LE TEMPEST : LA REPONSE A UNE MENACE TOUJOURS D'ACTUALITE

J.L. BRAUT – J. SAVINA

Salon RF &Hyper – 5 avril 2012

THALES

Définition de la menace Tempest

- « la menace Tempest est définie comme l'interception et l'exploitation des signaux parasites compromettants « S.P.C » en vue de reconstituer les informations traitées »

- Elle s'adresse aux appareils de traitement de l'information « A.T.I », aux équipements de cryptophonie et équipements de chiffrement.

Signification de Tempest

- Total Electronic and Mechanical Protection against Emission of Spurious Transient,
- Transient ElectroMagnetic Pulse Emanations Standart
- Suppression des signaux inTEMPESTifs
- Se Rapporte aux investigations et aux études des émissions compromettantes
- TEMPorary Emanations and Spurious Transmission
  « Rayonnements temporaires et émission parasite »
- Telecommunications Electronic Material Protected from Emanating Spurious Transmissions
  « Matériels électroniques de Télécommunication protégés contre les émanations de signaux parasites»
- TEMPEST = ANTICOMPROMISSION ELECTROMAGNETIQUE

Les signaux parasites compromettants

Définition :

- **Signaux parasites :**

  Tout matériel ou système qui traite ou transmet des informations sous forme électrique émet des perturbations électromagnétiques temporaires.

  Ces perturbations provoquées par les variations d'état des différents circuits du matériel (ou du système) durant son fonctionnement sont appelées :

signaux parasites

Les signaux parasites compromettants

Définition :

- **Signaux parasites compromettants (S.P.C.):**

  Certains des signaux émis sont représentatifs des informations traitées.

  Leur interception et leur exploitation permettent de reconstituer ces informations

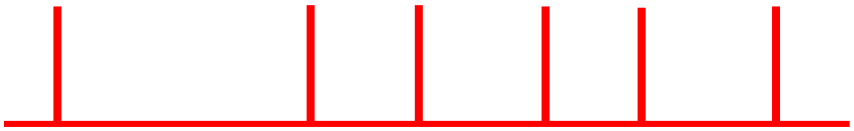
  Ces signaux sont appelés :

signaux parasites compromettants

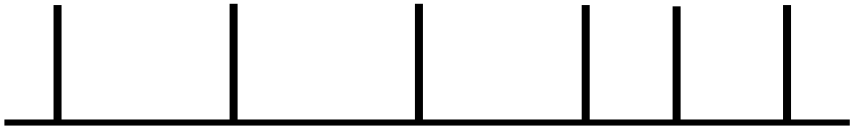
S.P.C.

Signaux parasites compromettants

Signal source



Signal corrélé aux fronts montants du signal source



Signal non corrélé au signal source

Les signaux parasites compromettants

Mode de propagation des signaux parasites compromettants :

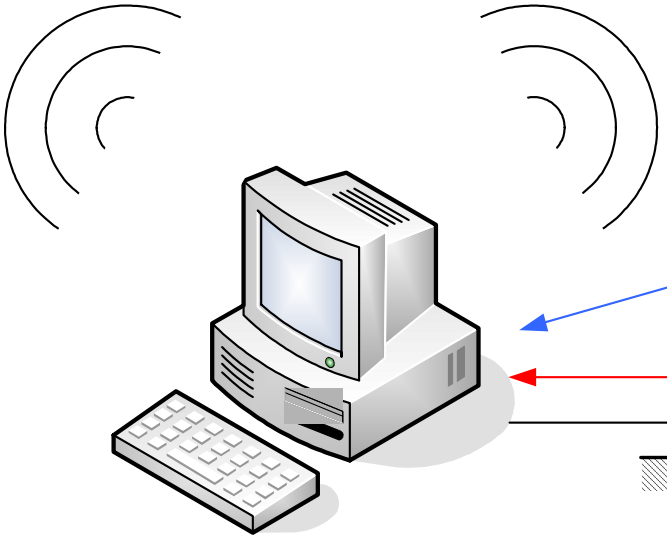
Les perturbations électromagnétiques se propagent toujours suivant deux modes:

- **Par rayonnement**
  - En espace libre
- **Par conduction**
  - Sur les conducteurs en liaison avec le matériel
  - Sur les conducteurs voisins du matériel (zone de couplage)

Les signaux parasites compromettants

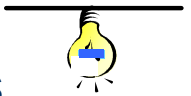
Par rayonnement

Rayonnement en espace libre



Par conduction

Sur les conducteurs fortuits

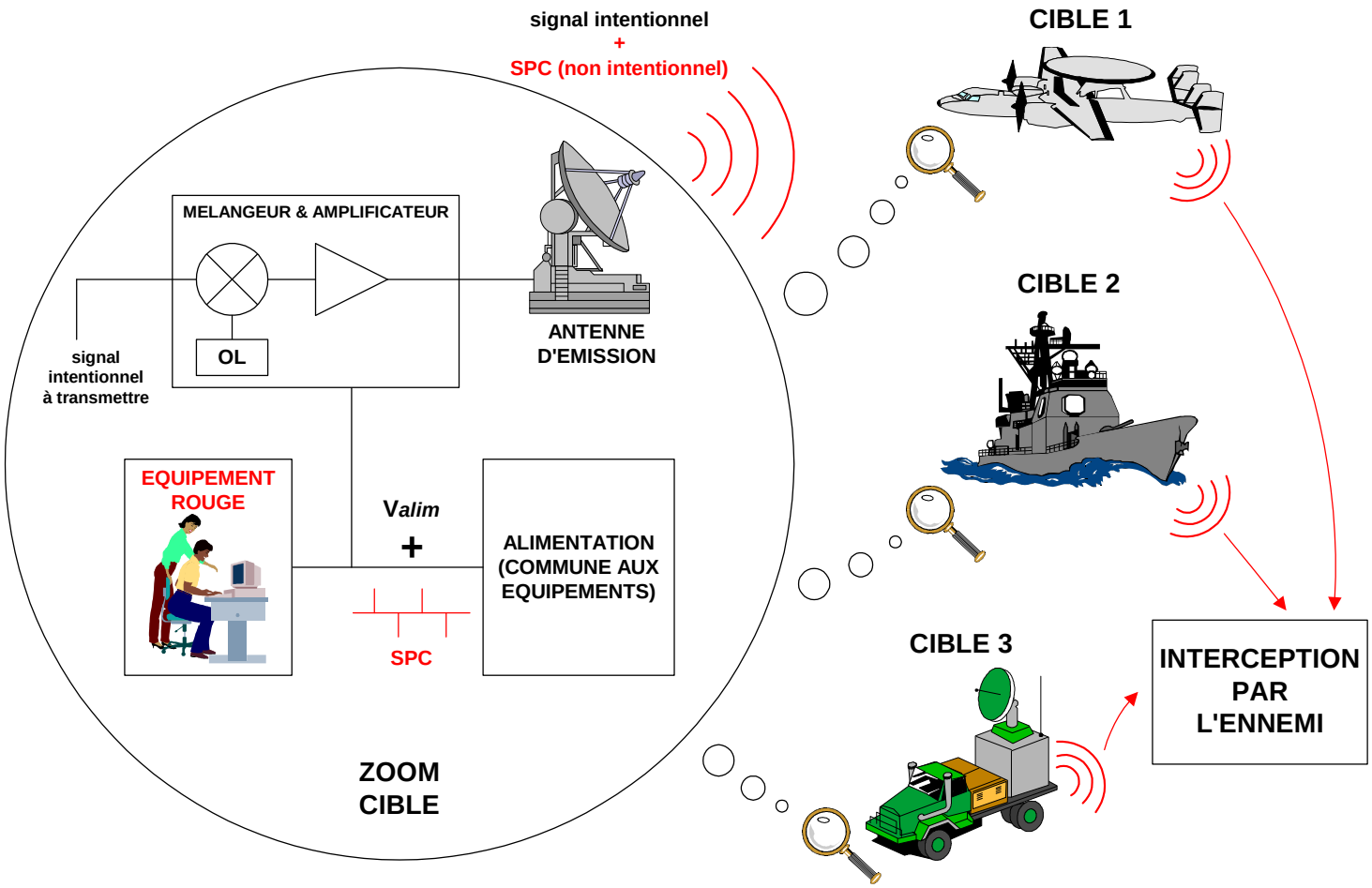


Sur les conducteurs reliés au matériel :

- Réseau de transmission
- Réseau d'alimentation
- Réseau de terre

THALES

Fuite d'informations et interception (exemple)



Règlementation

Règlementation

- **Chaque état possède sa propre réglementation TEMPEST.**
  - USA : NACSIM, NSTISSAM,…
  - UK : BTR
  - …
- **Hormis l'OTAN, il n'y a pas d'organisme international de réglementation dans le domaine TEMPEST.**

- **Présentation de la réglementation**
  - France
  - OTAN

Règlementation française

Instructions interministérielles :

- Protection contre les signaux parasites compromettants: 300/SGDN/TTS/DR du 20/06/1997
- Obligatoire pour le traitement d'informations classifiées de défense (instruction générale interministérielle 900 du 20/07/1993)
- Recommandée pour le traitement d'informations sensibles (recommandation 901 du 02/03/1994)

Normes françaises:

- Installation des sites : 485/ SGDN (D.R)
- Zonage : 495/ SGDN (D.R)
- Liste des équipements agréés: 490/ SGDN (D.R)

Les normes de mesure Tempest utilisées sont les normes OTAN (AMSG / SDIP)

Les normes Tempest OTAN

- Allied Military Security Guideline,
- Secan Doctrine and Information Publication
- Les SDIP remplacent AMSG depuis 2006

SDIP 27 level A	AMSG 720 B	Standard de test
SDIP 27 level B	AMSG 788 A	Zone NATO N°1 Installations protégées
SDIP 27 level C	AMSG 784 B	Zone NATO N°2 Plateformes tactiques
SDIP 28	AMSG 799	Zonage Tempest
SDIP 29	AMSG 719 G	Règles d'installation

Protection Tempest des Systèmes

THALES

Concept Rouge/Noir

Définitions

- Rouge : **terme générique qui désigne les conducteurs, fibres optiques, composants, équipements ou systèmes qui véhiculent des signaux classifiés de défense non chiffrés et aux zones dans lesquelles apparaissent ces signaux.**

- Noir : **terme générique qui désigne les conducteurs, fibres optiques, composants, équipements ou systèmes qui véhiculent des signaux non classifiés ou chiffrés et aux zones dans lesquelles apparaissent ces signaux.**

Principe de la protection TEMPEST

- **Il faut dissocier les parties où les informations rouges sont traitées ou véhiculées (même non intentionnellement) des parties noires.**
- **Seules les informations noires peuvent être accessibles aux personnes non autorisées.**
- **Le concept rouge/noir permet de définir :**
  - L'architecture et le besoin de protection TEMPEST
  - Le type de dispositifs de protection
  - L'emplacement de ces dispositifs

Zonage des locaux :

Le zonage des locaux consiste à les classer en quatre zones selon l'affaiblissement qu'ils présentent par rapport à la limite de la zone de sécurité.

Ces zones sont par ordre d'affaiblissement croissant :

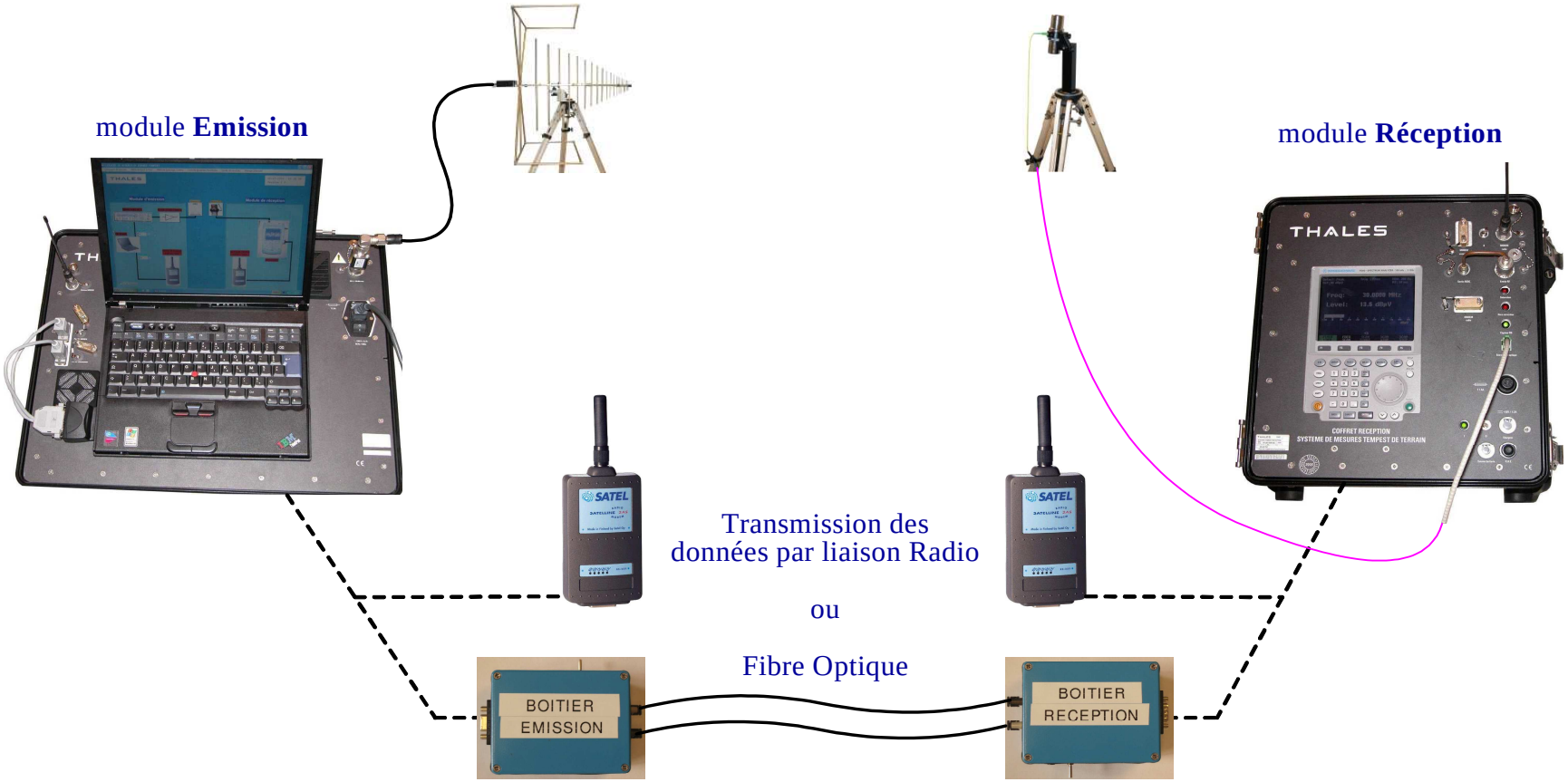
- Zone 0
- Zone 1
- Zone 2
- Zone 3

Le zonage des locaux ne prend en compte que les SPC émis en rayonnement.

Le banc de zonage THALES/DIS

module **Emission**

module **Réception**



Transmission des
données par liaison Radio

ou

Fibre Optique

THALES

Le banc de zonage THALES – Caractéristiques

❑Champ E côté émission :

➢ Antenne ETS-LINDGREN 3303 (bande 1M-30M)

➢ Antenne AH SYSTEMS SAS-521F-2 (bande 30M-1G)

❑ Champ E côté réception :

➢ Antenne THALES ADOC 1001 (bande 10k-1G) en version 2 V/m

THALES

Niveau de protection des équipements :

Le zonage des matériels consiste à classer ces matériels en quatre catégories A, B, C, D en fonction de leur degré de protection face à la menace TEMPEST.

- Catégorie A : Matériel conforme à l'AMSG 720 B / SDIP 27 Level A
- Catégorie B : Matériel conforme à l'AMSG 788 A / SDIP 27 Level B
- Catégorie C : Matériel conforme à l'AMSG 784 B / SDIP 27 Level C
- Catégorie D : autres matériels, conformes norme civile ou Mil.

Zonage TEMPEST:

L'association entre la zone des locaux et la classification des équipements, en tenant compte du type d'informations traitées (CD ou SD) permet de s'adapter au mieux à la menace Tempest.

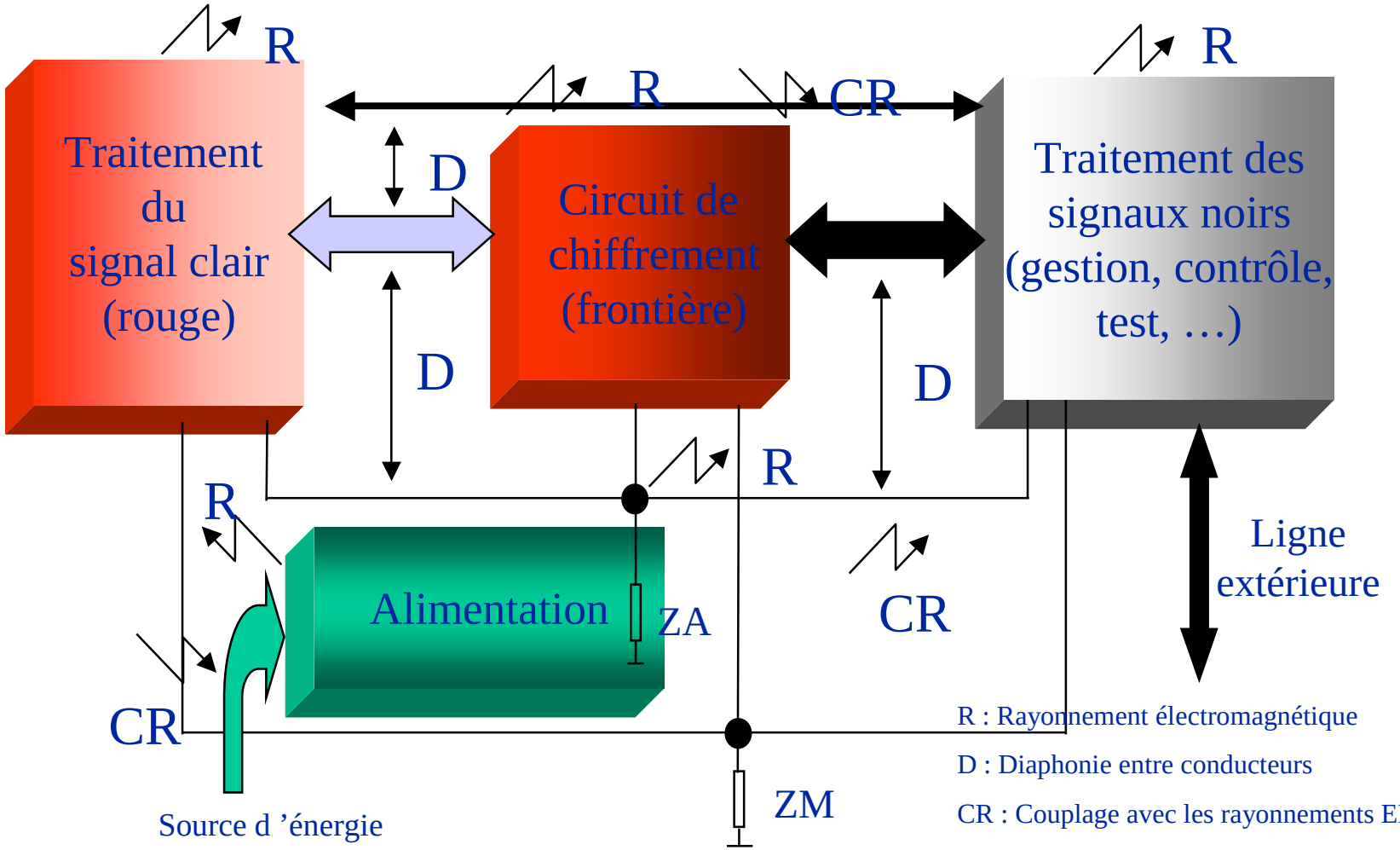
Il faut aussi respecter les règles d'installation des matériels définies dans la directive 485/SGDN/DCSSI/DR ou dans les Normes OTAN AMSG 719 G ou SDIP 29.

Protection Tempest des équipements

THALES

Protection Tempest d'un équipement

Mécanismes favorisant la prolifération des signaux rouges :



R : Rayonnement électromagnétique

D : Diaphonie entre conducteurs

CR : Couplage avec les rayonnements EM

ZA, ZM : Couplage par impédance commune

THALES

Protection TEMPEST des équipements

Limiter les signaux compromettants

- Limiter le nombre de signaux sensibles
- Rendre ces signaux les moins compromettants possibles
- Réduire le plus possible l'amplitude des signaux émis

- Règles de conception :
  - Pour le choix initial des signaux rouges
  - Pour le choix des liaisons d'interfaces rouges
  - Pour les choix d'architecture interne
  - Dans la réalisation des circuits et du câblage internes
  - Dans l'implantation des alimentations et des circuits de masses
  - Dans la réalisation du boîtier

Protection Tempest d'un équipement

Utiliser des technologies peu « polluantes » :

- Front des signaux les moins raides possible,
- Utilisation de liaisons parallèles au lieu de liaisons série,

Maitriser les SPC à la source :

- Isolation, lors de l'implantation des cartes , des composants et des pistes véhiculant les signaux sensibles,
- Blindage / capotage des cartes
- Filtrage des entrées-sorties
- Filtrage des alimentations
- Blindage du matériel et/ou de ses sous ensembles,

Protection TEMPEST des équipements

Règle fondamentale :

La séparation ROUGE / NOIR est la base de l 'anticompromission électromagnétique

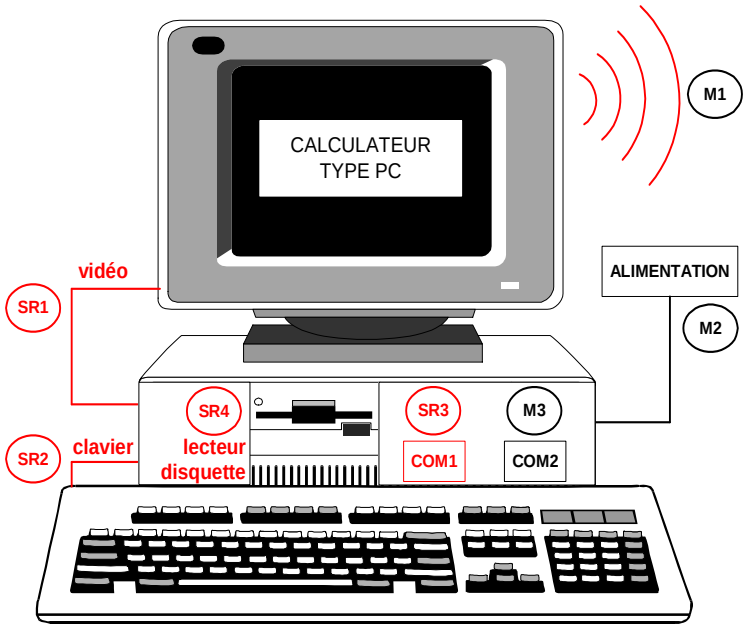
THALES

Les essais TEMPEST

Les essais TEMPEST :

- Essais de validation TEMPEST
  - Les essais sont effectués complètement sur le prototype selon la norme SDIP 27:
  - Nécessité d 'un **plan de test** définissant les signaux rouges à tester, les montages et les méthodes d'essais ainsi que la **matrice de test.**
  - Le Plan de Test doit être approuvé par l'organisme étatique (DCSSI, CELAR) chargé de la qualification
  - Les tests d 'émission en rayonné et en conduit sur les média sont effectués en cage de Faraday
  - On recherche une corrélation entre les signaux de sortie et les signaux rouges
  - Rédaction d'un **rapport de test**
- Essais de qualification TEMPEST
  - Les essais de qualification sont de la responsabilité l'organisme étatique (DCSSI ou CELAR)
  - L'agrément éventuel est prononcé par le DCSSI
- Essais de contrôle industriel (en production)
  - Essais effectués par prélèvement série
  - Reprise uniquement des essais « pertinents » repérés lors des essais de qualification

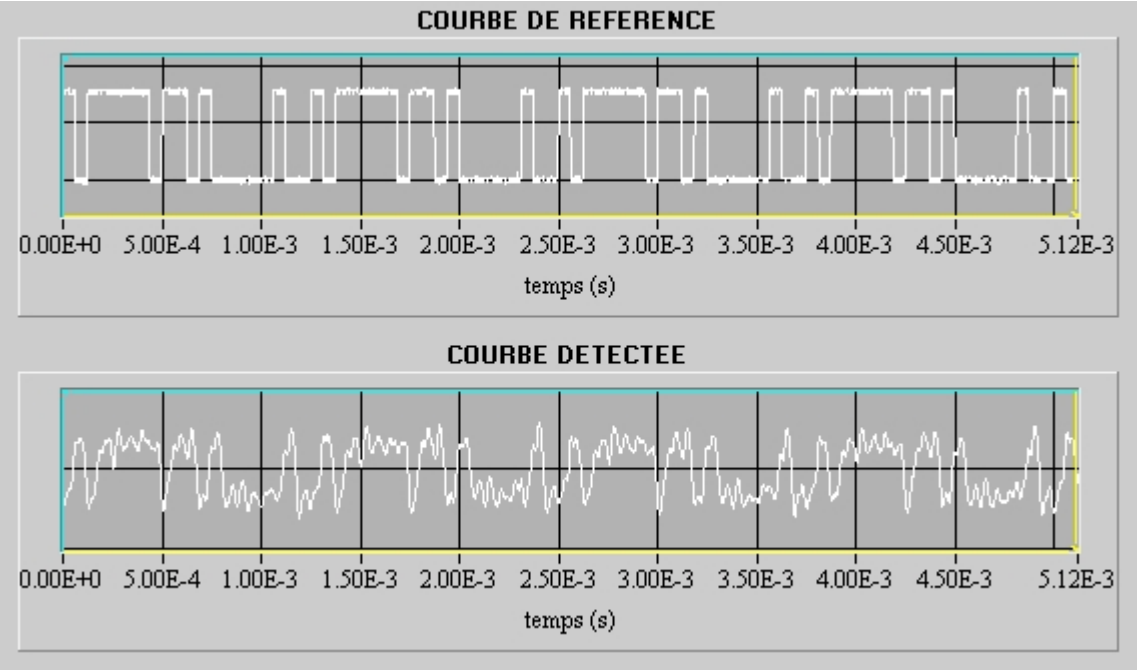
exemple de matrice de test



EQUIPEMENT SOUS TEST MATRICE DE TEST TEMPEST			MEDIAS DE TEST							
			Rayonnement E	Rayonnement M	Alimentation P1	Alimentation P2	COM2 ligne1	COM2 ligne2	COM2 ligne3	COM1 données
SR	1	vidéo	*	*	*	*	*	*	*	
	2	clavier	*		*	*	*	*	*	
	3	COM1	*	*	*	*	*	*	*	*
	4	disquette		*						

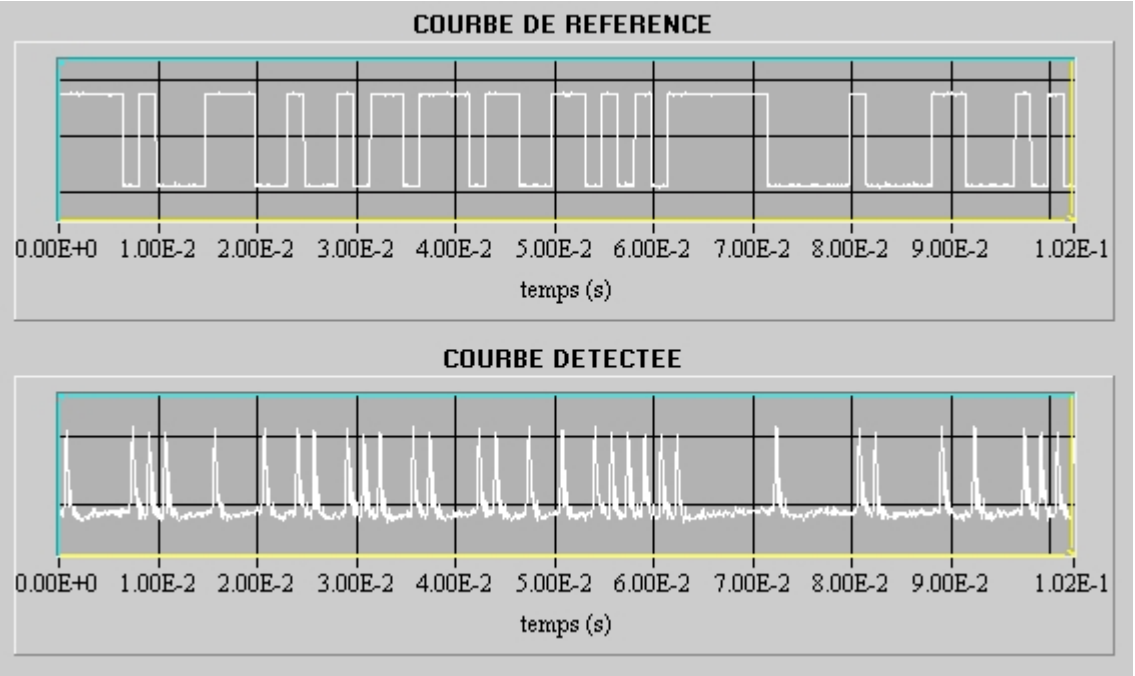
Exemple de signaux compromettants

- Bande de base:



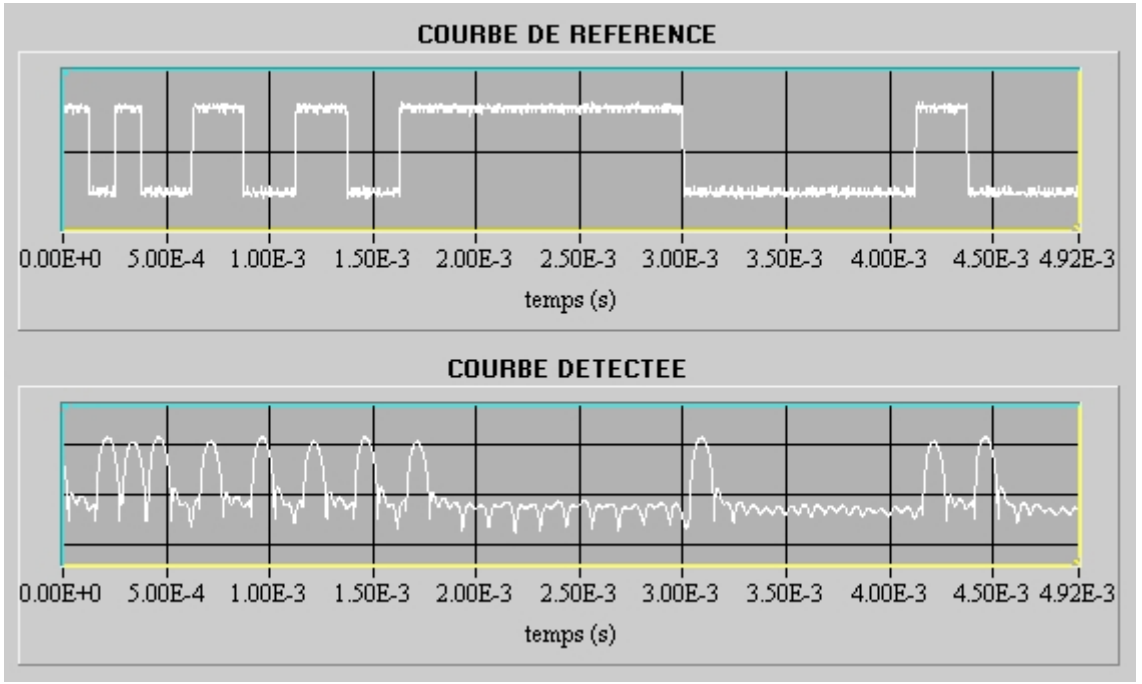
Exemple de signaux compromettants

- Dérivée redressée :



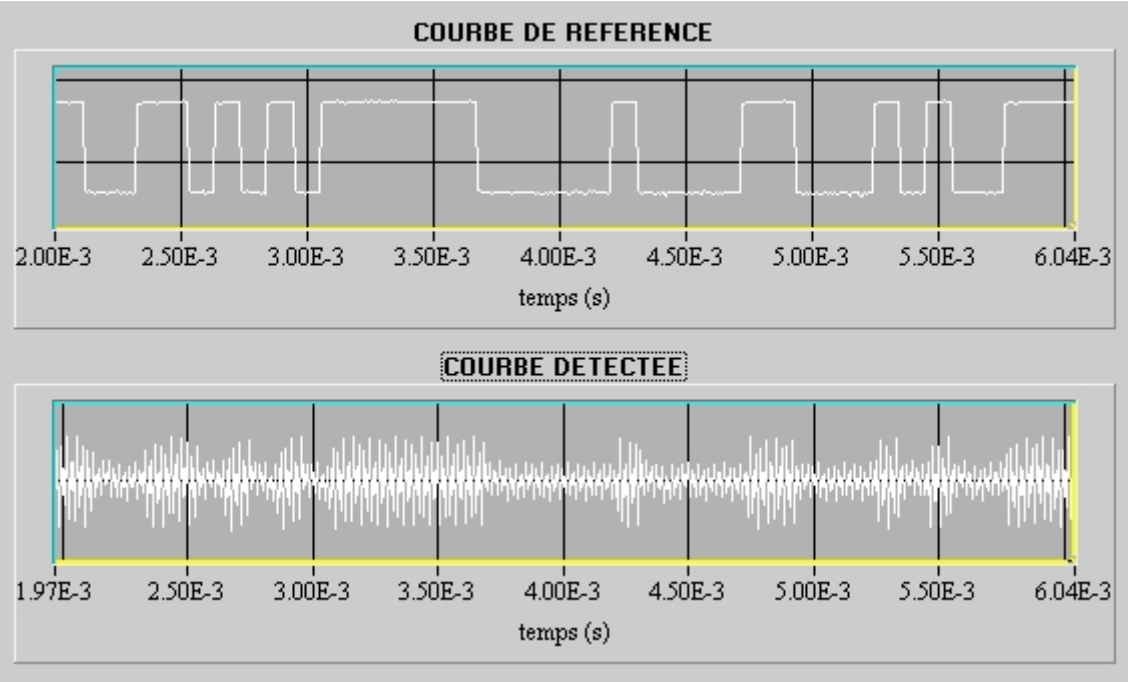
Exemple de signaux compromettants

- Dérivée redressée :



Exemple de signaux compromettants

- Modulation HF ou par horloge :



THALES

Les menaces connexes

« Anticompromission acoustique

Attaque proche:

Acoustique : écoute directe

écoute via des moyens électroniques

µ directif , accéléromètres

Attaque lointaine:

Acoustique : écoute via des moyens électroniques

µ directif, vibromètre laser

THALES

Anticompromission optique

Attaque proche

Optique : vision directe
moyens optiques courte portée
Longue vue courte portée

Attaque lointaine

Optique : moyens optiques longue portée
Longue vue, télescope

THALES

Tempest « Nouvelles technologies, nouvelles menaces »

Réseau CPL, WI-FI, bluetooth

⇒Désactiver impérativement les cartes Wi-Fi

Rayonnement des clés USB

⇒Utilisation clés USB blindées

⇒Lecteur protégé

En revanche:

⇒moins de risque pour les écrans plats versus les écrans CRT.

⇒Utilisation de plus en plus fréquente de Fibre Optique.

Avantage des nouvelles normes

Normes d'éco-conception:

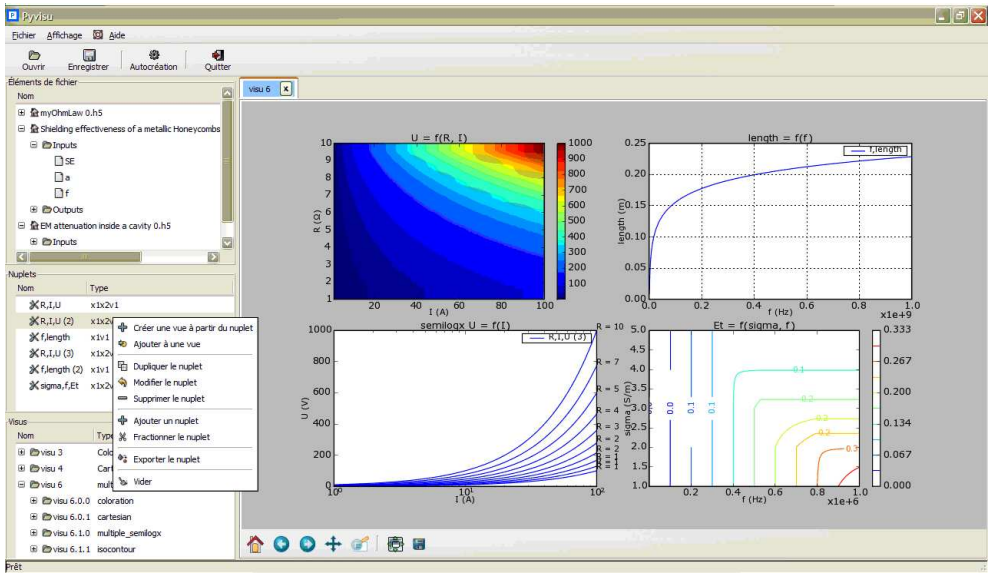
- **Les nouveaux standards d'économie d'énergie limitent la portée des SPC et obligent l'hostile à se rapprocher**

- **Meilleur rendement => limitation des perturbations rayonnées et des porteuses potentielles**

Les méthodes prédictives de détection des SPC

Des outils numériques d'aide à la conception prenant en compte des modèles physiques:

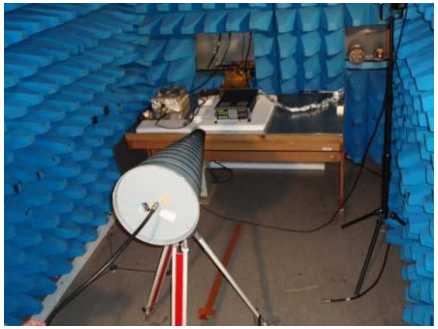
- Modèles de couplage
- Modèles de rayonnement des pistes
- Diffraction à travers les blindages
- Diaphonie des câbles et des connecteurs
- Modèles de propagation
- Prise en compte de critères normatifs



THALES

La validation des systèmes

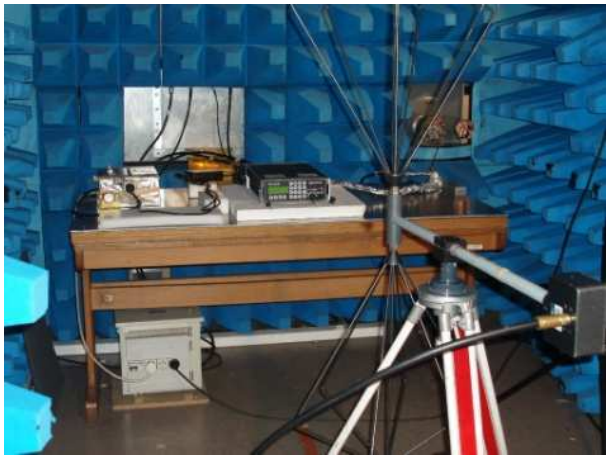
- **Mesure du risque résiduel sur installation:**
- **Tempest,**

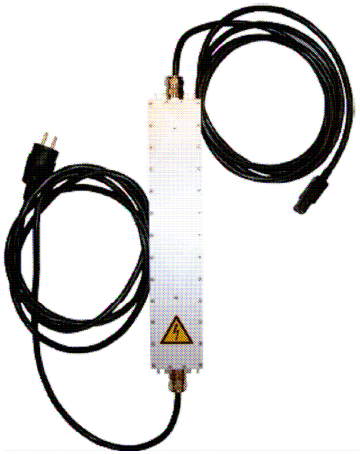


- **Anti compromission acoustique,**

- **Anti compromission optique**

Les réponses THALES





THALES

Conclusion

La menace Tempest est à prendre au sérieux,

Les règles Tempest sont à prendre en compte dans toutes les phases de développement du système:

Conception, fabrication, transport, installation, exploitation, maintenance, évolutions

L'anticompromission est une composante opérationnelle des systèmes d'information critiques, civils ou militaires.