Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER

« CYBER SECURITE »

RENFORCER LA PROTECTION DES SYSTEMES INDUSTRIELS DU NAVIRE

Edition janvier 2017

DGITM / Direction des Affaires Maritimes

Contenu

SENSIBILISATION SUR LA SECURISATION DES SYSTEMES INDUSTRIELS

Pour une installation industrielle, les compagnies d'assurance n'hésitent plus désormais à classer en premier lieu le risque « cyber » et ceci bien avant le risque terroriste et de catastrophes naturelles. Cette nouvelle approche provient d'une part de la prise de conscience de la menace au travers d'attaque au format destructeur de type STUXNET/HAVEX/DRAGONFLY… et d'autre part d'un système industriel qui s'est fortement ouvert à des sous traitants externes et à l'internet des objets.

Par ailleurs, il convient de différencier l'informatique dédié à un système industriel (OT) et l'informatique dite conventionnelle de type bureautique/gestion (IT). Les solutions de cyber sécurité de l'informatique classique ont été conçues pour traiter en priorité des enjeux de confidentialité et pour bloquer toutes les activités suspectes. Ces solutions intrusives ne permettent pas de garantir pleinement la sécurité d'une installation industrielle. Ainsi, ces solutions peuvent générer trop d'erreurs de jugement d'un programme de détection (faux positif) qui amène un arrêt du système industriel.

Dans ce contexte, la numérisation du navire étant désormais une réalité, il ne bénéficie plus d'un niveau de sécurité informatique de type « air gap » consistant à l'isoler physiquement de tout réseau informatique. Le navire s'intègre donc tout naturellement dans la toile internet. Le navire se compose d'un ensemble de systèmes industriels pilotés par des automates régissant la conduite, l'énergie et les opérations commerciales du navire. Dans ce contexte, ce guide vise à sensibiliser les compagnies maritimes aux cybers risques spécifiques de l'internet industriel à bord du navire afin d'y adapter des règles d'usage préconisées en fonction du risque.

A- EVALUATION DES RISQUES

Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux cybers menaces qu'elles introduisent. A bord du navire, les automates programmables (API) sont omniprésents et peuvent gérer la conduite et les opérations de cargaison du navire.

A1- VULNERABILITES DU NAVIRE

Les systèmes industriels critiques présents à bord du navire peuvent être classés de la manière suivante :

- système de propulsion (moteur principal, énergie, conduite),
- système de gestion de la sécurité (incendie, voie d'eau),
- gestion de la cargaison (sécurité transfert cargaison, gestion de la stabilité),

La vulnérabilité d'un système industriel n'est plus à démontrer. Les APT (Advanced Persistant Threat) de type STUXNET ont illustré leurs compétences en matière de sabotage. Les vulnérabilités d'un système peuvent porter sur les sept domaines suivants (Référence étude DAM de septembre 2016 : http://www.developpement-durable.gouv.fr.vpn.e2.rie.gouv.fr/Surete-des-navires.html) :

(1) **L'absence de développement sécurisé** : développements internes, absence d'intégration de la sécurité, session non verrouillée,
(2) **Un faible niveau de protection des accès** : contrôle d'accès très simple avec une gestion de l'utilisateur et du mot de passe trop faibles ou inexistant, absence d'antivirus sur les postes de travail et serveurs, des utilisateurs disposant de privilèges administrateur.
(3) **L'absence de cloisonnement entre les systèmes d'information de gestion et les systèmes industriels non sécurisé** : ce principe permet de s'introduire via le système de gestion informatique dans le réseau industriel. Cette faille est la cible de nombreuses attaques récentes. Ces ponts servent à remonter des informations issues de la production directement dans les systèmes de pilotage. Cette méthode d'accès permet à la fois le recueil d'information et le sabotage.
(4) **Absence de supervision anormale du système.**
(5) **La non mise à jour et la faiblesse des protocoles de gestion courants** (FTP, Telnet, VNC, SNMP…) utilisés sans chiffrement qui ouvre l'accès à la récupération de login/mot de passe, à des connexions illégitimes aux serveurs,
(6) **L'utilisation croissante de systèmes informatiques standards non durcis** : Ces produits sur étagères permettent une réduction des coûts et d'interopérabilité (protocole TCP/IP, standard Ethernet ou les systèmes d'exploitation Microsoft Windows ou Linux : du fait de leur simplicité et de leur généralisation, le coût de ces technologies les a rendues incontournables). Ces systèmes sont par conséquent la proie de logiciel malveillant.
(7) **L'absence de contrôle des intervenants sur les systèmes industriels :** la surveillance des sous-traitants reste bien souvent insuffisante. Les conséquences de cette non-gestion peuvent être la perte de données, la détérioration d'équipements, la mise en danger du navire de son équipage et de l'environnement.

A2- RISQUES

Le cyber risque pour le navire est de deux ordres :

- La dégradation de l'image de la compagnie pouvant aboutir à une perte de compétitivité de la compagnie,
- Le sabotage du navire par système dormant ou opéré sur demande pouvant aboutir à la perte du navire, la perte de l'équipage ou l'atteinte à l'environnement.

En référence aux enquêtes réalisées par la Direction des Affaires Maritimes et à l'audit d'un navire conduit par l'Agence Nationale de Sécurité des Systèmes d'Information, le résultat de l'analyse des risques appliqué aux systèmes industriels embarqués à bord du navire peut être matérialisé de la manière suivante (Extrait de l'annexe n°2) :

Opération	**Risque**	**Impact potentiel**	Evaluation du risque avant la mise en place de mesures préventives	**Mesures préventives**	Evaluation du risque après la mise en place de mesures préventives
Conduite des systèmes industriels critiques à bord du navire	**(1) Acte d'intelligence économique offensive**	Dégradation de l'image de la compagnie	**Modéré**	Stratégie globale de sécurisation	**Bas**
	(2) Espionnage	Perte de compétitivité de la compagnie	**Modéré**	Stratégie globale de sécurisation	**Bas**
	(3) Sabotage	▪ La perte du navire, ▪ la perte de l'équipage, ▪ l'atteinte à l'environnement.	**Sévère**	Stratégie globale de sécurisation et maitrise de l'internet des objets	**Modéré**
				Stratégie globale de sécurisation et maitrise de l'internet des objets + surveillance passive	**Bas**
				Stratégie globale de sécurisation et maitrise de l'internet des objets + surveillance passive + durcir la chaine ICS	**Très bas**

B- RENFORCER LA PROTECTION

Il n'existe pas de solution miraculeuse ou idéale. En référence à l'évaluation de la cyber sécurité faite à bord du navire, 3 niveaux de protection peuvent s'intégrer dans un système de gestion de protection de l'installation industrielle mis en place par une compagnie maritime.

B1- PREMIER NIVEAU : « STRATEGIE GLOBALE DE SECURISATION »

Objectif : Apporter un cadre pérenne de sécurisation des systèmes embarqués,
Exigence fonctionnelle : Ce principe répond au deux tiers des mesures à mettre en place - par le plus haut niveau de direction de la compagnie - pour faire face à un cyber acte de malveillance. Ces mesures de gestion portent sur la formation, la gestion de procédure au travers de normes ou outils adaptée à une compagnie maritime (code ISM/ISPS). Les systèmes d'information industriels doivent être intégrés dans les politiques de sécurité des systèmes d'information de l'entreprise, comme tout autre système d'information et ceci, dès l'origine du projet.

Règles d'usage : Cette sécurisation globale du système industriel du navire doit porter sur l'usage de **règles d'hygiène de l'informatique** adaptées au système industriel du navire :

- **Contrôle d'accès physique aux équipements :** Fermer les armoires automates à clé, contrôler les accès des postes de contrôle : machine, cargaison et passerelle..
- **Cloisonnement des réseaux :** séparer les réseaux par des équipements dédiés ou des VLAN. filtrer les flux au moyen de pare-feu, tracer les flux rejetés et les analyser,
- **Gestion des comptes :** Définir une politique de gestion des comptes utilisateur, ne pas laisser les comptes par défaut sur les équipements, gérer les mots de passe,
- **Durcissement des configurations** : installer uniquement les logiciels nécessaires, ne pas laisser d'outils de développement sur des serveurs de production ou stations opérateur, désactiver les modes de configuration et de programmation à distance sur les installations critiques,
- **Gestion des journaux d'événements et d'alarmes :** Activer les fonctions de traçabilité si les équipements et logiciels le permettent, centraliser les journaux et générer des alertes pour des événements anormaux,
- **Sauvegardes & restaurations :** Définir une politique de sauvegarde permettant la reconstruction d'une installation suite à un acte de malveillance,
- **Cartographier les installations :** Equipements, constructeur, N° série, historique,
- **Documentation :** Définir une politique de gestion de la documentation,
- **Protection antivirale :** Définir une politique antivirale, protéger en priorité les équipements et applications en contact direct avec l'extérieur et les utilisateurs,
- **Protection des automates :** Protéger l'accès aux automates par un mot de passe, désactiver les modes de configuration et/ou de programmation à distance lorsque la fonctionnalité existe.

B2- DEUXIEME NIVEAU : « OUTILS DE SURVEILLANCE PASSIVE »

Cette étape fait suite à une **analyse de risques des systèmes industriels** à bord du navire.

Objectif : scruter le réseau à la recherche des signaux faibles (Détection comportementale). Ces mesures n'empêcheront pas un incident mais permettront de le détecter et d'en limiter autant que possible les effets. Plus un incident sera détecté tôt, plus il sera possible de mettre en place des mesures pour en réduire et confiner les effets.
Exigence fonctionnelle : disposer à bord du navire d'une capacité opérationnelle pour prévenir, détecter et répondre à une cyber attaque qui visent l'internet industriel du navire.
Règles d'usage : Cette sécurisation correspond aux mesures suivantes :

- **Sonde de surveillance :** La surveillance passive consiste à positionner une sonde au niveau du réseau. Cet objet surveille l'inventaire et les commandes effectuées sur le réseau industriel. Le système apprend la cartographie de l'installation. Une représentation visuelle du réseau est alors définie en fonction des évolutions naturelle du système. La connaissance du réseau est réalisée par un modèle mathématique (gabarit) : la matrice compare à l'issue tout ce qui est hors gabarit au niveau de la conduite de l'exploitation du système industriel. Le système de surveillance peut être intégré à un SOC. Ce principe utilise le mode d'action de l'attaquant qui cartographie le système attaqué.
- **Gestion des configurations :** Cette mesure consiste à **c**omparer les programmes et configurations actifs dans les équipements (version N exécutée) avec une version de sauvegarde identifiée comme la référence (version N sauvegardée). Avant la mise en service de nouvelles versions, une analyse des écarts entre les versions N et N-1 devrait avoir lieu.

B3- TROISIEME NIVEAU : « DURCISSEMENT DE LA CHAINE DU SYSTEME INDUSTRIEL »

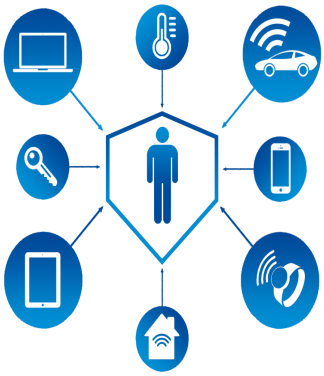
Cette étape fait suite à l'analyse de risques et s'applique au système sensible du navire en **segmentant les réseaux essentiels à la conduite** du navire..

Objectif : élever le niveau de difficulté de prise en main du système industriel par un attaquant,
Exigence fonctionnelle : Afin d'élever le niveau de protection du système industriel embarqué, il convient de disposer d'équipement préparé à faire face à un acte de malveillance. L'idéal est de disposer d'une chaine entièrement certifiée : de la supervision à l'automate programmable en passant par le commutateur, le pare-feu. Cette chaine peut être certifiée. Il est à noter que la certification des capteurs/actionneurs apparait difficile. Aussi, il convient de les sécuriser par une protection physique. En complément de cette certification, il convient d'effectuer une veille active des failles du système industriel (patchs). La robustesse de ce système repose sur une chaine certifiée et une veille CERT.
Règles d'usage : Cette sécurisation répond aux points d'actions suivants :

- **Equipement sensible du navire :** Certifier la chaine du système industriel critique,
- **Veille des mises à jour des API** : assurer une veille active par la compagnie,

C- MAITRISE DE L'INTERNET DES OBJETS (IOT)

Depuis une dizaine d'année, le réseau internet se transforme progressivement en un réseau étendu, appelé « Internet des objets », reliant plusieurs milliards d'êtres humains mais aussi des dizaines de milliards d'objets.



L'IOT, grâce à l'omniprésence de ses capteurs et systèmes connectés, fournit au système de pilotage des informations qui permettent d'identifier et de résoudre des problèmes. Ces systèmes permettront à termes aux compagnies maritimes de bénéficier d'une meilleure rentabilité du navire. Ce gain d'efficacité permettra ainsi une baisse des coûts d'exploitation et de maintenance du navire.

L'une des prochaines intégrations de l'IOT dans le monde maritime concerne le suivi de conteneurs. En 2017, la société française TRAXENS va équiper 200.000 EVP d'un boitier intelligent. Ce dernier permettra le suivi en mer, à terre du conteneur au travers d'outils de communication reliés au réseau GSM et satellitaire qui l'environne. Le navire sera qu'en a lui équipé d'un ordinateur central afin de relayer les informations délivrées par le boitier équipant le conteneur.

Pour être pleinement efficace, ces objets doivent être sécurisé afin d'éviter tous actes de malveillance tel que la prise en main à distance de ces objets qui prennent part à un réseau de machines zombies pour perturber un système (Attaque de type DDOS).

Objectif : sécuriser l'IOT connecté au système industriel,

Exigence fonctionnelle : L'IOT peut être amené à collecter des données sensibles du système industriel. Ces données peuvent être enregistrées sur un CLOUD. Il convient de s'assurer de la nécessité de besoin d'un IOT dans la conduite des systèmes industriel du navire. L'évaluation de la cyber sécurité des systèmes industriels doit permettre de rationaliser ce besoin pour le navire.

Règles d'usage : Cette sécurisation consistent à adopter les règles suivantes :

- **Evaluer la nécessité d'objet connecté à un système industriel embarqué** : Cette évaluation doit nécessairement prendre en compte la sécurisation de l'IOT notamment si l'archivage des données est transmis à un CLOUD.
- **Définir une politique pour l'utilisation des IOT :** Le haut niveau de la compagnie devrait valider cet engagement. Cette politique devrait statuer sur la désactivation ou l'utilisation de ces outils pour échanger des données entre les réseaux, sur la désactivation des ports USB sur les systèmes, sur la restriction des fonctionnalités de l'IOT. Plus la surface d'attaque sera limitée, plus le champ d'action du cybercriminel sera limité via l'internet des objets.

D- CONCLUSION

Le secteur informatique compte pas moins de 4 pôles d'activités qui se syntétise autour de l'informatique de gestion (IT), l'informatique industriel et technologique (OT), l'informatique des réseaux et télécommunications et enfin le domaine de l'informatique multimédia. Le navire est construit autour d'une composante d'informatique industrielle auquel il convient d'intégrer une composante d'informatique d'administration.

La rencontre de ces deux mondes qui évoluait jusqu'à présent de manière parallèle engendre des vulnérabilités qu'il convient d'appréhender et de définir une stratégie d'harmonisation. La non prise en compte de ces failles systèmes pourrait avoir de grave conséquence pour le navire et la compagnie.

Pour faire face à cette menace, il convient de mettre en place des règles d'usage concernant l'hygiène d'informatique industrielle. Ces règles doivent s'adapter aux particularités du système industriel qui impose une disponibilité des systèmes. La mise en place de ces règles doivent être élaborer en concertations avec le service machine du navire qui possède la connaissance de la conduite de l'ensemble des équipements embarqués : propulsion, énergie, stabilité, gestion de la cargaison du navire et système d'alarmes.

En complément, la compagnie peut compléter ces bonnes pratiques de mesures spécifiques sur des équipements sensibles du navire. Ces mesures font suite à une analyse du risques et peuvent prendre la forme de systèmes de surveillance passive, de segmentation de réseaux et de certification d'une chaine industrielle.

Enfin, il convient dès à présent d'identifier par la compagnie, les règles d'usage des objets connectés à internet qui sont amenés à collecter et à traiter des informations systèmes. Ces objets peuvent être la porte d'entrée d'un attaquant. La mise en place de l'ensemble de ces mesures doit s'incrire dans une politique globale de sécurisation des systèmes d'information du navire.

E- ANNEXE N°1 – DEFINITIONS

- **API (Programmable Logic Controllers) :** Un automate programmable industriel est un équipement qui permet de réaliser, de façon continue et sans intervention humaine, la commande de processus industriels machine ou processus continu. En fonction de ses données d'entrées (capteurs), l'automate envoie des ordres vers ses sorties (actionneurs).

- **APT (Advanced Persistant Threat) :** ver évolué de type STUXNET et dérivé,

- **CERT :** Computer Emergency Response Team,

- **Commutateur :** le commutateur industriel permet d'interconnecter différents équipements ou segments de réseaux communiquant en Ethernet,

- **CLOUD :** Le « cloud computing » correspond à l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau,

- **DDOS (Distributed Denial Of Service) :** attaque de type déni de service distribué qui consiste à noyer en informations inutiles un service (Attaque de type « Mirai »),

- **ICS (Industrial Control System) :** l'ensemble des réseaux industriel,

- **Internet industriel** : intelligence du processus qui agit sur les capteurs /actionneurs,

- **IT :** technologies standardisées de l'informatique classique ou conventionnelle,

- **IOT (Internet Of Things) :** internet des objets,

- **OT (Operationnel Technologie) :** Informatique dédié à un système industriel,

- **Pare-feu (firewall):** ce système permet d'assurer l'interconnexion entre un réseau industriel que l'on cherche à protéger et un autre réseau,

- **Patchs :** application de correctifs apportés à une faille système. Dans le domaine industriel, il convient de s'assurer que le patch est bien adapté car il pourrait remettre en cause le bon fonctionnement de l'installation.

- **Sonde (Censor) :** capteur numérique sur un réseau qui surveille des vulnérabilités,

- **Réseau industriel :** langage machine/machine,

- **Système ACTIF :** action physique sur les entrées/sorties d'un système d'information,

- **Système PASSIF :** dispositif qui analyse l'échange de données sans interférer le système,

- **SCADA (Supervisory control software) :** supervision/pilotage d'un système industriel,

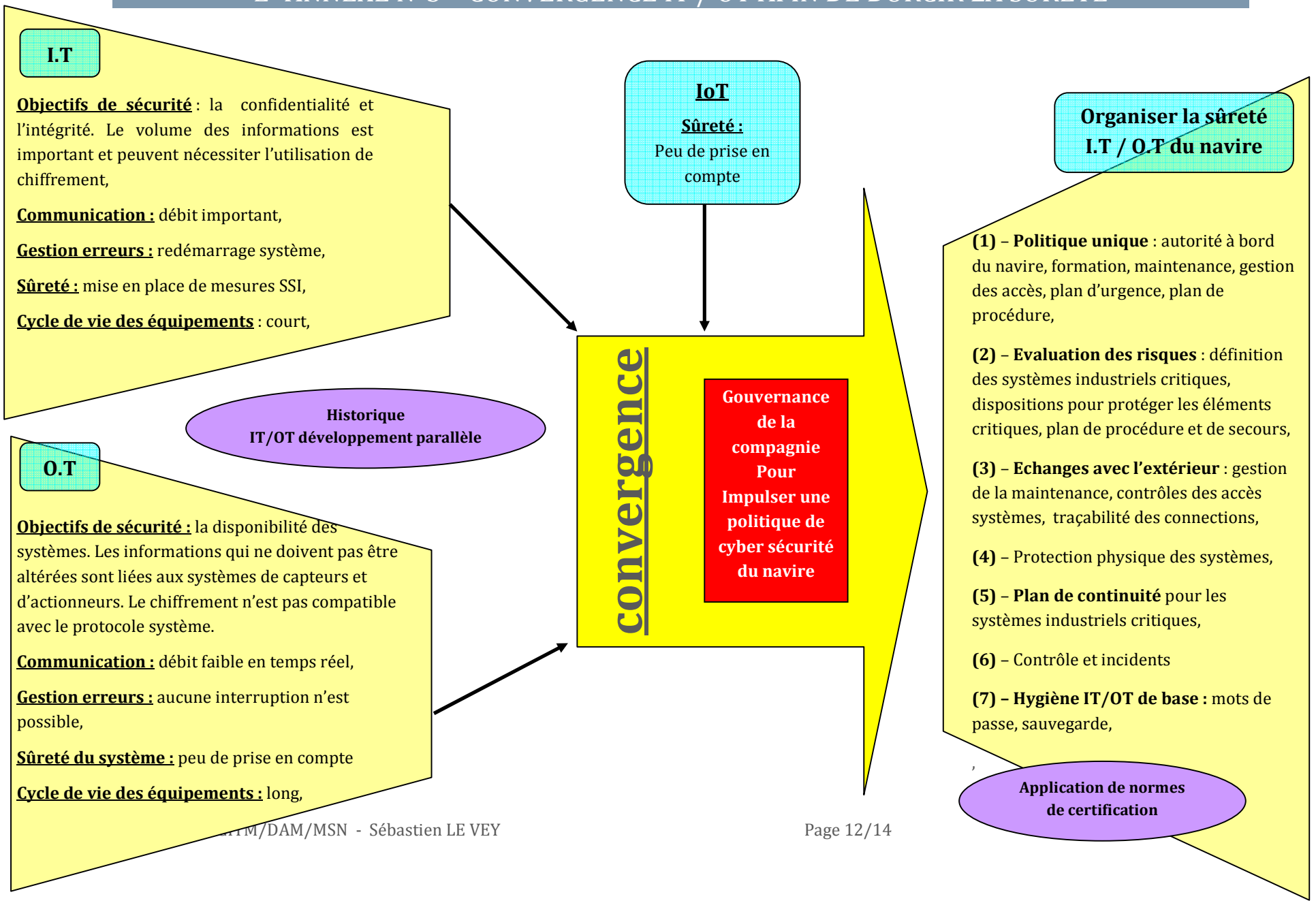
- **SOC :** Security Operation Center,

E- ANNEXE N°2 – MATRICES DES RISQUES

Opérations	Risques	Criticité		Evaluation du risque avant la mise en place de mesures préventives	Mesures préventives	Evaluation du risque après la mise en place de mesures préventives	Règles d'usage	Outils
		Impact potentiel	Menace probabilité					
A- Conduite des systèmes industriels critiques à bord du navire ▪ Propulsion ▪ Energie ▪ Cargaison ▪ Stabilité ▪ Alarmes	Acte d'intelligence économique offensive	Dégradation de l'image de la compagnie	**Occasionnelle** (Revue documentée SGDSN de 2016)	**Modéré**	Stratégie globale de sécurisation	**Bas**	**Hygiène OT de l'informatique :** - Evaluer IOT, - Politique, - cartographie, - contrôle accès, - sauvegarde, - restauration …	**A- Norme de certification** -Code ISM, -Code ISPS, -IEC 61162-460 - famille ISO CEI 27000, **B- Formation** -Sensibilisation, - Formation, officiers **C- Outils technologique** - Sonde de surveillance, - API certifié, - pare-feu, - VPN, - NAS
	Espionnage	Perte de compétitivité de la compagnie						
	Sabotage	- La perte du navire, - la perte de l'équipage, - l'atteinte à l'environnement.		**Sévère**	Stratégie globale de sécurisation et maitrise de l'internet des objets	**Modéré**		
					Stratégie globale de sécurisation et maitrise de l'internet des objets + surveillance passive	**Bas**	**Surveillance passive**	
					Stratégie globale de sécurisation et maitrise de l'internet des objets + surveillance passive + durcir la chaine ICS	**Très bas**	**Segmenter les réseaux essentiels**	
B- Conduite des systèmes industriels non critique	Sabotage	Perte de compétitivité de la compagnie		**Modéré**	Stratégie globale de sécurisation	**Bas**	**Hygiène OT de l'informatique**	
C- Conduite du navire ▪ ECDIS, DP, ▪ AIS, GPS, ▪ Radar, VDR	Usurpation du signal	- Dégradation de l'image de la compagnie - La perte du navire, - la perte de l'équipage, - l'atteinte à l'environnement.		**Fort**	La procédure de navigation doit intégrer la possibilité d'un acte de malveillance sur les outils de navigation.	**Modéré**	Recouper les éléments de navigation	
	Interférence volontaire du signal			**Fort**	La procédure de navigation doit intégrer la reprise en mode manuel	**Modéré**	Plan de continuité et surveillance de signaux faibles	
D- Gestion administrative du navire ▪ Bureautique ▪ Gestion	Sabotage	Perte de compétitivité de la compagnie		**Modéré**	Stratégie globale de sécurisation	**Très bas**	**Hygiène IT de l'informatique** - Evaluation, - politique, - contrôle accès …	

Nota : Risque = Vulnérabilité x (Impact x Menace) ;
Les vulnérabilités des opérations sont issues de l'étude DAM de septembre 2016 «*renforcer la cyber sécurité du navire* ».

E- ANNEXE N°3 – CONVERGENCE IT / OT AFIN DE DURCIR LA SURETE



E- ANNEXE N°4 – POUR ALLER PLUS LOIN

ANSSI :

Pour aller plus loin : www.ssi.gouv.fr

Guide ANSSI (Technique) :

- Maitriser la SSI des systèmes industriels – juin 2012,
- La cyber sécurité des systèmes industriels : mesures détaillées – janvier 2014,
- La cyber sécurité des systèmes industriels : méthode de classification et mesures principales – janvier 2014,
- Profil de protection d'un progiciel serveur applicatif SCADA - Version 1 du 01 juillet 2015,
- Profil de protection d'un automate programmable industriel - Version 1.1 du 13 juillet 2015,
- Profil d'un commutateur industriel - Version 1.1 du 13 juillet 2015,
- Profil d'un pare-feu industriel - Version 1.1 du 13 juillet 2015,
- Profil d'une passerelle VPN industrielle - Version 1.1 du 13 juillet 2015,
- Exigences de cyber sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels - Version 1 de mars 2016,

Guide ANSSI (Formation) :

- Guide pour une formation sur la cyber sécurité des systèmes industriels – février 2015,

Surveillance :

- Site du CERTA : http://www.certa.ssi.gouv.fr/
- Site US-CERT : https://www.us-cert.gov/

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER