CHAPITRE 15 - Le principe des organisations à haute fiabilité et sûreté appliqué au navire de commerce du futur conduit de terre

Bernard Dujardin

CHAPTER 15
Le principe des organisations à haute fiabilité et sûreté appliqué au navire de commerce du futur conduit de terre

Bernard DUJARDIN
Professeur d'économie
École Nationale Supérieure de Techniques Avancées (ENSTA)
Université Paris-Tech, France

Abstract: *Shore Controlled and Monitored Ship (SCMV) is based on a paradigm of security/safety reducing the maritime risk. Security is achieved by implementing a fail-safe principle whose redundancy is the key word. HRO (Highly Reliable organization) and HSO (Highly Sure Organization) are applied to the SCMV. HSO treats secure communications by an intrusion alarm system in the multi-layer network and neutralising any layer plagued by a virus.*

Résumé : *Le navire conduit de terre (NCT) repose sur un paradigme de sécurité/sûreté diminuant le risque maritime. La sécurité est obtenue par l'application d'un principe fail safe dont la redondance est le maître-mot. HRO (Highly Reliable Organization) et HSO (Highly Sure Organization) sont appliqués au NCT. HSO traite la sécurisation des communications par un système d'alerte de toute intrusion dans le réseau multicouche et de neutralisation de toute couche gangrenée par un virus.*





Bref retour sur l'Histoire des véhicules robotisés

En 1977, alors que les premiers rovers lunaires sont développés en Union soviétique et aux États-Unis, un premier véhicule terrestre autonome est conçu par le Laboratoire d'analyse et d'architecture des systèmes du CNRS. Le HILARE 1 est identifié par un nom à double sens. Certes, il signifie « Heuristiques Intégrées aux Logiciels et aux Automatismes dans un Robot Évolutif ». Mais son concepteur Raja Chatila, actuel directeur de l'Institut des systèmes intelligents et de robotique (ISIR), devait faire face à tant de scepticisme sur l'avenir d'un tel objet, qu'il s'en était prémuni préventivement par une pirouette acronymique. Depuis, les métros automatiques se répandent, malgré les réticences syndicales dans les grandes villes. Bientôt les voitures autopilotées circuleront sur nos routes. Dans le domaine du génie maritime, si la torpille peut être considérée comme un navire autonome, conçue dès le XIXe siècle pour une mission sans retour, les sous-marins inhabités se multiplient en mer pour répondre aux besoins de l'économie du pétrole offshore et de la défense navale (lutte anti-mines)[1]. Les patrouilleurs de surveillance maritime pilotés de terre, comme le *Protector* israélien sont des acteurs de la vie maritime depuis plus de dix ans. Les navires à positionnement dynamique de la prospection pétrolière n'existent qu'en se passant de barreur : aucun n'est en mesure de faire de la navigation stationnaire. Le navire inhabité ASDS «*Of-Course-I-Still-Love-You*» est un navire océanique de récupération du premier étage du lanceur Falcon 9 de SpaceX. Il est opérationnel depuis le 8 avril 2016.

Sémantique du navire conduit de terre (NCT - Shore Controlled and Monitored Vessel - SCMV)[2]

Le modèle de référence initial des navires sans équipage **embarqué** est d'abord militaire[3] : un navire permettant d'opérer dans des zones à risque létal pour l'être humain et capable d'une longue endurance inhumaine à la mer. La première étude de fond sur le navire de charge sans pilote provient de l'University College of London en 2003/4[4]. Le navire conduit de terre n'est pas un drone, terminologie réservée à des aéronefs sans pilote. Ce n'est pas un vaisseau spatial. Ce n'est pas un navire intelligent à moins que quelqu'un sache définir et quantifier l'intelligence d'un robot

1) Pour une histoire plus détaillée : article : Bernard Dujardin : « Le navire sans pilote », *La Baille,* nº 293 – septembre 2006.

2) AAWA exposé de position : sous la direction d'Esa Jokioinen – directeur de la Blue Ocean Team : juin 2016 «Remote and Autonomous Ship – The next steps».

3) Article : Seth Cooper et Matthew Norton (juillet 2002) «New Paradigms in Boat Design: An Exploration into Unmanned Surface Vehicles.» Symposium 2002 de l'Association for Unmanned Vehicles Systems.

4) Bucknall R., Freire P. (2003), «Unmanned cargo ships – A 2020 Vision» The Marine Engineer - Afloat or Ashore - IMarEST Colloquia series ; Bucknall R., Freire P. (2004), «Unmanned cargo ships» J. Marine Design and Operations 1, p. 3-10.

avec précision. Ce n'est pas un navire autonome dont les limites sont connues[5], préprogrammé pour conduire une mission déterminée : un sous-marin autonome de surveillance de pipeline surnage le tuyau en l'observant et en signalant d'éventuelles anomalies ; un chasseur autonome de sous-marins (projet ACTUV de la DARPA), dispose son équipement sonar d'écoute et de poursuite dans une zone maritime de passage éventuel de submersibles pour les détecter, les identifier et les pister. Un navire autonome n'a aucun lien avec la terre. Ses communications extérieures se limitent à des points GPS pour recaler l'estime de sa centrale à inertie. Le navire autonome est peu vulnérable aux cyberattaques de ce fait. Toutefois, il présente un défaut majeur : une incapacité à prendre une initiative. Programmé pour respecter les règles Colregs et ne respecter que ces règles, il n'a pas de capacités cognitives pour réagir à un événement qui sort de ces règles. S'il est prioritaire sur une route de collision dans une mer encombrée (détroit de pas de Calais), que doit-il et peut-il faire si un navire vu à gisement constant ne change pas sa route ? La réponse n'existe pas à ce jour.

Sur le NCT, le chef de quart comme sur un navire à équipage a pour fonction de prendre les initiatives, telles qu'attaquer sur le canal 16 de la VHF le navire rencontrant, éblouir au projecteur la passerelle pour réveiller le personnel de quart, sonner des coups de trompe, transgresser résolument les Colregs pour échapper à la situation, analyser si l'intention du navire est malveillante ou non et, si oui, agir en conséquence pour la contrer, en usant, par exemple, d'un laser de dissuasion et d'interception (LDI) et en limiter les conséquences, toutes options qui appellent une faculté immédiate d'analyse puis de décision qu'aucune programmation informatique ne peut prendre en compte et qui justifie le maintien de l'homme dans la boucle pour un navire sans pilote à vocation commerciale.

5) «The overall system autonomy is still very much a subject of active research, in autonomous decision making and mission planning. A standard watchdog system with a 'limp home' recovery might not be sufficient for the platform. A back up remote monitoring and control module will be required to prevent such calamity.» CheeKuang Tam, Richard Bucknall, Manhar Dhanak, Raju Datla: «Towards an Autonomous Surface Vessel» - 11th International Conference on Computer and IT Applications in the Maritime Industries - Liege, April 2012.

Figure 1 : Exemple de NCT

Le projet achevé aujourd'hui du Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) cofinancé par l'Union européenne dans le cadre du 7e PCRD est plus ambitieux que le NCT. Le concept est celui du navire autonome sans officier de quart, piloté par une organisation automatisée de la décision, surveillé par un contrôleur à terre. Bien que les conclusions du consortium MUNIN soient positives, elles soulèvent des problèmes qui sont loin d'avoir une solution opérationnelle, dont le principal est de savoir à partir de quel moment, le navire MUNIN va éveiller l'attention du contrôleur sur signal faible[6] dans un cas d'espèce comme celui évoqué ci-dessus.

Une comparaison s'impose avec le véhicule routier autonome et ses limites. Programmé pour respecter le code de la route, si une voiture folle fonce contre lui, que doit-il faire ? L'éviter à tout prix en transgressant le code de la route et monter sur le trottoir au risque d'écraser des piétons ou sacrifier ses passagers ? Le traitement informatique d'un dilemme n'a pas aujourd'hui de réponse satisfaisante. Si la circulation routière est assurée uniquement par des véhicules autonomes, la problématique soulevée dans cet exemple n'a plus lieu d'être. Si un mélange de véhicules pilotés et autonomes diminue le taux de l'accidentologie routière, la cohabitation de ces véhicules est à encourager.

6) «In addition to the vessel itself, a shore-side control center is also provided. This is where the autonomously operating vessels are monitored by qualified personnel. This center also needs to have the capability to assist or even remotely operate the ship, in case of unintended and unforeseen events.» Hans-Christoph Burmeister – MUNIN, June 2013 - IEEE Oceans 2013 conference.

Rendre la mer plus humaine

Si la mer est un risque pour l'homme, ce n'est pas parce que la mer est à l'occasion, inhumaine, c'est parce que l'homme s'y aventure de son propre chef. Rendre la mer plus humaine, c'est la faire passer d'un état parfois peu humain à un état qui l'est plus. C'est un des objectifs majeurs du NCT comme navire du futur. Non seulement les conditions de conduite éliminent pour son conducteur le « fait de mer », le risque maritime « corps », mais de surcroît, il lui offre des conditions de travail conformes à la physiologie circadienne à laquelle la nature l'oblige. Entre autres avantages, la femme devient l'égale de l'homme pour conduire les NCT[7].

Avec le NCT, la mer passe d'un état d'hostilité pour l'homme à un état de bienveillance (sea-friendly)[8]. L'activité des hommes est ancrée aux parties solides de la planète. La mer n'est plus pour le conducteur de NCT un passage obligé. Comme ce navire est inhabité, il n'est plus tenu comme le navire à équipage à prendre la route la plus rapide pour rallier sa destination. Ce facteur de sécurité de la navigation ne peut être ignoré.

Les porteurs d'eau ont disparu depuis longtemps, victimes d'une automatisation que personne au monde ne regrette : l'adduction d'eau à domicile. Le NCT pose la question de l'aversion à l'incertitude (biais de statu quo[9]) qui conduit au constat de Samuel Johnson : "To do nothing is in every man's power.[10]" Le navire sans équipage, tout comme le drone, se heurte à la pesanteur sociologique alimentée par la crainte que le métier de pilote de navire comme d'avion risque de disparaître. Si le véhicule routier autonome n'obéit pas au même réflexe conservateur, c'est parce que sa conduite est très peu professionnalisée et qu'il est la première cause de décès accidentel.

Une innovation de rupture sans percée technologique

Le NCT est au navire à équipage ce qu'est le porte-conteneurs au cargo traditionnel. Le conteneur est une boîte rectangulaire qui ne repose sur aucun progrès technique.

---

7) Communication : Bernard Dujardin : «Towards an equality between women and men in ocean navigation working conditions» Maritime Women: Global Leadership UMM / OMI – April 2014.

8) Article : Bernard Dujardin : « Travailleurs de la mer au XXIe siècle », *La Jaune et la Rouge,* nº 644, avril 2009.

9) Article : Samuelson W., Zeckhauser R. «Status quo bias in decision making» - *Journal of Risk and Uncertainty*, July 1988.

10) Article : Samuel Johnson - *The Rambler,* no. 155, September 1751.

Il en est de même pour le NCT[11]. Sa faisabilité opérationnelle est atteinte en 2015 avec la mise à disposition du monde maritime par Inmarsat du Global Fleet Xpress Satcom[12], premier réseau spatial à couverture mondiale à haut débit nécessaire aux liaisons NCT-Terre[13]. Les communications nécessaires à la conduite du NCT ne transitent pas par la toile du World Wide Web (www) et n'utilisent pas le protocole internet TCP-IP dont un niveau de sûreté acceptable ne peut être garanti dans la durée. Elles passent par des liaisons Satcom louées, des protocoles de communication et un système d'exploitation propres. La sécurité passe par la prise en compte dans le processus de décision des latences : de communication de la source navire vers l'opérateur à terre ; de traitement de l'information par l'opérateur (réaction) ; de transmission de l'ordre à la source. Le temps de transit spatial du processus dure entre une seconde quand un seul satellite en orbite géostationnaire est utilisé et deux secondes quand deux satellites sont en jeu (cas le plus fréquent). Ces temps sont plus triplés dès lors que les communications sont chiffrées. La distance parcourue par un navire à 20 nœuds est de 10 m en une seconde. Les aides à la navigation à la disposition de l'officier de quart sont programmées pour lui rappeler et tenir compte en permanence de cette contrainte physique spécifique à la conduite de terre. Elles sont couplées avec un dispositif d'autocontrôle en mesure de déclencher en urgence des réactions autonomes du NCT concernant la régulation de la vitesse et l'angle de barre. La sensibilité de la bande Ka à la pluie rend indispensable de garantir la permanence des communications en mode dégradé à moindre débit par une liaison redondante sur la bande Ku (10 à 18 GHz) voire sur la bande C (3 à 7 GHz).

Il est attendu du NCT une baisse du coût de possession[14] du navire de charge de 22 %[15]. La suppression des espaces vie et travail, nécessaires à la présence humaine, diminue les coûts de construction en série (30 %). Elle fait gagner une capacité commerciale supplémentaire (de 20 à 5 %, de manière dégressive à proportion de la taille du navire). L'automatisation et la télé-navigation grèvent le coût des équipements de communication, de surveillance, de contrôle et de navigation (40 %). L'impératif de fiabilité nécessite des redondances qui augmentent les coûts de l'appareil de

11) Appel à projets ADEME : Bernard Dujardin, Francis Faye « Le navire du futur : le navire conduit de terre », janvier 2012.

12) Le niveau de sécurité de ce réseau obéit aux normes américaines DoD 8500 Mission Assurance Category (MAC) level III/ National Institute of Standards and Technology (NIST) 800-53 Low Assurance.

13) 60 Mbits/s en bande Ka (18 à 31 GHz).

14) Coût d'investissement plus coût d'exploitation annuel pendant les 15 ans de durée d'amortissement économique plus éventuellement coût de démembrement. In « La conduite des programmes d'armement » - Cour des comptes - Rapport public annuel 2010 – février 2010. Les méthodes comptables de calcul sont développées dans la documentation classifiée du Comité des prix de revient des fabrications d'armement (CPRA) du Ministère de la Défense.

15) Source : Rolls Royce 2016. L'analyse de coût qui suit est issue des travaux de l'étude citée en note 11.

propulsion – mode électrique - et de direction (30 %). La production d'énergie (tout électrique pour la propulsion et les équipements) en conteneurs diesel est rationalisée et son coût diminué de 10 %. Les coûts de fonctionnement diminuent du fait de l'absence de présence humaine à bord et de la souplesse de la navigation par slow steaming (entre 20 et 40 % selon le cours du pétrole). Le coût de maintien en condition opérationnelle (MCO) est resserré (entre 5 et 10 % selon la taille des flottes) par une systématisation de la maintenance prédictive et par la mise en commun au sein d'une flotte homogène d'un maximum d'équipements sur le modèle de l'aéronautique civile. La conteneurisation des unités de production d'énergie électrique et les baies électroniques facilitent un échange standard et évitent des immobilisations au port.

L'objectif de sécurité/sûreté au cœur de la mise en œuvre du NCT

Le NCT reprend, en l'améliorant, le paradigme de sécurité/sûreté du navire conduit par un équipage embarqué. Le navire du futur vise une diminution des dangers de la navigation. L'analyse méthodique de la matrice de ces risques est à la base de la démarche conceptuelle :

- identifier et documenter les risques (sécurité) et les menaces (sûreté) potentiels ;
- identifier et documenter les points vulnérables du système de transport NCT et de son organisation ;
- identifier et documenter les conséquences potentielles des défaillances possibles et des arbitrages techniques de chaque composant du système NCT ;
- déterminer une stratégie de limitation des risques et de contention (containment) des menaces en fixant des priorités par pondération des vulnérabilités, risques et menaces, et de leurs conséquences évaluées en termes physiques et financiers.

La sécurité et la sûreté du navire sont obtenues par la combinaison d'une Highly Reliable Organization (HRO) et d'une Highly Sure Organization (HSO). L'objectif à atteindre est celui d'un système fail safe, principe bien connu de l'aéronautique (redondances et contrôles croisés) et fail secure, principe de protection visant à neutraliser le plus en amont possible les capacités de nuire.

Sécurité du NCT

Un NCT navigue dans le respect strict des conventions de l'OMI (International Maritime Organization)[16]. La conduite du navire de terre commande la fiabilité la plus élevée. Le facteur d'insécurité de la navigation est le facteur humain. « Toute manœuvre réussie est une catastrophe évitée de justesse. » La conclusion à tirer est : moins il y a de facteur humain dans un processus technique, plus la sécurité est assurée (d'où la suppression du troisième pilote dans l'aviation commerciale, la haute sécurité des métros automatisés). Plus le facteur humain est employé dans les conditions normales du cycle circadien propre à l'espèce, moins il ne présente de risque. Le NCT est conduit par un équipage réduit relevé toutes les huit heures, travaillant pendant les heures de bureau. Les trois relèves quotidiennes s'effectuent à partir de centraux navigation (CN - Navigation Workstation) situés sur des méridiens espacés de 120° de longitude (8 heures).

	Jour 1			Jour 2
Central Navigation	La Réunion	Guadeloupe Saint-Martin	Wallis	La Réunion
Temps Univers.	04.00	12.00	20.00	04.00
UT + 4	**08.00**			
UT - 4	16.00 →	**08.00**		
UT + 12		16.00 →	**08.00**	
UT + 4			16.00 →	**08.00**

La conduite du NCT repose sur un environnement cognitif qui diffère de celui du navire traditionnel. Certes, le risque de navigation continue à dépendre du facteur humain. Que le chef de quart sommeille sur sa passerelle ou dans un CN à terre, le risque se ressemble. Mais les conditions de travail ne sont pas les mêmes[17] : assistance permanente d'un officier supérieur dans un CN ; moindre risque de somnolence à terre pendant les heures de travail diurnes ; pas de fatigue liée au mouvement et au bruit de la plate-forme ; pas de mal de mer ; pas de stress de la navigation ; surveillance effective de l'alcoolémie et d'autres addictions ; assurance d'un véritable repos du conducteur ; remplacement au pied levé d'un officier malade. Le danger inhérent à une mauvaise compréhension des communications internes chez les équipages multinationaux – naissant des conflits linguistiques - disparaît avec un équipage établi à terre, réduit à un officier de quart et un officier supérieur superviseur.

16) Convention consolidée SOLAS IMO 2009 ; code ISM et principes directeurs IMO 2010 ; convention STCW avec ses amendements 2010 IMO 2011.

17) Article : Dominique Jégaden, médecin en chef honoraire (Marine), chercheur associé du LESTIC, Université de Bretagne Sud « Le stress et l'ennui chez les marins », *La Revue Maritime*, nº 489, septembre 2010.

Le CN en charge de conduire plusieurs navires concentre une équipe de plusieurs officiers, qualifiés chefs de quart passerelle STCW, (autant que de navires à conduire) – qualifiés Ship Security Officer au titre du code ISPS (International Ship and Port Facility Security) – qui réfèrent à l'officier superviseur pour réagir face à un incident. L'officier superviseur, qualifié capitaine STCW, dispose d'une capacité de personne désignée au titre du code ISM (International Safety Management), de Company Security Officer au titre du code ISPS, de Company Cyber Security Officer[18] pour répondre aux exigences de cybersûreté[19]. Les relations sociales de cette équipe diffèrent de celles d'un équipage resserré dans un espace clos, vivant éloigné de leurs cellules familiales. Avec le NCT, la spécificité de conduite du navire est affirmée. Les officiers de conduite sont libérés de toute tâche commerciale, de suivi des opérations de manutention des cargaisons et de maintenance en mode prédictif, toutes tâches conduites à terre par l'agent de l'armateur dans les ports d'escale. En conséquence, la criticité du risque de navigation est fortement réduite.

La question de la sauvegarde de la vie humaine en mer ne se pose plus sous l'angle de la sauvegarde du personnel embarqué[20]. La crainte obsédante de l'homme à la mer que tout marin rencontre un jour ou l'autre lors de ses navigations, disparaît. La perte totale du navire ne peut être que « biens » et non « corps et biens ». Par contre, le NCT bien qu'inhabité est un obstacle mobile à la navigation. La règle 5 des ColRegs[21] précise : « Tout navire doit en permanence assurer une veille visuelle et auditive… ». Le NCT dispose d'une capacité de veille en mesure de collecter et de transmettre un flux continu d'informations comportant des images vidéo en haute résolution, des sons et un grand nombre de relevés de mesures instrumentales au CN. Les données recueillies alimentent des moteurs d'inférence traitant les signaux en vue de les interpréter au regard des risques analysés fournissant à la conduite du navire une assistance à la décision (decision-making aids). Le seuil de vulnérabilité du NCT est moindre que celui du navire à équipage embarqué. Les performances attendues des senseurs de son système de veille optronique et électronique sont supérieures à celles d'une veille humaine en passerelle. L'amplificateur de lumière à balayage (vision nocturne) et la visibilité dans l'infrarouge[22] permettent notamment de détecter des objets que ni les jumelles, ni le radar quelle que soit sa fréquence d'émission, ne sont en mesure de repérer, telles que la tête d'un naufragé surnageant dans un rayon de 1 000 m autour du navire[23].

---

18) Note d'orientation : OMI FAL 40/INF. 5 January 2016 : «Guidelines on the facilitation aspects of protecting the maritime transport network from cyberthreats».

19) En matière de sûreté, le terme de cybersécurité est impropre.

20) Le poste de conduite du CN assure la veille pour chaque NCT du système mondial de détresse et de sécurité en mer (SMDSM - GMDSS). Le NCT dispose d'une drome de sauvetage à mise à l'eau téléopérée (International Convention on Maritime Search and Rescue - IMO 2006).

21) Convention Collision Regulations de l'OMI.

22) Équipement FLIR (forward looking infrared).

23) Si le système est couplé avec une aide au traitement du signal (suite logicielle type Automatic Sea

Les dispositifs de lutte contre les sinistres que sont l'incendie et la voie d'eau doivent pouvoir se passer de la présence humaine. S'ils n'ont pas à se préoccuper de l'évacuation ou de la sécurisation des personnels embarqués, ils doivent, par contre, être en mesure d'être opératifs sans intervention humaine. Ils sont établis sur un double réseau de pompes d'assèchement. Le ballastage dispose d'un système automatisé de correction d'assiette et de gîte pour neutraliser des gîtes permanentes avec ou sans voie d'eau (cas de dessaisissement dans la cargaison). Il est en mesure de prendre également des gîtes de sauvegarde en cas de voies d'eau à la flottaison.

La lutte contre l'incendie diffère selon que sont concernés les locaux techniques ou les cales destinées au fret. Le réseau du système de détection et de surveillance des incendies est doublé. Les locaux techniques usent principalement de moyens de défense et de lutte contre l'incendie à technologie gazeuse neutre (diazote) ou inerte (à base d'argon ou/et de dioxyde de carbone). Les cales et les soutes sont équipées d'asperseurs d'extinction couplés au réseau de distribution en eau de mer, combinés au réseau d'assèchement. Le plan informatisé de lutte contre les incendies permet tant le déclenchement automatique des moyens de lutte que leur pilotage à distance par le CN.

Aveugler totalement ou partiellement une voie d'eau avec des moyens de fortune (pinoche, paillet Makaroff, prélart, matériau polymérisant, etc.) que ce soit par l'intérieur de la coque ou par l'extérieur, nécessite une présence humaine à bord. Cette procédure de sauvegarde est impossible sur le NCT. Le traitement du risque voie d'eau est d'abord préventif. La structure du navire est à double coque. Les navires sont cloisonnés jusqu'au pont principal par tranche transversale et longitudinale.

D'autres éléments de sécurité spécifiques au NCT sont prévus. Le risque de rupture de la structure (cas *Erika*) est détecté en amont par des jauges de contrainte et un accéléromètre 3D mesurant l'effort sur la poutre[24], automatisant une réduction de vitesse en urgence et donnant des indications précises au CN pour qu'il adapte vitesse et route à l'état de la mer. Le positionnement GPS du navire manquerait-il à faillir pour différentes raisons (pannes de satellite, brouillage ou cryptage des signaux), une centrale à inertie (gyrolaser) en mesure d'établir une position précise à un nautique près au bout de 24 heures prend le relais. Les porte-conteneurs à cale ouverte sont équipés de glissières au-dessus du pont principal pour prévenir la chute accidentelle des conteneurs à la mer…

Vision 2013).

24) Brevet WO 2002097763 A1 - Christophe Capitant 2002.

High Reliability Organization (HRO)

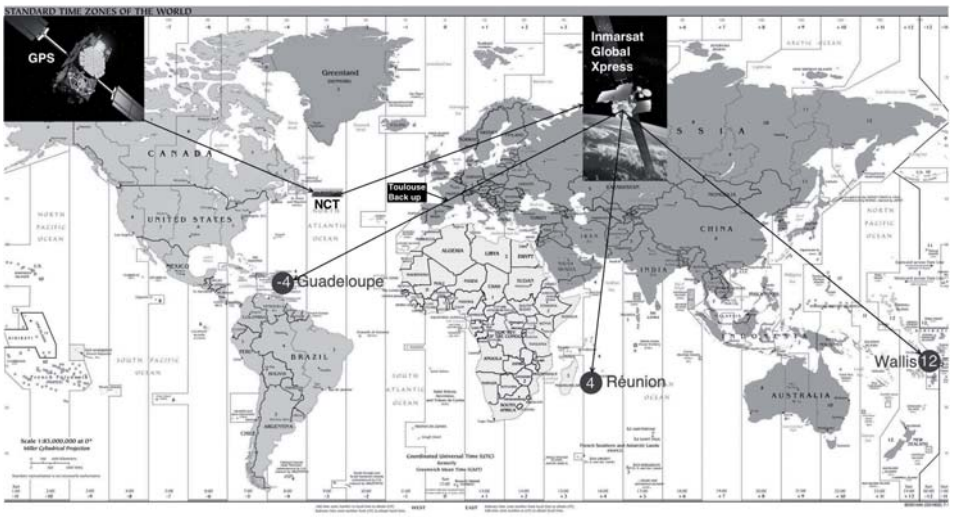
Les principes d'une organisation à haute fiabilité sont partagés par la HSO (voir ci-dessous) :

- l'organisation minimise au mieux le risque sans prétendre au risque zéro impossible à atteindre ;
- le système technique du NCT est assimilé à un système qui met en jeu la vie humaine (life-critical) dans toutes les phases de son fonctionnement ;
- la gestion optimisée des compétences de l'équipe du CN sur le modèle du crew resource management (CRM) de l'aérien organise l'équipe de conduite à terre ;
- l'autorité hiérarchique est d'intensité limitée (low authority gradient) ;
- le processus de décision corrèle 2 à 3 points de vue ;
- les capacités à détecter et à signaler les signaux faibles sont développées et alimentées par plusieurs sources dont l'apprentissage automatique ;
- l'aptitude à anticiper est également développée ;
- la résilience est valorisée par un potentiel de sauvegarde en modes dégradés successifs.

Sur le plan technique, l'organisation est fail safe. Cela signifie redondances et approche à tolérance de pannes (fault-tolerant system). D'un côté, des redondances passives : doubles sources indépendantes d'énergie, double système de gouverne, double ligne de propulsion (propulsion électrique : chaque ligne est isolée l'une de l'autre par un cloisonnement étanche). Répartition des groupes électrogènes diesels conteneurisés dans la proue et la poupe. Soutes à carburant liquide[25] (marine gasoil) divisées. Double système de senseurs (optroniques, électroniques et ultrasonores) et de communications de veille (AIS, SMDSM, VHF) réparti sur deux mâtures. Système de communication de contrôle du navire (matériels y compris aériens et fréquences) avec les CN usant de propriétés d'auto-configuration, d'autoadaptation et d'auto-réparation pour garantir la continuité et la permanence des liaisons descendantes et montantes. Trois CN répartis en longitude plus un CN back-up[26].

25) Le GNL, carburant plus propre alternatif et complémentaire, est stocké dans une citerne unique (IMO type C).

26) Le CN back up, outre sa fonction de back-up, prend en charge les entrées et sorties de ports, la navigation sur les canaux et chenaux d'accès portuaires, la veille sûreté pendant le séjour dans les terminaux portuaires du NCT en soutien des agents portuaires de la compagnie.



De l'autre côté, des redondances actives : un système de conduite du navire calqué sur celui d'un pilotage d'avion à commandes électriques ; redondance triple - triple-mode redundancy. Trois systèmes indépendants assurent les mêmes tâches simultanément et l'exécution des ordres n'est effective que si la majorité est en accord. En cas de désaccord, passage à chaud en modes plus ou moins dégradés (hot stand-by and guaranteed continuity of service) pouvant se terminer en navigation ultra-précautionneuse automatique (autonomous mode) permettant au NCT de naviguer en mode de survie aussi longtemps que nécessaire.

Sûreté du NCT

La sûreté du navire de commerce, dans une époque de piraterie, d'arnaque et de terrorisme, est une des préoccupations majeures de la chaîne de transport. Le chantage à la rançon ou au diktat politique par prise d'otages n'a pas lieu d'être avec un navire dont l'équipage de conduite est à l'abri à terre. Le système d'alerte SSAS (Ship Security Alert System) n'est pas nécessaire sur un NCT. La prise de contrôle du navire est rendue difficile dès lors que le cahier des charges du NCT impose un pupitre de conduite embarqué blindé (nécessaire pour les manœuvres portuaires et dans les canaux qui obligent d'embarquer à bord un pilote et des lamaneurs) et des œuvres vives spécialement conçues pour éviter une interception par neutralisation mécanique des systèmes de propulsion et de gouverne. Si tant est qu'un tel événement survienne, il est immédiatement détecté, localisé et suivi. Une intervention de forces de police maritime n'est pas handicapée par un bouclier d'otages derrière lesquels les assaillants se protégeraient. Le NCT n'a pas besoin d'un système d'autoprotection parce qu'il porte en lui-même son propre système d'auto-dissuasion. Il fait l'économie de gardes armés privés à bord.

La sûreté concerne également les CN et le NCT dans les terminaux portuaires. Le central navigation (CN), considéré comme point sensible, quelle que soit sa localisation, est conçu en infrastructure critique pour prévenir une intrusion et, en cas d'échec de cette prévention, pour neutraliser celle-ci. Le CN back up[27] joue un rôle de bouclier. À chaque relève de quart, le CN prenant est authentifié par le navire par l'intermédiaire du CN sortant. Le protocole du transfert de responsabilité repose sur une base technique et juridique éprouvée.

La sûreté portuaire du NCT relève d'un dispositif comparable à celui des navires avec équipage. Les différences sont que sur un NCT sans personnel embarqué, s'il n'y a pas de contrôle des entrées et sorties des navigants, le contrôle des allées et venues d'intervenants extérieurs (agent de la compagnie, pilote, lamaneurs, autorités douanière et sanitaire, entreprises de manutention, de maintenance et de livraison de soutes, etc.) est organisés par l'agent portuaire de la compagnie avec ses vigiles. L'optronique du NCT est organisée de manière à assurer en escale une fonction de surveillance jour et nuit des superstructures du NCT au profit de l'agent de la compagnie, responsable de la sécurité et de la sûreté du navire au port – avec l'aide du CN back up.

La cybersûreté est d'une importance majeure. Les redondances prévues dans la conception HRO constituent le premier étage de la réponse. Elles sont à compléter pour neutraliser au maximum toute menace sur les systèmes liés à la conduite du navire, à son contrôle et à la sécurité de la navigation, tous systèmes dépendant de communications extérieures. La technologie logicielle du NCT relève des principes d'un système d'armes – sans facteur humain dans la boucle – alors que celle du navire à équipage relève des principes d'un système d'information dont on connaît la vulnérabilité aux contingences humaines. Le système d'exploitation est un système propriétaire conçu uniquement pour une tâche : la conduite du navire.

Les protocoles de communication en couches supérieures, situés au-dessus de ceux des fournisseurs de liaison point à point CN – NCT, n'obéissent pas à des normes publiées ou publiques. Le NCT, sans présence humaine à bord, n'a pas besoin de connexion au www à la différence d'un navire à équipage dont les membres ont accès à l'Internet au moins pendant leurs temps de repos.

27) Le CN back up peut dans certains cas critiques prendre le contrôle du NCT.

High Security Organization (HSO)

Les principes propres d'une organisation à haute sûreté sont complémentaires de la HRO :

- priorité à la sécurité sur la sûreté ;
- vulnérabilité aux actes malveillants considérée comme permanente quel que soit le lieu où se trouve le NCT ;
- application au NCT du code international pour la sûreté des navires et des installations portuaires (ISPS)[28] ;
- approche cybersûreté visant à neutraliser les techniques sophistiquées d'exploitation des vulnérabilités des systèmes (Advanced Persistent Threat) par l'organisation d'un Cyber Risk Management (CRM)[29], d'où la fonction de Company Cyber Security Officer confiée à l'officier superviseur ;
- système d'alerte précoce de la moindre anomalie de comportement du navire et de toute intrusion active ou passive sur le réseau multicouche de la chaîne de contrôle et de conduite ;
- neutralisation de toute couche gangrenée par une intrusion ;
- confidentialité rigoureuse du plan de cybersûreté.

Le système fail secure a pour objectif d'assurer la sûreté maximale du NCT. Le dispositif de protection est concerné par trois points : système de conduite, traitement des données et transmissions terre-NCT.

Sur le premier point, le matériel est protégé dès lors qu'il est enfermé dans des baies blindées et durcies contre les impulsions électromagnétiques (IEM) et, pour les aériens, placé dans des endroits difficiles d'accès (mâtures) et/ou conçu pour entraver son identification et sa localisation.

Sur le second point, les aspects logiciels et données sont à prendre en compte. La partie logicielle du traitement des données, les clés d'accès et les algorithmes de cryptage obéissent à des règles d'accès strictes (application du principe de moindre privilège) et d'implémentation non télématique par médiation d'un support physique[30].

---

28) Code International Ship and Port facility Security – Guide de sûreté maritime et code ISPS – OMI 2012.

29) Communication : IMO FAL 40/INF 5 - janvier 2016.

30) L'interception des programmes logiciels transmis sur les réseaux filaires ou non de communication est rendue impossible.

Les données reçues de l'extérieur sont à protéger des interférences mal intentionnées : les données GPS sont corrélées en continu avec celles que produisent le calculateur d'estime du CN et la centrale à inertie embarquée pour s'assurer de la fiabilité des sources GPS ; les mises à jour ECDIS ne sont pas délivrées directement au NCT et aux CN - elles sont, au préalable, filtrées par le CN back up ; la véracité des données AIS est analysée[31] - la détection des truquages des données AIS dans le domaine de la position, de la route et de la vitesse fond des navires et des positions fantômes est un facteur de sécurité autant que de sûreté[32].

Sur le troisième point, les télécommunications constituent l'ombilic qui relie le navire au CN. Elles sont susceptibles de subir des attaques de plusieurs types : interception passive, intrusion, neutralisation. Les points de vulnérabilité sont les stations d'émission/réception embarquée (navire) ou à terre (CN), le réseau de communication type Inmarsat. L'ensemble de ces menaces est à prendre en compte.

L'interception passive des communications (écoute clandestine) est entravée par le cryptage asymétrique des données, conçu de manière à ne pouvoir être cassé que dans des délais qui donnent aux informations collectées le temps d'être périmées. Le caractère point à point des transmissions terre - NCT donne au cryptage une moindre visibilité qui n'est qu'une protection apparente. Une attaque de pirates informatiques, quelle qu'elle soit, est toujours plus efficace quand elle est ciblée.

L'intrusion peut présenter deux formes. La première consiste à neutraliser la seule liaison terre-navire et à substituer à sa place une liaison pirate en laissant la liaison navire-terre opérer comme si rien ne se passe. L'interception par l'Iran d'un RQ-170 Sentinel, drone américain en mission d'espionnage, le 4 décembre 2011, en est une illustration. Le CN doit être informé aussi rapidement que possible d'une agression de ce type pour reprendre le contrôle du NCT. Sa détection repose sur un dispositif de sécurisation des communications par accusé de réception éprouvé (implémentation de fonctions de hachage) qui avertit des anomalies à risque. L'anomalie une fois détectée et analysée comme agression, la reprise en main de la maîtrise du NCT consiste à basculer les communications sur un réseau de communication redondant. La seconde forme d'intrusion est de faire parvenir au CN des informations conformes à celles qui sont prévues alors que le navire suit une autre route. Cette malveillance est extrêmement difficile à mettre en œuvre. Elle nécessite d'investir le navire sans

31) Les transpondeurs AIS ne fournissent pas des positions GPS validées. Chaque navire est en mesure d'y introduire des positions d'autres origines : estime, centrale à inertie, points par relèvements et astronomique ou n'importe quoi. Les antennes de réception AIS de chaque mâture du NCT sont utilisées comme base télégoniomètre : l'analyse des signaux radioélectriques AIS reçus donne le gisement de l'émetteur et une approximation de sa distance.

32) Rapport: AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea, Windward, October 2014.

être repéré, de connaître la localisation des centres névralgiques, d'y pénétrer et de connaître leur mode d'emploi pour intervenir du bord sur le système de conduite du navire. La gestion temporelle de la redondance des systèmes embarqués de conduite du navire est conçue de manière à détecter une agression de ce type en temps utile pour engager une mesure de sauvegarde.

La neutralisation des communications de conduite du navire par brouillage ou par destruction d'émetteurs-récepteurs est un cas d'agression dont la détection repose sur le même principe que l'intrusion. Elle est contrée par basculement prioritaire sur un réseau de communication redondant en état de fonctionner. L'ultime action est la mise automatique en mode de survie du NCT. Sur la question des back-ups, la discrétion est de rigueur. Elle ne peut en conséquence être détaillée.

L'accident de navigation qu'il soit causé par l'erreur humaine (atteinte à la sécurité) ou la volonté humaine (atteinte à la sûreté) relève toujours du facteur humain, quels que soient les habits qu'on veut faire porter à la réalité pour dégager les responsabilités. M. de La Palice dirait que le facteur humain est consubstantiel à l'existence de l'homme. Tendre vers le risque zéro oui, mais tout en gardant à l'esprit que le « Concordia Complex (CC) »[33] ne sera jamais éradiqué, qu'il se fasse valoir sur la route d'un navire avec équipage embarqué ou sur celle d'un navire avec équipage à terre.

Le NCT reste pour peu de temps encore le navire du futur. Il ne se substitue pas au navire avec équipage, mais il vient compléter l'offre de transport maritime. L'actualisation des conventions de l'OMI, en vue d'insérer ce navire dans la circulation maritime mondiale, est en cours. Dans les années 2020, le NCT fera partie du paysage maritime si les travaux de l'OMI aboutissent en temps utile. La sécurité de la navigation s'est considérablement améliorée depuis un demi-siècle bien que la sûreté maritime se soit dégradée. Le NCT s'inscrit dans la dynamique d'une mer plus sûre tant au niveau de la sécurité que de la sûreté, la sécurité ayant nécessairement la priorité sur la sûreté en temps de paix.

33) Rapport : Maurizio Catino « Analisi preliminare sui fattori umani e organizzativi del disastro della nave Costa Concordia » - Aprile 2012.