# TAMARIS : Traitement et Authentification des MenAces et RISques en mer

Michel Morel, Anne Littaye, Claire Saurel, Olivier Poirel, Aldo Napoli, Stephane Vales, Gwenaele Proutiere-Maulion

# TAMARIS

# Traitement et Authentification des MenAces et RISques en mer

Michel MOREL[1], Anne LITTAYE[2], Claire SAUREL & Olivier POIREL[3], Aldo NAPOLI[4], Séphane VALES[5], Gwenaele PROUTIERE MAULION[6]

[1] DCNS, SIS/DDP
BP 403 - 83055 TOULON CEDEX, FRANCE.
TEL : 04 98 03 92 59 - www.dcns.fr
[2]ECOMER, Bureau d'étude en ECOlogie Marine, Etude & Recherche,
3 lot Cuchintcherry – 64210 Bidart, France.
Tel : 06 70 39 44 76 - ecomers@orange.fr
[3]ONERA, Office Nationale d'Etudes et de Recherches Aérospatiale
2 avenue Edouard Belin, BP 74025, 31055 Toulouse
Tel : 05 62 25 26 33 www.onera.fr
[4] Mines Paris, Ecole des Mines Paris – Centre de Recherche sur la gestion des Crises,
Rue Claude Daunesse – 06904 Sophia Antipolis, France.
Tel : 04 93 95 74 86 - www.crc.ensmp.fr
[5] INTUILAB, les Triades A, rue Galilée, BP 77242, 31672 Labége
Tel : 05 62 24 51 65 - www.intuilab.com
[6] Centre de Droit Maritime et Océanique de l'Université de Nantes,CDMO, chemein de la Censive du Terte, BP 81307, 44313 Nantes
Tel : 06 08 45 99 47 gproutieremaulion@hotmail.com

**Résumé** – L'objectif du projet de démonstrateur proposé TAMARIS, est d'intégrer un processus et des outils innovants de traitement de l'information pour l'analyse d'une situation qui est une série d'alertes correspondant à un comportement suspect de navire. Ce comportement suspect peut se dérouler dans le temps (sur plusieurs jours, voir mois) et sur un espace maritime étendu (plusieurs centaines de miles nautiques). L'analyse est traduite par l'élaboration en temps réel d'un dossier d'enquête électronique. Ce dossier standardisé, permet de rassembler l'ensemble des informations (des connections à des bases de données et à Internet permettent ce renseignement) et l'analyse sur un seul support réactualisé au fil du déroulement de la situation. Ce dossier peut être transmis aux autorités décisionnelles afin de suivre en permanence les évolutions et d'être informées de l'authentification progressive du comportement suspect durant son déroulement. Ce dossier est constitué et visualisé sur une table tactile, ce qui permet à une équipe d'experts de différentes organisations de travailler ensemble et en direct de façon interactive. Ce dossier constitue une archive quasi complète et chronologique qui peut être transmise également à des enquêteurs pour mener des investigations ultérieures.

**Abstract** – TAMARIS goals is to study and develop a demonstrator to support operational user to identify the threat associated to suspect event detected from abnormal vessel behaviours. Behaviour is understood in vessel movement and in performed activities taking into account the contextual conditions (meteorological, geographical, environmental and regulation).

## 1. Introduction

Les systèmes actuels de surveillance des approches maritimes, comme par exemple, SPATIONAV (en France) ou SIVE (en Espagne) permettent de réaliser des tenues de situation du trafic maritime dans les zones d'approche nationale, c'est à dire de visualiser, sur les écrans de surveillance des opérateurs, les déplacements des navires (pistes) dans la zone surveillée. Un historique de 72 heures est conservé en cas de besoin d'analyse à posteriori d'une situation.

La réactualisation de ces systèmes intègre progressivement des algorithmes d'analyse de ces déplacements de navires pour détecter des événements anormaux comme une route de collision, un changement important de cap, une vitesse excessive, un arrêt, etc. Les algorithmes futurs seront basés sur des moteurs de règles (ou d'inférences). Ces versions utiliseront de plus des nouvelles données de positions des navires comme l'AIS, le futur LRIT (Long Range Identification and Tracking system), etc. Ces nouvelles données permettront de réaliser des tenues de situation du

trafic plus complètes et précises sur tous les types de navires.

En complément de ces nouvelles fonctionnalités prévues dans les versions améliorées ci-dessus, actuellement à l'étude ou en démonstration, notamment à la DARPA (Defense Advanced Research Projects Agency ; USA – projet PANDA), le projet TAMARIS (Traitement et Authentification des MenAces et des RISques en mer) propose d'étudier, développer et tester un démonstrateur qui permette d'aider les experts à authentifier la nature de la menace qui est associée aux événements anormaux détectés. Par exemple, la détection d'un abordage génère une alerte qui est transmise à TAMARIS pour authentifier la nature de la menace correspondante.

Le projet TAMARIS utilise une méthodologie innovante, des informations externes et des outils d'assistance aux experts pour confirmer ou infirmer les hypothèses d'interprétation progressive d'une suite d'alertes corrélées qui correspondent à un comportement suspect d'un ou plusieurs navires. Cette analyse fait l'objet de dossiers d'enquête standardisés qui à chaque actualisation, sont transmis en temps quasi réel à une autorité décisionnelle pour l'informer des évolutions de la situation ou en temps différé, sous sa forme finale, à des enquêteurs. Selon la nature de la menace et son imminence, cette autorité peut alors décider d'une intervention maritime coordonnée pour en arrêter le déroulement et limiter les conséquences. La constitution en temps réel de ces dossiers standardisés, l'intégration de données externes et de résultats d'analyse à travers un seul outil constitue une aide à la décision dans un cadre opérationnel. Dans le cas d'une enquête à posteriori, actuellement, un enquêteur doit, dans un premier temps rassembler toutes les pièces et rechercher les informations nécessaires pour faire son analyse. Or le nombre d'enquête est de plus en plus important ; TAMARIS constitue une aide à la compilation de l'ensemble des faits qui pourront être analysés par les enquêteurs.

## 2. Positionnement du Projet dans un Système de Surveillance Maritime

Le schéma ci-après positionne le projet **TAMARIS** dans une solution globale pour la sécurité et la sûreté en mer.

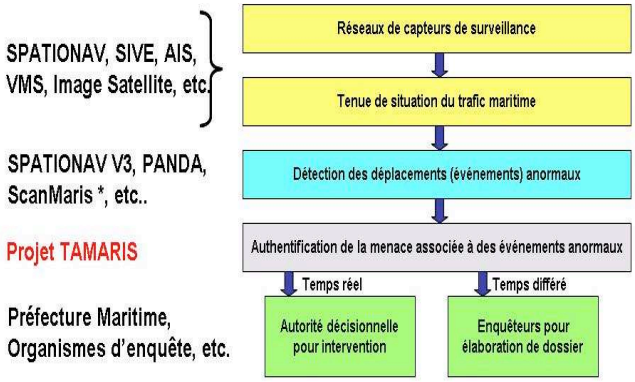


Figure 1 : Positionnement de TAMARIS dans une solution globale

*ScanMaris (Surveillance et Contrôle des Activités des Navires en Mer) est un projet retenu par l'ANR en 2007 dans le programme sur la sécurité globale qui développe un atelier pour évaluer des algorithmes de détection automatique d'événement anormal en utilisant les techniques des AMAS (Adaptatif Multi-Agents System). Ces techniques sont également utilisées dans le projet PANDA de la DARPA.*

## 3. Contexte

Les navires qui empruntent les routes martimes (comme l'approvisionnement en énergies et le transport de passagers) sont vulnérables à de nombreuses menaces, en particulier à des actes terroristes qui visent à causer d'importantes pertes humaines (ferries et navires de croisière), des pertes économiques (destructions des navires et infrastructures côtières), une insécurité des transports (routes maritimes et flux de marchandises) et des catastrophes environnementales majeures (pollutions maritimes et atmosphériques).

Concernant les attaques terroristes, la communauté internationale des experts a analysé de nombreuses stratégies visant des cibles maritimes (voire CRS Report of Congress – Maritime Security : Potential Terrorist Attacks and Protection Priorities, January 9, 2007). Les terroristes peuvent mener des attaques avec des embarcations suicides «bourrés» d'explosifs, des tankers, des navires de croisière et des ferries contre d'autres navires marchands, des bâtiments de guerre ou des infrastructures côtières. Ils peuvent également utiliser des navires commerciaux comme plateforme pour des attaques armées, mais aussi s'emparer de navires transportant des hydrocarbures ou du gaz naturel liquéfié pour les utiliser comme «bombe» pour des attaques ayant des conséquences humaines (nombreuses victimes), économiques (restriction des approvisionnements, hausses des assurances et des matières premières, etc.), sociales (insécurité, instabilité et effet psychologique sur les populations, etc.) et environnementales désastreuses (pollutions maritimes et atmosphériques) .

Il apparaît donc primordial d'avoir des outils de traitement d'informations hétérogènes (texte, image, message, etc.) et une méthodologie pour authentifier rapidement un acte terroriste ou criminel à partir des alertes générées automatiquement par les systèmes actuels ou futurs de surveillance maritime (comme SPATIONAV, ICSS, SIVE, SYTAR, etc.). Ces outils permettront également à des enquêteurs, en temps différé, de mener des investigations, de faire des études statistiques, formuler des recommandations pour faire évoluer les réglementations et les équipements des navires et améliorer les moyens de surveillance.

# 4. Descriptions des Innovations Scientifiques et Techniques

Pour assister les «pools» d'experts dans leur travail d'authentification d'un comportement suspect, le démonstrateur TAMARIS mettra en œuvre des outils scientifiques :

- De mise en corrélation des alertes qui composent le comportement suspect et d'informations complémentaires pour authentifier la menace au plus tôt.
- D'évaluation de la cohérence logique des hypothèses prises pour aboutir à l'authentification de la menace.
- De géocollaboration entre les experts, afin de les aider à prendre en commun des décisions concernant le traitement des alertes et la constitution de dossiers d'enquête.
- D'aide à l'élaboration de dossiers d'enquête électroniques selon une forme standardisée.
- D'indexation des informations contenues dans les dossiers d'enquêtes pour un accès ultérieur classifié.
- D'aide juridique pour s'assurer que les éléments d'authentification (image, texte, etc.) sont des preuves acceptables par les tribunaux qui pourront être saisis.
- De validation des informations contenues dans les dossiers d'enquête en accord avec la réglementation en vigueur sur la protection de l'information.

Pour l'exploitation du démonstrateur TAMARIS par les experts, des technologies et des techniques innovantes sont intégrées :

- Une table interactive tactile de nouvelle génération (multi-utilisateurs, seulement quelques prototypes existent à ce jour) pour visualiser, manipuler et configurer des informations hétérogènes sur une grande surface d'affichage, dynamiquement et à plusieurs experts simultanément.
- Un ensemble d'interfaces homme – machine, s'appuyant sur la table interactive, adaptées à la mise en œuvre des outils scientifiques évoqués ci avant, prenant en compte les facteurs humains et les aspects cognitifs des experts dans leur démarche multi - hypothèses et progressive pour authentifier une menace.
- Une boite à outils pour traiter, exploiter, accéder à des informations externes aidant à la prise de décision.
- Une base de données structurées pour archiver des dossiers d'enquête indexés et une interface d'accès utilisant des clés de droit à en connaître. Ces dossiers constituent une base de connaissance pouvant être également utilisée dans la résolution d'un cas soumis à expertise.

# 5. Etat de l'Art

Ces outils et moyen d'exploitation innovants ont la possibilité d'apporter une forte valeur ajoutée TRES DEMANDEE aux opérateurs et à l'ensemble des acteurs de la sécurité globale aux frontières maritimes. Cependant, leur efficacité est conditionnée à une bonne appropriation des outils par les opérateurs et les experts, et à la capacité de ces mêmes outils à s'intégrer dans le processus de travail associé qui comporte des aspects d'organisation, de collaboration et de décision, tous trois critiques.

Il existe donc une série des enjeux techniques qui sont nouveaux dans TAMARIS et qui n'existent pas dans les systèmes actuels. Ces enjeux sont ceux des interfaces homme-machine et des capacités cognitives des opérateurs. Ce sont les suivants :

- Le lien avec les suivis de comportements suspects requiert une capacité à agréger, contextualiser et rejouer les situations dans l'espace et dans le temps pour améliorer leur compréhension et leur interprétation collectives. Le système doit proposer des infrastructures et des moyens d'interaction allant dans ce sens.
- L'authentification des menaces et des risques repose largement sur la capacité des experts à intégrer des informations auxiliaires dans le système, souvent obtenues par communication avec des entités externes, et à produire une analyse à réelle valeur ajoutée. Les ajouts d'informations et les analyses se faisant de manière asynchrone, TAMARIS propose une flexibilité suffisante aux experts pour leur permettre de travailler efficacement.
- L'élaboration du dossier d'enquête est la phase qui agrège le plus de compétences expertes. Cette élaboration doit se faire dans le respect des standards et son efficacité dépend directement du niveau de synthèse et de pertinence des informations qui y sont placées. La combinaison d'aide au raisonnement, de vérifications logiques et de support réglementaire dans un même outil, nécessite une compréhension fine des processus métiers pour les opérateurs et les experts.
- La gestion des anomalies (alertes successive sur un comportement suspect) )et les itérations sur les dossiers d'enquête réclament des possibilités de suivi et de notification, complémentées par une bonne gestion des interruptions (le processus d'analyse est asynchrone et porte potentiellement sur plusieurs événements en parallèle) et enfin des exigences en terme d'intégration et de classification des données.

L'exploitation de ces thématiques se limite à l'heure actuelle essentiellement à la recherche en Interaction Homme Machine [Neumann – Navigation in space, time and topics – ICA-ACI-2005]. Les applications industrielles en sont rares car elles sont difficiles à mettre en place et exigent des techniques d'interaction particulières combinant espace (2 à 3 dimensions) et temps (1 dimension). L'utilisation de ce type d'application sur des tables interactives multi-pointeurs et multi-utilisateurs, qui offrent une souplesse et un espace d'affichage suffisant pour ces interactions, dans un contexte opérationnel, est une activité technologique de pointe encore en

développement. Techniques qui seront utilisées et évaluées dans le démonstrateur TAMARIS.

Il est a noter que ces nouvelles techniques seront utilisées dans le démonstrateur TAMARIS pour assister un groupe d'experts pour authentifier rapidement une menace, mais aussi pour fournir à ce groupe d'experts, issus de différentes organisations, un espace de travail collaboratif qui permettra d'étudier et définir un mode de fonctionnement (processus) le plus adapté aux tâches des experts.

# 6. Architecture du Démonstrateur

Les composantes techniques du démonstrateur sont les suivants ::

- Outil pour suivre la chronologie des alertes sur des événements anormaux ponctuels qui sont détectés en continu par les centres opérationnels.
- Outil pour aider les utilisateurs experts à analyser et à interpréter les comportements suspects à partir de la chronologie des alertes dans le temps et l'espace. Cet outil suggèrera au besoin à l'utilisateur d'aller chercher des informations supplémentaires, de manière à orienter l'authentification des comportements suspects détectés. Ces analyses et ces interprétations sont réalisées durant le déroulement du comportement suspecté et enrichies à chaque alerte.
- Outil d'élaboration des dossiers d'enquête standardisés argumentant la nature des menaces et des risques associés à chaque nouvel événement anormal détecté (alerte), et lorsqu'un opérateur collecte des informations externes pertinentes. Ces mises à jour successives sont transmises à l'autorité décisionnelle pour leur permettre de suivre le déroulement de la situation et pour être informé de la nature de la menace expertisée et des risques associés, de son niveau de criticité.
- Outil d'indexation des contenus des dossiers d'enquête pour les archiver dans une base consultable en ligne par différents organismes avec des clés de droit à en connaître

Le schéma ci-après donne l'architecture des ces composantes de traitement, de fusion et d'analyse de l'information, et précise comment seront exploités ces outils pour générer des dossiers d'enquêtes électroniques durant le déroulement d'un comportement suspect.

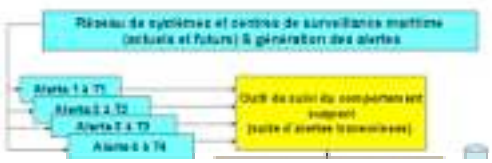

Figure 2 : Architecture du démonstrateur TAMARIS

Pour répondre à l'exigence opérationnelle de réalisation d'une expertise détaillée, durant le déroulement d'un comportement suspect, pour authentifier au plus tôt la menace et les risques associés, les outils **TAMARIS** sont basés sur les technologies innovantes suivantes :

- Une boîte à outils pour aider l'utilisateur à authentifier de manière optimale les comportements suspects correspondant à une chronologie d'alertes faisant état d'événements anormaux détectés, et à argumenter cette authentification pour contribuer à l'élaboration du dossier d'enquête.
  - ✓ Un outil d'authentification incitera l'utilisateur à enrichir les informations fournies par les alertes, en lui suggérant d'acquérir d'autres informations spécifiques, de manière à rendre plus efficace son processus d'authentification de comportements suspects. Ce module exploitera une base de modèles de comportements qui pourra être enrichie par le retour d'expérience à partir d'autres cas analysés dans le passé. Il procédera par comparaison entre les informations sur les alertes transmises à l'utilisateur et celles qu'il aura acquises lui – même d'une part, et les modèles de comportements d'autre part.
  - ✓ Un autre outil associera aux informations qui permettent au module précédent d'authentifier un comportement suspect, la mention des réglementations maritimes concernées ou éventuellement violées par ces informations, lorsque cela s'avèrera pertinent. Cela permettra de produire une argumentation avec une valeur ajoutée du point de vue juridique.
- Une procédure et un standard électronique pour élaborer les dossiers d'enquête et leurs mises à jour. Les informations contenues dans les dossiers sont indexées automatiquement. Des combinaisons de ces index permettent de créer des clés de droit à en connaître. Clés qui donnent, aux organismes en consultation de la base des dossiers, uniquement un accès aux informations pertinentes pour leurs missions.
- Une base structurée qui permettra d'archiver les dossiers d'enquête, les analyses des alertes, les hypothèses d'identification retenues, les sources d'informations consultées, avec une interface web sécurisée et conviviale pour la consultation selon des clés protégées de droit à en connaître. Cette base permettra, entre autres, d'enrichir les modèles

de comportement utilisés pour l'authentification de comportements suspects.

- Un ensemble d'interfaces homme machine pour les experts, ces interfaces reposent sur des tables interactives multi-pointeurs et multi-utilisateurs de grande dimension. Elles permettent d'analyser de grandes quantités d'informations avec des interactions naturelles et efficaces, en contexte collaboratif. En outre, les différentes interfaces (suivi, analyse et interprétation, élaboration du dossier d'analyse, etc.) seront conçues pour être homogènes et interopérables, de sorte à assurer une continuité et une flexibilité dans le travail des opérateurs et des experts.

# 7. Conclusion

En synthèse, TAMARIS apporte la couche fonctionnelle manquante aux systèmes de surveillance maritimes existants et futurs. Cette couche d'analyse et d'interprétation est essentielle pour authentifier la nature précise d'une menace liée à un comportement suspect d'un ou plusieurs navires.

Par exemple, les systèmes actuels et futurs détectent un abordage en mer (événement anormal = alerte) entre plusieurs navires à partir de leurs positions (pistes radar, AIS, VMS, etc.). Ces alertes transmises à TAMARIS seront suivies et analysées pour authentifier la nature de cet abordage qui peut être (liste non exhaustive) :

- Une collision (sinistre).
- Une assistance d'un navire en détresse (avarie).
- Un contrôle en mer.
- Un changement d'équipage en mer.
- Un transbordement de marchandise (capture de pêche illicite, drogue, arme, etc.).
- Un transfert d'immigrés clandestins sur plusieurs navires.
- Un acte de piraterie.
- Un détournement de navire pour une attaque terroriste (tanker et LNG) ou prise d'otage (ferry et navire de croisière).
- Etc.

Intégré dans un système de surveillance maritime, TAMARIS va contribuer à l'efficacité des moyens de sécurité globale visant à la protection des états et de leurs citoyens en facilitant et accélérant la détection, le suivi et l'authentification d'une menace.

# Remerciements

Le projet TAMARIS a été sélectionné par l'Agence Nationale de la Recherche (ANR) pour être subventionné dans le cadre du programme 2008 sur les concepts systèmes et outils pour la sécurité globale.

Le projet TAMARIS d'une durée de 2 ans devrait démarrer début 2009 pour se conclure donc début 2011.

Les événements anormaux utilisés en entrées du démonstrateur TAMARIS seront ceux détectés par le démonstrateur SCANMARIS. Projet qui a également été sélectionné pour financement par l'ANR en 2007. Le premier prototype SCANMARIS sera disponible début 2009.