M2 SeCReTS

Politiques de sécurités et aspects juridiques

Compatibilité Électromagnétique

&

Sécurité des Systèmes d'Information, entre compromission et agression

E. DUPONCHELLE

19 janvier 2016

LE LSF EN QUELQUES MOTS…

Laboratoire sécurité des technologies sans fil

- Expertise des menaces liées à l'emploi des nouvelles technologies de communication et traitement de l'information:
  - contrôle d'accès sans contact, CPL, WIFI, Bluetooth, GSM, 3G, LTE, PMR etc…
- Expertise liée aux menaces d'origines électromagnétiques
- Évaluation de produits au regard des signaux compromettants
- Suivi et mise à jour de la réglementation
- Réalisation de campagnes de mesures sur site
- Travaux de recherche menés conjointement avec des laboratoires universitaires et étatiques, français et étrangers

SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça ??
4. Conclusion

1. CONTEXTE

Les menaces acoustiques et visuelles ne seront pas traitées dans notre intervention.

Cependant il est indispensable de les traiter avant de se préoccuper des menaces électromagnétiques.

1. CONTEXTE

Sécurité des Systèmes d'Information (SSI)

- Confidentialité ;
- Intégrité ;
- Disponibilité…

1. CONTEXTE

Compatibilité électromagnétique (CEM)

- Émissivité d'une électronique – bruits EM générés par un circuit électronique ;
- Susceptibilité d'une électronique – sensibilité d'une électronique à l'environnement électromagnétique ;
- Marquage CE ➔ réduire les risques de pollutions EM et la défaillance d'une électronique.

1. CONTEXTE

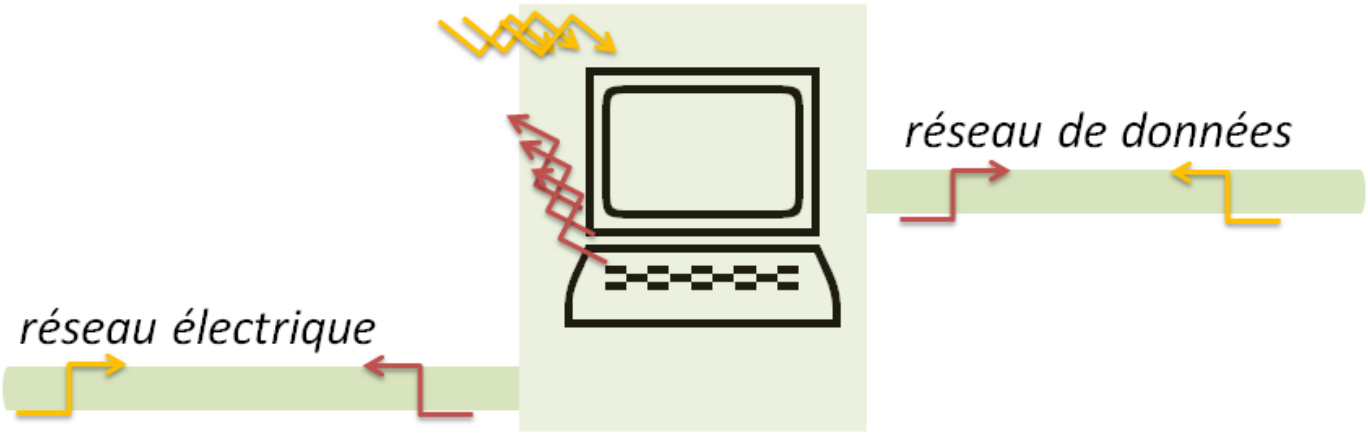
Risques de la CEM pour la SSI

- Risques de compromission des données: corrélation potentielle entre le bruit EM généré par un SI et les informations traitées par celui-ci;

- Risques pour l'intégrité et la disponibilité des réseaux et des données: susceptibilité d'un SI soumis à des champs EM de forte puissance.

1. CONTEXTE

Risques de la CEM pour la SSI

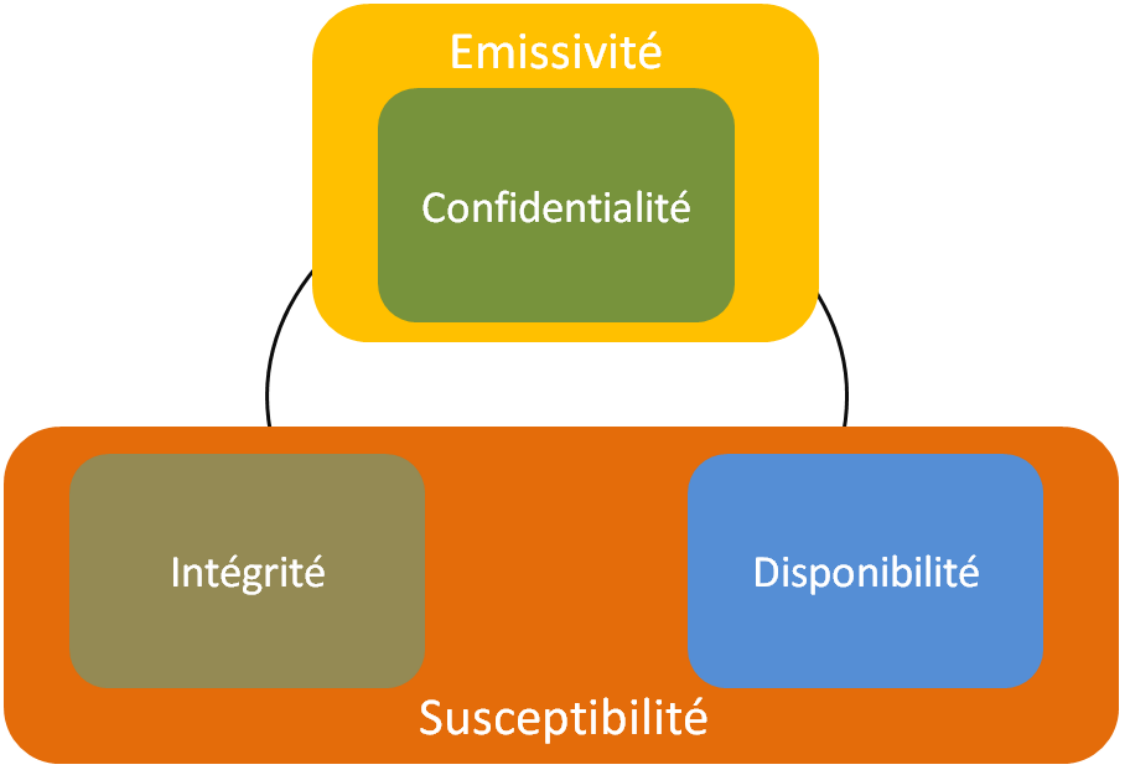


<u>émissivité, risque pour la confidentialité:</u>
signaux électromagnétiques compromettants

<u>susceptibilité, risque pour l'intégrité et la disponibilité:</u>
interférences électromagnétiques intentionnelles

1. CONTEXTE

Risques de la CEM pour la SSI

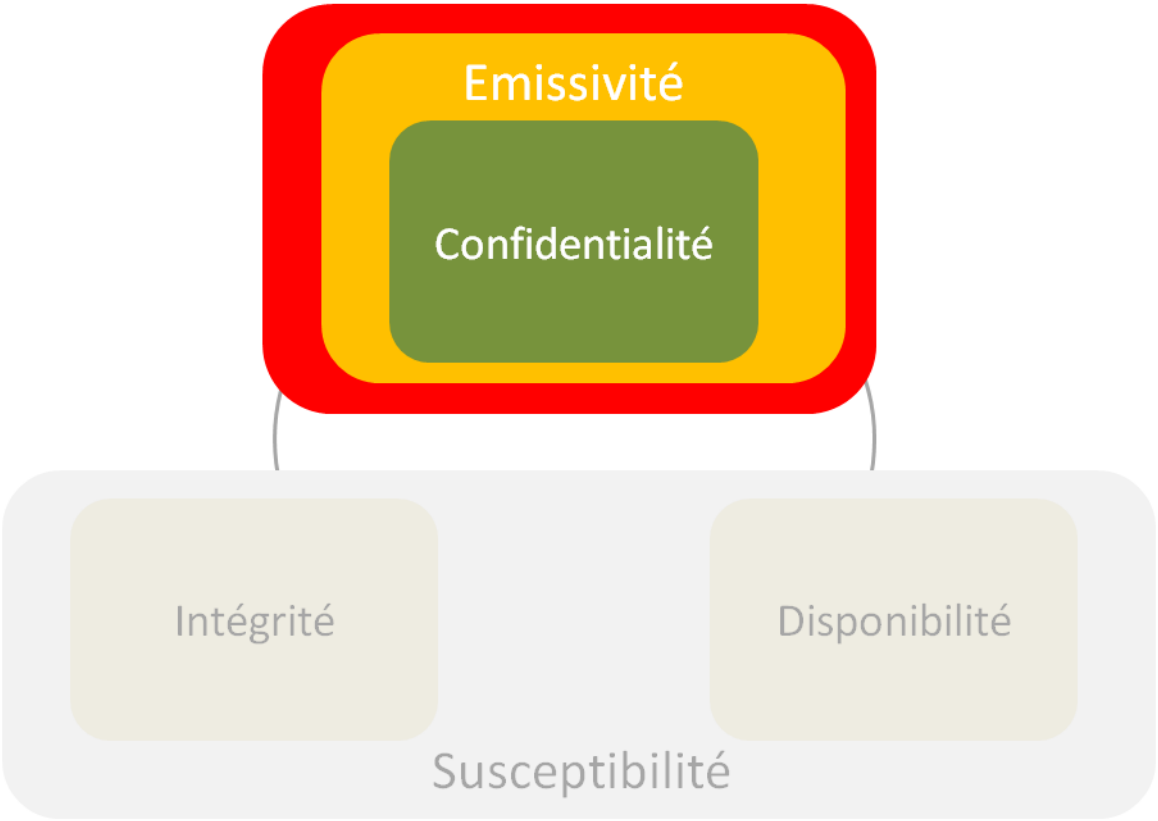


SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. **Signaux compromettants**
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux compromettants



2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux compromettants

2 grandes familles de signaux compromettants

Les signaux parasites compromettants

quelques **nW** => quelques **m**

Les signaux intentionnels compromettants

quelques **mW** => quelques **km**

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux parasites compromettants

Quelques publications…

Interception de signaux vidéos d'écrans CRT
[Van Ecke, 1985]

Interception de signaux vidéos d'écrans CRT et écrans LCD
[Kuhn, 2003]

Interception de signaux claviers - PS2
[Vuagnoux et al., 2010]

Interception de signaux type CPL
[Diquelou et al., 2010]

Interception de signaux vidéos
[Du et al., 2013]

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux parasites compromettants

"Quand vos machines diffusent vos données à votre insu"

Magazine MISC n°44

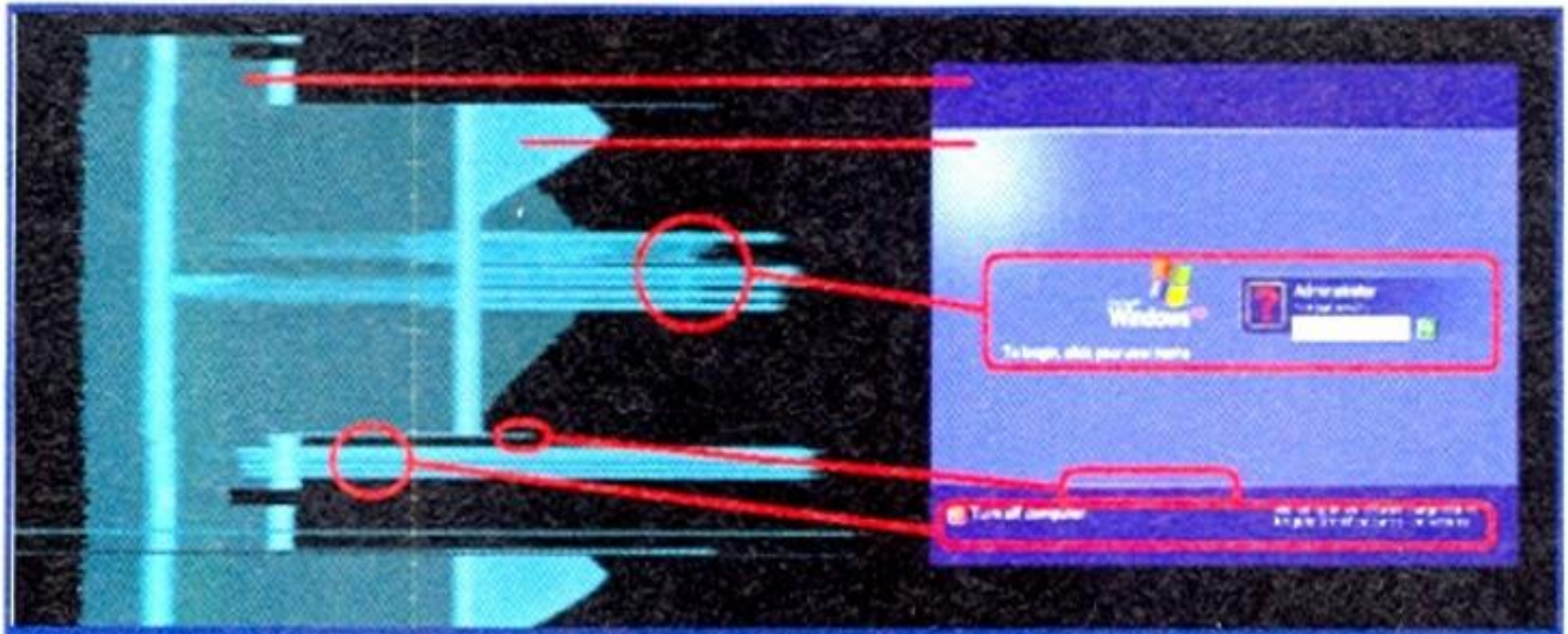
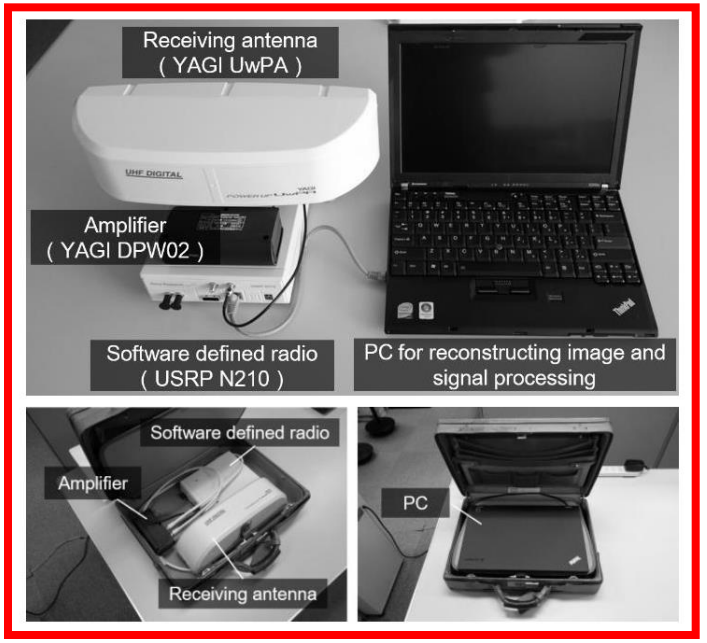


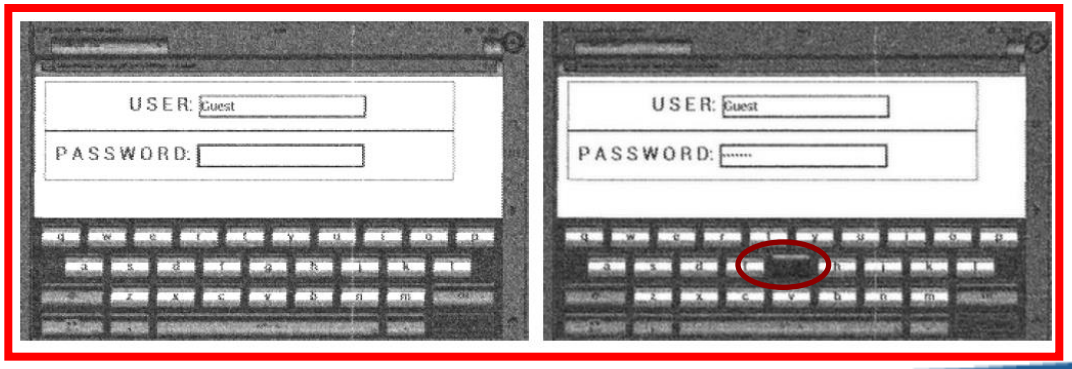
Fig. 3 : Deux trames et leur décodage

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux parasites compromettants

Publications récentes…





Y. Hayashi et al., IEEE, 2014

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux compromettants

2 grandes familles de signaux compromettants

Les signaux parasites compromettants

quelques **nW** => quelques **m**

Les signaux intentionnels compromettants

quelques **mW** => quelques **km**

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux intentionnels compromettants

Dans ces cas, tous les paramètres sont normalisés :

En conséquence, la confidentialité **ne repose plus que**

sur la robustesse de l'algorithme implémenté par le constructeur…

quand il y en a un…

… et qu'il est "mis en œuvre" par l'utilisateur.

Ajouter une surcouche de sécurité : IPsec, TLS, etc….

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux intentionnels compromettants

Utilisation d'équipements sans fil

- **Fréquence de fonctionnement 27 MHz**
- Très bonne propagation en conduction
- unidirectionnel

Source Internet

Utilisation d'équipements sans fil

- Fréquence de fonctionnement 2,4 GHz
- Très bonne propagation en vue directe
- Généralement bidirectionnel

Source Internet

- Bluetooth – grande surface d'attaque
- Le nano récepteur présente une double fonctionnalité : Clavier et Souris
  - Possibilité d'injecter du code sur le PC victime
  - Reconfiguration du firmware envisageable
  - Exfiltration de données envisageable par cette porte dérobée

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

a. Signaux intentionnels compromettants

Utilisation d'équipements sans fil

- Équipement RF ou infrarouge
- Pas de crypto

Source Internet

- Infrarouge – attention aux fenêtres

3 notions de distances doivent être considérées

Exemple du WIFI

- Distance de fonctionnement « contractuelle » ***- 100m***
- Distance de fonctionnement « optimisée » ***- 500m***

Source Internet

- Distance vue de l'attaquant

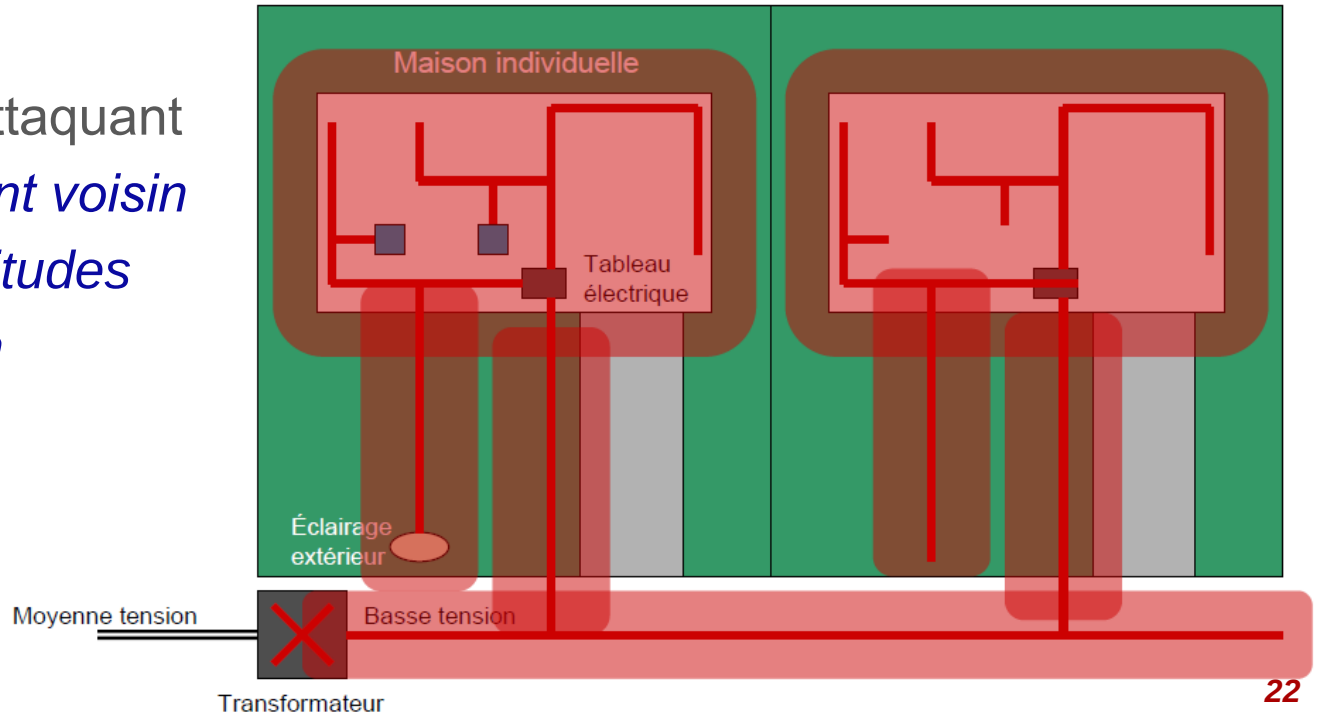
(avec des moyens rudimentaires)

Bien supérieure à 10 km

3 notions de distances doivent être considérées

Exemple du CPL

- Distance de fonctionnement « contractuelle » - *l'intérieur du pavillon*
- Distance de fonctionnement « optimisée »
  - *peut-être dans le lieu commun après le compteur*
- Distance vue de l'attaquant
  depuis l'appartement voisin
  ou depuis des servitudes
  autour d'un pavillon



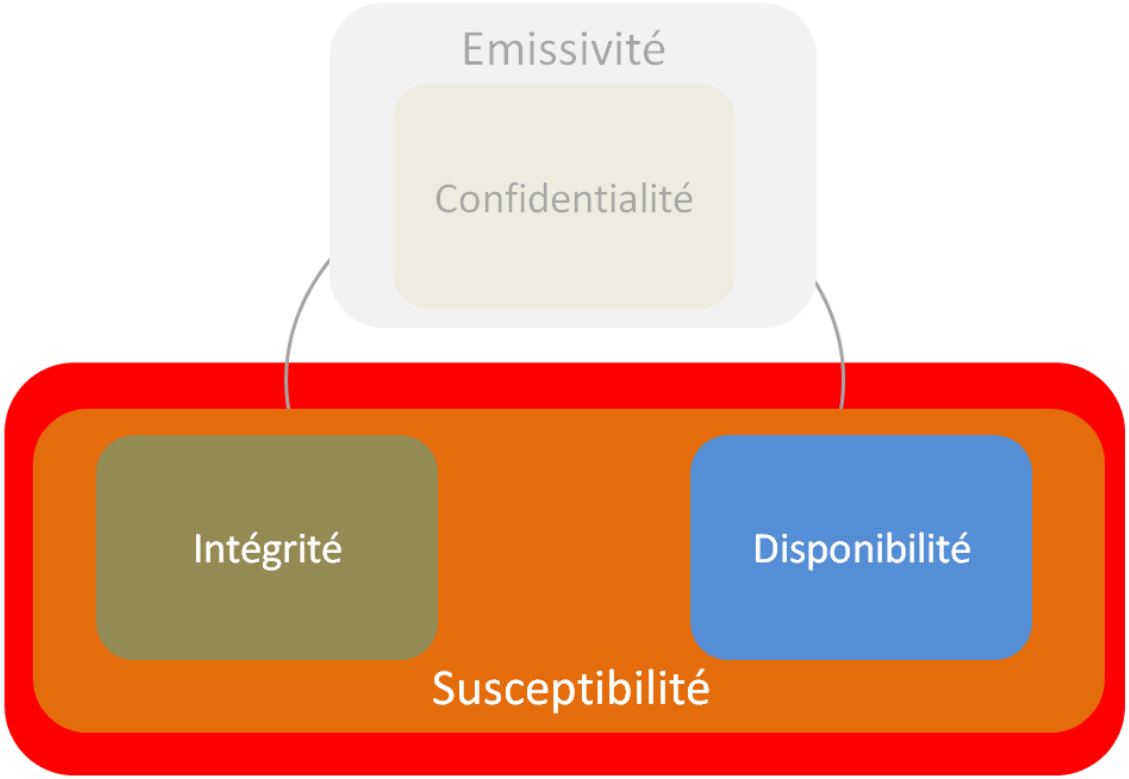
Source Internet

SOMMAIRE

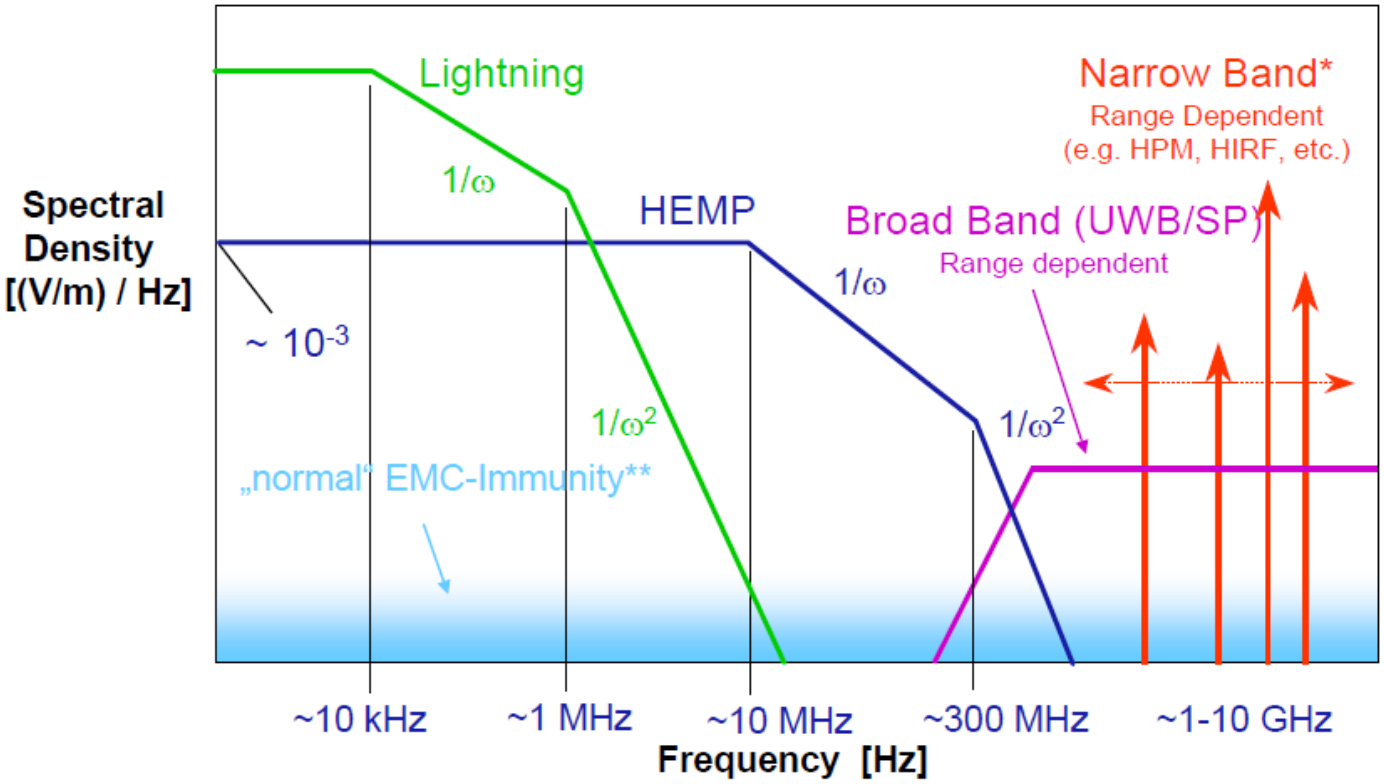
1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. **Agressions électromagnétiques intentionnelles**
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

b. Agression électromagnétique intentionnelle



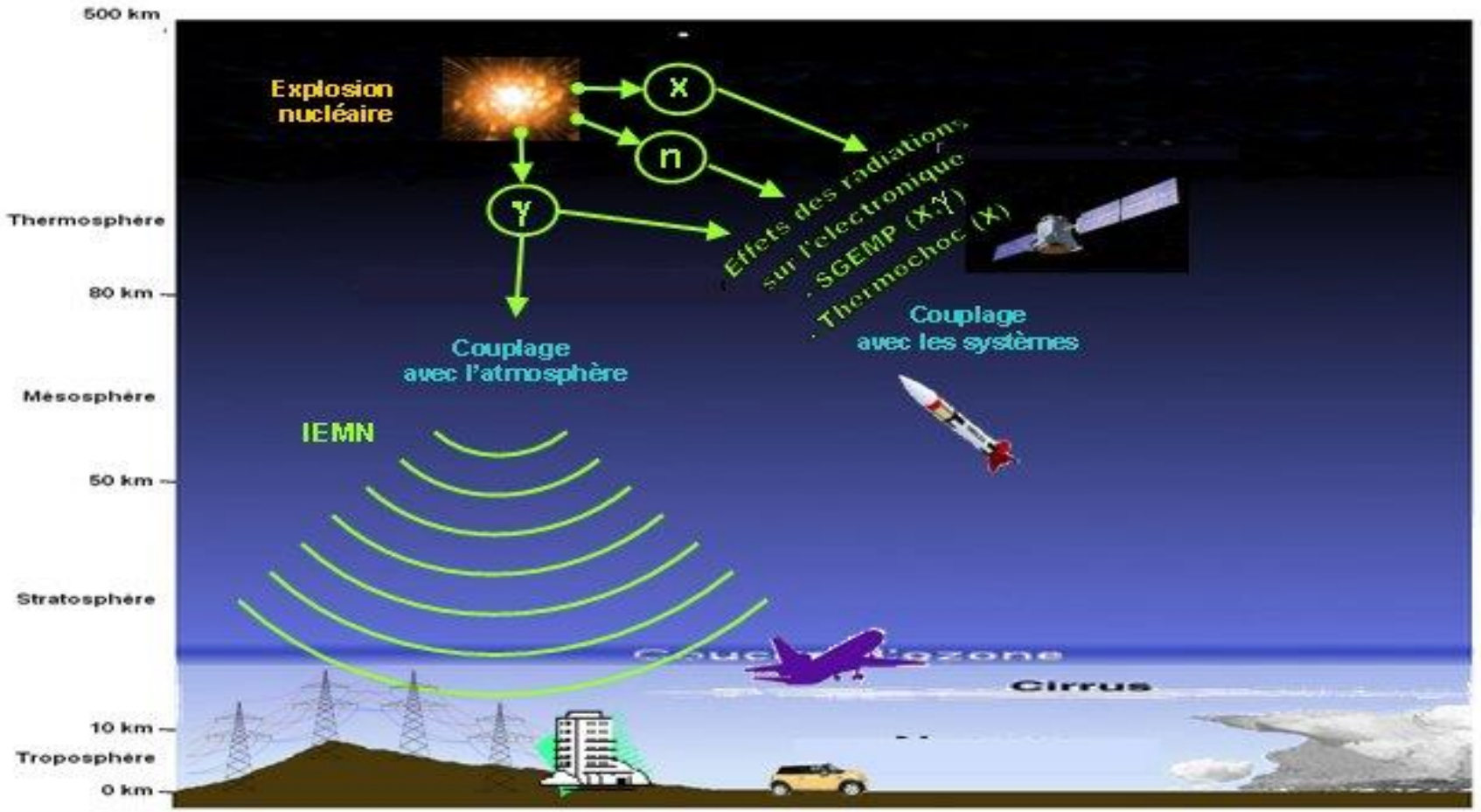
Environnement électromagnétique – IEC153104



* Narrow Band in the range of ~0.5 to ~ 5 GHz ** usually not HPEM
*** Important spectral contributions up to ~10 MHz, depending on range and application

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

b. Agression électromagnétique intentionnelle



Source : Nuclétudes

Pas le sujet de cette présentation

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

b. Agression électromagnétique intentionnelle

Un peu d'histoire…

IEMN-HA

The Starfish Prime Nuclear Test
from more than 800 miles away

Source Internet

STARFISH,

Perturbation du réseau électrique

July 9, 1962

Lutte anti-satellite – FISHBOWL

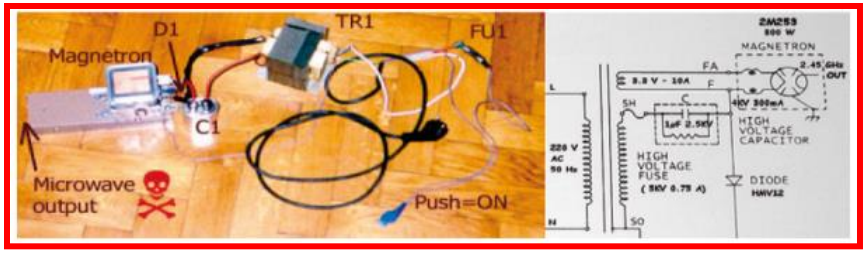
Pas le sujet de cette présentation

AGREMI (en anglais « IEMI »)

Une évolution des technologies et des usages

- Forte puissance

Diehl, Germany



Micro-onde modifié, KTH

Source EPFL

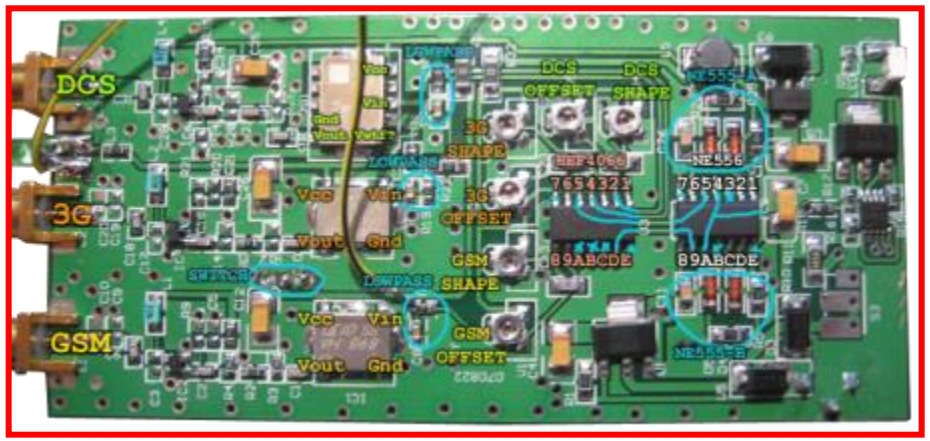
Source en conduction, Russie

Taser

AGREMI (en anglais « IEMI »)

Une évolution des technologies et des usages

- Faible puissance - brouilleurs



Source Internet

AGREMI (en anglais « IEMI »)

Cas connus d'utilisation – F. Sabath, 2011

- Japon, cellule terroriste, attaque des machines de jeu d'un casino;
- Saint-Pétersbourg (Russie), arrêt d'un système de sécurité dans une bijouterie avec un micro-onde modifié;
- Daghestan (Russie), brouillage des réseaux de police;
- Europe, plusieurs cas de brouillage intentionnel;
- Russie, arrêt d'un système de contrôle d'accès par les rebelles Tchétchènes;
- Londres (GB), chantage auprès d'une banque;
- Pays-Bas, attaque d'un réseau bancaire…

AGREMI (en anglais « IEMI »)

Une prise de conscience (1/3)

"Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes"

Zurich EMC Symposium, Février1999; IEC 61000-2-13:2005

AGREMI (en anglais « IEMI »)

Une prise de conscience (2/3)

1999, publication d'une résolution par l'Union Radio-Scientifique International (URSI) portant sur les problématiques AGREMI et la nécessité de sa prise en compte

The International Electrotechnical Commission (IEC) SC77C (EMC: High Power Transient Phenomena)

AGREMI (en anglais « IEMI »)

Projets nationaux et internationaux (3/3)

SECRET, FP7, UE;

STRUCTURES, FP7, UE;

HiPOW, FP7,UE;

MURI, USA…

Source Internet

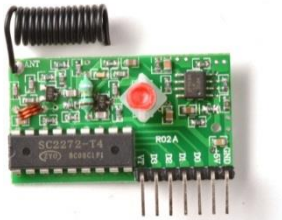
SOMMAIRE

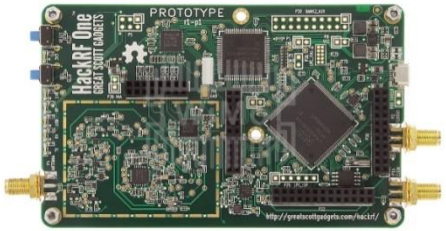
1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. **Évolutions des outils d'analyse RF**
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

2. VEILLE SCIENTIFIQUE ET TECHNIQUE

c. Évolutions des outils d'analyse RF

Evolution des équipements

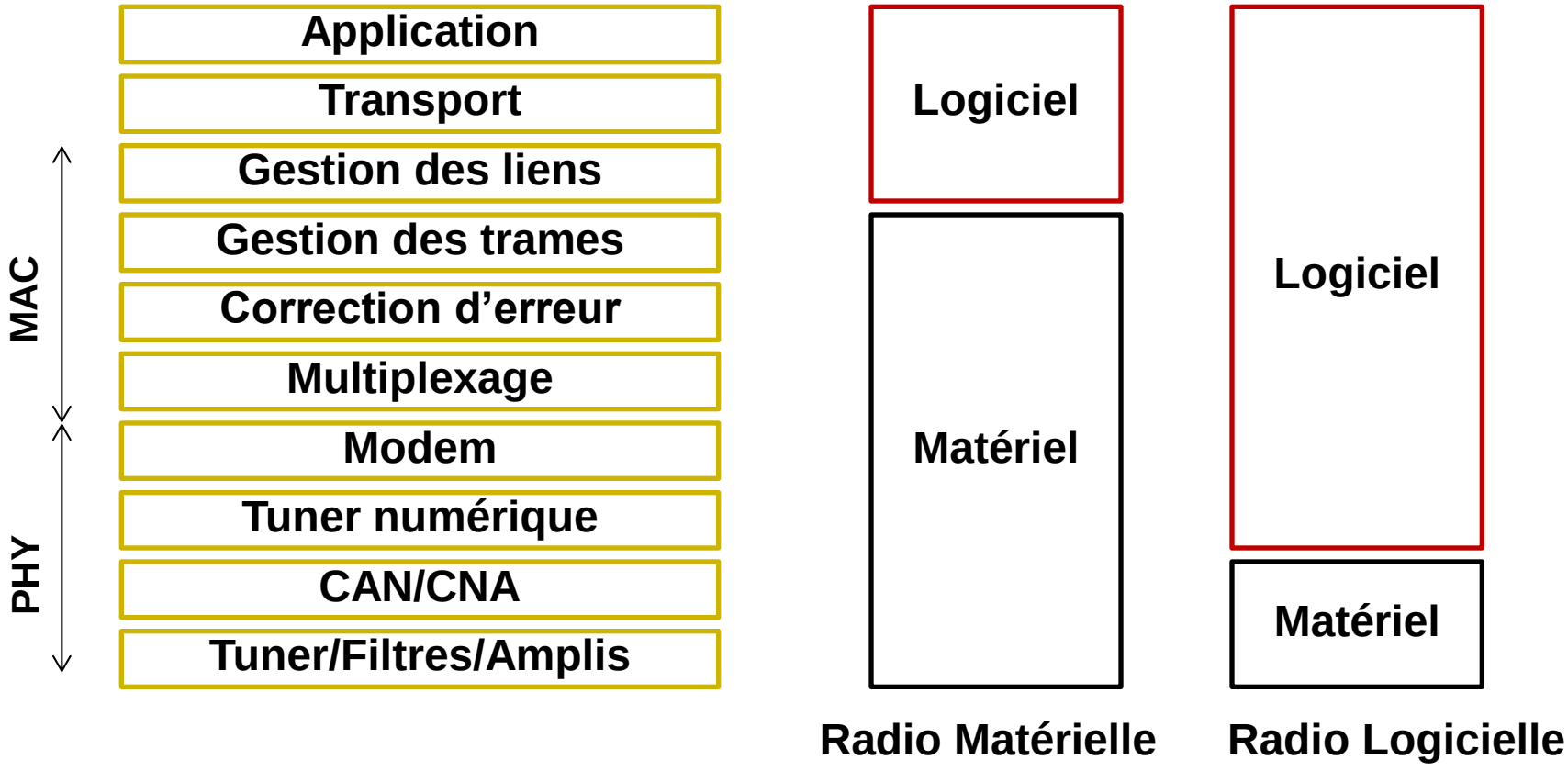




Source Internet

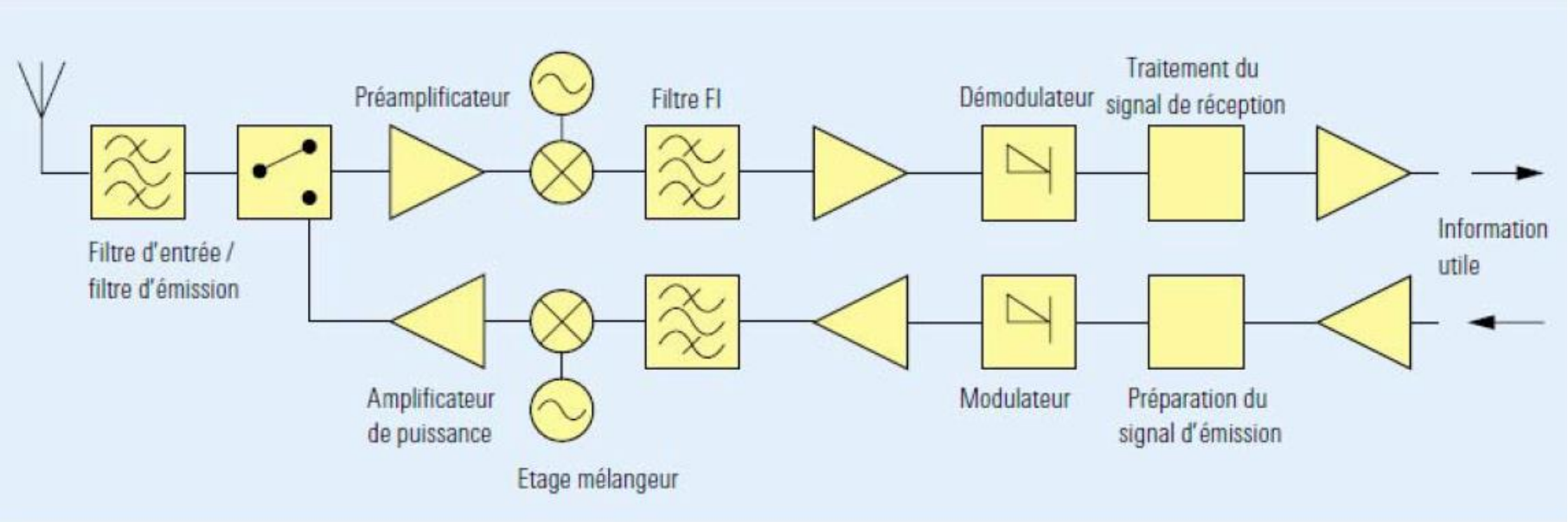
c. Évolutions des outils d'analyse RF

Radio matérielle vs. Radio logicielle

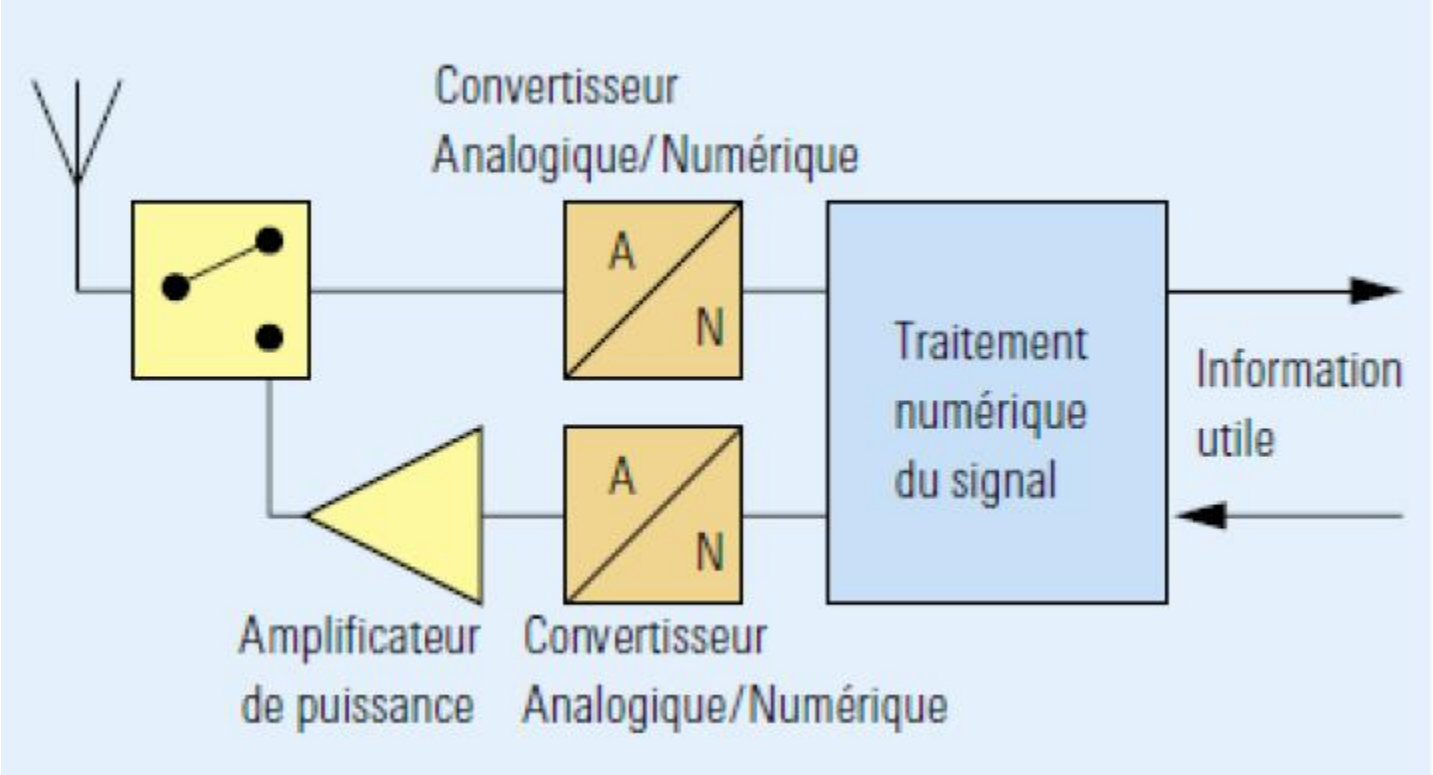


c. Évolutions des outils d'analyse RF

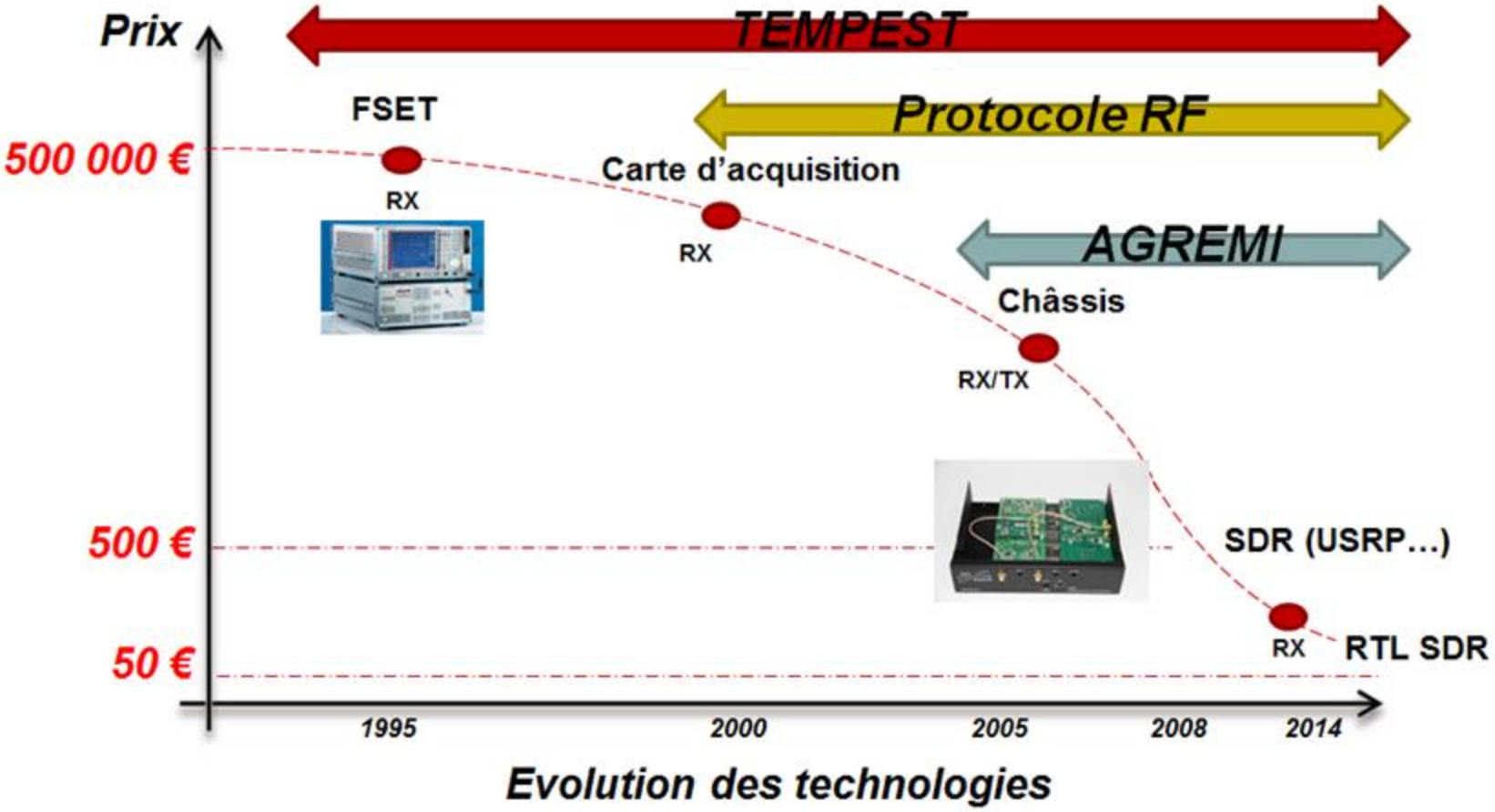
Radio matérielle vs. Radio logicielle



Radio matérielle vs. Radio logicielle



Evolution des équipements



SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. **Démarche de sécurisation électromagnétique**
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

Objectif :

Tirer profit d'une seule démarche de sécurisation pour se protéger au mieux contre les menaces AGREMI et TEMPEST.

Données d'entrée :

- Profil de l'attaquant
- Échelle du système
- Définition du périmètre de sécurité
- Identification des chemins de fuites

Périmètre sécurisé

Source Internet

Périmètre sécurisé

Source Internet

Quelques exemples de facteur d'échelle

Périmètre sécurisé

Source Internet

Quelques exemples de facteur d'échelle

Immeuble de bureaux

Source Internet

Quelques exemples de facteur d'échelle

Salle informatique

Source Internet

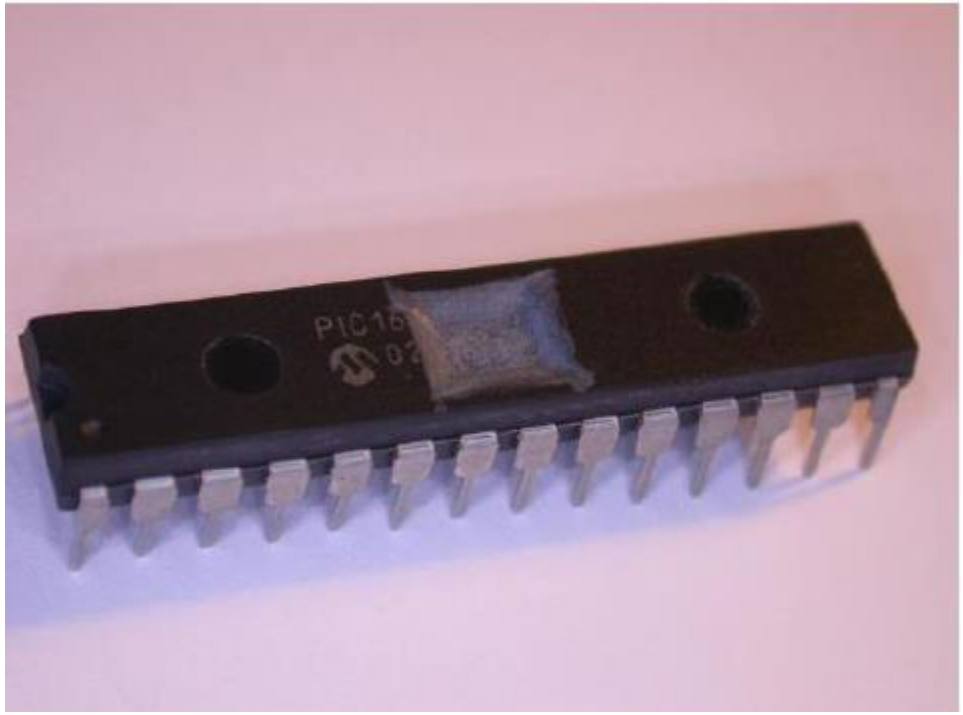
Quelques exemples de facteur d'échelle

Équipements TEMPEST

Source Internet

Quelques exemples de facteur d'échelle

Composant crypto (carte à puce)



Source Internet

Quelques exemples de facteur d'échelle

Cas particuliers

Shelters, Avions,

Bateaux, Satellites

Source Internet

SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. **Analyse de risques**
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

3. DÉMARCHE DE SÉCURISATION ÉLECTROMAGNÉTIQUE

a. Analyse des risques

Analyse des risques pour une infrastructure

Bâtiment	Systèmes électroniques
- Atténuation du bâtiment - Architecture de l'infrastructure	- Susceptibilité - Émissivité

- Position des équipements dans l'infrastructure;
- Intégration d'éléments de protection;
- Utilisation des équipements caractérisés…

Mise en œuvre de moyens de détection

Caractérisation de la susceptibilité

Classification des effets induits par des AGREMI

0	Indéterminé	Non détecté
1	Pas d'effet	Pas de perturbation
2	Interférence	Faible influence – influence non critique
3	Dégradation	Influence critique sur la disponibilité du système
4	Sévère	Pertes des fonction critiques
5	Destruction	Arrêt du système avec défaut matériel/logiciel

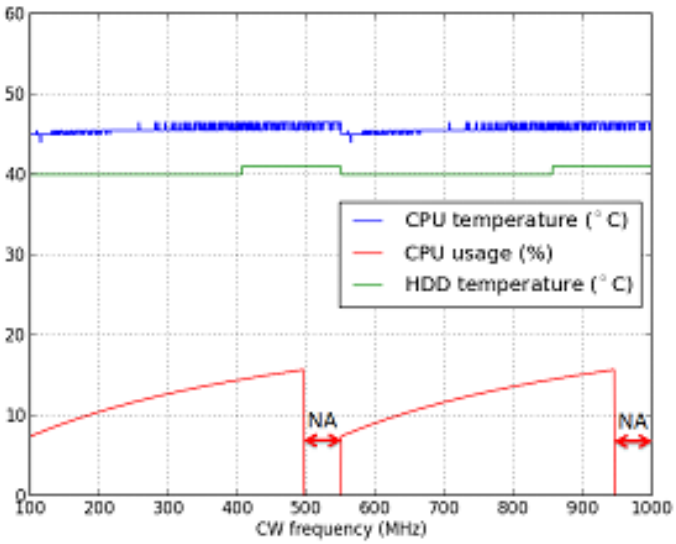
Caractérisation de la susceptibilité

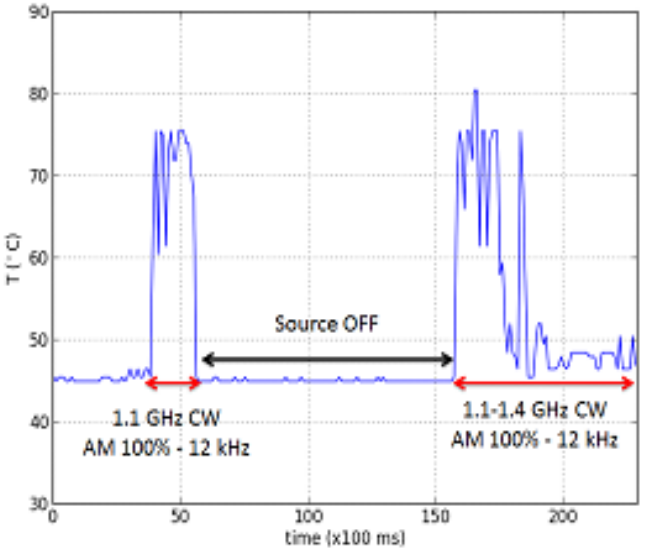
Ambiguïté: « sans effet » ou « effet non détecté »

- Travaux ANSSI 2013/2014 : caractérisation des effets induits par des AGREMI sur des réseaux informatiques
- Méthode : instrumentation des capteurs d'un ordinateur COTS et de l'analyse des logs « systèmes » en temps-réel

Caractérisation de la susceptibilité

Capteur de température



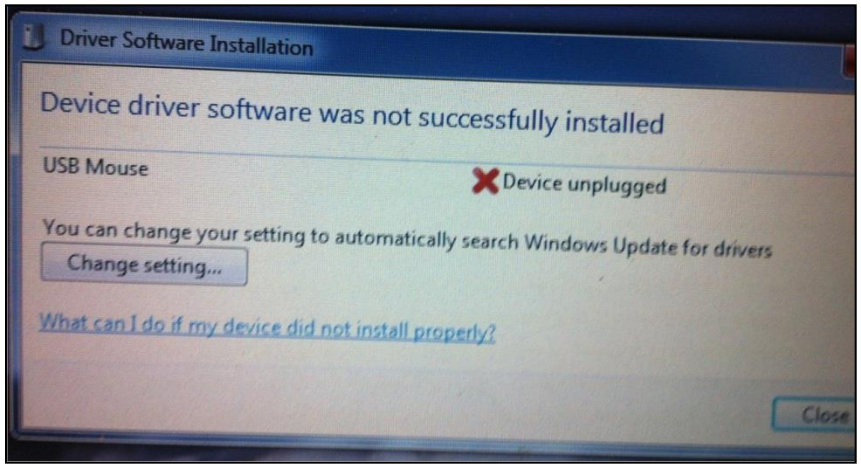


Source Kasmi et al., CEM France 2014

Figure 1: Evolution of the CPU and HDD temperature (°C) and the CPU usage (%) in regards of the 100 % AM CW frequency (a) Variability of the measured CPU temperature due to the CW illumination between 1.1 and 1.4 GHz (b)

Caractérisation de la susceptibilité

Interfaces de communication




```
hub 1-0:1.0: port 1 disabled by hub (EMI?), re-enabling...
usb 1-1: reset full-speed USB device number 2 using uhci_hcd
usb 1-1: USB disconnect, device number 2
usb 1-1: USB disconnect, device number 3
usb 1-1: new low-speed USB device number 4 using uhci_hcd
usb 1-1: device descriptor read/64, error -71
usb 1-1: string descriptor 0 read error: -71
usbhid 1-1:1.0: can't add hid device: -71
usbhid: probe of 1-1:1.0 failed with error -71
usb 1-1: device not accepting address 5, error -71
hub 1-0:1.0: unable to enumerate USB device on port 1
usb 1-1: unable to read config index 0 descriptor/all
usb 1-1: can't read configura
---SYSTEM CRASH
```

```
input: PS/2 Generic Mouse as /devices/platform/i8042/serio1/input/input0
psmouse serio1: bad data from KBC - timeout
atkbd serio0: Unknown key pressed (translated set 2, code 0x9e on isa0060/serio0).
atkbd serio0: Use 'setkeycodes e01e <keycode>' to make it known.
psmouse serio1: alps: Unknown ALPS touchpad: E7=10 00 64, EC=10 00 64
psmouse serio1: bad data from KBC - timeout
```

Kasmi et al., System Design and Assessment Note, 2014

Caractérisation de la susceptibilité

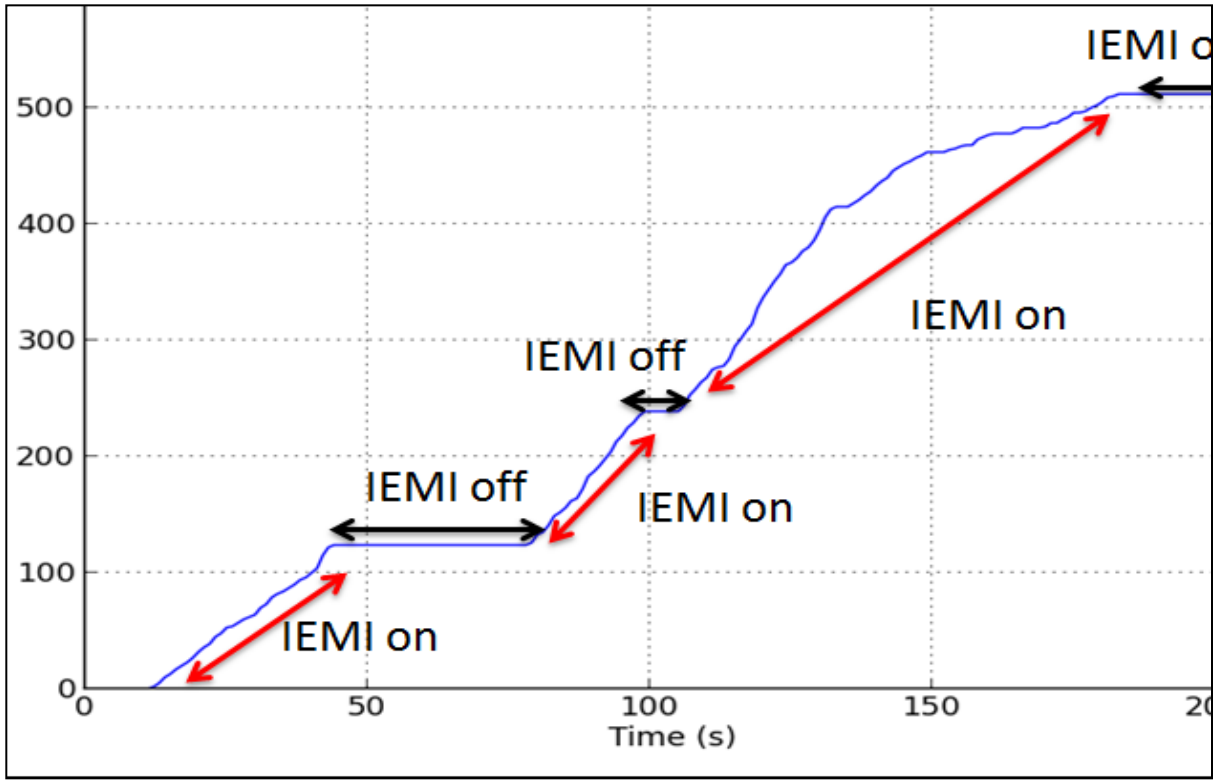
Interfaces de communication

Interface	Effets
PS/2	Données reçues corrompues
	Données reçues non reconnues
	Identifiant du périphérique modifié
USB	Déconnexion/reconnexion du périphérique
	Corruption du descripteur du périphérique
	HUB désactivé

Source Kasmi et al., CEM France 2014

Caractérisation de la susceptibilité

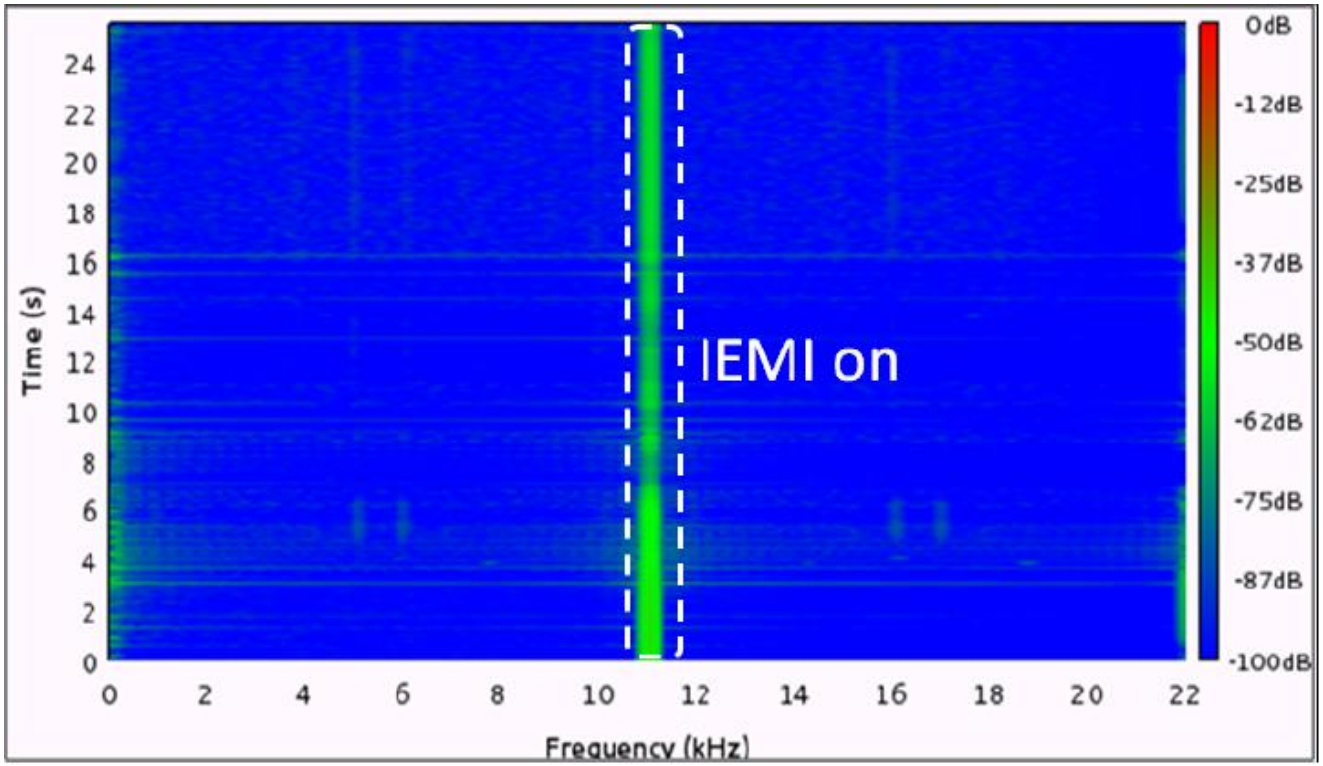
Lien Ethernet



Kasmi et al., System Design and Assessment Note, 2015

Caractérisation de la susceptibilité

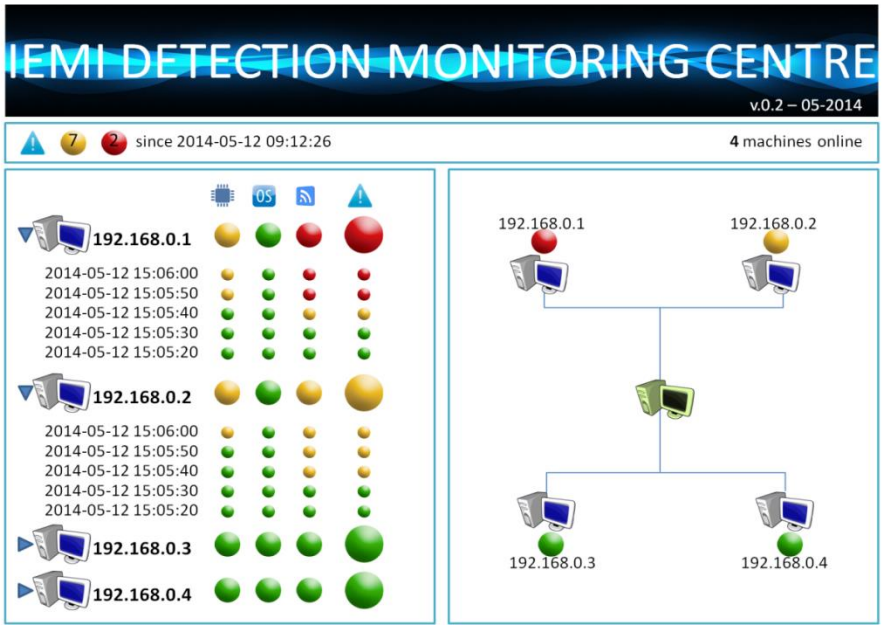
Carte son – mesure du planché de bruit

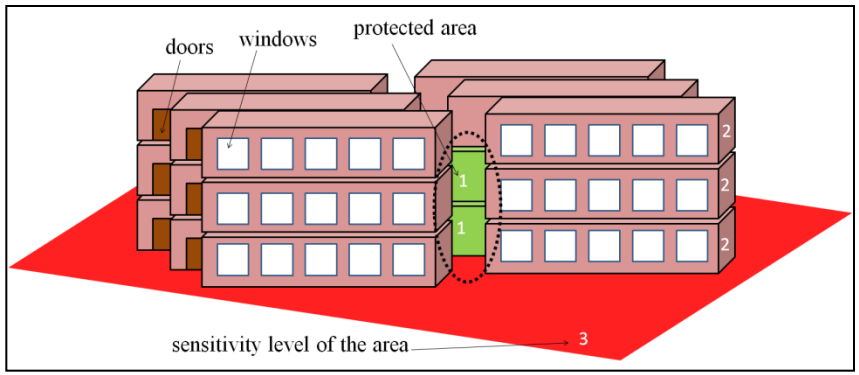


Kasmi et al., System Design and Assessment Note, 2015

Caractérisation de la susceptibilité

Passage à l'échelle





Principe de zonage

Kasmi et al., System Design and Assessment Note, 2015

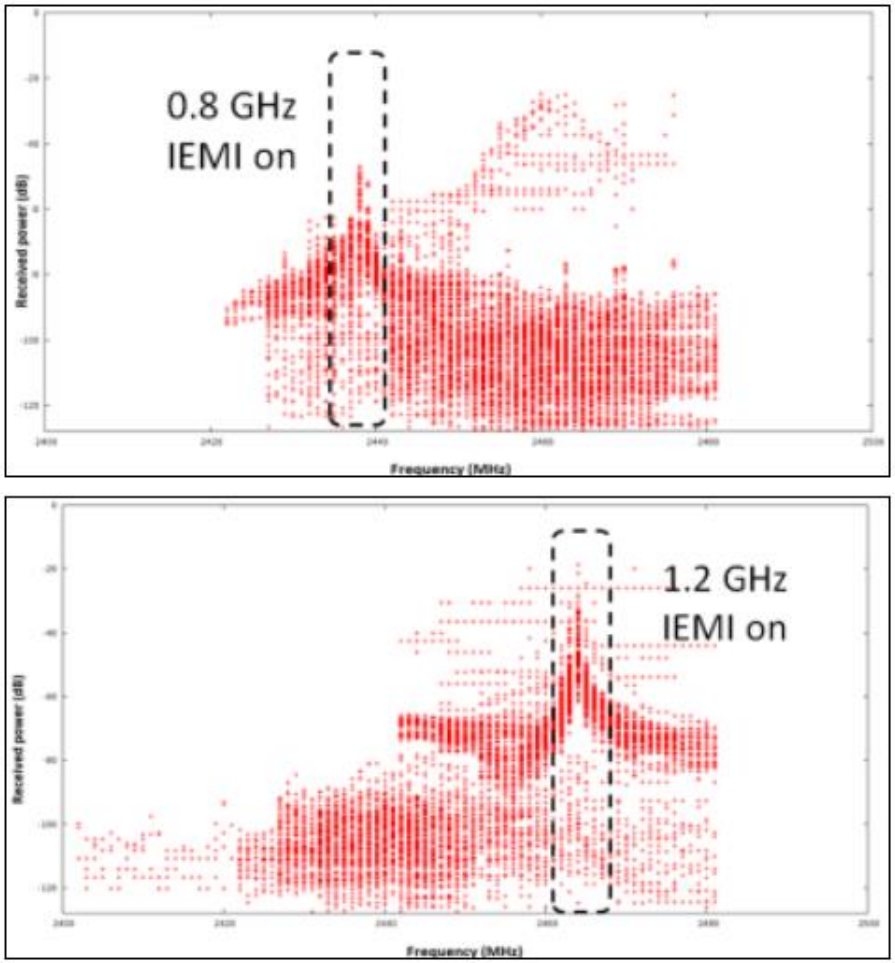
Caractérisation de la susceptibilité

Ambiguïté: Problématiques de « couverture » ou de « brouillage »

- Travaux ANSSI 2013/2014 : exploitation des ressources internes des modems pour la détection de perturbations intentionnelles
- Méthode : instrumentation des modems au niveau des couches physique et logique pour la détection

Caractérisation de la susceptibilité

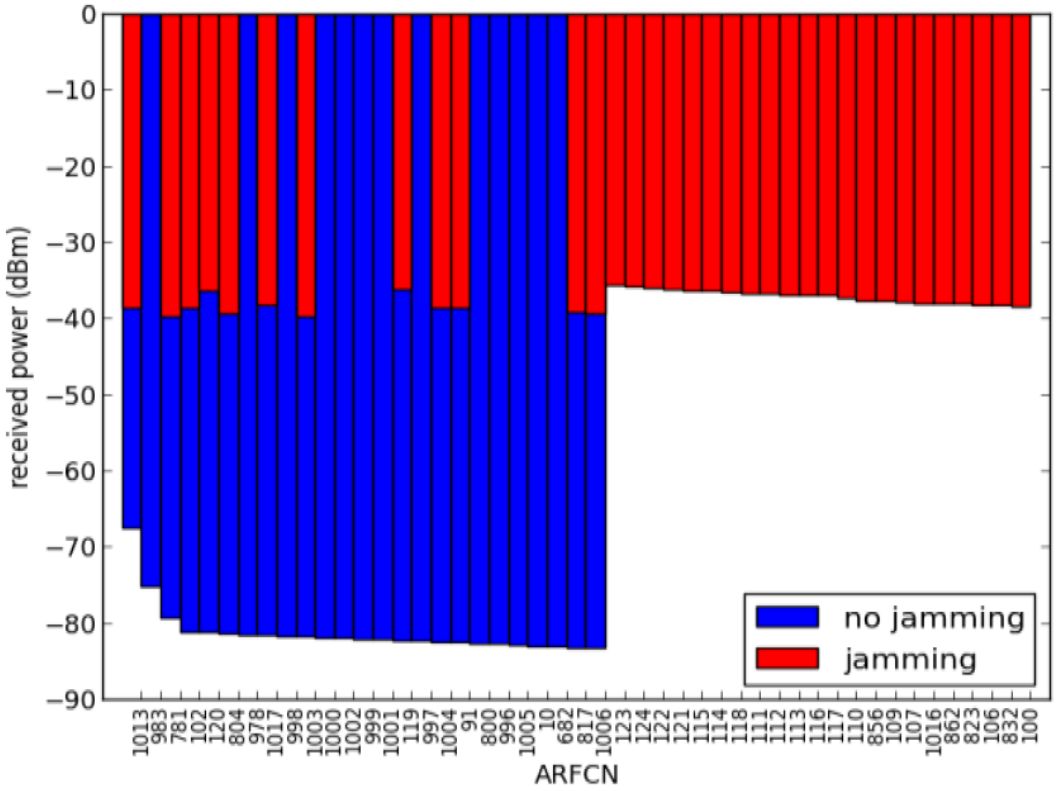
Lien Wi-Fi



Kasmi et al., System Design and Assessment Note, 2015

Caractérisation de la susceptibilité

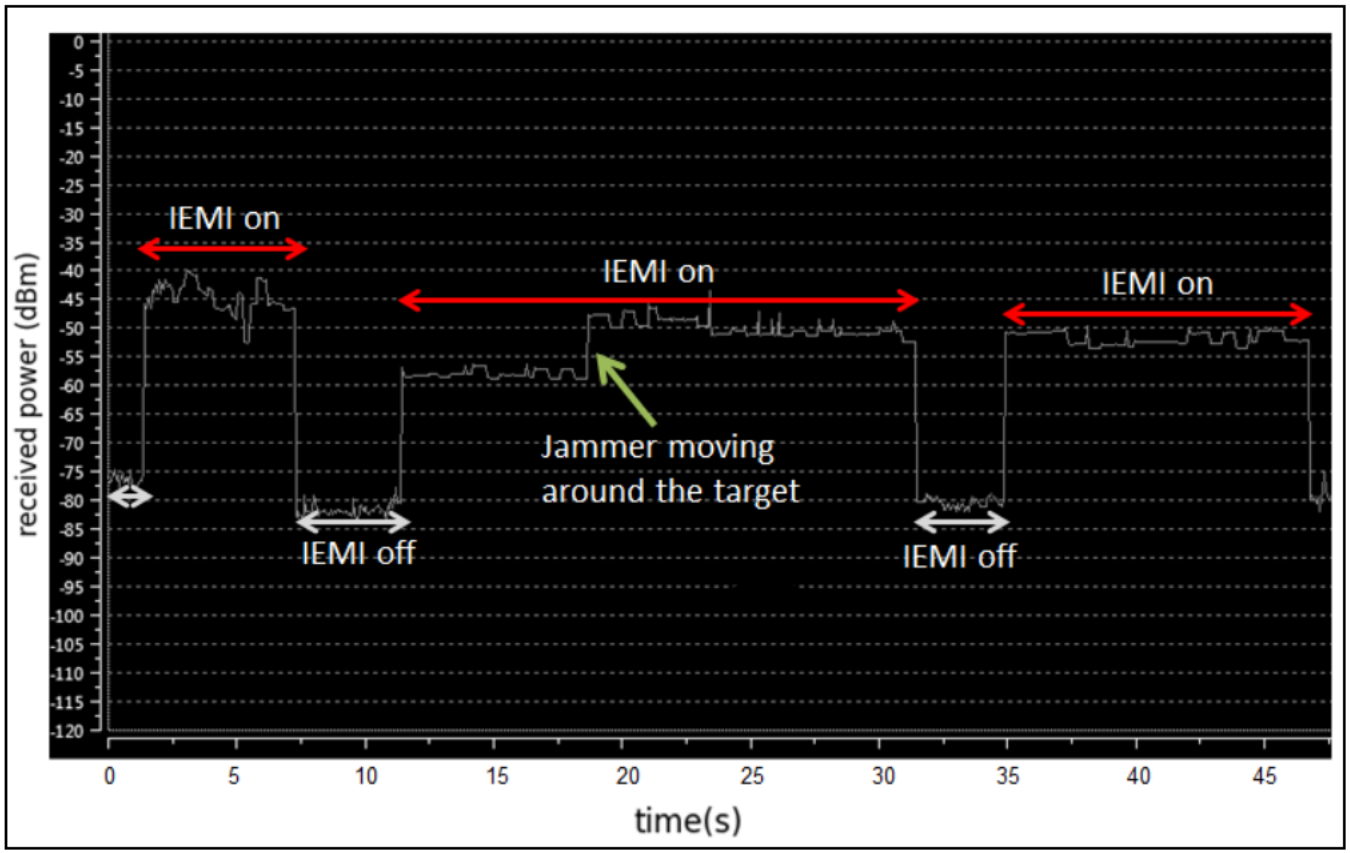
Lien 2G/3G



Kasmi et al., System Design and Assessment Note, 2015

Caractérisation de la susceptibilité

Lien 2G/3G



Kasmi et al., System Design and Assessment Note, 2015

SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. Et les pièges dans tout ça??
4. Conclusion

b. Moyens de protection

Annexe 2 de l'Instruction interministérielle n°300

http://www.ssi.gouv.fr/reglementation-ssi/signaux-parasites-comprettants-spc

Mesures organisationnelles

AGREMI

- *Redondance & duplication des sites*

AGREMI / TEMPEST

- *Choisir des technologies minimisant les risques*
  - *Fibre optique*
  - *Fonctionnement sur batterie*
- *Le bon équipement à la bonne place (zonage des locaux)*

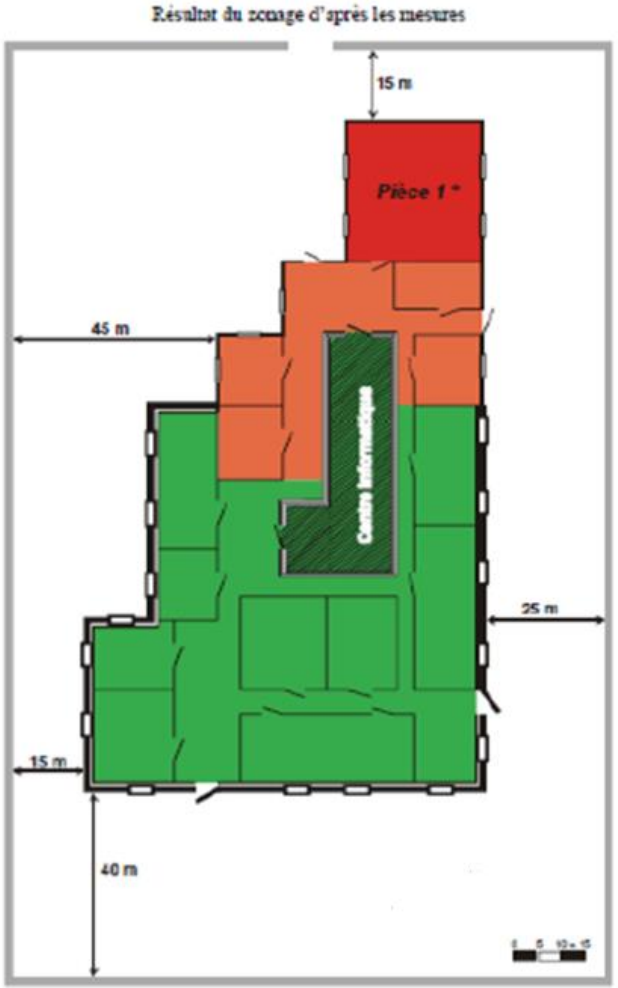
3. DÉMARCHE DE SÉCURISATION ÉLECTROMAGNÉTIQUE

b. Moyens de protection

Mesures organisationnelles

- *Le bon équipement à la bonne place (zonage des locaux)*

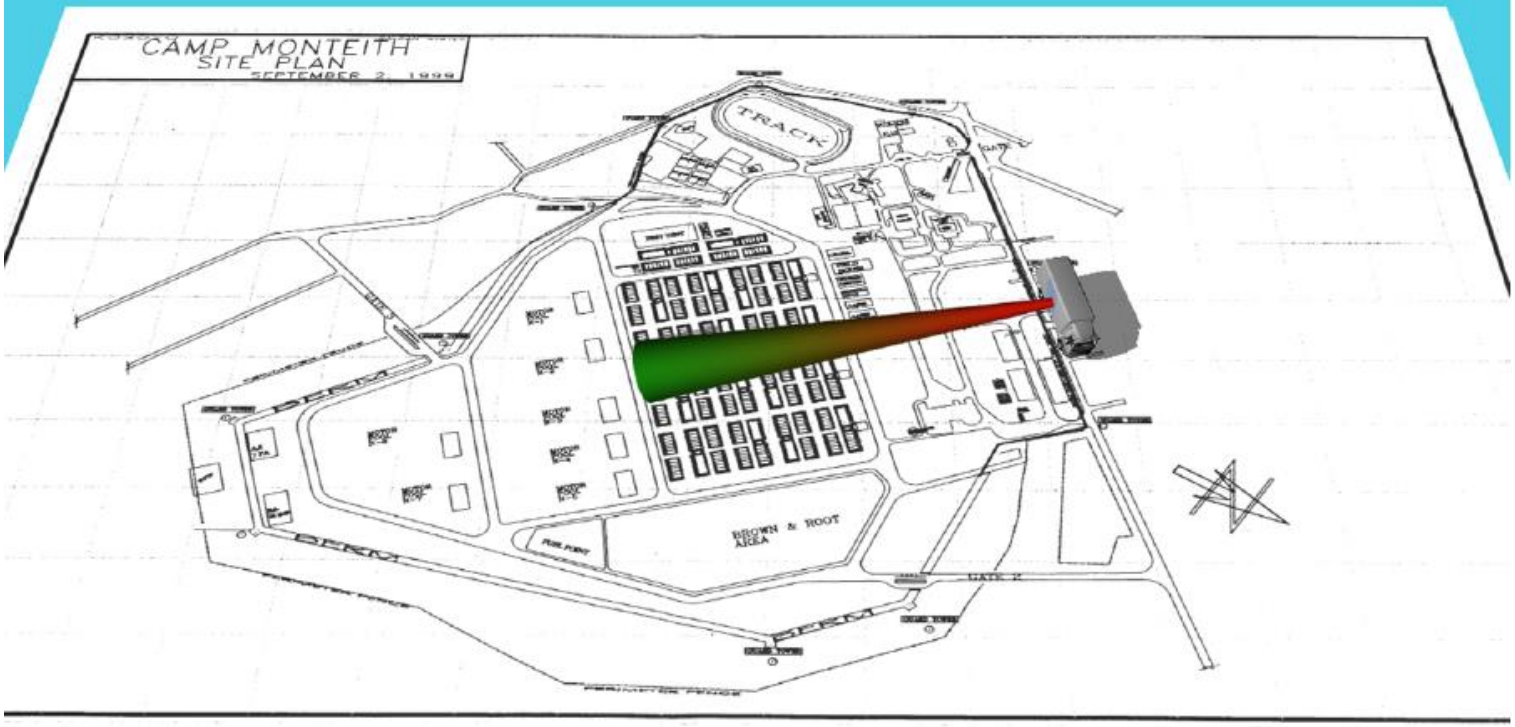
1. Détermination de la limite de zone de sécurité TEMPEST avec l'AQSSI locale
2. Définition des points de mesure
3. Réalisation des mesures
4. Attribution des zones du bâtiment



Mesures organisationnelles

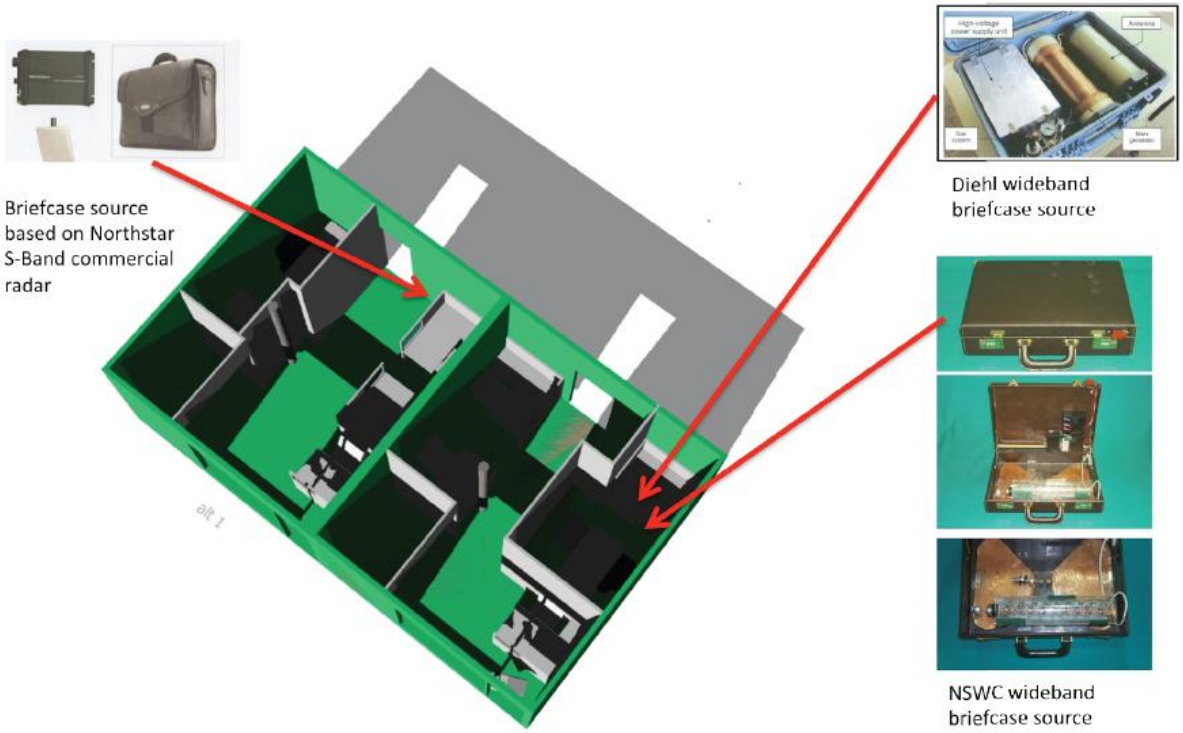
- *Le bon équipement à la bonne place (zonage des locaux)*

Source NATO RTO SCI-132 Final Report



Mesures organisationnelles

- *Le bon équipement à la bonne place (zonage des locaux)*



Source NATO RTO SCI-132 Final Report

Propagation par rayonnement

- *Durcissement de l'infrastructure*
  - *Ferraillage comportant un maillage de petite dimension*
  - *Matériau conducteur pour le revêtement des murs extérieurs*
  - *Utilisation de verres athermiques*
- *Mise à la terre*
  - *Du ferraillage de la structure du bâtiment*
  - *Des gaines de climatisation*
  - *Du chauffage central*
  - *Des servitudes : détecteurs périmétriques, alarmes…*
- *Faradisation légère : durcissement des locaux borgnes*

Propagation par rayonnement

- *Durcissement des systèmes*
  - *Baie informatique CEM*
  - *Cage de Faraday*
  - *Équipement TEMPEST*

- *Mesure d'émissivité et de susceptibilité des équipements composants le système*
  - *Serveurs, routeurs, terminaux utilisateurs*
  - *Alarmes, détecteurs, etc…*

Source Internet

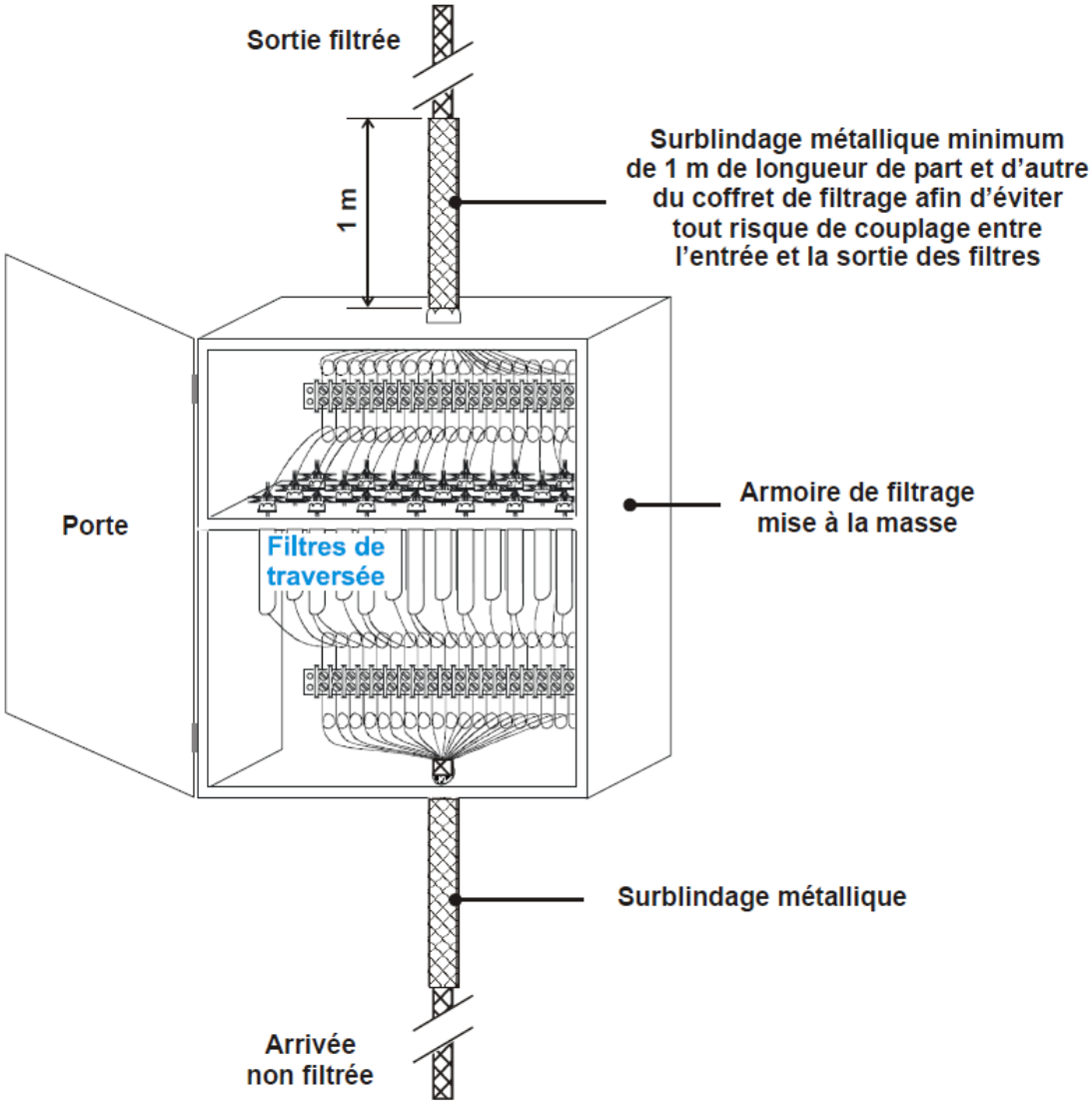
Propagation par conduction

- *Écrêtage et filtrage des arrivées*
  - *Énergie, télécommunications, signaux de servitudes*
- Caractérisation des filtres, EMC Europe 2014, ANSSI
  - *Essais sur table*
  - *Qualité de l'installation sur site*

3. DÉMARCHE DE SÉCURISATION ÉLECTROMAGNÉTIQUE

b. Moyens de protection

Exemple de mise en œuvre d'une armoire de filtrage



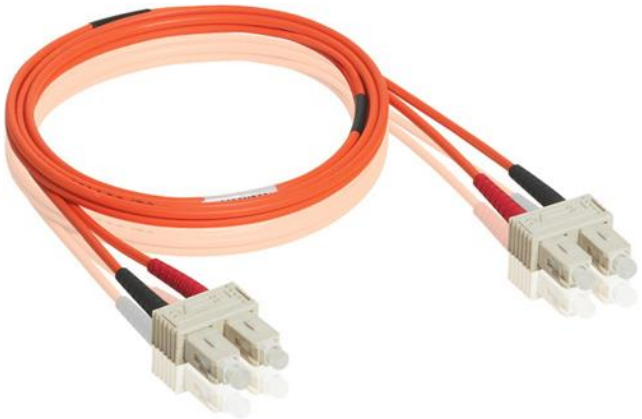
Source Internet

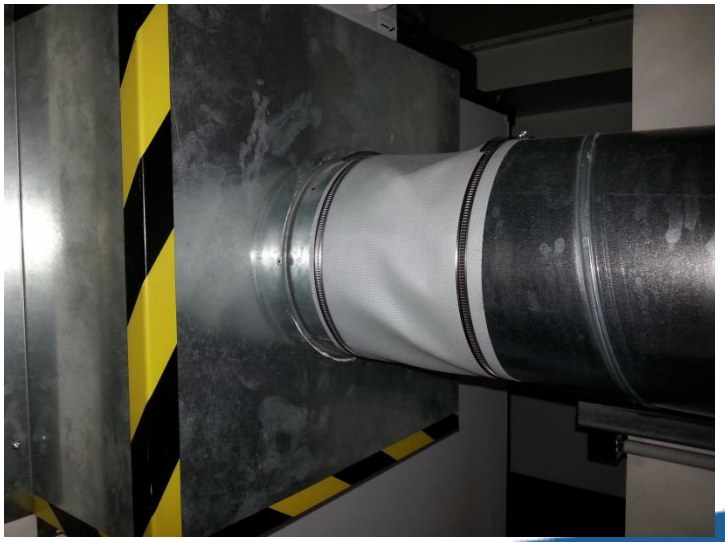
Propagation par conduction

- *Écrêtage et filtrage des arrivées*
  - *Énergie, télécommunications, signaux de servitudes*
- Caractérisation des filtres, EMC Europe 2014, ANSSI
  - *Essais sur table*
  - *Qualité de l'installation sur site*
- *Mesure en conduction sur site*
  - *Estimation de l'atténuation réelle d'un conducteur métallique*
  - *Vérification des performances des filtres déjà installés*

Propagation par conduction

- *Utilisation de fibres optiques*
- *Manchonnage des canalisations métalliques*
  - *Chauffage et gaines d'aération*





Source ANSSI

SOMMAIRE

1. Contexte
2. Veille scientifique et technique
   a. Signaux compromettants
   b. Agressions électromagnétiques intentionnelles
   c. Évolutions des outils d'analyse RF
3. Démarche de sécurisation électromagnétique
   a. Analyse de risques
   b. Moyens de protection
   c. **Et les pièges dans tout ça??**
4. Conclusion

Retour au facteur d'échelle et à l'analyse de risque

Si l'on considère la présence d'un piège à l'intérieur du périmètre de sécurité,

Alors il faut mettre à jour l'analyse des risques :

Ce sont de nouveaux vecteurs de fuite

(Acoustique, RF…)

Retour au facteur d'échelle et à l'analyse de risque

Il faut opter pour des méthodes et des moyens de protection en profondeur comme par exemple :

- Isolement des postes Internet
- Interdiction des téléphones portables dans les locaux sensibles
- Déploiement de solutions de détection
- Etc…

4. CONCLUSION

Les applications utilisant les ondes électromagnétiques sont en constante évolution.

Ceci implique de nouvelles vulnérabilités et de nouvelles menaces qu'il convient de prendre en compte au plus tôt afin de **maintenir la disponibilité, l'intégrité** des systèmes et **garantir la confidentialité** des informations traitées.