Étude du comportement d'une chaîne de mesure de température analogique face à des impulsions électromagnétiques intentionnelles

Antoine Duguet[1,2], Tristan Dubois[1], Geneviève Duchamp[1], David Hardy[2], Franck Salvador[2]

[1]Univ. Bordeaux, CNRS, Bordeaux INP, IMS UMR 5218, F-33400 Talence, France
[2]Thales SIX GTS France SAS, 4 Avenue des Louvresses, 92230 Gennevilliers

Cette contribution s'inscrit dans le cadre d'un projet de thèse CIFRE, entre le Laboratoire IMS et Thales SIX GTS France, visant à évaluer la sécuité des systèmes pour l'Internet des Objets face à des Interférences Électromagnétiques Intentionnelles.

L'Internet des Objets (*Internet of Things*, *IoT*) est une thématique visant à faciliter l'interopérabiloté d'objets électroniques en les connectant au réseau Internet. Le nombre d'objets connectés sur le réseau est en croissance depuis quelques années et continuera d'augmenter dans les années à venir d'après [1]. Ceci favorise leur utilisation dans de plus en plus d'applications critiques. Or, les objets développés selon cette philosophie sont principalement composés de *COTS* (*Commercial Off-The-Shelf*) qui ne présentent aucun durcissement physique, pour le moment du moins.

Parmi toutes les sources d'interférences électromagnétiques, nous nous intéressons ici à celles à caractère intentionnel et offensif. De part la grande diversité des formes d'onde employées dans ce type d'attaque [2]-[4], il est difficie de définir un cadre de test de la susceptibilité des dispositifs électroniques face à des attques intentionnelles. C'est pourquoi l'objectif global de cette étude est de mettre en œuvre une méthodologie de test de la susceptibilité électromagnétique des dispositis électroniues face aux attaques électromagnétiques. L'analyse des phénomènes de perturbation observés devrait de plus permettre la proposition de règles de durcissement des systèmes électroniques de type *IoT*.

Afin de mettre en œuvre cette méthodologie, un dispositif électronique de type *IoT* a été développé sur un circuit imprimé permettant l'assemblage d'un large choix de références de *COTS*. Dans le cadre cette étude, nous avons fait le choix de constituer un système classique pour l'*IoT* comprenant notamment un microcontrôleur, des capeturs, des actionneurs ainsi qu'une communication sans fil.

L'objectif de cette contribution est de mettre en avant le comportement d'une chaîne de mesure de température analogique, implémentée sur le dispositif démonstrateur, lorsqu'elle est soumis à des signaux d'interférences de type impulsionel modulé. Le signal considéré est donc un train d'impulsions modulées autour d'une porteuse (600 MHz - 6 GHz). Ces signaux sont injectés à la cible en mode conduit par le biais d'une méthode proche de la *DPI* (*Direct Power Injection*).

Pour le moment, seul le capteur de température de la chaîne a été soumis à interférences. Les résultats vous seront présentés durant la journée de l'école dorctorale.

[1] M. Hasan, *Number of connected IoT devices*, `https://iot-analytics.com/number-connected-iot-devices/`.

[2] I. G. *et al*, "Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses," *IEEE Commun. Surv. Tutor*, t. 22, n° 1, p. 645-670, 2020.

[3] J. L. E. *et al*, "Electromagnetic Watermarking : exploiting IEMI effects for forensic tracking of UAVs," *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, p. 1144-1149, 2019.

[4] L. C. Lavau, "Impact of IEMI pulses on a barometric sensor," *2022 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, p. 290-294, 2022.