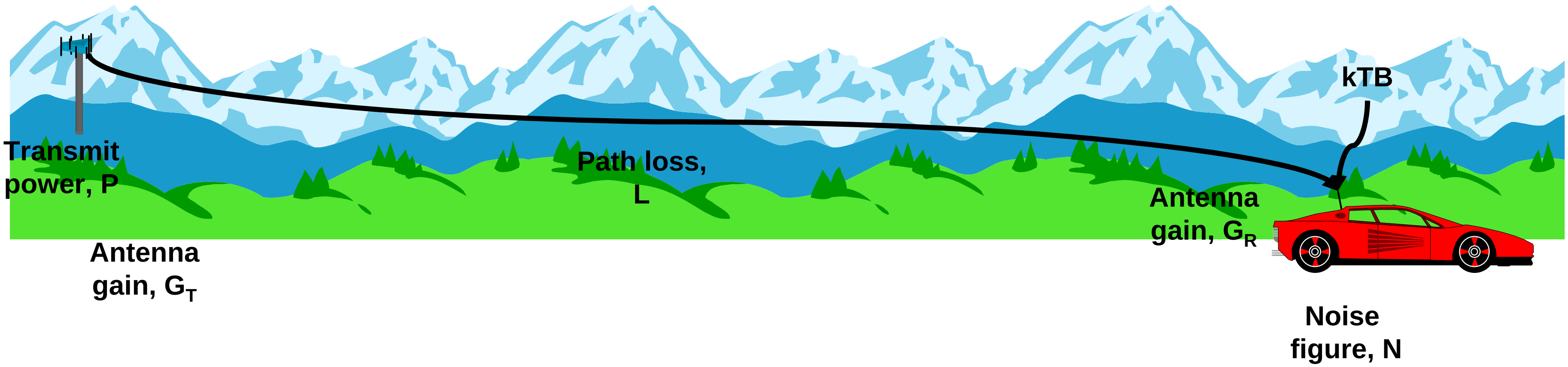
- Example: a VHF receiver with a bandwidth of 20 kHz



  – Noise figure is a measure degradation of the real system to an ideal receiver
    - Caveats!!!: operating temperature, bandwidth, impedance

Sensitivity

- The full story behind receiver sensitivity:

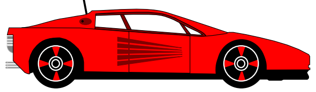


- The full story is a link budget analysis – we'll leave that until later. The simplified question:
  – What input level to the receiver will give acceptable performance?

$$P_{in} = (kTB \text{ noise}) + (NF \text{ degradation}) + (SNR_{acceptable\_performance})$$
$$= (-174 \text{ dBm/Hz}) + 10\log B + NF_{dB} + (SNR_{acceptable\_performance})$$

Sensitivity

- How do you define "acceptable performance?"



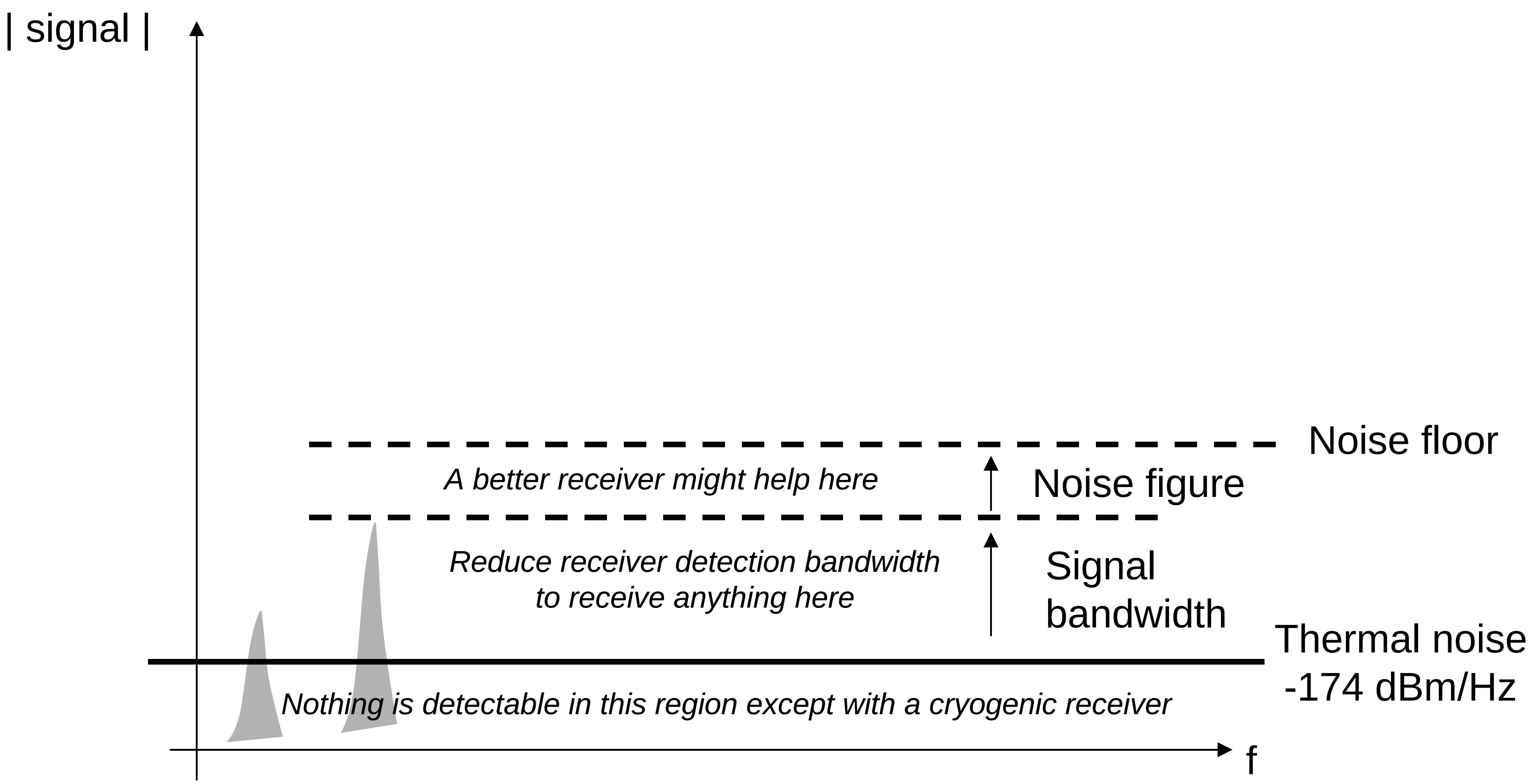
  - Data: SNR at demodulator to give a particular BER or BLER
  - Voice: SNR at demodulator to give a particular SINAD
  - Video: SNR at demodulator to give particular picture SNR

- Assume a receiver bandwidth of 4 MHz, SNR at demodulator of 45 dB, NF=8 dB (much like a TV receiver)
  - What is the required input signal level in dBm, μW, μV in 75 Ω?

$$
\begin{aligned}
P_{in} &= (-174 \text{ dBm/Hz}) + 10\log B + NF_{dB} + (SNR_{acceptable\_performance}) \\
&= (-174) + 10\log(4 \bullet 10^6) + 8 + 45 \text{ dBm} \\
&= -174 + 66.02 + 8 + 45 \text{ dBm} \\
&= -55 \text{ dBm} \quad = -25 \text{ dB}\mu\text{W} \quad = .003\ \mu\text{W} = 1500\ \mu\text{V in } 75\ \Omega
\end{aligned}
$$

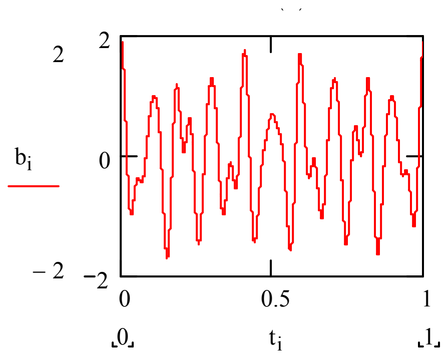
Noise Floor

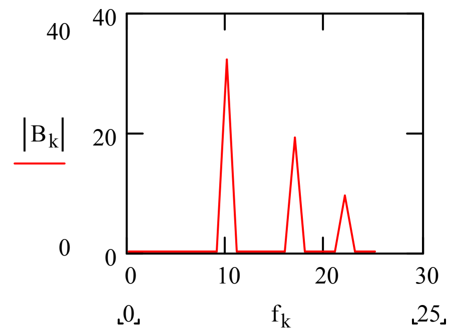
- Signals below the noise floor of a receiver are not discernable.



Modulation - baseband signals

- Consider a baseband signal, consisting of a few sinusoids. Examine the signal in the time domain and in the frequency domain:

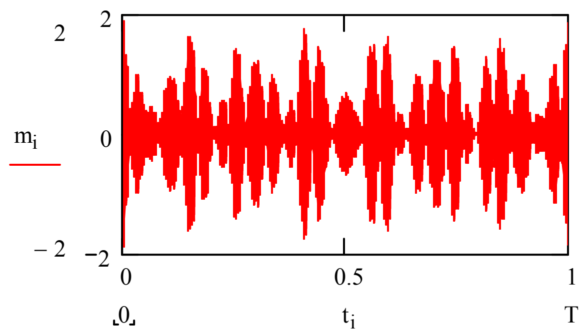


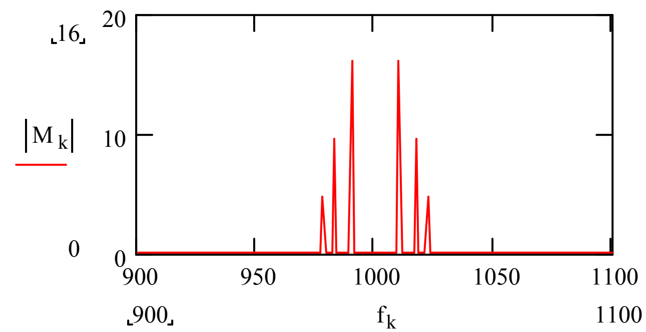


- This signal cannot be transmitted very far in its present format, nor can we allow multiple users to share the same spectrum, so the signal has to be modulated onto a “carrier”

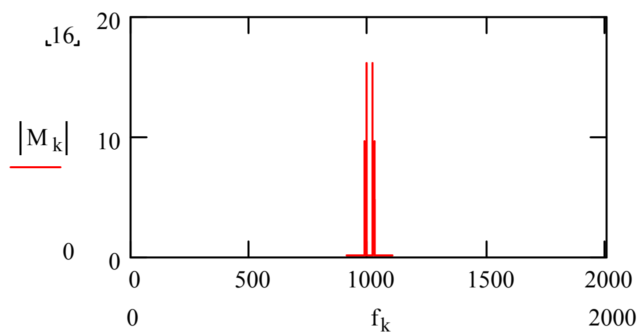
Modulation - passband signals

- By “translating” the previous signal to a “carrier” frequency, we obtain a passband signal:



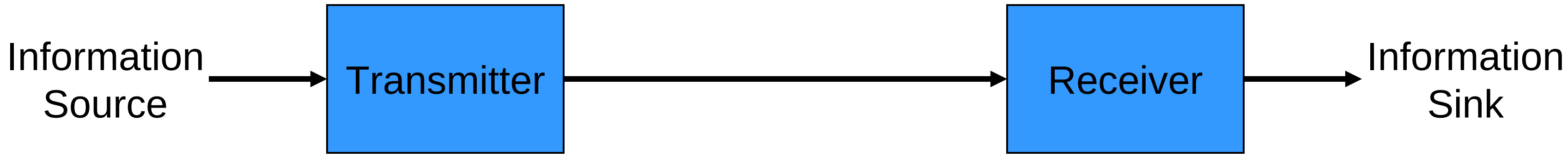


- This signal has all of its energy near the carrier frequency, in this case 1000 Hz



Modulation - a generic communications system

- Consider a simple communications system:

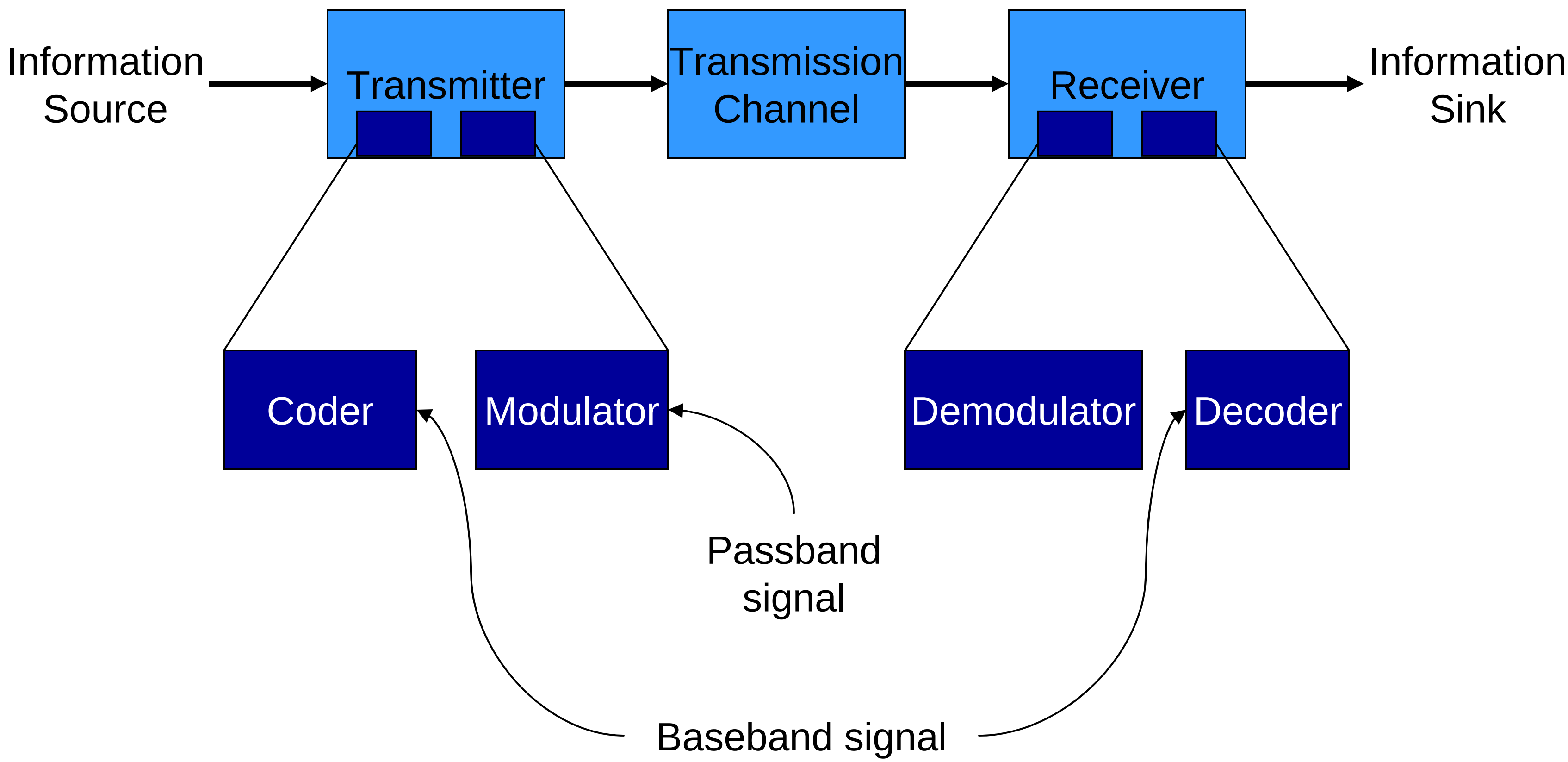


Modulation - a generic communications system

- Consider a simple communications system:

Modulation - a generic communications system

- Consider a simple communications system:



Modulation - modifiable signal parameters

- Consider a generic equation for a modulated signal *m(t)*, generated by a baseband signal *b(t).* Start with an unmodulated carrier signal:

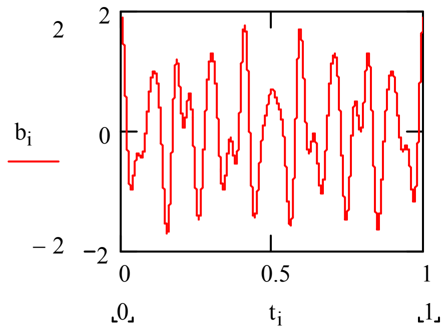
$$m(t) = A_c \cos(w_c t + \phi_c)$$

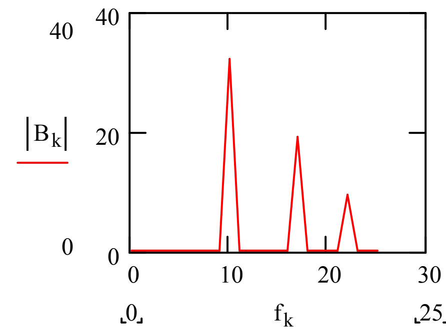
- we can modulate the carrier's
  - amplitude (as set by m_A)
  - frequency (as set by m_f), or
  - phase (as set by m_p)

Or multiple parameters could be modulated simultaneously

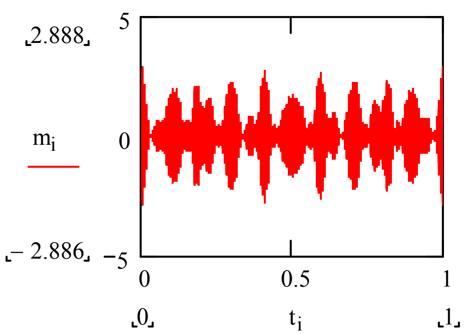
$$m(t) = A_c \left[1 + m_A b(t)\right] \cos((w_c + m_f b(t))t + m_p b(t) + \phi_c)$$

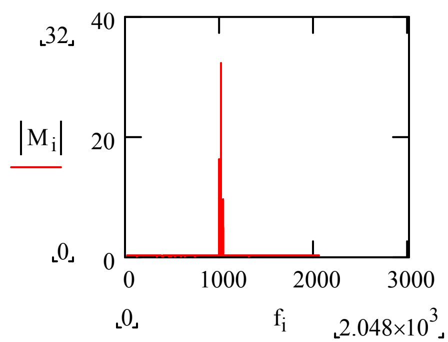
Analog modulation - AM

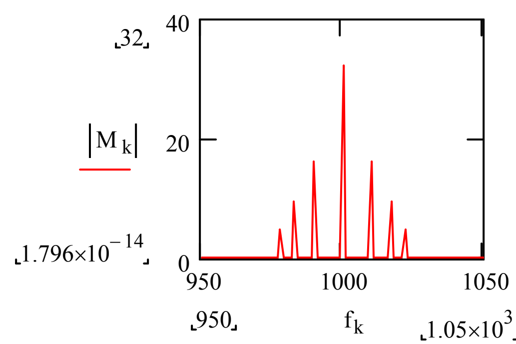




- With the baseband signal as before, set m_A to 1 (100% modulation) and the other modulation parameters to zero to obtain a purely AM signal







FM and PM

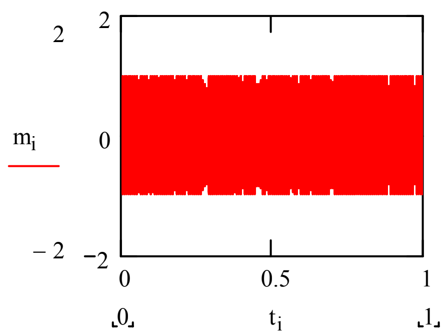
- FM and PM can be thought of as the same modulation technique with proper choice of the input signal:
  - Define the instantaneous phase of a sinusoid:

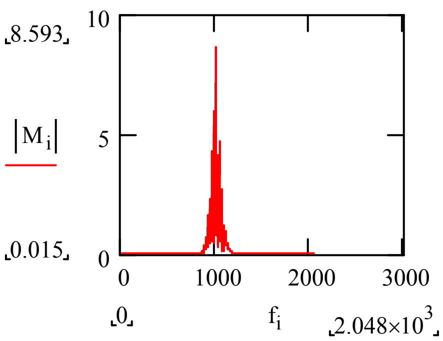
$$\phi(t) = \int_{-\infty}^{t} \omega(x)dx$$

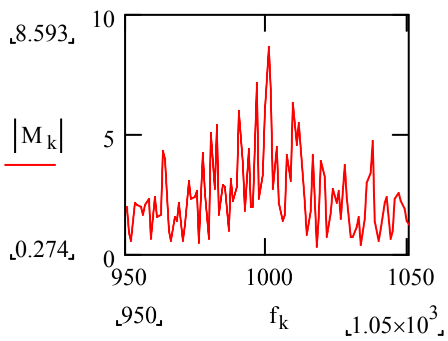
  - so, by integrating the modulating waveform presented to a phase modulation system, we have a frequency modulation system. And conversely, by differentiating the input to a frequency modulated system, we have a phase modulated system.

Bandwidth requirements of FM/PM systems

- Again, consider the earlier baseband modulating signal, this time frequency modulating the carrier.





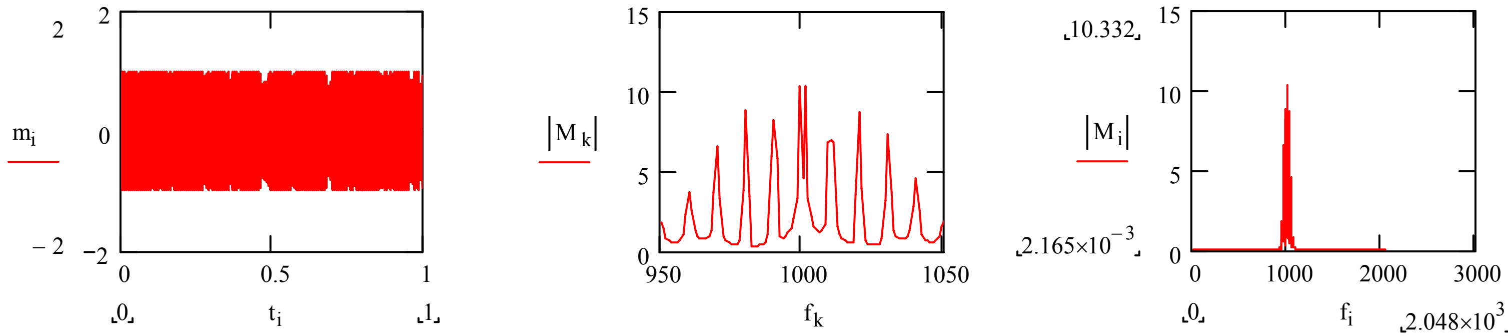


Bandwidth requirements of FM/PM systems

- An FM signal with a simple sinusoidal modulating waveform

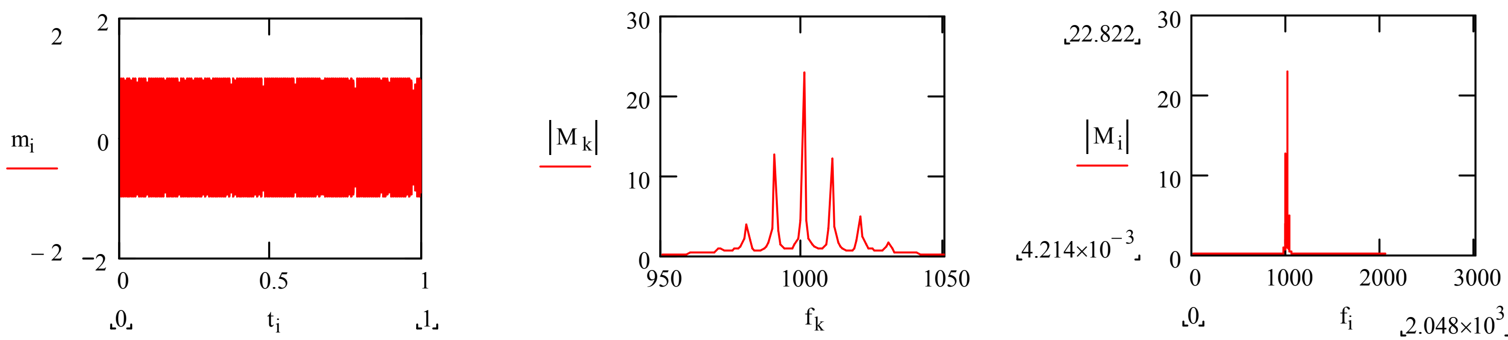
M := fft(m)

$m_f = 5\,s^{-1}$



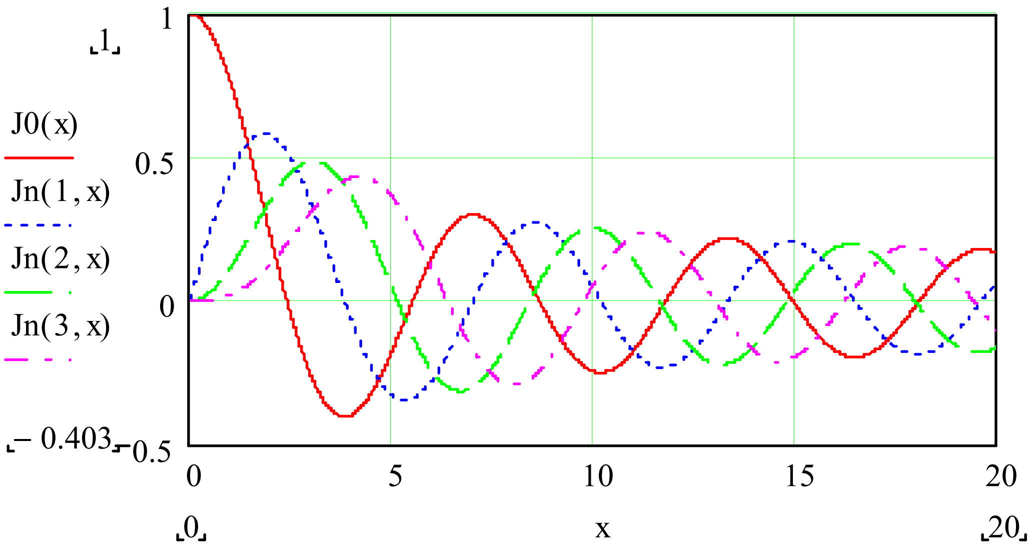
M := fft(m)

$m_f = 2\,s^{-1}$



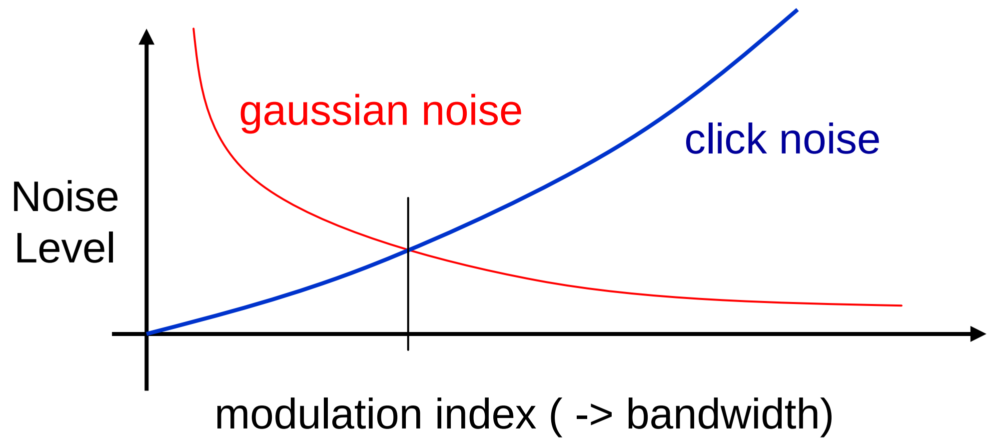
Sideband amplitudes for a sinusoidally modulated carrier

- The i^{th} sideband amplitude is described by a ith order Bessel function of the 1st kind



Performance considerations for FM systems

- Noise/bandwidth tradeoffs in FM



Digital Modulation

- As before, the generic expression for a modulated signal

$$m(t) = A_c\left[1 + m_A b(t)\right]\cos((w_c + m_f b(t))t + m_p b(t) + \phi_c)$$

- For digital modulation, *b(t)* is a digital waveform – discrete in time and level:

$$b(t) = b(nT) \in \{l_1, l_2, \ldots, l_m\}$$

- The modulated signal "shifts" between discrete states, so digital modulation techniques are referred to differently than analog modulation:

Analog	**Digital**
AM	Amplitude Shift Keying (ASK)
FM	Frequency Shift Keying (FSK)
PM	Phase Shift Keying (PSK)

M-ary signaling

- The size of the baseband signaling set may be binary:

$$b(t) = b(nT) \in \{l_1, l_2\} = \{0,1\}$$

- Or M-ary

$$b(t) = b(nT) \in \{l_1, l_2, ..., l_m\}$$

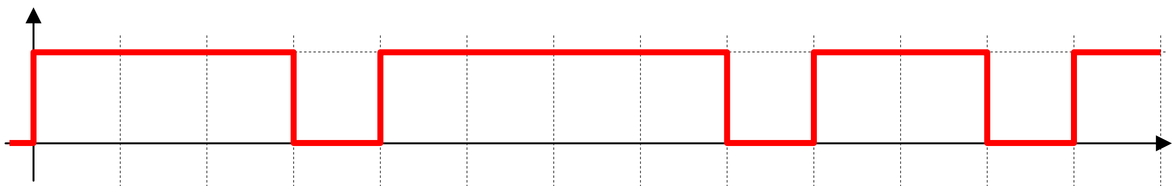
M-ary signaling

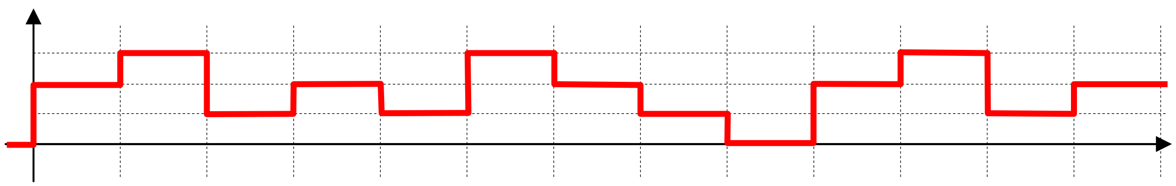
- The size of the baseband signaling set may be binary:

$$b(t) = b(nT) \in \{l_1, l_2\} = \{0, 1\}$$

- Or M-ary

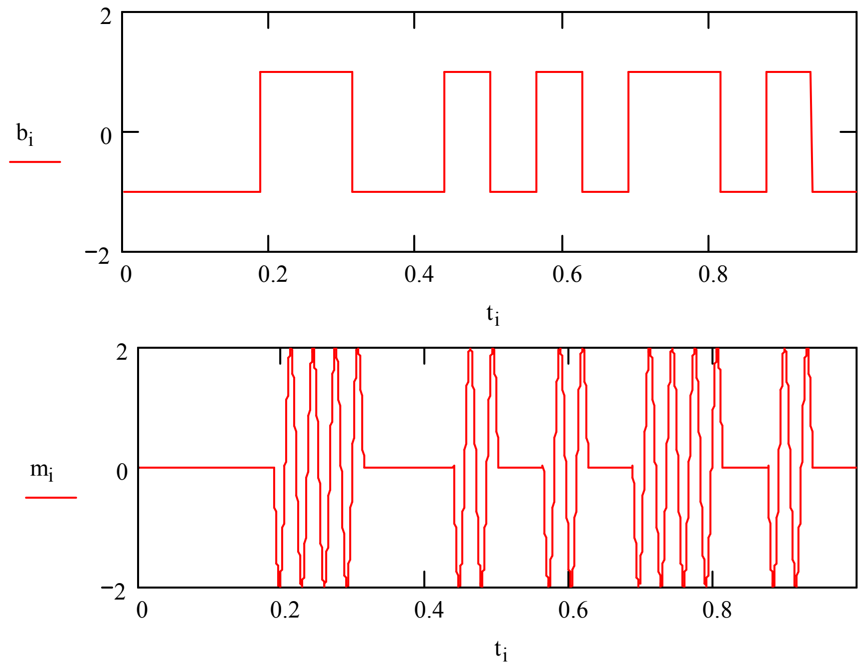
$$b(t) = b(nT) \in \{l_1, l_2, \ldots, l_m\}$$





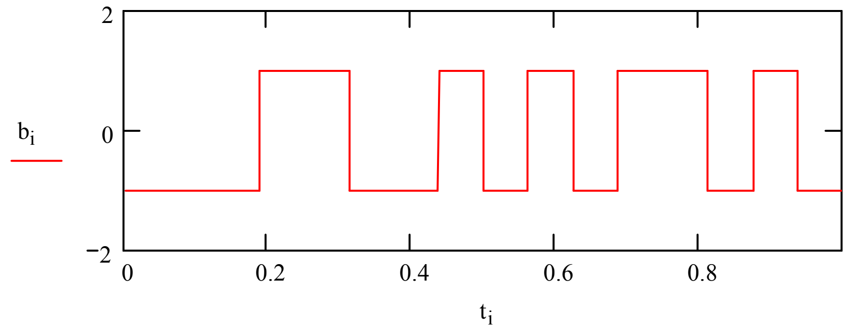
ASK

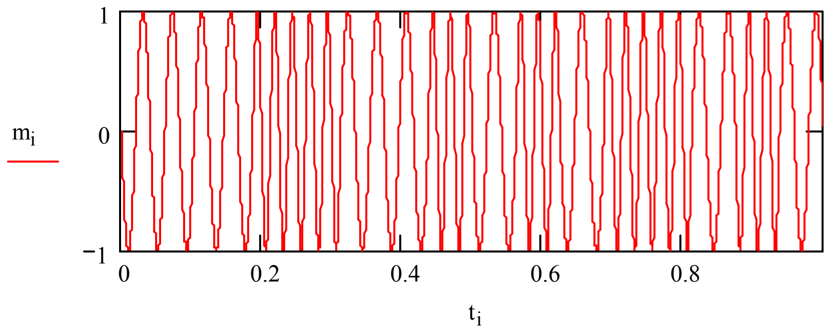
- Amplitude Shift Keying (ASK) = On-Off Keying (OOK) if the modulation is 100%



FSK

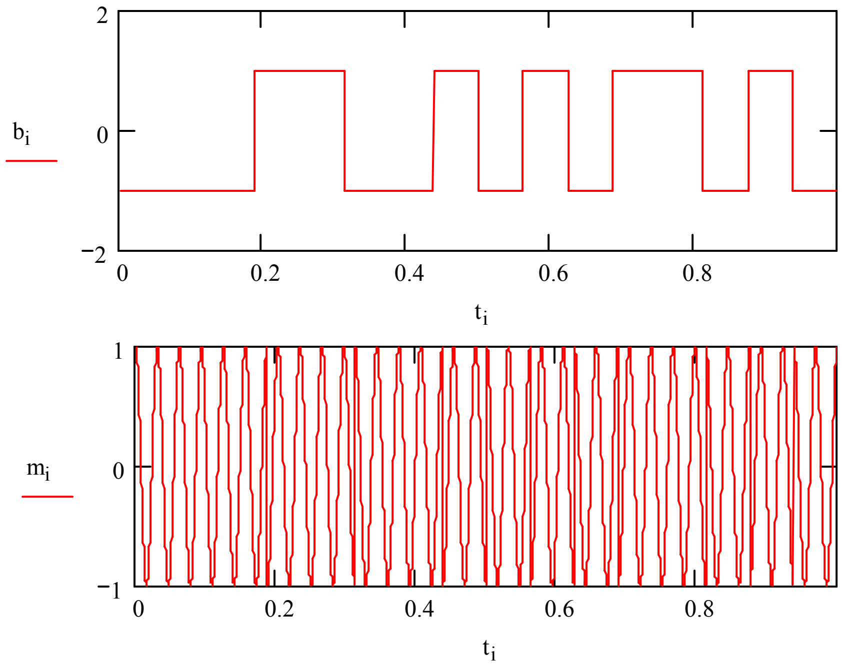
- FSK maintains the carrier magnitude





PSK

- PSK maintains the carrier amplitude and the ***average*** carrier frequency



Practical examples of analog and digital modulation systems

	Analog	Digital
AM	•AM broadcast 550-1650 kHz •Shortwave broadcast 2-30 MHz •HF Amateur radio (especially SSB) •TV video	Guided light wave systems •Cable modems •DSL •4800-56k analog modems •FAX modems •HDTV •high speed amateur packet radio
PM	• ????	•212 analog modem (1200 bps) •deep-space links •spread spectrum systems
FM	•FM broadcast 88-108 MHz •TV audio •C-band satellite TV •AMPS cellular •Police/fire/public service VHF/UHF radio	•103 analog modem (300 bps) •News & amateur HF radio teletype (RTTY) •low speed amateur packet radio (1200 bps) •Tactical military radio systems

Impairment Effects for Different Modulation Schemes

	Analog	Digital
AM	• Interferer creates a “beat-tone”	• Interferer can shift decision level
PM	• ????	• Interferer can shift constellation, interfering with decisions • Interference can appear to be excess noise
FM	• For higher modulation indices, FM capture effect suppresses weaker signal. May quiet desired signal or make interferer undetectable	• Low modulation index reduces FM capture effect