Attaque de commandes radios

Cap'Tronic
17 novembre 2016

Presented by
Yves Rűtschlé

Les grues et leurs télécommandes

Les Software Defined Radios

Fondamentaux du traitement de signal et des transmissions radio

- Transformée de Fourrier et spectre
- Modulations
- Transposition de fréquence

Travaux pratiques!

Conséquences sur le risque

Plan

Contexte

Pourquoi cette idée?

Au cours d'analyses de risques en usine, on constate l'utilisation courante de télécommandes radio. Personne ne sait vraiment nous dire comment elles fonctionnent.

Pourquoi utiliser des commandes radios?

- Moins de câblages
- Opérateur plus proche de la charge

Pas que en usine: les ponts roulants et grues de ports fonctionnent sans doute également avec ça.

La grande question

Quel est le niveau de sécurité?

Notre mission...

Connaissant uniquement la marque d'une grue...

Voir ce qu'on arrive à trouver en temps et argent limité

Se procurer une télécommande

En fait, il y a plein de fabricants de télécommandes qui s'adaptent à toutes les marques de grues. On en trouve facilement sur Internet:

Quelques exemples

- Autec Dynamic Radio System , 863-870MHZ, Channel spacing: 25kHz.
- Konductix , 433.05 — 434.5MHz, 70 channels with 25kHz spacing.
- Telecontrol F21 , $81.50
- Telecontrol F23 , 310—331MHz, 425–446MHz, '32 bits safety code', $100.
- Telecontrol F26 Konecrane , 310—331MHz, 425–446MHz, '32 bits safety code' $150.

And the winner is...

Telecontrol F26 Konecrane

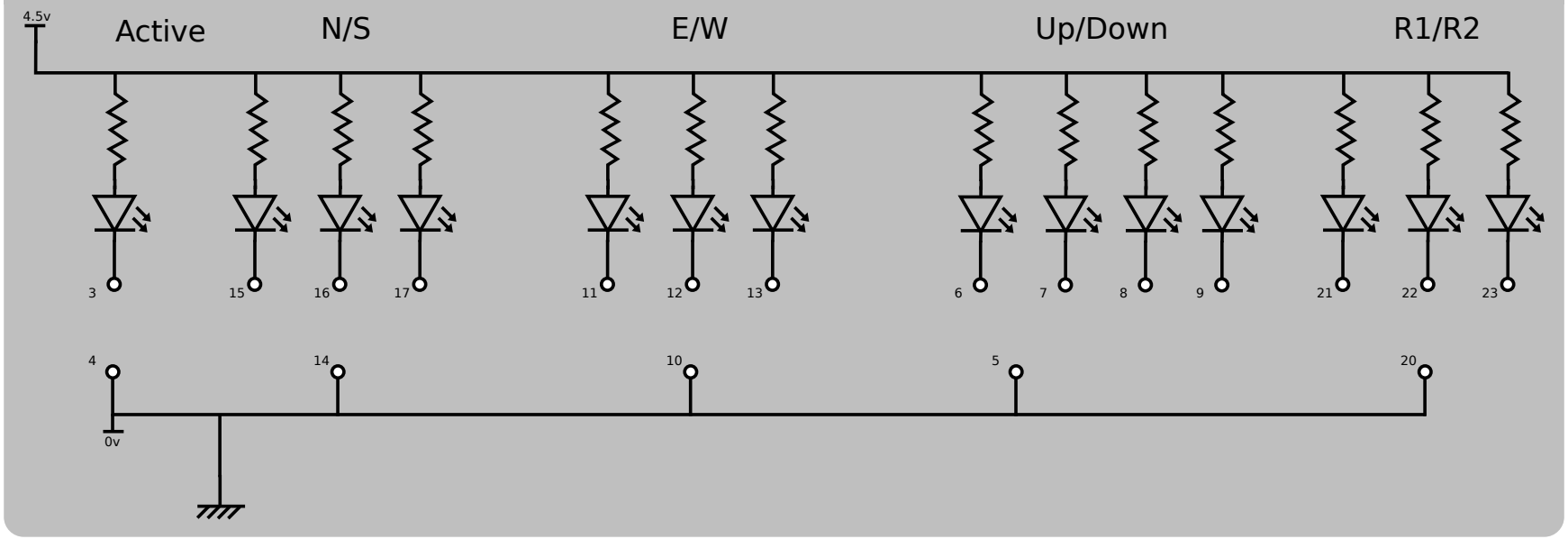
- Konecrane utilisé par nos clients
- Disponible 'facilement' sur Internet

L'appareil...

Comment ça marche?

À l'oreille, c'est des relais.

Notre grue représentative...



Plan

SDR: qu'est-ce que c'est?

- Matériel générique limité à un ADC/DAC
- Connecté à un PC par USB
- Modulations, démodulation tout réalisé en software
- Plus souple que composants discrets: le FPGA de la radio
- Inconvénient: la latence est plus importante

SDR: Le HackRF

Pour 300€ sur site radio-amateurs

1MHz à 6Ghz, RX et TX

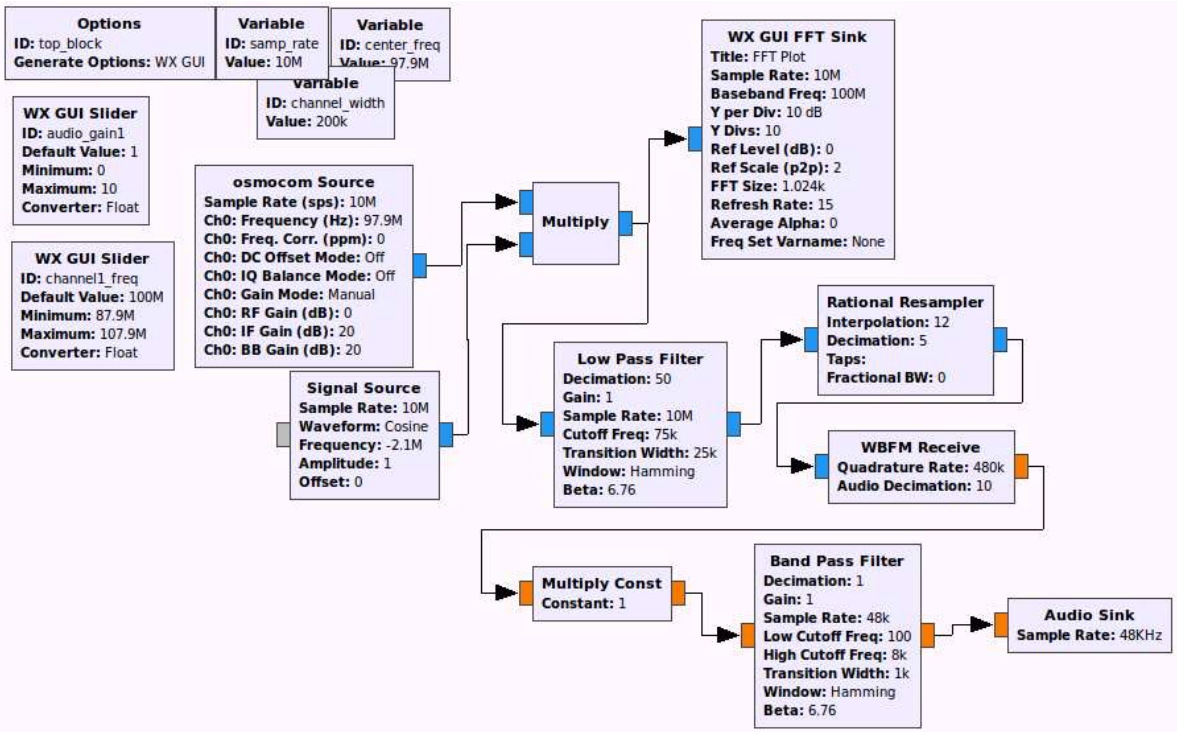
Il y en a d'autres (clés TNT, USRP d'Ettus)

Gnu Radio

- Le logiciel de SDR le plus courant
- Logiciel libre
- Bas niveau en C++
- Haut niveau en Python

Gnu Radio Companion génère le Python à partir d'un schéma

Exemple: une radio FM



apsys
SIMPLIFYING COMPLEXITY

SDR

Software Defined Radio: Remplacer une radio à 3€ par 1000€ de matériel

Plan

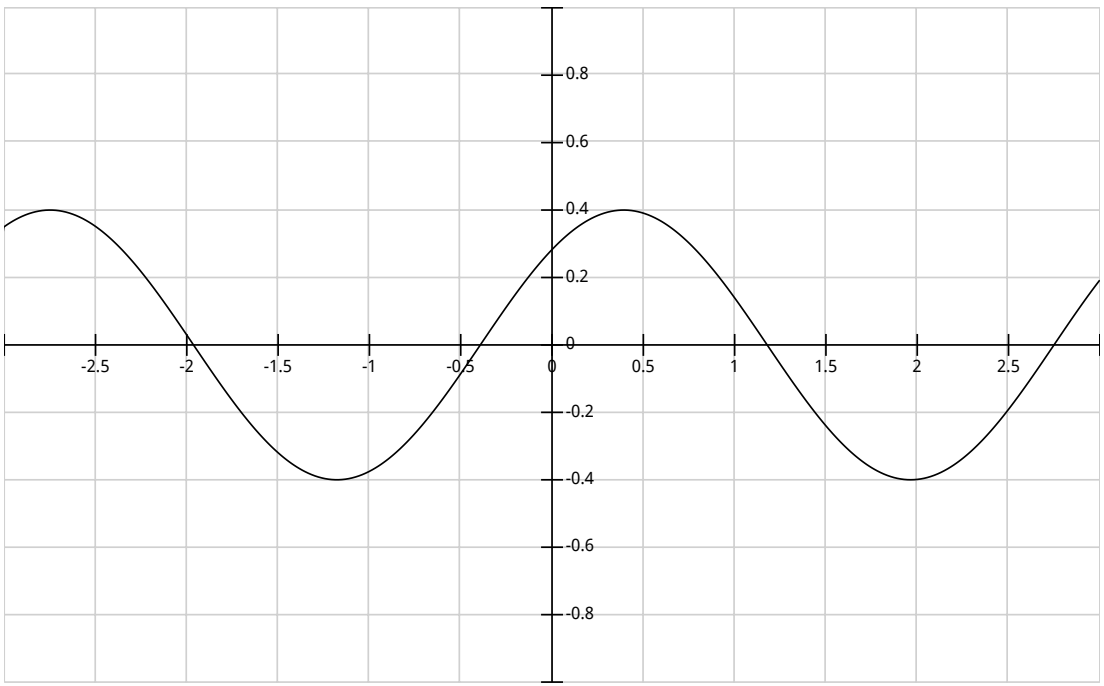
Plan

Transformée de Fourrier et spectre

Formule générale d'un signal sinusoidal

$$s(t) = A.sin(\omega t + \phi)$$

- A: amplitude
- ω: "pulsation" (équivalente à la fréquence: $\omega = 2\pi f$)
- ϕ: déphasage



Exemple:
$0.4sin(2t + \frac{\pi}{4})$

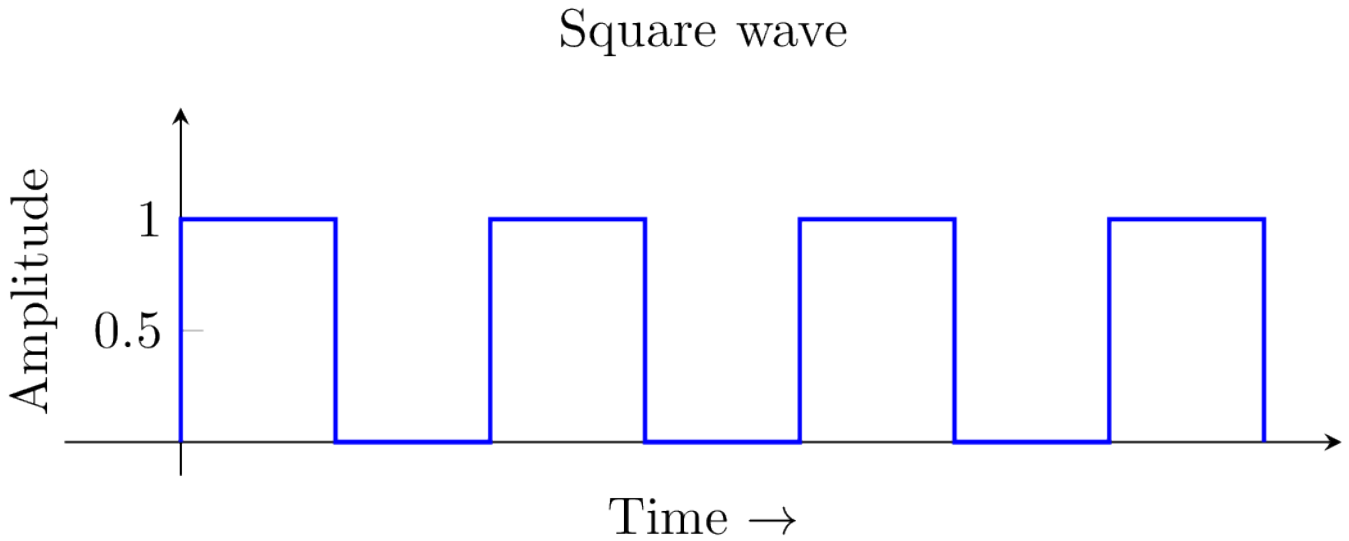
Série de Fourrier

Série de Fourrier

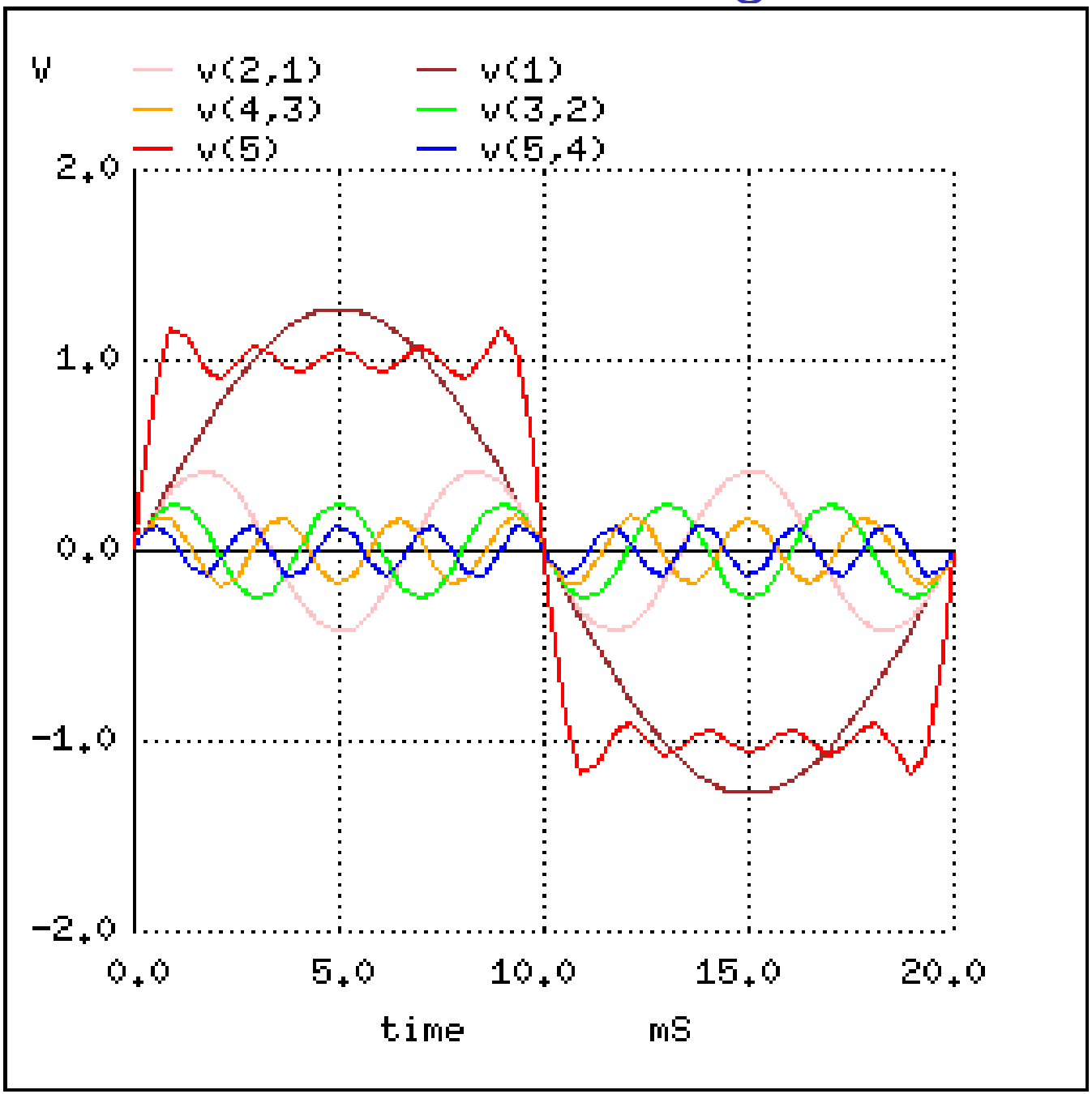
$$s_f(t) = \sum_{i=1}^{\infty} A_i sin(i.\omega.t)$$

Tout signal périodique est transformable en une somme de fonctions trigonométriques

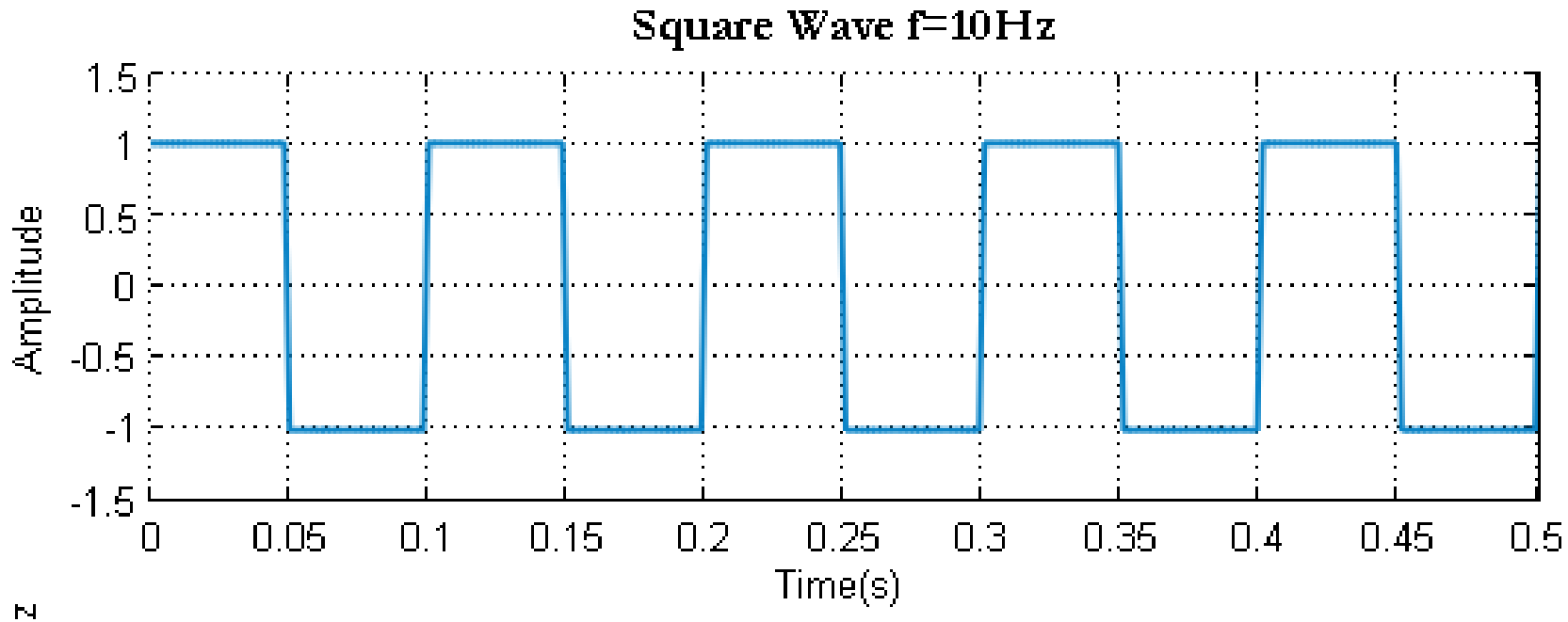
Transformée de Fourrier d'un signal carré

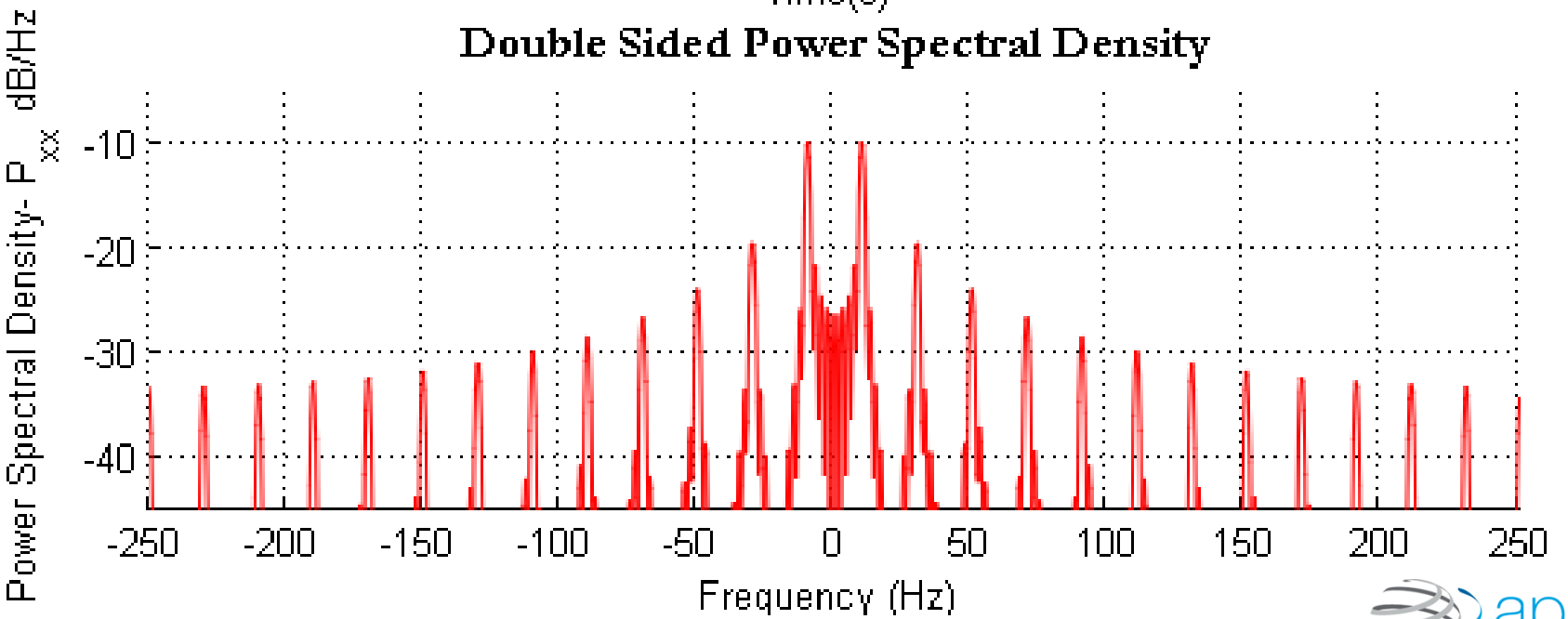


Transformée de Fourrier d'un signal carré



Spectre


Square Wave f=10Hz
Amplitude
1.5
1
0.5
0
-0.5
-1
-1.5
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
Time(s)


Double Sided Power Spectral Density
Power Spectral Density- P xx dB/Hz
-10
-20
-30
-40
-250
-200
-150
-100
-50
0
50
100
150
200
250
Frequency (Hz)

Plan

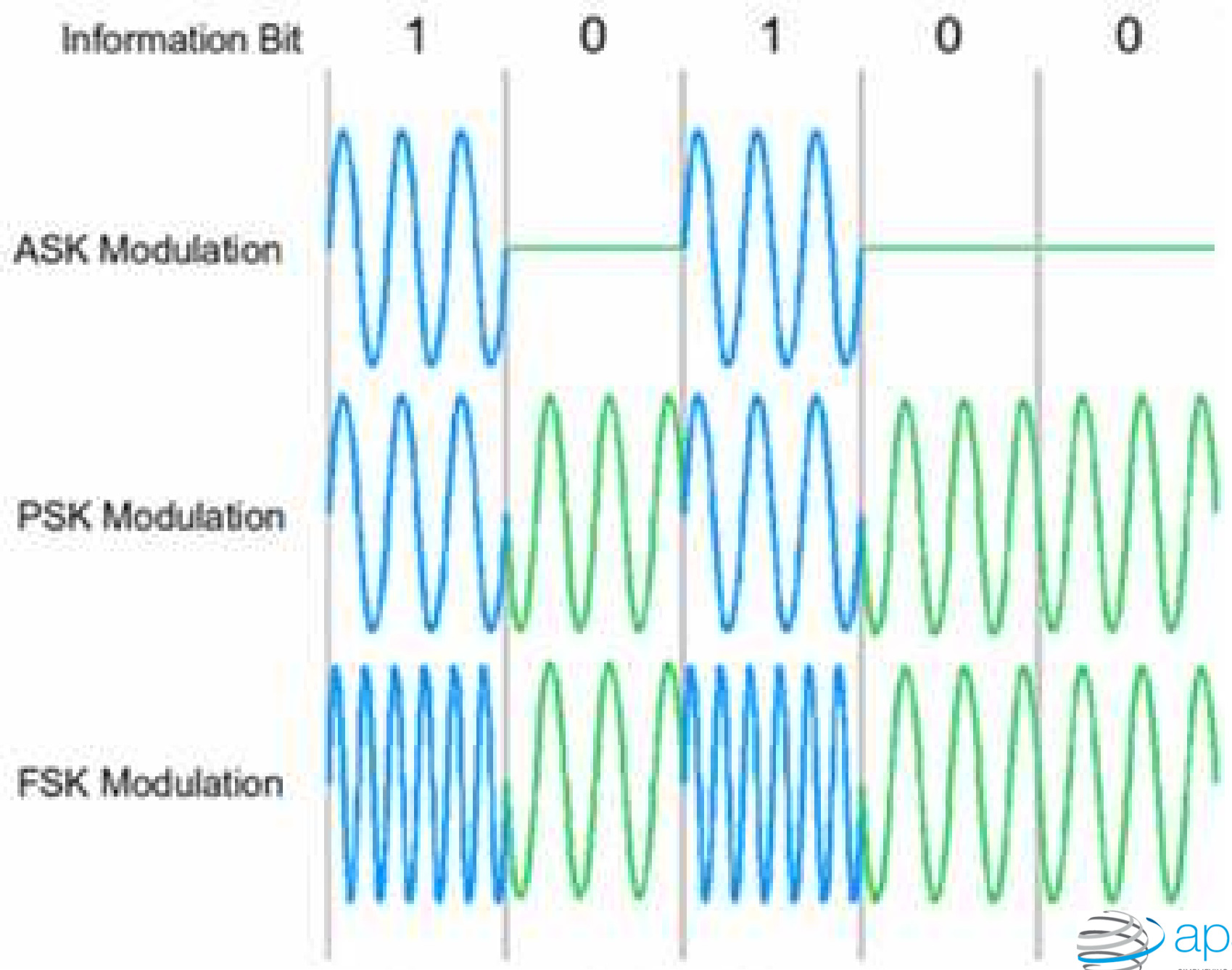
Modulations

Comment transporter de l'information sur une onde?

$$s(t) = A.sin(\omega t + \phi)$$

- Modulation d'amplitude: $s(t) = A(t).sin(\omega t)$
- Modulation de fréquence: $s(t) = A.sin(\omega(t)t)$
- Modulation de phase: $s(t) = A.sin(\omega t + \phi(t))$

Modulations



Plan

Transposition de fréquence

But: Déplacement d'un signal d'une fréquence à une autre.

Rappel de terminale

$$cos(a).cos(b) = \frac{1}{2}[cos(a+b) + cos(a-b)]$$

Il suffit de multiplier par une sinusoide à une certaine fréquence.
Pour des signaux:

Transposition de fréquence

$$cos(\omega_1 t).cos(\omega_2 t) = \frac{1}{2}[cos((\omega_1+\omega_2)t) + cos((\omega_1-\omega_2)t)]$$

Plan

Travaux pratiques!

- Recherche des fréquences: Gnuradio-Companion
- Démodulation
- Sauvegarde de trame
- Visualisation des données: kst2
- Modulation et rejeu

Plan

Qu'est-ce que ça change?

Attaque de systèmes radios devient assez facile. La distance n'est pas forcément une protection (attaque montable sur un drone).
Pour les ayatolahs de l'analyse de risque:

Potentialité d'une attaque radio

Catégorie	Ancienne potentialité	Nouvelle potentialité
Niveau d'attaquant	Expert	'Proficient'
Équipement	Spécifique	Spécialisé

Comment se protéger?

Recherche

Détection d'émissions non autorisées en se basant sur les variations de composants (variations de timing ou de puissance)

Sécuriser la commande

Approcher les constructeurs de télécommandes, car des solutions existent: rolling codes avec appariement, employés sur les voitures et volets électriques.
Ces solutions existent depuis longtemps (clé de 206 de 2001).

Questions?