Barrière intelligente à haute efficacité de détection et localisation précise d'intrusion par fibres optiques pour la surveillance périmétrique des sites sensibles

M. GIUSEFFI[1], V. DEWYNTER[1], P. FERDINAND[1], S. MAGNE[1], S. ROUGEAULT[1], J.-M. PALUT[2], M. PINABIAU[2], C. CANEPA[3], J.-C. DAROCHA[3], B. GAUVAIN[4], A. LE GALL[4], D. LE NAN[4], R. BLIN[5], S. PIOT[5], J.-F. SAGEAU[5], L. DEVATINE[6] et G. PASTEUR[6]

[1]CEA LIST, Laboratoire de Mesures Optiques, Centre d'Etudes de Saclay, F-91191 Gif-sur-Yvette cedex, France.

[2]CEA SPACI, Laboratoire de Protection Physique, Centre d'Etudes de Saclay, F-91191 Gif-sur-Yvette cedex, France.

[3]ACOME, Usines de Romagny, 50140 Mortain

[4]DCNS Services Brest, CS 72 837, 29228 Brest Cedex 2

[5]SITES, 2 bis Avenue du Centre, 92500 Rueil-Malmaison

[6]RTE, Immeuble Ampère, 34 Rue Henri Régnault, 92068 Paris La Défense Cedex

marie.giuseffi@cea.fr, veronique.dewynter-marty@cea.fr, pierre.ferdinand@cea.fr, sylvain.magne@cea.fr, stephane.rougeault@cea.fr,jean-michel.palut@cea.fr, michel.pinabiau@cea.fr, christophe.canepa@acome.fr, jean-claude.darocha@acome.fr, bernard.gauvain@dcn.fr, alain.le-gall@dcnsgroup.com, david.le-nan@dcn.fr, rebl@sites.fr, sp@sites.fr, jfs@sites.fr, louis.devatine@rte-france.com, gerard.pasteur@rte-france.com

Résumé – Le projet *SmartFence* vise à améliorer la sécurité des sites sensibles par l'introduction d'une nouvelle technologie, issue du monde des télécommunications optiques, pour la surveillance périmétrique. Le système intègre un instrument optoélectronique connecté à l'une des extrémités d'un câble sensible innovant contenant plusieurs fibres optiques, lui-même déployé sur la clôture. Ce système de surveillance associé à une base de données intelligente, permet de déterminer le profil des déformations et des courbures le long du câble sensible, provoquées lorsque l'on tente d'escalader la clôture, avec une localisation spatiale métrique du point où a lieu l'intrusion, et ce sur une portée multi kilométrique.

Abstract – *SmartFence* project aims to provide an enhanced perimeter security related to critical sites or infrastructures by introducing an advanced concept coming from the optical fibre telecommunication technology. The measurement system will contain an optoelectronic unit connected to one input of an innovative sensitive optical cable including several fibres, mounted directly on the fence. This system based on optical sensing approach associated to a smart data base enables to determine strains and bending profile along the sensitive cable, due to an intruder climbing the fence, with a one-meter spatial localisation of the intrusion point, on a multikilometric range.

1. Contexte et motivations du projet

Ces dernières années, le contexte mondial de la sécurité, désormais qualifiée de « globale », a atteint un niveau d'instabilité qui ne s'était pas vu depuis longtemps. Les nombreuses tensions mondiales, découlant principalement d'activités terroristes, d'espionnage ou d'actions criminelles continuent de laisser planer de graves conséquences pour les pays occidentaux, et leurs infrastructures essentielles. Pour s'opposer à ces menaces avec succès, les forces de sécurité doivent faire preuve d'une vigilance constante et bénéficier de moyens de plus en plus performants.

Ainsi, aux Etats-Unis, suite aux attentats du 11 septembre 2001, le gouvernement a créé le DHS (*Department of Homeland Security*) qui est le résultat de la fusion de 22 agences, et a mis en place une stratégie nationale concernant ce secteur. *De facto*, les dépenses fédérales de la défense ont bondi de 13,2 milliards de dollars en 2000 à 41,3 milliards en 2004, pour atteindre cette année 42,7 milliards (dont 1 milliard pour la recherche en seule sécurité intérieure).

Dans ce domaine, les produits et solutions présents sur le marché peuvent être classés en trois catégories. Tout d'abord, ceux qui étaient présents avant les attentats du 11 septembre. Ce segment est en déclin. La seconde est composée de produits ou technologies qui existaient avant les attentats mais n'étaient pas commercialisés. Ce segment est en forte progression. Enfin, la troisième catégorie présente des

solutions et technologies nouvelles ou en phase de R&D. Ce segment connaît un fort potentiel de croissance. Au total, en 2005, le marché mondial du *Homeland Security* était estimé à 42,4 milliards de dollars ; 54 % étant détenus par les Etats-Unis, 20 % par l'Europe et 26 % par le reste du monde.

Dans un tel contexte, la R&D dans le domaine de la sécurité civile, vise un certain nombre d'objectifs (tant pour les secteurs civils que militaires) pour lutter plus efficacement contre les risques et menaces.

C'est pourquoi au niveau européen, parallèlement à ce qui se fait outre-Atlantique, les états et l'Europe ont, depuis 2004, fait de cette thématique un objectif affirmé de leurs agendas respectifs. Les états membres réfléchissent désormais à des mesures qui pourraient être mises en place afin d'améliorer les échanges d'informations entre eux, constituer des équipes communes d'enquêteurs et renforcer la protection des infrastructures sensibles de l'Union Européenne. C'est également dans ce contexte que de nombreux *clusters* européens se sont créés, par exemple dans le domaine de la sûreté maritime, sans oublier les Pôles de compétitivité français, très actifs dans ce domaine[1].

Au niveau européen, cette politique, initiée par le *GOP*[2], s'est tout d'abord déclinée dans le cadre du programme PASR *Preparatory Action in the field of Security Research* (avec le projet SeNTRE en particulier, suivi actuellement de STACATO) puis aujourd'hui dans le cadre du PERS (Programme Européen de Recherche sur la Sécurité) du 7ème PCRD, et parallèlement en France[3] par l'action d'un comité intergouvernemental, et dans celui de l'appel CSOSG de l'ANR. De leur côté, les entreprises impliquées dans les secteurs de la sécurité/défense renforcent également leur axe de management stratégique dédié à ce secteur. Un colloque du Haut Comité Français pour la Défense Civile (HCFDC) organisé en partenariat avec la DGA, et regroupant les principaux acteurs correspondants, a d'ailleurs récemment fait le point sur ce thème le 29 mars 2007 [1].

Le présent projet s'inscrit donc dans ce contexte et vise à améliorer la sécurité des sites sensibles grâce à une nouvelle technologie, issue des télécommunications par fibres optiques, pour la surveillance périmétrique.

Il faut savoir, qu'au niveau de la sécurité globale d'un site, il convient de considérer différentes menaces liées au type d'intrus (allant du petit rôdeur, en passant par le voleur occasionnel, la bande organisée, l'agent d'un service action étranger, jusqu'au terroriste). Face à ces différentes menaces, dans certains lieux sensibles, voire très sensibles, la protection se doit d'être élevée, donc difficilement 'fraudable' dès lors que l'intrus se trouve dans son lobe de couverture[4].

[1] Cf. le Livre Vert – Vers une politique maritime de l'Union : Une vision européenne des océans et des mers.

[2] C'est sous la présidence Grecque qu'a été créé le *GOP* (*Group of Personalities),* chargé de réfléchir au concept de sécurité au plan européen, puis d'établir un plan d'action et un budget correspondant, de manière à préparer le chantier européen dans ce domaine.

[3] Cf. le récent « Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme » de mars 2006.

[4] Il est en fait très difficile de se protéger contre des sabotages menés par des gens bien entraînés. Plusieurs tentatives d'infiltration effectuées à titre expérimental et réussies par des agents de services spécialisés l'ont malheureusement démontré. Sans parler de l'action spectaculaire de Greenpeace à la centrale nucléaire de Belleville-sur-Loire dans le Cher, le 27 mars 2007 …

Parmi les applications immédiates, on peut naturellement citer : les centrales nucléaires, les installations industrielles telles que les usines chimiques (SEVESO), les bases militaires, les ambassades, les centres de télécommunications, les complexes gaziers et pétroliers, les sites pyrotechniques, les parcs automobiles, les ports et aéroports, les lignes ferroviaires grande vitesse … sites dont certains sont souvent loin d'être immunes aux agressions ou même aux sabotages, et qui requièrent des systèmes périmétriques anti-intrusion de plus en plus sophistiqués.

Le but de ce projet est donc de développer une technologie innovante de détection périmétrique fondée sur les fibres optiques. Un certain nombre de technologies utilisées dans les télécommunications et le domaine des Capteurs à Fibres Optiques (CFO) sont en effet duales : fibres et connectique associée, composants d'extrémité, moyens de tests comme la réflectométrie ... De fait, les avancées en terme de performances et de disponibilité de ces composants et matériels peuvent maintenant être mises en application dans le domaine de la sécurité, et faire bénéficier ce secteur de moyens de mesure/détection plus performants que l'existant.

L'approche innovante envisagée vise la surveillance performante de zones et d'infrastructures critiques, ainsi qu'un enregistrement permanent des événements et des situations d'alerte. La solution développée sera opérationnelle 24 h sur 24, quelles que soient les conditions environnementales en s'insérant dans le système global géré par le PC de sécurité du site concerné. De par le principe de détection mis en œuvre, elle assurera un meilleur niveau de détection, et un taux de fausses alarmes bien mieux maîtrisé que ce qu'offrent les solutions traditionnelles. Elle pourra être déployée aisément et à un coût optimisé le long des périmètres à protéger, sur une longueur pouvant aller jusqu'à plusieurs km, voire des dizaines de km !

2. Enjeux, objectifs et verrous scientifiques

Les approches existantes sont les câbles à chocs et les systèmes à détection de coupure. Analysons succinctement leurs avantages et inconvénients respectifs.

2.1 Câbles à chocs

Le principe des câbles à chocs est de mesurer les vibrations, soit par l'intermédiaire de fils électriques soit *via* des fibres optiques. Ils permettent de détecter une menace de base (intrus non 'spécialiste') et offrent donc une sécurité de faible niveau, pour des applications qualifiées de peu 'sensibles', comme par exemple les hangars d'aéroport ou les parcs automobiles.

Les avantages de cette technologie sont que les câbles sont peu onéreux et discrets. Par contre, elle présente un taux non négligeable de fausses alarmes, par exemple en conditions météorologiques difficiles (grêle, vent …) conduisant ainsi

sur une portée kilométrique à de fréquentes alarmes intempestives. Les câbles ne sont en outre pas sensibles aux mouvements lents, aspect exploité par les intrus ‘spécialistes’. Ils ne peuvent pas non plus être installés le long d’un lieu de passage. En pratique, la levée de doute requiert une technologie complémentaire, telle des caméras vidéo, ce qui accroît le coût global de l’installation.

2.2 Détection de coupure

Cette technologie consiste à détection la coupure d’un élément (soit un barreau équipé d’un câble électrique, soit tout le panneau de la barrière devenu détecteur). Si une fibre remplace le fil électrique, on obtient en cas d’intrusion : la détection de coupure (localisation par panneau) et la détection de l’écartement des barreaux, *via* les pertes optique induites.

La sécurité est de faible niveau et concerne des applications peu ‘sensibles’ (intrus non ‘spécialiste’). Les éléments de détections sont simples et discret mais il faut en complément pallier le risque d’escalade qui est non détectable, par des ‘bavolets’ en partie haute, qui peuvent être inclinés entre 30° et 90°, ou bien encore des concertinas (fils barbelés équipés de lames de rasoir ...).

2.3 Enjeux du projet *SmartFence*

Ainsi, comme toute nouvelle technologie se doit de pallier les inconvénients des techniques traditionnelles, l’approche objet du projet *SmartFence* présentera :

- une meilleure efficacité de détection,
- un faible taux de fausses alarmes,
- une quasi infraudabilité,
- une faible sensibilité à l’environnement.

Ce sont donc ces enjeux qui sont visés dans le projet. Pour y parvenir, les verrous à lever sont les suivants. Il faudra parvenir à développer un câble multifibres discriminant les effets de l’environnement d’une agression réelle. Une base de données logicielle contenant des signatures d’événements types (environnement, menaces) sera également développée. Il s’agira enfin valider le concept global du triple point de vue technique, ergonomique et économique.

FIG. 1 : Barrière de tests de système de sécurité périmétrique (photo CEA)

3. Méthodologie mise en œuvre

Dans cette approche, un câble sensible contenant plusieurs fibres optiques est déployé sur ou au sein de la barrière. Il s’agit d’un Capteur à Fibres Optiques qui permet de déterminer le profil des déformations (allongements) et des courbures le long du câble, ainsi que leurs orientations spatiales, avec une localisation métrique sur une portée multi kilométrique. L’instrument optoélectronique connecté à son extrémité permet la surveillance temps réel. Le câble détecte les déformations et les courbures provoquées lorsque l'on tente d'escalader ou de détériorer la clôture, et un algorithme de traitement permet de localiser le point d'intrusion et de déclencher l’alarme à bon escient.

La constitution d’un tel câble à fibres optiques permet de discriminer une courbure induite par l’influence du vent ou d’un simple appui sur la clôture, de celle induite par un intrus malveillant.

Cette possibilité sera exploitée et couplée à une base d’événements acquis par retour d’expérience, de manière à accroître la fiabilité de la détection par une réduction du taux de fausses alarmes.

De plus, l’insensibilité aux champs électromagnétiques (isolation galvanique) de la silice constituant la fibre, la rend insensible aux interférences électromagnétiques qui affectent les technologies ‘électriques’. La fibre est donc indétectable par tous moyens, électriques ou électroniques, rendant la détection ‘furtive’. Simultanément, cette insensibilité apporte un avantage complémentaire : l’électronique déportée en bout de fibre ne risque pas d’être détruite par induction électromagnétique comme cela peut être le cas avec un système filaire de la part d’un agresseur averti.

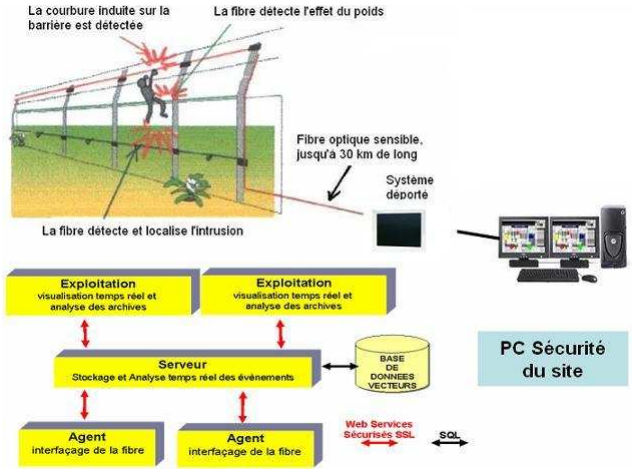

FIG. 2 : Barrière intelligente équipée du câble multifibres, associée au système opto-électronique + logiciel type base de données intelligente

4. Retombées scientifiques et industrielles

4.1 Retombées scientifiques

Le projet *SmartFence* permettra de prouver que le concept de câble à fibres optiques utilisé permet de remonter aux courbures appliquées à la structure et à leurs orientations. En outre, il mettra en œuvre une instrumentation innovante à Fibres Optiques pour cette application et conduira au développement d'une base de données événementielle, et d'un logiciel 'intelligent' de détection, permettant la discrimination et la localisation des évènements.

4.2 Retombées industrielles

Le projet *SmartFence* aura diverses retombées industrielles pour les partenaires du projet. Il va engendrer la mise au point d'un procédé industriel de fabrication du câble de mesure multifibres optiques. Un procédé de détection globale sera mis au point et pourra, au-delà de ce secteur, trouver des applications dans un certain nombre d'autres domaines et ainsi ouvrir d'autres secteurs de marchés de la sécurité des biens et des personnes. Nous mettrons au point et qualifieront une véritable 'barrière intelligente'. Cela permettra une prise de parts de marché, en France, en Europe et dans le reste du monde, dans un secteur très mal couvert par l'industrie française à ce jour.

5. Applications

Il y a clairement deux types de cibles sur le marché des systèmes de sécurité anti-intrusion que le système que nous proposons pourra viser. D'une part, le secteur public, et d'autre part le secteur privé.

Les marchés publics concernent, de manière non exhaustive, les ministères, les pénitenciers, les ambassades, les centres de R&D nationaux, les bâtiments de stockage & d'archivage (grandes bibliothèques, archivages nationaux ...), les bases militaires (différents corps d'armée), …

Les marchés privés concernent plutôt les ports, et aéroports, les centrales nucléaires, les sites pétrochimiques, les pipe-lines, les parcs automobiles, les sites pyrotechniques (stockage d'explosifs, de feux d'artifice …), …

Précisons que dans ces deux secteurs de marché, même si les procédures de sélection et d'achat diffèrent, tant les motivations que les critères qui prévalent sont les mêmes.

L'achat d'un système anti-intrusion répond naturellement à un besoin de sécurité. C'est un investissement non négligeable qui nécessite un long processus de réflexion, et qui le cas échéant se caractérise par différentes étapes comme un appel d'offre.

Les critères d'achat constituent l'ensemble des éléments considérés lors de la prise de décision, à savoir :

La sensibilité de détection: Il s'agit de la capacité du système à détecter/localiser une agression de manière « intelligente », par exemple perpétrée par des 'spécialistes',

Le taux d'alarmes intempestives : Le défaut majeur des systèmes de sécurité actuels, placés en extérieur, est le déclenchement de fausses alarmes. Ce critère est important, il caractérise la fiabilité du produit,

La résistance du produit : Les attaques perpétrées contre les sites de haute sécurité sont parfois effectuées par des personnes entraînées possédant un matériel sophistiqué, il faut donc un système qui puisse néanmoins fonctionner,

La rapidité de la détection : En cas d'alerte, le signal de détection/localisation généré par le système à destination du PC de sécurité du site doit être fourni rapidement pour permettre aux forces de sécurité d'intervenir à temps,

Le temps de réarmement : Après toute tentative d'intrusion, il faut que la réactivation du système de surveillance s'effectue rapidement pour éviter qu'une seconde tentative ait lieu alors que le système est 'aveugle',

Le coût d'achat et de maintenance : Si l'efficacité ou les performances d'un système sont les motivations principales d'achat, il en est de même pour le prix et le coût de maintenance du système.

Ces différents points seront bien sûr pris en compte dans le cahier des charges et évalués grâce aux tests fonctionnels et aux essais terrain du système de détection développé.

Conclusion

Le projet *SmartFence* va démarrer début 2008. Nous aurons pour ce projet une approche expérimentale, comparative avec les systèmes de sécurité périmétrique existant afin de pallier les problèmes de ces derniers. L'approche innovante envisagée permettra une surveillance vraiment performante (faible taux de fausses alarmes, grande détectivité …) et permanente de zones et infrastructures critiques (centrales nucléaires, installations industrielles, complexes gaziers, pétrochimiques, aéroports …) et un enregistrement des événements et situations d'alerte, 24 h sur 24, quelles que soient les conditions climatiques, en s'insérant dans le système global géré par le poste commande de sécurité du site concerné. Un tel système devrait permettre d'une part améliorer la sécurité des sites concernés et d'autre part permettre aux partenaires de gagner des parts de marché et de se positionner sur le domaine de la sécurité périmétrique.

Références

[1] http://www.hcfdc.org