Protection contre les interférences électromagnétiques intentionnelles

Autor(en): **Lugrin, G. / Mora, N. / Rachidi, F.**

Objekttyp: **Article**

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

Band (Jahr): **106 (2015)**

Heft 6

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-856662

Protection contre les interférences électromagnétiques intentionnelles

Peut-on utiliser les techniques classiques de la CEM ?

Les conséquences d'une attaque par le biais d'interférences électromagnétiques intentionnelles sur des infrastructures critiques, telles que les réseaux électriques ou de communication, pourraient se révéler catastrophiques. Le projet de recherche Structures a donc été mené avec pour objectif d'identifier les menaces, les risques, ainsi que les caractéristiques des infrastructures critiques. Il a en outre permis de définir des stratégies de protection efficaces, que celles-ci soient basées ou non sur les techniques classiques de la CEM.

G. Lugrin, N. Mora, F. Rachidi, M. Righero, M. Rubinstein

Les réseaux électriques, les réseaux de communication, les réseaux de transports, les structures de maintien de l'ordre et de la santé sont autant d'exemples d'infrastructures dont le fonctionnement est essentiel pour notre société. Des attaques abouties sur ces infrastructures critiques pourraient avoir des conséquences dévastatrices [1].

Or, parmi les différents types de menaces terroristes, les interférences électromagnétiques intentionnelles (IEMI) pourraient tenter des attaquants potentiels : elles peuvent en effet être générées anonymement et à une certaine distance des barrières physiques. De plus, de nombreuses sources d'interférences sont disponibles actuellement [2-4].

C'est dans ce contexte que le projet Structures a été mis sur pied. Financé par l'Union européenne, il a débuté en juillet 2012 en ayant pour objectif d'étudier les menaces d'attaques électromagnétiques sur des infrastructures critiques. Pour ce faire, les partenaires du projet ont :

- examiné les menaces ;
- identifié les caractéristiques principales des infrastructures dont dépend notre société ;
- testé des stratégies de protection actuelles et des techniques de mesure ;
- effectué des simulations et des mesures ;
- et, finalement, condensé les résultats dans des recommandations accessibles à une large audience.

Cet article donne des pistes pour évaluer les risques et se protéger contre les interférences électromagnétiques intentionnelles, et ce, en discutant en particulier la pertinence d'utiliser certaines des techniques classiques de la compatibilité électromagnétique (CEM).

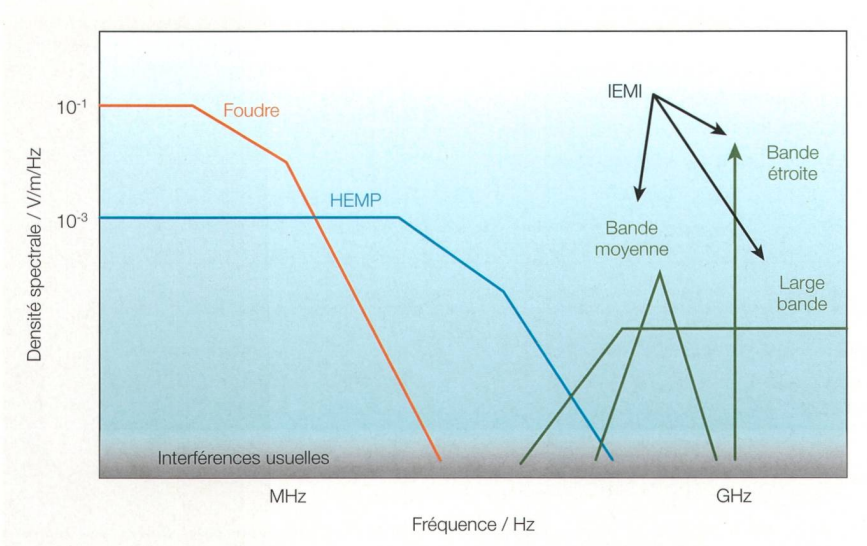

Figure 1 Comparaison des champs rayonnés par la foudre, par les impulsions nucléaires de haute altitude (HEMP) et par les IEMI, d'après [7].

Les IEMI en bref

Comme pour une interférence classique, l'énergie électromagnétique peut être soit « rayonnée » par une antenne sous la forme d'un champ électromagnétique, soit « conduite », c'est-à-dire injectée directement dans un câble et se propager comme une onde de tension et de courant.

Les IEMI peuvent, en outre, s'introduire dans une infrastructure de deux manières :

- Quand le signal d'interférence pénètre par un point d'entrée conçu pour laisser passer les signaux normaux, par exemple une antenne, on parle de couplage « front-door ».
- Au contraire, lorsque le signal d'interférence entre dans la structure par des ouvertures non conçues pour cela, comme les fentes autour d'une porte, on parle de couplage « back-door ».

Le fait de perturber la communication d'un téléphone mobile avec un brouilleur est donc un exemple d'attaque rayonnée front-door. Par contre, la création d'un champ électromagnétique puissant qui traverse les murs d'un bâtiment pour endommager des ordinateurs est un exemple d'attaque rayonnée back-door.

Domaine fréquentiel

Sur la **figure 1** [5-7], on compare les spectres fréquentiels des champs électriques dus à la foudre, à l'impulsion électromagnétique générée par l'explosion d'une bombe nucléaire en haute altitude (HEMP, pour high-altitude elec-

Niveau	Vulnérabilité du système
1	Va très probablement survivre
2	Va potentiellement survivre
3	Vulnérabilité inconnue
4	Potentiellement vulnérable
5	Très probablement vulnérable

Tableau Niveaux de vulnérabilité d'une infrastructure [8].

tromagnetic pulse), aux interférences usuelles (par exemple les bruits industriels) et aux IEMI (dans cet article, le terme « IEMI » est utilisé pour les interférences intentionnelles d'origine non nucléaire).

Les IEMI rayonnées sont représentées dans la partie droite de la **figure 1.** Elles sont en général comprises dans une plage de fréquences allant de quelques centaines de MHz à quelques GHz. Leur spectre peut prendre différentes formes : très large bande (ultrawideband), bande moyenne (mesoband) ou bande étroite (par exemple les « micro-ondes de haute puissance »). Comme présenté plus bas, la variété et l'extension de la bande passante, ainsi que les différences entre les IEMI et les interférences plus classiques rendent difficile l'utilisation des protections de la CEM classique.

Quant aux IEMI conduites, elles peuvent contenir des basses fréquences (voire du courant continu) et sont limitées en haute fréquence par les caractéristiques des câblages dans lesquels elles se propagent.

Analyse de risque

Dans cette section sont présentées très brièvement deux méthodes d'analyse de risque. Basées sur des démarches simples ou des mesures réalisables facilement, elles permettent d'évaluer le degré de résistance d'une installation et les améliorations possibles.

Analyse qualitative générale

Une analyse qualitative est proposée dans [8] pour évaluer la vulnérabilité d'une infrastructure, localisée dans un bâtiment ou sur un site, en collectant des informations de base à son propos.

Dans la pratique, un questionnaire sur l'infrastructure et son « histoire » est rempli avec l'aide des experts de l'infrastructure analysée. Si certains principes de protection n'ont pas été appliqués lors de sa construction, il y a une probabilité plus élevée que l'infrastructure soit plus vulnérable que si elle a été construite selon des recommandations typiques. Une fois que ses caractéristiques sont définies, elles sont comparées (grâce à un réseau de neurones artificiels) à une base de données d'infrastructures dont les caractéristiques et la vulnérabilité sont connues.

Cette méthode permet de classer la vulnérabilité du système dans l'un des cinq niveaux présentés dans le **tableau.** Le niveau 3, « vulnérabilité inconnue », correspond à une infrastructure dont trop de caractéristiques sont inconnues pour pouvoir donner une indication fiable de vulnérabilité.

Simple et rapide, cette méthode permet d'obtenir une première indication. Par contre, elle ne procure pas de pistes claires pour améliorer la robustesse de l'infrastructure étudiée.

Analyse basée sur les services

L'audit commence en établissant une liste des services fournis par l'infrastructure. Une analyse est ensuite réalisée pour chacun d'eux. Celle-ci est basée sur 3 axes principaux [8]:

- Les conséquences de la perte de ce service. Cet élément est évalué grâce aux renseignements donnés par les experts de l'infrastructure.
- La probabilité que ce service soit menacé par une attaque. Il s'agit là d'étudier notamment la possibilité d'approcher des sources d'interférence d'un équipement critique.
- La robustesse du service, soit celle de l'ensemble des équipements qui permettent de réaliser ce service. Les niveaux de susceptibilité (niveaux de perturbations tels que des effets indésirables apparaissent) des équipements critiques sont par exemple mesurés ou obtenus à partir de la littérature scientifique.

Finalement, la vulnérabilité de chaque service est estimée à partir de ces trois éléments. Cette méthode permet de déterminer les équipements critiques et le niveau de mitigation, c'est-à-dire le niveau d'atténuation qui rend les effets supportables.

Détermination des niveaux de mitigation

Une fois que la vulnérabilité a été estimée et que les équipements à protéger ont été identifiés, le niveau de mitigation de l'équipement peut être calculé [9]. Étant donné que le but de la mitigation est de réduire la menace à un niveau inférieur à la susceptibilité d'un équipement, l'amplitude de la mitigation requise est le rapport entre l'amplitude de la menace et la susceptibilité de l'équipement :

$$Mitigation = \frac{Menace}{Susceptibilité}$$

où la menace et la susceptibilité sont des amplitudes de champ électrique, de tension ou de courant.

Par exemple, si un équipement peut être perturbé lorsqu'il est exposé à un champ électrique égal ou supérieur à 30 V/m et qu'il risque d'être soumis à un champ de 300 V/m, le niveau de la mitigation (atténuation) devrait atteindre au moins un facteur 10.

Stratégies de protection de la CEM

Une fois que le niveau de mitigation souhaité a été défini, comment l'atteindre ?

Les techniques de protection de la CEM sont destinées à réduire la pénétration des champs rayonnés ou des perturbations conduites vers un équipement sensible. Les outils de protection de base sont le blindage, le filtrage et les dispositifs de protection contre les surtensions.

Blindage

De manière générale, les techniques de blindage conventionnelles conviennent tout à fait pour réduire le niveau des IEMI rayonnées de type back-door.

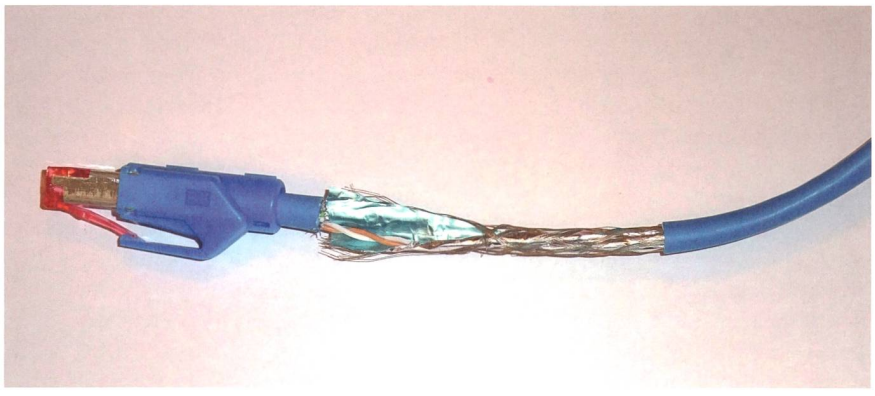

Figure 2 Exemple de câble blindé.

Figures: EPFL

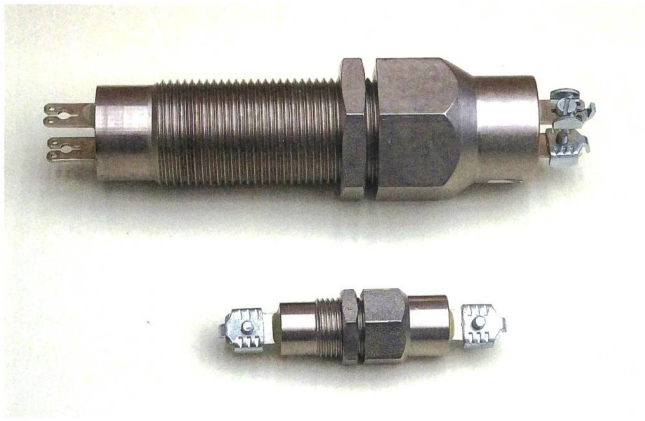

Figure 3 Deux exemples de dispositifs de protection contre les surtensions produits par la société Meteolabor.

Les équipements sensibles devraient, d'une part, être placés dans des armoires métalliques aux endroits où les champs attendus peuvent dépasser 30 V/m. Les niveaux d'atténuation à l'intérieur de ces armoires sont suffisamment élevés (jusqu'à environ 100 dB à 1 GHz) pour être efficaces. Néanmoins, il a été observé qu'à l'intérieur de certains racks munis de grandes ouvertures (vitres) les niveaux des champs à haute fréquence n'étaient pas forcément réduits, ceci étant aussi valable pour un rack dont la porte métallique reste ouverte.

D'autre part, les câbles, du fait de leur longueur, agissent comme des antennes qui captent les rayonnements perturbateurs et les conduisent jusqu'aux équipements qui y sont connectés. L'utilisation de câbles blindés (figure 2) est conseillée, car ceux-ci permettent de réduire fortement cet effet. Le blindage doit être continu, c'est-à-dire qu'aux extrémités des câbles, le blindage doit être si possible connecté sur la totalité de son périmètre à la surface métallique dans laquelle il pénètre.

Filtres

En principe, des filtres peuvent être appliqués partout où un conducteur pénètre dans un blindage. L'objectif de cette mesure consiste à stopper les courants d'interférence induits sur ce conducteur qui pourraient pénétrer à l'intérieur du blindage et atteindre un équipement électronique. En fonction de la ligne à protéger, le filtre sera de type passe-bas ou passe-bande.

Seul un nombre limité de produits commerciaux sont disponibles pour la protection contre les interférences électromagnétiques de haute puissance et ils sont généralement dimensionnés contre les impulsions nucléaires HEMP. L'information disponible à leur propos ne permet pas en principe de comprendre leur applicabilité et leurs performances contre les IEMI et relativement peu d'études ont été réalisées à leur sujet.

Dispositifs de protection contre les surtensions

Les IEMI injectées dans des câbles peuvent endommager les appareils électroniques qui y sont connectés. Pour limiter cet effet, un dispositif de protection contre les surtensions (SPD) peut être placé sur le câble qui relie la source de perturbations à sa victime. Il dispose d'une caractéristique courant-tension non linéaire qui réduit les tensions excédant le niveau acceptable par une diminution rapide de sa résistance en cas de tension élevée.

Les SPD sont abondamment mis en œuvre pour résoudre des problèmes d'interférences électromagnétiques. Cependant, une majorité de ces dispositifs sont conçus pour être montés sur des rails DIN et ne peuvent donc pas être utilisés contre les IEMI car leur comportement à haute fréquence n'est en général pas satisfaisant. Seuls les SPD de type traversant (feedthrough) présentent de bonnes performances à haute fréquence. En général, les dispositifs de type feedthrough dimensionnés pour la protection contre la foudre et les impulsions nucléaires (HEMP) qui incluent un étage de protection ayant une réponse très rapide (comme une diode TVS qui supprime les tensions transitoires) vont bien protéger contre les impulsions très courtes [10]. Deux exemples de ce type de protection sont présentés dans la figure 3.

Le choix d'un SPD pour les lignes d'énergie électrique est relativement aisé car il existe des SPD adaptés disponibles commercialement. De plus, même en l'absence de protection, ce type de lignes transmet mal les hautes fréquences et réduit donc considérablement les perturbations au-dessus de quelques centaines de MHz. La situation est plus délicate pour les lignes destinées au transfert d'information, par exemple entre une antenne de réception et un amplificateur à faible bruit. La difficulté réside dans le fait que la protection ne doit pas entraver le passage du signal en temps normal, mais qu'elle doit pouvoir encaisser beaucoup d'énergie, y compris dans la bande passante du signal utile, en cas de perturbation.

Autres méthodes de protection

Les méthodes de protection décrites jusqu'à présent sont basées sur la CEM classique. Néanmoins d'autres méthodes, comme la détection des attaques, la sécurité physique et la redondance peuvent être utilisées de manière complémentaire.

La panne d'un système électronique due à une IEMI peut être mise par ignorance sur le compte d'un matériel défectueux ou d'un « bug » d'un logiciel. Ainsi, beaucoup de temps et d'argent peuvent être gaspillés à en rechercher la cause, en particulier si la panne est intermittente. Un système de détection peut donc se révéler utile pour réagir rapidement dans le cas d'une attaque qui dure ou pour donner de précieux renseignements pour la suite en cas de perturbation de courte durée. Ces détecteurs peuvent permettre de déterminer rapidement la raison du problème et potentiellement d'en localiser la source [11]. Ils peuvent aussi commander un système qui met en œuvre des actions appropriées, comme le fait de redémarrer des machines ou de répéter certains calculs qui pourraient avoir été faussés à cause des interférences.

En fonction de l'infrastructure à protéger, il est en outre conseillé de créer des zones avec accès limité autour des systèmes critiques, ainsi que de mettre en place des règles de sécurité physique, comme des zones interdites aux visiteurs ou des contrôles d'accès.

Finalement, pour réduire l'impact d'une attaque ou le temps de réparation, il est préconisé d'appliquer le principe de redondance en installant, par exemple, des systèmes en parallèle ou des éléments de rechange. Il est aussi conseillé d'utiliser des algorithmes de calcul tolérants aux erreurs.

Conclusion

La prévention du couplage back-door et front-door en utilisant les techniques de mitigation classique est possible pour autant que les perturbations opèrent

dans les mêmes limites de fréquence et d'amplitude que les perturbations traditionnelles en CEM. En ce qui concerne les perturbations back-door, aucun impact négatif sur le fonctionnement de l'équipement protégé n'est alors à prévoir : la limitation principale réside dans le coût. Concernant la protection du couplage front-door, une mise à jour peut être requise du fait que les limiteurs et filtres commerciaux ne sont pas typiquement conçus pour supporter des perturbations avec une puissance ou une énergie importante.

Le renforcement des infrastructures critiques peut se faire typiquement par l'installation d'armoires blindées, par l'utilisation de ventilations ou de fenêtres correctement blindées et l'installation de portes métalliques avec des joints. Cependant, étant donné la complexité du problème, il est suggéré de combiner ce type de renforcement avec une stratégie de mitigation appropriée qui considère les nombreuses variables impliquées dans la menace des IEMI.

Références

[1] D. Watts : Security & Vulnerability in Electric Power Systems. 35th North American Power Symposium, University of Missouri-Rolla, Rolla, Missouri, pp. 559-566, October 2003.

[2] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein, R. Cherkaoui : Overview of IEMI Conducted and Radiated Sources : Characteristics and Trends. 2013 EMC Europe International Symposium, Brugge, Belgium, pp. 24-28, 2-6 Sept. 2013.

[3] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein, R. Cherkaoui : La vulnérabilité des réseaux électriques en cas d'attaques électromagnétiques. Caractéristiques des sources d'interférences intentionnelles. Bulletin SEV/AES 5/2013, pp. 39-43, 2013.

[4] N. Mora, F. Vega, G. Lugrin, F. Rachidi and M. Rubinstein : Study and classification of potential IEMI sources. System Design and Assessment Notes, Note 41, 2014.

[5] D. Giri and F. Tesche : Classification of Intentional Electromagnetic Environments (IEME). IEEE Transactions on EMC, Vol. 46, pp. 322-328, August 2004.

[6] D. Giri : High-power Electromagnetic Radiators : Nonlethal Weapons and Other Applications. Harvard university press ed., 2004.

[7] International Electrotechnical Commission, IEC 61000-2-13 ed.1.0: High-power electromagnetic (HPEM) environments - Radiated and conducted, 2005. Copyright 2005 IEC Geneva, Switzerland [1]. www.iec.ch.

[8] N. Mora, G. Lugrin, R. Cherkaoui, F. Rachidi, and M. Rubinstein : On the vulnerability analysis against IEMI. European Electromagnetics International Symposium EUROEM 2012, Toulouse, France, July 2-6, 2012.

[9] ITU-T K.81, High-power electromagnetic immunity guide for telecommunication systems, 08/2014.

[10] P. Bertholet, A. Kaelin, G. Lugrin, N. Mora, M. Nyffeler, F. Rachidi, and M. Rubinstein : Design and realization of a high-voltage adapter for the testing of surge protective devices against intentional electromagnetic interferences. American Electromagnetics International Symposium (AMEREM), Albuquerque, New Mexico, USA, 2014.

[11] D. Recordon, M. Rubinstein, M. Stojilovic, N. Mora, G. Lugrin, F. Rachidi, L. Rouiller, W. Hirschi, and S. Sliman : A comparator-based technique for identification of intentional electromagnetic interference attacks. 2014 International Symposium on Electromagnetic Compatibility (EMC Europe), Gothenburg, Sweden,,pp. 1257-1262, Sept 2014.

Auteurs

Gaspard Lugrin est doctorant au sein du groupe de compatibilité électromagnétique de l'École polytechnique fédérale de Lausanne (EPFL) sous la direction du Prof. Farhad Rachidi.
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.
nicolas.mora@epfl.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.
farhad.rachidi@epfl.ch

Marco Righero travaille au sein du Laboratoire des antennes et de compatibilité électromagnétique (LACE) de l'Istituto Superiore Mario Boella (ISMB).
ISMB, 10138 Torino, Italy, righero@ismb.it

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

[1] The authors thank the International Electrotechnical Commission (IEC) for permission to reproduce information from its International Standard IEC 61000-2-13 ed.1.0 (2005). All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Zusammenfassung **Schutz gegen absichtlich erzeugte elektromagnetische Störungen**

Können konventionelle Techniken aus dem EMV-Bereich verwendet werden?

Angriffe mit absichtlich erzeugten elektromagnetischen Störungen (Intentional Electromagnetic Interferences (IEMI)) auf Infrastrukturen wie Strom- oder Kommunikationsnetze können katastrophale Folgen haben. Das Forschungsprojekt «Structure» wurde daher mit dem Ziel durchgeführt, potenzielle Bedrohungen, Risiken sowie Merkmale kritischer Infrastrukturen zu identifizieren. Zudem ermöglichte es die Definition wirksamer Schutzstrategien.

Aus der Studie geht hervor, dass zur Vermeidung von IEMI-Angriffen grundsätzlich herkömmliche Mitigationstechniken für elektromagnetische Verträglichkeit (EMV), wie Abschirmung, Filterung oder die Installation von Schutzvorrichtungen gegen Überspannungen, eingesetzt werden können. Diese sind aber nur dann wirksam, wenn die Störungen innerhalb der Grenzfrequenzen und -amplituden herkömmlicher EMV-Störungen liegen. Es wird deshalb empfohlen, diese Techniken durch weitere Schutzmassnahmen zu ergänzen. So ermöglichen beispielsweise die Einrichtung von Angriffserkennungssystemen oder von physischen Sicherheitsmassnahmen (Zugangsbeschränkungen in der Umgebung von kritischen Infrastrukturen), der Einbau von Redundanzen und der Einsatz von fehlertoleranten Rechenalgorithmen einen noch wirksameren Schutz dieser Anlagen. CHe