N° 60
Décembre
2022

Lettre d'information de

Guerrelec

Si vis pacem para bellum…electronicum

Le mot
Du Président

Chers adhérents,

Après deux années difficiles, marquées par une crise sanitaire mondiale, des événements climatiques exceptionnels et une crise majeure en Europe, l'association GUERRELEC se devait d'apporter sa contribution à la réflexion dans son domaine. Après le succès du symposium de l'AOC EUROPE qui s'est tenu en France à Montpellier en mai dernier, GUERRELEC vous propose d'organiser au printemps prochain un séminaire sur l'analyse des informations recueillies sur la guerre en UKRAINE et plus généralement sur le retour de la guerre en haute intensité, afin d'en déduire des enseignements et des perspectives sur la guerre électronique du futur. Ce séminaire sera placé sous la haute autorité du ministre des Armées et se déroulera au Mont Valérien, dans l'enceinte de la DIRISI.

Enfin je vous souhaite à tous et à tous ceux qui vous sont chers une excellente année 2023.

Le Président

SEMINAIRE

« GUERRE ELECTRONIQUE et HAUTE INTENSITE »

Leçons du conflit ukrainien

MARDI 6 JUIN 2023

SEMINAIRE

ACTIONS DANS LE SPECTRE ELECTROMAGNETIQUE ET HAUTE INTENSITE

Organisé par l'ASSOCIATION GUERRELEC, chapitre La Fayette de l'AOC

Présentation de la journée par le président de Guerrelec
Pierre GRANDCLEMENT (9h00 – 9h10)

Introduction « Guerre Electronique et Renseignement dans la haute intensité »
(9h10 – 9h30)

Le déroulement des opérations dans le spectre électromagnétique en Ukraine
(9h30 - 10h00)

Convergence Cyber-GE : opportunité ou nécessité ?
(10h00 – 10h30)

Le renseignement du futur
(10h30 – 11h00)

Table ronde sur l'adaptation de la guerre électronique aux conflits modernes
(11h30 – 12h15)

REPAS OFFERT PAR GUERRELEC (12h30 – 14h)

La Guerre Electronique arrive dans l'espace
(14h00 – 14h30)

L'accélération de la montée en TRL des développements
(14h30 – 15h00)

L'impact des normes sur les temps de développement et les coûts des programmes
(15h00 – 15h30)

Table ronde sur la GE et le renseignement : entre souveraineté et approche européenne
(16h00 – 16h45)

Conclusion du séminaire
(16h45 – 17h05)

Conclusion de la journée par le Président de Guerrelec
Pierre GRANDCLEMENT (17h05 – 17h15)

Russie et brouillage des communications : le système MURMANSK-BN

Murmansk-BN est un système moderne de guerre électronique développé par la société russe KRET. Le système est conçu pour brouiller les communications à très longues distances et a été développé comme faisant partie d'un ensemble stratégique de guerre électronique. Il fonctionne comme un réseau centré. Le système est entré en service dans les armées russes en 2014 et a été déployé la même année lorsque le 475th centre indépendant de GE de la marine russe l'a installé en Crimée, au sud de Sébastopol. Un autre système est installé dans l'enclave russe de Kaliningrad et peut-être un troisième à l'est de l'Ukraine. Le rôle premier de ce système est de brouiller les émissions en HF des forces de l'OTAN et en particulier le système global de communications HF des Etats-Unis et du système de communications satellitaires HF (High-Frequency military satellite Global Communications System - HFGCS). D'après des sources russes, il peut brouiller les systèmes de communications jusqu'à une distance de 5 000 à 8 000 kilomètres.

Le système **Murmansk-BN** s'articule en différents camions de type militaire emportant les équipements dédiés comme les quatre mâts extensibles. Deux de ces mâts sont portés par des camions de marques *Kamaz* ou *Ural* et des remorques équipées de mâts d'antennes. Ces mâts peuvent se déployer jusqu'à une hauteur de 32 mètres. Chaque système *Murmansk-BN* complet se compose de quatre ensembles d'antennes, ce qui fait seize antennes en tout. Chaque ensemble de quatre antennes peut fonctionner seul ou en groupe. Selon des rapports, le système peut être intégré dans le commandement de la guerre électronique et de contrôle. Le système est composé également d'un module de commandement porté par un camion *Kamaz 6350* et un autre *Kamaz 6350* porteur d'un groupe électrogène afin d'alimenter le système antennaire. Le groupe électrogène est capable de fournir une puissance de 400KW permettant au *Murmansk-BN* de supprimer les communications HF dans une zone pouvant aller jusqu'à 640 000 km^2. D'autres véhicules composent le dispositif comme un camion transport de carburant et un pour le transport des servants.

Le camion porteur d'une antenne extensible est du type *Kamaz 53501* à châssis 8x8. Chaque camion tire une remorque équipée d'une autre antenne. Le *Kamaz 5350* est disponible en châssis 4x4, 6x6 ou 8x8. La cabine est pourvue de trois sièges. Ils ont un poids à vide de 9 200 kg et peut emporter 6 000 kg. Ils sont équipés d'un moteur *Kamaz AZ-740.13.260* diesel turbocompressé d'une puissance de 260 chevaux. Leur vitesse maximum sur route est de 100km/h et l'autonomie est de 1 000 kilomètres. Le *Kamaz 6350* est un camion qui a été développé à partir de 1987 et qui est entré en service au sein de l'armée russe en 2002. Il a un poids à vide de 11 400 kg et une charge utile de 10 000 kg.

Murmansk-BN est l'un des plus efficaces systèmes de guerre électronique dans le monde. C'est un système de brouillage spécialement étudié contre les systèmes de l'OTAN et les communications satellitaires HF américaines. Il est efficace pour la reconnaissance radio, l'interception et la suppression du signal ennemi de proche à une distance pouvant aller de 5 000 à 8 000 kilomètres. Il couvre l'entière bande des ondes courtes de 3 à 30 MHz qui est habituellement employée par les aéronefs et les navires de guerre. Son temps de mise en œuvre est généralement de 72 heures. Le système est capable de détecter et brouiller les émissions HF ennemies des unités stratégiques et tactiques de commandement et de contrôle. Le brouilleur est spécifiquement destiné à s'attaquer aux systèmes de communications HF y compris contre le *HFGCS.* D'après des informations de sources russes, les systèmes de bord des avions *F-35 « Lightning II »* de l'USAF seraient gravement perturbés par les interférences créées par le *Murmansk-BN*. Les pilotes des chasseurs furtifs américains ont constaté de fréquentes pannes de leurs systèmes d'avionique en survolant la mer Baltique et la mer Noire. La guerre électronique des systèmes russes

commence à avoir de l'impact sur les avions furtifs de l'USAF. Le *Murmansk-BN* scanne automatiquement une large zone. Si des émissions radio y sont détectées, le système débute le brouillage en bandes étroites ainsi l'ennemi ne peut plus échanger d'informations. *Murmansk-BN* est capable d'intercepter les communications entre navires de guerre, avions et satellites. Il est également capable de bloquer le flux d'informations venant des satellites vers les unités de combat spécifiques. Cela est très intéressant car les satellites de reconnaissance sont capables de guider précisément les missiles vers leurs objectifs. *Murmansk-BN* rend les bombes guidées ennemies sans effet. Les avions de reconnaissance et d'alerte avancée sont incapables de partager leurs informations (toujours de sources russes).

Quelques chiffres

TYPE : Système mobile de brouillage des Communications satellitaires
Fréquences de brouillage : 3 à 30 MHz
Taille de la zone de brouillage : 640 000 km^2
Distance de brouillage : 5 000 à 8 000 km
Objectifs brouillés : Capable d'intercepter et de brouiller les Coms entre les navires, les avions et les satellites
Temps de déploiement : 72 heures
Véhicules : Kamaz 53501 et Kamaz 6350

Pierre Alain ANTOINE

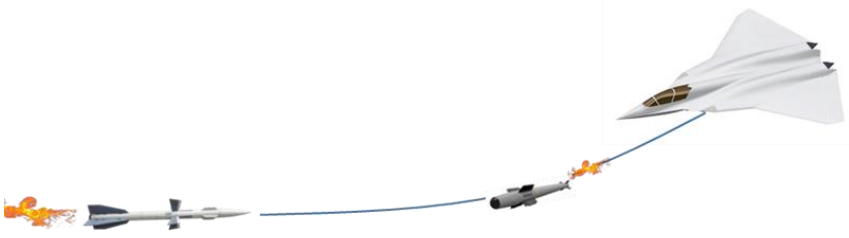
Un nouveau paradigme pour l'autoprotection : le missile anti-missile aéroporté

Les systèmes de missiles et les technologies associées évoluent à une vitesse croissante. L'émergence puis la prolifération de systèmes intégrés de défense aérienne (IADS) est un défi pour les opérations aériennes dans les conflits de haute intensité et une contrainte forte lors d'opérations plus restreintes.

Les nouveaux missiles, qu'ils soient air- air ou sol-air, sont de plus en plus robustes face aux techniques classiques d'autoprotection, communément appelées « soft kill ». Le développement de nouvelles capacités pour les autodirecteurs de missiles, telles que la détection multimode (ex. EM et IR) par exemple, tend à renforcer cet état de fait.

Les anciens systèmes de missiles laisseront progressivement la place à des systèmes modernes, mais représenteront encore durant de longues années une menace importante, cette concomitance complexifiant la tâche des systèmes d'autoprotection. La demande de systèmes d'autoprotection threat agnostic, moins dépendants d'une connaissance fine des menaces et plus robustes aux évolutions technologiques de ces dernières, se fait de plus en plus pressante.

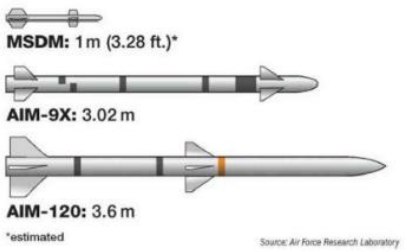
Ainsi, les évolutions technologiques dans le domaine des missiles permettent d'envisager, dans un avenir assez proche, la réalisation d'effecteurs d'autoprotection de type « petit missile » permettant l'interception et la neutralisation du missile assaillant avant impact.



Lorsque disponible, cette capacité « hard kill » constituera un changement de paradigme pour l'autoprotection terminale car elle augmentera considérablement les chances de survie d'une plateforme engagée par des missiles. Ce sera tout particulièrement pertinent dans des environnements caractérisés par la multiplication des menaces dites « pop-up », par la non-colocalisation des conduites de tir actives et des effecteurs (y compris le multi-domaine) et l'introduction de systèmes de désignation performants basés sur des capteurs passifs.

Les défis technologiques à relever sont ainsi nombreux. L'effecteur doit être compact, optimisé en coût et très précis. Le système de détection et de conduite de tir doit non seulement fournir une détection fiable mais également permettre la simplification de l'effecteur. L'ensemble doit également faire preuve d'une grande réactivité et nul doute que l'intelligence artificielle présentera une forte plus-value. Enfin, le système complet doit permettre la neutralisation du missile assaillant, quel que soit son secteur d'arrivée, tout en garantissant la sécurité du porteur vis-à-vis de l'éventuelle gerbe d'éclats générée.

Mais, en regard de l'importance de l'enjeux, des solutions commencent à émerger : un programme de démonstrateur a ainsi déjà été lancé aux États-Unis.



Fort de son métier de missilier et de concepteur de systèmes d'armes, actif aussi bien dans les domaines de la protection de zones que du combat aérien, et fort de ses compétences en matière de systèmes d'autoprotection - en particulier en détection des missiles, MBDA entend être un acteur majeur de cette évolution de l'autoprotection.

Des initiatives sont en cours au sein de notre société pour jeter les bases de solutions innovantes et relever les défis techniques associés à cette nouvelle capacité. Fondées sur un travail en collaboration étroite avec les utilisateurs permettant de cerner le juste besoin opérationnel, nous sommes convaincus qu'elles rencontreront également l'adhésion des administrations concernées et des plate-formistes. Au-delà de l'importance opérationnelle de cette nouvelle capacité, il est également crucial pour l'industrie européenne impliquée dans l'autoprotection d'avancer au bon rythme sur ce type d'innovation, faute de risquer un décrochage important vis-à-vis de ses concurrents.

Sébastien Palaprat – MBDA France

L'Ukraine a modifié des MiG-29 pour utiliser le missile américain antiradar AGM-88 HARM

D'après le site opex360.com de tenu par Laurent Lagneau et paru fin août 2022, le Pentagone a mentionné la livraison de missiles AGM-88 HARM (High speed, Anti-Radiation Missile), utilisés principalement pour détruire les radars adverses.

En clair, il s'agit du MiG-29 « Fulcrum » qui en est le porteur. « Nous avons déterminé que l'intégration de l'AGM-88 HARM sur le MiG-29 comme étant techniquement faisable » a déclaré le responsable du Pentagone. Ainsi a-t-il poursuivi, « Nous leur avons fourni cette capacité. Il s'agit donc en fait de la deuxième tranche de missiles HARM que nous leur livrons ».

S'agissant des capacités aériennes ukrainiennes, « nous nous sommes concentrés sur la façon dont nous pouvons améliorer leur flotte d'avions existante. C'est là que les missiles HARM entrent en jeu, en leur donnant cet avantage supplémentaire. Et nous nous sommes également procuré des milliers de pièces de rechange pour leurs MiG dans le monde entier », a-t-il expliqué.

Depuis l'armée de l'air ukrainienne ne se prive pas d'employer cette nouvelle capacité SEAD (Supression of Enemy Air Defence) obtenue en « Crash Programm ».

Pierre-Alain ANTOINE

Impact de la convergence des technologies numériques et de l'ingénierie numérique dans un système de défense électronique aéroporté

Depuis une décennie maintenant, ceux qui ont eu la chance d'assister physiquement à la conférence de l'Association of Old Crows à Washington ont vu l'omniprésence du concept américain de domination du Spectre Electromagnétique. En parallèle, l'évolution rapide de technologies issues des télécommunications, d'une part, et de l'ingénierie numérique, d'autre part, conduira à une nouvelle génération de systèmes de Guerre Electronique aéroportés.

Cet article propose une analyse de l'impact de ces deux grandes tendances sur les systèmes de défense électronique aéroportés.

Numérisation du Spectre Electromagnétique

Pendant de nombreuses années, les ingénieurs de GE ont mis au défi les fabricants de composants hyperfréquence de fournir des solutions de numérisation à bande ultra-large (jusque 20 GHz). Mais en 2010, un point de bascule s'est produit lorsque le marché des télécommunications est devenu le domaine réclamant les exigences les plus élevées pour les composants clés que sont les convertisseurs Analogique-numérique et leur contrepartie les convertisseurs Numérique-analogique. Les développements des réseaux mobiles avec la 4G, la 5G et bientôt la 6G conduisent à un nouvel ensemble de composants réalisant le rêve de tous les ingénieurs GE : la conversion RF directe sur porteuse. Cela signifie que le signal d'intérêt est directement numérisé dès sa réception à des fréquences respectant le critère de Shannon (La représentation discrète d'un signal exige des échantillons régulièrement espacés à une fréquence d'échantillonnage supérieure au double de la fréquence maximale présente dans ce signal) et élimine ainsi les dégradations précédemment apportées par les premiers étages de réception analogique.

En conséquence, les capteurs, effecteurs et systèmes de GE vont entrer dans une nouvelle ère : celle du système dont les traitements s'appliquant directement sur des échantillons numériques pourra être défini par logiciel avec toutes les possibilités qui en résultent, suggérant des traitements d'Intelligence Artificielle IA de plus en plus efficaces sur de grands volumes de données.

Ingéniérie Numérique

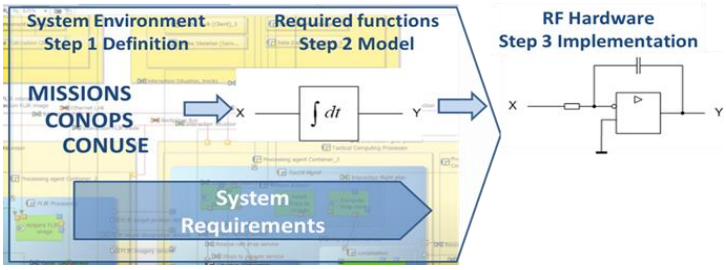
Pour l'architecture de système GE où le temps de réaction rapide et la dépendance croisée des fonctions (détection, brouillage, leurre) sont critiques, le Software Defined System apportera un degré de liberté plus élevé dans la programmation, ce qui implique de mettre en œuvre de nouvelles méthodes d'ingénierie comme nous le verrons ci-dessous.

Depuis 2010, la simulation GE et l'expertise en ingénierie des systèmes, reposant notamment sur « l'ingénierie des systèmes basée sur le modèle » (Model Based System Engineering, MBSE) offrent la possibilité de maîtriser la complexité de l'environnement GE, la conception du système et en rendre explicite l'architecture. L'ingénierie des systèmes basée sur le modèle permet de virtualiser l'ensemble données et tâches, des exigences à la conception puis à l'intégration. L'ingénierie numérique est un ensemble de données, de processus et d'outils qui forme et informe un jumeau numérique (digital twin) du système réél. Les outils d'ingénierie système basée sur le modèle, tels ceux qui font partie de la plateforme CAPELLA, sont nécessaires au développement de l'ingénierie numérique. Ils s'appuient, au minimum, sur 3 étapes :

- L'environnement Modèle et simulation est la couche décrivant la mission, les menaces, le concept d'opération, le concept d'utilisation. Ces données évoluent rapidement, et certainement plus vite que la capacité de définir les exigences du système et de concevoir un nouveau système.
- Le modèle fonctionnel est la couche définissant ce qu'un système est censé faire, sans inclure de détails sur la façon dont il doit être mis en œuvre. L'évolution de l'environnement définit le nombre de fonctionnalités.

- Le modèle de mise en œuvre et sa simulation sont une étape au cours de laquelle l'utilisateur et l'industriel doivent définir des exigences système fortes et suffisamment robustes pour faire face à l'évolution de l'environnement au cours des 20 prochaines années. Le modèle de mise en œuvre et la simulation d'un système dépendent de la complexité de son environnement, de ses fonctionnalités et des types de technologie choisis pour le mettre en œuvre.

Le processus classique consistait à définir les missions et le CONOPS dans la phase initiale du projet, puis à développer le modèle fonctionnel et enfin, après une analyse logique, à concevoir la partie Hardware de l'architecture.



Conception du système de GE

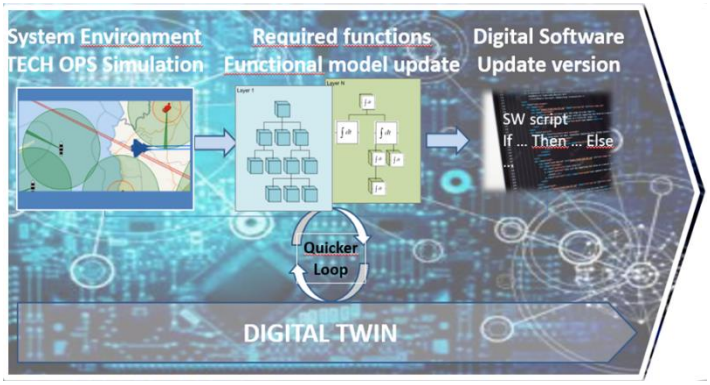
Pour les systèmes de GE, il s'agissait de sélectionner le nombre de récepteurs nécessaires pour détecter toutes les menaces même le signal le plus faible en couvant toute la plage de dynamique. La phase de conception et la phase de validation ont utilisé les exigences du système qui sont fournies par les principaux documents de référence. Dans la phase de mise en œuvre, le compromis physique était un processus long et complexe pour gérer les exigences complexes du système de GE et des technologies RF Hardware de pointe. La mise à niveau du système, en fonction de l'évolution des menaces et de l'environnement, nécessitait des évolutions du matériel, mais le nombre de changements restait limité pendant la durée de vie d'un système en raison de l'effort souvent très important de rétrofit.

La contribution majeure du nouveau **système défini par logiciel et de l'ingénierie de conception** permet d'éviter la phase de compromis de mise en œuvre complexe décrite précédemment.

Les exigences opérationnelles sont définies avec un ensemble de scenarii pendant toute la durée de vie du produit:

- La simulation de scénario permet de suivre ou de mieux anticiper l'évolution rapide de l'environnement,
- Le **jumeau numérique** du système GE est progressivement défini au travers d'un ensemble d'outils de simulation,
- Un continuum de simulation et de modélisation à partir de simulations de scénarios, de modélisations technico-opérationnelles et de modélisations fonctionnelles est mis en place en phase de développement, avant l'implémentation finale dans le hardware numérique ultra large bande.

La simulation et la modélisation deviennent alors des outils permettant un travail continu au travers de discussions fréquentes impliquant l'utilisateur final et le spécialiste du système de GE. La simulation de la mission, Conops et Conuse, conduit directement à l'optimisation du nombre d'exigences et de performances de la fonction système. L'ensemble des fonctions peut aussi être amélioré pour répondre à l'évolution des besoins opérationnels : l'évolution du système devient, à la fin du processus d'ingénierie numérique, une mise à jour logicielle du système en service. Le jumeau numérique du système GE est conservé pendant la durée de vie du système et permet de simuler la pertinence d'évolutions futures.



Nouvelle conception du système de GE numérique : mise à jour fréquente pour répondre à l'évolution rapide de l'environnement

Le délai de livraison peut être optimisé grâce à la possibilité de fournir une mise à jour uniquement par logiciel. Certains auteurs poussent le concept encore plus loin, comme dans « Take the red pill: the new digital acquisition reality » [Will Roper 15 Sept 2020], où l'acquisition numérique est connectée à l'ingénierie numérique pour

proposer des évolutions dans le cycle de vie du système avec des optimisations automatiques de l'architecture en cohérence du budget du donneur d'ordre et aux besoins opérationnels de la force. Mais il reste encore du travail pour atteindre cet objectif.

En résumé :

Tant la convergence des technologies que l'ingénierie numérique offrent l'opportunité tout au long de la vie du produit, depuis sa phase amont d'expression des besoins opérationnels jusqu'aux étapes finales de son évolution, en passant par ses étapes de développement et de validation :

- développer une nouvelle génération d'architecture de GE pour faire face à l'évolution de l'environnement, en particulier les défis de dominance du spectre électromagnétique,
- pour gérer et gérer les fonctions GE exigeantes (Détection, Identification, Localisation, brouillage, Leurrage).

L'ingénierie numérique du système de GE permettra de concevoir la future génération distribuée sur différentes plates-formes ouvrant une nouvelle dimension à la guerre électronique.

Ainsi, le développement des architectures physique numériques et ouvertes ainsi que celui des processus d'ingénierie basés sur les modèles conduit Thales à adapter ses moyens et ses équipes pour tirer profit des architectures numériques complexes modernes et les intégrer dans les produits GE en cours de développement.

Nicolas Breuil, Architecte Ligne Produits Guerre Electronique Aéroportée
Yves Urien, Responsable Ligne Produits Guerre Electronique Aéroportée

---

Les Sentinelles oubliées-Le renseignement humain derrière le rideau de fer

Auteur : Roland Piétrini

Editions : Pierre de Taillac

Taille et nombre de pages : 19 x 14 cm, 278 pages

ISBN : 978-2-364-45221-3

Prix : 16,90 euros

« Les sentinelles oubliées, ce sont des hommes qui ont assuré de 1947 à 1991, des missions de renseignement particulièrement risquées derrière le rideau de fer. Roland Piétrini était l'un d'entre eux. Il révèle les méthodes utilisées par la Mission militaire française de liaison (MMFL) près du haut commandement soviétique en Allemagne de l'est et par les postes militaires des ambassades. Son récit fait découvrir le quotidien de ces militaires français opérant au cœur des pays alors ennemis : ceux du pacte de Varsovie. Et ces missions n'étaient pas sans risque. Ils étaient pourchassés par le KGB et furent souvent pris pour cible…certains en sont morts. A lire absolument dans cette période de fortes tensions entre l'est et l'ouest.