

IEMI : Vers « les attaques actives »

Tristan Dubois

MCF Université de Bordeaux/Laboratoire IMS – UMR5218

tristan.dubois@u-bordeaux.fr

Geneviève Duchamp, Maxime Girard, Patrick Hoffmann

PLAN

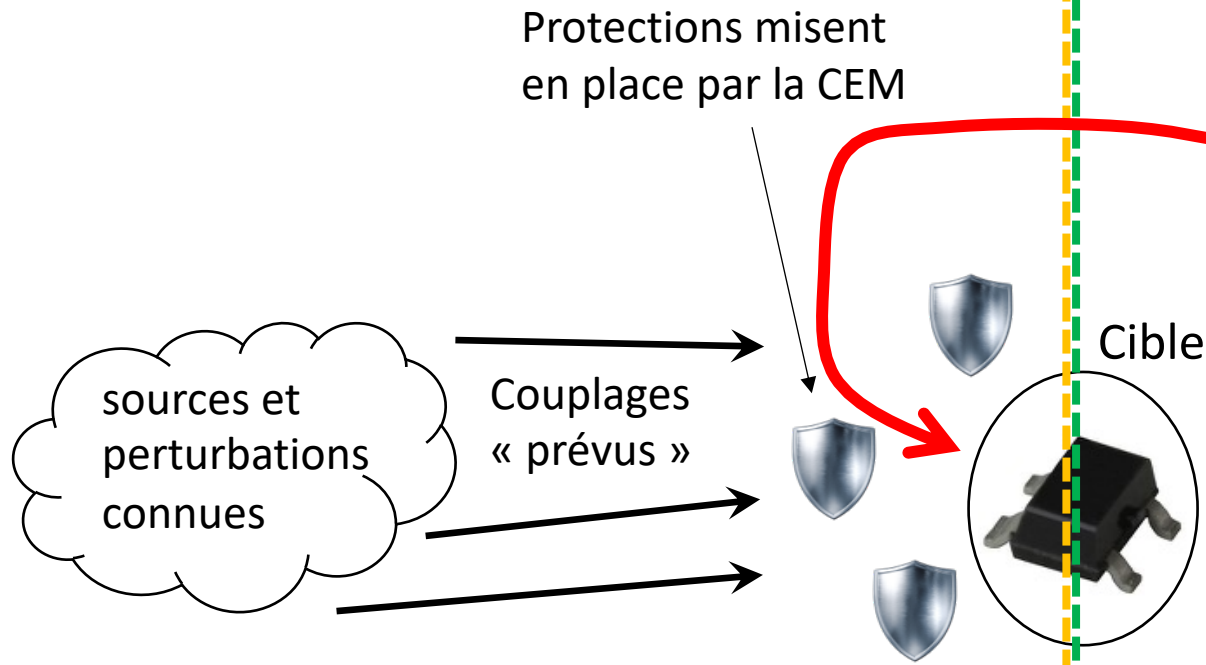
- CEM/IEMI
- Les IEMIs
 - Les sources
 - Les signaux
 - Les effets
- Techniques d'injection / Modélisation de la susceptibilité
- Cas d'étude
- Conclusions

CEM / HEMP / IEMI

HEMP/EMP (attaque globale)

CEM

IEMI (attaque ciblée)



IEMI : Perturbations hors-normes par définition dont le but est de :
Perturber le fonctionnement de la cible en contournant les protections mises en place par la CEM.

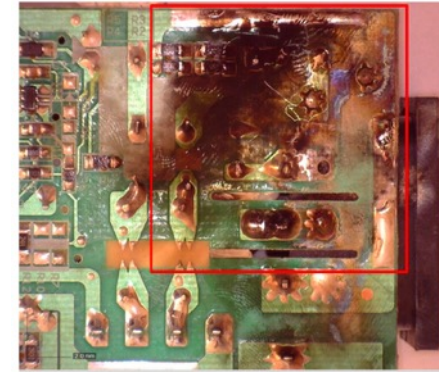
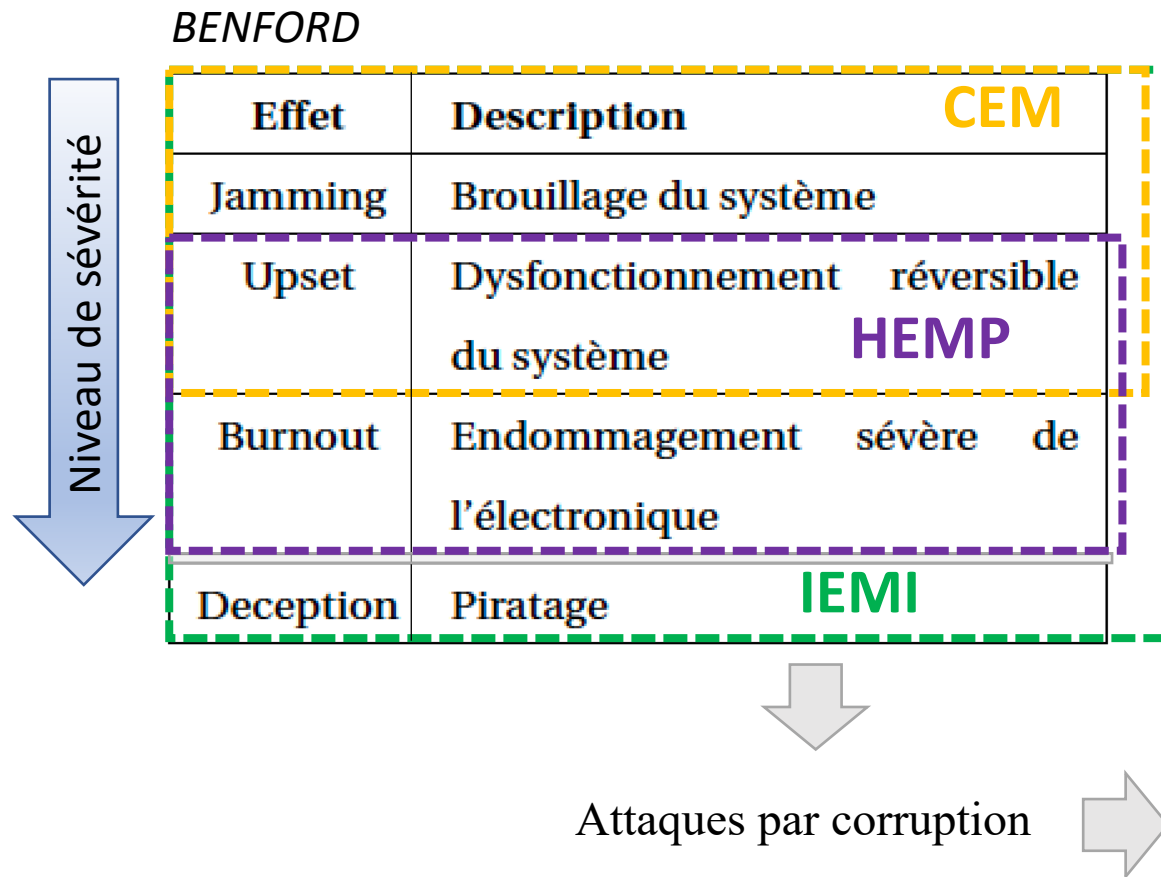
Normes : Assure le fonctionnement d'un système électronique dans un environnement électromagnétique sans perturber cet environnement.

Comment ?

En jouant sur :

- les **niveaux d'amplitude**,
 - les **formes d'onde**,
- des signaux d'interférence.

Effets sur la cible : classification



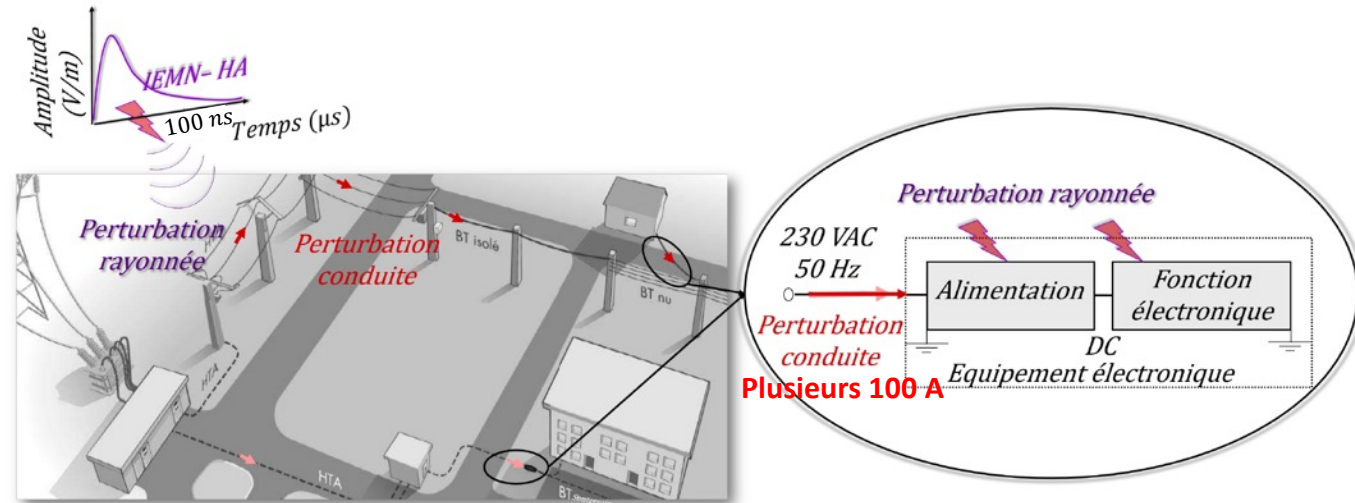
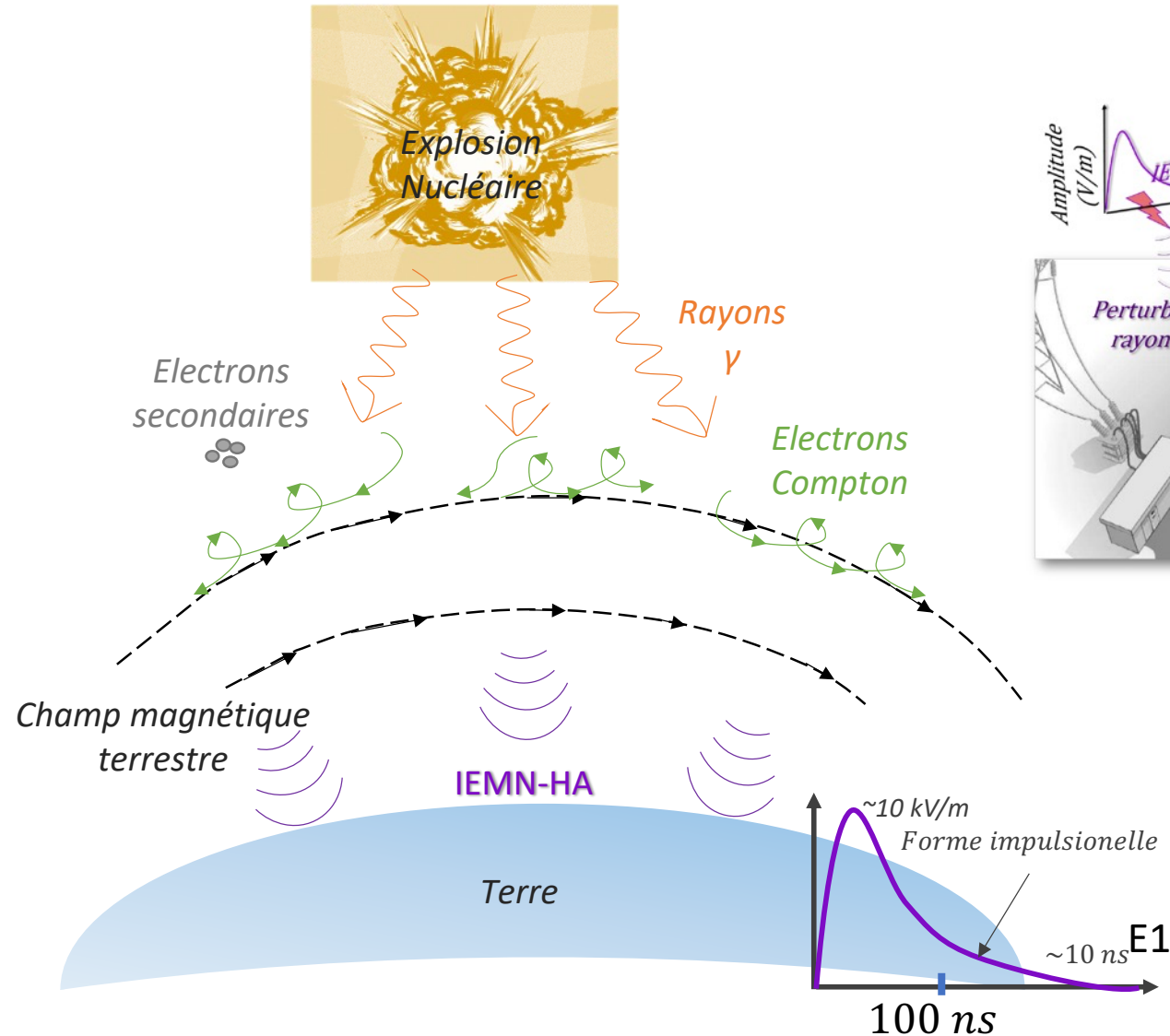
Ajout d'une information malveillante :
**Domaine de la Sécurité
Electromagnétique**

Les sources IEMs

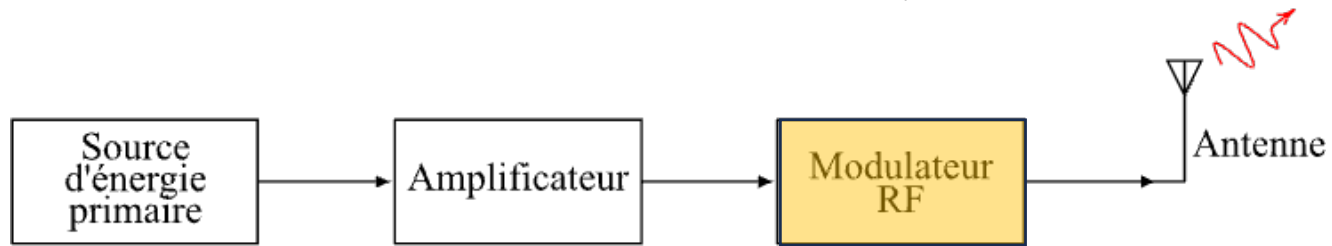
- Les impulsions EM de fortes amplitudes d'origine nucléaire (HEMP)
- Les armes à énergie dirigée EM (AED EM) – Impulsion électromagnétique; Microonde de moyenne et forte puissance (MFP)

Les HEMP : impulsion nucléaire - IEMN-HA

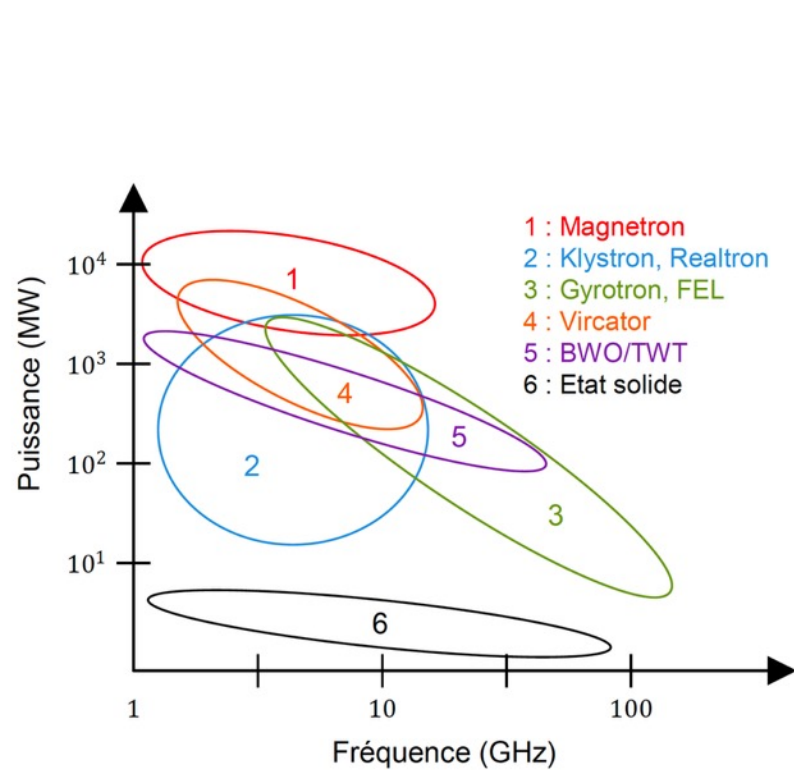
Effet	Description
Jamming	Brouillage du système
Upset	Dysfonctionnement réversible du système
Burnout	Endommagement sévère de l'électronique
Deception	Piratage



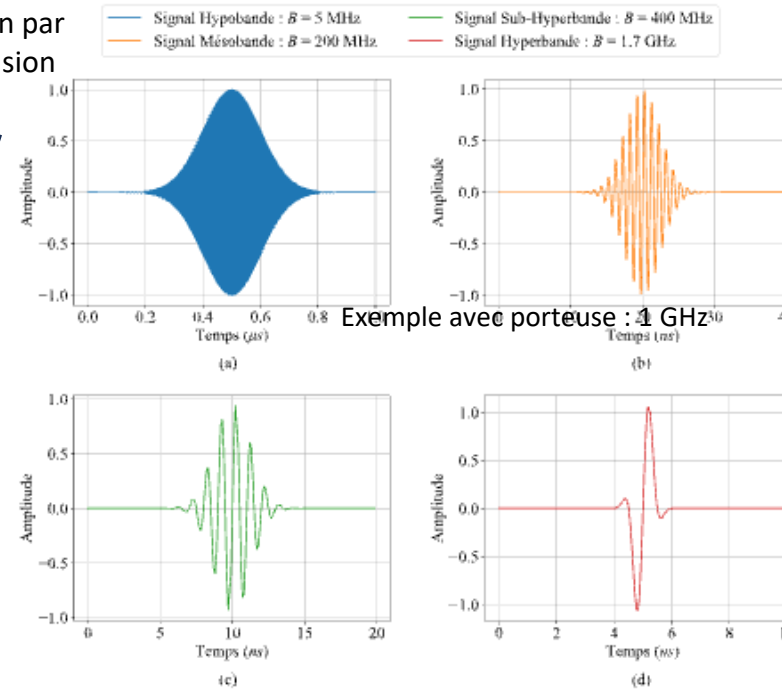
IEMI : Les sources MFP (Micro-ondes de forte puissance)



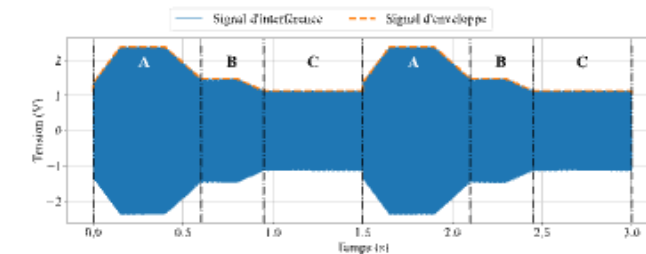
Effet	Description
Jamming	Brouillage du système
Upset	Dysfonctionnement réversible du système
Burnout	Endommagement sévère de l'électronique
Deception	Piratage



Modulation par une impulsion



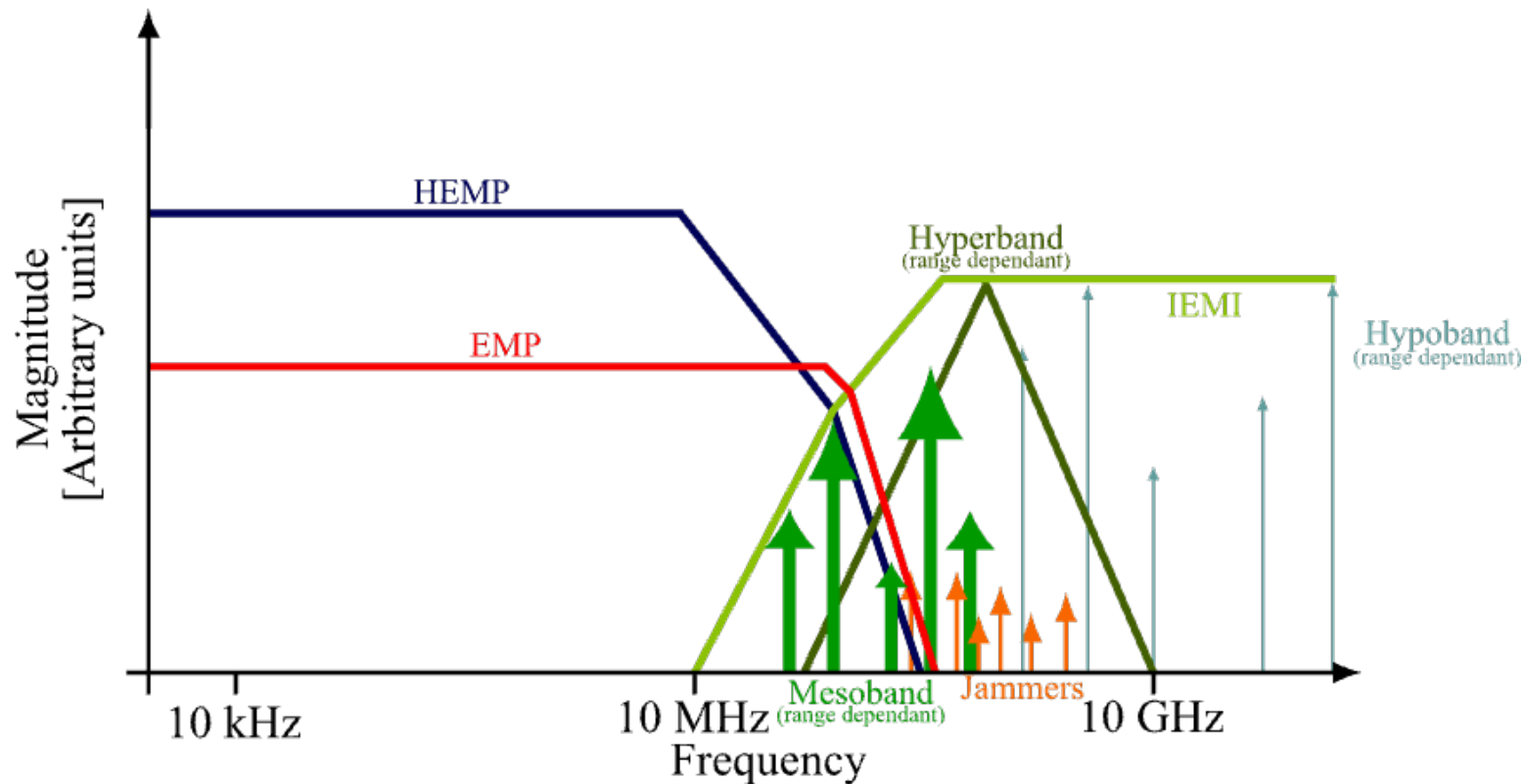
Modulation par un signal arbitraire



Clayborne D. TAYLOR and D. V. GIRI : High-power Microwave Systems and Effects. Taylor & Francis, 1994

F. Sabath and all.: Overview of Four European High-Power Microwave, IEEE Trans. On EMC, 2004

Signaux d'interférence électromagnétique



EMP/HEMP

- Sources de type impulsion
- Durée : 100 ps à qq ns

Hyperbande

- Sources de type impulsion modulée
- Durée : 100 ps à ns

Mesobande/Sub-hyperbande

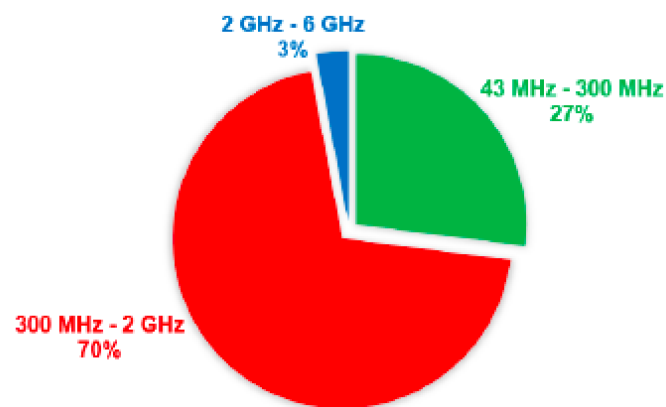
- Sources de type sinusoïde amortie modulée
- Durée : 10 ns à 100 ns

Hypobande

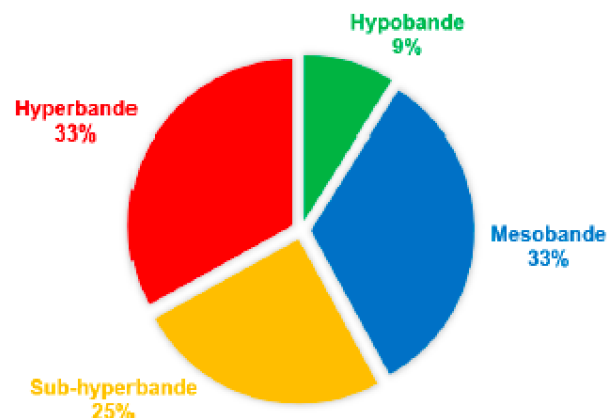
- Source de type RADAR ou PM
- Durée : 100 ns à 100 μ s

Tendance des types de signaux IEMI : 2014

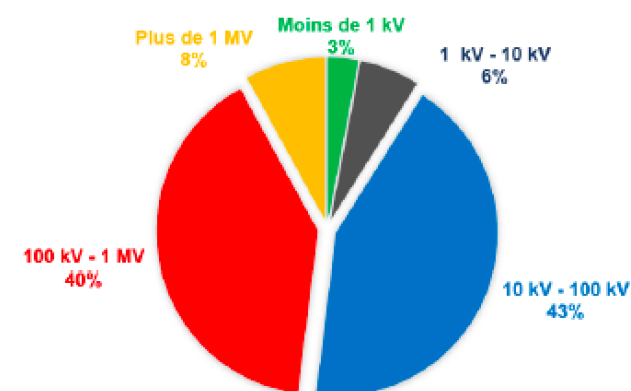
Répartition des sources IEMI suivant leur fréquence centrale



Répartition des sources IEMI suivant leur étalement spectral



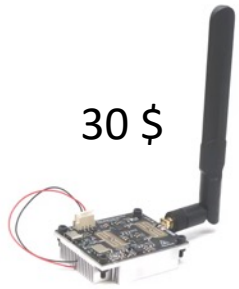
Répartition des sources IEMI suivant leur niveau d'amplitude de champ électrique émis (/m)



Signaux d'intérêts :

- 70 % : Fréquence centrale entre 300 MHz et 2 GHz
- 60 % : Signaux « Mesobande/Sub-hyperbande » (compromis entre amplitude et occupation spectrale)
- 80 % : Amplitude de champ électrique comprise entre 10 kV/m et 1 MV/m (au niveau de l'antenne d'émission)

Les armes IEMI



30 \$

Brouilleur wifi, BLE
(2 W)



1000 \$

Brouilleur
100 MHz – 6 GHz
(1 – 3 W)



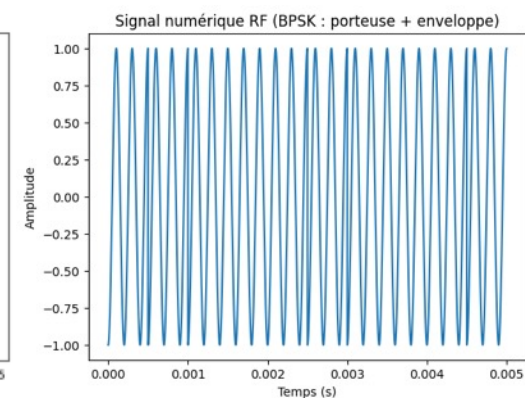
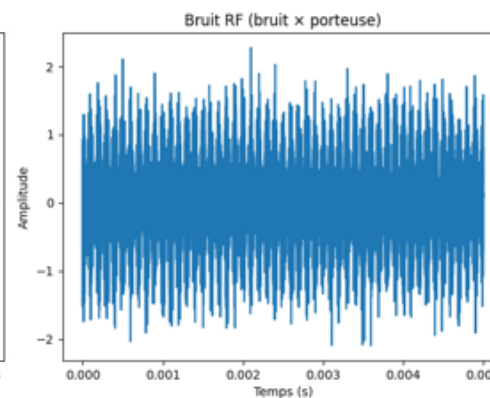
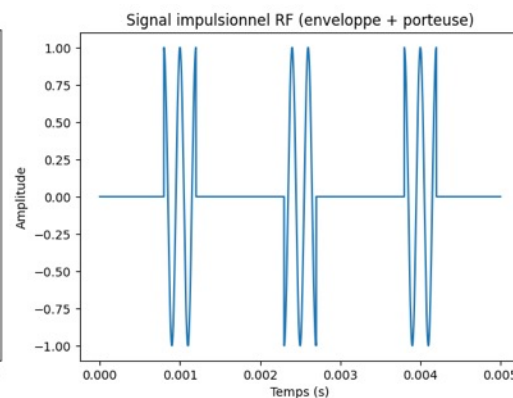
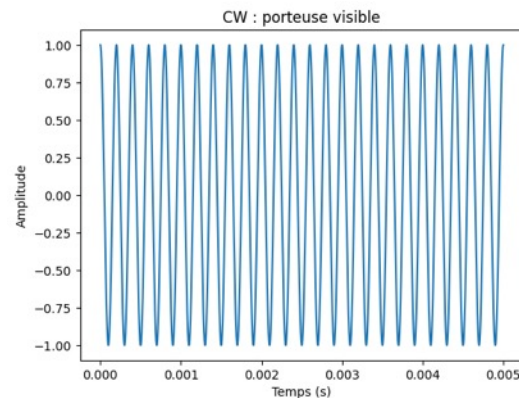
Armes à énergie dirigée (AED EM)

Brouilleur anti drone
1.5 GHz, 2.4 GHz, 5.8 GHz
(50 W)

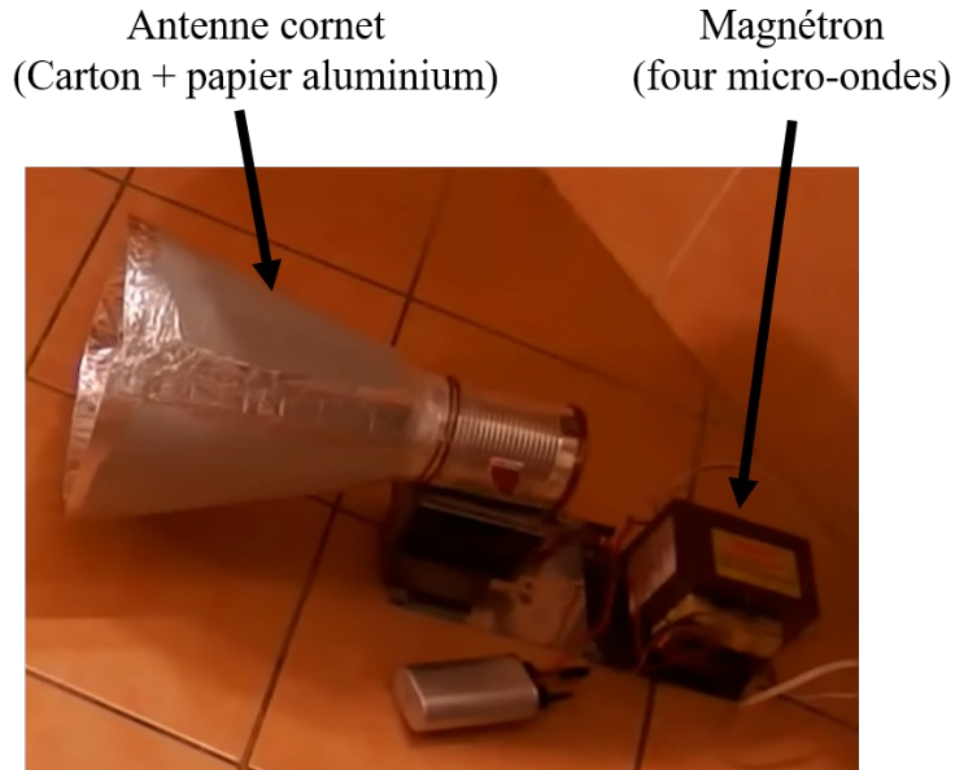


Brouillage et perturbation radar/Sys. Com.
8 – 14 GHz, 18 – 40 GHz
(estimée à 30 kW (bande 2 – 4 GHz))

Peuvent utiliser des signaux CW, sous forme de bruit, ou impulsionnel

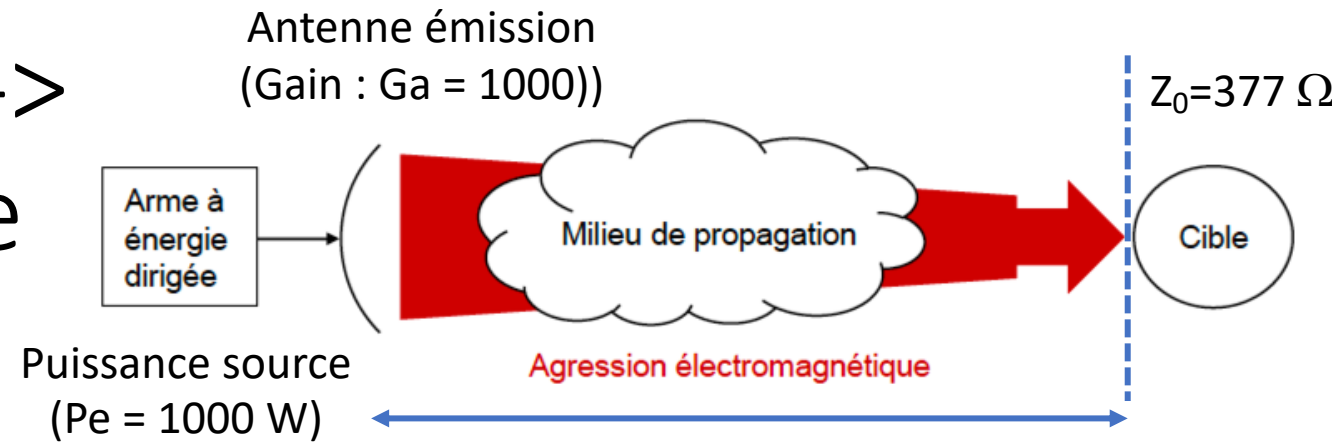


Les AED EM artisanales -> vers de la 'attaque active



Signal CW

Seuils max essais CEM
immunité rayonnée

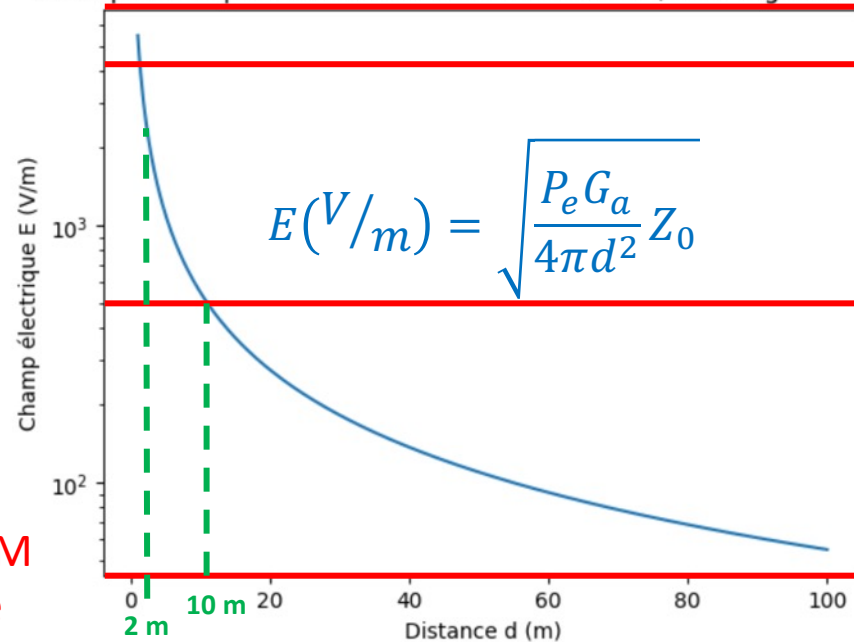


$$D \left(\text{W/m}^2 \right) = \frac{P_e G_a}{4\pi d^2}$$

d (Champ lointain)

$$D \left(\text{W/m}^2 \right) = \frac{E^2}{Z_0}$$

Champ électrique E en fonction de la distance d (axe Y logarithmique)



Armement

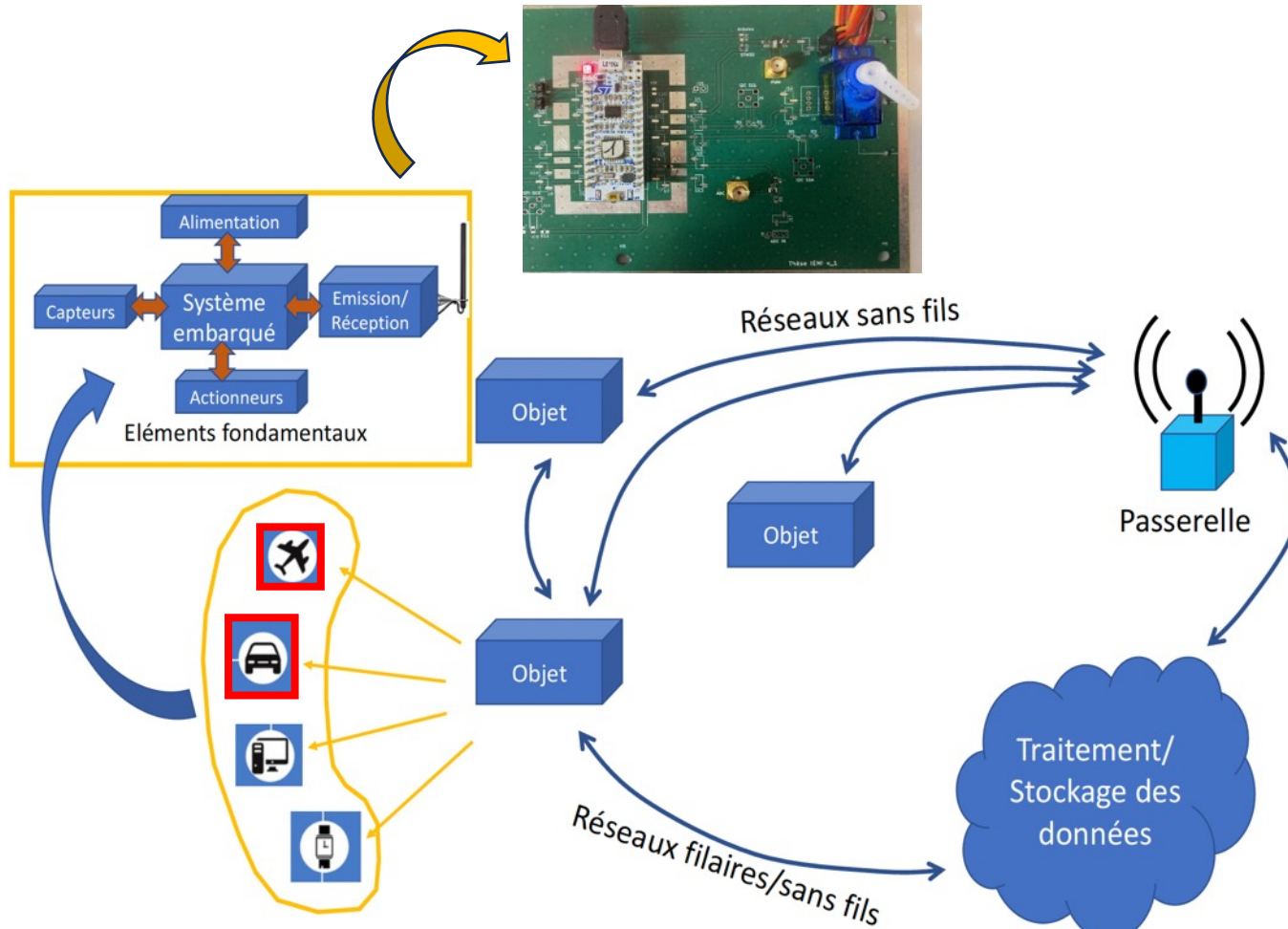
Aéronautique

Automobiles

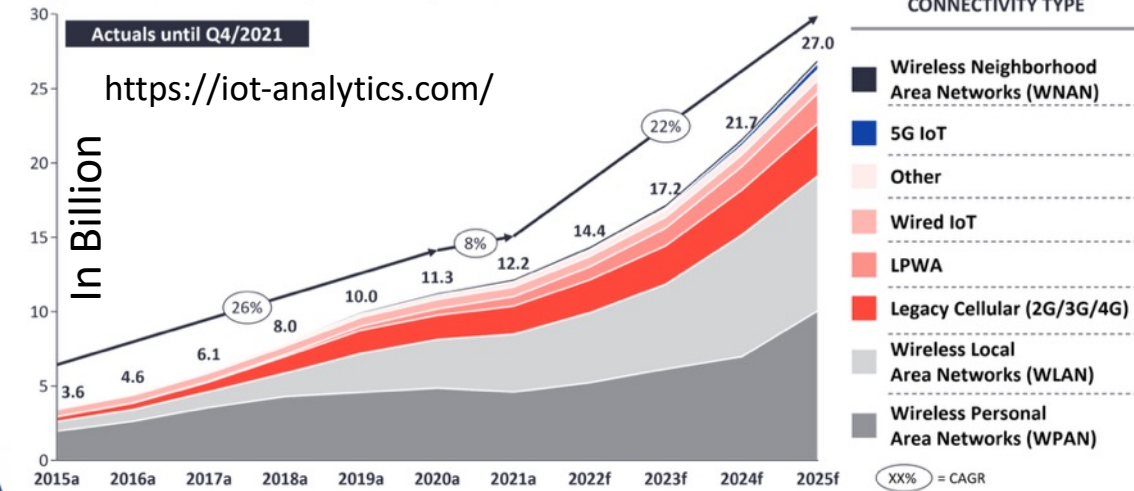
Produits médicaux
Produits grands
publiques

Robotique

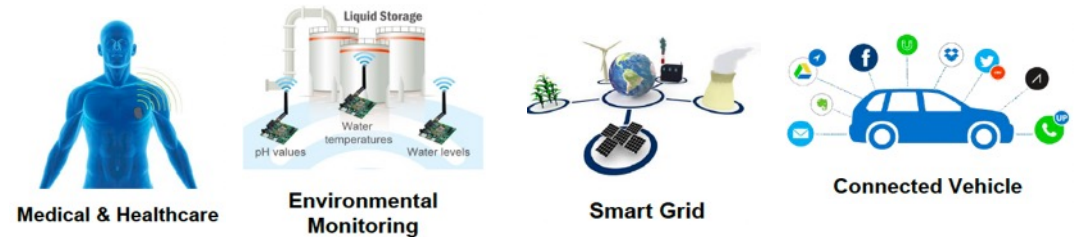
Les victimes : Les objets électroniques



Number of global active IoT Connections (installed base) in Bn



- La santé intelligente (objets connectés pour la santé).
- Les transports intelligents (véhicules autonomes).
- L'industrie 4.0 (IIoT, robotique/cobotique ...).
- L'armement (robotique/armes EM)

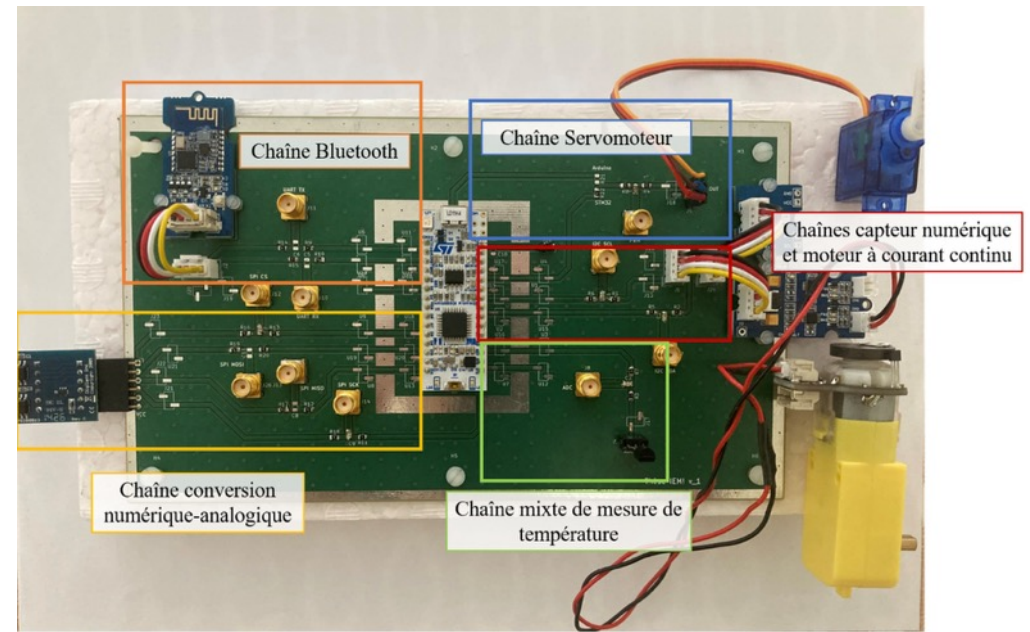


[Y. Yang, 2017] Y. Yang, et al., « A Survey on Security and Privacy Issues in Internet-of-Things », IEEE JIOT, 2017

[S. Popineau, 2021] S. Popineau, et al., « IOT perspectives in 2021 », Whitepaper GIFAS, 2021

[A. Pekar, 2021] A. Pekar, et al., « Applkcation Domain-Based Overview of IoT Network Traffic Characteristics », ACM Computing Surveys, 2021

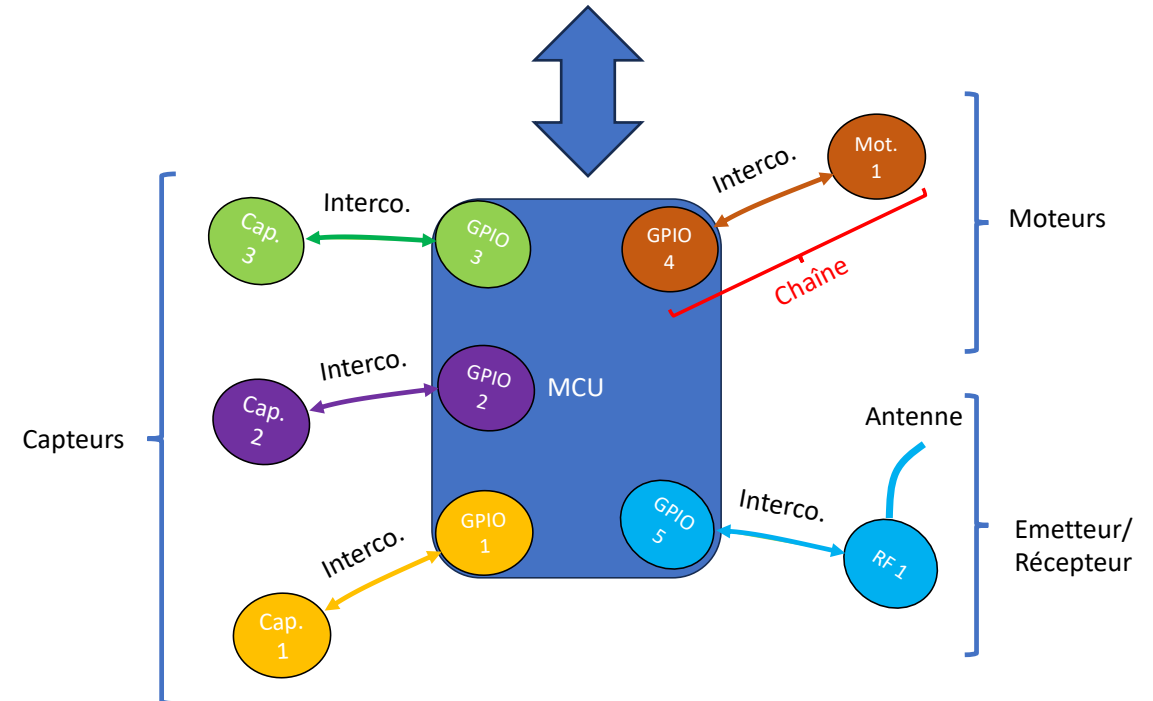
Scénario de perturbation



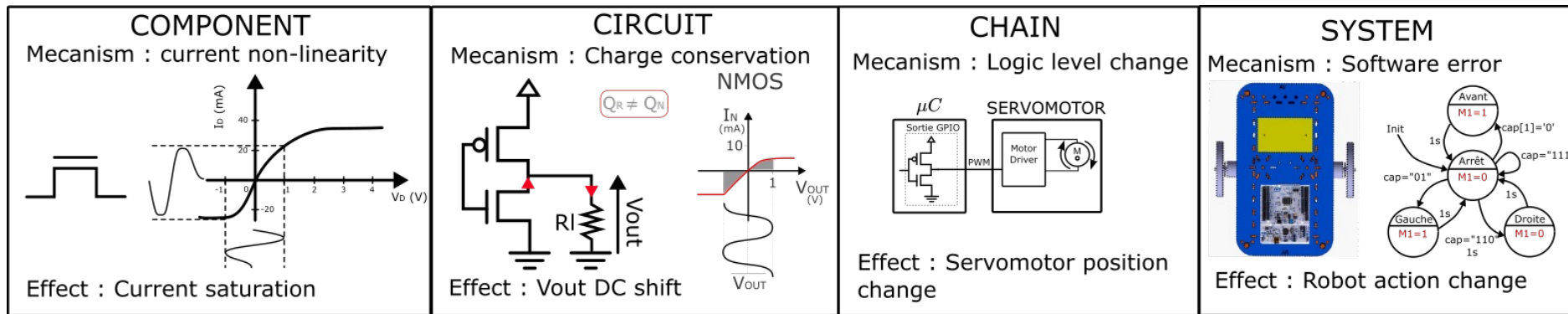
Couplages privilégiés sur le interconnexions et antennes



Comment modéliser le comportement d'un objet électronique soumis à une IEMI?



Stratégie d'étude et de modélisation : du composant au système



CAUSE & EFFECT

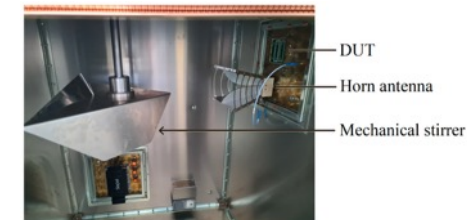
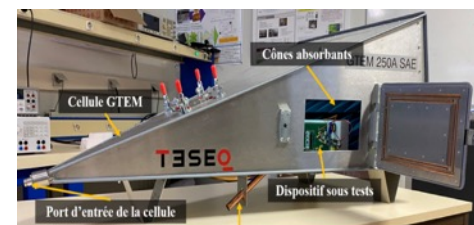
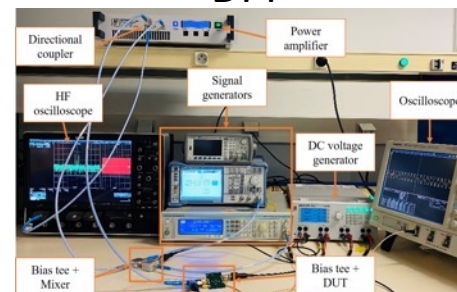
~GTEM

~CRBM

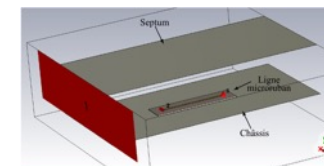
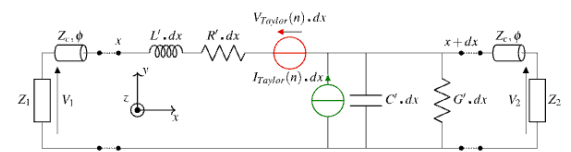
~ DPI

Cartes spécifiques

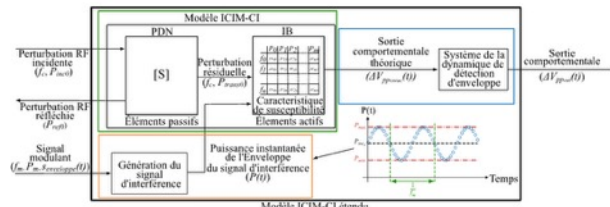
Sim. électrique



Modél. couplages



Modél. Susceptibilité



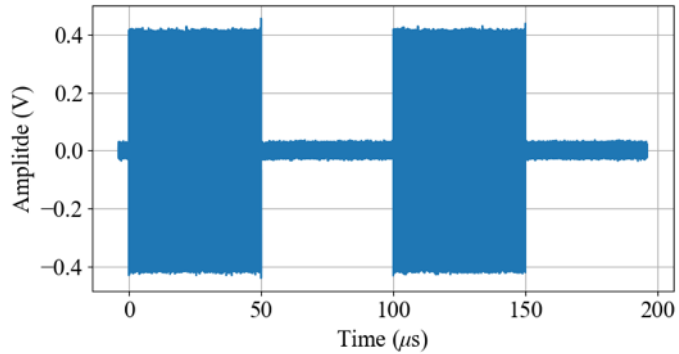
CA



Cas d'études

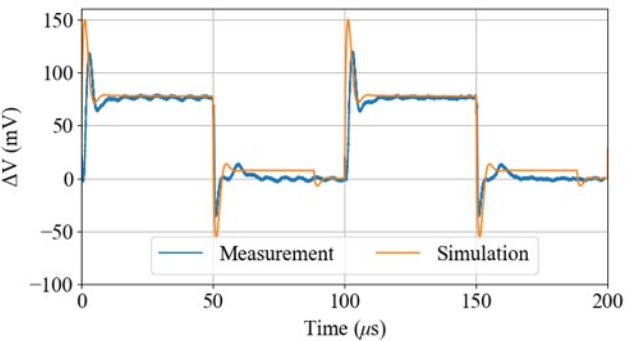
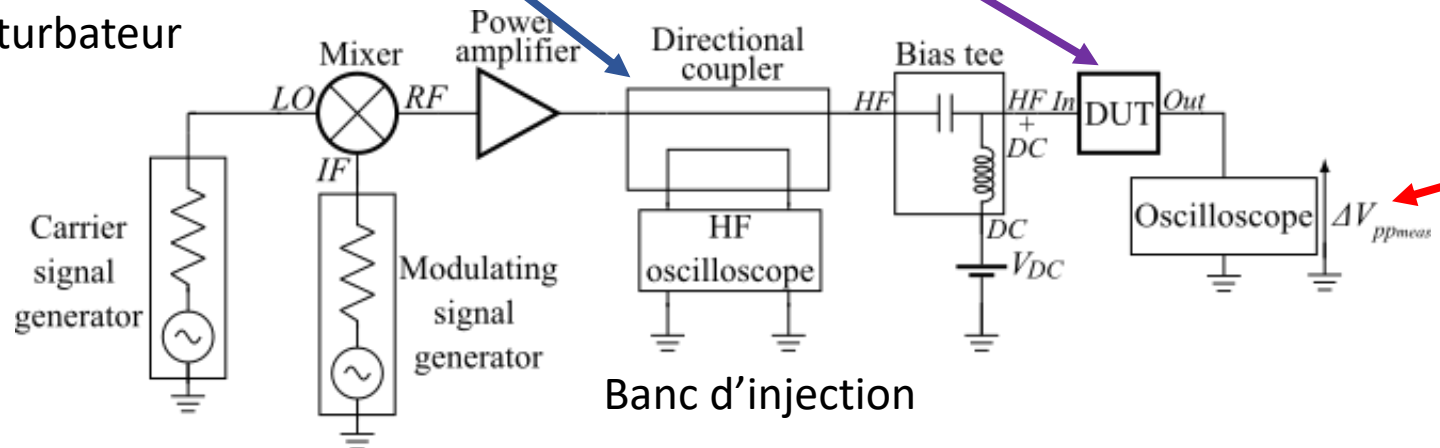
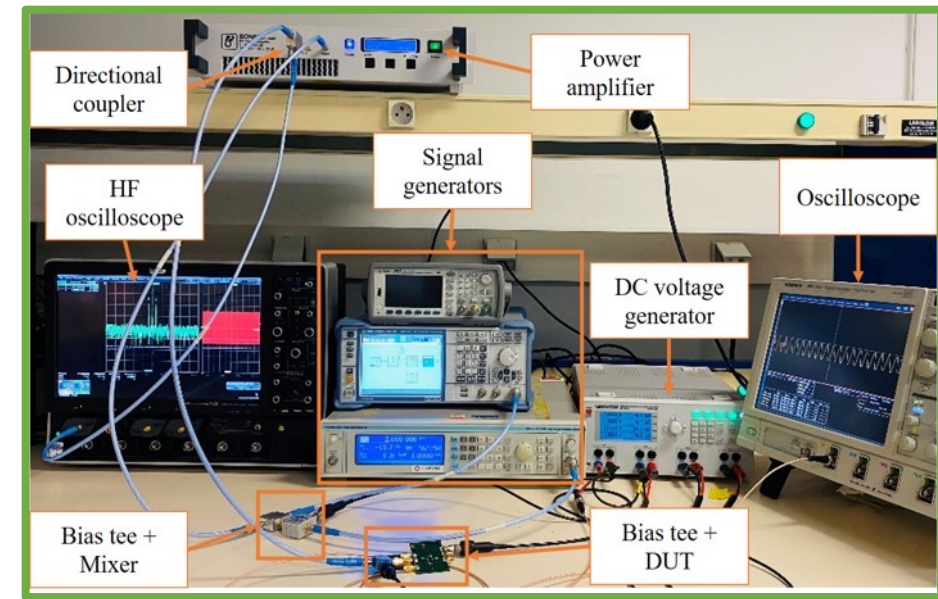
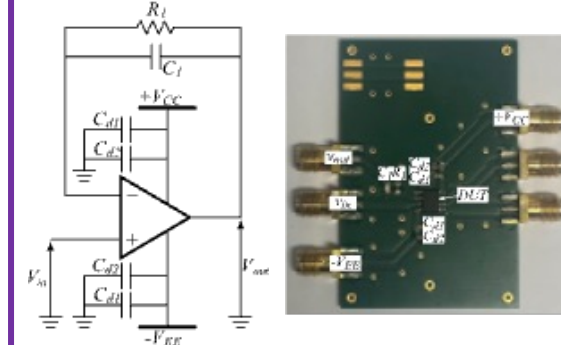
- Susceptibilité d'un AOp
- Susceptibilité GPIO UC/FPGA

Susceptibilité AOp



Signal perturbateur

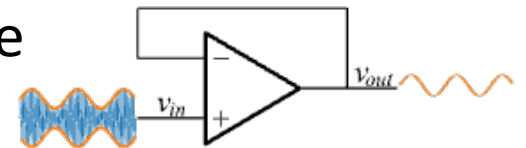
Montage amplificateur monté en suiveur



Signal mesuré

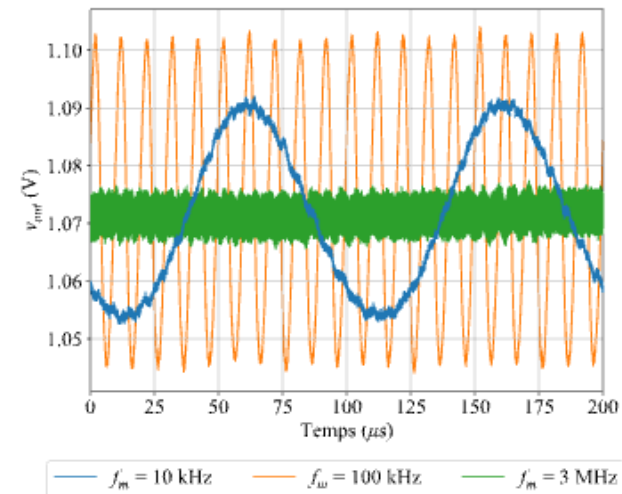
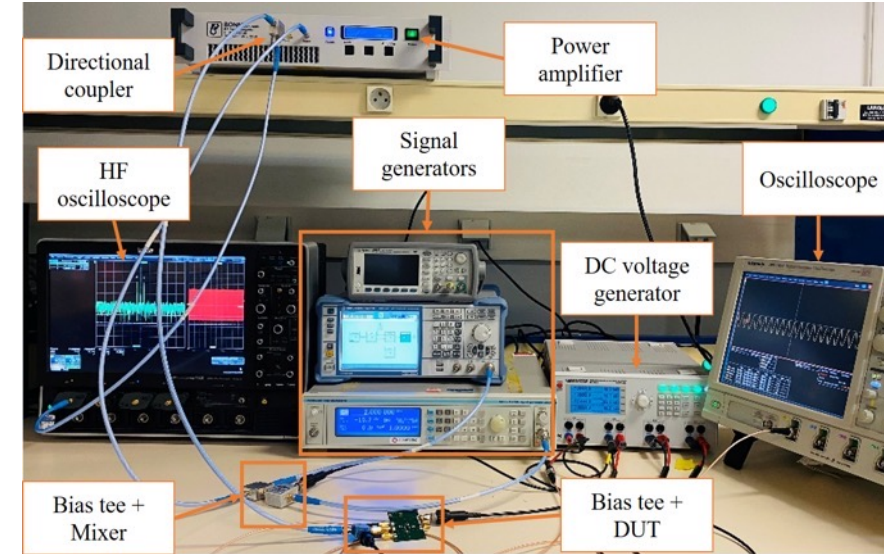
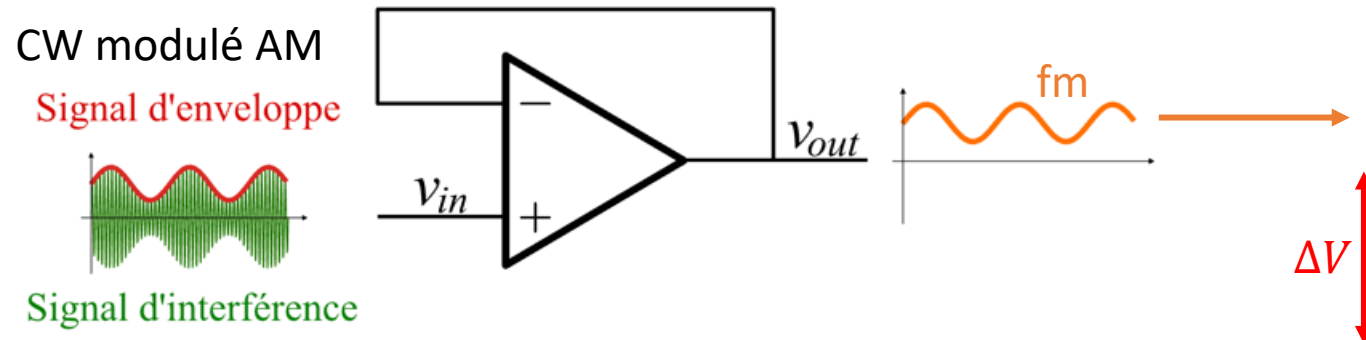
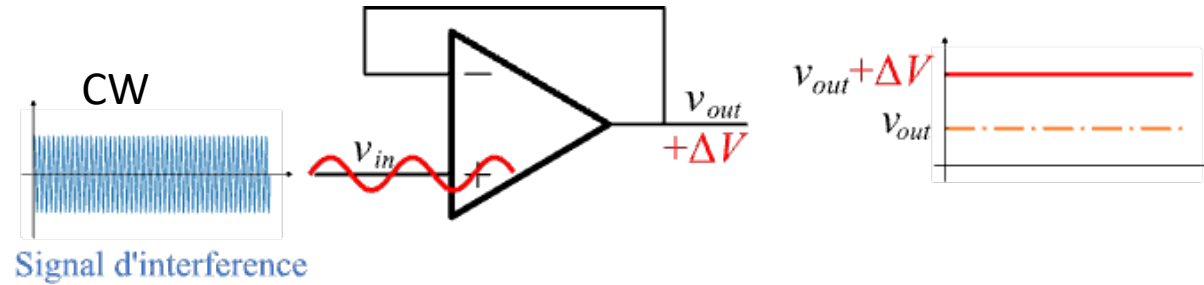
Mesure de la réponse temporelle du montage face à une impulsion modulée en amplitude injectée en conduit à son entrée

Mécanisme de détection d'enveloppe →

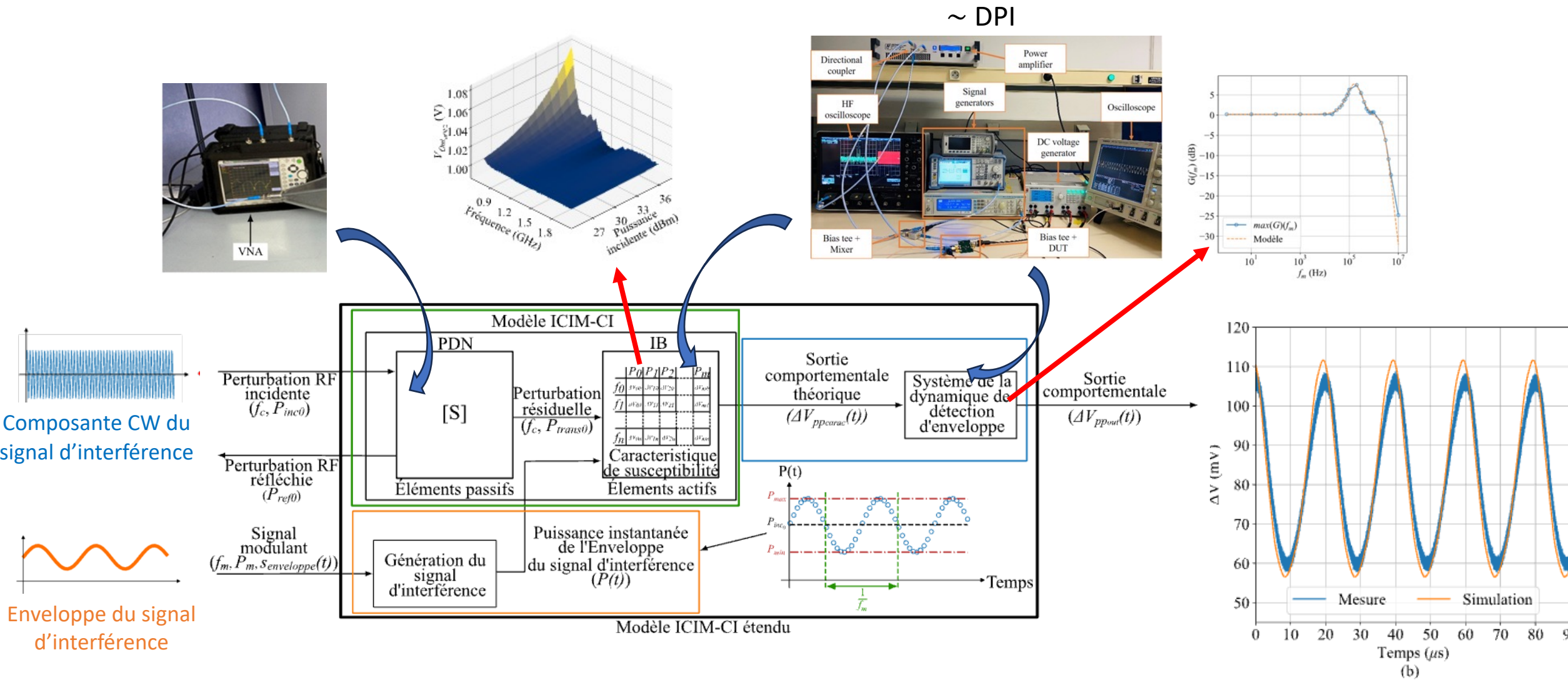


Susceptibilité AOp : phénomène physique

Comportement d'un AOp monté en suiveur face à une IEM :
Mécanisme de redressement / détection d'enveloppe

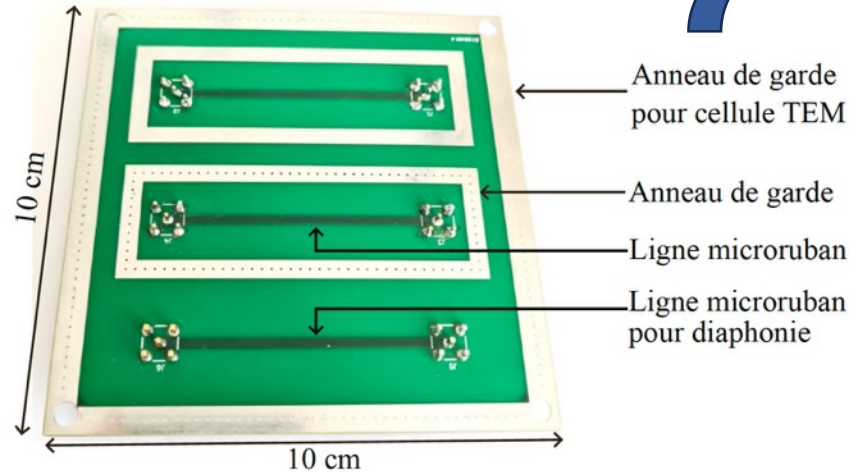


Susceptibilité AOp : Modélisation ICIM-CI

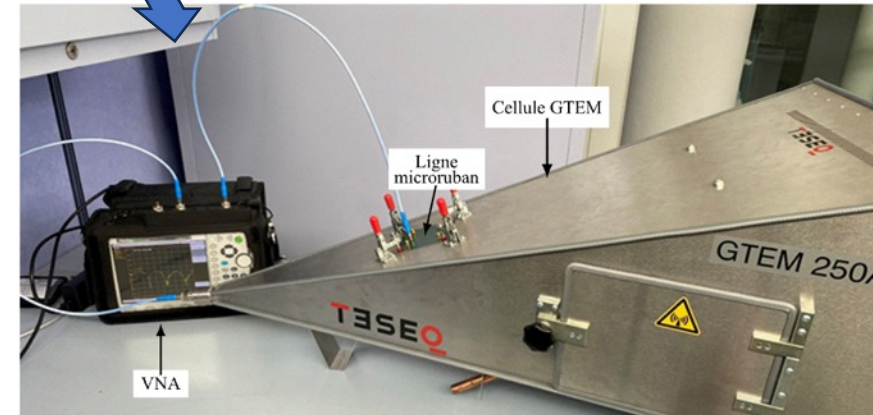


Susceptibilité Aop : Modélisation couplage

Ligne microruban : piste PCB

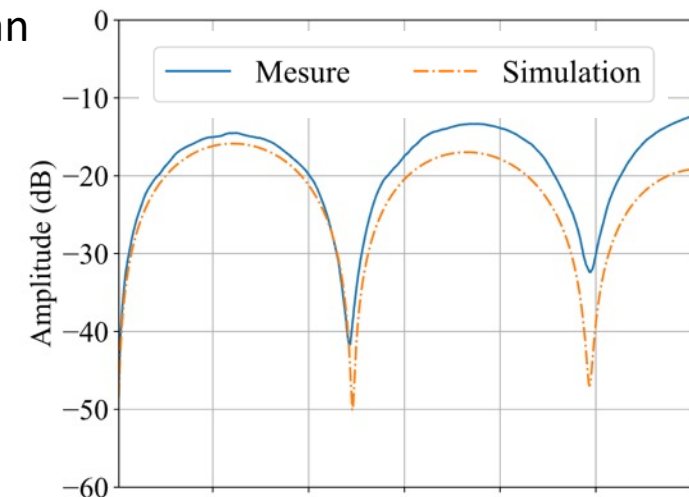
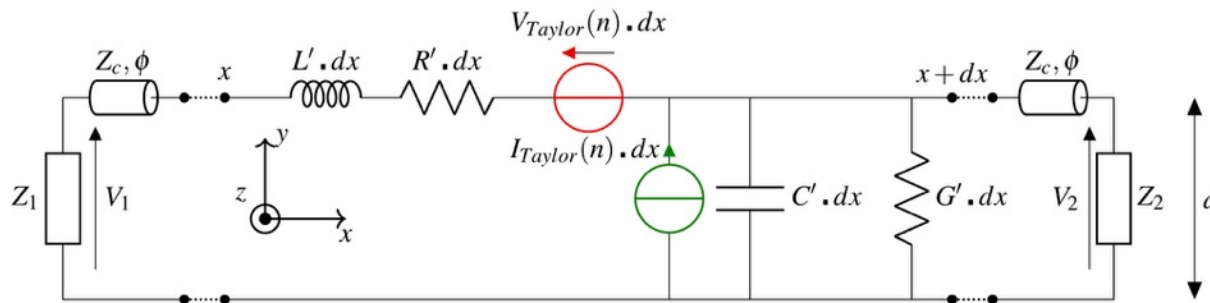


Banc en cellule GTEM permettant de caractérisé le couplage



Couplage entre l'onde injectée dans la cellule et la ligne microruban

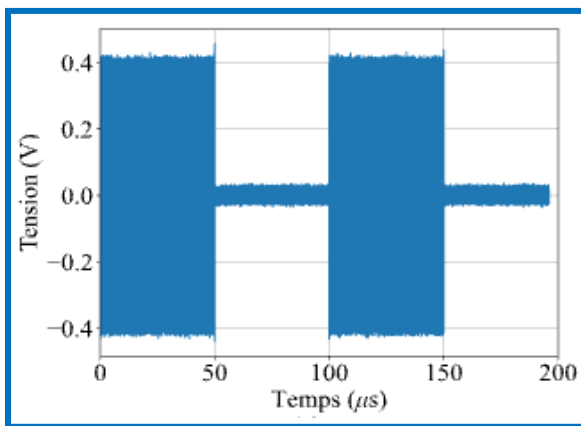
Modèle de Taylor du couplage



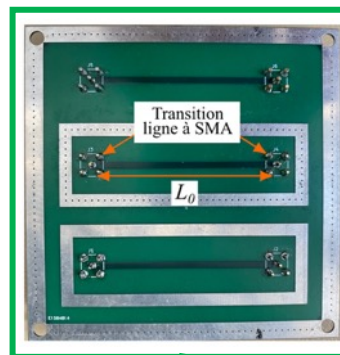
Susceptibilité AOp : Comparaison mesure / simulation

Signal mesuré

Signal perturbateur

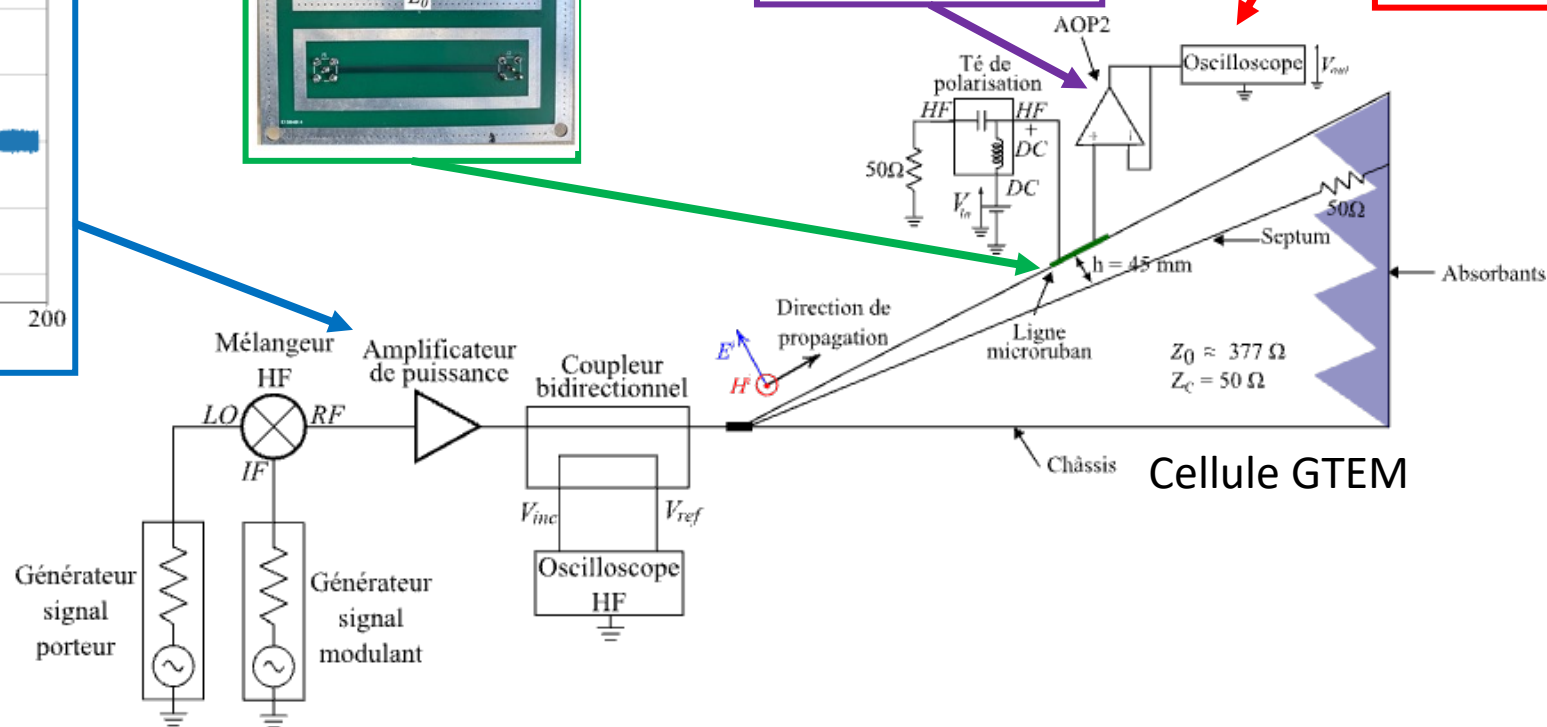
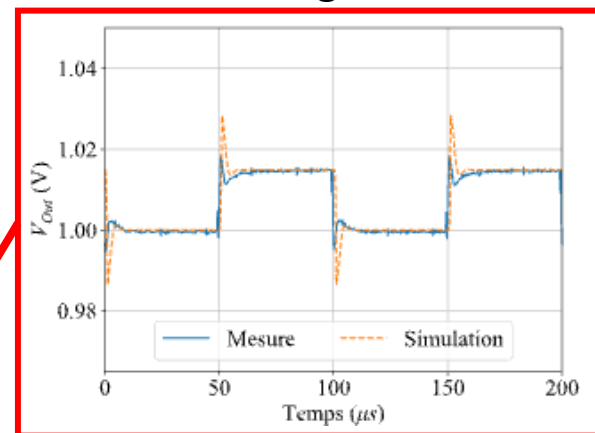
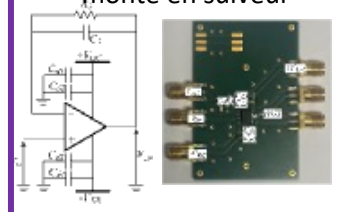


Ligne microruban



Circuit sous test

Montage amplificateur monté en suiveur



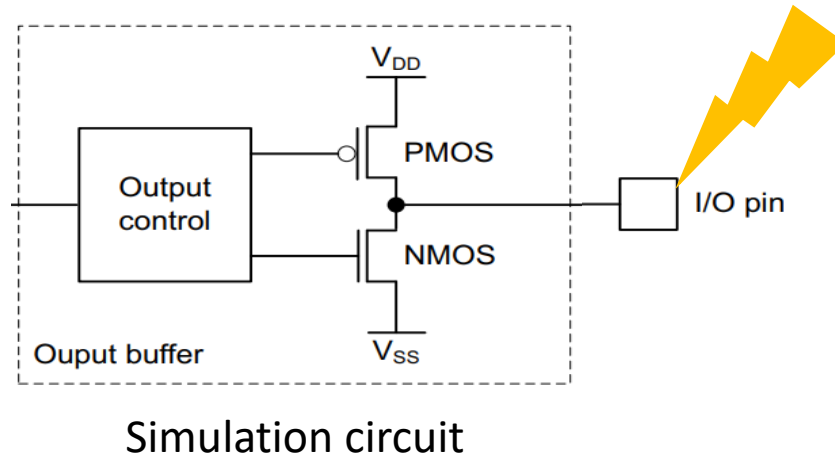
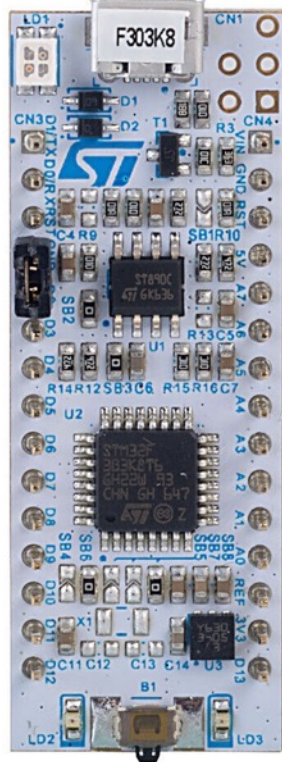
Cellule GTEM

Merci pour votre attention

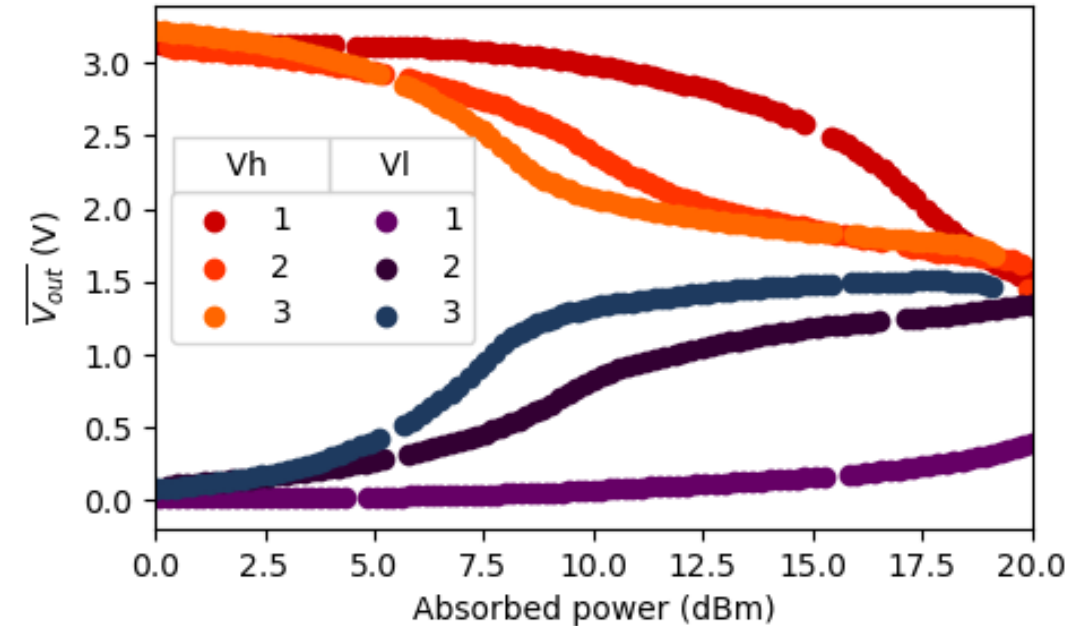
DPI – GPIO

Injection sur la sortie numérique de trois ICs

Sortie d'un GPIO = Sortie inverseur CMOS

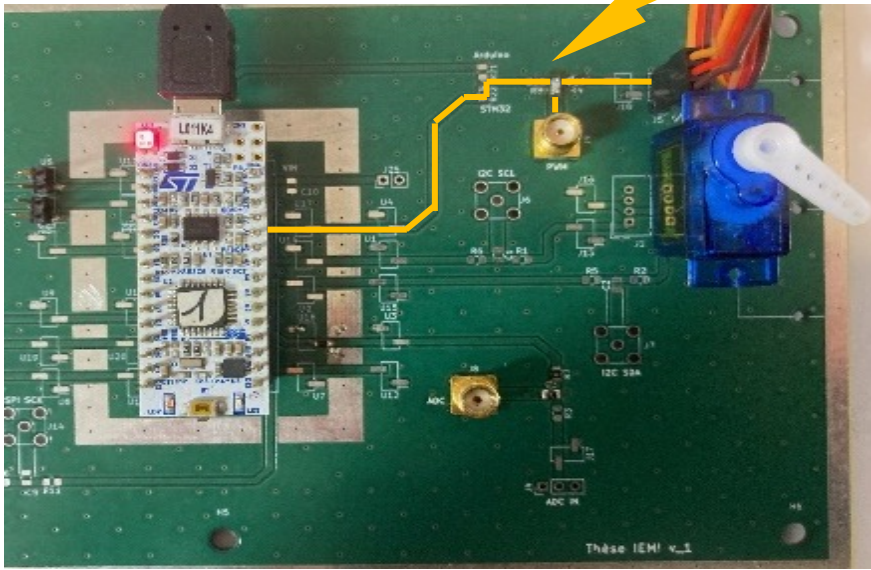


1. Arduino 2. STM32 3. FPGA

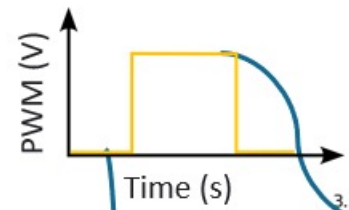


- Susceptibilité sortie numérique d'un IC = susceptibilité sortie inverseur CMOS
- Mécanisme : Redressement de la tension de la tension niveau haut et bas

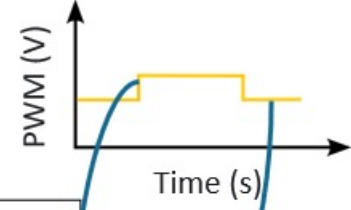
DPI – Servo



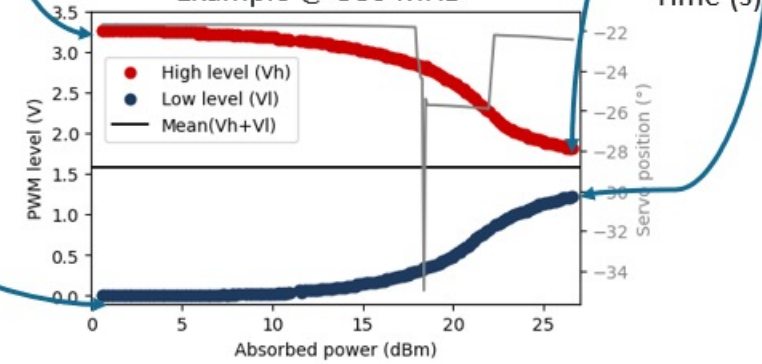
@ low power injection



@ high power injection

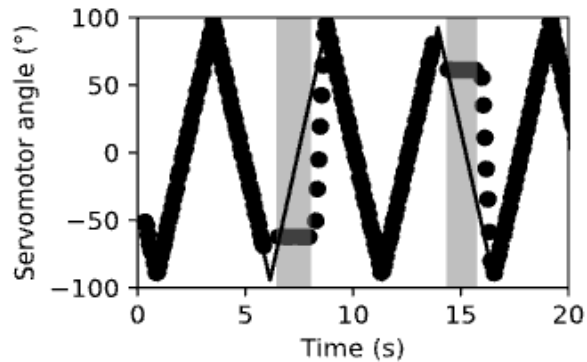


Example @ 380 MHz



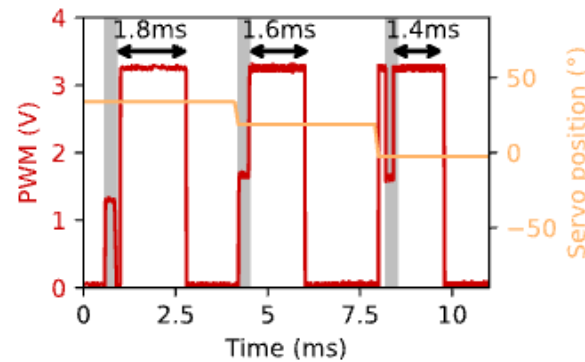
Différentes susceptibilités fonctionnelles en fonction de l'utilisation :

Mode scan



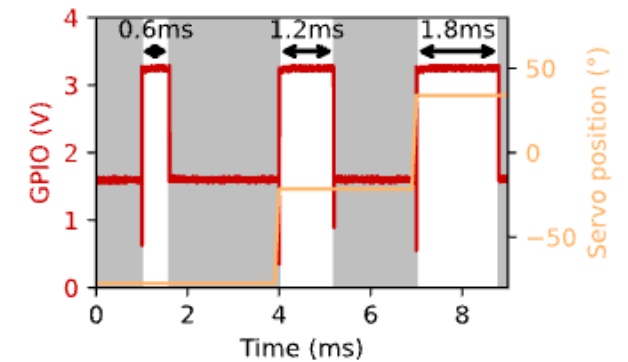
Stop scan

Mode statique



Contrôle position

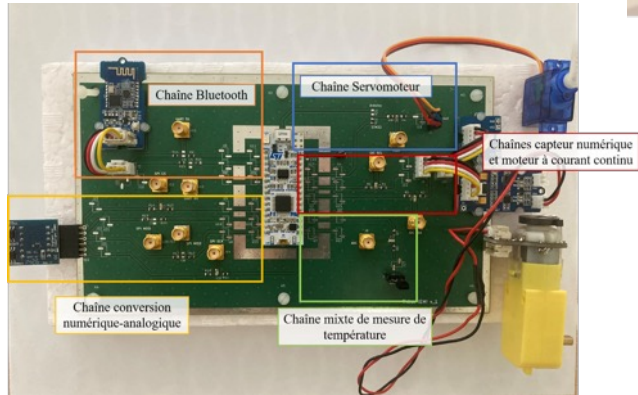
Mode arrêt



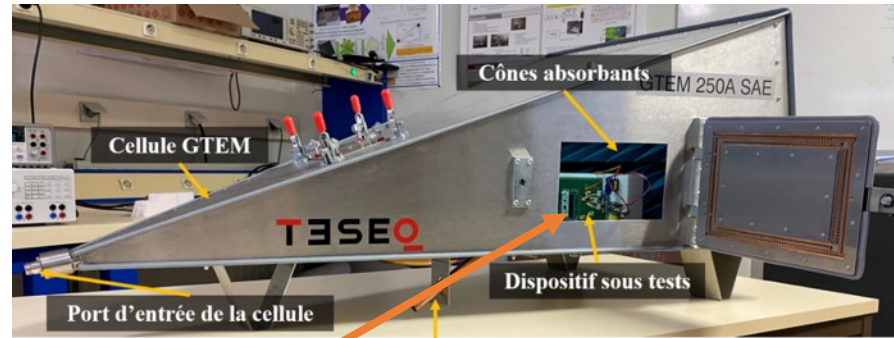
Contrôle position

GTEM/CRBM – Carte IoT

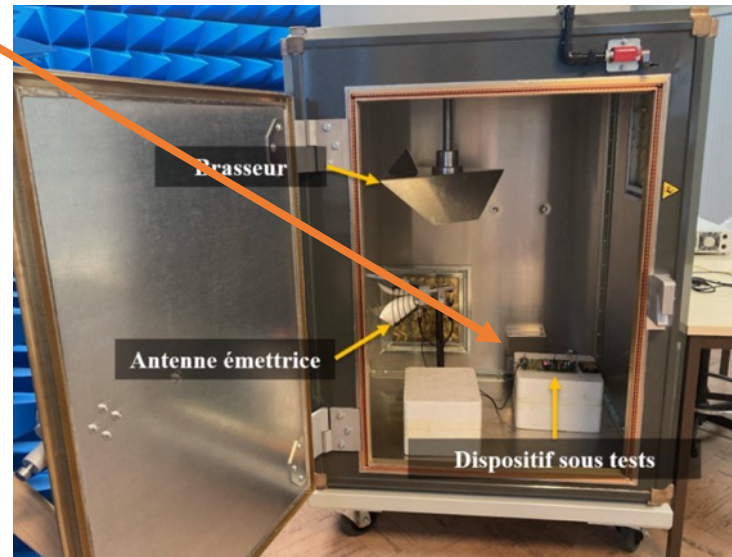
THALES



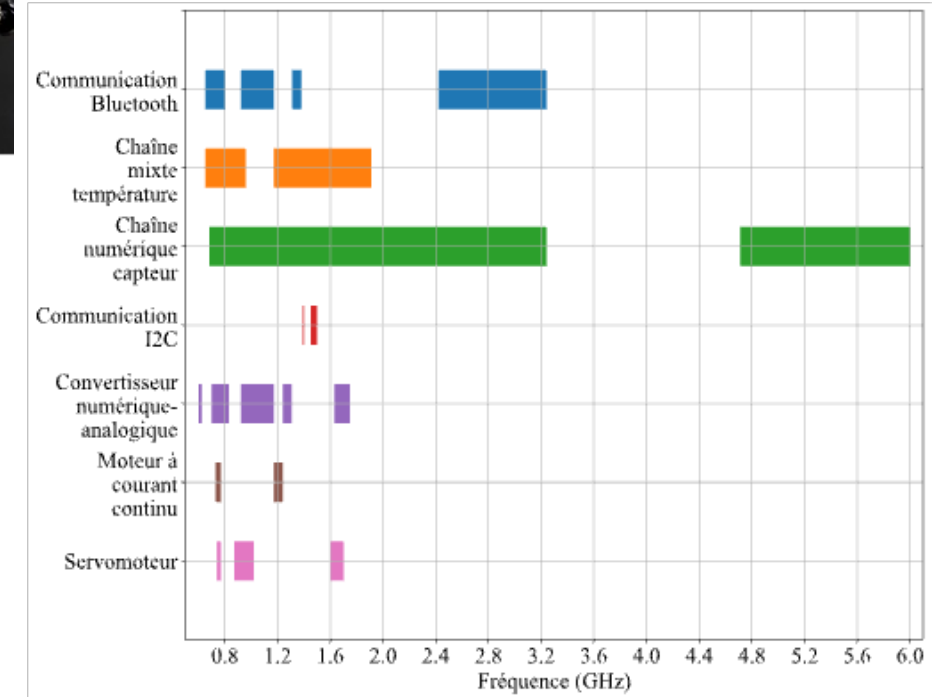
Objet IoT composé de fonctions électroniques



Cellule GTEM



Chambre réverbérante à brassage de modes



Recensement des
susceptibilités fonctionnelles
de l'objet IoT