Agence Nationale de la Recherche ANR	**Date d'ouverture de l'appel à projets de recherche :** **29/01/07**	DGA

CONCEPTS SYSTEMES ET OUTILS POUR LA SECURITE GLOBALE

CSOSG

Appel à Projets 2007

Date limite d'envoi des projets de recherche : <u>mercredi 18 avril 2007 à 12h</u>

MOTS CLES :

sécurité globale, protection du citoyen, infrastructures vitales, réseaux, gestion de crise, systèmes, mode d'organisation, technologies, analyse de risques, vulnérabilités.

La mise en œuvre de l'appel à projets est réalisée par l'Université de Technologie de Troyes, qui a été mandatée par l'ANR pour assurer la conduite opérationnelle de l'évaluation et l'administration des dossiers d'aide. L'Université de Technologie de Troyes met en place sur le site web de l'appel à projets un espace dédié, destiné à la mise en relation de partenaires pour faciliter la constitution de consortium (consulter www-csosg.utt.fr).

Informations importantes

Date limite d'envoi des projets sous forme électronique :

le mercredi **18 avril 2007 à 12h** sur le site *www-csosg.utt.fr*

et

Date limite d'envoi des projets sous forme papier (en recommandé avec accusé de réception) : le mercredi **18 avril 2007 à 24h**, le cachet de la poste faisant foi, à l'adresse :

Université de Technologie de Troyes
Appel à Projets ANR -CSOSG
12, rue Marie Curie, BP 2060
10010 Troyes Cedex.

Contacts :

Correspondants dans l'unité support de l'ANR :

pour toute information de nature technique ou scientifique :

En priorité, Patrick Lallement – pl.csosg@utt.fr – Tél : 03 25 71 56 80

Eric Châtelet – ec.csosg@utt.fr -Tél : 03 25 71 56 34

Philippe Cornu – phc.csosg@utt.fr - Tél : 03 25 71 56 89

pour toute information de nature administrative et financière :

Miguel Inacio – mi.csosg@utt.fr -Tél : 03 25 71 85 59

Il est recommandé aux proposants :

1. de lire attentivement l'ensemble du présent document et le règlement relatif aux modalités d'attribution des aides de l'ANR avant de déposer un projet de recherche ;
2. de ne pas attendre la date limite d'envoi des projets pour réaliser leur soumission de projet de recherche par voie électronique. A cette fin, la pré inscription sur le site de l'appel à projets devra être effectuée au plus tard une semaine avant la date limite de dépôt des dossiers ;
3. de respecter la taille limite des dossiers déposés qui est de 10 Mo ;
4. de consulter si besoin l'Université de Technologie de Troyes, unité support de l'ANR (de préférence par courrier électronique) ;
5. de consulter les sites suivants pour tous compléments d'informations :

http://www-csosg.utt.fr
http://www.agence-nationale-recherche.fr

Sommaire

1. Contexte et objectifs de l'appel à projets 4
2. Champ de l'appel à projets 6
3. Critères d'éligibilité et d'évaluation 10
4. Dispositions relatives au financement 12
5. Modalités relatives aux pôles de compétitivité 13
6. Modalités de soumission 13

Annexes 15

1. Procédure de sélection 15
2. Modalités relatives aux pôles de compétitivité 15
3. Définitions 16
4. Modalités relatives au suivi des projets 18
5. Résumés des projets sélectionnés lors de CSOSG 2006 18

1. Contexte et objectifs de l'appel à projets

1.1. Contexte

Assurer la sécurité des biens et des personnes dans un espace de liberté et de justice, tel est l'objectif de la stratégie européenne de sécurité adoptée par le Conseil Européen en 2003 et réaffirmée en 2004, suite aux attentats de Madrid.

Le rapport d'un Groupe de Personnalités, mandaté par la Commission Européenne soulignait la nécessité de financer la recherche sur un champ très large de missions de sécurité très proche du concept de sécurité globale[1].

La sécurité globale peut être définie comme la capacité d'assurer à une collectivité donnée et à ses membres un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles[2]. Cette définition recouvre de fait les différentes composantes suivantes : sécurité économique, sécurité sanitaire, sécurité informatique et numérique (données, réseaux…), sécurité du territoire, aérienne et maritime, sécurité civile… Ces différentes composantes de la sécurité recouvrent notamment la protection contre les actions de type malveillance (lutte contre le terrorisme, la criminalité et la fraude…).

Cette approche générale, qui se caractérise par un traitement d'ensemble de la sécurité, systémique et transversal, traitant des causes comme des effets, est celle retenue par la Commission Européenne dans le volet sécurité (PERS) du programme cadre de recherche de l'U.E. (7ème PCRD, 2007 -2013). Au travers des travaux déjà lancés depuis 2004 (travaux préparatoires sur la recherche en sécurité : PASR) et des groupes de réflexion européens réunissant acteurs publics et privés, l'Europe a défini quatre grandes missions verticales de sécurité :

- la sécurité du citoyen (protection contre le terrorisme et le crime) ;
- la sécurité des infrastructures, des sites et des réseaux ;
- la sécurité des frontières (terrestres et maritimes);
- la gestion de crise, intervention et réparation[3].

Du point de vue national, une coordination interministérielle (en place depuis 2005), a apporté son plein soutien à l'initiative européenne d'un programme sur la sécurité, recensé les besoins étatiques et entamé un dialogue avec les acteurs nationaux de la recherche académique et industrielle en sécurité. Enfin, en 2006, une liste de priorités nationales de recherche en sécurité a été établie et la première édition du programme ANR « Concepts Systèmes et Outils pour la Sécurité Globale » a été lancée et a permis le financement de 14 projets de recherche (cf. annexe 5).

1.2. Objectifs

La recherche en sécurité globale est une recherche finalisée, capable de faire émerger des solutions concrètes face à des enjeux globaux sur le court, moyen et long terme. Pour ce faire,

[1] Research for a secure Europe : report of "Group Of Personalities" (GOP) in the field of security research, 2004, http://europa.eu/eur-lex/en/com/cnc/2004/com2004_0590en01.pdf (executive summary en annexe)

[2] Définition de l'INHES (Institut National des Hautes Études de Sécurité)

[3] Rapport final de l'ESRAB, (European Security Research Advisory Board), septembre 2006, http://ec.europa.eu/enterprise/security/articles/article_2006-09-25-kf_en.htm

elle doit favoriser les approches systémiques, transverses et pluridisciplinaires en associant des partenaires industriels, académiques ainsi que les acteurs de la sécurité, qu'ils soient privés ou publics (prescripteurs et/ou opérateurs).

Une approche systémique doit considérer les vulnérabilités et l'interdépendance des systèmes de plus en plus complexes qui régissent les flux et infrastructures vitales nécessaires à nos sociétés, comme les réseaux d'énergie, les réseaux informatiques, qui gèrent en particulier les flux financiers, traitent et diffusent l'information, les transports de personnes et de biens, les complexes industriels, les systèmes sanitaires, les réseaux de distribution d'eau…
L'approche système est également nécessaire vis-à-vis de la nature des solutions à apporter afin de proposer des concepts et architectures assurant la cohérence entre les phases de planification, de prévention, de surveillance, de détection, de protection, de gestion de la crise et de restauration de l'activité. Ces concepts et architectures doivent permettre d'orienter et de cibler des axes d'efforts technologiques et organisationnels essentiels au traitement des menaces et des risques.

La transversalité est nécessaire au regard de la diversité des acteurs, de l'hétérogénéité et du grand nombre des secteurs d'activités. Les défis imposés par les vulnérabilités pesant sur ces secteurs d'activité, de façon globale, réclament une meilleure synergie des acteurs afin de rationaliser les approches et démultiplier les efforts isolés.

La recherche en sécurité couvre par nature de très nombreux domaines et disciplines scientifiques qui sont appelés à concourir à l'amélioration de la sécurité. Elle fait appel aux sciences dites « dures » (physique, chimie, sciences de la vie, sciences de l'ingénieur, mathématiques, informatique…) et aux sciences humaines et sociales (sociologie, ethnologie, anthropologie, gestion, économie, droit, psychologie, ergonomie…) tant l'interdépendance entre les technologies, les modes d'organisation et l'homme, conditionne l'efficacité de tout système de sécurité.

Une approche prospective, novatrice et structurée de la sécurité nécessite d'articuler efficacement la recherche amont et aval, dans l'objectif de fournir des solutions appliquées mais aussi applicables, tant du point de vue de l'acceptabilité des systèmes que de leur efficacité pratique et économique. En particulier, il est absolument nécessaire d'anticiper les phases de certification et de normalisation des systèmes et équipements de sécurité. Une recherche partenariale, associant les acteurs de la recherche, mais aussi les prescripteurs et opérateurs de la sécurité, permettra de déboucher sur des avancées significatives répondant aux attentes concrètes des citoyens.
La recherche en sécurité globale représente donc de très forts enjeux en termes d'innovation, de compétitivité économique et de souveraineté.

En 2006, pour sa première édition, le programme Concepts Systèmes et Outils pour la Sécurité Globale avait pour ambition de susciter des projets de recherche répondant à ces caractéristiques à l'aide de cinq thématiques transverses (analyse de la vulnérabilité, gestion de l'alerte, modélisation et simulation, traitement de l'information, sécurité et société).

Pour son édition 2007, l'Agence Nationale de la Recherche lance un appel à projets en partenariat avec la Délégation Générale pour l'Armement (DGA).

Cet appel à projets ciblera un certain nombre de fonctions spécifiques ou capacités, sous ensembles des missions suivantes, qui constituent donc le périmètre de la sécurité couvert :

- la sécurité du citoyen qui recouvre la lutte contre le terrorisme et la grande criminalité, les problématiques liées à la « petite » criminalité et à la délinquance mais également la gestion de la preuve (police scientifique par exemple) ;

- la protection des infrastructures vitales et des réseaux (transport, énergie, informatique) et leurs interconnexions ;

- la gestion de crise, quelle que soit son origine (malveillance, catastrophe d'origine naturelle ou accidentelle) et cela lors des phases de préparation et de planification jusqu'à la réparation ;

- la sécurité des frontières maritimes terrestres et aériennes ainsi que la gestion des flux matériels et immatériels et des interconnexions.

A contrario, les domaines suivants sont exclus de ce périmètre et par conséquent du champ de l'appel à projets : la sécurité routière (traitée dans le cadre du programme ANR PREDIT), la sécurité alimentaire (abordée dans le programme ANR PNRA à l'exception des actions de malveillance sur la chaîne alimentaire), la sécurité / sûreté de fonctionnement des systèmes lorsqu'ils ne traitent exclusivement que des solutions répondant à des dysfonctionnements de nature endogène. Ce qui relève du « principe de précaution », dans les domaines de la biologie et de la santé par exemple, est également exclu. La sécurité des Systèmes d'Informations peut être abordée dans le champ de l'appel à projets, lorsqu'elle fait partie des solutions à mettre en œuvre afin de répondre aux missions et capacités visées. On notera que la sécurité et la sûreté des Systèmes d'Informations fait l'objet d'un programme spécifique de l'ANR (Sécurité et Sûreté Informatique).

Le choix des fonctions/capacités visées, a été effectué dans un souci de cohérence avec d'une part les priorités nationales établies par la coordination interministérielle sur la recherche en sécurité depuis juin 2006, et d'autre part, avec le déroulement du programme européen PERS[4], en évitant les doublons inutiles mais en préparant également les équipes de recherche françaises aux futurs appels à projets européens (comme le PERS post 2008).

2. Champ de l'appel à projets

L'ambition de l'appel à projets 2007 est de renforcer l'orientation mission du programme CSOSG mais également de promouvoir l'émergence d'une thématique de recherche par nature systémique, transverse, interdisciplinaire et partenariale.

Il sera visé une recherche finalisée de haut niveau regroupant les acteurs pertinents, publics et/ou privés, académiques et industriels, opérateurs ou prescripteurs de la sécurité, dans une logique de partenariat (cf. critères d'éligibilité, § 3.1).

De par la nature du sujet, l'interdisciplinarité est considérée comme un facteur clef de succès et, en particulier, la participation d'équipes des sciences humaines et sociales est fortement souhaitée pour la plupart des sujets.

Les projets de recherche pourront traiter de tout ou partie d'une thématique en répondant aux objectifs décrits, qui devront être déclinés selon des cas d'étude concrets s'y rattachant de façon pertinente (et reposant sur une analyse de risque par exemple). Les projets devront contribuer à une meilleure compréhension des enjeux organisationnels, sociaux, culturels, économiques, juridiques et/ou technologiques de la sécurité et/ou démontrer la faisabilité de systèmes, méthodes et outils à l'aide de réalisations ou démonstrateurs limités.

[4] Voir programme de travail de la thématique sécurité du 7ème PCRD, 22 décembre 2006, http://cordis.europa.eu/fp7/cooperation/security-en.htm

Axe thématique 1 - Protection du citoyen : anticipation, prévention et surveillance

L'efficacité des moyens d'anticipation et de prévention repose au préalable sur une analyse de la vulnérabilité des systèmes en tenant compte des aspects organisationnels, techniques ainsi que les modes de relations entre les différents acteurs. Les outils de traitement de l'information sont essentiels à la perception de la situation issue de données très largement hétérogènes.

Les systèmes de surveillance des flux de personnes et de marchandises se doivent d'être de plus en plus performants en regard de l'intensification des échanges et de leur complexité.

Ces trois axes de recherches seront traités selon les indications suivantes.

L'analyse prospective des menaces et des risques recouvre :

- l'analyse des vulnérabilités des systèmes dont celles liées à l'émergence des nouvelles technologies (comme l'évolution et la généralisation des technologies de l'information ou de la communication et leur utilisation à des fins malveillantes) ou à la complexité organisationnelle liée au grand nombre d'acteurs et à leur diversité ;

- l'analyse d'impact sur les systèmes lorsque ces vulnérabilités sont exploitées de façon intentionnelle ou non ;

- la méthodologie pour la prise en compte des scénarios complexes (juxtaposition des risques variés, effets dominos) et le recensement des modes opératoires associés ;

- les méthodes et moyens permettant d'une part la prévention des actes comme ceux de la petite et de la grande criminalité, et d'autre part, la réduction des effets de ces actes.

Les outils de traitement de l'information et des connaissances sont composés :

- des outils d'extraction, de croisement et de fusion de données hétérogènes;

- des outils de veille, de recherche, l'indexation et l'exploitation de données.

En particulier, ces outils devront permettre d'acquérir une meilleure connaissance des réseaux criminels, terroristes… et d'améliorer le suivi de leurs activités. On s'intéressera également aux nouveaux moyens, méthodes et outils contribuant à développer les capacités d'investigation (police scientifique et criminelle).

Dans le champ de la surveillance des flux de personnes et/ou de marchandises, les projets de recherche devront traiter plus précisément :

- des systèmes et des outils pour la surveillance (avec détermination de caractéristiques) voire l'identification et l'authentification des personnes, de manière coopérative ou non coopérative, sans contact ou à distance ;

- des systèmes d'aide à l'exploitation des flux de données issus des différents capteurs en temps réel et en temps différé ;

- des systèmes et outils de surveillance et de contrôle de l'intégrité des marchandises, containers et véhicules sur toute la chaîne logistique ;

- des systèmes de détection des produits illicites ou dangereux sur tout ou partie de la chaîne logistique (flux et noeuds intermodaux).

Au-delà des solutions technologiques, les projets devront obligatoirement traiter des aspects éthiques, sociaux et juridiques liés à la capture puis à l'utilisation de ce type d'information.

Axe thématique 2 - Protection des infrastructures fermées ou ouvertes

Les projets de recherche traitant de cet axe thématique devront définir précisément les solutions potentielles selon un angle systémique prenant en compte les avancées technologiques mais aussi les contraintes liées aux modes d'organisation, de doctrine d'emploi et de coopération des divers acteurs publics et privés impliqués dans la protection des infrastructures.

Ces systèmes viseront à la protection et à la sécurisation :

- de sites sensibles et vitaux comme des complexes industriels, les aéroports, les ports, les sites de production, de stockage ou de distribution de l'énergie… ;

- d'un espace ouvert et complexe comme une rue passante, un espace public, un centre commercial, un hall d'aéroport, une entrée de port, un lieu d'interconnexion de différents modes de transport… ;

- d'événements planifiés et ouverts comme des manifestations culturelles, sportives ou exceptionnelles (type rencontres du G8)…

Axe thématique 3 - Protection des réseaux

Deux types de réseaux feront l'objet des sujets de recherche quant à l'amélioration de leurs systèmes de protection vis-à-vis d'attaques et actes malveillants :

Pour les réseaux d'eau potable et de la chaîne alimentaire et pharmaceutique, les projets devront traiter des :

- systèmes de contrôle et de supervision à même d'identifier, localiser et contrer, en temps réel ou adapté, les menaces biologiques et chimiques, sur le réseau d'eau potable ;

- outils et dispositifs permettant de diagnostiquer la présence d'agents biologiques et chimiques puis d'assurer la traçabilité des lots contaminés intentionnellement.

Pour les réseaux et moyens de transport, deux axes de recherche spécifiques seront abordés :

- la protection des systèmes de contrôle–commande et de supervision, embarqués ou non, dans les transports ainsi que leur interdépendance ;

- les outils de simulation des transmissions d'épidémies et de pandémies par les transports, permettant l'analyse des situations spécifiques liées à la nature du moyen de transport examiné (aérien, terrestre ou maritime) et de l'agent épidémique retenu.

Axe thématique 4 – La gestion de crise : déploiement et protection des intervenants

Cette thématique a pour objet l'amélioration des systèmes des outils et/ou des modalités pour l'intervention des acteurs de la sécurité publique et civile lors des premiers instants de la crise et de sa gestion sur le terrain :

- on s'intéressera aux modalités d'émergence des crises, d'élaboration des savoirs et des cadres cognitifs mobilisés (pour l'anticipation, la prévention, la gestion et le retour à la normale…), à la conception et à la mise en œuvre des actions et des mesures, aux dimensions organisationnelles, aux perceptions et aux comportements des différents acteurs individuels et collectifs (population, intervenants, experts, pouvoirs publics…), aux conditions effectives de gestion et de prise en charge de la sécurité parmi l'ensemble des règles, des contraintes et des nécessités qui pèsent sur l'activité ;

- en termes d'approche système, on s'intéressera aux modes d'analyse et de perception de la crise, aux modes d'organisation, à la modélisation comportementale des personnes impliquées (intervenants, population touchées) ainsi qu'à leur coopération, pour la simulation et l'entraînement ;

- les outils permettant la tenue de situation lors de la gestion de crise et lors d'un déploiement rapide (mode de communication, de transports d'urgence, systèmes d'information et de commandement…) ;

- les équipements d'intervention individuels à large spectre de protection permettant de réduire la contrainte physiologique, d'améliorer les communications entre les intervenants et d'accroître les performances des équipements et des systèmes de protection face aux différents types d'agression ;

- les systèmes mobiles et portables de détection et d'identification NRBCE (Nucléaire, Radiologique, Biologique, Chimique et Explosifs).

Axe thématique 5 – La gestion de crise : neutralisation et réparation

Lorsque la crise est survenue, les capacités visées permettront un retour rapide à la normale.

Les projets de recherche devront traiter des :

- systèmes et moyens de recherche et de secours aux victimes (moyens permettant la prise en charge de très nombreuses victimes par exemple) ;

- systèmes, moyens et méthodes permettant le fonctionnement en mode dégradé puis le retour à la normale (ou ordinaire) ;

- moyens de réhabilitation et de décontamination de zones (bâtiments, lieux publics) suite à un attentat et /ou un incident NRBCE.

On traitera également les moyens de neutralisation de véhicules automobiles à distance, non coopératifs, et ne présentant aucun danger pour ses occupants et pour l'environnement au sens large.

3. Critères d'éligibilité et d'évaluation

Sont décrits ci-après les critères d'éligibilité et d'évaluation utilisés au cours de la procédure de sélection décrite en annexe (§1).

3.1. Critères d'éligibilité

Pour être éligible, le projet doit satisfaire les conditions suivantes :

- les dossiers sous forme électronique et sous forme papier (les deux documents devant être identiques) doivent être soumis dans les délais, dans les formats demandés et être complets ;
- le coordinateur du projet ne doit pas être membre du comité d'évaluation du programme ;
- le projet doit entrer dans le champ de l'appel à projets ;
- la durée du projet doit être comprise entre 18 mois et 36 mois ;
- le projet doit réunir au moins deux partenaires ;
- le projet doit compter au moins un partenaire appartenant à chacune des catégories suivantes :
  - o Organisme de recherche (université, EPST, EPIC…) [5] ;
  - o Entreprise [6].

  Les projets relevant uniquement des sciences humaines et sociales, pourront être proposés en mobilisant seulement des organismes de recherche.
- Equilibre du partenariat :
  - o le partenariat entre organismes de recherche et entreprises devra être effectif sur toute la durée du projet sauf pour les projets uniquement SHS;
  - o l'implication d'un ou plusieurs prescripteur(s) ou opérateur(s) public(s) ou privé(s) de la sécurité [7] sera explicite au travers de leur participation au consortium en tant que partenaire **ou** membre d'un comité de pilotage ou de suivi du projet [8].

Important : les dossiers ne satisfaisant pas aux critères d'éligibilité ne seront pas soumis pour avis d'experts extérieurs et ne pourront en aucun cas faire l'objet d'un financement.

3.2. Critères d'évaluation

Les projets seront examinés selon les critères suivants :

[5] cf. définition complète en annexe § 3.3

[6] cf. définition complète en annexe § 3.3

[7] cf. définition complète en annexe § 3.3

[8] Un comité de suivi et de pilotage dont la composition, le rôle et les tâches seront explicités, le cas échéant dans le descriptif technique du projet.

- Pertinence de la proposition au regard des orientations de l'appel à projets

  o adéquation aux axes thématiques de l'appel à projets (cf. § 2) ;

  o présentation claire des missions de la sécurité globale abordées, selon une approche système, pluridisciplinaire et multi-acteurs de la recherche en sécurité ;

  o contribution réelle :

  - à une meilleure compréhension des enjeux organisationnels, sociologiques ou technologiques de la sécurité ;
  - à la démonstration de la faisabilité de systèmes par la levée de verrous technologiques ou méthodologiques.

- Qualité scientifique et technique :

  o clarté d'exposition des objectifs contribuant effectivement à une meilleure sécurité des citoyens et/ou à la compréhension des enjeux organisationnels, humains et technologiques de la sécurité ;

  o excellence scientifique en termes de progrès des connaissances par rapport à l'état de l'art ;

  o caractère innovant ;

  o levée de verrous technologiques.

- Méthodologie, qualité de la construction du projet et de la coordination :

  o positionnement par rapport à l'état de l'art ou de l'innovation technologique ;

  o faisabilité scientifique et technique du projet, choix des méthodes ;

  o structuration du projet, rigueur de définition des résultats finaux (livrables), identification de jalons ;

  o qualité du plan de coordination (expérience, gestion financière et juridique du projet) ;

  o stratégie de valorisation et de protection des résultats du projet, gestion des questions de propriété intellectuelle ;

  o stratégie en termes de gestion de la confidentialité des informations, des résultats et des livrables (en précisant les niveaux de diffusion de l'information).

- Impact global du projet :

  o utilisation ou intégration des résultats du projet par la communauté scientifique, industrielle ou la société, et impact du projet en termes d'acquisition de savoir-faire ;

  o perspectives d'application industrielle ou technologique et de potentiel économique et commercial, plan d'affaire, intégration dans l'activité ; industrielle. Crédibilité de la valorisation annoncée.

- Qualité du consortium[9] :

[9] Pour un projet partenarial organisme de recherche/entreprise, la labellisation du projet par un pôle de compétitivité (cf. § 5) est considérée comme un indicateur de qualité. Cet indicateur sera pris en compte dans le cadre de l'examen par le comité de pilotage. Il est rappelé qu'il n'est pas nécessaire que tous les partenaires d'un projet soient membres du pôle ou localisés dans sa région pour que ce projet puisse bénéficier du label de "projet de pôle".

- o niveau d'excellence scientifique ou d'expertise des équipes ;
- o adéquation entre partenariat et objectifs scientifiques et techniques ;
- o complémentarité du partenariat ;
- o implication réelle des utilisateurs finaux (partenariat, comité de suivi ou de pilotage).
- o rôle actif des PME.

- Adéquation projet – moyens et faisabilité du projet :

  - o calendrier ;
  - o le projet propose une organisation du pilotage des travaux garantissant un démarrage effectif rapide à la notification du projet ;
  - o justification de l'aide demandée selon les lots techniques, par partenaires, et par type de dépenses envisagées.

Les modalités de l'évaluation des projets par le comité d'évaluation seront précisées dans son règlement intérieur, qui sera publié avant le 15 mars 2007 sur les sites Internet de l'ANR et de l'appel à projets (voir adresses en page 2).

4. Dispositions relatives au financement

Le financement attribué à chaque partenaire sera apporté sous forme d'une aide non remboursable, selon les dispositions du « Règlement relatif aux modalités d'attribution des aides de l'ANR », disponible sur le site internet de l'ANR.

Seuls pourront être bénéficiaires des aides, les partenaires résidant en France, les laboratoires associés internationaux des organismes de recherche et des établissements d'enseignement supérieur et de recherche français ou, les institutions françaises implantées à l'étranger. La participation de partenaires étrangers est néanmoins possible dans la mesure où chaque partenaire étranger assure son propre financement dans le projet.

Important : il ne sera pas attribué d'aides de montant inférieur à 15 000 € à un partenaire d'un projet.

Pour les entreprises[10], le **taux maximum** d'aide est le suivant :

Dénomination	**Taux maximum d'aide pour les PME[11]**	**Taux maximum d'aide pour les entreprises autres que PME**
Recherche fondamentale[12]	Non Applicable	Non Applicable
Recherche industrielle	60% des dépenses éligibles	50% des dépenses éligibles
Développement pré-concurrentiel	Non Applicable	Non Applicable

[10] cf. définitions données en annexe § 3.3

[11] en particulier, est une PME une entreprise **autonome** comprenant jusqu'à 249 salariés, avec un chiffre d'affaires inférieur à 50 M€ ou un total de bilan inférieur à 43 M€ (cf. Annexe § 3.3).

[12] cf. définitions données en annexe § 3.1

L'objectif de l'ANR est que la majorité des projets reçoivent un financement d'un montant compris entre 500 k€ et 1500 k€. Toutefois, il n'est pas n'exclu que soient financés des projets d'un montant inférieur ou supérieur.
Les bénéficiaires pourront commander des travaux à des tiers extérieurs (en France ou dans l'Espace Économique Européen) dans le respect des modalités fixées par le règlement financier de l'ANR.
Les dépenses relatives au recrutement de personnel sous contrat à durée déterminée (CDD) sont éligibles.

5. Modalités relatives aux pôles de compétitivité

Les partenaires du projet pourront mentionner si le projet fait partie des projets labellisés, ou en cours de labellisation, par un pôle de compétitivité (ou plusieurs, en cas de projet interpôles).

Les partenaires d'un projet labellisé par un (des) pôle(s) de compétitivité et retenu par l'ANR dans le cadre de cet appel à projets pourront se voir attribuer un complément de financement par l'ANR.

Le partenaire coordinateur ou le(s) partenaire(s) concerné(s) devront transmettre à l'ANR, pour chaque pôle de compétitivité concerné, un formulaire d'attestation de labellisation dûment rempli et signé par un représentant de la structure de gouvernance du pôle, dans un délai maximum de deux mois après la date limite d'envoi (mercredi 18 avril 2007) des projets sous forme électronique. La procédure à suivre est décrite en annexe (§ 2).

6. Modalités de soumission

Le dossier de soumission pour l'appel à projets devra comporter l'ensemble des éléments nécessaires à l'évaluation scientifique et technique du projet.

Les éléments du dossier de soumission, seront mis en ligne sur le site Internet de l'ANR et le site Internet de l'Appel à Projets (www-csosg.utt.fr), au plus tard le mardi 30 janvier 2007.

La description scientifique et technique devra être rédigée de préférence en anglais sauf pour les projets pour lesquels l'usage du français s'impose. Au cas où :

- la description scientifique et technique est rédigée en anglais, une traduction en français de la description courte du projet devra être fournie (§ 2, Annexe B du dossier de candidature).

- la description scientifique et technique est rédigée en français, le coordinateur du projet concerné devra fournir une traduction en anglais à l'UTT, dans un délai de dix jours, si le comité d'évaluation désigne un ou des experts externes étrangers non francophones pour les expertises.

Les dossiers soumis sous forme électronique et sous forme papier devront comporter les mêmes éléments.

Le **dossier de soumission** devra impérativement être transmis par le partenaire coordinateur :
sous forme électronique au plus tard le **mercredi 18 avril 2007 à 12h** sur le site dédié suivant :

www-csosg.utt.fr

(L'inscription préalable sur le site de soumission par le coordinateur du projet est obligatoire pour pouvoir soumettre une proposition, une semaine avant la date limite de dépôt des dossiers)

et

sous forme papier, en un exemplaire original signé, **par voie postale**, en recommandé avec accusé de réception**, au plus tard le mercredi 18 avril 2007 à 24h**, **le cachet de la poste faisant foi, à l'adresse suivante :**

Université de Technologie de Troyes
Appels à Projets ANR -CSOSG
12, rue Marie Curie, BP 2060
10010 Troyes Cedex.

Un accusé de réception sous forme électronique sera envoyé au coordinateur par l'unité support.

La **lettre d'engagement** (cf. dossier de candidature) devra être postée (pli recommandé avec accusé de réception) **au plus tard le lundi 25 Juin 2007** à **24h** (le cachet de la poste faisant foi), à la même adresse.

Pour tout renseignement, les personnes à contacter, de préférence par courrier électronique, sont :

pour toute information de nature technique ou scientifique concernant l'appel à projets :

En priorité, Patrick Lallement – pl.csosg@utt.fr – Tél : 03 25 71 56 80

Eric Châtelet – ec.csosg@utt.fr -Tél : 03 25 71 56 34

Philippe Cornu – phc.csosg@utt.fr - Tél : 03 25 71 56 89

pour toute information de nature administrative et financière :

Miguel Inacio – mi.csosg@utt.fr -Tél : 03 25 71 85 59

Annexes

1. Procédure de sélection

Les principales étapes de la procédure de sélection sont les suivantes :

- **évaluation des projets** par le comité d'évaluation après réception des avis des experts extérieurs ;
- **examen des projets** par le comité de pilotage et **proposition d'une liste des projets à financer** par l'ANR (liste principale et éventuellement liste complémentaire) ;
- établissement de la **liste des projets sélectionnés** par l'ANR (liste principale et éventuellement liste complémentaire) et publication de la liste ;
- envoi aux coordinateurs des projets non sélectionnés d'un avis synthétisé des comités ;
- finalisation des dossiers administratif et financier pour les projets retenus et publication de **la liste des projets retenus** pour financement.

Les rôles respectifs des principaux acteurs de la procédure de sélection sont :

- le **comité d'évaluation,** composé de membres des communautés de recherche concernées, français ou étrangers, issus de la sphère publique ou privée, a pour mission d'évaluer les projets et de les répartir dans trois catégories : A (recommandés), B (acceptables), et C (rejetés) ;
- les **experts extérieurs,** désignés par le comité d'évaluation, donnent un avis écrit sur les projets. Au moins deux experts sont désignés pour chaque projet ;
- le **comité de pilotage,** composé de personnalités qualifiées et de représentants institutionnels ont pour mission de proposer, à partir des travaux du comité d'évaluation, une liste de projets à financer par l'ANR.

Les dispositions de la charte de déontologie doivent être respectées par les personnes intervenant dans la sélection des projets, notamment les dispositions liées à la confidentialité et aux conflits d'intérêt. La charte de déontologie de l'ANR est disponible sur son site internet.

Les modalités de fonctionnement et d'organisation des comités d'évaluation et de pilotage sont décrites dans des documents disponibles sur le site internet de l'ANR.

La composition des comités du programme est affichée sur le site internet de l'ANR :

(www.agence-nationale-recherche.fr)

2. Modalités relatives aux pôles de compétitivité

Le formulaire d'attestation de labellisation d'un projet par un pôle de compétitivité se trouve avec l'ensemble des documents téléchargeables constituant le dossier de soumission.

Le partenaire coordinateur ou le(s) partenaire(s) concerné(s) devront :

- transmettre le formulaire renseigné sous forme électronique à la structure de gouvernance de chaque pôle de compétitivité concerné (un projet interpôles peut faire l'objet d'une labellisation par chacun des pôles concernés) ;
- réceptionner une version papier dûment signée de l'attestation de labellisation, en cas d'accord du pôle pour la labellisation, pour chaque pôle concerné ;

- transmettre :
    - o à l'ANR la(les) attestation(s) de labellisation dûment signée(s) par courrier ou par fax (coordonnées indiquées sur le formulaire) ;
    - o à l'unité support (le cas échéant) une copie de la(les) attestation(s) de labellisation dûment signée(s) par courrier ou par fax (coordonnées indiquées sur le formulaire).

Les attestations dûment signées devront être transmises à l'ANR dans un délai maximum de deux mois après la date limite d'envoi des projets sous forme électronique.

3. Définitions

3.1. Définitions relatives aux différents types de recherche

1) **Recherche fondamentale** : Par ce terme, la Commission Européenne entend « une activité visant un élargissement des connaissances scientifiques et techniques non liées a priori à des objectifs précis industriels ou commerciaux » (JOCE 28/02/2004 L 63/23).

2) **Recherche industrielle :** Par ce terme, la Commission Européenne entend « la recherche planifiée ou des enquêtes critiques visant à acquérir de nouvelles connaissances, l'objectif étant que ces connaissances puissent être utiles pour mettre au point de nouveaux produits, procédés ou services ou entraîner une amélioration notable des produits, procédés ou services existants » (JOCE 28/02/2004 L 63/23)**.**

3) **Développement pré-concurrentiel :** Par ce terme, la Commission Européenne entend « la concrétisation des résultats de la recherche industrielle dans un plan, un schéma, ou un dessin pour des produits, procédés ou services nouveaux, modifiés ou améliorés, qu'ils soient destinés à être vendus ou utilisés, y compris la création d'un premier prototype qui ne pourra pas être utilisé commercialement. Elle peut en outre comprendre la formulation conceptuelle et le dessin d'autres produits, procédés ou services ainsi que des projets pilotes, à condition que ces projets ne puissent pas être convertis ou utilisés pour des applications industrielles ou une exploitation commerciale. Elle ne comprend pas les modifications de routine, procédés de fabrication, services existants et autres opérations en cours, même si ces modifications peuvent représenter des améliorations » (JOCE 28/02/2004 L 63/23).

3.2. Définitions relatives à l'organisation des projets

Pour chaque projet, un **partenaire coordinateur** unique est désigné et chacun des autres **partenaires** désigne un **responsable scientifique et technique.**

Partenaire coordinateur : Organisme de recherche ou entreprise d'appartenance du coordinateur.

Coordinateur : Il est le responsable de la coordination scientifique et technique du projet, de la mise en place et de la formalisation de la collaboration entre les partenaires, de la production des livrables du projet, de la tenue des réunions d'avancement et de la communication des résultats. L'organisme auquel appartient le coordinateur est appelé partenaire coordinateur.

Partenaire : unité d'un organisme de recherche ou entreprise.

Responsable scientifique et technique : Il est l'interlocuteur privilégié du coordinateur et est responsable de la production des livrables du partenaire. Pour l'organisme assurant la coordination générale du projet, le responsable scientifique et technique du projet est en général le coordinateur du projet dans son ensemble. Toutefois, notamment dans le cadre de projets de grande taille, la coordination du projet peut être assurée par une tierce personne de la même entreprise ou du même laboratoire.

Projet partenarial organisme de recherche / entreprise : projet de recherche pour lequel au moins un des partenaires est une entreprise, et au moins un des partenaires appartient à un organisme de recherche (cf. définitions au § 3.3 de la présente annexe).

3.3. Définitions relatives aux structures

Organisme de recherche : Est considéré comme organisme de recherche, une entité, telle qu'une ***université ou institut de recherche***, quel que soit son statut légal (organisme de droit public ou privé) ou son mode de financement, dont le but premier est d'exercer les activités de recherche fondamentale ou de recherche industrielle ou de développement expérimental et de diffuser leur résultats par l'enseignement, la publication ou le transfert de technologie ; les profits sont intégralement réinvestis dans ces activités, dans la diffusion de leurs résultats ou dans l'enseignement ; les entreprises qui peuvent exercer une influence sur une telle entité, par exemple en leur qualité d'actionnaire ou de membre, ne bénéficient d'aucun accès privilégié à ses capacités de recherche ou aux résultats qu'elle produit.(Document adopté le 22/11/06 par la Commission Européenne[13])

Entreprise : Est considérée comme entreprise, toute entité, indépendamment de sa forme juridique, exerçant une activité économique. Sont notamment considérées comme telles, les entités exerçant une activité artisanale, ou d'autres activités à titre individuel ou familial, les sociétés de personnes ou les associations qui exercent régulièrement une activité économique (Recommandation 2003/361/CE de la Commission Européenne du 6 mai 2003 concernant la définition des petites et moyennes entreprises [14]).

Petite et Moyenne Entreprise (PME) : La définition d'une PME est celle de la Commission Européenne, figurant dans la Recommandation 2003/361/CE de la Commission Européenne du 6 mai 2003[15]). Notamment, est une PME une entreprise autonome comprenant jusqu'à 249 salariés, avec un chiffre d'affaires inférieur à 50 M€ ou un total de bilan inférieur à 43 M€.

Opérateur : organisation publique ou privée, produisant des biens ou des services et qui, à ce titre doit assurer la sécurité de ses usagers, clients, personnels, des citoyens et de l'environnement.

Prescripteur : autorité édictant des règles, normes, orientations relatives à la sécurité.

[13] *Encadrement communautaire des aides d'État à la recherche, au développement et à l'innovation* - http://ec.europa.eu/comm/competition/state_aid/reform/rdi_fr.pdf

[14] JO L du 20.5.2003, p. L 124/39

[15] *id.*

4. Modalités relatives au suivi des projets

Le suivi des projets est assuré selon les modalités suivantes :

4.1. Suivi des projets

Chaque projet fait l'objet d'un suivi effectué par l'UTT en tant qu'unité support pour le compte de l'ANR suivant les modalités définies dans les actes attributifs.

Les moyens mis en oeuvre pour ce suivi sont en particulier :

- des comptes rendus intermédiaires semestriels d'avancement, un rapport à mi-parcours et un rapport final permettant notamment de mesurer l'impact du projet ;
- des visites sur site réalisées par l'unité support ;
- la participation des proposants à des colloques de suivi organisés par l'unité support.

Pour certains projets, la Délégation Générale pour l'Armement (DGA) sera associée au suivi.

4.2. Diffusion des résultats obtenus

D'une manière générale, mais sous réserve des clauses de confidentialité, les projets doivent favoriser une large diffusion des résultats obtenus au sein de la communauté de recherche suivant les modalités définies dans les actes attributifs.

Cette communication peut s'appuyer notamment sur :

- la création éventuelle d'un site web pour le projet ;
- des communications dans des séminaires, colloques et/ou forums, qui pourront être organisés, co-organisés ou soutenus par l'ANR ou l'unité support.

En outre, l'aide apportée par l'ANR au projet devra être mentionnée sur les publications avec la référence du numéro ANR du projet.

5. Résumés des projets sélectionnés lors de CSOSG 2006

ASPIC : Aide par la Simulation à la Protection des Infrastructures Critiques

L'objectif du projet ASPIC - Aide par la Simulation à la Protection des Infrastructures Critiques - est de développer le démonstrateur d'un outil d'aide au positionnement et au déploiement de capteurs pour optimiser la surveillance et la protection des infrastructures critiques (ex : aéroports, gares de métro…).
L'objectif est de modéliser un site et son environnement en 3D, de positionner les capteurs dans cet environnement virtuel et de visualiser de manière interactive leur enveloppe de couverture. La simulation de menaces, d'incidents ou du comportement de la foule en situation de crise permettra de vérifier l'efficacité du système à déployer.
Le responsable sécurité d'un site pourra ainsi concevoir et optimiser virtuellement la protection du site contre diverses menaces et définir le système de sécurité le plus performant en termes de protection et de coût.
Cet outil permettra également d'effectuer des audits de sécurité sur des sites existants, de simuler des menaces nouvelles, de mettre en évidence les vulnérabilités résiduelles et de proposer des améliorations afin de renforcer la protection du site.

Le projet utilisera des briques technologiques préexistantes ou fera appel à des développements spécifiques pour modéliser la topologie du terrain, des bâtiments ou des infrastructures, la couverture, la portée et la sensibilité des capteurs. Des modules de simulation de propagation de la menace (nuage de nature biologique ou chimique) ainsi que du comportement humain sont inclus au système pour affiner la mise en place des capteurs et des moyens de protection.

CANADA : Comportements Anormaux : Analyse, Détection, Alerte

Le projet CAnADA est destiné à fournir un ensemble d'outils et d'approches permettant la détection et la gestion « temps réel » des comportements pouvant compromettre la sécurité des personnes et des biens en s'appuyant sur des données vidéo. Il s'agit de classifier les comportements d'individus afin de les interpréter en termes de menace. L'objectif est de communiquer l'information pertinente aux acteurs pouvant faire revenir la situation à un niveau aussi normal que possible, grâce aux canaux de communication les plus adaptés. Les verrous à lever sont de nature scientifique et technologique (gestion des flux multiples, des occultations, extraction des motifs de comportements sur des fenêtres temporelles variables) mais aussi juridiques (liés à « l'acceptabilité » d'un tel système). Afin de gérer l'ensemble de ces difficultés, le projet utilise les contextes applicatifs envisagés pour établir un maximum d'hypothèses réalistes (conditions d'éclairage, environnement connu a priori) permettant de simplifier la recherche. Ce projet s'organise autour d'un consortium représentant les compétences indispensables à l'accomplissement des objectifs fixés. (laboratoires de recherche, industriels et partenaires en prise directe avec les problèmes de sécurité.

DEMOLOC : Démonstrateur de localisation de victimes

Le projet vise à démontrer la faisabilité d'un appareil portable destiné à équiper des forces de sécurité telles que pompiers et des utilisateurs de matériel de secours et de sécurité en montagne. Cet objet a pour objectif de fournir des informations critiques lors d'un incident portant atteinte à la sécurité de l'un des membres de l'équipe. L'objectif est de permettre au groupe de localiser la ou les victimes éventuelles et d'acquérir en parallèle des informations préalables sur son état de santé (motricité, respiration,…). Pour la localisation, le système s'appuie sur la technique radio appelée Ultra Large Bande (ULB) dont le principe est basé sur l'émission d'impulsions très brèves offrant une résolution spatiale suffisamment forte pour être exploitable pour la localisation par triangulation. Sont ciblés des contextes d'utilisation pour lesquels les solutions classiques GPS ou radio GSM ne sont pas utilisables. Ces contextes sont typiquement des bâtiments ou des coulées d'avalanche. Le système sera en outre doté d'un équipement de mesure des mouvements dont les signaux peuvent fournir des indications précieuses sur l'état de la victime. Le projet commencera donc par la définition de quelques scénarios d'usage qui déboucheront sur une spécification technique du démonstrateur. Les travaux consisteront à réaliser une plate-forme radio Ultra Large Bande et un module de capture du mouvement (chute, position,...) qui seront couplés à des systèmes Tetrapol au moyen de techniques de packaging 3D avancés. Le projet débouchera sur des démonstrations et tests en situation réelle via l'aide de forces d'intervention en haute montagne et des forces d'intervention incendie dans le sud de la France.

EGSISTES : Evaluation Globale de la Sécurité Intrinsèque aux Systèmes de Transports En Souterrains

Le projet porte sur le développement de méthodes et de modèles physiques permettant d'analyser et d'évaluer le niveau de sécurité globale d'un système de transport souterrain. Cette approche globale de la sécurité intègre à la fois le risque accidentel et les actes de malveillance. La première partie du projet porte ainsi sur l'élaboration et/ou l'adaptation de méthodes globales d'analyse de risques permettant d'identifier les dangers relatifs aux systèmes de transports souterrains. La seconde partie porte sur l'approfondissement des connaissances phénoménologiques des incidents en réseau souterrain afin d'améliorer l'évaluation de leurs conséquences sur les usagers et l'environnement. Cette partie se concentrera notamment sur les problématiques de dispersion de gaz légers (fumées d'incendie par exemple), de gaz denses, de gaz dynamiquement inertes, et de particules. La problématique de la génération et de la propagation des ondes de pression liées à une explosion sera également traitée dans ce projet. Le troisième objectif porte sur le développement de modèles physiques, en s'appuyant notamment sur les connaissances apportées par la seconde partie du projet, et sur les méthodes d'implémentation de ces modèles dans des modèles numériques. Pour chaque type de risque modélisé (rejet massif, rejet Nucléaire Radiologique Biologique Chimique et explosion), l'enjeu sera de proposer des modèles physiques et des méthodes d'implémentation

numériques permettant une évaluation des conséquences de l'incident sur des échelles de la taille de tout ou partie du réseau souterrain et également sur des échelles plus locales.

INTERSECTS : Intelligence territoriale des menaces contre la sécurité et l'ordre dans les quartiers sensibles en France et aux Etats-Unis - Analyse sociologique des dispositifs publics d'intelligence territoriale et de prévention des risques en France et aux Etats-Unis»

La recherche porte sur la façon dont les autorités responsables de la sécurité et de l'ordre public se munissent d'informations et de connaissances relatives aux différents types de menaces, principalement dans les zones urbaines ou périurbaines dites «sensibles», où vivent et agissent certaines catégories d'individus identifiés comme présentant un risque, notamment les populations spécifiques des casseurs et récidivistes légaux. On étudie comment les différentes organisations publiques susceptibles de contribuer au recueil, au traitement et à l'exploitation de renseignements touchant à la sécurité du territoire considéré parviennent, ou non, à coopérer entre elles pour améliorer la surveillance et la prévention des risques. On s'intéresse principalement aux aspects humains et organisationnels de cette activité d'intelligence territoriale, mais on examine également les usages qui sont faits des dispositifs techniques et juridiques. L'analyse empirique des systèmes territoriaux d'acteurs de trois sites de chacun de ces pays est guidée par trois ensembles de questions: 1- la gestion interne de l'information par chaque acteur, 2- la gestion des échanges d'informations entre les différents acteurs, 3- les effets sociaux de la surveillance. Le projet est conçu dans une perspective d'aide à l'action des institutions en charge de missions de sécurité (préfectures, police, gendarmerie, justice, maires…): il aura des retombées dans le domaine de la formation professionnelle et sur le plan du pilotage stratégique et opérationnel des activités d'intelligence territoriale.

ISYCRI : Interopérabilité des Systèmes en situation de Crise

Dans une situation de crise (catastrophe naturelle, conflit, etc.), plusieurs intervenants (sécurité civile, forces armées, ONG, etc.) sont appelés à agir simultanément et dans l'urgence. L'interopérabilité s'avère une composante majeure de l'objectif de réduction de la criticité de la situation. Cette problématique relève d'une approche globale de la sécurité et traite du besoin d'améliorer l'efficacité des réseaux d'acteurs mis en jeu en contexte critique. Ces travaux se baseront sur des approches complémentaires portant sur le traitement des risques, l'interopérabilité, la complexité et la systémique. Une caractéristique du projet ISyCri est de se pencher simultanément sur deux plans : (i) la coordination des réactions, éventuellement prédéfinies, des divers partenaires (réactivité), (ii) l'adaptabilité de cette réaction collective à l'avancement dans la situation de crise (flexibilité). Le projet est organisé en trois lots techniques : L1 dédié à l'étude des collaborations en situation de crise, L2 chargé de la conception de l'architecture inter organisationnelle et L3 dédié aux travaux sur les modes de pilotage, un lot de démonstration (L4) qui expérimente et évalue les propositions et enfin un lot de gestion du projet (L0). Les résultats relèveront d'une part de l'examen du domaine des crises en vue d'établir un référentiel de connaissance et d'autre part de l'étude des solutions conceptuelles et technologiques à l'interopérabilité en contexte critique.

LISE : Linguistique, normes, traitement automatique des langues et Sécurité : du "data et sense-mining" aux langues contrôlées

Le chaînon faible de nombreux systèmes est la communication humaine. Prévoir quand et comment la menace arrivera ainsi que les messages, instructions, protocoles d'urgence nécessaires à transmettre et à traduire est impossible ; il faut donc savoir analyser l'information, prévoir la façon de l'écrire afin qu'elle soit comprise par tout un chacun et traduisible par une machine sans risque d'erreurs. Le projet consiste à partir de la théorie micro-systémique à élaborer une méthodologie fondée sur des analyses linguistiques approfondies afin de dégager des normes linguistiques pour des applications de sécurité. Deux technologies novatrices et complémentaires, «data et sense-mining» et «langue contrôlée généralisante», seront développées pour des applications en matière de traitement de l'information (reconnaissance de messages et de leur sens, syntaxiquement ou sémantiquement anormaux ou normaux) et de diffusion (alertes, protocoles médicaux et messages d'urgence). Les normes définies permettront d'analyser, de rédiger, de vérifier des messages,

protocoles, alertes et également d'obtenir des traductions fiables et compréhensibles. Toutes les couches de la linguistique seront utilisées, signaux « forts » ou « faibles.

MANIF : Moyen Aérien Nouveau pour l'Identification dans les Foules

Le projet MANIF a pour objectif de traiter de l'utilisation coordonnée des moyens aériens, y compris les moyens type drone, dans les contextes de rassemblement en zone urbaine. La dimension sera celle du système global et de son emploi, notamment pour explorer les modalités de traitement de l'information des capteurs, de coordination des porteurs par une approche en simulation, doublée de démonstration sur les points critiques ou innovants. MANIF traite donc des thématiques de surveillance, de protection et d'opérations. Une meilleure compréhension du besoin (acceptabilité, opérations, droit), une meilleure adaptation des moyens (aériens, capteurs, télécommunications) au besoin, une évaluation appropriée des exigences en traitement de l'information et en exploitation de ces systèmes dans les postes de commandements opérationnels et des risques associés à l'utilisation des moyens aériens nouveaux lors des opérations en résultera. Ceci conduira à une meilleure maîtrise de ces situations, donc à une réduction de l'impact sociétal et économique considérable de ces évènements. Enfin, la mise en place d'une analyse systématique du besoin et des solutions ainsi que leur planification sera de nature à faciliter l'émergence d'une filière industrielle propre à satisfaire les besoins en sécurité.

PROTER : Procédures terrain rapides NRBC

Le projet PROTER (Procédure terrain rapide) permet de construire des procédures de terrain rapides bâties sur des innovations technologiques en matière de traitement et de traçabilité des victimes, des intervenants et de leurs actions.

Il comporte cinq volets correspondant à des préoccupations opérationnelles d'intervention pour les secours sur un évènement Nucléaire Radiologique Biologique Chimique (NRBC) ou catastrophe industrielle :
- Délimitation des zones opérationnelles d'exclusion ou d'intervention,
- Gestion terrain coopérative des intervenants de toutes les unités et des victimes,
- Déploiement rapide d'un système de traitement des victimes,
- Procédure de tri des victimes et de décontamination (détection, tri, déshabillage) automatisée,
- Suivi des victimes en post événement.

En préliminaire aux études et réalisations, une analyse fonctionnelle est conduite avec des utilisateurs (SDIS) afin de déterminer les spécifications des sous-ensembles nécessaires aux évaluations terrain.
Le projet conduit à un démonstrateur avec des objectifs de réduction des délais d'intervention, d'augmentation du débit de traitement, d'une gestion en temps réel des équipes et des victimes ainsi que de leur suivi post évènementiel (cadre d'un exercice du type PIRATOX).

REALEX : Evaluation des risques et de la menace, analyse de situation et expertise en temps réel pour la gestion des crises NRBC

Depuis dix ans, les actes de vandalisme, de malveillance voire de terrorisme contre des installations industrielles (sites chimiques, systèmes de transport de matières dangereuses) se sont multipliés.
Du à leur potentiel susceptible d'engendrer des phénomènes dangereux en cas de destruction, elles représentent des cibles d'importance pour des actes délibérés.
La connaissance de la vulnérabilité au voisinage et dans ces installations permet de mettre en évidence les enjeux sur lesquels un événement majeur pourrait avoir des conséquences. Pour des terroristes, ces sites représentent également des sources potentielles d'approvisionnement en substances dangereuses pour leur dissémination dans des lieux publics (métro...) ou comme des précurseurs d'explosifs ou d'engins chimiques improvisés.
Au regard de l'émergence de ces nouvelles menaces, le projet REALEX poursuit deux objectifs :
D'une part compléter l'évaluation des risques menée en sécurité industrielle, par une évaluation de la vulnérabilité de ces installations aux actes délibérés et en assurer la prévention à l'échelle de sites industriels,

D'autre part, extrapoler cette évaluation au-delà des aspects de prévention afin de mieux caractériser la situation pour le dimensionnement de la réponse face à l'imminence d'un événement ou juste après son occurrence. A ce titre, l'organisation et le recours en temps réel à un appui technique et scientifique (expertise pluridisciplinaire) contribueront à l'aide à la décision des gestionnaires de crise à caractère NRBCE (Nucléaire, Radiologique, Biologique, chimique et Explosifs).

Le projet qui regroupe des centres d'études et de recherches, un industriel, ainsi que des organismes directement concernés par ces préoccupations, associera également les pouvoirs publics au sein d'un comité de pilotage.

SAFIMAGE : Plate-forme de traitement en temps Réel des flux IP à haut débit

Le projet de recherche porte sur la conception d'une plate-forme générique matérielle et logicielle d'inspection de paquets IP en temps réel (niveaux 2 à 7) sur des liaisons à haut débit (jusqu'à 10 Gb/s par liaison).
Cette plate-forme intéresse toute application s'appuyant sur l'analyse du contenu des informations circulant sur les liens IP. Elle permet la détection d'intrusion ou d'attaque de réseaux, le marquage et/ou traçabilité de contenus, la détection d'utilisation frauduleuse du réseau via des applications P2P, l'analyse automatique des contenus de sites internet/blogs/Chats/fichiers texte, etc.
Pour réduire drastiquement les coûts produits par rapport aux solutions existantes et atteindre les performances indispensables aux traitements envisagés, cette plate-forme utilise la nouvelle génération de processeurs de service réseau (nombreuses fonctions ardware, multi-cores MIPS, environnement de développement standard, etc.)

SIMAVI : SIMulation d'Aéronefs Virtuels pour les missions de sécurité

Le projet SIMAVI (SIMulation d'Aéronefs Virtuels) a pour but d'élaborer une démarche rationnelle de choix de concepts de surveillance permanente sur zone, fondée sur la simulation de concepts concurrents. Il est organisé en quatre phases complémentaires :

- Analyse du besoin,
- Élaboration des concepts,
- Évaluation des concepts en simulation,
- Synthèse et recommandations.

Un recensement des plates-formes et des capteurs disponibles actuellement et à moyen terme et de leurs performances permettra d'élaborer des concepts répondant aux spécifications techniques de besoin. Deux classes de concepts seront proposées, basés sur l'utilisation de dirigeables et de drones.
La comparaison, en simulation, des différentes plates-formes sera réalisée sur quatre scénarios. Le premier traitera de la surveillance côtière. Les trois derniers seront joués sur un terrain numérique urbain et mettront en œuvre des données réelles recueillies au-dessus de Paris.
La synthèse du projet permettra de conclure sur l'intérêt de la simulation pour évaluer des concepts de surveillance en réalité virtuelle. Elle permettra d'identifier les apports relatifs des différentes plates-formes et d'identifier les technologies manquantes ou à intégrer pour disposer d'un ensemble de moyens adaptés à un traitement performant et économiquement acceptable des missions de sécurité retenues.

SRIP : Emploi des moyens robotisés pour prévenir et traiter les incidents

Le projet SRIP vise à étudier les futurs systèmes robotisés dédiés à des missions en coopération avec les hommes dans des environnements présentant des menaces potentielles intentionnelles ou accidentelles. Plus précisément, il s'agira de définir les concepts d'emploi de systèmes robotisés d'intervention en zone dangereuse pour des missions de collecte d'information pour la prévention des risques ou de traitements post-accidentels (industriels, transport des matières dangereuses…). Ces concepts sont destinés aux agents d'intervention et en premier lieu les pompiers.
La démarche permettra, à partir d'une analyse opérationnelle préliminaire d'aboutir à des définitions de systèmes aptes à répondre à un certain nombre de besoins et diminuant de façon sensible le

niveau de dangerosité de la mission pour les hommes, et enfin à la réalisation d'un démonstrateur permettant la validation des concepts.

TARANIS : Technologies pour l'Apprentissage des Risques majeurs par Animation et Simulation

Le projet TARANIS (Technologies pour l'Apprentissage des Risques majeurs par ANImation et Simulation) propose la réalisation d'un système d'entraînement de cellules de crises fondé sur des outils de simulation novateurs permettant aux formateurs de restituer les situations les plus réalistes possibles. La simulation apportera une maîtrise des entraînements en rendant tangible la situation de crise virtuelle qui peut ainsi effectivement réagir aux décisions des entraînés.
Un tel système devra combler le vide pédagogique entre les entraînements grandeur réelle sur le terrain et l'analyse à froid des plans d'urgence. Le système permettra la pratique répétée des situations de crises, y compris des situations extrêmes que les très coûteux exercices grandeurs nature ne peuvent réaliser.
Le projet TARANIS est mené par un consortium composé d'acteurs de la recherche qui ont l'expérience de la réalisation de tels outils de simulation dans le secteur militaire, familier de leur utilisation pour l'entraînement des forces. Par la création d'un système ouvert et extensible, le projet vise à rapprocher d'autres industriels, chercheurs et utilisateurs finaux intéressés par ce type de technologies. Un site pilote de déploiement et d'évaluation du système est déjà prévu en collaboration rapprochée avec à la Communauté d'Agglomération du Havre.