La vulnérabilité des réseaux électriques en cas d'attaques électromagnétiques

Autor(en): **Lugrin, G. / Mora, N. / Sliman, S.**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **104 (2013)**

Heft 5

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-856484

La vulnérabilité des réseaux électriques en cas d'attaques électromagnétiques

Caractéristiques des sources d'interférences intentionnelles

Quels impacts pourraient avoir des interférences électromagnétiques intentionnelles sur les réseaux d'énergie électrique ? Un projet de recherche est actuellement en cours à l'EPFL et à la HEIG-VD pour tenter de les qualifier et quantifier. Un premier résultat constitué de la définition des caractéristiques des sources d'interférences électromagnétiques intentionnelles ainsi que d'un passage en revue des sources référencées est décrit dans cet article.

G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein, R. Cherkaoui

Les interférences électromagnétiques peuvent être regroupées en deux catégories principales : les interférences générées naturellement, essentiellement par la foudre, et les interférences produites artificiellement, telles que les bruits industriels ou les rayonnements dus aux télécommunications. Parmi ce second type de perturbation sont aussi considérées, depuis environ une quinzaine d'années, les interférences électromagnétiques intentionnelles (IEMI), c'est-à-dire générées volontairement par des personnes dans le but de nuire [1].

Par rapport aux attaques physiques, les interférences électromagnétiques intentionnelles représentent une menace particulièrement sournoise pour les systèmes électriques et électroniques car elles peuvent être menées anonymement et traverser les barrières physiques. D'autre part, elles ont des caractéristiques en fréquence et en amplitude qui peuvent différer grandement des interférences conventionnelles [2].

Plusieurs cas d'attaques électromagnétiques ont été reportés ces dernières années [3]. Par exemple, au Japon, des criminels ont utilisé un générateur électromagnétique pour interférer avec le processeur d'une machine à sous et ont déclenché artificiellement un gain. Ou encore, à Moscou, le travail normal d'un central téléphonique a été interrompu par une injection à distance d'une tension dans une ligne téléphonique. Ceci a laissé deux cent mille personnes sans service téléphonique pendant un jour. D'autres exemples ont également été reportés, mais il n'y a néanmoins pas assez d'informations et de recul pour effectuer de réelles statistiques.

Le passage en revue des sources actuellement disponibles décrit dans la suite de cet article montre que les moyens techniques existent pour perpétrer des attaques, et ce, d'autant plus que le dimensionnement des réseaux est antérieur aux possibilités actuelles de production d'interférences. De plus, les nombreux systèmes électroniques de mesure et de communication, ainsi que ceux utilisés dans les actions automatiques et à distance, pourraient également présenter des vulnérabilités aux attaques électromagnétiques.

Diverses études ont été menées sur la susceptibilité à ce type de perturbations de différents systèmes électroniques individuels, tels que des composants électroniques ou des ordinateurs [4-10], ainsi que sur celle des réseaux ferroviaires [11-12]. Des études de susceptibilité des réseaux d'énergie électrique ont également été effectuées dans d'autres pays [13-14] ; les résultats obtenus sont néanmoins en partie classifiés, du fait des informations sensibles qu'ils contiennent.

Comme la société d'aujourd'hui est très largement dépendante d'un apport fiable en électricité, un projet analysant l'impact des IEMI sur les réseaux électriques a été lancé en décembre 2011. Financé par Swisselectric Research, il est mené par l'École polytechnique fédérale de Lausanne (EPFL) et la Haute école d'ingénierie et de gestion du canton de Vaud (HEIG-VD), avec le concours de Montena EMC, Armasuisse, Meteolabor et l'Université KTH (Royal University of Technology, Suède).

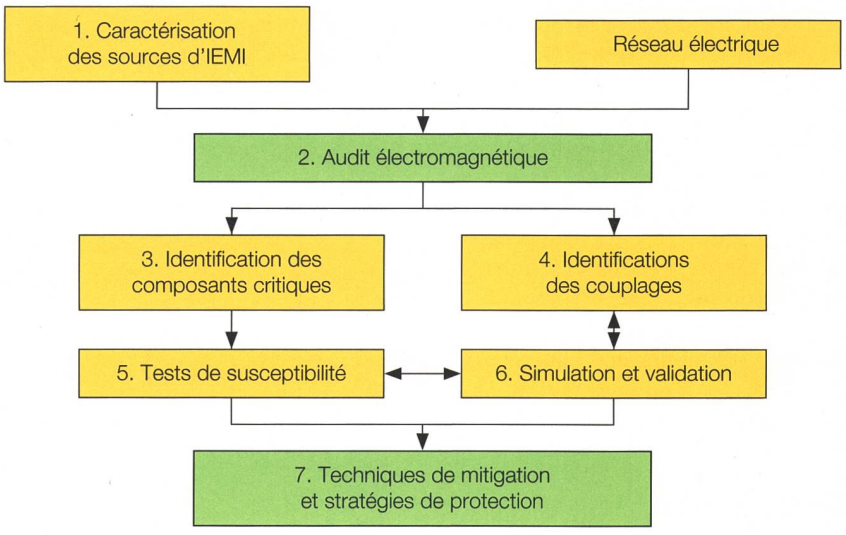


Figure 1 Les différentes phases du projet.

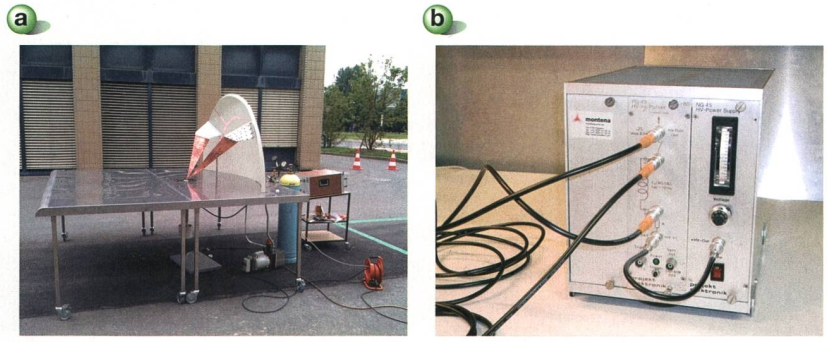


Figure 2 Exemples de sources d'interférences : (a) rayonnée et (b) conduite.

Déroulement du projet

Pour pouvoir quantifier l'impact des IEMI sur le réseau électrique suisse, l'environnement électromagnétique qui peut être créé par des sources doit être dans un premier temps défini (**figure 1,** point 1). C'est pourquoi la première phase du projet a pour but de dresser un portrait des sources actuellement disponibles. De fait, elle a permis d'appréhender le problème et de s'informer des travaux qui ont été réalisés dans ce domaine pour en retenir et en synthétiser les points importants. Les données réunies concernant les sources et les manières de les caractériser feront l'objet de cet article.

Comme illustré dans les points 2 à 4 de la **figure 1,** un audit électromagnétique d'au moins une installation électrique permettra ensuite d'identifier des tendances générales concernant les points d'entrée des perturbations, les composants critiques (c'est-à-dire les composants importants susceptibles d'être perturbés) et les couplages (c'est-à-dire la manière dont l'énergie est transmise de la source à l'équipement victime).

Une analyse de susceptibilité (**figure 1,** point 5) permettra alors de savoir si les équipements de protection jouent encore leur rôle pour les formes d'ondes pouvant être générées par les IEMI, notamment dans les gammes de fréquences supérieures à celles pour lesquelles ils ont été dimensionnés. De même, les équipements considérés comme particulièrement critiques seront testés en laboratoire afin d'en déterminer la susceptibilité. En effet, même s'ils ont été dimensionnés selon les standards de la compatibilité électromagnétique (CEM), ils ne sont pas forcément capables de supporter les amplitudes importantes qui peuvent être produites par les IEMI.

Pour leur part, les couplages (**figure 1,** point 6) pourront être estimés de manière expérimentale et par simulation numérique en utilisant différents modèles. Cette partie présente un défi eu égard aux hautes fréquences, à la taille des infrastructures testées et à la complexité de celles-ci. C'est aussi l'occasion de mettre en œuvre des modèles récents décrits dans la littérature (par exemple dans [15]).

Finalement, le but sera de proposer des techniques de mitigation (c'est-à-dire de réduction des impacts) et des stratégies de protection pour atténuer l'effet d'une éventuelle attaque (**figure 1,** point 7). Il est aussi envisagé de développer des moyens de protection spécifiques.

Les caractéristiques des sources d'IEMI

Au cours de cette première partie du projet, quelques normes déjà existantes dans le domaine des IEMI [1,16], ainsi que la littérature (voir par exemple [17]), ont été passées en revue afin de retenir les manières appropriées de décrire et de classer les sources. Cette classification est utile principalement pour évaluer les perturbations électromagnétiques qui peuvent être subies par un équipement. Cependant, elle pourrait aussi être utilisée après une attaque pour déterminer le profil de l'attaquant. En effet, si une information suffisante est disponible, il pourrait être possible de découvrir le type d'équipement employé ou quelques-unes de ses caractéristiques avec un certain degré de précision.

Les types de couplage

Les sources peuvent injecter de l'énergie dans un système de deux manières différentes, c'est-à-dire en utilisant un couplage soit conduit, soit rayonné (**figure 2**).

Lors d'un couplage conduit, l'énergie électromagnétique est injectée directement dans les câbles d'énergie ou d'information. Elle se propage ensuite aisément le long de ceux-ci, en particulier dans le cas des câbles d'information qui permettent la propagation de signaux haute fréquence avec une atténuation relativement faible.

Dans le cas d'un couplage rayonné, un signal est émis à l'aide d'une ou plusieurs antennes. L'agresseur peut donc se coupler sur un équipement même s'il se trouve à une certaine distance de la victime. Les ondes rayonnées peuvent ensuite atteindre directement un équipement victime ou induire des ondes de courant et de tension le long des câbles se propageant jusqu'à l'équipement.

Caractéristiques électromagnétiques

Une source, telle qu'un radar ou un émetteur radio, qui émet une onde de forme approximativement sinusoïdale

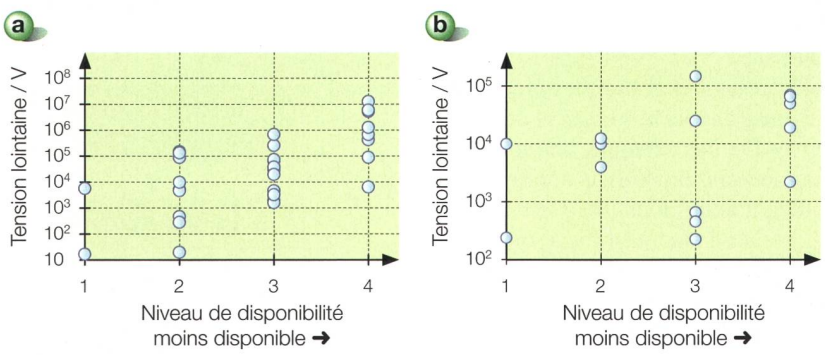


Figure 3 Tension lointaine (champ électrique à une distance générique de 1 m) en fonction de la disponibilité : (a) couplage rayonné, (b) couplage conduit.

dans un spectre concentré autour d'une fréquence est dite à bande étroite (hypoband). Si la source est réglée sur une fréquence à laquelle le système victime est particulièrement sensible, elle peut l'endommager de manière permanente en induisant des claquages des isolants et des échauffements.

Au contraire, une source générant une impulsion émettra sur une large bande (hyperband). Ce type de source est à même d'induire des erreurs dans un protocole de communication.

Une source produisant un signal ayant des caractéristiques intermédiaires à celles présentées ci-dessus est qualifiée de « mesoband ». Les sources de ce type peuvent être particulièrement compactes (voir par exemple [18-20]).

A noter que les distinctions entre ces divers types de bandes passantes sont définies en utilisant une norme mathématique qui permet de classer de manière univoque une source dès que l'on connaît la forme d'onde qu'elle produit.

La « force » de la source est aussi quantifiable en utilisant différentes normes mathématiques en fonction de l'effet considéré. Par exemple, l'endommagement des composants dépend principalement de l'énergie du signal, les erreurs générées dans un protocole de sa densité spectrale de puissance, etc. Une mesure de la « force » d'une source rayonnée est donnée par la tension lointaine (far voltage). Cette dernière correspond au produit du champ électrique mesuré à une certaine distance de l'antenne multiplié par cette distance [1]. Pour une source conduite, l'amplitude de la tension générée peut être utilisée.

Caractéristiques qualitatives

Un autre aspect important est la « transportabilité », c'est-à-dire la facilité à transporter une source ; elle dépend de la taille et du poids de cette dernière. Une source de petite taille, que l'on peut cacher dans une poche ou dans une valise, pourra être approchée plus près de l'équipement cible. Les sources de grande taille permettent, quant à elles, de produire en général des champs électromagnétiques très importants (champ électrique de plusieurs dizaines de kV/m à une distance de 100 m [21], à comparer avec un téléphone portable émettant un champ de l'ordre du V/m à une distance de 5 cm de l'appareil [22]).

La transportabilité est mesurée sur quatre niveaux. Le niveau I correspond à une source que l'on peut glisser dans une poche ou porter sur soi et le niveau IV à une source que l'on peut transporter uniquement en camion. A titre d'exemple, les quatre niveaux de transportabilité sont présentés dans le **tableau 1.**

La « disponibilité » [16] représente la facilité pour une personne ou une organisation à obtenir ou construire une source, en fonction du prix et de la sophistication technologique de celle-ci. Les sources peu coûteuses et faciles à obtenir sont susceptibles d'être utilisées par un plus grand nombre de personnes.

La disponibilité se mesure aussi sur quatre niveaux, le niveau I correspondant à une source disponible pour tout un chacun et le niveau IV à une source disponible seulement pour des personnes ou des organisations disposant de fonds importants. Une autre norme [23] préfère utiliser le « niveau de technologie de la source », qui correspond à la facilité de sa mise en œuvre, ce qui est étroitement lié à sa disponibilité.

La probabilité d'occurrence d'une source diminue en fonction de l'énergie, de la complexité de la technologie et de la difficulté à produire la perturbation [24].

Niveau de transportabilité	Description
I	peut être porté dans une poche ou sur le corps
II	peut être porté dans une valise ou un sac à dos
III	peut être transporté dans un véhicule à moteur
IV	peut être transporté en camion

Tableau 1 Les différents niveaux de transportabilité (d'après la norme ITU-T K.81 [16]).

Passage en revue des sources

Cette partie du projet poursuit plusieurs buts. Le premier est de créer une liste de sources actuellement disponibles, un outil très utile pour effectuer une analyse de risque. Il était en outre intéressant de mettre en œuvre la classification proposée, d'une part pour vérifier qu'elle s'applique, mais surtout pour mettre de l'ordre dans l'abondance des sources disponibles. Cela a aussi permis de mettre en évidence les liens entre les différents paramètres décrits dans la section précédente.

La démarche a consisté à passer en revue la littérature disponible pour obtenir des informations sur un grand nombre de sources. Comme elles proviennent principalement d'articles scientifiques, de nombreuses sources rapportées correspondent plutôt bien à l'état de l'art. Bien qu'il soit impossible que la liste soit exhaustive, elle fournit des informations sur le type de dispositifs qui pourraient être utilisés contre le réseau électrique ou une autre infrastructure.

Les tendances détectées

De manière générale, plus une source génère un champ important, moins il est facile de se la procurer, comme illustré dans la **figure 3a**. Pour les perturbations conduites, la tendance est moins nette **(figure 3b)**. Cependant, la puissance d'une source conduite ne dépend pas seulement de la tension qu'elle peut générer, mais aussi du système auquel elle est connectée.

De manière générale, la disponibilité et la transportabilité sont liées

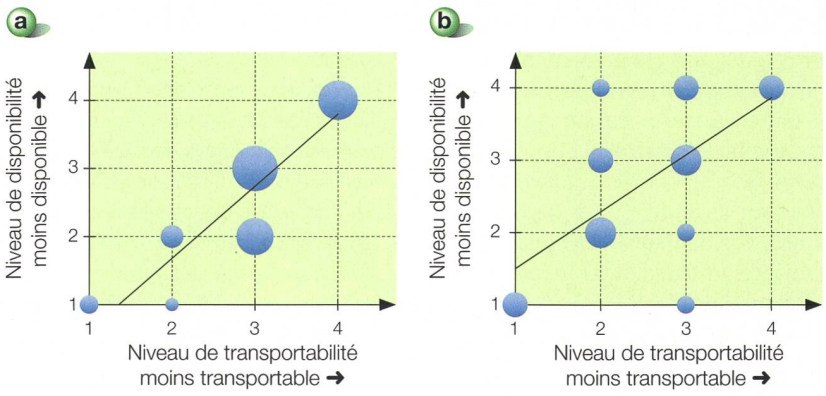
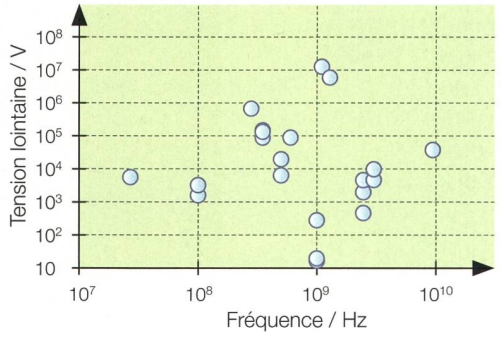


Figure 4 Disponibilité en fonction de la transportabilité : (a) couplage rayonné, (b) couplage conduit.



Figures: EPFL

Figure 5 Tension lointaine en fonction de la fréquence.

(figure 4). Les sources les plus faciles à se procurer sont en principe les petites sources portables. Les grandes sources sont généralement plus chères ou utilisent des techniques plus sophistiquées. La tendance est un peu moins nette pour les sources conduites, pour lesquelles la miniaturisation peut faire appel à des techniques plus avancées.

La figure 5 représente l'amplitude du champ électrique (la tension lointaine) en fonction de la fréquence centrale pour les sources rayonnées. Les sources les plus puissantes émettent plutôt à des fréquences autour de 200 MHz et 2 GHz, ce qui est lié à des aspects techniques. À noter cependant que les sources à large bande émettent de l'énergie bien en deçà et au delà de leur fréquence centrale.

Concernant l'évolution dans le temps, il semble y avoir une tendance de la recherche vers des sources plus compactes et donc plus facilement transportables. Plus de détails concernant les sources d'IEMI sont donnés dans les articles [25,26].

Conclusion

Dans cet article est présenté un passage en revue des sources rayonnées et conduites qui pourraient être considérées comme des sources potentielles d'interférences électromagnétiques contre des infrastructures associées aux réseaux d'énergie électrique. Il a été tenté d'inclure autant de sources que possible à partir de celles trouvées dans la littérature scientifique et disponibles sur le marché. Les sources ont été classées dans un catalogue d'après les critères utilisés communément dans le domaine des IEMI.

La classification des sources d'IEMI peut être faite soit en fonction de leur « force » ou de leurs attributs spectraux, soit selon des critères qualitatifs, tels que la transportabilité et la disponibilité. Pour analyser le potentiel des sources, des sources reportées dans la littérature scientifique ont été classées en fonction de leur portabilité et de leur disponibilité. Malgré leur grand nombre, il est possible de faire ressortir quelques tendances générales. Cette liste de sources fournit aussi des informations importantes pour les autres phases du projet visant à déterminer l'impact des IEMI sur les réseaux d'énergie électrique.

Références

[1] International Electrotechnical Commission : IEC 61000-2-13, High-power electromagnetic (HPEM) environments – Radiated and conducted. 2005.
[2] F. Sabath and H. Garbe : Risk potential of radiated HPEM environments. Proceedings of the 2009 IEEE International Symposium on Electromagnetic Compatibility, Austin (TX), USA, pp. 226-231, 2009.
[3] F. Sabath : What can be learned from documented Intentional Electromagnetic Interference (IEMI) Attacks ?. General Assembly and Scientific Symposium 2011 XXXth URSI, 13-20 Aug., pp. 1-4, 2011.
[4] R. Hoad, N. J. Carter, D. Herke and S. P. Watkins : Trends in EM Susceptibility of IT Equipment. IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, pp. 390-395, Aug. 2004.
[5] D. Nitsch, M. Camp, F. Sabath, J. L. ter Haseborg and H. Garbe : Susceptibility of Some Electronic Equipment to HPEM Threats. IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, pp. 380-389, Aug. 2004.
[6] J. Xu, W.-Y. Yin, J.-F. Mao and L.-W. J. Li : Thermal Transient Response of GaAs FETs under Intentional Electromagnetic Interference (IEMI). IEEE Transactions on Electromagnetic Compatibility, Vol. 50, No. 2, p. 340-346, May 2008.
[7] D. Månsson, R. Thottappillil, T. Nilsson, O. Lunden and M. Bäckström : Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation. IEEE Transactions on Electromagnetic Compatibility, Vol. 50, No. 2, pp. 434-437, May 2008.
[8] F. Brauer, F. Sabath and J. L. ter Haseborg : Susceptibility of IT network systems to interferences by HPEM. Proceedings of the 2009 IEEE International Symposium on Electromagnetic Compatibility, Austin (TX), USA, pp. 237-242, 2009.
[9] J. H. Hagmann, S. Dickman and S. Potthast : Application and Propagation of Transient Pulses on Power Supply Networks. Proc. of the 10th Int. Symposium on Electromagnetic Compatibility, York, England, pp. 7-12, Sept. 2011.
[10] L. Palisek and L. Suchy : High Power Microwave effects on computer networks. Proc. of the 10th Int. Symposium on Electromagnetic Compatibility, York, England, pp. 18-21, Sept. 2011.
[11] D. Månsson, R. Thottappillil, M. Bäckström and O. Lunden : Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI. IEEE Transactions on Electromagnetic Compatibility, Vol. 50, No. 1, pp. 101-109, 2008.
[12] R. Thottappillil, D. Månsson and M. Bäckström : Response of Civilian Facilities to Intentional Electromagnetic Interference (Electromagnetic Terrorism), with Emphasis on the Swedish Railway Network. Krisberedskapsmyndigheten (KBM), 2008.
[13] R. Montaño, M. Bäckström, D. Månsson and R. Thottappillil : On the Response and Immunity of Electric Power Infrastructures against IEMI - Cur-

Zusammenfassung **Verletzlichkeit der Stromnetze bei elektromagnetischen Angriffen**

Merkmale von IEMI-Quellen

Welche Auswirkungen könnten bewusst hervorgerufene elektromagnetische Störungen (Intentional Electromagnetic Interference, IEMI) auf Stromnetze haben? Derzeit läuft an der EPFL und der HEIG-VD ein Forschungsprojekt, das versucht, diese zu qualifizieren und zu quantifizieren.

Das Projekt ist wie folgt aufgebaut: Zunächst muss die elektromagnetische Umgebung, die durch diese Quellen erzeugt werden kann, definiert werden. Anschliessend sollen mithilfe eines elektromagnetischen Audits von mindestens einer elektrischen Anlage die allgemeinen Tendenzen in Bezug auf die Eintrittsstellen der Störungen, die kritischen Komponenten und die Schaltungen identifiziert werden. Dann soll eine Suszeptibilitätsanalyse zeigen, ob die Schutzeinrichtungen noch ihre Rolle bei den Wellenformen spielen, die durch die IEMI erzeugt werden können. Schliesslich können die Schaltungen experimentell und durch digitale Simulation unter Zuhilfenahme verschiedener Modelle berechnet werden. Das Ziel besteht darin, Mitigationstechnologien und Schutzstrategien vorzuschlagen, um die Auswirkungen eines möglichen Angriffs abzuschwächen.

In diesem Artikel wird ein erstes Ergebnis vorgestellt, das in der Definition der Merkmale der IEMI-Quellen besteht sowie in einem Überblick über die verzeichneten Quellen. CHe

rent Swedish Initiatives. Asia-Pacific Symposium on Electromagnetic Compatibility, Singapore, May 2008.
[14] W. A. Radasky and E. Savage: Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid. Metatech Report Meta-R-323, Jan. 2010.
[15] F. Rachidi and S. V. Tkachenko, Ed.: Electromagnetic Field Interaction with Transmission Lines. From Classical Theory to HF Radiation Effects. Southampton, Boston, WIT Press, 2008.
[16] International Telecommunication Union: ITU-T K.81, High-power electromagnetic immunity guide for telecommunication systems. 2009.
[17] D. V. Giri and F. M. Tesche: Classification of Intentional Electromagnetic Environments (IEME). IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, pp. 322-328, Aug. 2004.
[18] M. Armanious, J. S. Tyo, M. C. Skipper, M. D. Abdalla, W. D. Prather and J. E. Lawrance: Interaction Between Geometric Parameters and Output Waveforms in High-Power Quarter-Wave Oscillators. IEEE Transactions on Plasma Science, Vol. 38, No. 5, pp. 1124-1131, 2010.
[19] M. Armanious, J. S. Tyo, S. D. Keller, M. C. Skipper, M. D. Abdalla and L. L. Altgilbers: A small size resonant antenna for high power applications. 2011 IEEE International Symposium on Antennas and Propagation (APSURSI), pp. 1189-1192, 2011.
[20] F. Vega, F. Rachidi, N. Mora, B. Daout and M. Sallin: Design and optimization of mesoband radiators using chain parameters. 2011 International Conference on Electromagnetics in Advanced Applications (ICEAA), pp. 1310-1313, 2011.
[21] W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath and D. Nitsch: Survey of Worldwide High-Power Wideband Capabilities. IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, pp. 335-344, Aug. 2004.
[22] S. S. Seker, G. Apaydin and C. G. Celik: Electric field measurements of different mobile handsets in near zone. 2003 IEEE International Symposium on Electromagnetic Compatibility, EMC '03, Vol. 1, pp. 411-414, 2003.
[23] IEC 61000-2-13: Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted. 2005.
[24] D. Månsson: Intentional Electromagnetic Interference (IEMI): Susceptibility investigations and classification of civilian systems and equipment. Dissertation, Uppsala, 2008.
[25] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein and R. Cherkaoui: Overview of IEMI Conducted and Radiated Sources: Characteristics and Trends. Submitted to EMC Europe 2013.
[26] N. Mora, G. Lugrin, F. Rachidi and M. Rubinstein: On the characterization of potential IEMI threats. Submitted to the Sensor and Simulation Notes, 2013.

Informations sur les auteurs

Gaspard Lugrin a obtenu son Master en génie électrique à l'EPFL en 2011. Il y travaille actuellement comme doctorant au Laboratoire de compatibilité électromagnétique.

EPFL SCI STI FR, Station 11, 1015 Lausanne,
gaspard.lugrin@epfl.ch

Nicolas Mora Parra est doctorant au sein du Groupe de compatibilité électromagnétique de l'EPFL, sous la direction du Prof. Farhad Rachidi.

EPFL SCI STI FR, Station 11, 1015 Lausanne,
nicolas.mora@epfl.ch

Sana Sliman est ingénieure de recherche à l'Institut des technologies de l'information et de la communication (IICT) de la HEIG-VD.

HEIG-VD, Institut ICT, 1401 Yverdon-les-Bains,
Sana.Sliman@heig-vd.ch

Prof. **Marcos Rubinstein** est professeur à la Haute école spécialisée de Suisse occidentale (HES-SO) au sein de l'Institut ICT.

HEIG-VD, Institut ICT, 1401 Yverdon-les-Bains,
marcos.rubinstein@heig-vd.ch

Prof. **Farhad Rachidi** est professeur à l'EPFL. Il est président de la Conférence internationale de la protection contre la foudre (ICLP) et éditeur en chef de l'IEEE Transactions on Electromagnetic Compatibility.

EPFL SCI STI FR, Station 11, 1015 Lausanne,
farhad.rachidi@epfl.ch

Dr **Rachid Cherkaoui** est maître d'enseignement et de recherche à l'EPFL. Il y dirige le Groupe réseaux électriques. Ses activités de recherche sont relatives aux domaines de l'ouverture des marchés de l'électricité, de la production et du stockage d'énergie décentralisés et la vulnérabilité des réseaux.

EPFL STI-DEC/GR-SCI, Station 11, 1015 Lausanne,
rachid.cherkaoui@epfl.ch

[1] Cette opération est effectuée dans le but d'annuler l'atténuation du champ rayonné, qui est inversement proportionnel à cette distance.