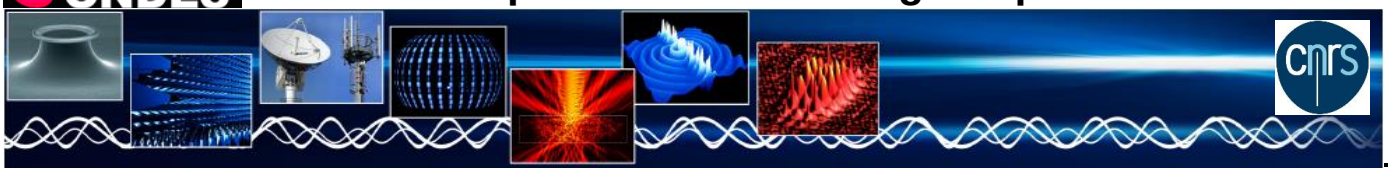
GDR ONDE – GT5 CEM
«Compatibilité ElectroMagnétique »



Journée thématique « Sécurité des systèmes électroniques et communicants »

GT 5 CEM	*Animateurs – organisateurs*	*Lieu*	*Date*
	Christophe Guiffaut, Christian Vollaire, Alexandre Boyer	Sorbonne Université Paris - Jussieu	Mardi 21 mai 2019

Objectifs :
La multiplication des systèmes autonomes, des objets connectés et des appareils mobiles communicants pose le problème de la sécurité des informations véhiculées, de la fiabilité à la fois matérielle et logicielle au-delà des garanties apportées par le cadre normatif. Les attaques intentionnelles et les écoutes illicites d'un système peuvent prendre plusieurs formes et s'appuyer sur des failles matérielles, utiliser des canaux auxiliaires backdoor (injection sur câble d'alimentation) ou frontdoor (émission rayonnée). L'objectif de cette journée est de réunir les communautés CEM et sécurité informatique des systèmes pour aborder conjointement cette thématique en fort développement. Elle s'adresse aux Doctorants, Post-Doctorants, Chercheurs et Enseignant Chercheur ainsi qu'aux Industriels.

Mots clé :
- Susceptibilité et Emissivité des systèmes et des composants, Immunité EM, Interférence EM, Intégrité du signal
- Techniques d'accès et de compromission d'information (ex : injection de fautes), attaques intentionnelles (déni de services), écoutes illicites, canaux auxiliaires, sécurité fonctionnelle
- Compromission des appareils mobiles, embarqués et PCs

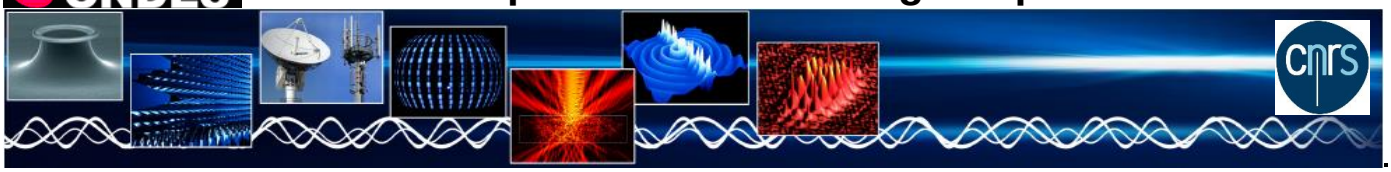
La journée fera l'objet de présentations invités et de présentations orales qui seront validées sur la base d'un résumé d'une à deux pages. Une table ronde discussion/débats clôtura l'évènement et ouvrira des perspectives.

Dates à retenir :
Soumission des résumés jusqu'au lundi 29 mars 2019.
Participation gratuite mais inscription **obligatoire** jusqu'au vendredi 12 avril 2019.

Les résumés et l'inscription seront transmis par e-mail aux animateurs du GT 5 :
alexandre.boyer@insa-toulouse.fr
christian.vollaire@ec-lyon.fr
christophe.guiffaut@xlim.fr

Comité de pilotage : Philippe Besnier, Pierre Bonnet, François Costa, Jean-Luc Schanen et les animateurs du GT5

GDR ONDE – GT5 CEM
«Compatibilité ElectroMagnétique »



Programme

8H20	**Accueil**	
8H45	**Session 1**	Chair : Christophe Guiffaut
8H45 – 10 mn	**Introduction**	Christophe Guiffaut, "*Présentation journée*"
8h55 – 30 mn	**Invité**	G. Camurati, "*Screaming Channels : quand un émetteur radio diffuse des canaux auxiliaires*"
9H25 – 20 mn		A. Rey "*Optimisation de l'évaluation et des tests de sécurité des systèmes cyber-physiques par analyse des canaux auxiliaires*"
9H45 – 20 mn		L. Morel and D. Couroussé, "*Idols with Feet of Clay: On the Security of Bootloaders and Firmware Updaters for the IoT*"
10H05 – 20 mn		L. Claudepierre, "*TRAITOR : a multi clock-glitch attack platform reproducing EMI effects at low-cost*"
10H25 – 15 mn	**Pause Café**	
10H40	**Session 2**	Chair : Christian Vollaire
10H40 – 30 mn	**Invité**	J. Lopes Esteves, "*Exemples d'interactions entre CEM et Sécurité de l'Information*"
11H10 – 20 mn		Virginie Deniau, Jonathan Villain, Eric Simon, Anthony Fleury, Christophe Gransart, "*Détection de cyber attaques sur réseau Wi-Fi par classification de données spectrales*"
11H30 – 20 mn		C. Marchand, "*Sécurité dans l'Internet des Objets : de la communication aux capteurs*"
11H50 – 20 mn		V. Houchouas, Y. Chatelon, E. Cottais, M. Darces, M. Hélier, J-L. Esteves "*Estimation statistique de couplages au sein de châssis d'équipements électroniques*"
12H15 – 1H30	**Déjeuner**	
13H50	**Session 3**	Chair : Pierre Bonnet
13H50 – 30 mn	**Invité**	P. Hoffmann, "La susceptibilité électromagnétique face aux agressions intentionnelles"
14H20 – 20 mn		L. Curos, T. Dubois, G. Mejecaze, F. Puybaret, J.-M. Vinassa, "Analyses de destructions d'alimentations soumises a des impulsions forts niveaux"
14H40 – 20 mn		S. Iben Jellal, S. Baranowski, M. Bocquet, "*Présentation d'un banc d'analyse du signal Zigbee confronté à des agressions électromagnétiques intentionnelles*"
15H00 – 20 mn		T. Dubois, G. Duchamp, "*Comportement d'une carte à base d'amplificateur opérationnel face à une perturbation électromagnétique de type impulsionnel modulé*"
15H20 – 15 mn	**Pause Café**	
15H35	**Session 4**	Chair : Philippe Besnier
15H35 – 30 mn	**Invité**	E. Nogues et J. Micolod, "*Analyses par canaux auxiliaires, Attaques en fautes, Tempest et signaux compromettants*"
16H05 – 20 mn		I. Junqua, J-P. Parmantier, W. Quenum, "*Couplages électromagnétiques haute fréquence dans des bâtiments – application des concepts de topologie électromagnétique et power balance*"
16H25 – 20 mn		J. Alaa Eddine, E. Pistono, F. Ndagijimana, "*Mesure de l'efficacité de blindage électromagnétique pour le blindage de bâtiments*",(G2Elab, RFICLab)
16H45 – 20 mn		A. Liakouti, K. El Khamlichi Drissi et C. Pasquier, "*Evaluation du rayonnement EM à l'aide d'une électronique embarquée*"
17H05 – 20 mn	**Discussion et Clôture**	Christophe Guiffaut et Christian Vollaire
17H25		

Description du lieu

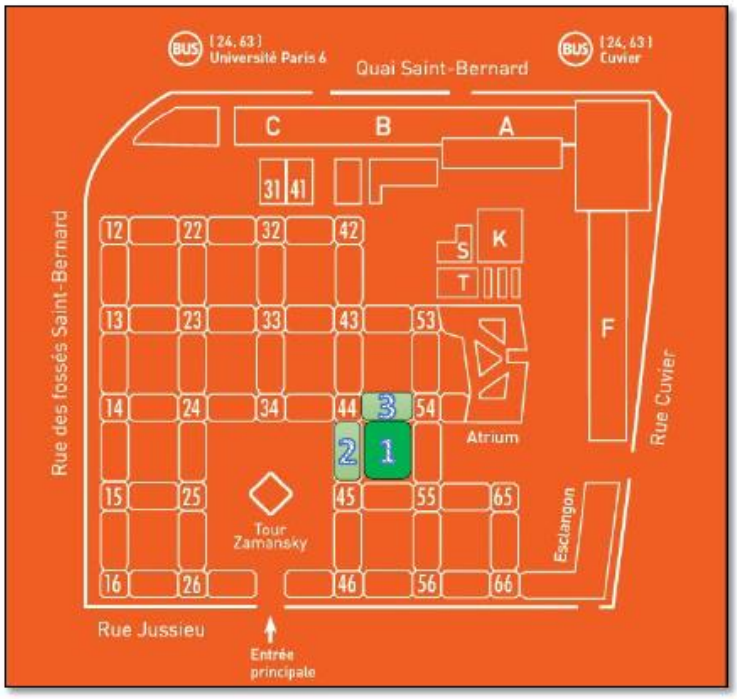
Centre international de Conférence Sorbonne Université (CISCU) – Paris

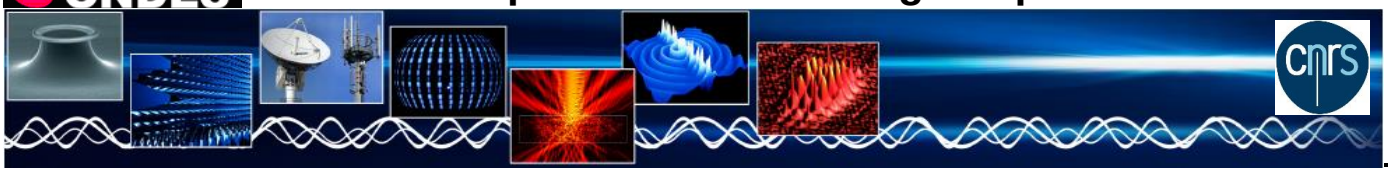
Le CISCU est situé au cœur du 5ème arrondissement de Paris, en plein centre du quartier latin, la salle 109 se trouve entre les tours 44 et 54 de l'Université de Sorbonne JUSSIEU au 1er étage avec Accès par la tour 44. Voir la position (3) sur la carte ci-dessous où sont indiquées les adresses des rues entourant le site. L'accès principale est rue Jussieu.

Le CICSU est desservi par de nombreux modes de transport :

Métro lignes 7 et 10 (arrêt Jussieu)

Bus lignes 89 et 67 (arrêt Jussieu), 24 et 69 (arrêt Université Paris VI), 86 et 87 (arrêt IMA ou Saint-Germain Cardinal Lemoine)





INVITES :

José Lopes Esteves , "*Exemples d'interactions entre CEM et Sécurité de l'Information*", Laboratoire sécurité des technologies sans-fil (ANSSI).

Patrick Hoffmann, "*La susceptibilité électromagnétique face aux agressions intentionnelles*", Laboratoire Microondes de Fortes puissances du CEA Gramat.

Giovanni Camurati, "*Screaming Channels : quand un émetteur radio diffuse des canaux auxiliaires*",.Laboratoire EURECOM, Nice.

Erwan Nogues et julien Micolod, "*Analyses par canaux auxiliaires, Attaques en fautes, Tempest et signaux compromettants*", DGA MI.

SESSION 1

Alexis Rey "*Optimisation de l'évaluation et des tests de sécurité des systèmes cyber-physiques par analyse des canaux auxiliaires*", CEA LETI.

Lionel Morel and Damien Couroussé, "Idols with Feet of Clay: On the Security of Bootloaders and Firmware Updaters for the IoT", CEA LIST, Grenoble.

Ludovic Claudepierre, "*TRAITOR : a multi clock-glitch attack platform reproducing EMI effects at low-cost*",. INRIA, Rennes.

SESSION 2

Virginie Deniau[1], Jonathan Villain[2], Eric Simon[3], Anthony Fleury[2], Christophe Gransart[1], "*Détection de cyber attaques sur réseau Wi-Fi par classification de données spectrales*", [1] IFSTTAR-COSYS, Villeneuve d'Ascq, [2] IMT Lille Douai, [3] Groupe IEMN-TELICE.

Cedric Marchand, "*Sécurité dans l'Internet des Objets : de la communication aux capteurs*", Ecole centrale de Lyon, Institut des Nanotechnologies de Lyon.

Valentin Houchouas[2], Y. Chatelon[1], E. Cottais[2], M. Darces[1], M. Hélier[1], J-L. Esteves[2] "*Estimation statistique de couplages au sein de châssis d'équipements électroniques*", [1] L2E Université Sorbonne, [2] ANSSI

SESSION 3

L. Curos [1], T. Dubois [2], G. Mejecaze [1,2] F. Puybaret [1], J.-M. Vinassa [2], "*Analyses de destructions d'alimentations soumises a des impulsions forts niveaux*", [1] : CEA, DAM, CEA-Gramat, [2] : Univ. Bordeaux, CNRS, Bordeaux INP, IMS UMR 5218, Talence.

Sara Iben Jellal[2], Sylvie Baranowski[1], Michael Bocquet[2], "*Présentation d'un banc d'analyse du signal Zigbee confronté à des agressions électromagnétiques intentionnelles*", [1] : DOAE, UMR 8520-IEMN, Université de Lille, Lille, [2] : DOAE, UMR 8520-IEMN, UPHF, Valenciennes.

Tristan Dubois, Geneviève Duchamp, "*Comportement d'une carte à base d'amplificateur opérationnel face à une perturbation électromagnétique de type impulsionnel modulé*", Laboratoire IMS / Université de Bordeaux, Talence.

SESSION 4

Isabelle Junqua[1], Jean-Philippe Parmantier[1], Wilfrid Quenum[1], "*Couplages électromagnétiques haute fréquence dans des bâtiments – application des concepts de topologie électromagnétique et power balance*", ONERA/DEMR, Université de Toulouse, Toulouse.

Jalal Alaa-Eddine[1], Emmanuel Pistono[2], Fabien Ndagijimana[1], "*Mesure de l'efficacité de blindage électromagnétique pour le blindage de bâtiments*", [1] Université Grenoble Alpes, laboratoire G2Elab, [2] Université Grenoble Alpes, laboratoire RFICLab.

Achraf Liakouti, K. El Khamlichi Drissi et C. Pasquier, "*Evaluation du rayonnement EM à l'aide d'une électronique embarquée*", Institut Pascal, Université Clermont Auvergne, UMR 6602, Clermont Ferrand.

Screaming Channels : quand un émetteur radio diffuse des canaux auxiliaires.

Aujourd'hui, il devenu courant d'avoir des applications électroniques qui nécessitent à la fois un microprocesseur et une radio pour des communications sans fil. Par exemple, on peut penser à une montre connectée qui communique avec un téléphone portable, par moyen d'un signal Bluetooth.

Très souvent ces objets utilisent des circuits intégrés à signaux mixtes, qui combinent un microprocesseur (numérique) avec un émetteur-récepteur radio (analogique/radiofréquence).

D'une part, les circuits à signaux mixtes ont de nombreux avantages, notamment en termes de coûts, surface, consommation, et facilité d'intégration dans d'autres produits. D'autre part, il est assez difficile de concevoir une puce dans laquelle le bruit généré par la partie numérique n'a pas d'effet dévastateur sur les performances radio. Un des problèmes majeurs est le couplage entre les deux parties, dû au fait qu'elles sont toutes les deux sur le même substrat de silicium. Des couplages peuvent apparaitre aussi au niveau du PCB ou de l'alimentation/masse.

Vue l'importance et la popularité de ce type de puces, ce sujet a été largement étudié. Cependant, la recherche a focalisé ses efforts sur les aspects fonctionnels, et non pas sur les conséquences au niveau de la sécurité des données.

Le bruit généré par les composants numériques, peut être corrélé a des données sensibles telles qu'une clef de chiffrement. Ce bruit peut se propager vers la partie analogique de la radio, où il est capté, amplifié, et transmis en radio, dans le bruit de la transmission légitime des données. Il devient donc possible d'écouter ces fuites à plusieurs mètres de distance, avec une simple radio logicielle et des techniques de démodulation adaptées. Cela constitue un nouveau type de canal auxiliaire, qu'on appelle « Screaming Channel », parce qu'il est caractérisé par une puissance assez élevée par rapport au fuites électromagnétiques conventionnelles. Celles-ci sont des émissions involontaires à très basse puissance, qui peuvent être exploitées seulement en proximité du circuit numérique, avec des sondes de champs magnétiques.

Nous démontrons cet effet « Screaming » sur une puce très populaire qui contient un processeur Arm Cortex-M4 et un émetteur-récepteur Bluetooth. Nous menons une attaque par canaux auxiliaire sur une implémentation logicielle du AES à 10m de distance en chambre anéchoïque, et à quelques mètres dans un environnement de bureau.

Il est impératif de considérer les canaux auxiliaires « Screaming » pendent la conception des nouvelles puces, et de développer des contremesures qui soient adaptée à ce type de circuit, pour lesquels le cout et la consommation de puissance sont primordiaux.

Exemples d’interactions entre CEM et Sécurité de l’Information

José Lopes Esteves
Laboratoire sécurité des technologies sans-fil
Agence nationale de la sécurité des systèmes d’information (ANSSI)

La compatibilité électromagnétique a pour objectif de définir un cadre pour que les équipements électroniques puissent fonctionner ensemble dans une sorte de “respect mutuel”. Les normes et procédures de test permettent de garantir des seuils maximums d’émissions électromagnétiques et de mettre en oeuvre des mesures permettant d’assurer un fonctionnement nominal dans ce cadre. En sécurité de l’information, un attaquant qui n’est pas tenu de respecter les normes et qui en connait les seuils peut être considéré. L’enjeu est alors de déterminer ce que peut obtenir cet attaquant, si il peut contourner des fonctions de sécurité implémentées par des équipements électroniques et dans quelles conditions.

Plusieurs évolutions technologiques participent à une augmentation de la vraisemblance de l’exploitation des effets d’interactions électromagnétiques sur des équipements électroniques pour porter atteinte à la sécurité de l’information traitée par ces équipements. Du point de vue des cibles, la miniaturisation, l’augmentation des fréquences de fonctionnement, la diminution de la marge de bruit semblent annoncer des difficultés de limiter l’émissivité et la susceptibilité des équipements. Du point de vue de l’attaquant, la démocratisation de moyens permettant de collecter et traiter des signaux parasites et de développer des sources de signaux agiles en vue de pertuber les cibles contribue à une diminution du profil d’attaquant, c’est à dire des moyens et des connaissances dont il doit disposer pour réaliser une attaque.

Cette présentation s’appuiera sur plusieurs exemples d’attaques exploitant des phénomènes de CEM pour porter atteinte à la sécurité de l’information afin de mettre en évidence les relations entre l’émissivité des équipements et les menaces pour la confidentialité qui peuvent en découler et réciproquement entre la susceptibilité et les impacts potentiels sur l’intégrité et la disponibilité de l’information traitée.

La susceptibilité électromagnétique face aux agressions intentionnelles

Patrick Hoffmann

Ingénieur-Chercheur au laboratoire Microondes de Fortes puissances du CEA Gramat[1]

Le CEA Gramat a développé, depuis de nombreuses années, une expertise sur la vulnérabilité des systèmes électroniques face à des menaces électromagnétiques, qu'elles proviennent d'une impulsion créée par l'interaction d'une explosion nucléaire haute altitude (IEMN-HA[2]) avec les couches de l'atmosphère ou d'une arme électromagnétique puissante. Ce dernier domaine recouvre un ensemble de types de signaux électromagnétiques parfois différents, parfois similaires mais sous des dénominations diverses, qu'il est parfois difficile d'appréhender. Le CEA Gramat a structuré ses travaux relatifs à cette partie en 3 sous-domaines de signaux électromagnétiques, ayant tous en commun, la capacité à altérer temporairement ou définitivement les structures électroniques qu'ils rencontrent :

1. les AED EM (Armes à Energie Dirigée ElectroMagnétiques) qui recouvrent :
    - l'étude de l'efficacité des signaux provenant de sources électromagnétiques à des fins militaires
    - l'étude de la vulnérabilité des systèmes opérationnels vis-à-vis de ces mêmes sources.
2. les AGREMI (AGressions ElectroMagnétiques Intentionnelles) axées sur l'étude de la sécurité des équipements électroniques présents dans des systèmes ou infrastructures civils vis-à-vis de signaux issus de sources électromagnétiques de même nature que celles du point précédent.
3. les transitoires rapides qui regroupent tous les signaux électromagnétiques impulsionnels, engendrés par des sources électriques, et provoquant des dysfonctionnements des équipements électroniques situés à proximité. Cette partie est un sous-domaine de la CEM (Compatibilité ElectroMagnétique).

Les travaux relatifs à l'altération potentielle, occasionnée par ces signaux sur l'électronique, sont regroupés dans le domaine général de la susceptibilité électromagnétique. Le présent travail a pour vocation de présenter la méthodologie d'identification de cette susceptibilité électromagnétique appliquée aux AGREMI. La manière d'aborder cette notion de susceptibilité est caractérisée par l'absence de normalisation des signaux vulnérants, puisque, par nature, ils s'adaptent aux failles détectées dans les systèmes électroniques. La méthodologie, appliquée à l'étude de la susceptibilité électromagnétique, est ici limitée aux agressions par conduction. Nous considèrerons, que la partie antennaire des systèmes « frontdoor[3] » est traitée séparément et que les niveaux de puissance AGREMI maintiennent ces antennes dans le régime linéaire. Le signal incident pris en compte est donc celui parvenant à la base d'une antenne de réception. Pour les systèmes « backdoor[4] », nous

---

[1] Commissariat à l'Energie Atomique et aux Energies Alternatives Centre de Gramat (CEA, DAM, CEA Gramat, F-46500 Gramat, France))

[2] Impulsion ElectroMagnétique d'origine Nucléaire Haute Altitude

[3] Systèmes électroniques dont les voies de couplage AGREMI sont uniquement les voies antennaires

[4] Systèmes électroniques dont les voies de couplage AGREMI sont toutes les parties métalliques hormis les antennes

considèrerons que le signal vulnérant est parvenu, par couplages successifs, jusqu'à l'entrée des composants électroniques présents sur les cartes imprimées. Les grandeurs permettant de relier les caractéristiques de susceptibilité des deux types de systèmes au signal AGREMI rayonné sont l'aire efficace d'antenne (A_e) pour les systèmes frontdoor et la section efficace de couplage (σ_e) pour les systèmes backdoor. Ces deux termes ont la même définition, soit le rapport, dans une direction donnée, entre la puissance maximale disponible à la réception (à la base de l'antenne pour A_e et sur la broche d'un composant pour σ_e) et la densité de puissance incidente.

Ces bornes techniques, pour la présentation, ayant été posées, intéressons-nous aux principes de la méthodologie permettant d'accéder à la susceptibilité électromagnétique. L'idée maîtresse est de chercher à lier chaque caractéristique de la forme temporelle du signal AGREMI (appelons les β_k) aux caractéristiques de susceptibilité des structures électroniques (α_i). Le signal AGREMI n'étant pas normalisé, nous cherchons à établir une expression analytique de ce signal la plus générique possible (pour un signal ne possédant qu'un ton par impulsion) :

Équation 1

$$AGREMI(t) = \sum_{k=1}^{N} A_k \cdot \varphi_k\left(\frac{t-kT-\tau_k}{\Delta_k}\right) \cdot m_k(t-kT) \cdot sin\big(\omega_k(t-kT) + \theta_k + \phi_k(t)\big) = f[\beta_k(t)]$$

Le signal étant impulsionnel, l'indice k représente le numéro d'impulsion ; φ_k, Δ_k, m_k, ϕ_k représentent respectivement l'enveloppe de l'impulsion (une porte trapézoïdale par exemple), sa durée, le signal modulant éventuel et la modulation de phase, pour les caractéristiques β_k les moins intuitives. Cette expression, qui n'est probablement pas définitive, permet de traiter analytiquement, les fonctions de transfert des parties linéaires de la chaîne de susceptibilité et d'appréhender temporellement le comportement non-linéaire des parties semi-conductrices actives et l'influence des caractéristiques β_k sur ces non-linéarités. Expérimentalement, cette expression est programmée dans un générateur de formes arbitraires, entrée de l'amplificateur de puissance dont la sortie préfigure le signal AGREMI. La démarche expérimentale ou théorique consiste alors à chercher les lieux de susceptibilité (α_i) dans la structure électronique étudiée. A une certaine configuration des paramètres β_k, que nous appellerons la forme d'onde, nous associons un type de susceptibilité permettant d'alimenter une matrice de vulnérabilité entre formes d'onde et famille de cibles électroniques. Nous illustrerons cette démarche dans deux études réalisées au CEA Gramat dans le cadre de thèses (Pouant, 2015) et (Girard, 2018).

Nous conclurons par une introduction à la plateforme d'étude de la susceptibilité électromagnétique des chaînes de réception radiofréquences, CALYPSO, développée au CEA Gramat et par des perspectives de travaux collaboratifs avec des laboratoires universitaires.

Girard, Maxime. 2018. *Recherche de vulnérabilité des étages de réception aux agressions électromagnétiques de fortes puissance : cas d'un LNA AsGa.* Université de Bordeaux. 2018. Thèse.

Pouant, Clovis. 2015. *Caractérisation de la susceptibilité électromagnétique des étages d'entrée de composants électroniques.* Université de Montpellier. 2015. Thèse.

Optimisation de l'évaluation et des tests de sécurité des systèmes cyber-physiques par analyse des canaux auxiliaires

Alexis Rey

Le fonctionnement d'un système embarqué dépend de plus que son logiciel (plateforme matérielle, environnement d'exécution). Par conséquent, la sécurité des informations traitées par ces systèmes doit être évaluée selon plusieurs aspects :

- le code source est analysé de manière statique pour détecter des vulnérabilités issues du logiciel lui-même
- le système en fonctionnement est scanné pour vérifier l'absence de vulnérabilités connues
- il est ensuite soumis au *fuzzing*, qui consiste à envoyer des entrées innatendues voir invalides en grand nombre pour potentiellement déclencher un bug

Avec l'augmentation de la taille et de la complexité des systèmes logiciels, le fuzzing trivial s'est vite révélé inefficace. Il est donc nécessaire de guider le fuzzer pour qu'il puisse converger vers d'éventuelles fautes (ou parcourir le flot de contrôle du logiciel) plus rapidement.
Ma thèse porte sur l'optimisation de ce type de tests de sécurité, grâce aux informations contenues dans les canaux auxiliaires physiques (temps de réaction, variations de consommation, rayonnements électromagnétiques). Mon but est d'extraire des canaux auxiliaires de l'information sur le flot de contrôle du logiciel embarqué, pour que le fuzzer puisse associer un score à chaque entrée soumise au système testé.

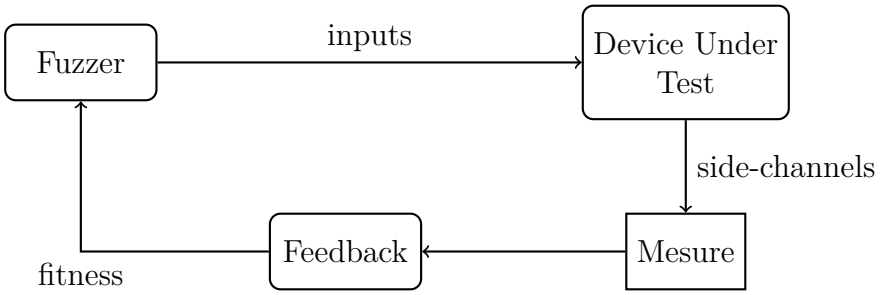


FIGURE 1 – Fuzzing asissté par canaux auxiliaires

Le fuzzer en tant que tel doit faire muter les entrées à soumettre au DUT, en ayant connaissance de « l'impact » des précédentes entrées testées. Le test doit donc inclure une rétroaction entre le DUT et le fuzzer, qui :

- analyse les acquisitions numériques des signaux des canaux auxiliaires
- actualise sa connaissance du flot de contrôle du logiciel embarqué
- produit un score (fitness) relatif à chaque entrée testée à l'aide du modèle interne du flot de contrôle

Le CFG du logiciel embarqué est modélisé par une chaîne de Markov, dont chaque état représente une portion du code exécuté (du *basic block* à la fonction). Les probabilités de transition représentent donc la probabilité pour le logiciel d'effectuer (ou non) un saut.

La rétroaction a deux rôles :

- actualiser périodiquement le modèle du CFG, soit le nombre d'états apparents de la chaîne de Markov et sa matrice de transition
- comparer chaque acquisition avec le modèle pour en déduire le chemin suivi le plus probable, et utiliser cette probabilité en tant que score pour le fuzzer

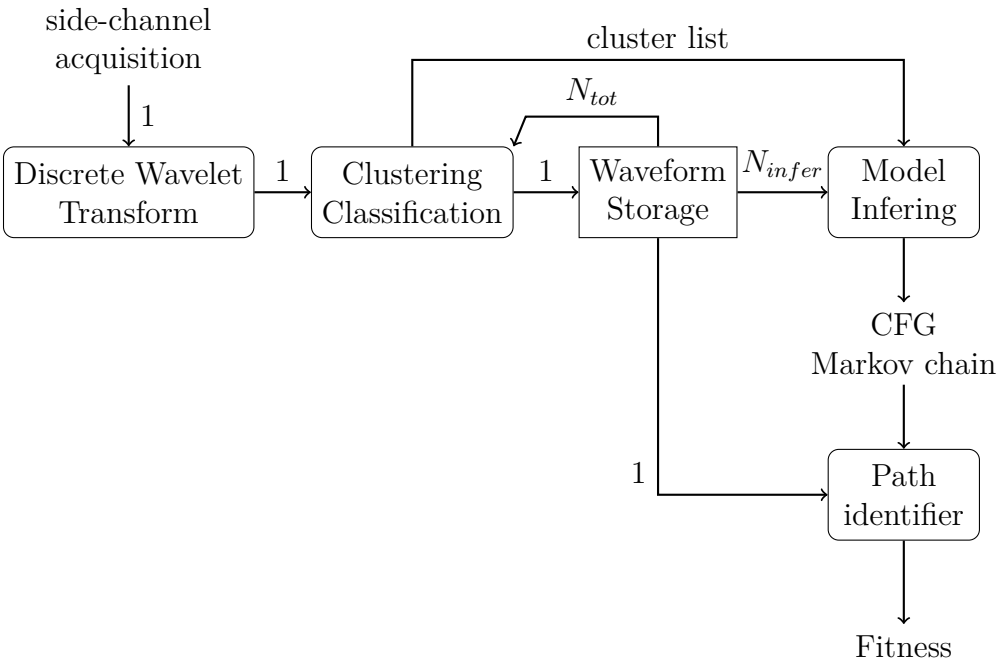


FIGURE 2 – Architecture globale de la rétroaction

L'acquisition est effectuée entre la soumission de l'entrée mutée au système, et sa réaction. Chaque acquisition réalisée subit préalablement une transformée par ondelettes discrètes, pour deux raisons :

- représenter le signal sur un espace temps-échelle, permettant d'analyser les signatures fréquentielles des instructions tout en les localisant dans le temps
- effectuer un filtrage du bruit par réduction des coefficients de faible amplitude

Chaque acquisition traitée est ensuite classifiée sur des clusters « artificiels », dont les labels n'ont pas de signification réelle. Cela permet de trier les acquisitions, chacune correspondant à un chemin d'exécution particulier, selon plusieurs critères (durée, coefficients d'ondelettes...).
Les clusters sont périodiquement redéfinis pour inclure les acquisitions qui n'auraient pas pu être classées.

Lorsque suffisamment de données issues de clusters différents ont été acquises, le modèle du CFG est actualisé à l'aide d'une inférence bayésienne en 2 étapes :

- un premier réseau bayésien actualise la distribution de probabilité connue sur le nombre d'états N_s de la chaîne de Markov
- le nombre d'états le plus probable est choisi
- une deuxième inférence (sous la forme de l'algorithme de Baum-Welch), retrouve la matrice de transition de la chaîne de Markov connaissant N_s

Enfin, chaque acquisition est comparée au modèle pour pouvoir extraire la probabilité du chemin d'exécution qui semble avoir été suivi.

Les chemins les plus probables étant ceux qui ont été spécifiés, il est plus intéressant pour le fuzzer d'explorer les chemins les moins probables qui ont plus de risques de déclencher des fautes.

Idols with Feet of Clay: On the Security of Bootloaders and Firmware Updaters for the IoT

Lionel Morel and Damien Couroussé

February 15, 2019

1 Abstract

IoT devices are generally implemented with low-cost embedded solutions, and connectivity and communication capabilities are the raison d'être of such devices. But this is also a double-edged sword, since connectivity also implies (1) to open the door to more attacks possibilities, (2) and the targeted system, once breached, can be the support for attacks at a larger-scale, possibly involving many connected systems.

Our observation is that, nowadays, such IoT devices lack proper hardware and software security protections. Bootloader and Firmware Update (BFU) mechanisms are critical components in the software stack of IoT devices. The BFU are particularly sensitive since they need the highest privileges possible on the platform to setup the system. As such, an attacker able to compromise the BFU can gain a full control over the target system. Moreover, the update mechanism often supported by the BFU is essential to ensure devices can be upgraded and maintained for a long time. If not properly secured, the BFU would allow an attacker to gain control over a system throughout its whole lifetime, including future upgrades.

In this presentation, we provide an overview of the threats targeting BFUs, and existing protections. We cover the hardware and software attacks that are known to the scientific literature. Also, we argue that vulnerabilities to physical attacks, in particular to fault injection attacks, are mostly left un-attended.

TRAITOR : a multi clock-glitch attack platform reproducing EMI effects at low-cost.

Ludovic Claudepierre
INRIA

F-35000 Rennes, France
ludovic.claudepierre@inria.fr

I. Introduction

Fault-injection is a well-known method to physically attack an embedded system and particularly the microncontrollers of this equipment. Such an attack aims to find and exploit vulnerabilities of the hardware part to induce malfunction in the software part and at the end bypass software security or retrieve sensitive information. The Electromagnetic injection (EMI) has the advantages of being non-invasive and having reproducible effects. Nevertheless, the complex and expensive test-bench makes it hard to implement. During experiments, it has been exposed that EMI has a strong impact on the clock signal of the microcontroller. This lead us to create a cheaper platform called TRAITOR inducing fault by clock glitch with similar effects than EMI.

II. Electromagnetic injection : technique and effects

In Figure 1, an example of EMI test-bench is given. It is composed of a generation chain with a Keysight 33509B pulse generator, a Keysight 81160A signal generator and a Milmega 80RF1000-175 power amplifier. This signal is radiated through a Langer R0.3-3 probe located just above the surface of the chip. The microcontroller targeted in this study is the STM32F100RB, embedding an ARM-cortex-M3 core running at 24 MHz.

Such a method of injection requires a lot of parameters to tune in order to improve the efficiency of EMI (probe location, shape of the radiated wave, time location of the injection). Moreover, it has to face physical and material limitations such as coupling efficiency, clock jitter, and sensitivity of a targeted instruction.

Fig. 1: Test bench for fault attacks by electromagnetic injection.

All along the experiments it has been possible to conclude in the vulnerability of Phase-Locked Lopp (PLL). Indeed, it has been observed that EMI strongly disrupts the clock signal (Figure 2). Furthermore, the most susceptible location to EMI on the chip corresponds to the analog peripheral feeding (including the PLL). Finally, when the PLL is disabled and the chip clock is directly plugged to the crystal, the fault rate induced by EMI is close to zero.

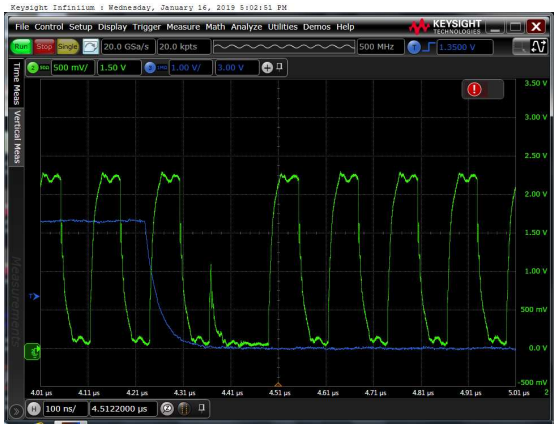


Fig. 2: Clock glitch due to electromagnetic injection.

III. TRAITOR : Reproducing EMI effects by clock control

The platform called TRAITOR consists in reproducing the clock disruption observed during EMI with the ability of duplicate it at any clock edge to fault several targeted instructions and achieve complex attacks. The platform is far cheaper than EMI test-bench and is easy to implement. As the TRAITOR replaces the clock signal by its own, the attacker is free of physical limitation met during EMI. The multiple fault capability of this platform makes the attacker able to bypass the usual counter-measures to single-fault attacks and in particular the double PIN verification. Furthermore, this type of attack can completely edit a program at run-time and, from a standard piece of code, make it malicious. We note that the amplitude of the glitch can also be monitored in order to change the effect on the instruction.

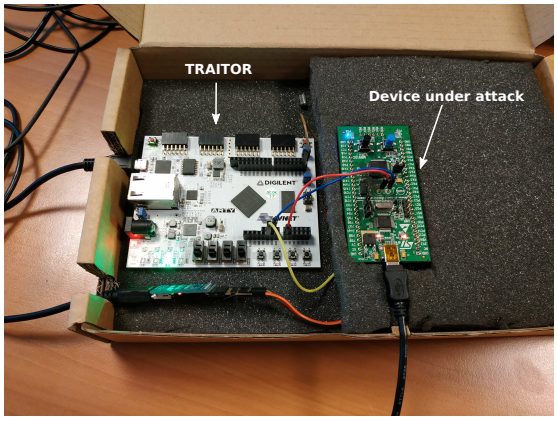


Fig. 3: TRAITOR platform with the targeted chip (STM32).

IV. Conclusion

Electromagnetic injection is a non-invasive way to attack a chip which requires expansive furniture and with a lot of parameters to be tuned to reach the best efficiency. This EMI affects the clock signal of the chip inducing glitches. TRAITOR is a light and cheap platform proposed to reproduce these clock glitches on a targeted microcontroller. This platform makes the attacker able to produce multi-fault on a program at run-time and so retrieve sensitive information (cryptographic key) or active back-doors.

Acknowledgment

This work has been carried out in collaboration with IETR.

Détection de cyber attaques sur réseau Wi-Fi par classification de données spectrales

Virginie Deniau[(1)], Jonathan Villain[(2)], Eric Simon[(3)], Anthony Fleury[(2)], Christophe Gransart[(1)]

(1) IFSTTAR-COSYS, Villeneuve d'Ascq, France, (2) IMT Lille Douai, France, (3) Groupe IEMN-TELICE, Université de Lille, France

Résumé :

Dans de nombreux domaines, les réseaux de communication ou informatiques comportent à la fois des sections filaires et sans fil. Ici, on s'intéresse à la partie sans fil qui peut être victime d'attaques ciblées, visant du déni de service en empêchant la bonne réception des signaux de communication ou bien des attaques « man-in-the-loop » visant à intercepter des informations. Dans cette communication, nous présentons des travaux qui se basent sur l'analyse de l'activité électromagnétique pour détecter de telles attaques sur un réseau Wi-Fi IEEE 802.11n. L'approche repose sur l'analyse de données spectrales par technique de classification.

Introduction :

Les réseaux de communication Wi-Fi sont aujourd'hui largement déployés dans les espaces publiques, personnels ou professionnelles. Ainsi, pour les hackers, ils représentent des moyens d'accès à certaines informations qui permettront ensuite d'organiser des attaques plus ciblées ou avec une meilleure réussite. Dans certains secteurs professionnels, les réseaux Wi-Fi sont également employés pour des applications opérationnelles, souvent liés à de la maintenance et de simples attaques par déni de service peuvent engendrer des conséquences immédiates. Ainsi, l'objectif de nos travaux est de détecter ces attaques au moment où elles s'exécutent.

Les scénarios d'attaque étudiés correspondent à des attaquants qui utiliseraient des brouilleurs pour provoquer un déni de service ou qui émettraient des trames de dé authentification pour déconnecter un client d'un point d'accès licite. L'attaquant peut chercher à bénéficier de l'ensemble de la ressource Wi-Fi ou, chercher à connecter le poste client à un point d'accès illicite et ainsi intercepter ses données privées. L'attaque par trames de dé authentification est une attaque protocolaire. Dans ce travail, nous souhaitons développer une approche capable de détecter et de distinguer les attaques par brouillage et les attaques protocolaires.

Mises en œuvre des attaques par brouillage et par trames de dé authentification

L'attaque par brouillage consiste à émettre intentionnellement un signal qui couvre les fréquences utilisées par le système de communication afin de dégrader la qualité du signal reçu par un dispositif de communication. Les signaux de brouillage sont des interférences électromagnétiques intentionnelles (IEMI) relativement peu puissantes qui dégradent les performances des réseaux de communication sans les endommager. Différents types de signaux de brouillage peuvent être utilisés [1]. La majorité des brouilleurs commerciaux génère un signal qui balaye de manière répétée une bande de fréquence [f_1, f_2] dans une durée T. Ce type de signaux peut être exprimé par:

$$s(t) = A\cos\left(2\pi\left(\frac{f_2 - f_1}{2T}t + f_1\right)t\right), \quad 0 < t < T, \quad (1)$$

où A est l'amplitude du signal d'interférence. Dans notre étude, le signal de brouillage balaie la bande de fréquences 2,4 GHz à 2,5 GHz dans un intervalle de temps $T = 10\ \mu s$.

L'attaque par trames de dé authentification utilise des trames définis dans la norme IEEE 802.11. Dans un réseau composé de plusieurs points d'accès(AP), lorsqu'un poste client se déplace il peut se trouver déconnecté d'un AP et reconnecté à un autre. Si le client est connecté à un AP et s'en éloigne, la puissance du signal Wi-Fi reçu diminue et il peut également détecter le signal de balise Wi-Fi d'un autre AP avec une puissance croissante. Dans ce cas, une procédure d'itinérance est lancée. Elle consiste à déconnecter le client du premier AP et à le reconnecter au second AP à l'aide des trames d'authentification et de dé authentification IEEE 802.11. L'attaque par dé authentification envoie à un poste client une trame de dé authentification même si celui-ci ne se déplace pas.

Pour nos travaux, ces attaques ont été mises en œuvre en chambre anéchoïque pour ne pas perturber les réseaux environnants. Un canal Wi-Fi de 20 MHz centré à la fréquence 2.412 GHz a été utilisé. Des acquisitions spectrales de 20 MHz de largeur centrées à la fréquence 2.412 GHz, ont été effectuées au cours des attaques. Les attaques par brouillage ont été mises en œuvre avec trois niveau de puissance : une puissance faible rendant le signal de brouillage totalement inefficace, une puissance intermédiaire créant une légère baisse de débit et une puissance mettant le système Wi-Fi en limite d''interruption.

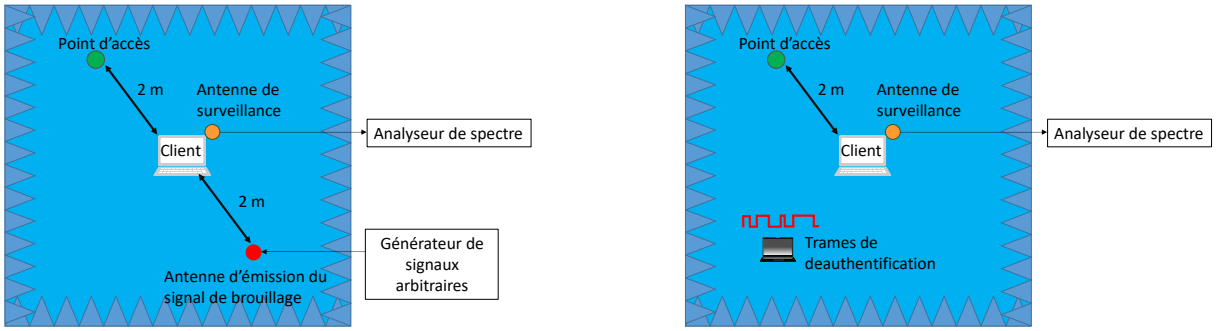


Figure 1 : Expérimentations d'attaques par brouillage (à gauche) et par dé authentification (à droite)

L'analyse en composantes principales sur les données des spectres

La classification des données est réalisée en déterminant préalablement les relations qui lient des variables explicatives, c'est-à-dire des grandeurs observées (Ici les spectres collectés pendant les attaques) à un critère que l'on cherche à classer (le type d'attaque). Une étape préalable est d'étudier les profils que l'on souhaite identifier. Dans cette étude nous voulons identifier 6 profils: une communication Wi-Fi sans attaque, une dégradation des performances en plaçant des matériaux absorbants autour de l'AP, 3 différentes puissances de brouillage et une attaque par dé authentification [2].

Une analyse en composantes principales (ACP) sur les données des spectres (ici 99 spectres par profil) met en avant la différence entre ces profils afin de vérifier si les différentes classes peuvent être séparées [3]. A l'issue de l'ACP, les spectres sont projetés dans un nouvel espace à partir des composantes associées aux vecteurs propre. Le plan vectoriel, représenté figure 2, associé aux 2 vecteurs propre possédant les valeurs propres les plus élevées, représente 95,17% de la variabilité des spectres.

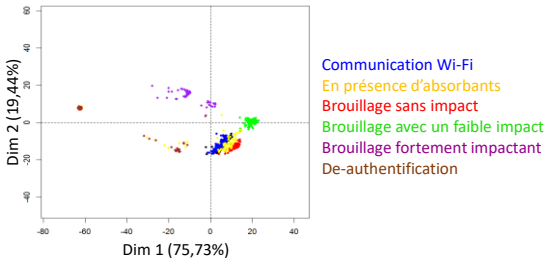


Figure 2 : Représentation des spectres en fonction des deux premières composantes de l'ACP

On observe sur ce plan (Figure 2) que l'attaque par dé authentification est pour partie bien séparée des autres classes. Ce résultat est intéressant car la nature du signal d'attaque par dé authentification n'est pas différente d'une communication normale. Néanmoins, une partie des spectres se positionnent dans un espace bien séparé de celui de la communication Wi-Fi seule. Nous observons également une bonne séparation des situations de brouillage fort et modéré. Ce résultat est encourageant pour développer une approche de détection capable de distinguer différents types d'attaques. Au cours de la présentation ces différents résultats seront analysés en détail.

[1] V. Deniau, C. Gransart, G. L. Romero, E. P. Simon, and J.Farah, IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals, IEEE Transactions on EMC, vol. 59, no. 5, pp. 1625-1633, 2017.
[2] J. Villain ; V. Deniau ; A. Fleury ; E. P. Simon ; C. Gransart ; R. Kousri, EM Monitoring and Classification of IEMI and Protocol-Based Attacks on IEEE 802.11n Communication Networks, IEEE Transactions on Electromagnetic Compatibility, 2019 , Early Access.
[3] S. Wold, K. Esbensen, and P. Geladi, Principal component analysis, Chemometrics and intelligent laboratory systems, vol. 2, no. 1-3, pp.3752, 1987.

Sécurité dans l'Internet des Objets : de la communication aux capteurs

Résumé :

L'Internet des Objets (IoT) est aujourd'hui un écosystème bien connu dans lequel des objets plus ou moins intelligents communiquent au travers d'un réseau de communication. Le nombre d'objets connectés augmente depuis des années à une vitesse impressionnante passant d'environ 500 millions en 2016 à plus de 6.5 milliards en 2018. A ce rythme, il y aura 6 fois plus d'objets connectés que d'habitant sur terre en 2025. En conséquence, le nombre de données récoltées et transmises devient énorme et selon les applications, ces données peuvent être sensibles et nécessiter d'être protégées. Cependant, il ne faut pas oublier que la première contrainte dans ce contexte concerne la consommation énergétique des systèmes électronique mis en place. Il apparaît que combiner la sécurité et la consommation d'énergie est un grand challenge auquel il faut répondre dans le contexte de l'IoT.

Concernant ces aspects de sécurité, un certain effort a été effectué afin d'identifier les challenges et les risques d'un manque de sécurité dans l'IoT mais aussi afin d'améliorer la sécurité des protocoles de communications. Il est également possible de trouver des solutions proposant d'ajouter un accélérateur matériel permettant d'ajouter un certain niveau de protection des données récoltées sur les nœuds de capteurs, avant qu'elles ne soient envoyées sur le réseau. Malheureusement, ce type de solutions augmente à la fois la surface et la consommation d'énergie des nœuds de capteurs. Dès lors, il est nécessaire de trouver de nouvelles solutions, permettant si possible d'amener la sécurité au plus proche des capteurs.

Nous allons donc, dans un premier temps, passer en revue l'ensemble des solutions actuellement proposées afin d'améliorer la sécurité de l'Internet des objets depuis la communication jusqu'au nœud de capteurs. Puis, nous aborderons une direction possible au travers d'une brève présentation des activité de recherche démarrant au sein du Laboratoire des Nanotechnologie de Lyon autour d'un nouvel axe visant à intégrer les technologie émergent développé dans des systèmes hétérogènes complexe pour combiner la sécurité et la consommation d'énergie dans l'Internet des objets.

Estimation statistique de couplages au sein de châssis d’équipements électroniques

Contact: Valentin Houchouas
Inspecteur de l’Agence nationale de la sécurité des systèmes d’information (ANSSI)
Doctorant à Sorbonne Université (laboratoire d’électronique et électromagnétisme, L2E)

Travaux réalisés avec:
Yves Chatelon (L2E)
Emmanuel Cottais (ANSSI)
Muriel Darces (L2E)
Marc Hélier (L2E)
José Lopes Esteves (ANSSI)

La sécurité électromagnétique (SE) peut être considérée comme la réunion de la compatibilité électromagnétique (CEM) et de la sécurité des systèmes d’information (SSI). L’étude de la SE d’équipements peut amener à considérer les couplages (électromagnétiques ou électriques) entre systèmes. En effet, si un signal portant une information sensible se couple sur un autre système, il existe un risque que la diffusion de l’information ne soit plus maîtrisée (perte de confidentialité de l'information). Il existe aussi le risque qu’un équipement perturbe un autre équipement et l’empêche de fonctionner correctement (perte de la disponibilité ou de l’intégrité de l’information).

Il est commun de trouver des équipements électroniques et informatiques placés dans des châssis métalliques assurant un blindage électromagnétique qui permet de maintenir un bon niveau de compatibilité électromagnétique en limitant leur susceptibilité à leur environnement et leur « émissivité » vers leur environnement. Cependant, ces châssis peuvent se comporter comme des cavités réverbérantes, le plus souvent chaotiques, ce qui rend difficile l’estimation des couplages à l’intérieur de ceux-ci. En effet, la grande disparité et la méconnaissance du contenu (cartes électroniques, câbles, ventilateurs, etc.) de ces équipements rend les études déterministes (modèle de circuit, simulation électromagnétique) difficilement applicables. Dès lors, il semble pertinent d'utiliser des méthodes d'analyses statistiques afin de caractériser ces phénomènes en obtenant les densités de probabilité des grandeurs d'intérêts (courant, tensions, etc.).

Depuis les années 1950, la théorie des matrices aléatoires se développe de plus en plus. Après avoir été appliquée à des problèmes de physique quantique, elle permet de résoudre des problèmes de physique semi-classique, particulièrement en électromagnétisme où elle est appelée *Random Coupling Model* (RCM). Cette méthode permet d'associer deux modes de couplages. Le premier, déterministe, prend en compte le couplage en espace libre entre plusieurs accès dans un système (entre une carte et un câble, par exemple). Il peut être facilement obtenu soit par la mesure, soit par la simulation, ou encore par un modèle ad hoc. Le second considère les couplages depuis les différentes résonances dans la cavité, en utilisant la théorie des matrices aléatoires. Le RCM permet aussi de prendre en compte des ouvertures dans des cavités. Alors que de nombreux modèles ne sont valides que pour de petites tailles d'ouvertures, un modèle d'ouverture généraliste a été proposé pour être utilisé conjointement au RCM. Le RCM prend aussi en considération les pertes (liées au facteur de qualité) de la cavité envisagée.

L'application de cette méthode semble pertinente pour évaluer les probabilités de couplages dans le cadre de la sécurité électromagnétique des systèmes d’information.

Ces probabilités sont nécessaires pour maîtriser les risques (identifiés en amont lors d'une analyse de risques) pendant la phase de conception d’un système. En effet, les propriétés réverbérantes d'un système pouvant être séparées du comportement en espace libre, il devient alors possible de multiplier à faible coût l’évaluation des risques de couplages pour différentes configurations (géométries de placement typiquement).

La présentation reviendra d’abord rapidement sur les origines de la théorie des matrices aléatoires et du RCM. Ensuite, l'exploitation de cette méthode sera présentée dans le cadre de l'estimation de la densité de probabilité d’un courant ayant pour origine le couplage entre une onde plane et une ouverture (de l’ordre de grandeur de ce que l’on peut trouver sur un ordinateur) dans une cavité. Les différentes étapes seront présentées ainsi que les outils développés ayant permis son application. Afin de valider le fonctionnement de cette méthode, celle-ci a été confrontée à des données expérimentales dont la statistique a été obtenue grâce à l'ajout d’un petit brasseur de modes dans la cavité étudiée (un modèle de châssis d'ordinateur).

ANALYSES DE DESTRUCTIONS D'ALIMENTATIONS SOUMISES A DES IMPULSIONS FORTS NIVEAUX

L. CUROS [1,2], T. DUBOIS [2], G. MEJECAZE [1,2], F. PUYBARET [1], J.-M. VINASSA [2]

[1] : CEA, DAM, CEA-Gramat, F- 46500 Gramat, France
[2] : Univ. Bordeaux, CNRS, Bordeaux INP, IMS UMR 5218, 351 cours de la libération, F-33400 Talence, France

laurine.curos@cea.fr

RÉSUMÉ

Cet article présente les effets d'impulsions électromagnétiques conduites de forte amplitude (plusieurs centaines d'ampères) sur le comportement électrique d'alimentations à découpage. Les injections sont effectuées en mode commun et en mode différentiel jusqu'à la destruction de l'alimentation. Des analyses de composants ont été réalisées et permettent d'émettre des hypothèses sur leur destruction.

MOTS-CLEFS : *Alimentations à découpage ; Analyses de défaillances ; Destructions de composants*

INTRODUCTION

Face à la menace croissante de perturbations par Interférences ElectroMagnétiques Intentionnelles (IEMI), les systèmes électroniques et en particulier les étages d'alimentation sont de plus en plus confrontés à des risques de défaillances, voire de destructions [1]. Dans ce cadre, des injections d'impulsions de forts courants ont été effectuées en mode commun et en mode différentiel sur 15 alimentations à découpage identiques de type flyback. Cette alimentation présentée sur la figure 1 a été conçue pour ces travaux suite à une étude approfondie, en termes de topologies et de composants, d'alimentations disponibles dans le commerce. Durant les essais, le niveau d'injection a été augmenté progressivement jusqu'à atteindre le seuil de destruction de l'EST (Equipement Sous Test). Sur l'alimentation testée, différents effets ont été observés. La plupart du temps, les mêmes composants ont été détruits. Leur analyse a permis de définir des scénarios décrivant la chronologie des destructions des différents composants de l'alimentation.

COMPREHENSION DES DESTRUCTIONS

Afin de comprendre les destructions des composants, des analyses aux rayons X (RX), au microscope optique ainsi que des caractérisations électriques ont été réalisées. L'analyse RX de la diode D1 (Fig. 2) montre la rupture du bonding engendrant une zone de particules métalliques conductrices causant un court-circuit. La mesure du courant traversant D1 lors de l'injection de l'impulsion sur l'alimentation ainsi que l'analyse bibliographique [2] suggèrent que la défaillance de la diode est due à un courant trop élevé dépassant fortement les seuils fournis dans la datasheet. De même, l'analyse RX du pont de diodes (Fig. 3), permet d'émettre l'hypothèse d'une destruction due à un fort courant. En effet, une jonction métallique (en parallèle de la puce) est visible entre les deux contacts (Fig.3) d'une des diodes de la diagonale court-circuitée. Enfin, l'analyse au microscope du MOSFET (Fig. 4), permet de visualiser une fusion de la couche de métallisation de la source, entrainant des courts-circuits entre les broches drain-source et/ou grille-drain. Les analyses suggèrent que la défaillance est due à un courant élevé au niveau du drain du MOSFET créant ainsi une augmentation de la température et donc, un emballement thermique [3]. Au niveau du contrôleur PWM, une analyse au microscope (images non présentées ici) a permis de visualiser la destruction de l'interrupteur du bas de la commande du MOSFET

(pin Drv du contrôleur). À la vue des analyses, la circulation d'un fort courant lors de la destruction en court-circuit de grille-drain du MOSFET pourrait expliquer cette destruction.

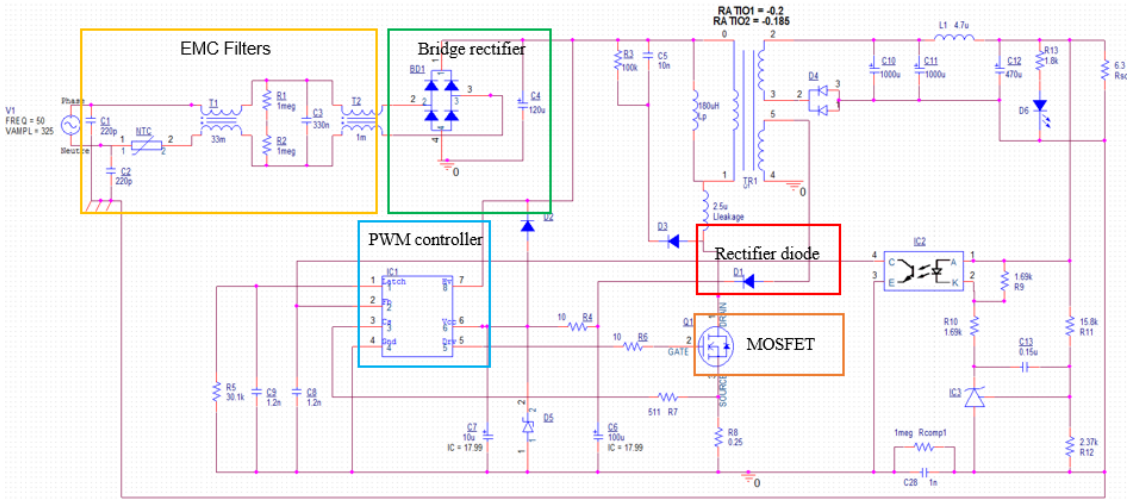


Fig. 1 : Schéma électrique de l'alimentation à découpage de type flyback.

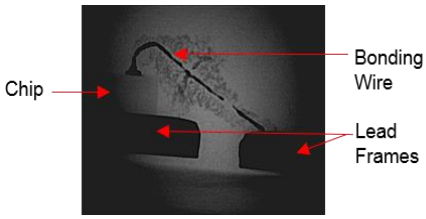


Fig. 2 : Analyse RX de la diode D1 en court-circuit.

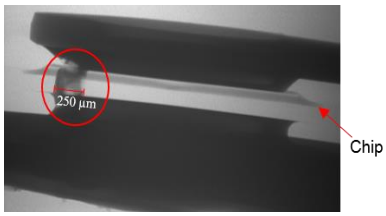


Fig. 3 : Analyse RX d'une diode en court-circuit du pont de diodes.

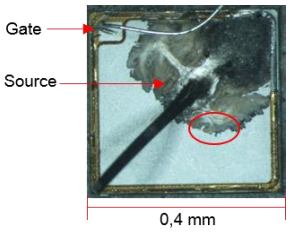


Fig. 4 : Analyse au microscope du MOSFET.

La destruction de l'alimentation peut correspondre à différents scénarios. En considérant un courant de fort niveau injecté dans le pont de diode BD1, le MOSFET Q1 ainsi que le shunt R8, celui-ci provoque la destruction de ces trois composants. De plus, un court-circuit entre la grille et le drain du MOSFET Q1 crée un chemin de courant vers la broche Drv du contrôleur et circulant à travers la résistance externe de grille R6. Ainsi ce courant peut détruire l'interrupteur du bas de la commande du MOSFET. Concernant la diode D1 d'alimentation du contrôleur, celle-ci peut être détruite à la suite d'une perturbation interne du contrôleur engendrant un appel de courant à ses pins d'alimentation (Vcc ou HV). Cet appel de courant est potentiellement suffisant pour détruire la diode D1. Des mesures complémentaires doivent être effectuées pour confirmer ces différentes hypothèses.

CONCLUSION

Ce papier permet de mettre en évidence les composants les plus susceptibles dans une alimentation à découpage de type flyback lors de l'injection d'une impulsion de fort niveau : pont redresseur, contrôleur PWM, MOSFET (et résistances associées) et diode de redressement. Les analyses aux rayons X et au microscope permettent d'émettre des premières hypothèses concernant des scénarios de destruction. Le but sera maintenant de confirmer ces hypothèses par des mesures de courants et de tensions sur les composants au moment de la destruction de l'alimentation. La dernière étape sera de modéliser ces destructions afin d'être capable de prévoir les effets d'une impulsion électromagnétique conduite fort niveau sur des équipements électroniques.

RÉFÉRENCES

[1] D. Nitsch et al., *"Susceptibility of some electronic equipment to HPEM threats"*, IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 380-389, 2004.

[2] J. Lutz and al., *"Semiconductor Power Devices – Physics, Characteristics, Reliability"*, Springer, 2011.

[3] M. Bouarroudj-Berkani et al., *"Fatigue des composants électroniques de puissance : Physique de défaillance"*, Techniques de l'ingénieur, D3126 v1, November 2010.

Journée thématique
« Sécurité des systèmes électroniques et communicants »
21 mai 2019, Paris – Jussieu

Présentation d'un banc d'analyse du signal Zigbee confronté à des agressions électromagnétiques intentionnelles

S. Iben Jellal[2], S. Baranowski[1], M. Bocquet[2]
[1] : *DOAE, UMR 8520-IEMN, Université de Lille, F59000, Lille, France*
[2] : *DOAE, UMR 8520-IEMN, UPHF, F59313, Valenciennes, France*
sara.ibenjellal@uphf.fr

Résumé
L'expansion des technologies sans fil a pris une ampleur considérable, ce phénomène laisse libre court à toutes les possibilités mais également toutes les attentes ; en effet, elles permettent d'améliorer les performances des systèmes en terme d'efficacité, de flexibilité et d'évolutivité…
La plupart de ces technologies opèrent dans la bande libre ISM (autour de 2.4 GHz), bande dans laquelle une quantité importante d'applications et de systèmes existent, augmentant ainsi les risques de vulnérabilité et problèmes de compatibilité électromagnétique (CEM).
Ce papier présente un banc de mesure qui a été développé afin d'étudier l'immunité d'un réseau de capteurs Zigbee face à des perturbations électromagnétiques intentionnelles.

Mots clés—Communication sans fil, CEM, brouillage par balayage,

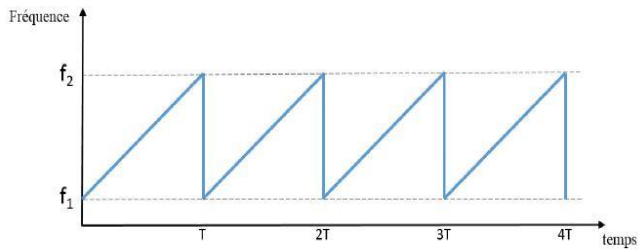
I. Introduction

Le suivi des marchandises est utile pour assurer la traçabilité des produits, par exemple, dans le domaine ferroviaire, le suivi des wagons de fret est autant nécessaire pour garantir cette traçabilité, que pour optimiser la gestion logistique [1]. Des réseaux de capteurs supportés par le protocole Zigbee peuvent être utilisés pour réaliser cette fonction [2]. La nature de ces marchandises peut inciter des personnes malveillantes à perturber intentionnellement les communications de ces capteurs; il est donc nécessaire de qualifier la robustesse de ces réseaux face à des agressions volontaires.

II. Perturbations générées intentionnellement

Dans la bande ISM, des perturbations électromagnétiques peuvent être générées volontairement par des brouilleurs, afin de réaliser des tentatives d'interruption de la communication ou la mise en panne temporaire ou définitive d'un système (appelé Déni de Service). Nous nous sommes intéressés à un type de brouilleur fréquemment rencontré sur le marché: le brouillage par balayage. Ce signal est présenté dans la figure 1.

Dans le banc de mesure développé, le brouillage est réalisé par un générateur qui émet un signal wobulé de f_1 à f_2, de puissance P_J, et de temps de balayage T .



Le signal de brouillage (Jamming signal) est défini par l'équation :

$$J(t) = P_J \cos(2\pi f(t) + \varphi)$$
$$f(t) = f_0 + kt; k = \frac{f_2 - f_1}{T}$$
$$f(t) = f_0 + kt; \quad k = f_2 - f_1$$

Figure 1 : Caractéristiques du signal émis par le brouilleur : Balayage en temps et en fréquence

III. Description du banc de mesure

Afin d'étudier les performances d'un système Zigbee face à des signaux interférents dans la même bande de fréquences, nous avons développé et mis en place le banc de mesure présenté dans la figure 2.

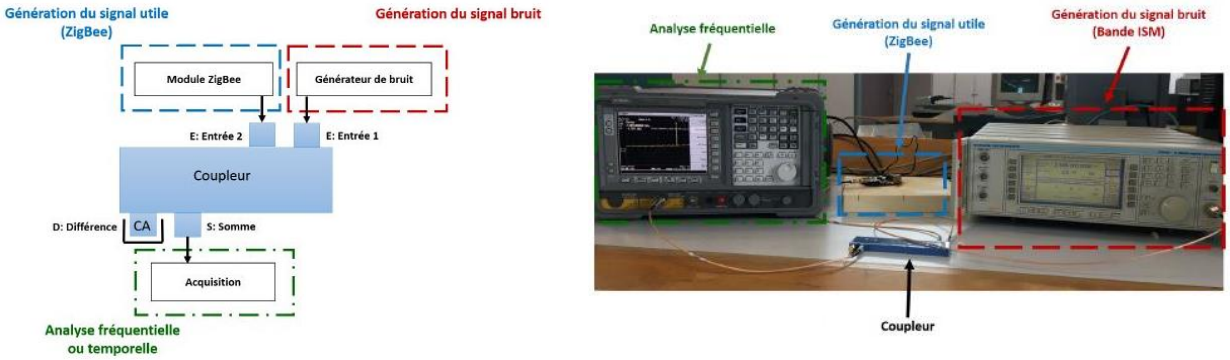


Figure 2: Schéma et photo du banc de mesure des perturbations générées.

Ce banc est constitué d'un coupleur 180° qui permet de sommer le signal de bruit (ici le brouillage intentionnel défini précédemment) avec le signal utile (ici le signal Zigbee). La sortie de ce coupleur permet l'analyse de la robustesse de la transmission en temporel comme en fréquentiel [3]. Le principal intérêt de l'utilisation du coupleur est de maitriser complètement les paramètres de l'étude et de faire abstraction des paramètres de propagation.

IV. Résultats

Les résultats des mesures ont montré que l'effet de ce type de perturbations sur un système de communication dépend de deux paramètres : la puissance du brouillage et le temps du balayage. Selon les expérimentations réalisées, la transmission est garantie à partir d'un rapport SNR de 36 dB indépendamment de la période du balayage. Cependant, pour des valeurs de SNR inférieur à 36 dB, plus le temps de balayage est grand plus l'interférent est efficace [1].

V. Conclusion

Le banc de mesure a permis d'analyser la robustesse de la liaison Zigbee face à des agressions intentionnelles. Il permet de faire d'autres analyses avec d'autres types de perturbations, par exemple un signal Wi-Fi environnant, des perturbations rayonnées par des systèmes de puissance….
De même, l'immunité de n'importe quel système de télécoms dans la bande passante du coupleur peut être étudiée à l'aide de ce banc de mesure.

VI. Remerciements

Ce travail a été effectué dans le cadre d'un doctorat financé par l'Institut Catholique d'Arts et Métiers de Lille (ICAM) et la Région Nord-Pas-de-Calais en France.

VII. Références

[1] S. Iben Jellal « Etude du suivi des wagons de fret à des fins logistiques par onde radio –Impact des interférences électromagnétiques sur le système proposé », Thèse, Université de Lille, août 2018.
[2] U. Biaou, « Étude et mise en œuvre d'une plateforme hybride basée sur du sans fil pour l'efficience énergétique et le contrôle d'accès dans le train », Thèse, UPHF Valenciennes, décembre 2017.
[3] N. Ben Slimen, « Recherche de procédures de caractérisation de l'environnement électromagnétique ferroviaire adaptés au contexte des systèmes de communication embarqués », Thèse, Université de Lille, décembre 2009.

Comportement d'une carte à base d'amplificateur opérationnel face à une perturbation électromagnétique de type impulsionnel modulé

T. Dubois, G. Duchamp

Laboratoire IMS / Université de Bordeaux ; 351 Cours de la Libération, 33400 Talence, France

tristan.dubois@u-bordeaux.fr

Résumé

Ce document présente les effets d'une perturbation électromagnétique de type impulsionnel modulé sur le fonctionnement d'un amplificateur opérationnel (AOp) monté en suiveur. Le signal d'interférence est injectée de façon conduite sur l'entrée non-inverseur de AOp.

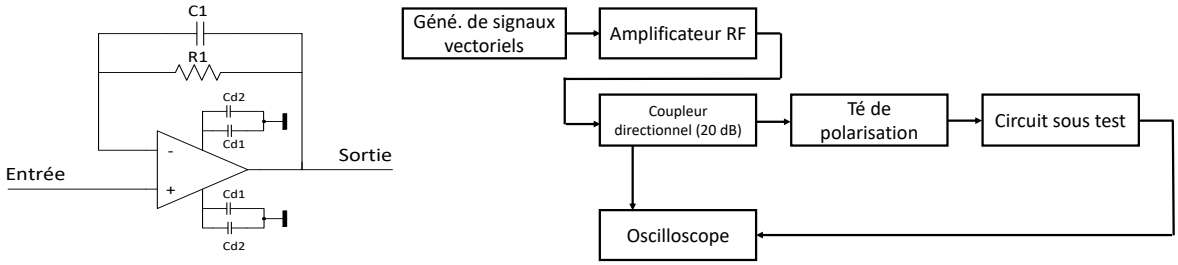
1. Introduction

Aujourd'hui, les circuits électroniques sont de plus en plus présents tant dans le domaine civil que militaire et dans des applications variées telles que l'automobile et l'aéronautique. Dans le même temps, les progrès réalisés dans le domaine des radiofréquences ont rendu les sources microondes de fortes puissances de plus en plus accessibles augmentant la menace IEMI (Interférence Électromagnétique Intentionnelle) [1]. Les signaux générés par ces sources sont généralement du type impulsionnel modulé permettant d'avoir de fort niveau de puissance instantanée tout en nécessitant des énergies raisonnables. Beaucoup d'étude visant à étudier l'influence de signaux d'interférence sinusoïdaux sur le fonctionnement de circuit électronique analogique existent [2-3] mais peu s'intéressent à des signaux du type impulsionnel modulé [4].

Dans ce contexte, ce papier présente l'étude de la réponse d'un circuit à base d'amplificateur opérationnel soumis à un signal d'interférence du type impulsionnel modulé. On s'intéressera notamment à la réponse transitoire du circuit et on cherchera à déterminer l'influence de la forme d'onde du signal impulsionnel sur la réponde du circuit en vue d'optimiser ses effets.

2. Circuit sous test et banc de mesure

Le circuit sous test est un amplificateur opérationnel AD8622 de la société Analog Devices qui a déjà fait l'objet de plusieurs publications dans le cadre de la compatibilité électromagnétique [5-6]. Le composant est reporté sur un PCB double couche de type FR4 classique. La figure 1(a) présente le schéma électrique du circuit étudié.



(a) (b)

Figure 1. (a) Circuit sous test, (b) Schéma du banc de mesure.

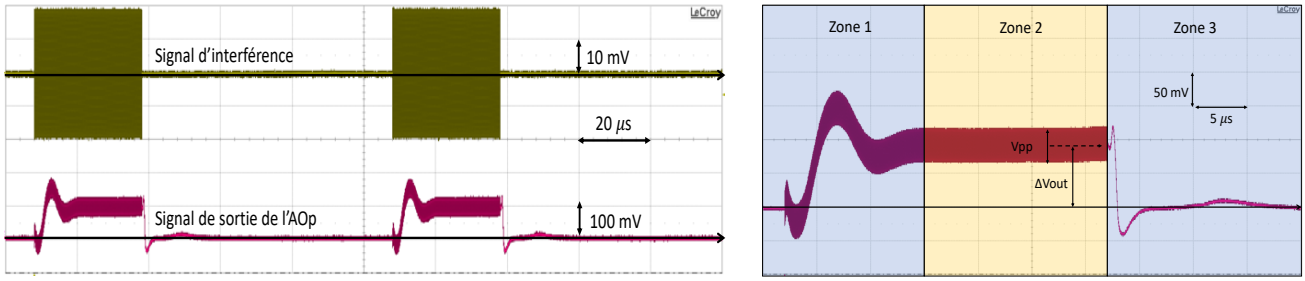
Le banc de mesure utilisé pour injecter le signal d'interférence est présenté en figue 1(b). Un générateur de signaux vectoriels associés à un amplificateur permet de générer le signal d'interférence. Le signal est ensuite injecté à l'entrée du circuit sous test via un coupleur directionnel et un té de polarisation. Un oscilloscope HF est utilisé pour d'une part mesurer une image du signal injecté ainsi que le signal de sortie du circuit.

3. Réponse du circuit face à une interférence de type impulsionnel modulé

La figure 2 (a) présente l'image du signal d'interférence mesurée via le coupleur ainsi que la réponse du circuit. La puissance du signal d'interférence est fixée à 5 dBm. Sa fréquence est de 750 MHz. Premièrement, on observe que globalement le circuit agit comme un démodulateur d'amplitude. L'envelope du signal est en partie mesuré à sa sortie. Deuxièmement, comme observé sur la figure 2(b), on peut observer 3 zônes caractérisant le signal de sortie de l'AOp. Une première zône transitoire correpondant au front montant de l'impulsion. Ce régime transitoire peut être modélisé, en première approximation, par la réponse à une impulsion d'un circuit du 2nd ordre du type RLC série, caractérisé par l'équation différentielle suivante :

$$\frac{d^2v(t)}{dt^2} + 2\zeta\frac{dv(t)}{dt} + {\omega_0}^2 v(t) = \Delta Vout,$$

Avec v(t) la tension aux bornes du condensateur, ζ le facteur d'armortissement et ω_0 la pulsation propre du système.



(a) (b)

Figure 2. (a) Signal d'interférence et signal mesuré en sortie du circuit, (b) Zoom sur le signal de sortie.

La solution de cette équation en régime pseudo périodique s'écrit :

$$v(t) = \Delta Vout + Ccos(\omega_m t + \varphi)e^{-\zeta t}.$$

Avec $= \Delta Vout$ la valeur atteinte par v(t) après le régime transitoire, C l'amplitude de la partie sinusoïdale du signal et ω_m la pseudo période.

La première zône est suivie d'un régime permanent caractérisé par un offset de tension ΔVout et d'une composante alternative de fréquence correspondant à la fréquence du signal d'interférence et d'amplitude crête-crête Vpp. Il sera montré que cette zône de régime permanent correspond à la réponse du circuit lorsque l'interférence est purement sinusoïdale. Enfin la troisième zône correspond à un deuxième régime transitoire correspondant à la fin de l'impulsion. Suivant la fréquence et la puissance du signal d'interférence, les différents paramètres caractérisant chaque zône changent.

2. Influence de la forme de l'impulsion d'interférence

La forme de l'impulsion d'interférence joue un rôle important sur la réponse du circuit. En effet, l'augmentation de la largeur d'impulsion augmente la durée de la deuxième zône. Par contre, en réduisant la largeur de l'implsion, la deuxième zône se réduit dans un premier temps suivie de la première zône si bien qu'en dessous d'une largeur d'impulsion de 10 ns, plus aucun effet de l'interférence n'est observable sur la sortie de l'amplificateur opérationel. Basé sur ces observations, il est alors intéressant de rechercher la forme de l'interférence induisant un maximum de pertubation sur la sortie de l'amplificateur. La figure 3 montre le signal d'interférence induisant la plus grande dynamque d'amplitude en sortie de l'AOp, à puissance d'interférence fixe.

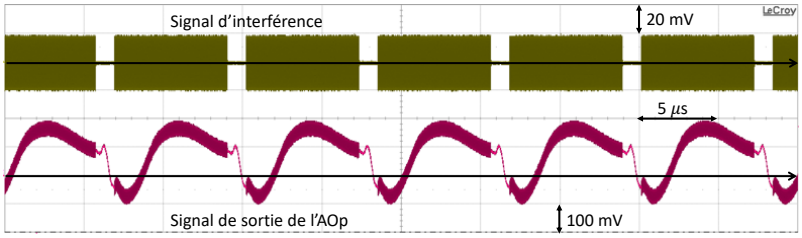


Figure 3. Signal d'interférence induisant un maximum de variation d'amplitude du signal de sortie pour une puissance d'interférence fixe.

4. Conclusion

Cette étude a permis de mettre en évidence l'effet d'une interférence de type impulsionnel sur le fonctionnement d'un amplificateur opérationnel monté en suiveur. Il a été notamment observé que l'amplificateur démodulait en partie le signal d'interférence. Une étude plus approfondie du signal de sortie de l'amplificateur a montré un régime transitoire et permanent s'apparentant à la réponde d'un système du second ordre tel un circuit RLC série. Enfin une étude de l'influence de la forme d'onde d'interférence a montré qu'au deçà d'une certaine largeur d'impulsion l'interférence n'avait plus aucun effet sur le circuit.

6. Bibliographies

[1] W. Radasky, et al., Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI), IEEE Trans. On EMC, 2004.

[2] A. Richelli, et al., "*Susceptibility of Operational Amplifiers to Conducted EMI Injected Through the Ground Plane into Their Output Terminal*", IEEE Trans. On Reliability, 2016

[3] F. Fiori, "*Operational amplifier input stage robust to EMI*", Electron Lett, 2001

[4] M. Girard, et al., "*Effects of HPEM stress on GaAs low-noise amplifier from circuit to component scale*", Microelectronics Reliability, 2018

[5] S. Hairoud, et al., "*Conducted immunity of three Op-Amps using the DPI measurement technique and VHDL-AMS modeling*", *EMCCompo 2013*

[6] T. Dubois, et al., "*Characterization and model of temperature effect on the conducted immunity of Op-Amp*", *Microelectronics Reliability, 2015*

COUPLAGES ELECTROMAGNETIQUES HAUTE FREQUENCE DANS DES BATIMENTS – APPLICATION DES CONCEPTS DE TOPOLOGIE ELECTROMAGNETIQUE ET POWER BALANCE

I. Junqua, J-P. Parmantier, W. Quenum

ONERA/DEMR, Université de Toulouse, F-31055, Toulouse, France, isabelle.junqua@onera.fr

I. INTRODUCTION

Le travail présenté a été réalisé dans le cadre du projet européen FP7 HIPOW (2012-2015) qui a pour objet la protection des infrastructures critiques aux attaques électromagnétiques (EM) intentionnelles, plus communément connues sous la terminologie IEMI/NNEMP [1]. Ces attaques EM désignent l'utilisation malveillante d'ondes radio fréquences pour perturber, endommager, voire détruire des composants, des fonctions et systèmes électroniques. Dans ce projet, l'Onera s'est concentré sur les infrastructures critiques de type bâtiments susceptibles d'accueillir des fonctions critiques et potentiellement vulnérables. Face aux attaques EM rayonnées de type IEMI/NNEMP, le bâtiment est alors considéré comme une enveloppe passive dont la topologie interne en termes de pièces, couloirs, accès internes et accès vers l'extérieur conditionne la pénétration et la propagation des champs EM induits aux niveaux des équipements critiques sensibles.

Dans ce contexte, le travail a consisté à analyser à l'aide d'expérimentations les fonctions de transfert électromagnétiques haute fréquence dans un bâtiment standard [2]. Dans un second temps, une méthodologie de simulation a été proposée basée sur les principes de topologie électromagnétique et Power Balance, initialement développés pour des applications dans des structures à fort caractère réverbérant pour estimer les niveaux induits par une source externe ou interne [2]. Finalement, durant l'exposé on montrera comment ces données numériques et ou expérimentales sont utilisées pour mener une analyse de risque.

II. ANALYSE EXPÉRIMENTALE DES INTERACTIONS ELECTROMAGNETIQUES INDUITES DANS UN BATIMENT

Ces expérimentations ont été menées sur le site de l'Onera Toulouse, sur un ensemble de bâtiments indépendants ou interconnectés entre plusieurs pièces de dimensions et points d'accès divers. Le principe de brassage de mode a été appliqué, comme dans les chambres réverbérantes. Plusieurs configurations de mesure de fonctions de transfert large bande (300MHz-6.3GHz) ont été étudiées:

- **Config. « intra » :** émission et réception sont dans la même pièce
- **Config. « inter »:** émission et réception sont placées dans 2 pièces différentes d'un même bâtiment
- **Config. « ext/int » :** l'émission est extérieure au bâtiment où se trouve l'élément de réception.

Dans les 2 dernières configurations, émission et réception pouvant être éloignées de plusieurs dizaines de mètres, le protocole expérimental a été adapté et optimisé en utilisant le réseau ethernet interne à l'Onera.
Des mesures de paramètres [S] entre émission et réception pour chaque position d'un brasseur placé dans la pièce, on a extrait les lois de distributions des paramètres S_{21} en configuration « intra » et les sections efficaces de couplage caractérisant les propriétés dissipatives dans différentes pièces (Fig. 1) [3]. Les mesures en configuration « inter » ont été post-traitées afin d'obtenir la cartographie de l'atténuation entre la pièce d'émission et les pièces de réception du même bâtiment.
En configuration « ext/int », on a également considéré plusieurs états des points d'entrée de l'énergie dans le bâtiment cible, à savoir des volets roulants métalliques ouverts, fermés ou demi-fermés de façon à évaluer les effets sur l'atténuation du bâtiment (Fig. 2).

[1] O.H. Arnesen, R. Hoad, *"Overview of the European project HIPOW"*, IEEE EMC magazine, Vol.3, Quarter 4, pp 64-67, 2014.

[2] I. Junqua, J-P. Parmantier, F. Issac, W. Quenum, *"Evaluation of RF transfer functions between the outside and the inside of buildings rooms"*, Interaction Notes 625, October 2014 (http://ece-research.unm.edu/summa//notes/In/IN625.pdf).

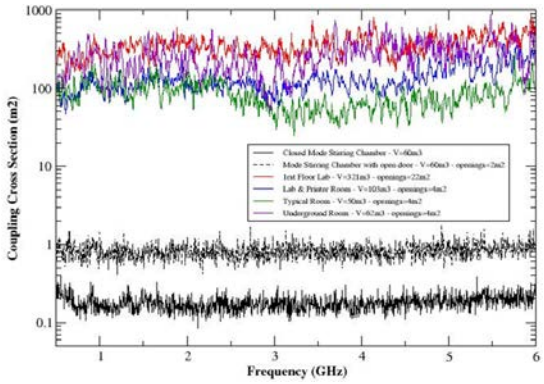


Fig. 1. Résultats en configuration « intra »

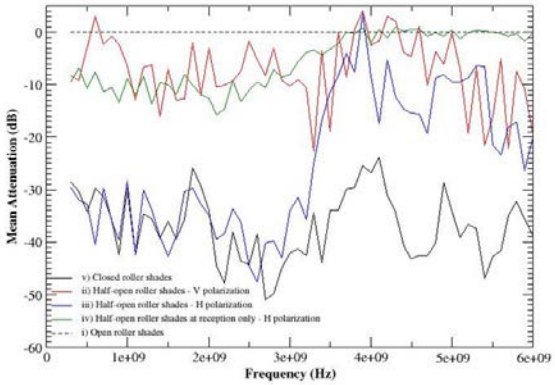


Fig. 2. Résultats en configuration « ext/int »

III. TOPOLOGIE ÉLECTROMAGNÉTIQUE & POWER BALANCE (EMT/PWB)

La méthodologie de modélisation EMT/PWB combine les concepts de topologie électromagnétique de façon à découper et représenter un système en un réseau de volumes topologiques et les principes Power Balance de quantification des interactions électromagnétiques dans et entre les volumes topologiques [4]. On suppose que les structures étudiées sont électriquement grandes et suffisamment complexes pour appliquer un modèle probabiliste des interactions électromagnétiques (comme dans les chambres réverbérantes) qui sont alors réduites à des densités de puissance ou puissance moyennes.

Les structures sont alors caractérisées par un ensemble de sections efficaces de couplage traduisant les mécanismes dissipatifs dans les structures et les mécanismes de transfert entre structures. Les configurations expérimentales ont été modélisées sous la forme de réseaux EMT/PWB (Fig.3). Les nœuds du réseau EMT/PWB sont caractérisés par les sections efficaces de couplage déduites des mesures en configurations « intra » et « inter » ou obtenues par des formulations analytiques simples comme pour les fenêtres des bureaux. Un exemple de validation de l'approche par comparaison entre mesure et simulation en configuration « ext/int » est donné sur la Fig.4 .

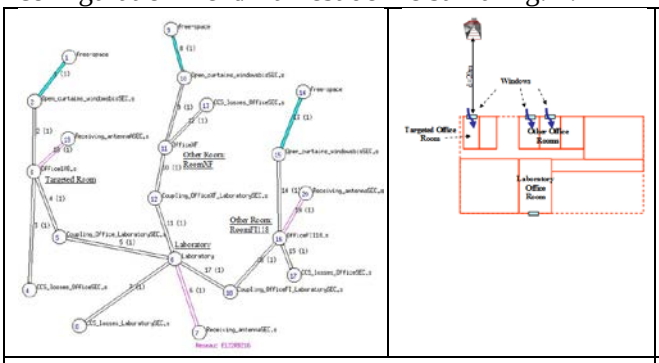


Fig. 3. Modèles EMT/PWB de la configuration « ext/int »

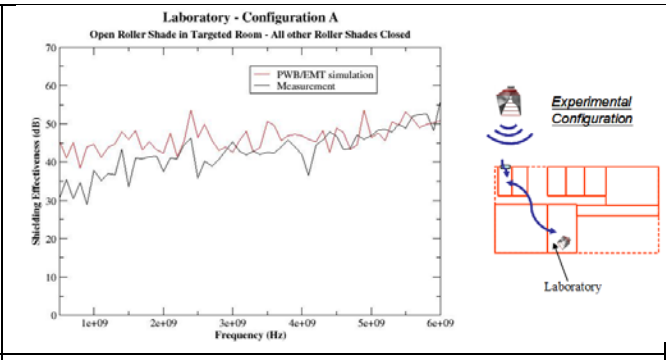


Fig. 4. Efficacité de couplage dans le laboratoire configuration « ext/int » - mesure et simulation

IV. CONCLUSION

Les essais ont permis d'analyser les interactions EM induites dans un bâtiment par une source externe ou interne et d'extraire les paramètres dimensionnants (caractère dissipatif, points d'accès). L'approche qui consiste à combiner topologie électromagnétique et concepts PoWer Balance a été appliquée et validée. Dans le papier final, on montrera des résultats de modélisations dans des configurations de bâtiments extrapolées et comment cette approche EMT/PWB peut aider à l'optimisation de la protection des bâtiments aux attaques EM intentionnelles de type IEMI/NNEMP en termes de faradisation ou de localisation des équipements sensibles.

Ces travaux ont été financés par le programme européen HIPOW du FP7 2012-2015 (Grant agreement n° 284802).

[3] C. Lemoine, *"Contribution à l'analyse statistique des mesures en chambre réverbérante à brassage de modes – applications à la détermination de l'efficacité de brassage et de l'incertitude de mesure dans un contexte CEM et radio-fréquence"*, thèse de l'INSA Rennes, 2008

[4] I. Junqua, *"Pénétration des ondes EM haute fréquence dans des systèmes : analyse et évaluation par l'approche PoWer Balance"*, thèse de l'USTL, 2010

Mesure de l'efficacité de blindage électromagnétique pour le blindage de bâtiments

J. Alaa Eddine[1], E. Pistono[2], F. Ndagijimana[1]
[1] Université Grenoble Alpes, laboratoire G2Elab
[2] Université Grenoble Alpes, laboratoire RFICLab,
Contact : jalal.alaa-eddine@univ-grenoble-alpes.fr

1. Introduction

Le blindage électromagnétique consiste à réduire le champ électromagnétique au voisinage d'un objet en interposant une barrière métallique entre la source du champ et l'objet à protéger. Ce blindage électromagnétique est nécessaire pour la sécurité dans les bâtiments avec la notion de confidentialité. Ainsi, dans ce cadre, pour protéger un bâtiment, divers types de matériaux de blindage peuvent être utilisés, comme par exemple des tissus, des peintures conductrices pour les murs et aussi des matériaux spécifiques qui peuvent être collés sur le verre des fenêtres et des portes. L'efficacité ou l'affaiblissement de blindage (SE) est le terme qui définit la diminution du champ électromagnétique. Il dépend du matériau utilisé, la bande de fréquence et la méthode de caractérisation utilisée. Nous présentons ici la méthode de test considérée avec des résultats d'efficacité de blindage pour différents matériaux utilisables dans les applications de blindage des bâtiments (tissus métallisés, peintures « anti ondes », film transparent avec traitement anti UV, etc...)

2. Caractérisation des matériaux pour le blindage des bâtiments

Pour caractériser les matériaux de blindage en termes d'efficacité de blindage, il existe plusieurs méthodes, normatives ou non, qui dépendent de la bande de fréquence et de la forme du matériau utilisé. La méthode considérée ici consiste à insérer le matériau à tester entre deux sections d'un guide d'onde WR340(R26) fonctionnant dans la bande de fréquence de 2GHz – 3.8 GHz, et de mesurer la transmission avec un analyseur vectoriel (voir figure1).

$$SE(dB) = transmission \text{à } vide - transmission\ avec\ matériau \qquad (1)$$

Compte tenu de la transmission à vide proche de 0dB, la transmission avec conducteur parfait permet d'atteindre une dynamique de mesure de 100 dB.

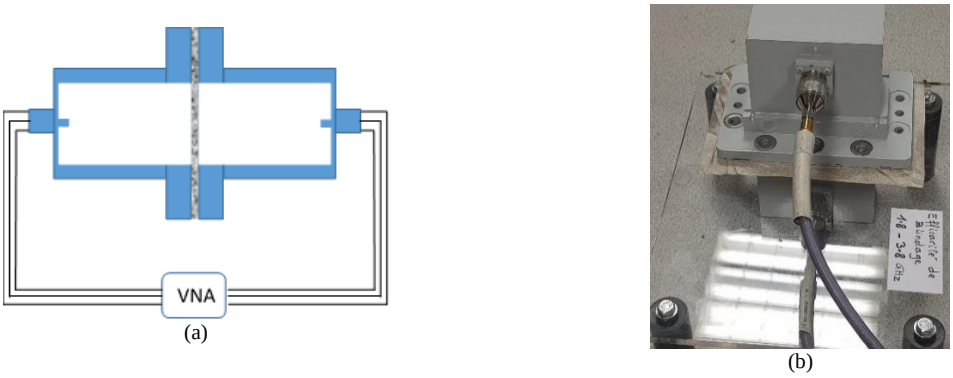
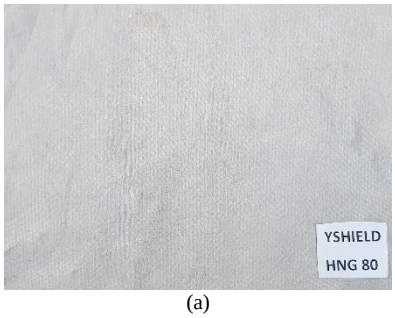


Figure 1: Banc de caractérisation de l'efficacité de blindage : (a) configuration de test, (b) photo du banc

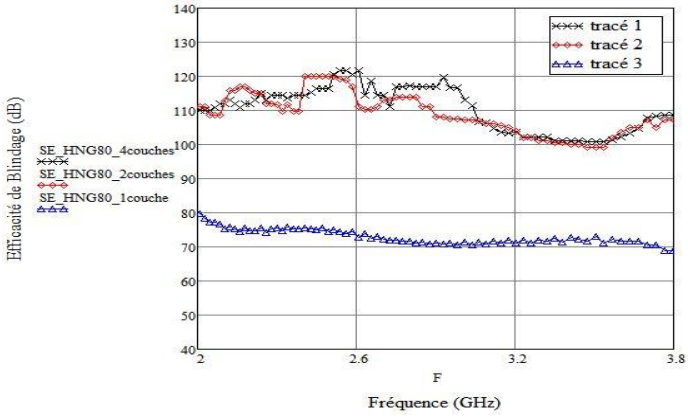
La méthode de test a été d'abord appliquée au tissus métallisé HNG80 qui est un tissu en polyester métallisé d'épaisseur 0.07 mm, et qui peut servir à de revêtement mural, plafonds etc.., et qui est spécifié pour une atténuation d'environ 80dB.

Comme présenté à la figure 2, la mesure montre une efficacité de blindage comprise entre 70 et 80 dB dans la bande considérée pour une couche, et de l'ordre de 110dB pour 2 et 4 couches superposées. La saturation est conforme à la dynamique propre de l'analyseur vectoriel utilisé (HP8753D) qui est de -110dB en transmission.

Deux autres types de matériau de blindage ont également été testés : (i) un film transparent d'épaisseur 0.06mm pour le blindage des vitres (SPECTRA40) présentant une efficacité de blindage de 20 à 30 dB (voir figure 3) et (ii) une peinture conductrice pour le blindage des murs (HSF54) présentant une efficacité de blindage de 5dB (respectivement 8dB) en monocouche (respectivement en double couche)

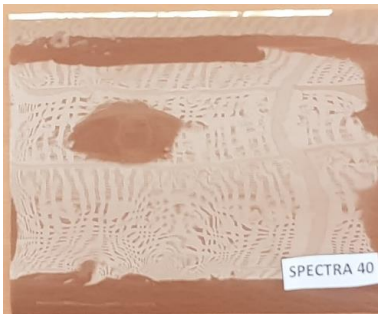


(a)

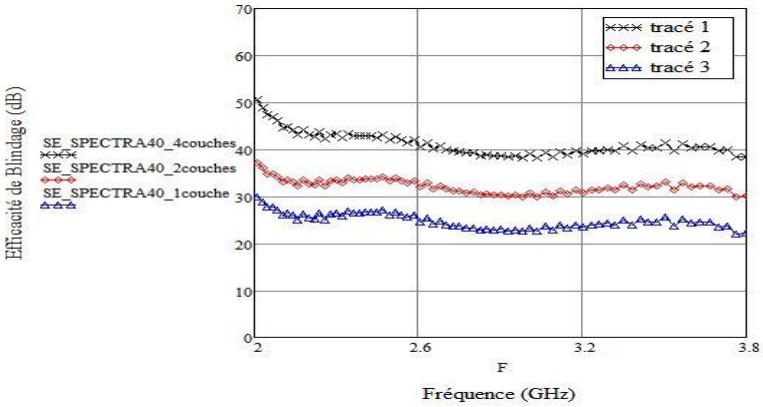


(b)

Figure 2: (a) tissus métallisé Yshield-HNG80, (b) efficacité de blindage mesuré



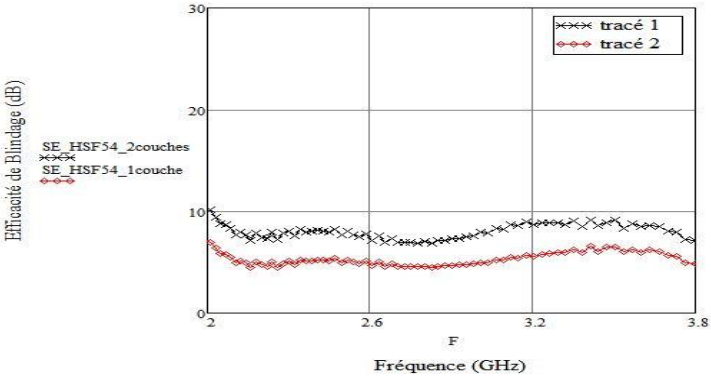
(a)



(b)

Figure 3: (a) film transparent traité anti UV SPECTRA40, (b) efficacité de blindage mesuré

(a)



(b)

Figure 4:(a) peinture conductrice Yshield-HSF54, (b) efficacité de blindage mesuré.

3. Conclusion

Une méthode de caractérisation des matériaux de blindage pour la protection des bâtiments est proposée ici. Elle permet de mesurer l'efficacité de blindage de matériaux utilisables dans le bâtiment sécurisé sur la bande de fréquence considérée est de 2 – 3.8GHz avec une dynamique de 100dB. Elle est facilement extensible aux fréquences plus hautes utilisées par les télécommunications par une de taille de guide appropriée. Nous discuterons des performances lors de la mise en œuvre de ces solutions de blindage dans le cas réel d'un local à sécuriser.

Evaluation du rayonnement EM à l'aide d'une électronique embarquée

A. Liakouti, K. El Khamlichi Drissi et C. Pasquier
Institut Pascal, Université Clermont Auvergne, UMR 6602, Clermont Ferrand, France

Résumé

Dans la majorité des problématiques en compatibilité électromagnétique, le rayonnement des électroniques revêt une importance capitale. La connaissance de ce rayonnement permet d'évaluer le degré de nuisance émise par un appareillage. Le secteur des communications (liaison numérique asymétrique-ADSL) et le secteur des réseaux électriques intelligents (courants porteurs en ligne-CPL) sont des terreaux de génération de rayonnement électromagnétique dans l'environnement proche et lointain. Afin de traiter cette problématique, le présent travail s'intéresse à l'estimation des champs électromagnétiques rayonnés en zone proche et éloignée d'un réseau filaire à l'aide d'une électronique embarquée placée dans des points stratégiques de l'installation. Ces points sont les discontinuités électriques et/ou géométriques des conducteurs filaires constituant la structure rayonnante. A partir de la mesure du courant et des deux premières dérivées spatiales du courant en ces points, on peut donner une expression approchée du champ électromagnétique en tout point de l'espace sans besoin de sondes de champ électrique et de champ magnétique. Nous suggérons de proposer un système de mesure à base d'électronique embarquée qui permettrait une évaluation de ce champ rayonné. Il semble évident que ce lien direct entre courant en quelques points et champ rayonné interroge quand à la sécurité d'une installation d'énergie ou de télécommunications et laisse à penser que le problème inverse peut trouver solution et par conséquent faciliter l'accès aux données.

Mots Clés : Courants Porteurs en Ligne (CPL), Rayonnement Electromagnétique, réseau électrique intelligent, électronique embarquée, compatibilité électromagnétique (CEM).

I. Introduction

Véhiculer des données numériques via les conducteurs filaires en vue d'applications comme l'accès à Internet, la domotique ou la gestion de l'énergie, est incontournable dans le domaine des télécommunications et de l'énergie. Cependant l'inconvénient majeur de l'usage de ces supports filaires réside dans la problématique de leur rayonnement non intentionnel engendré au voisinage des conducteurs en haute fréquence [1]. Ces rayonnements peuvent être une source de pollution EM susceptible de perturber, voire d'empêcher le fonctionnement normal des autres dispositifs électroniques voisins ce qui constitue un problème gênant pour l'aspect CEM [2] mais également une vulnérabilité d'accès à des données sécurisées. La modélisation des émissions rayonnées pour la prédiction des niveaux de champs rayonnés est une base théorique incontournable qui permet de poser la problématique dans le sens direct et entrevoir éventuellement des solutions pour éviter la remontée aux informations source.

II. Modèle approché du rayonnement EM appliqué sur le microcontrôleur

Pour déterminer le champ EM des structures filaires, nous mettrons en œuvre les expressions du modèle simplifié du champ électrique et du champ magnétique du rayonnement issu de travaux antérieurs [3]. Ces équations ont été implantées dans un microcontrôleur de type RENESAS [4] grâce au logiciel E2STUDIO. Les données d'entrée du microcontrôleur sont les valeurs des courants et ses deux premières dérivées aux discontinuités de la ligne, la fréquence de travail, les cordonnées géométriques de ces discontinuités, les coordonnées géométriques des points d'observation où on souhaite évaluer le champ électromagnétique rayonné. Les données de sortie sont les valeurs du champ électrique et du champ magnétique évalués pour les points d'observations en question.

1. Application à une ligne bifilaire coudée

Afin d'exécuter et de valider le code implanté dans le microcontrôleur, nous allons considérer le cas d'une ligne bifilaire en cuivre de conductivité $\sigma=5{,}96.10^{7}\ (\Omega.m)^{-1}$, de diamètre 2.5 *mm* formant un coude de 90° en son centre comme le montre la figure suivante.

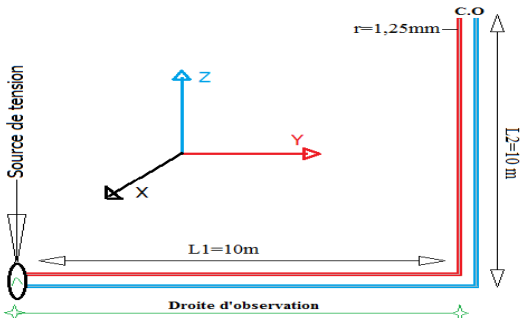


Figure 1. Configuration étudiée

Les deux conducteurs de la ligne sont espacés d'une distance d=5 mm. Cette ligne est excitée à son entrée par une source de tension sinusoïdale d'amplitude 1 $Volt$ à une fréquence variable et ayant une résistance interne de 50 Ω. A sa deuxième extrémité, la ligne est terminée par un circuit ouvert. Pour cette application nous confrontons les résultats obtenus sur le microcontrôleur sous le logiciel E2STUDIO à ceux que nous extrayons du simulateur Feko basé sur la théorie des antennes [5].

2. Résultats de simulation

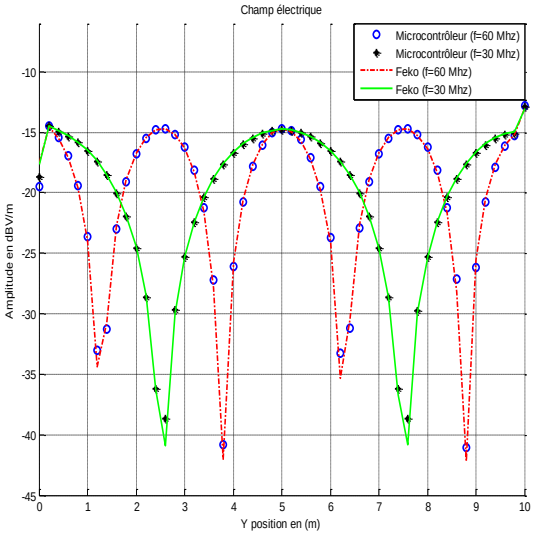


Figure 2. Module du champ électrique

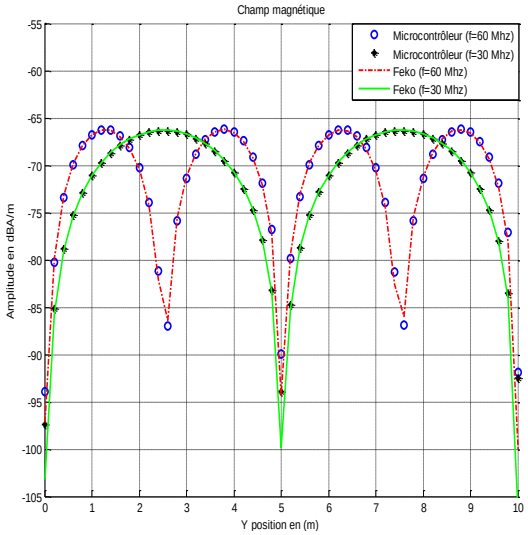


Figure 3. Module du champ magnétique

Au vu des figures ci-dessus, on note un très bon accord entre les résultats fournis par les deux approches pour les deux fréquences de traitement (30 Mhz est 60 Mhz), ce qui permet de confirmer les bases théoriques fondatrices [6] et le portage réalisé sur un microcontrôleur.

III. Conclusion

Dans ce travail, nous avons proposé une méthode de détermination du rayonnement électromagnétique engendré aux alentours de conducteurs filaires à l'aide d'un système électronique. Cette détermination est effectuée sans avoir besoin de la distribution du courant sur la totalité de la structure rayonnante mais seulement en se basant sur les points de discontinuités géométriques et électriques. Cela permet de traiter les situations pour lesquelles la distribution de courant le long de la ligne est inaccessible comme par exemple le cas des conducteurs enfouis dans les murs où seul l'accès aux extrémités est envisageable.

IV. Références

[1] Fahd HASSOUN - Etude de l'émission électromagnétique générée par une transmission haut débit sur un réseau de type XDSL ou PLC - 205 p - Thèse en Electronique et systèmes soutenue à Clermont-Ferrand le 29 Novembre 2006.

[2] Mohamed CHAABAN "Contribution À L'étude Du Rayonnement Des Conducteurs Filaires" Thèse en Electronique et systèmes soutenue à Clermont-Ferrand le 31 Mai 2011.

[3] Achraf LIAKOUTI "Analyse et modélisation du rayonnement électromagnétique des réseaux CPL" Thèse en Electronique et systèmes soutenue à Clermont-Ferrand le 11 Mai 2017.

[4] Renesas Electronics, "Renesas Microcontroller for motor control incorporating a multifunctional timer, high-speed 12-bit A/D converter", RX62T/62G datasheet, Jan. 2014

[5] A. BOYER, "Getting started with FEKO software", National Institute of Applied Sciences Toulouse, Nov. 2008, alexandre.boyer@insa-toulouse.fr.

[6] A. Liakouti, A. Benbassou, K. El Khamlichi Drissi, K. Kerroum, An Efficient Model of the Electromagnetic Field Radiated from Different PLC Configurations, Vol. 6, N. 4 ISSN 2039 – 5086 August 2016.