



RAPPORTS

Direction générale des
infrastructures, des
transports et de la mer

Direction des services de
transport

Département
de la sûreté
dans les transports

2 juillet 2015

Guide méthodologique relatif aux plans de sûreté des installations portuaires à l'attention des instructeurs et des rédacteurs de plans.



Ministère de l'Écologie, du Développement durable et de l'Énergie

Ministère
de l'Écologie,
du Développement
durable
et de l'Énergie

www.developpement-durable.gouv.fr

Historique des versions du présent document

Version	Date	Commentaires
01	15 octobre 2014	version initiale
02	6 juillet 2015	Transposition des anciennes références du code des ports maritimes vers les nouvelles références au code des transports. Intégration de l'arrêté ZAR du 1 ^{er} avril 2015. Modifications ou compléments apportés au document. Voir le tableau d'enregistrement des modifications ou compléments en fin de document.

Affaire suivie par

Carole RIFOSTA - adjointe au chef de bureau DGITM/DST/DSûT1

Tél. : 01 40 81 72 51 / Fax : 01 40 81 73 49

Courriel : carole.rifosta@developpement-durable.gouv.fr

Rédacteurs

Alain Péral – Préfecture Loire-Atlantique / Cabinet

Jean-François Caret – Agence Surtymar / Organisme de sûreté habilité

Laurent Nourisson – Société Versalis France / Responsable Service Sécurité

Xavier Baude – auditeur national – DGITM/DST/DSûT1

Carole Rifosta – adjointe au chef de bureau – DGITM/DST/DSûT1

Relecteurs

Nicolas Meunier – Préfecture du Pas-de-Calais / Cabinet SIDPC

Jean-Philippe Dubois – Préfecture du Calvados / Cabinet SIDPC

Gilles Quedec – Société Elengy / Cadre sûreté – ASIP des terminaux méthaniers

Michael Roquain – Société Euroports / QHSE Manager et ASIP

Sylvie Couloigner – auditrice nationale – DGITM/DST/DSûT1

Erwan Delan – auditeur national – DGITM/DST/DSûT1

Des représentants du GISTMOP :

Barnabé Watin-Augouard – Chargé de mission / Premier ministre – Secrétariat général de la mer

Jean-Philippe Roux – Adjoint mer du Haut fonctionnaire de défense et de sécurité / SDSIE

Jérôme Vallet – Commissaire divisionnaire, Chef de la division sûreté / DCPAF

Remerciements

Ce guide a été réalisé à l'initiative et sous le pilotage du Ministère de l'Écologie, du Développement durable et de l'Énergie.

Le MEDDE tient à remercier les différents experts qui ont contribué à la validation, par leur apport et leur expérience aux différentes étapes de son élaboration.

Un remerciement est également adressé aux différents relecteurs qui ont porté une analyse critique et qui ont permis de tester l'utilisation du guide avant sa diffusion.

Table des matières

Préambule.....	8
I Introduction.....	8
II Objectifs.....	8
III Contexte.....	8
IV Présentation du guide.....	9
V Élaboration d'un PSIP.....	10
Chapitre 0 : Dispositions générales.....	10
Fiche 0.1 – Responsabilités de l'agent de sûreté de l'installation portuaire (et éventuellement de l'exploitant) lorsqu'il est amené à rédiger un PSIP.....	10
Chapitre 1 : Identification de l'installation portuaire.....	12
Fiche 1.1 – Identification de l'installation portuaire.....	12
Chapitre 2 : Éléments administratifs.....	14
Fiche 2.1 – Tableau d'enregistrement des modifications ou compléments au PSIP.....	14
Fiche 2.2 – Auteur du PSIP, dates des avis et approbations, fin de validité.....	14
Fiche 2.3 – Identification et coordonnées des personnes responsables en matière de sûreté.....	15
Fiche 2.4 – Liste de diffusion du plan de sûreté de l'installation portuaire.....	15
Chapitre 3 : Synthèse de l'évaluation de la sûreté de l'installation portuaire.....	17
Fiche 3.1 – Synthèse de l'évaluation de sûreté de l'installation portuaire (ESIP).....	17
Chapitre 4 : Organisation générale de la sûreté de l'installation portuaire.....	18
Fiche 4.1 – Plan détaillé de l'installation portuaire.....	18
Fiche 4.2. – Organisation de l'installation portuaire en matière de sûreté.....	19
Fiche 4.2.1 – Structure de l'organisation de la sûreté de l'installation portuaire. Organigrammes.....	19
Fiche 4.2.2 – Effectifs de l'exploitant de l'installation portuaire affectés à des tâches de sûreté par fonction, nature de tâches, et niveau de sûreté.....	20
Fiche 4.2.3 – Ressources dédiées à l'exercice de la sûreté.....	23
Fiche 4.2.4 – Modalités de coordination en matière de sûreté entre l'ASIP, l'ASP et d'autres autorités.....	24
Fiche 4.2.5 – Modalités de communication avec le navire des renseignements relatifs à la sûreté et d'exemption de leur fourniture par le navire pour les services réguliers.....	25
Fiche 4.2.6 – Description de la procédure interne de changement de niveau de sûreté après transmission de la consigne par l'autorité publique.....	27
Fiche 4.2.7 – Mesures additionnelles lors de l'escale d'un navire de croisière.....	28
Fiche 4.2.8 – Moyens et prestations assurés pour chaque niveau de sûreté	

applicable.....	29
Fiche 4.2.9 – Si l'installation portuaire est désignée point d'importance vitale.....	30
Fiche 4.3 – Coordination avec les installations portuaires adjacentes ou ayant un accès commun.....	31
Fiche 4.3.1 – Articulation du plan de sûreté de l'installation avec le ou les plans de sûreté d'installation portuaire adjacente.....	31
Fiche 4.3.2 – Pour les installations portuaires comprenant une ou des ZAR desservies depuis la terre par un accès commun.....	32
Fiche 4.4 – Articulation avec les autres plans et procédures.....	32
Fiche 4.4.1 – Articulation du PSIP avec d'autres plans ou activités de prévention et d'intervention.....	33
Fiche 4.4.2 – Indication des procédures et consignes applicables.....	34
Fiche 4.5 – Gestion documentaire et protection du plan de sûreté de l'installation portuaire.....	34
Chapitre 5 : Accès et circulation dans les installations portuaires.....	37
Préambule.....	37
Fiche 5.1 – Dispositions communes aux ZAR et aux ZNLA au public dans les IP désignées PIV.....	38
Fiche 5.2 – Identification et caractéristiques des zones d'accès restreint.....	38
Fiche 5.2.1 – Référence de l'arrêté préfectoral créant la ZAR.....	39
Fiche 5.2.2 – Plan faisant apparaître le système de clôture, l'emplacement des points d'inspection-filtrage, les éventuelles séparations de secteurs et les différents accès.....	39
Fiche 5.2.3 – Catégories de personnels et d'activités concernés.....	39
Fiche 5.2.4 – Flux d'entrée et nombre de titres de circulation.....	40
Fiche 5.2.5 – Schéma de circulation.....	40
Fiche 5.3 – Protection et contrôle des accès en zone d'accès restreint.....	40
Fiche 5.3.1 – Modalités d'activation de la ZAR et visites de sûreté.....	40
Fiche 5.3.2 – Caractéristiques des clôtures et de tout autre équipement de protection périmétrique.....	41
Fiche 5.3.3 – Caractéristiques des différents points d'accès.....	42
Fiche 5.3.4 – Système de signalisation des interdictions de pénétrer en ZAR.....	44
Fiche 5.3.5 – Règles de surveillance (humaines et/ou par système automatique de vidéo-surveillance), pour chaque niveau ISPS.....	45
Fiche 5.3.6 – Règles de fonctionnement des différents PIF.....	46
Fiche 5.3.7 – Règles de vérifications documentaires.....	49
Fiche 5.3.8 – Pour les voies ferrées portuaires.....	50
Fiche 5.3.9 – Pour les ZAR d'installation portuaire auxquelles une ou plusieurs ZAR portuaires donnent accès.....	50
Fiche 5.3.10 – Procédures d'entretien des clôtures, des équipements d'inspection-filtrage et de tout autre équipement périmétrique et de contrôle d'accès.....	51

Fiche 5.3.11 – Procédures appliquées en cas d'incident de sûreté (pénétration irrégulière, panne des équipements d'inspection-filtrage, détérioration de clôtures, etc.).....	52
Fiche 5.4 – Gestion des titres de circulation.....	53
Fiche 5.5 – Zones non librement accessibles.....	55
Préambule.....	56
Fiche 5.5.1 – Plan de masse.....	57
Fiche 5.5.2 – Procédure de vérification d'autorisation d'accès.....	57
Fiche 5.5.3 – Mesures combinées de surveillance et contrôle d'accès.....	58
Fiche 5.5.4 – Mesures pour la surveillance du plan d'eau.....	61
Fiche 5.5.5 – Mesures pour empêcher l'introduction d'articles prohibés.....	62
Fiche 5.5.6 – Procédure pour superviser la livraison de provisions de bord.....	63
Fiche 5.5.7 – Procédure pour superviser la manutention de la cargaison.....	63
Fiche 5.5.8 – Articulation avec les règles de sûreté des ZAR adjacentes.....	64
Chapitre 6 : Conduite à tenir en cas d'alerte, d'incident avéré et de sinistre.....	65
Fiche 6.1 – Conduite à tenir en cas d'alerte, d'incident avéré et de sinistre.....	65
Fiche 6.2 – Les systèmes d'alarme et d'alerte internes et externes.....	66
Fiche 6.3 – Mesures pour faire face à une menace imminente, une alerte ou une atteinte en cours contre la sûreté.....	67
Fiche 6.4 – Recherche, détection et localisation d'objets, véhicules ou individus. .	68
Fiche 6.5 – Exigences précises de notification obligatoire des incidents à l'ASIP /ASP.....	68
Fiche 6.6 – Mesures prévues pour accueillir un navire faisant l'objet d'une alerte de sûreté.....	69
Fiche 6.7 – Mesures prévues à la suite d'une alerte de sûreté sur un navire se trouvant dans l'installation portuaire.....	69
Fiche 6.8 – Dispositions permettant de maintenir les opérations portuaires essentielles, notamment dans le cas d'activités d'importance vitale.....	70
Fiche 6.9 – Coordination avec l'agent de sûreté portuaire.....	70
Fiche 6.10 – Fiches réflexes pour chaque type d'incident.....	70
Fiche 6.11 – Articulation ou aménagement Sûreté – Sécurité en cas de sinistre. .	70
Fiche 6.12 – IP désignée PIV.....	71
Chapitre 7 : Dispositions visant à réduire les vulnérabilités liées aux personnes.....	72
Fiche 7.1 – Dispositions visant à réduire les vulnérabilités liées aux personnes...	72
Chapitre 8 : Audits, contrôle interne, mise à jour du plan.....	74
Fiche 8.1 – Audits, contrôle interne, mise à jour du plan.....	74
Chapitre 9 : Formation, exercices et entraînements de sûreté.....	78
Fiche 9.1 – Formation, exercices et entraînements de sûreté.....	78

Chapitre 10 : Informations communicables aux personnes chargées d'effectuer les visites de sûreté.....	81
Fiche 10.1 – Informations communicables aux personnes chargées d'effectuer les visites de sûreté.....	81
Annexes.....	82
Annexe 1 – Tableau relatif à l'auteur du PSIP et aux dates d'approbations.....	82
Annexe 2 – Exemple de tableau de synthèse de l'évaluation de sûreté.....	83
Annexe 3 – Organigrammes.....	84
Annexe 4 – Effectifs de l'exploitant.....	85
Annexe 5 – Modalités de communication avec le navire.....	87
Annexe 6 – Gestion documentaire et protection du plan de sûreté de l'installation portuaire.....	88
Annexe 7 – Identification et caractéristiques des zones d'accès restreint.....	89
Annexe 8 – Règles de surveillance en ZAR.....	91
Annexe 9 – Exemple de schémas type de transmission d'alerte.....	92
Annexe 10 – Exemple de formulaire d'incident de sûreté.....	94
Annexe 11 – Exemples de fiches réflexes.....	95
Annexe 12 – Exemples pour les entraînements et les exercices.....	102
Tableau d'enregistrement des modifications ou compléments apportés au document	105
Sigles et abréviations.....	106
Liste des textes réglementaires.....	110

Préambule

I Introduction

La réunion du groupe Interministériel de sûreté du transport maritime et des opérations portuaires (GISTMOP) en date du 6 juin 2013 a proposé des actions en réponse au rapport de l'inspection générale de l'administration (IGA).

Plutôt que de donner un avis sur la totalité des plans de sûreté des installations portuaires, il a été retenu de rédiger un guide méthodologique. Ce guide relatif aux plans de sûreté des installations portuaires est établi à l'attention d'une part, des rédacteurs de plans et d'autre part, des personnes chargées d'instruire les projets de plans qui leur sont présentés.

II Objectifs

Les principaux objectifs du présent document sont les suivants :

- apporter une aide aux rédacteurs de plans de sûreté afin de faciliter l'approbation. Il s'agit de lister les points de vigilance à respecter dans le cadre de l'élaboration des plans de sûreté ;
- apporter une aide aux instructeurs de plans de sûreté afin d'améliorer l'avis que ceux-ci auront à formuler lors du passage du dossier en comité local de sûreté portuaire (CLSP). Il s'agit, là aussi, de lister les points de vigilance à respecter dans le cadre de l'examen des plans de sûreté.

III Contexte

La sûreté portuaire fait l'objet d'un corpus juridique complet. Les principaux textes relatifs aux plans de sûreté sont rappelés en annexe (« Liste des textes réglementaires »). Cette réglementation s'est progressivement mise en place depuis 2004. La plupart des installations portuaires (IP) ont fait l'objet de deux (voire trois) plans successifs.

Une révision partielle de la réglementation est envisagée. Cette révision propose, notamment, de distinguer les installations portuaires à enjeux forts, moyens ou faibles. Lorsque ces évolutions réglementaires paraîtront, le présent guide méthodologique sera actualisé.

En attendant la révision partielle des textes, la version n° 2 du guide méthodologique relatif aux PSIP propose d'intégrer la nouvelle codification du code des transports paru le 30 décembre 2014, les modifications apportées à l'arrêté ZAR du 4 juin 2008 suite à la parution de l'arrêté du 1^{er} avril 2015, ainsi que des modifications ou des compléments apportés ponctuellement au document. À la fin du guide, un tableau d'enregistrement permet de comparer les dispositions apportées avant et après modifications.

L'élaboration du plan de sûreté est à la charge de l'exploitant. Le guide doit permettre à l'exploitant de répondre aux attentes des services de l'État, y compris les mesures de sûreté approuvées par le représentant de l'État lors de l'évaluation de sûreté de l'installation portuaire.

L'approbation du plan de sûreté reste de la responsabilité du représentant local de l'État (le préfet). Cette approbation a lieu après avis du CLSP. Le guide doit être une aide pour les membres du CLSP dans leur mission.

La fonction du plan de sûreté est un engagement de l'exploitant sur des mesures visibles, crédibles et efficaces pour protéger l'interface portuaire.

IV Présentation du guide

Le plan du présent document reprend le cadre proposé par l'arrêté du 22 avril 2008. Il est composé des 10 parties suivantes :

1. Identification de l'installation portuaire ;
2. Éléments administratifs ;
3. Synthèse de l'évaluation de la sûreté de l'installation portuaire ;
4. Organisation générale de la sûreté de l'installation portuaire ;
5. Accès et circulation dans les zones d'accès restreint de l'installation portuaire ;
6. Conduite à tenir en cas d'alerte de sûreté, d'incident avéré et de sinistre ;
7. Dispositions visant à réduire les vulnérabilités liées aux personnes ;
8. Audits et contrôle interne, mise à jour du plan ;
9. Formation, exercices et entraînements de sûreté ;
10. Informations communicables aux personnes chargées d'effectuer les visites de sûreté.

Pour chacune de ces parties, il sera développé des thématiques sous forme de fiches constituées des éléments suivants :

- L'intitulé de la fiche : correspondant à l'intitulé de l'arrêté du 22 avril 2008 ;
- Le cadre réglementaire qui précise les principales références réglementaires correspondant à l'intitulé de la fiche ;
- Les objectifs (les enjeux de la réglementation) qui visent à clarifier les attendus réglementaires lorsque les intitulés des fiches nécessitent un décryptage. Les objectifs sont parfois découpés en 3 sous parties :
 - Principe général, soit les attendus réglementaires ;
 - Principe particulier pour les instructeurs, soit les points de vigilance pour les membres de CLSP qui donnent un avis sur le plan de sûreté de l'installation portuaire (PSIP) ;
 - Principe particulier pour les exploitants, soit les points de vigilance pour les rédacteurs du PSIP ;
- Les conseils complémentaires qui ont pour objectif d'illustrer les déclinaisons possibles des objectifs réglementaires et de donner des conseils pratiques aux instructeurs et aux rédacteurs de plans. Ce point est découpé en 3 sous-parties :
 - Conseils complémentaires d'ordre général ;
 - Conseils complémentaires pour les instructeurs ;
 - Conseils complémentaires pour les exploitants.

Bien que la rédaction du guide s'appuie sur la trame de l'arrêté du 22 avril 2008, chaque instructeur ou rédacteur de PSIP doit prendre connaissance des sections A et B du Code International pour la Sûreté des Navires et des Installations Portuaires (Code ISPS) rendues obligatoires par le Règlement européen (CE) N° 725 / 2004, à savoir :

- section A/14 relative à « la sûreté de l'installation portuaire » ;
- section A/16 relative « au plan de sûreté de l'installation portuaire » ;
- section A/17 relative à « l'agent de sûreté de l'installation portuaire » ;
- section A/18 relative à la « formation, exercices et entraînements en matière de sûreté des installations portuaires » ;
- sections B/16.3 et B/16.8 relatives aux « standards minimums concernant le plan de sûreté de l'installation portuaire » ;
- sections B/18.5 et 18.6 relatives aux « exercices et entraînements ».

V Élaboration d'un PSIP

Chapitre 0 : Dispositions générales

Fiche 0.1 – Responsabilités de l'agent de sûreté de l'installation portuaire (et éventuellement de l'exploitant) lorsqu'il est amené à rédiger un PSIP

Cette fiche ne doit pas être reproduite dans un plan de sûreté. Elle a pour but de rappeler les responsabilités de l'agent de sûreté de l'installation portuaire (ASIP) lors de la rédaction du PSIP ; même si ses responsabilités ne se limitent pas à la rédaction du plan.

Le cadre réglementaire :

*Code ISPS annexé au Règlement (CE) N° 725/2004 du parlement et du conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires
Section A/17 agent de sûreté de l'installation portuaire*

*Code des transports, Titre III Police des ports maritimes, Chapitre II Sûreté portuaire
Sous-section 3 : Évaluations de la sûreté et plans de sûreté des installations portuaires
articles R.5332-27, R.5332-29, R.5332-32*

Les objectifs :

Principe général :

La section A/17.2 du Code ISPS annexée au Règlement européen (CE) N° 725/2004 définit les responsabilités d'un agent de sûreté de l'installation portuaire (ASIP) en 13 points parmi lesquels :

- « veiller à l'élaboration et à la mise à jour du PSIP ;
- mettre en œuvre le PSIP et procéder à des exercices à cet effet ;
- accroître la prise de conscience de la sûreté et la vigilance du personnel de l'installation portuaire... ».

Le Code des transports prévoit que :

- l'exploitant prend les mesures de sûreté nécessaires à son installation, en particulier, celles relatives aux ZAR ;
- l'exploitant établit le plan de sûreté de l'installation portuaire suivant les modalités de l'arrêté du 22 avril 2008 ;
- l'exploitant désigne l'ASIP chargé de la préparation et de la mise en œuvre du plan de sûreté.

L'exploitant donne à l'ASIP les moyens nécessaires pour qu'il puisse s'acquitter de ses tâches et responsabilités. L'exploitant et l'ASIP sont respectivement responsables en tant que personne morale et personne physique et sont passibles de sanctions administratives en cas de manquement aux dispositions du chapitre VI sanctions administratives et dispositions pénales du code des transports.

Les conseils complémentaires :

Conseils complémentaires pour les instructeurs :

Au démarrage de l'élaboration du plan, les instructeurs doivent contrôler que les ASIP(s) ont un agrément délivré par le représentant de l'État. Lorsque l'exploitant fait appel à un organisme de sûreté habilité (OSH), les instructeurs doivent vérifier la validité de l'habilitation de l'OSH ainsi que les agréments individuels des représentants de l'OSH chargés de rédiger le PSIP.

Si l'installation est classée point d'importance vitale (PIV), le rédacteur, les responsables de la sûreté de l'IP (ASIP et suppléants) et les destinataires du PSIP doivent être habilités Confidentiel Défense.

La désignation de l'ASIP nécessite un certificat d'aptitude (stage ASIP) défini selon les modalités de l'arrêté du 17 juin 2004. Les instructeurs doivent contrôler que les ASIP(s) en place ont suivi cette formation (existence de certificat...).

La désignation de l'ASIP est subordonnée à la possession d'un agrément et du certificat d'aptitude au stage ASIP. Cependant la demande d'agrément d'ASIP et le certificat d'aptitude au stage ASIP sont deux conditions indépendantes. Un ASIP peut demander un agrément et suivre a posteriori le stage ASIP.

Conseils complémentaires pour les exploitants :

L'exploitant est responsable de son plan. Pour établir ce plan, il peut solliciter l'appui d'un OSH qui travaillera en étroite collaboration avec l'ASIP.

Avant l'approbation du plan et pour démontrer son implication dans le processus, l'ASIP présentera lui-même, aux services de l'État (comité local de sûreté portuaire : CLSP), son plan. Même si la rédaction de celui-ci a été sous-traitée à un OSH, l'exploitant demeure responsable de la bonne exécution des mesures du PSIP.

L'exploitant peut désigner un ou plusieurs suppléants afin d'assurer la permanence de la fonction. L'ASIP et ses suppléants ont exactement le même niveau de responsabilité.

Chapitre 1 : Identification de l'installation portuaire

Fiche 1.1 – Identification de l'installation portuaire

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

« 1. Identification de l'installation portuaire (à placer en page de couverture) »

Les objectifs :

Principe général :

L'arrêté demande de préciser a minima :

- le numéro national attribué à l'installation portuaire ;
- l'identifiant international de la base de données Global Integrated Shipping Information System (GISIS).

Si l'installation est également désignée PIV, reprendre le cadre de l'arrêté du 22 avril 2008.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Le numéro national est attribué par le représentant local de l'État français à partir du principe établi dans les circulaires du représentant central de l'État français (voir annexe « liste des textes réglementaires »). Le numéro national peut être affecté préalablement à la création du numéro international.

L'identifiant international de la base de donnée GISIS est attribué par l'organisation maritime internationale (OMI). Ce numéro comprend d'une part, des lettres précisant le nom du port auquel l'installation portuaire est rattachée et d'autre part, un numéro. L'ensemble du numéro international figure sur le site internet de l'OMI : <http://gisis.imo.org/Public/> rubrique "Port Reception Facilities".

Pour créer le numéro international « GISIS », deux conditions doivent être réunies :

- avoir un PSIP approuvé ;
- avoir un arrêté d'identification de l'installation portuaire.

Lorsqu'une installation portuaire est déclassée, le numéro international GISIS devient obsolète. Si jamais l'installation portuaire est réactivée, il convient de s'adresser au Ministère de l'Écologie, du Développement durable et de l'Énergie (MEDDE) pour savoir si le numéro international initialement affecté reste valide.

Conseils complémentaires pour les instructeurs :

Le numéro national peut changer en cas de regroupement (voire fusion) ou scission d'installations portuaires. Le cas échéant, il convient d'attribuer un nouveau numéro pour éviter toute confusion.

Conseils complémentaires pour les exploitants :

Le nom de l'installation portuaire figurant sur le PSIP doit être identique au nom défini dans l'arrêté préfectoral de désignation de l'installation.

Pour mieux identifier l'installation portuaire, l'exploitant pourrait sommairement décrire l'activité du terminal avec quelques données statistiques sur le nombre d'escales soumis au code ISPS selon la nature de l'activité :

Nombre annuel d'escales de navires visés par la convention Solas, par type d'activité		
Type d'activités	Année N	Année N+1
- Matières dangereuses - RoPax - Croisières - Conteneurs - Ferries - Vrac solides, vrac liquides		

Même si l'IP n'est pas désignée PIV, le PSIP pourrait préciser :

- les coordonnées et la situation géographique du site ;
- l'adresse de l'installation portuaire ;
- le nom et la raison sociale de l'exploitant.

Chapitre 2 : Éléments administratifs

Fiche 2.1 – Tableau d'enregistrement des modifications ou compléments au PSIP

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

2. Éléments administratifs

2.1. Tableau d'enregistrement des modifications ou compléments au plan de sûreté de l'installation portuaire (nom, numéro) située dans le port de xx apportés par l'agent de sûreté de l'installation portuaire et approuvés par le préfet

Les objectifs :

Principe général :

Ce chapitre propose un tableau d'enregistrement des modifications ou compléments au PSIP. Hormis la date de modification, le tableau contient la nature des modifications, les visas et les décisions préfectorales.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Le PSIP doit a minima faire l'objet d'une révision annuelle (en particulier, suite aux audits internes). Il est fortement recommandé que les modifications fassent l'objet d'une présentation par l'ASIP et/ou l'ASP au représentant de l'État une fois par an pour validation. Ces modifications devront être clairement identifiables et repérables dans le document par un surlignage ou un autre dispositif.

Fiche 2.2 – Auteur du PSIP, dates des avis et approbations, fin de validité

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

2. Éléments administratifs

2.2. Auteur du plan, dates des avis et approbations, fin de validité (...)

Les objectifs :

Principe général :

Ce chapitre fait l'inventaire des informations utiles au plan. Ces informations sont les auteurs du plan, les dates des avis du CLSP, les dates approbation ESIP et PSIP, le n° ZAR et la copie de l'arrêté créant la ZAR.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Afin d'uniformiser l'intégralité du chapitre 2 et d'en faciliter la « lecture », il est conseillé de présenter le point 2.2 sous forme de tableau. À ce titre, un document est proposé en annexe n° 1.

Attention, la durée maximale de validité de l'ESIP est de 5 ans. Quant à la durée de validité du PSIP, elle est bornée par la date de fin de validité de l'ESIP. Le PSIP doit être modifié en parallèle à chaque révision de l'ESIP. Le PSIP doit mentionner les conséquences de chaque modification à l'ESIP (modification au PSIP ou non).

Fiche 2.3 – Identification et coordonnées des personnes responsables en matière de sûreté

Le cadre réglementaire :

*Arrêté du 22 avril 2008,
Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)
2. Éléments administratifs
2.3. Identification et coordonnées des personnes responsables en matière de sûreté.*

Les objectifs :

Ce chapitre fait l'inventaire des responsables de la sûreté pour l'installation portuaire.

Pas de recommandation particulière ; reprendre le cadre de l'arrêté.

Fiche 2.4 – Liste de diffusion du plan de sûreté de l'installation portuaire

Le cadre réglementaire :

*Arrêté du 22 avril 2008,
Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)
2.4. Liste de diffusion du plan de sûreté de l'installation portuaire
2.4.1. Volume 1 – Confidentiel Sûreté (Ce volume comprend le plan de sûreté de l'installation portuaire dans son entier)
2.4.2. Volume 2 – Distribution Limitée Sûreté : ce volume ne reprend que les informations, listées au point 10 du plan de sûreté de l'installation portuaire, communicables aux personnes chargées d'effectuer les visites de sûreté...*

Les objectifs :

Principe général :

L'objectif est de proposer un cadre pour la liste de diffusion du plan (volumes 1 et 2).

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

La diffusion du volume 1 doit être restreinte aux personnes habilitées « Confidentiel Sûreté » et qui utiliseront le plan de sûreté :

- la préfecture ;
- l'autorité portuaire ;
- l'exploitant ;
- le ministère de l'écologie, du développement durable et de l'énergie (MEDDE).

S'agissant de données protégées et non classifiées, il n'existe pas d'habilitation « Confidentiel Sûreté » (voir fiche 4.5). Cette protection est de niveau « Diffusion Restreinte » qui vise une diffusion auprès des personnes ayant à en connaître. Ainsi, chaque service assurera les copies qu'il juge nécessaires. Les destinataires du plan devraient signer une reconnaissance de responsabilité comme recommandé dans la fiche 4.5. Cependant pour garantir la maîtrise documentaire du PSIP et de ses mises à jour, le nombre de destinataires du PSIP devrait être limité au strict minimum (préfecture, autorité portuaire, exploitant, MEDDE).

Le volume 2 fait partie intégrante du volume 1 et il doit être diffusé aux services comme indiqué au paragraphe précédent.

Les informations du volume 2 comprennent essentiellement les consignes de sûreté pour le personnel, les fiches réflexes et les conduites à tenir en cas d'alerte. C'est pourquoi le volume 2 a surtout vocation à être diffusé auprès du personnel qui doit appliquer les consignes de sûreté sur le terrain.

Parmi les destinataires possibles du volume 2, peuvent être concernés :

- les ASIP ;
- le personnel ayant des tâches de sûreté (les gardiens, les agents chargés des visites de sûreté (ACVS)...)¹ ;
- pour partie, la personne qui reçoit les appels de l'extérieur et qui pourrait être amenée à appliquer la fiche réflexe « appel menaçant ».

Pour un PIV, afin de faciliter la diffusion du plan et son accès au personnel, la partie concernant le plan particulier de protection (PPP) peut être intégrée dans une annexe « rédaction réservée » classifiée Confidentiel Défense (CD) et uniquement accessible aux personnes « ayant besoin d'en connaître » et habilitées CD.

1 Voir au chapitre « sigles et abréviations » la définition du terme ACVS et le sens du terme gardien.

Chapitre 3 : Synthèse de l'évaluation de la sûreté de l'installation portuaire

Fiche 3.1 – Synthèse de l'évaluation de sûreté de l'installation portuaire (ESIP)

Le cadre réglementaire :

Règlement (CE) N° 725/2004, articles 3-3 à 3-6.

Code des transports, article R. 5332-28

Arrêté du 22 avril 2008,

Annexe 2 – Plan type de l'évaluation de sûreté de l'installation portuaire (ESIP)

Chapitre 8 – Propositions de mesures susceptibles de contrer les risques et maintien de l'efficacité de cette mesure

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

Chapitre 3 – Synthèse de l'évaluation de la sûreté de l'installation portuaire

Les objectifs :

Principe général :

Reproduire le chapitre 8 de l'ESIP tel qu'approuvé par arrêté préfectoral.

Principe particulier pour les instructeurs :

S'assurer de la prise en compte pleine et entière de la totalité des mesures.

Si le PSIP n'apporte pas de réponse immédiate à chaque mesure de l'ESIP, un échéancier devra être annexé au PSIP.

Principe particulier pour les exploitants :

Reprendre dans le chapitre 3 du PSIP sous forme de tableau, dans l'ordre des priorités fixées, l'ensemble des mesures figurant au chapitre 8 de l'ESIP approuvée par arrêté préfectoral sans y apporter quelque modification que ce soit.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Un exemple de rendu est fourni en annexe n° 2. Réserver la dernière colonne du tableau à la suite donnée à la mesure dans le PSIP.

Conseil complémentaire pour les exploitants :

L'exploitant doit vérifier la cohérence entre les mesures de l'ESIP – les mesures du PSIP et leurs mises en œuvre respectives. L'exploitant doit être en capacité d'apporter une réponse cohérente dans son PSIP pour chaque mesure de l'ESIP. La réponse apportée dans le PSIP doit être adaptée, pertinente et pouvoir être mise en œuvre.

Chapitre 4 : Organisation générale de la sûreté de l'installation portuaire

Fiche 4.1 – Plan détaillé de l'installation portuaire

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.1. Plan détaillé de l'installation portuaire

Reprendre ici le plan figurant dans l'évaluation de sûreté de l'installation portuaire en y ajoutant les protections mises en œuvre dans le cadre du plan de sûreté de l'installation portuaire.

Les objectifs :

Principe général :

Reprendre sur un plan de masse le périmètre de l'installation portuaire utilisé dans l'ESIP, afin d'y localiser les dispositifs de protection utilisés sur le terminal.

Principe particulier pour les instructeurs :

Vérifier que les périmètres utilisés dans l'ESIP puis dans le PSIP sont identiques à celui de l'arrêté qui désigne l'exploitant, le périmètre et les caractéristiques de l'installation portuaire.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Sur le plan de masse du terminal figurent les informations suivantes :

- les contours du périmètre de l'installation portuaire approuvé par arrêté ;
- le périmètre des clôtures (éventuellement contour IP = contour clôture) ;
- l'amarrage ;
- une légende.

Les dispositifs de protection incluent le cas échéant :

- l'emplacement des portails d'accès ;
- l'emplacement de l'éclairage ;
- les barrières de protection (barrières mobiles...) ;
- les dispositifs de protection périmétrique (infra-rouge...) ;
- l'emplacement de la vidéo-surveillance (avec les angles de vue des caméras) ;
- les postes de contrôle (pour les IP non ZAR) ou points d'inspection filtrage (pour les IP ZAR)...

Conseils complémentaires pour les exploitants :

L'exploitant peut annexer tous plans de masse qui localiseraient les dispositifs de protection.

L'exploitant peut représenter de manière schématique ses moyens de protection.

Les dispositifs de protection sont également renseignés dans le chapitre 5 « Accès et circulation dans l'installation portuaire » au paragraphe 5.3 relatif aux ZAR. Il doit donc y avoir une cohérence entre les deux chapitres.

Fiche 4.2. – Organisation de l'installation portuaire en matière de sûreté

Le paragraphe 4.2 visant à décrire l'organisation de la sûreté d'une installation portuaire, telle que définie dans l'annexe 4 de l'arrêté du 22 avril 2008, prévoit plusieurs sous-parties, lesquelles seront détaillées dans les fiches 4.2.1 à 4.2.9.

Fiche 4.2.1 – Structure de l'organisation de la sûreté de l'installation portuaire. Organigrammes

Le cadre réglementaire :

Code ISPS annexé au Règlement (CE) N° 725/2004 du Parlement et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires

Section B/16.3.1 décrire dans le détail l'organisation de la sûreté de l'installation portuaire

Section B/16.8.1 le rôle et la structure de l'organisation de la sûreté de l'installation portuaire

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

Structure de l'organisation de la sûreté de l'installation portuaire. Organigrammes.

Les objectifs :

Principe général :

Le but est de créer un organigramme décrivant l'ensemble des moyens humains alloués par la Direction de l'exploitant et de préciser si le ou les ASIP ont un rôle hiérarchique vis-à-vis du personnel ayant des tâches de sûreté (en interne à l'exploitant et/ou sous-traitées à un tiers). L'organigramme précisera a minima les liens hiérarchiques entre :

- la direction de l'exploitant ;
- les ASIP (et les éventuelles sous-directions dont dépendent les ASIP) ;
- le personnel ayant des tâches de sûreté (y compris la sous-traitance).

Principe particulier pour les instructeurs :

Les structures figurant sur l'organigramme devront être mises en cohérence avec d'autres paragraphes du PSIP, en particulier ceux visant à décrire les prestations, les effectifs et les moyens sous-traités.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

À ce stade, il n'est pas utile de préciser les liens entre l'organisation de l'entreprise et les services de l'État. Cet aspect est à développer dans un autre point de l'arrêté du 22 avril 2008 (coordination avec les services de l'État). Éventuellement, un organigramme qui présenterait de tels liens, peut figurer en annexe du PSIP.

Conseils complémentaires pour les exploitants :

L'organigramme doit être diffusé en interne dans l'entreprise afin que le personnel puisse identifier les ASIP au besoin.

Si l'organigramme change fréquemment, il peut être annexé au PSIP.

Éviter de mettre des noms propres ou des noms d'entreprises sous-traitantes au cas où ceux-ci changent fréquemment.

Des exemples sont proposés en annexe n° 3.

Fiche 4.2.2 – Effectifs de l'exploitant de l'installation portuaire affectés à des tâches de sûreté par fonction, nature de tâches, et niveau de sûreté...

Le cadre réglementaire :

Code ISPS annexé au Règlement (CE) N° 725/2004 du parlement et du conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires

Section A/16.3.6, les tâches du personnel de l'installation auquel sont attribuées des responsabilités en matière de sûreté et celles des autres membres du personnel de l'installation portuaire concernant les aspects liés à la sûreté

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

Effectifs de l'exploitant de l'installation portuaire affectés à des tâches de sûreté par fonction, nature de tâches, et niveau de sûreté ; modalités d'astreinte et de permanence ; équipes de protection et de gardiennage : personnel (effectif, provenance, formation), organisation, postes tenus, rondes, moyens complémentaires ;

Les objectifs :

Principe général :

Décrire l'ensemble des effectifs affectés à des tâches de sûreté. Cette description doit permettre de :

- comptabiliser l'ensemble des effectifs ayant des tâches de sûreté (y compris la sous-traitance) ;
- comprendre la fonction de chacun ;
- préciser la nature de tâches de chacun ;
- décliner des effectifs par niveaux ISPS ;
- décrire les modalités d'astreinte (au sens joignable ou contact permanent).

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Ci-dessous est proposé un modèle de présentation pour décrire les effectifs ; ainsi qu'un exemple détaillé en annexe 4.

Provenance du personnel	Fonction	Effectifs			Nature de tâches			Contact permanent
		Niveau 1 ISPS	Niveau 2 ISPS	Niveau 3 ISPS	Niveau 1 ISPS	Niveau 2 ISPS	Niveau 3 ISPS	
Personnel de l'exploitant	ASIP							
Personnel de l'exploitant	ASIP suppléant							
Personnel de l'exploitant	Autre							
Personnel sous-traitant	Autre							

Dans la colonne « Provenance du personnel », on peut lister les entreprises pour lesquelles travaille le personnel, à savoir l'exploitant et/ou des entreprises sous-traitantes.

Dans la colonne « Fonction », on cherchera à préciser les fonctions exercées par chaque catégorie de personnel, comme :

- ASIP ;
- ASIP suppléant ;
- Gardien (n'ayant pas le statut d'ACVS) ;
- ACVS ;
- Responsable qualité ;
- Contremaître...

Dans les colonnes déclinier les effectifs et les tâches par niveaux ISPS :

La section A/4.1 du Code ISPS annexée au Règlement CE N° 725/2004 demande de déclinier les mesures de sûreté selon 3 niveaux :

- Niveau 1 : mesures minimales appropriées appliquées en permanence ;
- Niveau 2 : mesures additionnelles appropriées à maintenir pendant une période déterminée, car le risque est accru ;
- Niveau 3 : mesures spéciales et temporaires, car l'incident est probable ou imminent.

Au niveau 1, ce sont les mesures minimales appropriées du PSIP. Ensuite, avec l'élévation du niveau ISPS, caractérisant une situation d'urgence, l'exploitant doit préciser s'il convient d'intensifier les effectifs et/ou les tâches de sûreté.

Ainsi, les mesures de sûreté à mettre en œuvre pour le niveau 1 ISPS doivent être appréciées au regard des mesures de sûreté qu'on est réellement capable de déployer en cas de passage aux niveaux 2 et 3 ISPS. Au niveau 1, l'exploitant mettra en œuvre des mesures minimales ; ensuite les mesures sont renforcées aux niveaux 2 et 3 ISPS.

Pour la colonne « Effectifs », on recensera et dénumbrera le personnel ayant des tâches de sûreté. On précisera si les effectifs sont renforcés pour faire face à une situation de crise (niveau 2 ISPS : risque accru ; niveau 3 ISPS : incident probable).

Pour la colonne « Nature de tâches », on cherchera à comprendre les missions de sûreté exactement confiées à chaque personne. Éventuellement, les tâches peuvent être intensifiées avec l'élévation du niveau ISPS. Parmi les exemples de tâches pouvant être exercées, on peut avoir :

- Rondier (ronde de jour, de nuit, dans le but de rechercher des colis suspects, de rechercher des intrusions, d'effectuer un rapprochement d'identité...)
- Réception des provisions de bord, des colis ;
- Inspection-filtrage (pour les ACVS et les IP soumises à ZAR) ou gardiennage (pour le personnel d'IP non soumises à ZAR et n'ayant pas le statut d'ACVS) ;
- Délivrance de badges, de titres de circulation ;
- Audit interne ;
- Gestion documentaire du PSIP ;
- Contrôle du matériel de protection (contrôle de l'état des clôtures, des radios, des portails d'accès, de la vidéosurveillance...)

Les natures de tâches peuvent également être décrites dans une fiche de poste qui sera annexée au PSIP.

Pour la dernière colonne « Contact permanent », on précisera :

- si l'ASIP est joignable 24 heures sur 24 et s'il est susceptible de rallier l'installation portuaire dans un délai raisonnable (ralliement immédiat, dans l'heure qui suit, sous 2H...)
- si le personnel affecté à des tâches de sûreté est présent pendant toute la durée de l'escale (y compris les temps d'attente à quai).

Conseils complémentaires pour les instructeurs :

Veiller à ce que le personnel ayant des tâches de sûreté soit présent pendant toute la durée de l'escale.

S'assurer que le PSIP prévoit un renfort du personnel et/ou des tâches de sûreté en cas d'élévation du niveau ISPS.

Conseils complémentaires pour les exploitants :

Veiller à la cohérence des informations entre l'organigramme et les effectifs.

Si une partie du personnel est externalisée (sous-traitée), alors il faudra prévoir un cahier des charges mentionnant les effectifs du sous-traitant par fonction, nature de tâches, niveaux ISPS, modalités d'astreintes. En cas de renforcement des effectifs avec l'élévation du niveau ISPS, le cahier des charges précisera un délai de ralliement pour le déploiement de ces effectifs. Le cahier des charges devra être cohérent avec le PSIP auquel il sera annexé.

Fiche 4.2.3 – Ressources dédiées à l'exercice de la sûreté

Le cadre réglementaire :

Section B/16.8.4 du Code ISPS annexé au RE N° 725/2004 « les systèmes de communications prévus pour assurer une communication efficace et continue entre le personnel de l'installation portuaire responsable de la sûreté, les navires se trouvant au port et, lorsqu'il y a lieu, les autorités nationales ou locales ayant des responsabilités en matière de sûreté »

En complément, on peut citer les responsabilités de l'ASIP prévu par le Code ISPS annexé au RE N° 725/2004, section A/14.2.7 « veiller à ce que le système de communication soit rapidement disponible »

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

« 4.2. Organisation de l'installation portuaire en matière de sûreté

Ressources dédiées à l'exercice de la sûreté : locaux (contenu, équipement, protection), moyens de transmission (caractéristiques selon les correspondants internes ou externes) »

Les objectifs :

Principe général :

Les ressources dédiées à l'exercice de la sûreté doivent décrire les locaux et les moyens de transmission dédiés à l'exercice de sûreté.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Les locaux peuvent inclure :

- une cellule de crise (en cas d'alerte ou d'incident, l'exploitant a-t-il une salle où il pourra communiquer voire accueillir des services de l'État, le personnel du navire...);
- le bureau dédié à la sûreté (bureau de l'ASIP où le PSIP est stocké) ;
- le poste de garde ;
- le point d'inspection filtrage (pour les installations portuaires soumises à ZAR uniquement).

Parmi les moyens de transmission internes peuvent figurer :

- les téléphones fixes, mobiles ;
- les postes UHF ;
- la messagerie électronique ;
- les moyens de transmission externes ;
- la VHF pour les liaisons navires / capitainerie.

Conseils complémentaires pour les exploitants :

Il faut uniquement citer les ressources dont on dispose ;

Les ressources doivent être redondantes. L'exploitant devrait avoir au moins deux sources distinctes de communication si l'une des deux ne fonctionne pas ;

Doivent figurer dans le PSIP principalement le matériel et les locaux permettant de donner ou de gérer une situation d'alerte. Il est donc important de se limiter à un matériel qui permet d'entrer rapidement en communication avec un tiers (en interne ou en externe) ;

Par ailleurs, l'ASIP doit veiller au bon fonctionnement du matériel de sûreté et il doit prévoir des procédures d'entretien et de contrôles périodiques (voir procédure prévue dans le chapitre 8 de l'arrêté du 22 avril 2008).

Fiche 4.2.4 – Modalités de coordination en matière de sûreté entre l'ASIP, l'ASP et d'autres autorités

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004 ; section B/16.8.3 les liens de l'organisation de la sûreté de l'installation portuaire avec d'autres autorités nationales ou locales ayant des responsabilités en matière de sûreté

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

Modalités de coordination en matière de sûreté entre l'agent de sûreté de l'installation portuaire, l'agent de sûreté portuaire et d'autres autorités : services de l'État (spécifier, après leur accord, les tâches effectuées dans l'installation portuaire par ces services), autorité portuaire, autorité investie du pouvoir de police portuaire ;

Les objectifs :

Principe général :

La description des modalités de coordination entre l'ASIP, l'ASP et les services de l'État doit expliquer les rôles et les missions de l'ASP et des services de l'État en matière de sûreté. Il faut préciser si les missions de chacun présentent un intérêt réel en matière de coordination avec l'ASIP.

Principe particulier pour les instructeurs :

Consulter les services de l'État pour valider les procédures de coordination définies par l'ASIP.

Lorsque les moyens humains et matériels déployés par une Autorité portuaire ou un service de l'État viennent compléter et appuyer les missions de l'exploitant au quotidien, alors la rédaction d'une convention est recommandée pour clarifier la répartition des tâches. Par exemple, la douane met à la disposition de l'exploitant des équipements d'imagerie radioscopique.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Dans l'ensemble, on se limitera à identifier les services de l'État ayant un rôle direct à l'égard de l'installation portuaire (douane, commissariat de sécurité publique, police aux frontières, gendarmerie maritime, là où ces services sont implantés, membres du CLSP...). Parfois les missions des services de l'État sont très précises, notamment ceux qui exercent des missions de contrôle à l'intérieur du terminal.

Conseils complémentaires pour les instructeurs :

Décrire les modalités de coordination uniquement sur la base d'un schéma d'alerte est trop réducteur. Un tel schéma devrait figurer dans le chapitre 6 « Conduite à tenir en cas d'alerte ».

Conseils complémentaires pour les exploitants :

Comme l'exploitant n'a pas de pouvoir hiérarchique sur les services de l'État, l'ASIP rappellera uniquement les principales missions de ces services et dans quelles situations il est susceptible de faire appel à ces services.

Si l'implication des services de l'État ou de l'Autorité portuaire est très imbriquée dans la sûreté de l'exploitant, la rédaction d'une convention est sans doute nécessaire.

L'ASIP doit pouvoir bénéficier de l'appui de l'ASP et des services de l'État pour rédiger cette procédure relative aux modalités de coordination.

Fiche 4.2.5 – Modalités de communication avec le navire des renseignements relatifs à la sûreté et d'exemption de leur fourniture par le navire pour les services réguliers

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

-Modalités de communication avec le navire des renseignements relatifs à la sûreté et d'exemption de leur fourniture par le navire pour les services réguliers

Les objectifs :

Principe général :

Les renseignements préalables à l'entrée du navire dans un port ou une installation portuaire précisent le niveau ISPS du navire lors de ses dix dernières escales. Ils doivent être fournis :

- au moins vingt-quatre heures à l'avance, ou
- au plus tard au moment où le navire quitte le port précédent si la durée du voyage est inférieure à vingt-quatre heures, ou
- si le port d'escale n'est pas connu ou s'il est modifié durant le voyage, dès que le port d'escale devient connu.

L'exemption de la fourniture de renseignements préalables est prévue par l'article 7 du RE N° 725/2004 et

ne concerne que les navires effectuant des services réguliers entre deux terminaux. Cette exemption sous-entend une demande de la compagnie auprès du Ministère en charge des transports et un accord de cette administration en retour. L'exemption doit être renouvelée à l'échéance du certificat international de sûreté du navire. La liste des navires concernés est remise à jour autant que de besoin. L'exemption est ensuite communiquée à la Commission européenne.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

L'arrêté du 22 avril 2008 demande de définir des modalités de communication des renseignements préalables. Dans les faits, l'exploitant d'une installation portuaire peut avoir besoin d'entrer en contact avec le navire pour différentes raisons. D'ailleurs, le RE N° 725/2004 prévoit une procédure en matière de communication entre l'exploitant et le navire, car l'ASIP et l'ASN doivent être en mesure de communiquer ensemble à tout moment, en particulier en cas d'incident ou de changement de niveaux ISPS, ou sur demande des services de l'Etat.

Pour plus de détail, on se reportera à l'annexe n° 5.

Conseils complémentaires pour les exploitants :

L'ASIP peut se procurer les renseignements préalables de plusieurs façons :

a) Ces renseignements sont communiqués de manière systématique par le navire auprès de l'AIPPP (capitainerie). À partir de là :

- soit la capitainerie répercute systématiquement cette information auprès de l'ASIP. Parfois certaines capitaineries disposent d'interface web où l'ASIP peut récupérer directement les renseignements préalables ;
- soit la capitainerie communique les renseignements préalables uniquement en cas de niveaux de sûreté différents entre le navire et l'installation portuaire. Malgré tout, l'exploitant devrait s'assurer que la capitainerie reçoit systématiquement les renseignements préalables même au niveau 1 ISPS ;

b) Les renseignements préalables ne sont pas communiqués usuellement par la capitainerie, l'ASIP peut se procurer l'information :

- auprès de l'agent maritime qui est en relation avec le navire. Éventuellement une convention entre l'exploitant et l'agent demandera une transmission systématique des informations avant l'escale ou alors l'ASIP refusera l'accès au navire si les renseignements ne sont pas reçus 24h à l'avance ;
- l'ASIP peut choisir de se procurer lui-même l'information auprès de l'agent maritime ou de la capitainerie, sur sa demande.

Il faut garder à l'esprit que l'obtention des renseignements préalables relève de la responsabilité de l'ASIP. Quand une tâche est déléguée à autrui (capitainerie ou agent maritime), l'ASIP doit décrire une procédure qui lui permettra d'obtenir systématiquement ces renseignements de leur part. L'ASIP devrait ponctuellement vérifier la bonne exécution des tâches qu'il délègue à autrui.

Le cas échéant, l'ASIP se rapprochera de l'ASP pour vérifier que les procédures relatives aux renseignements préalables prévues dans le PSP et le PSIP ne se contredisent pas.

Fiche 4.2.6 – Description de la procédure interne de changement de niveau de sûreté après transmission de la consigne par l'autorité publique

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004, section A/16.3.4 des procédures pour donner suite aux consignes de sûreté que le Gouvernement contractant sur le territoire duquel l'installation portuaire est située pourrait donner au niveau 3

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

-Description de la procédure interne de changement de niveau de sûreté après transmission de la consigne par l'autorité publique

Les objectifs :

Principe général :

Voir le libellé de l'arrêté.

Principe particulier pour les instructeurs :

La procédure devra être mise en cohérence avec l'organisation de la chaîne d'alerte usuellement définie par le représentant de l'État et l'Autorité portuaire.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Le changement de niveau ISPS est signalé par le représentant de l'État dans le département, soit directement par le représentant de l'État (préfecture) soit par l'intermédiaire de la capitainerie ou de l'ASP.

L'autorité préfectorale peut diffuser l'alerte selon le mode opératoire de son choix (messagerie électronique, téléphone, fax).

À la réception de l'avis informant du changement de niveau de sûreté, l'ASIP accuse réception et met en place les mesures du niveau de sûreté prévues par son PSIP.

Conseils complémentaires pour les exploitants :

L'exploitant doit relayer l'information auprès :

- du personnel (ASIP, ASIP suppléants, personnel ayant des tâches de sûreté) ;
- de l'agent de sûreté du navire (ou demander à la capitainerie de contacter l'ASN).

Il peut porter à la connaissance auprès :

- du personnel déjà présent ou pénétrant dans l'installation portuaire le changement de niveau ISPS, éventuellement en installant un panneau ;
- et éventuellement auprès des visiteurs de l'installation portuaire.

La procédure interne de changement de niveau après transmission de la consigne par l'autorité locale doit décrire et faciliter la mise en œuvre des mesures de sûreté issues du PSIP, sachant que ces mesures sont classées Confidentiel Sûreté et ne sont connues que des personnes ayant à en connaître.

Il s'agit d'une véritable fiche réflexe permettant de faciliter la communication efficace des instructions vers les fonctions impliquées (service de gardiennage, ACVS, personnel d'exploitation, ASIP et suppléants). Elle précise les dispositions prises pour informer les personnes susceptibles d'être autorisées à pénétrer sur l'installation portuaire (sous-traitants, visiteurs, avitailleurs, lamaneurs...).

Fiche 4.2.7 – Mesures additionnelles lors de l'escale d'un navire de croisière

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

Mesures additionnelles lors de l'escale d'un navire de croisière

Les objectifs :

Principe général :

Cette prescription concerne les installations portuaires qui n'ont pas une activité exclusivement dédiée à la croisière et qui peuvent en recevoir de manière exceptionnelle. Le PSIP prévoira des mesures de sûreté pour accueillir de telles escales complémentaires à celles mises en œuvre en temps normal.

Principe particulier pour les instructeurs :

Ces escales croisières occasionnelles devront être prévues dès la rédaction de l'évaluation de sûreté de l'installation. Tout changement durable d'activité sur le terminal non pris en compte lors de la rédaction de l'ESIP implique une révision de celle-ci.

C'est l'évaluation qui déterminera en fonction de la fréquence de ces escales croisières si on reste dans le cadre de « mesures additionnelles » ou si on s'oriente vers des mesures plus pérennes dans le cadre d'une ZAR à définir dans le chapitre 5 du PSIP.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Si l'installation portuaire est complètement dédiée à l'activité de croisière ; il n'est pas utile de prévoir des mesures additionnelles, car celles-ci sont déjà prévues dans le chapitre 5 du PSIP qui décrit les modalités d'activation d'une ZAR.

Si l'exploitant a un terminal non dédié à l'activité de croisière, le PSIP définira des mesures additionnelles en matière de sûreté, à savoir :

- le renforcement des moyens humains (gardiennage) ;
- la description des tâches supplémentaires à effectuer (rondes, contrôles d'accès, surveillance) ;
- le renforcement du matériel de sûreté ;
- la répartition des tâches entre le navire et l'exploitant, au besoin dans le cadre d'une DOS.

Fiche 4.2.8 – Moyens et prestations assurés pour chaque niveau de sûreté applicable

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.2. Organisation de l'installation portuaire en matière de sûreté

Moyens et prestations assurés pour chaque niveau de sûreté applicable, notamment pour ce qui concerne les prestations sous-traitées. Figurent en annexe chaque contrat de prestation, la description des tâches sous-traitées, les effectifs déployés suivant le niveau de sûreté et les modalités de contrôle de la bonne exécution du contrat par l'exploitant de l'installation portuaire, dont le contrôle sur place inopiné.

Les objectifs :

Principe général :

Décrire l'ensemble des moyens humains et matériels dédiés à la sûreté du terminal qui sont sous-traités à un tiers et qui font l'objet d'un cahier des clauses techniques et particulières ou d'une convention.

Principe particulier pour les instructeurs :

Vérifier que les cahiers des clauses techniques et particulières ou les conventions avec les sous-traitants existent et sont annexés au PSIP.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Liste, non exhaustive, des prestations de sûreté susceptibles d'être sous-traitées :

- entretien des clôtures ;
- matériels de détection d'articles prohibés (détecteur d'explosifs, détecteurs de métaux, portiques...) ;
- maintenance informatique de serveurs ;
- prestation de gardiennage et/ou d'inspection-filtrage (moyens humains) ;
- rondes de sûreté ;
- maintenance de caméras dédiées à la vidéoprotection, de l'éclairage...

L'exploitant devra prévoir des modalités de contrôle de la bonne exécution des contrats sous-traités. Il pourra entreprendre des contrôles inopinés de ces prestations, puis organiser des réunions ponctuelles avec le(s) prestataire(s) pour faire un point sur la bonne exécution du contrat.

En annexe du PSIP, l'ASIP peut ajouter une procédure décrivant la liste des points à contrôler, avec :

- la liste des points à contrôler (cadenas, clôtures, caméras...) ;
- la périodicité des contrôles ;
- l'agent en charge de faire les contrôles.

Les points contrôlés sont consignés dans le registre de sûreté.

Une attention particulière sera consacrée au contrat précisant les effectifs sous-traités en matière de sûreté. Ce contrat devra être mis en cohérence avec les chapitres 4 et 5 du PSIP, il stipulera :

- le nombre d'effectifs ;
- la déclinaison par niveaux ISPS des effectifs ;
- leurs tâches, leurs missions ;
- les modalités horaires et/ou d'astreinte ;
- les délais de réaction en cas de surcroît d'activité (saisonnalité de l'activité, changement de niveau ISPS) ;
- le recours à du personnel féminin pour les PIF ;
- les obligations de formation pour les agents chargés des visites de sûreté (dans le cadre d'un PIF) ;
- la prise en charge de la sensibilisation du personnel notamment pour les agents qui n'ont pas vocation à travailler en ZAR.

Fiche 4.2.9 – Si l'installation portuaire est désignée point d'importance vitale

Le cadre réglementaire :

Annexe 4 de l'arrêté du 22 avril 2008

Si l'installation portuaire est désignée point d'importance vitale, décrire :

–l'organisation hiérarchique (autorité, responsables, permanence de direction)

–l'identité du délégué pour la défense et la sécurité (titulaire, suppléant) et les fonctions qu'il occupe au sein de l'installation portuaire

–le fonctionnement de l'installation portuaire et son environnement

–l'effectif des personnels (employés et des sous-traitants) travaillant dans le point d'importance vitale (personnel d'exécution, cadres, nombre d'étrangers (Union européenne et hors Union européenne)).

Les objectifs :

Pas de recommandation particulière ; reprendre le cadre de l'arrêté si l'installation est classée PIV.

Fiche 4.3 – Coordination avec les installations portuaires adjacentes ou ayant un accès commun

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.3. Coordination avec les installations portuaires adjacentes ou ayant un accès commun

– Articulation du plan de sûreté de l'installation portuaire avec le ou les plans de sûreté d'installation portuaire adjacente (vérification de clôtures, notamment). Si l'installation portuaire est désignée point d'importance vitale, une attention particulière sera prêtée à l'articulation de son plan de sûreté avec le plan de sûreté des installations portuaires adjacentes ;

– Pour les installations portuaires comprenant une ou des zones d'accès restreint desservies depuis la terre par un accès commun, pour chacune de ces ZAR, procédures de coordination devant être mises en œuvre, notamment au niveau de l'accès commun. Les procédures de coordination doivent préserver le niveau de sûreté.

Les objectifs :

Principe général :

Par installations portuaires adjacentes, il faut comprendre les installations portuaires juxtaposées ou accolées, ayant des mesures de protection communes (accès commun, clôtures communes...).

Principe particulier pour les instructeurs :

Vérifier si une installation portuaire a un accès commun ou une clôture commune avec une autre installation portuaire.

Vérifier que les mesures de coordination prévues dans chacun des PSIP des exploitants concernés coïncident.

Vérifier l'existence d'une convention définissant et répartissant les mesures de sûreté prises en charge par chaque exploitant.

Fiche 4.3.1 – Articulation du plan de sûreté de l'installation avec le ou les plans de sûreté d'installation portuaire adjacente

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Si l'installation portuaire n'est pas adjacente et n'a pas d'accès commun avec une autre installation portuaire, alors la réponse à ce point réglementaire est « sans objet ».

Si une installation portuaire est adjacente ou a un accès commun avec une autre installation portuaire, les exploitants concernés doivent apprécier et décrire dans leur PSIP :

- les modalités de coordination avec l'IP voisine ;
- les mesures de sûreté prises en charge par chacun ;
- les mesures de sûreté communes définies dans le cadre d'une convention surtout si ces mesures sont prises en charge par un seul des deux exploitants.

La coordination entre deux installations portuaires adjacentes ou ayant un accès commun peut concerner :

- un accès commun, un portail commun ; il faut alors définir quel exploitant gère l'ouverture du portail, entretient le portail, vérifie son état, et à quel rythme ;
- des clôtures communes ; à nouveau qui gère, qui entretient, qui vérifie l'état des clôtures, et à quel rythme ;
- des codes d'accès, des clés ; il faut préciser qui distribue les clés ou diffuse les codes d'accès, et qui change les codes d'accès ;
- du personnel de sûreté faisant des rondes au profit de l'installation portuaire voisine : qui gère ce personnel, quelles sont leurs missions, et si le personnel est sous-traité qui détient les contrats ;
- d'autres mesures de contrôle d'accès.

Fiche 4.3.2 – Pour les installations portuaires comprenant une ou des ZAR desservies depuis la terre par un accès commun

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Deux exploitants ayant un accès commun permettant de rejoindre une ou des ZAR doivent démontrer que les mesures de sûreté prises par chaque exploitant permettent de préserver le niveau de sûreté.

Une convention doit être prise entre les deux exploitants pour garantir le niveau de sûreté avant d'entrer en ZAR.

Si le niveau de sûreté ne peut pas être garanti par l'IP voisine, l'exploitant mettra en place ses propres mesures de sûreté telles que prévues dans son PSIP et par l'arrêté ZAR.

Fiche 4.4 – Articulation avec les autres plans et procédures

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004, section A/16.5. Le plan de sûreté de l'installation portuaire peut être combiné avec le plan ou tout autre plan d'urgence portuaire ou faire partie de tels plans

Code ISPS annexé au RE N° 725/2004, section B/16.8.11. Les procédures permettant de tenir et de mettre à jour l'inventaire des marchandises dangereuses et des substances potentiellement dangereuses qui se trouvent dans l'installation portuaire, y compris leurs emplacements

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

4. Organisation générale de la sûreté de l'installation portuaire

4.4. Articulation avec les autres plans et procédures

– Articulation du plan de sûreté de l'installation portuaire avec d'autres plans ou activités de prévention et d'intervention. Le plan explicite les modalités d'interaction et de coordination avec les autres activités de prévention et de contrôle, notamment les procédures applicables aux matières dangereuses, ainsi qu'avec les autres plans d'intervention et d'urgence en vigueur dans l'installation portuaire ;

– Indication des procédures et consignes applicables, le cas échéant, dans des domaines connexes (mesures de défense et de protection, etc.), et prise en compte par le plan.

Fiche 4.4.1 – Articulation du PSIP avec d'autres plans ou activités de prévention et d'intervention

Les objectifs :

Principe général :

Il faut expliquer dans quelle mesure le PSIP peut s'appuyer sur d'autres procédures. On pourra distinguer :

- L'articulation du PSIP avec d'autres procédures internes à l'entreprise :
 - articulation avec des procédures applicables aux matières dangereuses ;
 - articulation avec des procédures d'urgence (procédure d'évacuation) ;
 - articulation avec des procédures de prévention ;
 - articulation avec les plans de continuité d'activités (effectifs minimums pour assurer le fonctionnement de l'activité).
- L'articulation du PSIP avec d'autres procédures externes à l'entreprise :
 - Vigipirate ;
 - règlement général et particulier de police ;
 - PSP ;
 - plans d'urgence (POLMAR, Vigimer...).

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Il ne faut pas uniquement lister et citer des procédures existantes dans une entreprise. Il faut pouvoir résumer ces procédures et expliquer leur complémentarité avec le PSIP. Si l'ASIP n'est pas en mesure de préciser les liens exacts entre son PSIP et d'autres types de plans, il faut éviter de les citer.

a) Articulation du PSIP avec d'autres procédures internes à l'entreprise :

- Articulation avec des procédures applicables aux matières dangereuses, visant à décrire :
 - les obligations de gardiennage sur le terminal des marchandises dangereuses ;
 - la quantité de marchandises dangereuses ou polluantes admissibles sur un terre-plein ;
 - la durée maximale du dépôt à terre pour les marchandises dangereuses en conteneurs ;
 - l'emplacement réservé pour le stationnement de véhicules de transport de matières dangereuses.
- Articulation avec des procédures de prévention :

De manière générale, la sécurité primera sur la sûreté. L'ASIP déterminera les mesures de sûreté – sécurité à mettre en œuvre pour faciliter les interventions de secours. L'ASIP précisera s'il existe des consignes générales dans l'entreprise qu'elle impose à l'ensemble des intervenants sur site (exemple : livret d'accueil pour les nouveaux arrivés, pour les personnes externes).
- Articulation avec des procédures d'urgence (procédure d'évacuation) :

Les mesures de sûreté doivent être adaptées de manière à ne pas entraver l'action des secours. L'exploitant devra se demander :

 - qui a la charge de constater l'incident ? Comment l'information remonte auprès d'un responsable ?
 - qui déclenche le plan d'urgence ; qui a cette responsabilité ? (est-ce la direction, l'ASIP, le responsable qualité...)
 - qui définit un périmètre de sécurité pour ne pas s'approcher de l'incident ?

- qui est chargé de prévenir la capitainerie, la préfecture, les services de secours ?
- qui diffuse les consignes à tenir en cas d'urgence auprès du personnel de l'entreprise, de visiteurs ?

L'exploitant devrait adopter les principes suivants :

- faciliter l'arrivée des secours ou des équipes d'intervention (ouverture des accès avec mise en place de moyens humains pour assurer le contrôle) ;
- accompagner les secours.

Si l'ASIP n'a pas de procédure d'urgence, il peut alors faire référence aux fiches réflexes qui figureront dans le chapitre 6 du PSIP « conduite à tenir en cas d'alerte » et dans le volume 2 du PSIP.

b) Articulation du PSIP avec d'autres procédures externes à l'entreprise :

A priori, l'exploitant n'a pas connaissance du contenu des procédures d'autres plans comme Vigipirate, Vigimer, Plan de Sûreté Portuaire (PSP). L'exploitant demandera aux interlocuteurs concernés s'il est vraiment utile de faire référence à de telles procédures. Charge aux services concernés d'expliquer en quoi peut consister l'articulation avec le PSIP de l'exploitant.

Pour le Plan de Sûreté Portuaire (PSP) relevant de l'autorité portuaire, on peut imaginer que :

- l'ASP demande à l'ASIP de faire remonter systématiquement les incidents de sûreté qui surviennent dans l'IP ;
- l'ASP organise des réunions régulières avec l'ASIP (préciser éventuellement la périodicité) ;
- l'ASP mutualise des exercices avec l'ASIP.

Fiche 4.4.2 – Indication des procédures et consignes applicables

Les objectifs :

Principe général :

Il peut exister des procédures ISO, de défense (cas des PIV) et de protection qui peuvent avoir un lien avec le PSIP. L'ASIP pourra décrire de manière concrète les liens entre ces plans.

Fiche 4.5 – Gestion documentaire et protection du plan de sûreté de l'installation portuaire

Le cadre réglementaire :

Règlement (CE) N° 725/2004, annexe II, A 10.3, A.16.3.11, A 16.7, a 16.8 – annexe III, B 4.1, B 16.8.6.

Code des transports, article R. 5332-29

Circulaire 323 DT MPL du 29 mars 2004, para 3.2.

Décret 2006-212 relatif à la sécurité des activités d'importance vitale, article 28.

Instruction Générale Interministérielle 1300 sur la protection du secret (arrêté premier ministre du

30 novembre 2011), articles 4 et 5 et annexe 3.

IGI 6600 du 26 septembre 2008, relative à la sécurité des activités d'importance vitale, para 1.3.6.

Arrêté du 22 avril 2008, Titre II, articles 6 et 7, Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP), Chapitre 4.5 – Gestion documentaire et protection du plan de sûreté de l'installation portuaire :

- Mesures visant à assurer le respect de la confidentialité du plan : prescriptions de protection de l'information contre la divulgation non autorisée ;
- Mesures et moyens de protection des données, des documents, des communications, des informations (documents écrits et données électroniques) dont la divulgation porterait atteinte au niveau de la sûreté, selon le niveau de confidentialité exigé ;
- Identification des personnes ayant accès aux informations de sûreté protégées et des responsables du système de protection ;
- Critères de diffusion : le plan de sûreté de l'installation portuaire comporte deux volumes physiquement séparés, l'un exhaustif, portant la mention « Confidentiel Sûreté », l'autre ne comprenant que les informations devant être connues par les personnes chargées d'effectuer les visites de sûreté, portant la mention « Diffusion Limitée Sûreté ». Ces informations sont énumérées limitativement au point 10 du présent plan.

Les objectifs :

Principe général :

Les documents traitant de la sûreté de l'installation portuaire font l'objet d'une mention de protection, limitant leur diffusion au seul besoin d'en connaître. Les supports informatiques traitant de la sûreté sont conservés et diffusés selon les mêmes procédures.

La documentation des exploitants ou installations portuaires classées OIV / PIV est quant à elle « classifiée », les personnels ayant à en connaître font l'objet d'habilitation spécifique, la diffusion et la conservation des supports physiques ou électroniques font l'objet des mesures de l'IGI 1300.

Principe particulier pour les instructeurs :

S'assurer de la décision (ou non) de classement en OIV/PIV.

Bien faire la différence entre documentation classifiée et documentation protégée, les règles de conservation et de diffusion étant très différentes.

S'attacher à limiter la diffusion des documents aux seules personnes ayant besoin d'en connaître.

Définir les critères de diffusion des volumes 1 et 2 du PSIP, sachant que le volume 1 porte la mention « Confidentiel Sûreté » et le volume 2 « Distribution Limitée Sûreté ». Le volume 2 contient, outre les éléments prévus au chapitre 10, les fiches procédures, les fiches réflexes et les conduites à tenir à usage des agents assurant des tâches de sûreté (prestataire de service et/ou agents de l'exploitant).

Principe particulier pour les exploitants :

Reprendre, sous forme de tableau, les mesures visant à assurer le respect de la confidentialité (exemple en annexe n° 6).

À chaque type de documents correspondent des destinataires sélectionnés et répertoriés dans des listes correspondant au niveau d'habilitation interne à l'IP (exemple en annexe n° 6), ou prévus aux chapitres 2.4.1 et 2.4.2 (voir également fiche 2.4). Ces destinataires élargissent alors une reconnaissance de responsabilité (exemple en annexe n° 6).

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

En référence à l'annexe 6, la documentation de sûreté doit être sécurisée. Il appartient à l'ASIP de démontrer que le niveau d'accès à la documentation sensible est sûr et maîtrisé. La documentation doit être accessible aux seules personnes autorisées et protégée contre tous les actes délictueux.

Peuvent être considérés comme sûres, par exemple :

- l'utilisation d'un coffre fort ;
- l'utilisation d'un meuble fermant à clé et situé dans un bureau sécurisé (par sécurisé il faut entendre bureau ou bâtiment sous alarme ou vidéoprotection avec intervention humaine immédiate en cas d'alarme intrusion) ;
- la mise en œuvre d'autres dispositifs de protection avec un niveau de sécurité équivalent.

Les documents informatiques doivent être protégés par des mesures empêchant que leurs données soient lues, effacées, détruites ou modifiées sans autorisation.

Les informations « sûreté » sensibles ne sont pas diffusées en clair sur le réseau VHF/UHF. L'utilisation de la téléphonie est privilégiée pour la communication de ces renseignements.

Définir une procédure de gestion des clés, des combinaisons et des codes :

Le PSIP décrit les dispositions pour la conservation et la gestion des clefs, des systèmes de verrouillage et des combinaisons, utilisées pour la sûreté :

- registres d'inventaires et d'utilisation des clés ;
- modalités de conservation, de diffusion et de changement des codes (protocole à prévoir si les codes sont communiqués à des tiers comme le lamanage, l'agent maritime...).

Pour l'envoi de documents, l'exploitant devrait utiliser des bordereaux d'envoi.

Pour l'échange des données informatisées, il devrait être réalisé, sauf exception, entre adresses nominatives.

Chapitre 5 : Accès et circulation dans les installations portuaires

Préambule

Actuellement la réglementation distingue deux catégories d'installations portuaires (IP).

Les IP abritant une ZAR, dites sensibles, car elles sont dédiées au transport de :

- passagers ;
- matières dangereuses (produits pétroliers, chimiques, gaz) ;
- conteneurs.

Les IP n'abritant pas de ZAR, dites non sensibles, car elles sont dédiées au transport de marchandises non dangereuses, comme les vracs solides (charbon, céréales, colis lourds...) et les vracs liquides (huiles végétales...).

Les mesures générales de contrôle d'accès et surveillance de chaque IP doivent être décrites dans le chapitre 5 du PSIP tel que défini par la trame de l'arrêté du 22 avril 2008.

Différents cas de figure peuvent se présenter :

Sensibilité de l'IP	Périmètre de la ZAR	Modalités d'activation de la ZAR	Fiches du présent guide à renseigner
l'IP abrite une ZAR, l'IP est dite sensible	La surface de la ZAR couvre l'ensemble de la surface de l'IP ; ZAR = IP	ZAR permanente la ZAR est activée H24	Renseigner les fiches 5.1 à 5.4 spécifiques à la ZAR ; ainsi que les fiches 5.5.6 et 5.5.7 traitant des provisions de bord et de la manutention de la marchandise.
l'IP abrite une ZAR, l'IP est dite sensible	La surface de la ZAR couvre l'ensemble de la surface de l'IP ; ZAR = IP	ZAR permanente, mais la ZAR est activée uniquement en présence d'une escale	Renseigner les fiches 5.1 à 5.4 spécifiques à la ZAR. En outre, lorsque la ZAR est inactivée, l'IP est, en général, assimilable à une ZNLA. L'exploitant doit définir les mesures de sûreté à appliquer, sur la base des fiches 5.5 (5.5.1 à 5.5.8). Plus particulièrement, il faut préciser les mesures de protection des points névralgiques retenus lors de l'ESIP, si la ZAR est inactive.
l'IP abrite une ZAR, l'IP est dite sensible	La surface de la ZAR ne couvre pas l'ensemble de la surface de l'IP ; ZAR ≠ IP	ZAR permanente, quelle que soit la modalité d'activation	Renseigner les fiches 5.1 à 5.4 spécifiques à la ZAR. L'exploitant doit définir les mesures à appliquer sur la surface non couverte par la ZAR, sur la base des fiches 5.5 (5.5.1 à 5.5.8). L'ESIP devrait préalablement se prononcer sur l'opportunité d'appliquer des mesures de sûreté sur la surface non couverte par la ZAR.
l'IP n'abrite pas de ZAR, l'IP est dite non sensible	Sans objet	Sans objet	L'IP est souvent assimilable à une ZNLA. L'exploitant doit définir les mesures de sûreté à appliquer, sur la base des fiches 5.5 (5.5.1 à 5.5.8).

Fiche 5.1 – Dispositions communes aux ZAR et aux ZNLA au public dans les IP désignées PIV

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.1. Dispositions communes aux zones d'accès restreint et aux zones non librement accessibles au public dans les installations portuaires désignées point d'importance vitale

Si l'installation portuaire est désignée point d'importance vitale, détailler les dispositions concernant :

- les équipes de protection et de gardiennage (effectif et formation des personnels, organisation du gardiennage et des rondes, postes tenus et moyens complémentaires, dénomination sociale du prestataire en cas de sous-traitance) ;*
- système d'astreinte et de permanence ;*
- dispositif de sûreté : PC de sécurité, énergie, système d'informations dont de télécommunications ;*
- protection des systèmes de sûreté.*

Les objectifs :

Principe général :

Pas de recommandation particulière ; reprendre le cadre de l'arrêté si l'installation est classée PIV.

Fiche 5.2 – Identification et caractéristiques des zones d'accès restreint

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.2. Identification et caractéristiques des zones d'accès restreint

Identification de chaque ZAR avec les informations suivantes :

- Référence de l'arrêté préfectoral créant la ZAR ;*
- Plan faisant apparaître le système de clôture, l'emplacement des points d'inspection-filtrage, les éventuelles séparations de secteurs et les différents accès ;*
- Catégories de personnels et d'activités concernés ;*
- Flux d'entrée et nombre de titres de circulation par catégorie définie à l'article R. 5332-37 du code des transports ;*
- Schéma de circulation. Il sera prêté une attention particulière aux circulations entre les ZAR extérieures aux installations portuaires et les ZAR situées dans une installation portuaire auxquelles elles donnent, le cas échéant, accès.*

Les objectifs :

Principe général :

Reprendre le cadre de l'arrêté et se référer aux fiches 5.2.1 à 5.2.5 ci-après.

Fiche 5.2.1 – Référence de l'arrêté préfectoral créant la ZAR

On reprendra les renseignements figurant sur l'arrêté ZAR :

- le nom de la ZAR ;
- le numéro de l'arrêté préfectoral.

Éventuellement, on pourra :

- rappeler la date de l'arrêté ;
- et mettre en annexe du PSIP l'arrêté ZAR.

Numéro de ZAR	Nom ou intitulé de la ZAR	Référence de l'arrêté préfectoral créant la ZAR	Date de l'arrêté ZAR	Pièce annexée à l'arrêté ZAR
ZAR n°1				
ZAR n°2				

Fiche 5.2.2 – Plan faisant apparaître le système de clôture, l'emplacement des points d'inspection-filtrage, les éventuelles séparations de secteurs et les différents accès

Un plan de masse figure déjà au chapitre 4, paragraphe 4.1 où on demande de localiser :

- les contours du périmètre de l'installation portuaire approuvé par arrêté ;
- le périmètre des clôtures (éventuellement contour IP = contour clôture) ;
- les portails d'accès ;
- l'éclairage ;
- les barrières de protection ;
- dispositifs de protection périmétrique (infra-rouge...) ;
- la vidéo-surveillance (+ angle de vue des caméras) ;
- les points d'inspection filtrage ;
- l'amarrage ;
- une légende sur le plan.

Insister sur les limites du périmètre de la ZAR et sur la localisation du ou des PIF.

Faire attention à l'échelle du plan de masse et à la lisibilité des informations.

Fiche 5.2.3 – Catégories de personnels et d'activités concernés

Le code des transports, dans son article R. 5332-37, liste 7 catégories de personnes que l'exploitant peut autoriser à entrer en ZAR. En annexe n° 7 sont rappelées les catégories de personnes.

L'exploitant mettra en évidence les catégories de personnes autorisées qui ont vocation à pénétrer régulièrement dans la ZAR.

Il s'agira également de préciser le type d'activités concernées. Par exemple, le PSIP mentionnera si des véhicules légers et des poids lourds entrent en ZAR.

Fiche 5.2.4 – Flux d'entrée et nombre de titres de circulation

L'exploitant comptabilisera :

- les flux par catégorie d'accédant. Ils seront mis à jour en fonction des statistiques enregistrées au niveau des PIF ;
- le nombre de titres de circulation émis pour les accédants à la ZAR et les véhicules pénétrant en ZAR.

En annexe n° 7 est proposé un modèle de tableau pour présenter les flux d'entrée et le nombre de titres de circulation.

Fiche 5.2.5 – Schéma de circulation

Le schéma de circulation doit faire apparaître le sens de circulation des personnes et des véhicules dans la ZAR. On reprendra le plan de masse en y ajoutant des flux de circulation et une légende. Le plan devrait également comprendre les zones de stationnement des véhicules légers et des poids lourds.

Dans certains cas, comme de simples appontements, il n'est pas utile de faire un tel schéma, le sens de circulation étant évident.

Un schéma de circulation sera particulièrement apprécié pour les installations portuaires accueillant un flux important de passagers (ferries, croisières) et de véhicules (RoPax, conteneurs, RoRo).

Pour les ZAR extérieures, on prendra en considération toute ZAR contiguë (mitoyenne) à l'installation portuaire.

Fiche 5.3 – Protection et contrôle des accès en zone d'accès restreint

Le paragraphe 5.3, tel que défini dans l'annexe 4 de l'arrêté du 22 avril 2008, prévoit plusieurs sous-parties, lesquelles sont détaillées dans les fiches 5.3.1 à 5.3.11.

Fiche 5.3.1 – Modalités d'activation de la ZAR et visites de sûreté

Le cadre réglementaire :

Arrêté du 4 juin 2008, modifié par arrêté du 1^{er} avril 2015

Article 13. – Visites de sûreté. – L'exploitant de l'installation portuaire s'assure, indépendamment des contrôles préalables à l'entrée en zone d'accès restreint, qu'aucune personne non autorisée ne circule dans la ou les zones d'accès restreint qui relèvent de sa compétence et qu'aucun article prohibé ou objet suspect n'y a été introduit. (...) Lors de l'activation d'une zone d'accès restreint et en cas de création d'une zone d'accès restreint temporaire, l'exploitant de l'installation portuaire effectue une visite de sûreté de l'ensemble de cette zone préalablement au début de l'exploitation de l'inspection-filtrage.

Le PSIP devrait rappeler les modalités d'activation de la ZAR, telles que définies par l'arrêté préfectoral créant et définissant la ZAR. L'exploitant doit effectuer une visite de sûreté avant l'activation de la ZAR. Cette visite a pour but d'inspecter le périmètre de la ZAR (y compris les locaux), avant d'activer la ZAR, afin de rechercher des articles prohibés ou des personnes non autorisées ou d'empêcher leur accès.

On peut distinguer trois cas de figure :

- la ZAR permanente ;
- la ZAR permanente, activée en présence d'une escale ;
- la ZAR temporaire.

Cas 1 : Pour la ZAR permanente, les mesures de sûreté spécifiques à la ZAR sont activées 24h/24h.

Cas 2 : Une ZAR permanente peut être **activée uniquement en présence d'une escale**. Autrement dit, le terminal ne fonctionne pas 24h/24h et a des périodes de fermeture. Dès lors, les mesures de sûreté sont :

- « temporairement désactivées » en l'absence de navire amarré à quai. On parlera de ZAR inactivée ;
- **activées sur l'ensemble de la durée de l'escale d'un navire à quai**, y compris si le navire est en attente après que les opérations commerciales soient achevées. Une visite de sûreté est effectuée avant l'arrivée du navire afin de s'assurer que le terminal est intègre.

Que se passe-t-il lorsque les mesures de la ZAR sont inactivées ?

- au minimum, un panneau est installé pour matérialiser l'interdiction de passage lorsque le service est inactif ;
- l'installation portuaire sera assimilée à une ZNLA. L'exploitant devra définir s'il est opportun d'adopter des mesures de surveillance et de contrôle d'accès (se référer aux fiches du paragraphe 5.5 du guide pour définir les mesures) ;
- dans de nombreux cas de figure, le terminal est purement et simplement fermé. Cependant, même en l'absence d'escale, l'exploitant peut choisir de maintenir des mesures de sûreté afin d'avoir une continuité des mesures ZAR par rapport à un régime où la ZAR est activée, en organisant des rondes de sûreté, en s'appuyant sur son dispositif de vidéoprotection ;
- lorsque l'exploitant réactivera la ZAR, une visite de sûreté sera impérative préalablement à l'arrivée du navire.

Cas 3 : En opposition à la ZAR permanente, on peut créer une **ZAR temporaire** comme définie par l'article 47 de l'arrêté du 4 juin 2008. La durée de ce type de ZAR est limitée à 2 mois. Il n'est pas possible d'aller au-delà, contrairement à la ZAR permanente où aucune durée n'est fixée. Comme les mesures de la ZAR temporaire ne sont pas nécessairement activées 24h/24h, une visite de sûreté est effectuée avant l'arrivée de chaque navire pour s'assurer que le terminal est intègre.

Fiche 5.3.2 – Caractéristiques des clôtures et de tout autre équipement de protection périmétrique

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

Pour chaque ZAR, préciser les informations ci-dessous. Si certaines catégories d'informations sont strictement identiques pour plusieurs ZAR, elles peuvent faire l'objet d'un paragraphe commun avant les paragraphes spécifiques à chaque ZAR.

– Caractéristiques des clôtures et de tout autre équipement de protection périmétrique ;

Les objectifs :

Principe général :

La protection périmétrique a pour objectif de matérialiser les limites de propriété, de dissuader et de retarder l'effraction.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Une photo est souvent plus parlante qu'un long discours pour décrire les clôtures choisies pour retarder l'accès au terminal et au navire.

Il existe différents types de clôtures :

- clôtures pleines ;
- clôtures grillagées ;
- clôtures en panneaux soudés ;
- clôtures mobiles.

Parmi les éléments caractérisant une clôture, le PSIP pourra préciser :

- si une double clôture est installée ;
- la profondeur du scellement de la clôture pour empêcher le passage d'une personne par-dessous la clôture (la profondeur de scellement est de 50 cm en général) ;
- si les abords extérieurs sont protégés par un fossé, un glacis empêchant le stationnement au ras de la clôture ;
- si la zone est débroussaillée pour éviter tout camouflage ou toute escalade ;
- si des bavolets et des concertinas sont installés ;
- si un éclairage a été installé le long de la clôture.

L'exploitant peut utiliser d'autres équipements de protection périmétriques comme des détecteurs dont la fonction est d'alerter l'approche ou la présence d'une personne. Il existe :

- des barrières infrarouge ;
- des barrières à hyperfréquence ;
- des tubes à pression (en dessous du sol) ;
- des câbles rayonnants (en dessous du sol) ;
- des détecteurs sur clôtures (câbles optiques, détecteurs à masselottes...).

Fiche 5.3.3 – Caractéristiques des différents points d'accès

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Caractéristiques des différents points d'accès ;

Arrêté du 4 juin 2008, modifié par arrêté du 1^{er} avril 2015

Article 13 : L'exploitant de l'installation portuaire s'assure, indépendamment des contrôles préalables à l'entrée en zone d'accès restreint, qu'aucune personne non autorisée ne circule dans la ou les zones d'accès restreint qui relèvent de sa compétence et qu'aucun article prohibé ou objet suspect n'y a été introduit.

Les objectifs :

Principe particulier pour les instructeurs :

Recenser les portails d'accès de manière exhaustive et décrire leurs caractéristiques.

Préciser les modalités de contrôle d'accès à chaque point d'accès.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

L'arrêté du 22 avril 2008 demande uniquement de décrire les caractéristiques des points d'accès. Cependant, toute personne et tout véhicule souhaitant pénétrer en ZAR doit se soumettre à un contrôle documentaire avant d'entrer (voir fiche 5.3.7). Dans ce cas, l'exploitant devrait préciser dans son PSIP les modalités des contrôles à chacun de ses points d'accès à la ZAR.

La description des caractéristiques et des modalités de contrôle à chaque accès peut être retranscrite sous forme de tableau synthétique, avec les informations ci-après :

- numéro ou nom du portail d'accès ;
- mettre une photo pour décrire plus facilement les caractéristiques d'un accès ;
- types de portails d'accès existants :
 - des portillons (largeur inférieure à 1,5 mètre) ;
 - des portails pivotants ;
 - des portails coulissants avec des rails scellés au sol ;
 - des autoportants guidés par portiques sans rail au sol ;
 - des portails à motorisation.
- mesures de contrôle d'accès :
 - existence d'un PIF à l'entrée de l'accès ;
 - autres modalités en l'absence de PIF (visiophone ; contrôle d'accès à distance ; gestions par clés ; gestion par badges...) ;
 - ouverture des portails d'accès gérés par des clés, des codes d'accès (digicodes), des badges ; prévoir alors une procédure décrivant la gestion de la diffusion des clés et des codes (voir fiche 4.5) ;
 - décliner les mesures par niveaux ISPS.
- profil des utilisateurs de l'accès réservé :
 - à des piétons (visiteurs, personnels) ;
 - à des véhicules (légers, poids lourds) ;
 - au mode ferroviaire ;
 - à d'autres modes (deux roues) ;
 - décliner les mesures par niveaux ISPS.
- modalités horaires :
 - fermé en permanence ;
 - activable pendant les heures d'exploitation du terminal ;
 - activable pendant les opérations commerciales du navire ;
 - ouvert sur demande auprès de l'ASIP ;
 - décliner les mesures par niveaux ISPS.
- qui gère l'accès (qui ouvre sur place l'accès) :

- gardien (n'ayant pas le statut d'ACVS) ;
 - ACVS ;
 - ASIP.
- qui donne l'autorisation d'emprunter l'accès :
 - gardien (n'ayant pas le statut d'ACVS) ;
 - ACVS ;
 - ASIP.

Fiche 5.3.4 – Système de signalisation des interdictions de pénétrer en ZAR

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Système de signalisation des interdictions de pénétrer en ZAR et, le cas échéant, dans les secteurs ;

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Mettre dans le PSIP une illustration des panneaux utilisés.

Le panneautage doit respecter plusieurs objectifs :

- il doit porter à la connaissance des personnes entrant en ZAR la liste des objets prohibés (les armes à feu ; les explosifs ; les dispositifs incendiaires ; les articles dont la détention, le port et le transport est interdit par la législation maritime française ou communautaire ou en vertu d'un accord international maritime en vigueur auquel la France fait partie) ;
- il doit être visible pour les personnes entrant en ZAR, plus particulièrement pour les personnes passant par le PIF ;
- une personne entrant en ZAR doit obligatoirement signaler aux ACVS les articles prohibés qu'elle transporte ;
- il permet d'indiquer les règles de circulation lorsque les dispositifs d'inspection-filtrage sont inactifs ;
- il peut faire référence à l'arrêté préfectoral créant la ZAR et à d'autres textes réglementaires (Code des transports en particulier) ;
- il doit préciser la qualité des restrictions d'accès et de circulation ainsi que les sanctions éventuelles encourues ;
- une signalisation multilingue devrait être étudiée ;
- les pancartes devraient être apposées en périphérie de manière judicieuse et répétée ; et installées à chaque point d'accès de la ZAR ;
- il devrait être visible de jour comme de nuit.

Fiche 5.3.5 – Règles de surveillance (humaines et/ou par système automatique de vidéo-surveillance), pour chaque niveau ISPS

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Règles de surveillance (humaines et/ou par système automatique de vidéo-surveillance), pour chaque niveau ISPS ;

Les objectifs :

Principe général :

Définir par niveaux ISPS, les mesures de surveillance de la ZAR qui s'appuieront sur :

- de l'éclairage ;
- des rondes de sûreté ;
- de la vidéoprotection.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Règles pour l'éclairage :

L'exploitant peut s'appuyer sur de l'éclairage pour surveiller le terminal. Il faudra alors :

- localiser l'éclairage sur un plan de masse ;
- préciser s'il fonctionne 24h/24h, pendant les opérations commerciales, uniquement la nuit ou pendant les opérations d'exploitation ;
- préciser si l'éclairage vient en appui des clôtures, de la vidéosurveillance, de rondes ;
- préciser si l'éclairage est renforcé aux niveaux 2 et 3 ISPS (par quel moyen et avec quelle intensité ?).

Règles pour les visites et les rondes de sûreté :

Voir fiche 5.3.1 concernant les visites de sûreté. Veiller à la cohérence des informations qui sont renseignées dans la fiche 4.2.2.

Le PSIP doit préciser :

- si les visites de sûreté sont effectuées avant l'activation de la ZAR et/ou avant l'arrivée du navire ;
- la fréquence des rondes pour chaque niveau ISPS ;
- les effectifs en charge d'effectuer ces rondes (ASIP, contremaître, ACVS...) par niveaux ISPS ;
- les objectifs poursuivis dans le cadre des rondes (rechercher des articles prohibés, colis suspects ; rechercher des intrusions ; vérifier l'état du matériel dédié à la sûreté) ;
- si le parcours des rondes est aléatoire ou non.

Il faudra prévoir d'enregistrer les rondes et de noter les événements rencontrés dans ce cadre.

Règles relatives à la vidéoprotection :

Le recours à la vidéoprotection n'est pas obligatoire pour une ZAR, sauf si l'ESIP l'impose. Cependant, elle est fort utile lorsque la surface du terminal est importante et lorsqu'il n'y a pas de PIF à chaque point d'accès.

Lorsque l'exploitant utilise un tel dispositif, le PSIP doit être très précis sur son usage réel, à savoir :

- si les images sont enregistrées en permanence ;
- si la diffusion des images est en continu et sans différé ;
- si la vidéo est activée uniquement lorsqu'elle détecte un événement ;
- si elle sert à effectuer une levée de doute après avoir eu une alarme sur la vidéo, et si une personne se rend sur le lieu où l'événement a été détecté ;
- préciser le champ de vision (angle de visualisation de 90°, 180°, 360°...) et les secteurs visualisés ;
- mentionner la qualité et la résolution de l'image notamment en fonction de la météo et la nuit ;
- si la vidéo permet d'assister le contrôle de flux de véhicules ou de personnes ;
- s'il est possible de zoomer sur une zone ;
- si la personne derrière les écrans de contrôle sait ce qu'elle doit observer (objets suspects, personnes ou véhicules non identifiés) ;
- préciser la durée de stockage des images vidéo (la conservation des images est limitée à 30 jours sauf en cas d'enquête) ;
- localiser l'endroit où s'effectue le report des images ;
- définir les horaires des services du personnel qui exploite la vidéo ;
- si la personne derrière les écrans de contrôle doit enfin savoir ce qu'elle doit observer (objets suspects, personnes ou véhicules non identifiés).

L'usage de la vidéo sera aussi décliné par niveaux ISPS.

En annexe n° 8 est proposé un modèle de tableau pour présenter les règles de surveillance de la ZAR.

Lorsqu'une vidéosurveillance existe, celle-ci doit être signalée. Elle ne peut être mise en œuvre que sous certaines conditions prévues par les lois et règlements (information du public, enregistrements, etc.) qui devraient être cités en référence sur l'affichage. Ainsi, un exploitant devrait préciser si les autorités publiques lui ont délivré une autorisation d'installation de caméras et s'il dispose de droits d'accès et de conservation des images pour une durée ne pouvant pas dépasser 1 mois.

Fiche 5.3.6 – Règles de fonctionnement des différents PIF

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

*– Règles de fonctionnement des différents points d'inspection-filtrage selon les niveaux ISPS (horaires, effectifs, règles d'inspection-filtrage, procédures d'exploitation des équipements) ;
Arrêté du 4 juin 2008, modifié par arrêté du 1^{er} avril 2015*

Les objectifs :

Principe général :

Les modifications apportées par l'arrêté du 1^{er} avril 2015 ont aménagé les modalités de l'inspection-filtrage, dans le but d'améliorer la fluidité des accès aux terminaux. Le nouvel arrêté permet de clarifier le partage de responsabilité entre exploitant de terminal et armement. Il introduit également des obligations nouvelles pour les exploitants de terminaux rouliers.

L'inspection-filtrage a pour but de détecter des articles prohibés ou des personnes non autorisées. L'inspection-filtrage peut mettre en œuvre une ou plusieurs opération(s) :

- un contrôle de sûreté ;
 - ouverture de la chose examinée (paquet, coffre de véhicule) ou d'un vêtement couvrant (manteau, pardessus) par leur propriétaire ;
 - examen effectué avec des moyens de détection (magnétomètre à main, endoscope, portique, etc.) ;
 - observation visuelle attentive ;
- un lever de doute :
 - une palpation de sécurité (avec le consentement préalable de la personne, par un agent de même sexe) ;
 - une fouille d'un bagage, d'un colis, d'un véhicule (de son intérieur, coffre), d'une remorque ou d'une unité de charge (avec l'accord préalable de la personne)

Le contrôle de sûreté s'apparente à un contrôle visuel qui permet de contrôler en masse des véhicules et de personnes. Il doit être plus fluide comparativement à un lever de doute, ces opérations demandent aux ACVS de dégager plus de temps pour effectuer une fouille de bagages, une palpation de sécurité. Le contrôle de sûreté et le lever de doute sont deux opérations distinctes qui doivent respecter des taux de contrôle. Cependant, l'existence d'un doute lors de contrôle de sûreté doit toujours entraîner une fouille ou une palpation de sécurité. Il s'agit alors d'une levée de doute.

Un taux pour les contrôles de sûreté et un deuxième taux pour le lever de doute sont fixés par arrêté préfectoral en application de l'article 49. Néanmoins, le taux de contrôle de lever de doute est moins élevé par rapport au taux fixé pour les contrôles de sûreté.

Les taux sont déclinés par types d'accédants, avec possibilité de regrouper les catégories d'accédants.

Les taux doivent être déclinés par niveau ISPS.

Principe particulier pour les exploitants :

Le PSIP doit décrire par niveaux ISPS, les règles de fonctionnement du ou des PIF, pour les points suivants :

- a) les horaires ;
- b) les effectifs ;
- c) la liste des équipements et utilisation de ces équipements ;
- d) la matérialisation de l'interdiction de passage lorsque le PIF est inactif ;
- e) les règles applicables aux personnes ;
- f) les règles applicables aux véhicules ;
- g) les règles applicables à la cargaison ;
- h) les règles applicables à la manutention ;
- i) les règles applicables à la livraison des provisions de bord ;
- j) le partage des responsabilités entre exploitant de terminal et armement.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

a) Les horaires : le PSIP précisera l'amplitude horaire pendant lequel le PIF est activé. Celui-ci doit être activé au moins une heure avant l'arrivée de l'escale et pendant toute la durée de l'escale ;

b) Dénombrer les effectifs affectés à chaque PIF par niveaux ISPS, y compris le personnel féminin. En cas de sous-traitance du personnel ACVS, se référer également à la fiche 4.2.8 ;

c) Le PSIP doit lister les équipements de sûreté disponibles à chaque PIF :

- équipement portatif de détection de masses métalliques sur les personnes ;
- dispositif permettant de procéder à l'abri des regards aux palpations de sécurité ;
- table de dépose permettant de procéder aux fouilles des bagages ;
- moyen de communication d'urgence pour alerter les forces de l'ordre ;
- si le terminal a plus de 350 000 passagers par an embarquant, le PIF comporte un ou des équipements d'imagerie radioscopique d'inspection des bagages, et un ou des portiques de détection des masses métalliques sur les personnes ainsi que les outils nécessaires au calibrage de ces équipements et l'outil servant au calibrage ;
- une installation accueillant des navires rouliers embarquant également des passagers doit disposer d'une capacité de détection de matières explosives déterminée par l'évaluation de sûreté

d) Indiquer les règles de circulation lorsque les dispositifs d'inspection-filtrage sont inactifs ;

e) Le PSIP doit mentionner les règles applicables aux personnes, à savoir :

- assurer de manière continue et aléatoire l'inspection-filtrage d'une partie des personnes, de leurs bagages et des marchandises qu'ils transportent (selon les taux d'IF définis par arrêté préfectoral) ;
- interdire l'accès à toute personne refusant de se soumettre ou de soumettre ses bagages ou son véhicule à l'inspection-filtrage ;
- alerter immédiatement les services de la police ou de la gendarmerie nationales et, le cas échéant, les navires présents à quai, lorsqu'une personne ou un véhicule pénètre en zone d'accès restreint en s'étant soustrait à l'inspection-filtrage ou en étant présumé porteur d'un article prohibé ;
- prévoir des procédures pour les personnes qui produisent un certificat médical et les personnes à mobilité réduite ;
- prévoir une palpation obligatoire sur les personnes qui ont provoqué une alarme des équipements de détection ;
- fouiller manuellement les bagages quand ceux-ci ont provoqué une alarme des équipements de détection ou quand le résultat de leur examen a généré un doute de l'opérateur. La fouille manuelle n'est effectuée qu'avec l'accord de la personne concernée ;

f) Le PSIP doit stipuler les règles applicables aux véhicules. L'inspection-filtrage des véhicules comprend l'un au moins des contrôles :

- le contrôle de sûreté du véhicule ;
- la fouille du véhicule ;
- la fouille des bagages transportés par le véhicule ; ;

Les contrôles de sûreté et les opérations de fouille réalisés dans l'habitacle, le coffre ou les compartiments de stockage des véhicules de tourisme et de leur attelage, des camping-cars et des caravanes requièrent

l'accord de leur conducteur ;

Les véhicules des services de police nationale, de gendarmerie nationale, de douane et les véhicules qu'ils accompagnent ne sont pas contrôlés ;

g) Le PSIP doit déterminer les règles applicables à la cargaison :

Le contrôle de la cargaison est effectué quelle que soit l'unité de charge. Il comprend le rapprochement des documents commerciaux décrivant la cargaison avec l'information préalablement reçue concernant les marchandises à charger sur le navire. Il comprend en outre l'une au moins des vérifications suivantes :

- contrôle de sûreté incluant au moins le contrôle visuel de l'intégrité de l'unité de charge ;
- fouille de l'unité de charge, et éventuellement de la cargaison ;
- en particulier, les procédures pour les conteneurs (contrôle des scellés, conteneurs vides) ;

h) Le PSIP doit définir les règles applicables à la livraison des provisions de bord :

Malgré les modalités de contrôles appliqués à la ZAR,, le PSIP doit définir une procédure pour superviser la livraison des provisions de bord (voir fiche 5.5.6), conformément au Code ISPS, paragraphe B/16.8.10. Pour cela, il est nécessaire de prévoir la réception par le bord en un point convenu de l'IP en liaison avec le navire ;

i) Le PSIP doit préciser les règles applicables à la manutention :

Conformément au Code ISPS, paragraphe B/16.8.9, le PSIP doit déterminer une procédure visant à superviser la manutention de la marchandise (voir fiche 5.5.7), en particulier si la manutention s'opère à l'intérieur de la ZAR.

j) Le partage de responsabilité entre exploitant de terminal et armement :

Par définition, l'introduction d'articles prohibés en zone d'accès restreint ou à bord d'un navire est interdite, sauf s'ils ont été déclarés et leur transport est autorisé par les lois et règlements en vigueur, et pour ce qui concerne le navire, par son capitaine.

Cependant le PSIP peut autoriser l'accès et la circulation du transport d'armes (armes de chasse) dans la ZAR. Cela implique qu'un protocole d'accord mutuel soit pris entre l'exploitant du terminal et l'armateur, afin de mettre en cohérence leurs mesures respectives. Ce protocole précise les articles prohibés acceptés à bord du navire et placés dans un local sécurisé ou dans un coffre de véhicule verrouillé.

Fiche 5.3.7 – Règles de vérifications documentaires

L'arrêté du 4 juin 2008 demande de définir les modalités de vérification documentaire pour chaque catégorie d'accédant à la ZAR ainsi que pour les véhicules. Cette fiche vient s'articuler avec la fiche 5.3.3 ; le but étant de savoir comment l'exploitant respecte les objectifs de l'article 13 de l'arrêté du 4 juin 2008 rappelé dans la fiche 5.3.3.

Le cadre réglementaire :

Arrêté du 4 juin 2008, modifié par arrêté du 1^{er} avril 2015, Sections 2 à 10.

Les objectifs :

Principe général :

Les modifications apportées à l'arrêté du 4 juin 2008 par l'arrêté du 1^{er} avril 2015 ont permis d'alléger les modalités des contrôles d'accès. L'exploitant continue de vérifier systématiquement le titre de transport ou de circulation. Il peut continuer de vérifier la concordance entre le nom porté sur le titre de transport ou de circulation et celui figurant sur un document officiel ou une pièce d'identité ; mais cette vérification n'est plus

systematique au niveau 1 isps.

Malgré ces allègements, le PSIP doit définir les modalités de vérification documentaire pour chaque catégorie d'accédant et leur véhicule (en annexe n° 7 sont rappelées les catégories de personnes et de véhicules). Tout en respectant les sections 2 à 10 de l'arrêté du 4 juin 2008, le PSIP devrait rappeler :

- les modalités de contrôle systématique sur les titres de circulation (permanent et temporaire) ;
- les modalités de concordance avec une pièce d'identité ;
- les modalités de concordance avec le numéro d'immatriculation du véhicule ;
- les cas de dispense de contrôle en cas d'urgence ;
- les modalités de contrôle du titre de transport ;
- les modalités de contrôle pour les situations particulières (des bagages non accompagnés, convention entre l'armateur et l'exploitant relative aux visites de sûreté).

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

L'exploitant pourrait présenter sous forme de tableau ses modalités de contrôle d'accès (contrôle documentaire) et d'inspection-filtrage, comme suivant :

	Modalités de contrôle d'accès par niveaux ISPS	Rappel des taux d'inspection-filtrage par niveaux ISPS			
Par type d'accédant (*)		Contrôle de sûreté des personnes	Contrôle de sûreté des véhicules utilisés par ces personnes	Lever de doute impliquant la palpation de sécurité sur les personnes	Lever de doute impliquant la fouille des bagages, des colis, des véhicules (intérieur, coffre), d'une remorque ou d'une unité de charge

(*) Les catégories peuvent être regroupées sous conditions d'avoir étudié le cas de chacune d'elles.

Fiche 5.3.8 – Pour les voies ferrées portuaires

Pas de recommandation particulière, reprendre le cadre de l'arrêté.

Fiche 5.3.9 – Pour les ZAR d'installation portuaire auxquelles une ou plusieurs ZAR portuaires donnent accès

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Pour les voies ferrées portuaires, joindre en annexe, le cas échéant, le document conventionnel avec

l'exploitant qui détaille la répartition des tâches ;

– Pour les ZAR d'installation portuaire auxquelles une ou plusieurs ZAR portuaires donnent accès, détail de la répartition des contrôles d'accès entre l'exploitant et l'autorité portuaire ; mention de la référence précise des parties du plan de sûreté de ces installations portuaires dans lesquelles figurent les procédures de contrôles complémentaires ; joindre les conventions entre l'autorité portuaire et l'installation portuaire ;

Les objectifs :

Principe général :

Pas de recommandation particulière.

Veiller à ce que la répartition de tâches entre l'exploitant et l'opérateur ferroviaire d'une part ; et l'exploitant et l'autorité portuaire d'autre part, fasse l'objet d'une convention annexée au PSIP.

Fiche 5.3.10 – Procédures d'entretien des clôtures, des équipements d'inspection-filtrage et de tout autre équipement périmétrique et de contrôle d'accès

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Procédures d'entretien des clôtures, des équipements d'inspection-filtrage et de tout autre équipement périmétrique et de contrôle d'accès ;

Les objectifs :

Principe général :

On pourra s'appuyer sur la procédure relative au contrôle de l'état du matériel défini dans la fiche 8 de l'arrêté du 22 avril 2008.

Penser à annexer au PSIP toute convention ou contrat définissant une prestation de sous-traitance concernant l'entretien des dispositifs de sûreté.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

En complément des procédures d'entretien des dispositifs de sûreté, il faut préciser les règles d'exploitation du PIF, qui sont tenues à jour grâce à un compte rendu mensuel d'exploitation du PIF, qui enregistre :

-
- le nombre journalier de personnes (répartition entre passagers et autres personnes) et de véhicules traités, conformément aux taux de contrôles imposés par le Préfet de département ;
- le nombre journalier de fouilles de véhicules, de bagages et de palpations de sécurité dont les palpations provoquées par l'alarme d'un moyen de détection, ventilé selon le dispositif de détection ;
- les principaux événements survenus, mesures correctives si les événements d'exploitation ont révélé un dysfonctionnement.

Fiche 5.3.11 – Procédures appliquées en cas d'incident de sûreté (pénétration irrégulière, panne des équipements d'inspection-filtrage, détérioration de clôtures, etc.)

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.3. Protection et contrôle des accès en ZAR

– Procédures appliquées en cas d'incident de sûreté (pénétration irrégulière, panne des équipements d'inspection-filtrage, détérioration de clôtures, etc.) ;

Les objectifs :

Principe général :

Reprendre le cadre de l'arrêté.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Veiller à la cohérence avec les fiches réflexes relatives aux conduites à tenir en cas d'alerte et avec la fiche 8 qui prévoit une procédure d'analyse de chaque incident de sûreté.

En cas d'incident suite à une intrusion dans la ZAR, la procédure devra décrire :

- la chaîne d'alerte entre la personne qui détecte l'intrusion et l'ASIP ;
- s'il convient d'appeler des renforts (délais de réaction pour l'intervention des renforts) ;
- s'il faut alerter les forces de l'ordre.

En cas d'incident suite à une panne des équipements d'inspection-filtrage, le PSIP :

- précisera si le matériel peut être remplacé et réparé ;
- définira un délai d'intervention pour réparer la panne ;
- prévoira un contrat avec le prestataire en charge de la maintenance du matériel ;
- mentionnera si l'exploitant dispose d'un stock de matériel permettant de se prémunir d'une panne éventuelle ;
- décrira les procédures alternatives à mettre en œuvre en attendant l'intervention d'un réparateur.

En cas d'incident suite à une détérioration de la clôture, le PSIP :

- détaillera les solutions palliatives pour surveiller la détérioration de la clôture en attendant sa réparation (rondier, surveillance vidéo...) ;
- exposera les modalités pour réparer la clôture dans les plus brefs délais ;
- prévoira un contrat avec le prestataire en charge de réparer la clôture ;
- définira un délai d'intervention.

Fiche 5.4 – Gestion des titres de circulation

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.4. Gestion des titres de circulation

- Procédures de délivrance et restitution des titres de circulation ;
- Méthodes d'information et sensibilisation aux règles de sûreté pour les personnes recevant des titres de circulation ;
- Procédures de coordination, le cas échéant, entre les ZAR situées en dehors d'une installation portuaire et les ZAR situées dans une installation portuaire ;
- Protection des systèmes d'information et des équipements de fabrication des titres ;
- Procédures de désactivation des titres inutilisés ;
- Détail de la répartition des tâches avec les exploitants d'installation portuaire en cas de mutualisation de la délivrance des titres de circulation avec mention de la référence précise des parties du plan de sûreté des installations portuaires concernées dans lesquelles se trouve la procédure de délivrance.

Code des transports

Article R. 5332-36 : La circulation des personnes et des véhicules dans une zone d'accès restreint est subordonnée au port apparent de l'un des titres de circulation définis dans la présente sous-section.

Article R. 5332-49: Les agents chargés des visites de sûreté qui ont été agréés à cette fin se voient délivrer le titre de circulation mentionné au I de l'article R. 5332-37. Ils portent en permanence de manière apparente, outre ce titre, un signe distinctif de leur fonction.

Arrêté du 4 juin 2008 relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation

Art. 4 – Titres et documents. – Les documents permettant d'accéder en zone d'accès restreint sont...

Art. 8. – Obligations attachées à la détention d'un titre de circulation de personne.

Art. 9. – Obligations attachées à la détention d'un titre de circulation de véhicule.

Les objectifs :

Principe général :

Reprendre le cadre de l'arrêté.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Définir les procédures de délivrance et restitution des titres de circulation (et procédures en cas de perte ou de vol) :

Pour les personnes :	Pour les véhicules :
- titres de circulation permanents ;	- titre de circulation de véhicule ;
- titres de circulation temporaires ;	- document de livraison ou d'enlèvement pour les véhicules apportant ou venant chercher une cargaison ou des provisions de bord ;
- titres de transport ;	- titre de transport des véhicules embarquant.

La procédure visera à définir :

- les conditions d'attributions des titres de circulation ;
- les demandes d'obtention d'un titre de circulation ;
- les modalités de remise et d'activation, le cas échéant, du titre de circulation ;
- en cas de perte ou de vol, qui il faut informer, qui désactive le titre de circulation le cas échéant ;
- la durée de validité du titre de circulation.

Préciser les méthodes d'information et de sensibilisation aux règles de sûreté pour les personnes recevant des titres de circulation :

- a) Rappeler des obligations attachées à la détention d'un titre de circulation de personne :
- a.1) accéder uniquement aux ZAR autorisées ;
 - a.2) les agents chargés des visites de sûreté portent de manière apparente leur titre de circulation et ont en outre un signe distinctif de leur fonction ;
 - a.3) port du titre de circulation de façon visible pendant la durée du séjour ;
 - a.4) ne pas prêter son titre de circulation à un tiers ;
 - a.5) signaler dans les plus brefs délais la perte ou le vol d'un titre de circulation ;
 - a.6) restituer le titre de circulation lorsqu'il arrive à la fin de la période de validité ;
- b) Rappeler les obligations attachées à la détention d'un titre de circulation de véhicule :
- b.1) ne pas permettre à une personne non autorisée de pénétrer dans la zone d'accès restreint en évitant les contrôles au moyen de ce véhicule ;
 - b.2) apposer le titre de manière apparente sur la lunette avant du véhicule pendant toute la durée du séjour dans la zone d'accès restreint ;
 - b.3) veiller à ce qu'aucune personne n'introduise un article prohibé à l'intérieur du véhicule ;
 - b.4) sans préjudice de dispositions liées à la sécurité, pendant les périodes où aucune personne ne se trouve à bord du véhicule, maintenir fermés à clé l'habitacle et le coffre du véhicule pendant toute la durée du séjour dans la zone d'accès restreint ;
 - b.5) ne pas permettre son utilisation pour un autre véhicule que celui pour lequel il a été délivré ;
 - b.6) signaler dans les plus brefs délais la perte ou le vol (y compris en cas de vol du véhicule) de son titre de circulation au service qui le lui a délivré ;
 - b.7) restituer le titre de circulation au service qui le lui a délivré, directement ou par l'intermédiaire de l'entreprise qui en a fait la demande de délivrance ; les titres de circulation sont remis dès que les motifs qui ont conduit à leur délivrance ont disparu ou dès la fin de leur période de validité ;
- c) La procédure définira si la remise du titre de circulation a fait l'objet d'une sensibilisation au préalable, via :
- c.1) un cours théorique et éventuels des tests à l'issue du cours ;
 - c.2) un dépliant précisant les consignes à respecter lors de la remise du titre de circulation ;
 - c.3) une attestation de responsabilité à signer après que le titulaire du titre de circulation ait pris connaissance des obligations à respecter.

Préciser les procédures de coordination entre les ZAR situées en dehors d'une installation portuaire et les ZAR situées dans une installation portuaire.

Prévoir des procédures de protection des systèmes d'information et des équipements de fabrication des titres. La procédure s'attachera à préciser :

- quelles sont les personnes ayant accès au système permettant de fabriquer des titres de circulation ;

- si les données informatiques sont protégées, sauvegardées.

Définir les procédures de désactivation des titres inutilisés ; la procédure déterminera :

- si les titres de circulation sont désactivés lorsque la fin de validité du titre arrive à son terme ;
- si une concordance est faite entre la durée de validité du titre de circulation et la fin de validité de l'habilitation délivrée à une personne.

Détailler la répartition des tâches avec les exploitants d'installation portuaire pour la délivrance mutualisée des titres de circulation, si nécessaire.

Enfin, rappeler les obligations de porter les badges de manière apparente (pour toutes les catégories de personnes ; utiliser des couleurs différentes selon le type de badge afin de faciliter la reconnaissance).

Fiche 5.5 – Zones non librement accessibles

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004, sections :

A14.2.2 contrôler l'accès à l'installation portuaire

A14.2.3 surveiller l'installation portuaire, y compris la ou les zones de mouillage et d'amarrage

A16.3.2 les mesures destinées à empêcher l'accès non autorisé à l'installation portuaire, aux navires amarrés dans l'installation et aux zones d'accès restreint de l'installation

A14.2.4 surveiller les zones d'accès restreint pour vérifier que les seules personnes autorisées y ont accès

A.14.2.5 superviser la maintenance de la cargaison

A.16.3.12 des mesures destinées à garantir la protection effective de la cargaison et du matériel de maintenance de la cargaison dans l'installation portuaire

B16.8.9 les procédures relatives à la maintenance de la cargaison

A14.2.6 superviser la maintenance des provisions de bord

B16.8.10 les procédures concernant la livraison des provisions de bord

A16.3.1 les mesures visant à empêcher l'introduction, dans l'installation portuaire ou à bord du navire, d'armes, de substances dangereuses et d'engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence n'est pas autorisée

A.16.3.15 des procédures pour faciliter les congés à terre pour le personnel du navire ou les changements de personnel, de même que l'accès des visiteurs au navire, y compris les représentants des services sociaux et des syndicats des gens de mer

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.5. Zones Non Librement Accessibles

Il peut exister au sein de l'installation portuaire des zones non librement accessibles au public qui ne sont pas des ZAR (...)

Le plan de sûreté de l'installation portuaire les décrit (plan, clôtures, accès), détaille leurs règles de fonctionnement (contrôle d'accès, circulation) et les articulations avec les règles de sûreté des ZAR adjacentes, en démontrant que la sûreté de l'installation portuaire dans son ensemble et de chaque installation portuaire adjacente n'est pas dégradée, quel que soit le niveau de sûreté.

Préambule

Avant d'entrer dans le détail des mesures à définir dans le cadre de la fiche 5.5, le développement, ci-dessous, est une tentative d'explication de la notion de ZNLA et son usage dans les installations portuaires. Elle sera affinée à l'occasion de l'évolution réglementaire.

En réalité, par principe une installation portuaire, qui n'est pas couverte par une ZAR, est une Zone Non Librement Accessible (ZNLA). Sachant qu'une installation portuaire est le lieu où s'effectue l'interface entre le navire et le port.

Lorsqu'une ZAR ne couvre pas l'entière surface de l'IP, la surface restante devient une ZNLA.

Plus rarement, une ZNLA peut se situer en dehors d'une IP, tout en restant au sein de la Limite de Sûreté Portuaire. Il peut s'agir de points névralgiques essentiels au fonctionnement du terminal. Bien que situés hors IP et qu'il n'y ait pas de contact direct avec le navire, l'exploitant peut estimer primordial de mettre en place des mesures de protection pour ces biens essentiels.

La définition et le périmètre d'une ZNLA sont à géométrie variable et nécessitent des mesures de sûreté moins restrictives en comparaison d'une ZAR. Néanmoins, lorsque les périmètres de la ZNLA et de l'IP se superposent, **le Code ISPS annexé au RE N° 725/2004, section A/14, impose les mesures essentielles suivantes :**

- contrôler l'accès à l'installation portuaire ;
- surveiller l'installation portuaire, y compris la ou les zones de mouillage et d'amarrage ;
- superviser la manutention de la cargaison ;
- superviser la manutention des provisions de bord ;
- empêcher l'introduction, dans l'installation portuaire ou à bord du navire, d'armes, de substances dangereuses et d'engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence n'est pas autorisée.

Au regard des exigences du RE N° 725/2004, le régime des mesures de sûreté à déterminer pour une ZNLA est avant tout assimilable à une « propriété privée » où l'exploitant va définir les mesures de protection qu'il juge nécessaire. Les mesures de sûreté attendues doivent s'appuyer principalement sur la vigilance du personnel de l'exploitant et sur leur capacité à réagir quand une personne pénètre dans l'IP sans autorisation d'accès.

Le préambule du chapitre 5 a déjà précisé les fiches qu'il convient de renseigner selon 4 cas de figure :

- IP = ZAR, la ZAR est permanente ;
- IP = ZAR, la ZAR est permanente, mais activée uniquement en présence d'une escale ;
- ZAR ≠ IP, la surface non couverte par la ZAR est assimilable à une ZNLA ;
- IP est non sensible et n'est pas couverte par une ZAR. L'IP est assimilable à une ZNLA.

Un dernier cas de figure doit être envisagé. Il s'agit d'une ZNLA qui se situe en dehors de l'IP. Vraisemblablement ce type de ZNLA a pour objectif de protéger un point névralgique identifié lors de la rédaction de l'ESIP. L'exploitant doit alors définir des mesures de sûreté en s'appuyant sur la fiche 5.5 (de 5.5.1 à 5.5.8).

Fiche 5.5.1 – Plan de masse

Les objectifs :

Principe général :

Décrire sur un plan de masse, le périmètre de la ZNLA, les clôtures et les accès. Pour plus de précisions, la procédure se basera sur la fiche 4.1 relative au « plan détaillé de l'installation portuaire ».

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Dans la plupart des cas de figure, les périmètres d'une installation portuaire et d'une ZNLA se confondent. La procédure est donc sans objet et se référera à la fiche 4.1.

Lorsque les périmètres de l'installation portuaire et de la ZNLA ne sont pas superposables, il peut être opportun d'avoir un plan de masse détaillant les mesures de protection de la ZNLA qui se différenciera du plan de masse figurant à la fiche 4.1.

Fiche 5.5.2 – Procédure de vérification d'autorisation d'accès

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A/16.3.2 les mesures destinées à empêcher l'accès non autorisé à l'installation portuaire, aux navires amarrés dans l'installation et aux zones d'accès restreint de l'installation

Les objectifs :

Principe général :

Être capable d'identifier les personnes autorisées à accéder :

- au navire ;
- à l'installation portuaire, en particulier lors de l'escale d'un navire.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Les mesures de sûreté appliquées à l'installation portuaire sont un prolongement des mesures de sûreté du navire. Avant de pouvoir identifier les personnes ayant vocation à rejoindre le navire, il faut au préalable identifier les personnes autorisées à pénétrer dans l'IP.

La capacité de l'exploitant à vérifier les autorisations d'accès des personnes présentes sur le terminal s'applique en particulier en présence du navire.

L'exploitant devrait définir une procédure permettant de savoir à l'avance l'identité des personnes souhaitant entrer dans le terminal. Puis, il devrait prévoir une procédure pour vérifier la concordance d'identité avec les personnes présentes sur le terminal et les personnes attendues le jour de l'escale.

Pour annoncer à l'avance l'identité des personnes souhaitant accéder au terminal, l'exploitant peut :

- s'appuyer sur la procédure « permettant d'aider les agents de sûreté du navire à confirmer l'identité des personnes cherchant à monter à bord du navire » figurant à l'annexe 5 ;
- utiliser des badges professionnels, des vêtements reconnaissables pour le personnel de l'entreprise ;
- des badges visiteurs.

Le rapprochement d'identité peut s'effectuer :

- au poste d'accueil de l'entreprise ; l'accueil délivre alors un badge pour rejoindre le terminal ;
- à un poste de garde situé à l'entrée du terminal ;
- à l'occasion de rondes de sûreté aléatoires sur le terrain.

Si jamais le navire reste en attente dans le terminal en dehors des opérations commerciales, alors que le terminal est fermé et qu'il n'y a aucun gardien pour vérifier l'identité des personnes accédant au terminal, l'exploitant devra détailler une procédure pour diffuser des codes d'accès ou des clés pour ouvrir les portes d'accès au terminal.

Les vérifications d'autorisation d'accès ne sont pas systématiques et elles s'opèrent de manière aléatoire.

L'exploitant peut s'appuyer sur une main courante afin d'enregistrer les noms des personnes entrant et sortant du terminal pour prouver l'application de sa procédure.

Si l'arrivée d'une personne n'a pas été anticipée ou annoncée au préalable, l'exploitant pourra demander au commandant du navire s'il donne l'autorisation à cette personne d'accéder au navire.

La procédure ne s'applique pas uniquement aux personnes, elle couvre également des modes de transport (véhicules légers, poids lourds, mode ferroviaire et des barges). L'exploitant devrait être prévenu de l'arrivée d'un mode de transport afin de l'autoriser à entrer dans le périmètre de l'installation portuaire, en présence d'une escale. L'exploitant peut envisager un système de « rendez-vous » où le transporteur précise le nom de son entreprise et l'horaire de son arrivée.

L'exploitant pourra :

- différencier ses mesures pendant les opérations commerciales (en présence du navire) et en dehors des opérations commerciales (hors présence du navire) ;
- décliner ses mesures par niveaux ISPS ;
- préciser la provenance du personnel en charge de vérifier les autorisations d'accès ;
- prévoir un délai de mise en œuvre des mesures de sûreté en cas de passage au niveau 2 ou 3 ISPS.

Fiche 5.5.3 – Mesures combinées de surveillance et contrôle d'accès

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A/14.2.2 contrôler l'accès à l'installation portuaire

Section A/14.2.3 surveiller l'installation portuaire, y compris la ou les zones de mouillage et d'amarrage

Les objectifs :

Principe général :

- définir des mesures de contrôle d'accès ;

- définir des mesures de surveillance ;
- la combinaison de ces deux mesures a pour objectif d'accroître la vigilance du personnel de l'exploitant et leur capacité à réagir quand une personne pénètre dans l'IP sans autorisation d'accès ;
- les mesures doivent être déclinées par niveaux ISPS. En particulier, à partir du niveau 2 ISPS, le terminal devra être étanche (fermé).

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

a) Décliner les mesures de sûreté par niveaux ISPS :

Comme le rappelle la fiche 4.2.2, la réglementation demande de décliner les mesures de sûreté selon 3 niveaux :

- Niveau 1 : mesures minimales appropriées appliquées en permanence ;
- Niveau 2 : mesures additionnelles appropriées à maintenir pendant une période déterminée, car le risque est accru ;
- Niveau 3 : mesures spéciales et temporaires, car l'incident est probable ou imminent.

Au niveau 1, ce sont les mesures appliquées en permanence, soit les mesures minimales du PSIP. Ensuite, avec l'élévation du niveau ISPS, caractérisant une situation d'urgence, l'exploitant doit préciser s'il convient d'intensifier les effectifs et/ou les tâches de sûreté. Les mesures de sûreté sont renforcées lors d'un passage au niveau 2 ou 3 ISPS ;

b) Délai de mise en œuvre des mesures renforcées en cas d'élévation du niveau ISPS :

Comme rappelé en annexe 8, même s'il n'y a pas d'obligation réglementaire, l'exploitant examine sous quel délai il peut accroître ses mesures de sûreté, en cas de changement de niveau ISPS. Par exemple :

- de manière immédiate : l'ASIP intensifie ses rondes ;
- sous 24h – 48h : un prestataire de sûreté prend le relais, la prestation est définie dans un contrat ;
- au-delà de 48h : les moyens sont encore intensifiés... ;

c) Mesures à appliquer pendant l'escale et en dehors d'une escale :

Les mesures de sûreté de l'installation portuaire sont un prolongement des mesures de sûreté du navire. C'est pourquoi l'exploitant devrait activer ses mesures de sûreté 1 ou 2 heure(s) avant l'arrivée de l'escale et pendant toute la durée de l'escale, en incluant les temps d'attente. Avant l'arrivée du navire, l'exploitant devrait procéder à une ronde sur le terminal afin de rechercher des articles prohibés, des colis suspects ou d'éventuelles intrusions.

En dehors d'une escale de navire, l'exploitant peut désactiver ou dégrader ses mesures de sûreté comparativement aux mesures appliquées en cas de présence d'un navire en bord à quai ;

d) Veiller à la cohérence des informations avec le chapitre 4 :

Les fiches du chapitre 4 décrivent les missions des effectifs affectés à des tâches de sûreté, les moyens et prestations sous-traitées, ainsi que les dispositifs de protection localisés sur un plan de masse. Dans la mesure où ces informations sont redondantes avec celles de la présente fiche 5.5.3, l'exploitant doit donc veiller à la cohérence des informations qui seront renseignées dans ces différentes fiches ;

e) Mesures de contrôle d'accès :

Définir la protection périmétrique retenue :

- l'exploitant pourra s'appuyer sur la fiche 5.3.2 pour qualifier ses mesures de sûreté physique, comme attendu ci-après ;
- type de clôture (mobile, fixe, grillagée...) ;
- éléments caractéristiques (double clôture, profondeur...) ;
- autres équipements périmétriques (barrières infra-rouge...).

Recenser les points d'accès et les modalités de contrôle à chacun de ces points :

- l'exploitant pourra reprendre des conseils figurant dans la fiche 5.3.3 pour définir cet objectif ;
- type de portail (portillon...) ;
- modalités de contrôle à chaque accès (digicodes, clés...) ; à la différence que pour une ZNLA, la notion de PIF ne s'applique pas. En revanche, un poste de garde à l'entrée principale de l'IP est pleinement envisageable ou recommandable dans certains cas.

À partir des niveaux 2 et 3 ISPS, l'installation portuaire devra être étanche (fermée). C'est pourquoi l'exploitant doit pouvoir s'appuyer sur des protections de sûreté physiques, même si ceux-ci peuvent rester ouverts au niveau 1 ISPS ;

f) Mesures de surveillance :

Comme évoqué dans la fiche 5.3.5, les mesures de surveillance de la ZNLA peuvent s'appuyer sur :

- de l'éclairage ;
- des rondes de sûreté ;
- de la vidéoprotection ;
- à la différence que la notion de visite de sûreté n'est pas systématique avant l'arrivée d'un navire, contrairement aux mesures à mettre en œuvre lors de l'activation d'une ZAR.

Au niveau 1 ISPS, les mesures de surveillance sont assimilables à une notion de vigilance, où la capacité de réaction du personnel est mobilisée en cas d'intrusion sur le terminal. Le personnel doit être capable de reconnaître les personnes présentes sur le terminal pendant une escale.

Les rondes du personnel seront particulièrement utiles pour accroître la vigilance.

Rappelons que les mesures de sûreté s'appliquent même lorsque le navire reste en attente dans le terminal et en dehors des heures ouvrées (en l'absence de personnels présents sur le terminal). Dans ce cas, l'exploitant devrait s'appuyer principalement sur ses mesures de contrôle d'accès. L'IP sera fermée et les codes d'accès, digicodes, clés seront diffusés aux seules personnes autorisées (essentiellement le personnel du navire) ;

g) Tableau de synthèse des mesures combinées de surveillance et de contrôle d'accès :

Mesures combinées de contrôle d'accès et de surveillance de la ZNLA								
Type de mesure	Niveau 1 ISPS		Niveau 2 ISPS		Niveau 3 ISPS		Rappel des effectifs ayant des tâches de sûreté définies dans le chapitre 4	Délai de mise en œuvre des mesures renforcées en cas de changement de niveau
	Mesures mises en œuvre en présence d'un navire (y compris poste d'attente)	Mesures mises en œuvre en dehors d'une escale de navire	Mesures mises en œuvre en présence d'un navire (y compris poste d'attente)	Mesures mises en œuvre en dehors d'une escale de navire	Mesures mises en œuvre en présence d'un navire (y compris poste d'attente)	Mesures mises en œuvre en dehors d'une escale de navire		
Clôture								
Points d'accès								
Caméras								
Rondes								
Poste de garde								
Autres équipements périmétriques								
Éclairage								

Fiche 5.5.4 – Mesures pour la surveillance du plan d'eau

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A14.2.3 surveiller l'installation portuaire, y compris la ou les zones de mouillage et d'amarrage

Les objectifs :

Principe général :

Reprendre le cadre réglementaire.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Cette mission se distingue de toute d'intervention. Si cette dernière relève de la compétence des services de l'État, la surveillance fait appel à tous les moyens existants.

L'exploitant sera au minimum vigilant sur les zones de mouillage et d'amarrage de son installation portuaire. Dans le cadre des opérations commerciales, le personnel donnera l'alerte en cas de besoin auprès de l'ASIP, s'il détecte un événement suspect. Cela implique que le personnel ait reçu une sensibilisation sur ce sujet et que cela fasse partie intégrante de ses missions.

Fiche 5.5.5 – Mesures pour empêcher l'introduction d'articles prohibés

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A/16.3.1 les mesures visant à empêcher l'introduction, dans l'installation portuaire ou à bord du navire, d'armes, de substances dangereuses et d'engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence n'est pas autorisée

Les objectifs :

Principe général :

Définir une procédure pour empêcher l'introduction d'articles prohibés.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Les mesures pour empêcher l'introduction d'articles prohibés peuvent concerner :

- les armes à feu ;
- les explosifs ;
- les dispositifs incendiaires ;
- les articles dont la détention, le port et le transport est interdit par la législation maritime française ou communautaire ou en vertu d'un accord international maritime en vigueur auquel la France est partie.

Au niveau 1 ISPS : l'exploitant informe les personnes avant d'entrer sur le terminal que les substances dangereuses et les articles prohibés sont interdits. L'exploitant pourra installer des panneaux informant de cette interdiction à chacun de ses points d'accès. Les informations figurant sur le panneau devraient être soumises à l'avis de l'autorité locale. L'exploitant pourra procéder à une recherche de colis suspects dans le cadre de rondes avant l'arrivée du navire afin de sécuriser le terminal et de stériliser la zone.

Avec l'élévation du niveau 2 ou 3 ISPS, en complément du panneautage, l'exploitant peut opter pour différentes solutions :

- les bagages, les colis, les coffres de véhicules sont examinés visuellement (on se contente de regarder,

sans fouiller avec les mains). L'ouverture de la chose examinée (bagage ou coffre de véhicule) doit être effectuée avec le consentement du propriétaire. Si la personne refuse de se soumettre à ces contrôles visuels, l'exploitant doit lui interdire l'accès au terminal et il peut avoir recours aux forces de l'ordre (sur réquisition du procureur) ;

- refuser l'entrée sur le terminal de colis, bagages ou véhicules ;
- transférer la responsabilité au navire pour les bagages ou colis devant monter à bord.

Un règlement intérieur, à référencer dans le PSIP, devrait prévoir de telles procédures.

Fiche 5.5.6 – Procédure pour superviser la livraison de provisions de bord

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A/14.2.6 superviser la manutention des provisions de bord

Section B/16.8.10 les procédures concernant la livraison des provisions de bord

Les objectifs :

Principe général :

Détailler une procédure pour superviser la livraison des provisions de bord.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

La procédure pourra préciser si :

- l'exploitant est informé au préalable par l'agent consignataire de toute livraison à bord du navire ;
- l'exploitant fixe un créneau horaire au livreur pour réceptionner la livraison ;
- la livraison est prise en charge par le personnel de l'exploitant ou par le personnel du navire ;
- l'exploitant vérifie l'intégrité de l'emballage et si la livraison correspond au bon de commande communiqué par l'agent consignataire ;
- en cas de suspicion sur l'intégrité du colis, si l'ASIP est alerté ;
- le véhicule de livraison est escorté jusqu'au navire, en cas de besoin ;
- les mesures sont renforcées pour les niveaux 2 et 3 ISPS.

Fiche 5.5.7 – Procédure pour superviser la manutention de la cargaison

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Section A/14.2.5 superviser la manutention de la cargaison

Section A/16.3.12 des mesures destinées à garantir la protection effective de la cargaison et du matériel de

manutention de la cargaison dans l'installation portuaire

Section B/16.8.9 les procédures relatives à la manutention de la cargaison

Les objectifs :

Principe général :

Déterminer une procédure pour superviser la manutention de la cargaison.

Principe particulier pour les instructeurs :

Les services instructeurs du PSIP devront vérifier l'existence de cette procédure, en particulier si l'ESIP a retenu parmi les points névralgiques du matériel dédié à la manutention de la marchandise (grues mobiles...). La procédure devra donc préciser les mesures de protection de ce matériel.

Les conseils complémentaires :

Conseils complémentaires pour les exploitants :

Avant d'embarquer sur un navire, l'exploitant doit s'assurer que la manutention de la cargaison n'ait pas fait l'objet d'une manipulation criminelle au préalable. La cargaison doit être contrôlée avant de monter à bord du navire.

Plus précisément, l'exploitant doit surveiller les équipements qui permettent de manutentionner la marchandise sur le navire (des embranchements de tuyaux, des grues...). La procédure mentionnera si le personnel inspecte le matériel de manutention avant usage, notamment dans le cadre de procédures de sécurité. Si le matériel est fermé à clé, le PSIP précisera les modalités de gestion des clés.

En particulier, pour les terminaux qui manutentionnent des conteneurs, le PSIP apportera des précisions sur :

- les contrôles visuels de l'intégrité apparente de l'unité de charge ;
- la fouille de l'unité de charge, et éventuellement de la cargaison ;
- le contrôle des scellés et des conteneurs vides.

La procédure doit être déclinée par niveaux ISPS.

Fiche 5.5.8 – Articulation avec les règles de sûreté des ZAR adjacentes

Le cadre réglementaire :

Arrêté du 22 avril 2008,

Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)

5. Accès et circulation dans l'installation portuaire

5.5. Zones Non Librement Accessibles

(...) et les articulations avec les règles de sûreté des ZAR adjacentes, en démontrant que la sûreté de l'installation portuaire dans son ensemble et de chaque installation portuaire adjacente n'est pas dégradée, quel que soit le niveau de sûreté.

Les objectifs :

Principe général :

Reprendre l'intitulé de l'arrêté. Les objectifs sont similaires à la fiche 4.3.

Chapitre 6 : Conduite à tenir en cas d'alerte, d'incident avéré et de sinistre

Fiche 6.1 – Conduite à tenir en cas d'alerte, d'incident avéré et de sinistre

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004 section A/16.3.3 – Le plan doit comprendre au moins : des procédures pour faire face à une menace contre la sûreté ou une atteinte à la sûreté, y compris des dispositions pour maintenir les opérations essentielles de l'installation portuaire ou de l'interface navire/port ;

*Arrêté du 22 avril 2008,
Annexe 4 – chapitre 6 – Conduite à tenir en cas d'alerte de sûreté, ou d'incident avéré ou de sinistre*

MSC/Circ 147 du 29 mai 2003 – Security Ship Alert System

Les objectifs :

Principe général :

Le plan doit décrire :

- les systèmes d'alerte internes à l'IP ;
- les systèmes d'alerte externes ;
- les mesures prévues à chacun des niveaux de sûreté pour faire face à une menace imminente, une alerte ou une atteinte en cours contre la sûreté ;
- les exigences précises de notification obligatoire de tous les incidents de sûreté à l'agent de sûreté d'installation portuaire et par celui-ci à l'agent de sûreté portuaire ;
- les mesures prévues pour accueillir un navire faisant l'objet d'une alerte de sûreté ;
- les mesures prévues à la suite d'une alerte de sûreté sur un navire se trouvant dans l'installation portuaire ;
- les dispositions permettant de maintenir les opérations portuaires essentielles, notamment dans le cas d'activités d'importance vitale ;
- les modalités de coordination avec l'ASP ;
- l'établissement de fiches réflexes pour chaque type d'incident ;
- la définition de l'articulation des mesures de sûreté, avec les mesures applicables en cas de sinistre, notamment l'intervention sur les sites de moyens de secours extérieurs ou l'évacuation, en respectant le principe selon lequel les mesures de sûreté ne doivent pas porter atteinte à la sécurité.

Si l'IP est désignée PIV, mentionner distinctement :

- l'organisation et les moyens mis en œuvre en cas d'alerte ;
- l'organisation et les moyens mis en œuvre en cas d'incident avéré ou de sinistre ;
- les modalités d'assistance à l'intervention éventuelle de la force publique.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

S'assurer de la prise en compte pleine et entière de la totalité des mesures et de leur faisabilité locale (disponibilité, délais d'intervention, modalités d'intervention, etc.).

Les personnels ayant des tâches de sûreté doivent avoir accès en permanence aux fiches réflexes. Ces fiches doivent être connues et faire l'objet d'entraînements (test de connaissance et mise en situation).

Fiche 6.2 – Les systèmes d'alarme et d'alerte internes et externes

Reprendre sous forme de tableau renseigné, les systèmes d'alarme et d'alerte internes (enregistreur-localisateur d'appels, téléphones, interphones, réseaux spécialisés, sirènes...) et externes :

Moyens d'alarme et d'alerte internes	Localisation au sein de l'IP
Enregistreur / localisateur d'appel	
Téléphone (réseau interne)	
Téléphone (réseau externe)	
Télécopie	
Messagerie électronique	
Interphone	
Sirène d'alarme restreinte	
Radio VHF	Réseau personnels exploitation / acteurs de la sûreté / ASIP

Moyens d'alerte externes	Emploi
Téléphone	Fixes et portables mettant en réseau les acteurs de la sûreté.
Téléphone	En ligne directe avec les services de secours.
Télécopie /messagerie électronique	Réception et émission des messages.
Réseau spécialisé force publique	Selon les directives propres à la force publique.

Pour une meilleure compréhension de l'articulation, placer en annexe les schémas type de transmission d'alerte (voir annexe n° 9).

Fiche 6.3 – Mesures pour faire face à une menace imminente, une alerte ou une atteinte en cours contre la sûreté

Les exploitants et ASIP sont limités par la loi et la réglementation dans leur action, y compris les sociétés prestataires de gardiennage. En effet, la sûreté de l'IP et des opérations qui s'y rattachent doivent être réalisées sous le contrôle d'un OPJ ou agent des douanes, en particulier dans le cadre d'une ZAR.

L'ASIP en tant que responsable de l'application des mesures de sûreté et de la protection de l'IP doit réagir avec discernement et en application des lois et de la réglementation. D'une manière générale, il garde pour priorité la protection des personnes présentes sur l'IP.

En cas d'incident imminent ou avéré, l'ASIP en liaison avec l'ASP et la capitainerie :

- alerte ou fait alerter les secours (police, pompiers, ...) et reste en contact ;
- alerte l'ASN des navires ;
- alerte sa hiérarchie directe et les autorités concernées (préfecture...)
- applique les procédures de conduite à tenir pertinentes ;
- s'assure de la mise en sécurité des installations de production (si existantes) ;
- recueille toutes les informations utiles à la compréhension de l'événement pour les relayer aux services compétents ;
- fait établir le recensement des personnes présentes et garder sur les lieux uniquement les personnes strictement nécessaires ;
- fait établir un périmètre de sécurité ;
- facilite l'accès et le stationnement des véhicules des services d'urgence ;
- anticipe la montée en puissance de l'incident et prépare les dispositions nécessaires prévues par le PSIP ;
- fait prendre les mesures de sûreté supplémentaires prévues au plan de sûreté ;
- rend compte des mesures prises et de la situation aux autorités concernées et à sa hiérarchie.

Fiche 6.4 – Recherche, détection et localisation d'objets, véhicules ou individus

L'application de ces mesures étant plus spécialement confiée aux services spécialisés de l'État, il s'agit surtout de transmettre l'alerte à l'ASP et à l'autorité locale qui se chargent d'alerter les services spécialisés, comme proposé ci-dessous :

Niveau	Niveau 1	Niveau 2	Niveau 3
Recherche	L'ASIP demande confirmation de l'incident et la nature de l'incident et de ses conséquences. Il informe immédiatement l'ASP et l'autorité locale de l'alerte.		
Détection			
Localisation d'objet			
Individu suspect			
Véhicule suspect			
Alerte police	L'ASIP (en tenant l'ASP informé) fait appel aux forces de police et/ou de gendarmerie dès l'alerte connue. Le personnel de l'IP assiste les forces de l'ordre dans les recherches.		
Alerte secours			
Évacuation	Déclenchée par l'ASIP (en tenant l'ASP et l'autorité locale informés), après avis des forces de l'ordre ou de secours.		

Fiche 6.5 – Exigences précises de notification obligatoire des incidents à l'ASIP /ASP

Tout incident de sûreté, survenu sur l'installation portuaire, doit être immédiatement notifié à l'ASIP d'abord par téléphone puis à l'aide du formulaire de compte-rendu d'incident de sûreté (cf. annexe n° 10). Le compte-rendu d'incident de sûreté sera archivé dans le registre de sûreté tenu par l'ASIP.

Dès qu'il a connaissance d'un incident de sûreté, survenu sur l'installation portuaire, l'ASIP informe immédiatement l'ASP, d'abord par téléphone, puis à l'aide du formulaire de compte-rendu d'incident de sûreté.

La procédure doit également prévoir de notifier l'incident aux points de contact auprès des gouvernements contractants pertinents (Code ISPS paragraphe B/16.3.6).

Les événements suivants (liste non exhaustive) doivent être signalés :

- découverte d'engins ou objets suspects ;
- alerte à la bombe ou découverte d'un engin explosif improvisé (EEI) ;
- présence de personnel non autorisé à l'intérieur de l'IP ;
- présence de personnes ou d'activités suspectes à l'intérieur de l'IP ;
- présence de navire ou bateau non autorisé ;
- découverte d'effraction sur les clôtures ou portails ;
- présence de véhicule non autorisé ou stationnant dans un emplacement interdit ;
- trouble de l'ordre public ou mouvement social.

Fiche 6.6 – Mesures prévues pour accueillir un navire faisant l'objet d'une alerte de sûreté

Comme prévu par la Convention SOLAS XI-2 Règle 6, en cas de menace directe à quai, au mouillage ou en mer, les navires disposent d'un SSAS² : deux boutons manuels d'alerte dissimulés en deux endroits du navire (dont un en passerelle de navigation) et qui permettent le déclenchement d'une alerte discrète et sa transmission par voie satellitaire aux organismes prévus (CROSS Gris-Nez) et à la compagnie maritime. Ces organismes transmettent l'alerte à l'ASIP, via la capitainerie (ASP).

L'ASIP, lorsqu'il est informé d'une menace en provenance d'un navire doit :

- identifier la menace ;
- informer les autorités portuaires ;
- informer les autorités préfectorales ;
- armer la salle de crise. Ce local dispose des moyens permettant les communications de sûreté montantes et descendantes.

Et selon la décision des services de l'État, les mesures suivantes peuvent être mises en œuvre :

- le navire reste au mouillage ;
- le navire est autorisé à accoster, dans ce cas des mesures particulières peuvent être prescrites : place à quai isolée, clôture de la zone d'amarrage, etc.

Fiche 6.7 – Mesures prévues à la suite d'une alerte de sûreté sur un navire se trouvant dans l'installation portuaire

L'ASIP, lorsqu'il est informé d'une menace en provenance d'un navire à quai dans l'IP doit :

- identifier la menace ;
- informer les autorités portuaires ;
- établir et maintenir le contact entre l'ASP et l'ASN concerné ;
- fait interdire l'accès à l'IP ;
- fait établir le recensement des personnes présentes et ne conserver sur les lieux que les personnes strictement nécessaires ;
- fait établir un périmètre de sécurité ;
- armer la salle de crise. Ce local dispose des moyens permettant les communications de sûreté montantes et descendantes ;
- se conformer aux directives et décisions de la Préfecture transmises par l'ASP.

² Système d'Alerte de Sûreté du Navire

Fiche 6.8 – Dispositions permettant de maintenir les opérations portuaires essentielles, notamment dans le cas d'activités d'importance vitale

Jusqu'au niveau de sûreté 2, l'installation portuaire travaille en conditions normales d'exploitation et doit par conséquent faire face à la régularité des mouvements et des trafics. Le principe d'arbitrage et d'organisation des mouvements et les priorités d'accostage des navires sont établis par poste à quai (par la capitainerie) en fonction de règles économiques ou commerciales.

À partir du niveau 3, et selon les décisions de l'État, des restrictions de navigation peuvent être mises en place.

Fiche 6.9 – Coordination avec l'agent de sûreté portuaire

L'ASIP, lorsqu'il est informé d'une menace de sûreté dans l'IP doit assurer les liaisons avec l'ASP et le PCS (PC sûreté) du port. Sous la coordination de l'ASP il doit :

- assurer les liaisons avec les services extérieurs pour les mises en application des mesures de sûreté de l'IP ;
- alerter les autres IP du port et vérifier avec les ASIP, de l'opportunité des mesures des PSIP à mettre en place ;
- s'assurer de la mise en application des mesures prévues dans l'IP ;
- rendre compte à l'ASP de la mise en application de ces mesures ;
- demander à l'ASP les renforts éventuels prévus par les plans de sûreté (PSP et PSIP).

Fiche 6.10 – Fiches réflexes pour chaque type d'incident

Ces fiches sont mentionnées dans cette partie du plan et sont placées en annexe n° 11. Elles font partie intégrante du volume 2 du PSIP.

Fiche 6.11 – Articulation ou aménagement Sûreté – Sécurité en cas de sinistre

Les services de secours sont autorisés à accéder sans titres d'accès ou annonce particulière dans l'IP. En cas de conflit entre sécurité et sûreté le principe appliqué est de faciliter l'accès des secours et de procéder à la vérification a posteriori des droits d'accès (réalité événementielle).

Cependant, l'ASIP, les services de secours et de sécurité publique devront avoir à l'esprit et être en mesure de gérer :

- la mise en sécurité prioritaire des personnes et la protection des biens ;
- la prévention d'un sur-accident (bouclage de zone, périmètre de sécurité, organisation de la circulation, ...)
- la facilitation de l'arrivée des secours (jalonnement, balisage, restriction de circulation et de stationnement) ;
- l'information aux secours (état de présence au contrôle d'accès, comptage au point de regroupement, ...) ;
- la facilitation de l'intervention (cordon de sécurité, dégagement des véhicules aux abords, acheminement des évacués vers un point de regroupement déterminé, ...) ;
- l'identification des personnes impliquées par le sinistre, celles évacuées et celles éventuellement blessées ;
- le renforcement de la surveillance des zones sensibles (sinistre créé pour diversion, ...) ;
- les mesures conservatoires à prendre en cas de détérioration d'infrastructure de sûreté.

Fiche 6.12 – IP désignée PIV

Les dispositions sont déjà décrites dans les différents paragraphes du PSIP. Deux méthodes : recopier intégralement ces dispositions dans cette partie du PSIP ou insérer des renvois vers les paragraphes intéressés :

- organisation et moyens en cas d'alerte ;
- organisation et moyens en cas d'incidents avérés ou de sinistres ;
- modalités d'assistance à l'intervention éventuelle de la force publique.

Chapitre 7 : Dispositions visant à réduire les vulnérabilités liées aux personnes

Fiche 7.1 – Dispositions visant à réduire les vulnérabilités liées aux personnes

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004 :

Section A/17.2.6 – ... Les tâches et responsabilités de l'ASIP comprennent... accroître la prise de conscience de la sûreté et la vigilance du personnel de l'IP ;

Section B/18.3 – Tous les autres membres du personnel de l'installation portuaire devraient connaître les dispositions du PFSP et être familiarisés avec elles dans certains ou dans l'ensemble des domaines suivants, selon qu'il convient :

.1 signification et implications des différents niveaux de sûreté ;

.2 identification et détection des armes et des substances et engins dangereux ;

.3 identification des caractéristiques et du comportement des personnes qui risquent de menacer la sûreté, et

.4 techniques utilisées pour contourner les mesures de sûreté.

MSC.1/Circ 1341 du 27/05/2010 : (en anglais uniquement)

Rappelle les dispositions applicables en faisant le distinguo entre les personnels chargés de tâches de sûreté et tous les autres personnels de l'installation portuaire et définit dans sa table 1 les items de formation/sensibilisation applicables à ces derniers.

Code des transports – Art. R. 5332.32

Arrêté du 22 avril 2008 – annexe 4 – chapitre 7

Arrêté du 18 juin 2008 : relatif à la délivrance d'un agrément nécessaire pour l'exercice de missions de sûreté ou d'une habilitation nécessaire pour l'accès permanent à une zone d'accès restreint.

Arrêté du 15 avril 2009 : portant création d'un traitement de données à caractère personnel relatif à la délivrance d'habilitations, d'agréments, ...

Les objectifs :

Principe général :

Le plan doit décrire :

- la sensibilisation du personnel de l'IP et des tiers (clients, fournisseurs, ...) ;
- les procédures d'agrément ou d'habilitation des personnes ;
- les relations avec les prestataires en matière de sûreté.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

La sensibilisation concerne l'ensemble du personnel pénétrant (travaillant) sur l'IP. Elle peut être délivrée par l'ASIP ou par un organisme de formation agréé par la direction interrégionale de la mer (DIR).

Le contenu de cette sensibilisation doit être conforme aux items du RE N° 725/2004 et de la MSC Circ. cités supra.

Les habilitations et agréments des personnels ne concernent que les ASIP et leurs suppléants, les personnels titulaires d'un titre de circulation permanent en ZAR et les agents chargés des visites de sûreté (ACVS) au poste d'inspection filtrage des ZAR.

Les relations avec le prestataire de sûreté étant formalisées par un cahier des clauses techniques particulières (CCTP), il convient de s'assurer de la bonne adéquation des dispositions contenues dans le plan et dans le CCTP.

Conseils particuliers pour les exploitants :

Sensibilisation du personnel :

Un plan de formation peut utilement être joint au registre de sûreté, permettant ainsi la mise à jour des formations effectuées ou à effectuer.

Cette sensibilisation s'adresse également aux fournisseurs et clients occasionnels. Elle peut être délivrée lors de la procédure d'établissement/délivrance du titre d'accès, sous forme de projection vidéo ou de remise d'un fascicule.

Procédures d'agrément ou d'habilitation des personnes :

Ces procédures sont définies par l'AM du 18 juin 2008. Elles concernent :

- les ASIP et leurs suppléants dont la qualité est subordonnée à la possession d'un agrément (valable 5 ans) délivré par le représentant de l'État dans le département ;
- l'obtention d'un titre de circulation permanent en ZAR est également subordonnée pour les personnels titulaires d'un tel titre à la possession d'un agrément (valable 5 ans) délivré par le représentant de l'État dans le département ;
- la demande de double agrément des personnes chargées des visites de sûreté dans les ZAR est adressée par chacune d'elles à l'ASIP. L'ASIP transmet la demande au Préfet du département, qui transmet ensuite le dossier au procureur de la République.

L'AM du 15 avril 2009 définit les modalités de renseignement de la base de données CEZAR, les droits d'accès à cette base et les procédures d'obtention / renouvellement des agréments et habilitations.

Le Préfet et le Procureur de la République notifient les décisions d'habilitation, de retrait ou de suspension d'habilitation en ZAR à l'intéressé et à l'exploitant de l'installation portuaire.

Relations avec le prestataire de sûreté :

Ces relations sont formalisées par un CCTP entre l'exploitant et le prestataire.

Ce CCTP décrit dans le détail l'objet des prestations assurées, leurs modalités d'exécution et le suivi de la prestation. Utilement placé en annexe du PSIP, il permet une évolution constante sans avoir à recourir aux avis du CLSP pour avaliser des *modifications mineures* ne touchant pas au cœur de la sûreté de l'IP.

Chapitre 8 : Audits, contrôle interne, mise à jour du plan

Fiche 8.1 – Audits, contrôle interne, mise à jour du plan

Le cadre réglementaire :

Code ISPS annexé au Règlement (CE) N° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires sections B/1.20, B/15.14, B/15.16, B/16.3, B/16.5, B/16.58, B/16.59, B/16.61, B/17.2, B/18.1 à B/18.6.

Code ISPS annexé au RE n° 725/2004 section A/16.3.13 : le plan de sûreté de chaque installation portuaire doit "comprendre au moins des procédures d'audit du plan de sûreté de l'installation portuaire"

Code ISPS annexé au RE n° 725/2004, section A/16.4 : "le personnel qui procède aux audits internes des activités liées à la sûreté spécifiées dans le plan ou qui évalue sa mise en œuvre ne doit pas avoir de rapport avec les activités faisant l'objet de l'audit, à moins que cela ne soit pas possible dans la pratique du fait de la taille et de la nature de l'installation portuaire".

*Arrêté du 22 avril 2008, Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)
« Chapitre 8. Audits et contrôles internes, mise à jour du plan »*

Les objectifs :

- contrôler la mise en place effective des dispositions prévues par le PSIP ;
- vérifier la bonne application du système de management de la sûreté, et l'adéquation de ce système avec les enjeux de l'IP ;
- vérifier l'appropriation des mesures décrites dans le PSIP par les différents acteurs ;
- s'assurer de l'adéquation et de l'efficacité des mesures prises et évaluer les opportunités d'amélioration ;
- décider des éventuels changements d'orientation stratégiques imposant si nécessaire la révision du PSIP.

Principe général :

Le plan de sûreté de l'installation portuaire traite au minimum chacun des points suivants :

- la procédure garantissant la prise en compte de la sûreté dans les aménagements et les nouveaux projets d'infrastructure ;
- le contrôle de l'état des matériels de protection, de surveillance, de contrôle et de communication (préciser procédures et périodicité d'entretien et enregistrement) ;
- la création et la tenue à jour d'un registre de sûreté comprenant une liste chronologique de tous événements liés à la sûreté : formation, incidents de sûreté et mise en œuvre et de suivi des mesures correctives, exercices et entraînements de sûreté accomplis, changements de niveau, etc. Sont également annexées les déclarations de sûreté remplies par l'ASIP et le capitaine ou l'ASN ;
- la procédure d'analyse de chaque incident de sûreté et, le cas échéant, de mise en œuvre et de suivi des mesures correctives ;
- la description du résultat de l'audit interne périodique des mesures et procédures de sûreté du plan et des mesures correctives.

Principe particulier pour les instructeurs :

Le CLSP émet un avis sur les projets d'infrastructure lorsque le représentant de l'État estime qu'ils présentent des enjeux en matière de sûreté.

En particulier, si suite à des travaux, le périmètre du terminal évolue ou si de nouveaux points névralgiques apparaissent, le CLSP devra apprécier s'il est opportun de réviser l'ESIP.

Les conseils complémentaires :

Conseils complémentaires d'ordre général :

Dans le cadre d'aménagements et nouveaux projets d'infrastructure, la participation de l'ASP à la réunion d'ouverture du chantier et aux réunions de suivi est fortement recommandée pour examiner la mise en œuvre des modalités de sûreté imposées avec l'ASIP.

Conseils complémentaires pour les exploitants :

Aménagements et nouveaux projets d'infrastructure :

Lorsqu'elle existe, l'exploitant peut faire référence à ses procédures internes démontrant l'intégration de la prise en compte des aspects liés à la sûreté lors d'aménagements et nouveaux projets d'infrastructure.

L'ASIP doit être informé lors des phases d'études d'aménagements et nouveaux projets d'infrastructure afin de vérifier l'apparition de nouveaux points de vulnérabilité et/ou l'interférence avec les dispositions existantes pour faire face aux menaces (exemple : modification des clôtures, création d'un nouvel accès, construction de nouveaux bâtiments avec de nouvelles activités...).

Le responsable du Port et l'ASP sont consultés lorsque les projets ont une incidence sur le domaine portuaire. Si les aménagements ou nouveaux projets affectent durablement la sûreté de l'IP, les mesures compensatoires doivent être présentées au préalable lors d'un CLSP.

Contrôle de l'état des matériels de protection, de surveillance, de contrôle et de communication :

En tenant compte des prescriptions du constructeur, l'exploitant ou le prestataire en cas de sous-traitance s'assurent du contrôle et de l'entretien des matériels et équipements de sûreté.

L'ASIP pourra prévoir une liste de points à contrôler (check list), avec :

- matériels de sûreté à contrôler (cadenas, clôtures, caméras...) ;
- la périodicité des contrôles ;
- l'agent en charge de faire les contrôles.

En cas d'existence de contrats de service pour assurer la maintenance préventive et curative, les rapports sont examinés par l'ASIP pour garantir la levée des réserves éventuelles et/ou la nécessité de prise de mesures palliatives (exemple : en cas de dysfonctionnement du système de vidéoprotection ou de détection des intrusions ou du contrôle d'accès, détecteur de masse métallique, réseau de transmission radio, etc.).

Les résultats des tests de performance des matériels et équipements utilisés dans l'IP, les principaux événements d'exploitation survenus, ainsi que les mesures palliatives et correctives prises si ces événements d'exploitation ont révélé un dysfonctionnement, sont enregistrés et archivés dans le registre de sûreté.

Registre de sûreté :

Le registre de sûreté constitue la traçabilité des activités importantes de la gestion de la sûreté de l'IP. Il peut se présenter sous format papier ou sous format électronique à condition qu'une procédure en garantisse la protection contre le piratage, l'accès aux personnes non autorisées, l'effacement ou la perte accidentelle des données. Il porte la mention « Confidentiel Sûreté ».

Il comprend au minimum une liste chronologique de tous événements liés à la sûreté. Il est organisé et classé pour faciliter les recherches (formation, incidents de sûreté et mise en œuvre et de suivi des mesures correctives, les comptes rendus des exercices et entraînements de sûreté, les changements de niveau de sûreté, les déclarations de sûreté remplies par l'ASIP ou l'ASP et le capitaine ou l'agent de sûreté du navire, les résultats des audits, les courriers échangés avec la préfecture ou avec le CLSP ou avec l'ASP, les

résultats des tests de performance des matériels et équipements de sûreté...).

La durée de conservation du registre de sûreté est au moins égale à la durée de validité du PSIP majorée de deux ans. Néanmoins, il appartient à l'ASIP d'apprécier s'il convient d'archiver certains événements pour une durée supérieure.

La procédure d'analyse de chaque incident de sûreté et, le cas échéant, de mise en œuvre et de suivi des mesures correctives :

Comme pour tout système de management, la remontée d'incident doit être valorisée comme l'identification des pistes d'amélioration. Le principe de mise en place du retour d'expérience contribue à l'amélioration continue et donc de l'efficacité opérationnelle des acteurs impliqués dans la gestion de la sûreté.

Lorsqu'elle existe, l'exploitant peut faire référence à ses procédures internes de système de management intégré pour le traitement des incidents/accidents.

La mention « Confidentiel Sûreté » sera portée sur les fiches rédigées. Leur diffusion sera limitée aux personnes habilitées (ASIP et suppléant(s), Direction, ASP).

L'analyse des incidents nécessite qu'elle soit conduite par des personnes disposant des compétences adaptées afin d'identifier les causes profondes et proposer les actions préventives et correctives.

L'analyse des incidents intègre notamment les phases suivantes :

- mener des actions pour réduire toutes les conséquences et/ou les vulnérabilités ;
- définir et mettre en place des actions correctives et préventives ;
- définir les indicateurs de mesure de l'efficacité des actions pendant une période déterminée ;
- porter à la connaissance des personnes impliquées les actions décidées ;
- inscrire au registre de sûreté le résultat de l'analyse de l'incident ;
- assurer le suivi de l'efficacité des actions mise en place jusqu'à leur clôture.

Selon le niveau de gravité de l'incident, l'analyse peut nécessiter la mise en place d'un groupe de personnes habilitées (ASIP et suppléants, OSH, expert en sûreté...).

Le choix des actions correctives et préventives sont établies en cohérence avec la faisabilité technique et le coût financier pour garantir leur réalisation. C'est pourquoi l'ASIP doit valider, préalablement avec sa Direction, le plan d'actions pour garantir que les mesures décidées seront réalisées dans les délais fixés. Il en assure le suivi jusqu'au terme de la réalisation.

Description du résultat de l'audit interne périodique des mesures et procédures de sûreté du plan et des mesures correctives :

a) Les objectifs de l'audit interne :

- s'assurer que le système de management de la sûreté pour la mise en œuvre des dispositions prévues par le PSIP demeure pertinent, adéquat et efficace ;
- relire chapitre par chapitre l'ensemble du plan afin d'en vérifier l'actualité et d'en tirer les modifications nécessaires ;
- évaluer l'efficacité des équipements nécessaires pour conduire les activités de maîtrise opérationnelles de la sûreté, vérifier la tenue du registre, veiller au respect des échéanciers fixés dans le PSIP et examiner l'application des consignes prévues dans le PSIP ;
- déterminer les besoins de changement au niveau de la politique, au niveau des objectifs et au niveau des autres éléments constitutifs du PSIP ;

- l'audit interne peut être couplé avec d'autres audits (ISO 9001...) ;

b) La périodicité de l'audit interne :

L'ASIP doit planifier et organiser un audit interne selon la périodicité définie dans le PSIP. L'audit interne doit être réalisé au minimum une fois pendant la durée de validité du PSIP. En complément, l'exploitant doit tenir compte de la fiche 2.1 qui recommande une révision annuelle du PSIP ou lors de modifications importantes pour maintenir une mise à jour continue ;

c) Le choix du personnel devant procéder à l'audit interne :

La conduite de l'audit interne doit être à l'initiative de l'exploitant, soit en faisant appel à son propre personnel, soit en commanditant un prestataire extérieur. L'audit interne ne devrait pas être réalisé par l'ASIP ou ses suppléants sauf si la taille de l'entreprise ne le permet pas (entreprise de moins de 20 salariés). L'exploitant peut procéder à des audits croisés avec d'autres ASIP appartenant au même groupe mais travaillant sur d'autres installations portuaires.

La réalisation d'audit du PSIP conduira l'(es) auditeur(s) à avoir accès à des informations sensibles. Il convient de vérifier préalablement la qualification d'(es) auditeur(s) pour l'accès aux informations classées « Confidentiel Sûreté ». Par défaut, l'auditeur recevra une lettre de la Direction l'autorisant à consulter des documents confidentiels. Selon le degré de connaissance de l'auditeur, il pourra être assisté d'auditeur(s) habilité(s) en Sûreté de la même société et/ou du même Groupe d'appartenance. Si l'exploitant se fait assister par un OSH, il faudra vérifier la mise à jour de son agrément ;

d) Les résultats de l'audit interne et son rendu :

L'audit fera l'objet d'un rapport écrit pris en compte par l'ASIP et la Direction de l'exploitant. Le rapport est archivé au registre de sûreté. Ce rapport peut prendre la forme d'une grille d'analyse listant les critères évalués et le résultat de l'évaluation (excellent, correct, insuffisant, non satisfaisant...).

Le PSIP devra prévoir une procédure d'analyse et un retour d'expérience suite à l'audit. Un plan d'actions correctives et un échéancier de mise en œuvre devront être définis et planifiés pour combler les lacunes constatées.

Mise à jour du PSIP :

L'ASIP assure la mise à jour au fil de l'eau du PSIP qui s'impose à la suite :

- d'une nouvelle ESIP ;
- d'un changement administratif figurant dans le PSIP (changement de fonction, n° de téléphone, adresse, etc.) ;
- d'une modification ou aménagement modifiant l'IP ;
- d'un incident ou d'une menace d'incident de sûreté mettant en cause l'installation portuaire ;
- d'un changement d'activité, de propriété ou de gestion de l'installation portuaire de l'IP ;
- d'un audit indépendant du PSIP ou de la vérification par les services compétents de l'État français d'un constat de lacunes identifiées de l'organisation de la sûreté de l'installation portuaire ou la remise en question de la pertinence d'un élément important du PSIP approuvé.

Il appartient à l'ASIP de veiller à la mise à jour du PSIP puis de transmettre les modifications au Préfet du département, lequel peut imposer une validation en CLSP. Pour rappel, la fiche 2.1 « Tableau d'enregistrement des modifications ou compléments au PSIP » recommande que le PSIP fasse a minima l'objet d'une révision annuelle et soit présenté au représentant de l'État.

Chapitre 9 : Formation, exercices et entraînements de sûreté

Fiche 9.1 – Formation, exercices et entraînements de sûreté

Le cadre réglementaire :

Code ISPS annexé au Règlement (CE) N° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires section A/18 et sections B/18.4, B/18.5 et B/18.6

*Arrêté du 22 avril 2008, Annexe 4 – Plan type du plan de sûreté de l'installation portuaire (PSIP)
« 9. Formation, exercices et entraînements de sûreté »*

Arrêté du 2 juin 2008 : fixant les conditions d'organisation des exercices et entraînements de sûreté dans les ports et les installations portuaires

Arrêté du 23 septembre 2009 : fixant les conditions d'approbation des formations des agents chargés des visites de sûreté préalables à l'accès aux zones d'accès restreint définies aux articles R. 5332-34 et R. 5332-35 du code des transports

Les objectifs :

Le Principe général :

L'arrêté demande de préciser a minima :

- programme et périodicité des exercices et entraînements ;
- formation initiale et continue des personnels de sûreté par catégorie (agents de sûreté portuaire, agents de sûreté des installations portuaires, personnes chargées d'effectuer les visites de sûreté, personnes assurant le gardiennage).

Principe particulier à destination des instructeurs :

Les entraînements/exercices permettent de vérifier l'appropriation des différents acteurs des mesures de sûreté décrites dans le PSIP et leur capacité à mettre en œuvre les contre-mesures prévues pour faire face à une menace. Ils peuvent prendre la forme d'interviews et/ou de mise en situation des différents acteurs.

Principe particulier à destination des exploitants :

Il s'agit de démontrer l'efficacité des actions menées pour sensibiliser le personnel de l'établissement dans le domaine de la sûreté (formations), ainsi que le personnel extérieur ayant à se rendre sur l'IP (information).

Pourront être décrits notamment :

- les procédures particulières d'accès des entreprises appelées à intervenir régulièrement sur le site si elles existent en matière de procédures d'habilitation et d'agrément ;
- les modalités des relations, du suivi et revue de contrat de la prestation de sûreté confié à un prestataire spécialisé.

Les conseils complémentaires :

Conseils complémentaires d'ordre général, relatifs à la formation initiale et continue des personnels :

Préalablement à toute prise de fonction d'ASIP ou à la tenue du poste d'ACVS, une formation initiale correspondant aux tâches et missions dévolues est réalisée dans le respect des objectifs pédagogiques et des durées minimales fixées par arrêté.

L'ASIP et ses suppléants suivent une formation dispensée par un organisme agréé. La formation est sanctionnée par un examen permettant la délivrance d'une attestation de formation ASIP nécessaire pour formuler la demande d'agrément au Préfet. Le maintien des compétences de l'ASIP et des suppléants est assuré par leur implication permanente dans les activités de sûreté (participation aux réunions organisées par l'ASP ou par la préfecture, aux audits, aux entraînements et aux exercices, aux congrès ou réunions portant sur la thématique de la sûreté portuaire, à la revue périodique du PSIP, au suivi de la veille documentaire des textes portant sur la sûreté).

Les conditions d'approbation des formations des ACVS sont prescrites par l'arrêté du 23 septembre 2009. Les formations sont déclinées par des formateurs disposant de références et qualifications professionnelles et comportant au minimum 2 modules (module 1 d'une durée minimale de 7 heures et module 2 d'une durée minimale de 14 heures). Un module 3 est requis lorsque les agents sont amenés à exploiter un équipement de détection radioscopique. Les ACVS doivent détenir le double agrément pour exercer dans l'IP.

L'employeur est tenu de planifier des actions de formation continue à l'attention de ses agents qui traitent des évolutions réglementaires ou techniques sur les thèmes enseignés en formation initiale. Sur une période de 3 ans, la durée minimum de la formation continue ne peut être inférieure à la moitié de la durée de la formation initiale. Pour chaque agent utilisant l'imagerie d'un équipement radioscopique, l'employeur est tenu d'organiser un entraînement périodique. Sa durée ne peut être inférieure à 6 heures sur une période de 3 mois, et à 3 heures si l'employeur met en œuvre sur l'équipement un dispositif de test par projection d'image de menace régulièrement utilisé.

Lorsque les agents de sûreté exercent dans une installation portuaire dépourvue d'une ZAR, l'employeur doit pouvoir :

- justifier de la mise en œuvre et la conformité du décret n° 2006-1120 du 7 septembre 2006 modifiant le décret n° 2005-1122 du 6 septembre 2005 relatif à l'aptitude professionnelle des dirigeants et des salariés des entreprises exerçant des activités de surveillance et de gardiennage, de transport de fonds et de protection physique des personnes et le décret n° 2005-1123 du 6 septembre 2005 relatif à la qualification professionnelle des dirigeants et à l'aptitude professionnelle des salariés des agences de recherches privées ;
- justifier de la mise en œuvre et la conformité du décret n° 2009-137 du 9 février 2009 relatif à la carte professionnelle, à l'autorisation préalable et à l'autorisation provisoire des salariés participant aux activités privées de sécurité définies à l'article 1er de la loi n° 83-629 du 12 juillet 1983 ,
- justifier de la mise en œuvre et la conformité de l'arrêté du 19 juin 2008 portant agrément d'un certificat de qualification professionnelle en application de l'article 1er du décret n° 2005-1122 du 6 septembre 2005 relatif à l'aptitude professionnelle des personnes exerçant une activité de surveillance.

Conseils complémentaires d'ordre général, relatifs à la programmation et à la périodicité des exercices et entraînements :

Les entraînements et exercices permettent en particulier :

- d'apprécier le niveau de formation des personnes et leur capacité à réagir en présence d'une menace ou d'un incident de sûreté ;
- de vérifier le niveau de connaissance et d'application des procédures, consignes et/ou fiches réflexes prévues par le PSIP ;
- de renforcer les pratiques et réflexes du personnel impliqué dans la mise en œuvre du PSIP ;
- de renforcer la coordination des services internes ou externes de l'IP impliqués dans la mise en œuvre des réponses face à une menace ;
- d'adapter les révisions du PSIP en tenant compte des retours d'expérience.

Entraînement : L'efficacité de la mise en œuvre des dispositions du PSIP est vérifiée au moyen d'entraînements organisés par l'ASIP, avec une périodicité au minimum trimestrielle. Ces entraînements portent sur les parties du PSIP, notamment celles visant à faire face aux menaces.

Exercice : Les exercices peuvent comprendre la participation d'ASIP, des services de l'État, d'ASP et d'ASN. Ils sont organisés au moins une fois par année civile, l'intervalle entre les exercices ne dépassant pas 18 mois. Ces exercices visent en particulier à vérifier les communications, la coordination, la disponibilité des ressources et les capacités de réaction et d'intervention des services impliqués. Lorsque les exercices sont organisés avec l'implication des services de l'État, une prévenance et un accord préalable des services concernés est nécessaire.

Conseils complémentaires pour les instructeurs, relatifs à la programmation et à la périodicité des exercices et entraînements :

Les thèmes choisis des entraînements et des exercices doivent être en cohérence avec l'ESIP et les mesures adoptées par le PSIP. Ils doivent prendre en compte également les considérations du CLSP et le résultat des audits réalisés par la DGITM / DST / DSûT.

Conseils complémentaires pour les exploitants, relatifs à la formation initiale et continue des personnels, à la programmation et à la périodicité des exercices et entraînements :

En cas de d'utilisation d'un prestataire spécialisé, l'exploitant doit s'assurer notamment que le prestataire justifie des autorisations et habilitations concernant les activités privées de surveillance et de gardiennage réglementant les activités privées de surveillance et de gardiennage, de transport de fonds et de protection physique des personnes.

Les entraînements et exercices font l'objet d'un compte rendu écrit mentionnant au minimum le thème, la date et l'heure, les services et participants, le relevé des constats factuels (points forts, points de faiblesses et les non-conformités), les résultats obtenus et l'évaluation de leur efficacité par rapport aux dispositions prévues par le PSIP, les éventuelles mesures correctives prises, le responsable de la mise en œuvre du suivi ainsi que le délai de réalisation.

Le compte rendu est signé par l'ASIP et archivé au registre de sûreté, il porte la mention « Confidentiel Sûreté ». L'ASIP s'assure de la réalisation des actions prévues jusqu'à leur clôture et vérifie l'efficacité des nouvelles mesures décidées.

Des exemples concrets sont fournis en annexe n° 12.

Chapitre 10 : Informations communicables aux personnes chargées d'effectuer les visites de sûreté

Fiche 10.1 – Informations communicables aux personnes chargées d'effectuer les visites de sûreté

Le cadre réglementaire :

Arrêté du 22 avril 2008 article 7 du titre II et article 10 de l'annexe IV

Les objectifs :

L'arrêté du 22 avril 2008 mentionne qu'une partie du plan de sûreté de l'installation portuaire peut être diffusée aux personnes chargées d'effectuer les visites de sûreté. Il s'agit de :

- l'identification et coordonnées des personnes responsables en matière de sûreté (paragraphe 2.3) ;
- le système de signalisation des interdictions de pénétrer en ZAR et les procédures appliquées en cas d'incident de sûreté (paragraphe 5.3) ;
- la formation initiale et continue des agents chargés d'effectuer des visites de sûreté (paragraphe 9).

Les procédures appliquées en cas d'incident de sûreté font souvent l'objet de fiches réflexe pour chaque type d'incident (exemple : alerte à la bombe, détection d'objet suspect, prise d'otage).

Ce document constitue le volume 2 du plan de sûreté de l'installation portuaire. Ce document est initialement prévu aux installations avec zone d'accès restreint.

Il est diffusé avec la mention " Distribution Limitée Sûreté ".

Les conseils complémentaires :

Conseils complémentaires pour les instructeurs :

Les principaux documents constitutifs du volume 2 sont l'annuaire des personnes responsables en matière de sûreté et les fiches réflexes. L'instructeur veillera à la pertinence des informations contenues dans ces documents. De la qualité des fiches réflexes dépendra la valeur des entraînements. Ces fiches doivent mettre à contribution les agents de l'installation portuaire.

Conseils complémentaires pour les exploitants :

La création d'un volume II pour une IP sans ZAR est fortement conseillée. Ce document peut concerner les agents de sécurité et de surveillance. C'est eux qui sont susceptibles de réagir et d'informer en cas d'incident de sûreté. Il en va, de même des agents susceptibles d'intervenir dans les entraînements (et donc en cas d'incident de sûreté).

Pour les IP(s) avec ZAR, il faut, aussi, pouvoir étendre la diffusion du document à d'autres agents que ceux chargés d'effectuer les visites de sûreté.

Le volume 2 peut rappeler les consignes et les tâches de sûreté données aux agents, ainsi que la liste des points de contrôle à vérifier lors de rondes (caméras, portails...).

Annexes

Annexe 1 – Tableau relatif à l'auteur du PSIP et aux dates d'approbations

AUTEUR DU PSIP	Organisme	
	Adresse	
	Date de l'habilitation OSH	
	Nature de l'habilitation	
	Liste et date d'agrément des consultants de l'OSH ayant participé à la rédaction du PSIP	
Date de l'avis du CLSP sur l'ESIP		
Date de l'avis du CLSP sur le PSIP		
Date de l'approbation et date de fin de validité de l'ESIP		
Date de l'approbation du PSIP		
Date de fin de validité du PSIP		Alignée sur la date de fin de validité de l'ESIP

En annexe :

- arrêté préfectoral approuvant l'ESIP ;
- arrêté préfectoral approuvant le PSIP.

Si besoin :

ZAR n°	Date de l'arrêté préfectoral définissant la ZAR	Date de l'arrêté préfectoral définissant les taux de contrôle

Annexer au PSIP si besoin d'autres arrêtés intéressant la sûreté de l'installation portuaire (agrément des ASIP suppléants, désignation OIV...).

Annexe 2 – Exemple de tableau de synthèse de l'évaluation de sûreté

Propositions de mesures à la suite de l'approbation de l'ESIP du xx-xx-20xx

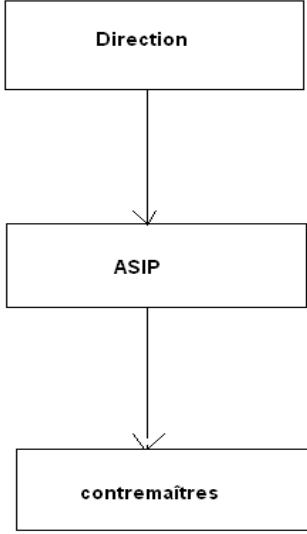
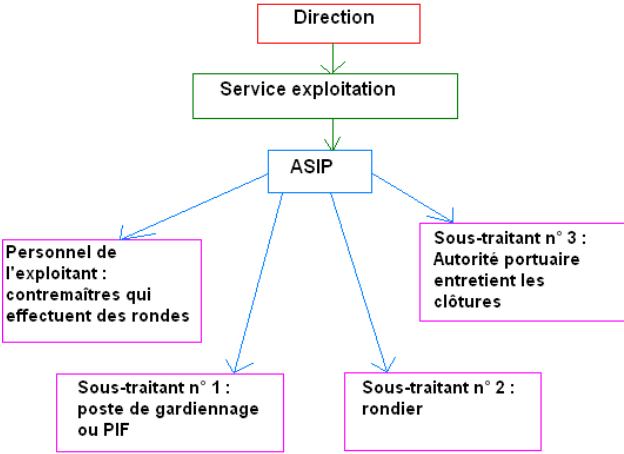
Les propositions de mesures préconisées dans l'ESIP approuvée le xx-xx-20xx, sont les suivantes :

PRIO	RECOMMANDATIONS	REPONSE APPORTEE – COMMENTAIRES
1		

Il s'agit ici de recopier textuellement le paragraphe 8 de l'ESIP (sans y changer quoi que ce soit, puisque approuvée par le préfet), en reprenant l'ordre de priorité et l'efficacité des contre-mesures.

Dans la dernière colonne « Réponse apportée – Commentaires » soit figure un renvoi automatique vers le paragraphe du PSIP apportant la réponse souhaitée (sous forme : Cf. § xxx), soit figure un commentaire précisant l'éventuel délai de réalisation de la contre mesure ou autre.

Annexe 3 – Organigrammes

Organigrammes – exemple n° 1 :	Organigrammes – exemple n° 2 :
 <pre> graph TD D[Direction] --> ASIP[ASIP] ASIP --> CM[contremaîtres] </pre>	 <pre> graph TD D[Direction] --> SE[Service exploitation] SE --> ASIP[ASIP] ASIP --> PE[Personnel de l'exploitant : contremaîtres qui effectuent des rondes] ASIP --> ST1[Sous-traitant n° 1 : poste de gardiennage ou PIF] ASIP --> ST2[Sous-traitant n° 2 : rondier] ASIP --> ST3[Sous-traitant n° 3 : Autorité portuaire entretient les clôtures] </pre>
<p>Dans cet exemple très simplifié, la sûreté repose uniquement sur :</p> <ul style="list-style-type: none"> • La Direction qui alloue les moyens matériels et humains ; • L'ASIP qui est sous l'autorité hiérarchique directe de la Direction et dont les missions sont définies dans le Code ISPS annexé au RE N° 725/2004 section A/17 ; • Les contremaîtres qui sont sous l'autorité de l'ASIP. On peut imaginer que les missions consistent principalement à effectuer des rondes de sûreté sur le terminal. 	<p>L'ASIP n'est plus sous l'autorité directe de la direction. Il est placé sous la hiérarchie d'un service intermédiaire. En revanche, il lui appartient de contrôler l'exécution des tâches de sûreté déléguées au personnel de l'exploitant (contremaîtres) et aux sous-traitants (sous-traitants n° 1, 2 et 3).</p> <p>On peut imaginer que les contremaîtres ont pour tâche principale d'effectuer des rondes de sûreté pendant les heures ouvrées (6h à 19h).</p> <p>La sûreté est sous-traitée à un 1er prestataire pour tenir un poste d'inspection filtrage (en ZAR) ou un poste de garde (terminaux non soumis à ZAR).</p> <p>En complément, l'exploitant fait appel à un second prestataire qui effectue des rondes de sûreté. On pourrait imaginer que ces rondes se fassent en dehors des heures des contremaîtres (de 19h à 6h).</p> <p>Enfin, parfois lorsque l'Autorité portuaire alloue des moyens matériels et/ou humains qui participent pleinement à la sûreté du terminal, on peut alors la considérer comme un sous-traitant à part entière. Ici l'Autorité portuaire finance et entretient les clôtures du terminal.</p>

Annexe 4 – Effectifs de l'exploitant

Provenance du personnel	Fonction	Effectifs			Nature de tâches			Contact permanent
		Niveau 1 ISPS	Niveau 2 ISPS	Niveau 3 ISPS	Niveau 1 ISPS	Niveau 2 ISPS	Niveau 3 ISPS	
Personnel de l'exploitant	ASIP	1	1	1	Voir section A/17.1 du Code ISPS annexé au RE ou fiche de poste			Permanence H24 répartie entre les 3 agents
Personnel de l'exploitant	ASIP suppléant	1	1	1	Voir A17.1 du RE725	Voir A17.1 du RE725 + 1 ronde de sûreté par escale	Voir A17.1 du RE725 + 2 rondes de sûreté par escale	
Personnel de l'exploitant	ASIP suppléant	1	1	1	Voir A17.1 du RE725	Voir A17.1 du RE725 + 1 ronde de sûreté par escale	Voir A17.1 du RE725 + 2 rondes de sûreté par escale	
<p>Commentaires : Les 3 ASIP sont à effectifs constants pour les 3 niveaux ISPS. Leurs missions en tant qu'ASIP sont clairement définies dans la section A/17.1 du Code ISPS annexé au RE725. Puis, à partir du niveau 2, les suppléants voient leurs missions se renforcer avec l'attribution de rondes de sûreté qui sont intensifiées avec l'élévation du niveau ISPS. Enfin, une astreinte est définie entre les 3 ASIP.</p>								
Personnel de l'exploitant	contremaître	1	2	2	Contrôle de l'état du matériel sûreté, 1 fois par semaine	Contrôle de l'état du matériel sûreté, 1 fois par jour	Installation portuaire est fermée, en cas de passage au niveau 3, le personnel de l'entreprise n'intervient plus	Heures ouvrées ou pendant l'escale
<p>Commentaires : En complément des 3 ASIP, l'exploitant s'appuie en partie sur son personnel, à savoir le contremaître. Ici, on lui attribue uniquement pour mission de contrôler l'état du matériel dédié à la sûreté.</p> <p>Au niveau 2 ISPS, un deuxième contremaître vient renforcer la fréquence des contrôles du matériel. Au niveau 3, on ne fait plus appel aux contremaîtres, l'installation étant fermée. Au niveau 3, on garde les mêmes effectifs qu'au niveau 2, mais l'impossibilité d'augmenter les effectifs est compensée par la fermeture de certains accès.</p> <p>Enfin, le(s) contremaître(s) intervient (nent) uniquement pendant les heures ouvrées ou pendant une escale.</p>								

Personnel de l'exploitant	manutentionnaire	1	1	2	Contrôle de scellés	Contrôle de scellés		Heures ouvrées
Personnel de l'exploitant	Responsable qualité	1	1	1	Audit interne			
<p>Commentaires : Il faut essayer de lister l'ensemble du personnel à qui on confie des tâches de sûreté. Ici, on s'appuie sur du personnel manutentionnaire dont les tâches sont distinctes des contremaîtres évoqués ci-avant. Les manutentionnaires ont pour tâche principale de contrôler les scellés des conteneurs. Les effectifs sont renforcés avec l'élévation du niveau ISPS.</p> <p>On peut être très précis dans le découpage des tâches, notamment en citant la personne chargée des audits internes.</p>								
Entreprise sous-traitante n° 1	Gardien	1	2	4	Inspection-filtrage contrôle documentaire, rapprochement d'identité, fouille visuelle des bagages... selon les taux définis par niveaux ISPS par la préfecture pour les ZAR			1 heure avant les opérations commerciales + pendant l'escale
Entreprise sous-traitante n° 2	Rondier	1	1	2	1 Ronde de sûreté la nuit	2 rondes de sûreté aléatoires	3 rondes de sûreté aléatoires	Hors opérations commerciales et/ou pendant l'escale
<p>Commentaires : L'exploitant fait appel à un (ou des) prestataire(s) de sûreté dont les effectifs et les missions peuvent évoluer avec le niveau ISPS. Les horaires de travail doivent être précisés. Ce peut être pendant ou en dehors des opérations commerciales du navire, pendant toute la durée de l'escale, pendant les heures ouvrées...</p> <p>L'exploitant peut multiplier le nombre de prestataires avec des tâches clairement réparties pour chacun et déclinées par niveaux ISPS.</p>								

Annexe 5 – Modalités de communication avec le navire

Le cadre réglementaire :

Code ISPS annexé au RE N° 725/2004

Sections A :

7.7, en cas de passage à un niveau supérieur

7.7.1 Dans ce cas, l'agent de sûreté du navire doit rester en liaison avec l'agent de sûreté de l'installation portuaire et coordonner les mesures appropriées, si nécessaire

11 Agent de sûreté de la compagnie

11.2.10 veiller à l'efficacité de la communication et de la coopération entre l'agent de sûreté du navire et les agents de sûreté pertinents des installations portuaires

14.5 l'agent de sûreté de l'installation portuaire et l'agent de sûreté du navire doivent rester en liaison et doivent coordonner les mesures appropriées

16.3.7 des procédures concernant l'interface avec les activités liées à la sûreté des navires

17.2.13 aider l'agent de sûreté du navire à confirmer, sur demande, l'identité des personnes cherchant à monter à bord du navire

Section B :

B16.8.13 les procédures permettant d'aider les agents de sûreté du navire à confirmer l'identité des personnes cherchant à monter à bord du navire, sur demande

Modalités de communication avec le navire – coordination des mesures :

Le PSIP devrait préciser comment l'ASIP (ou personnel exploitation) et l'ASN peuvent entrer en contact. Est-ce qu'ils passent par l'agent maritime, est-ce qu'ils ont des radios VHF ? Le but est de décrire par quel moyen l'ASIP ou un personnel en charge de la sûreté de l'IP pourra communiquer rapidement avec l'ASN plus particulièrement en cas d'alerte. En particulier, pour les navires réalisant des rotations régulières, comme les ferries, l'ASIP doit être en mesure d'entrer, à tout moment, en communication avec l'ASN, sur demande des services de l'Etat.

Le PSIP devrait mentionner si l'ASIP doit transmettre des consignes particulières à l'ASN (procédure de sécurité de l'exploitant que doit respecter le navire à l'approche du terminal ; procédures de sûreté comme la diffusion de digicodes...).

Procédures permettant d'aider les agents de sûreté du navire à confirmer l'identité des personnes cherchant à monter à bord du navire :

L'exploitant doit aider l'ASN à vérifier l'identité des personnes lorsqu'il le demande. Ainsi, le contrôle d'identité doit être réalisé avant d'accéder au navire, soit à l'entrée de l'installation portuaire. Pour que l'exploitant puisse correctement réaliser des contrôles d'accès à l'entrée de l'installation portuaire, il doit être en mesure de savoir quelles sont les personnes attendues sur le navire. Il peut s'agir de visiteurs, du personnel du navire, d'un visiteur imprévu (cas d'un médecin en urgence).

Le PSIP devrait décrire comment l'ASIP peut se procurer la crew list (la liste du personnel de bord et la liste des visiteurs attendus sur le navire). L'ASIP pourra se procurer une telle liste auprès de l'agent maritime ou directement auprès de l'ASN. Le PSIP précisera alors comment l'exploitant exploite cette crew list pour contrôler l'identité des personnes avant de monter à bord.

Procédure pour les déclarations de sûreté – DOS :

Une déclaration de sûreté est signée entre les deux partenaires navire/installation portuaire lorsqu'il en a été décidé ainsi par les gouvernements respectifs ou que le port ou le navire le jugent nécessaire. La DOS est utilisée lorsque le navire est exploité à un niveau de sûreté différent de celui de l'installation portuaire.

Annexe 6 – Gestion documentaire et protection du plan de sûreté de l'installation portuaire

	Non Protégé	Distribution. Limitée Sûreté	Confidentiel Sûreté
Sujet traité	Documentation Générale	Tâches de sûreté	Doctrine, plans, études, caractéristiques des équipements
Destinataires	Tous	Agents d'exécution des tâches de sûreté	Personnel identifié ayant à en connaître
Copie	Tous	Besoin d'en connaître	Exemplaire numéroté et enregistré
Diffusion interne /externe	Oui	Besoin d'en connaître	Personnel identifié ayant à en connaître
Courrier interne	Pas d'enveloppe	Enveloppe	Enveloppe
Courrier externe	Enveloppe normale	Double Enveloppe	Double enveloppe Recommandé AR
Mention	Néant	Diffusion restreinte ou Distribution Limitée Sûreté	Confidentiel Sûreté
Conservation	Sans Objet	Armoire ou tiroir fermant à clé	Armoire ou coffre de sûreté
Destruction	Sans Objet	Lacération	Détruit par lacération

Fonctions	Niveaux de protection des informations		
	Non Protégé	Distribution Limitée Sûreté	Confidentiel Sûreté
Directeur du Terminal	X	X	X
ASIP	X	X	X
ASIP suppléants	X	X	X

Attestation de reconnaissance de responsabilité

Nom et prénom :

Fonction :

Employeur :

Je, soussigné(e), déclare être pleinement conscient(e) de mes responsabilités en ce qui concerne la sauvegarde des informations protégées contenues dans le plan de sûreté de l'Installation Portuaire "XXX" du GPM de XXX et je reconnais être informé(e) des conséquences prévues par les dispositions légales en vigueur, notamment pour le cas où, sciemment ou par négligence, je laisserais parvenir ces informations à des personnes non autorisées à en avoir connaissance, y compris après la cessation de mes fonctions.

Date :

Signature de l'intéressé(e) :

Annexe 7 – Identification et caractéristiques des zones d'accès restreint

- Catégories de personnels et d'activités concernés :

Catégories de personnels, comme défini par le code des transports dans son article R. 5332-37 :	Catégories de personnels et d'activités concernés par la ZAR
I : les personnels de l'autorité portuaire, les personnes de l'exploitant de l'installation portuaire, les personnels des services sociaux, ainsi que les personnels intervenant habituellement dans la ZAR pour leur activité professionnelle, munis d'une habilitation et d'un titre de circulation	
II : les fonctionnaires et agents chargés d'exercer habituellement les missions de police, de sécurité et de secours sur le port, munis d'une habilitation sauf en ce qui concerne les fonctionnaires et agents de l'État en uniforme ou munis d'un ordre de mission ou d'une commission d'emploi, et d'un titre de circulation	
III : les personnels navigants des navires accueillis par l'installation portuaire et les personnes se trouvant à bord de ces navires pour y effectuer des tâches professionnelles liées à l'exploitation du navire, munis d'un titre de circulation temporaire	
IV : les personnes admises pour une courte durée dans la zone d'accès restreint, munies d'un titre de circulation temporaire	
V : les passagers des navires accueillis par l'installation portuaire, munis du titre de transport approprié	
VI : les agents des services de police, de sécurité ou de secours, dans le cadre de leurs interventions d'urgence	
VII : les représentants désignés par les organisations syndicales représentatives des personnels navigants des navires et des personnes se trouvant à bord de ces navires pour y effectuer des tâches professionnelles liées à l'exploitation du navire, munis d'un titre de circulation temporaire ou, exceptionnellement, d'une habilitation et d'un titre de circulation permanent	
Catégories d'activités	
Poids lourds	
Transports en commun	
Véhicules légers	
Deux roues	

• Flux d'entrée et nombre de titres de circulation :

Catégorie de personnels et d'activités concernés	Année N		Année N+1	
	Nombre de titres de circulation émis	Flux d'entrée comptabilisés au(x) PIF	Nombre de titres de circulation émis	Flux d'entrée comptabilisés au(x) PIF
I :				
II :				
III :				
IV :				
V :				
VI :				
VII :				
Poids lourds				
Transports en commun				
Véhicules légers				
Deux roues				

Annexe 8 – Règles de surveillance en ZAR

Thème	Provenance du personnel	Mesures de sûreté adoptées	Effectif par niveaux ISPS			Délai de mise en œuvre d'une élévation du niveau ISPS	
			Niveau 1	Niveau 2	Niveau 3	Délai de passage niveau 2 ISPS	Délai de passage niveau 3 ISPS
Eclairage							
Rondes							
Vidéo							

Pourquoi rappeler la provenance du personnel pour les missions de surveillance ?

Ce rappel permet de voir la cohérence avec les mesures du chapitre 4, en particulier le paragraphe 4.2 qui décrit les effectifs ayant des tâches de sûreté.

Pourquoi introduire la notion de délai de mise en œuvre ?

Vis-à-vis de la réglementation, il n'y a pas d'obligation à introduire une telle notion dans son PSIP. Toutefois, cela permet de voir sous quel délai l'exploitant est capable de réagir.

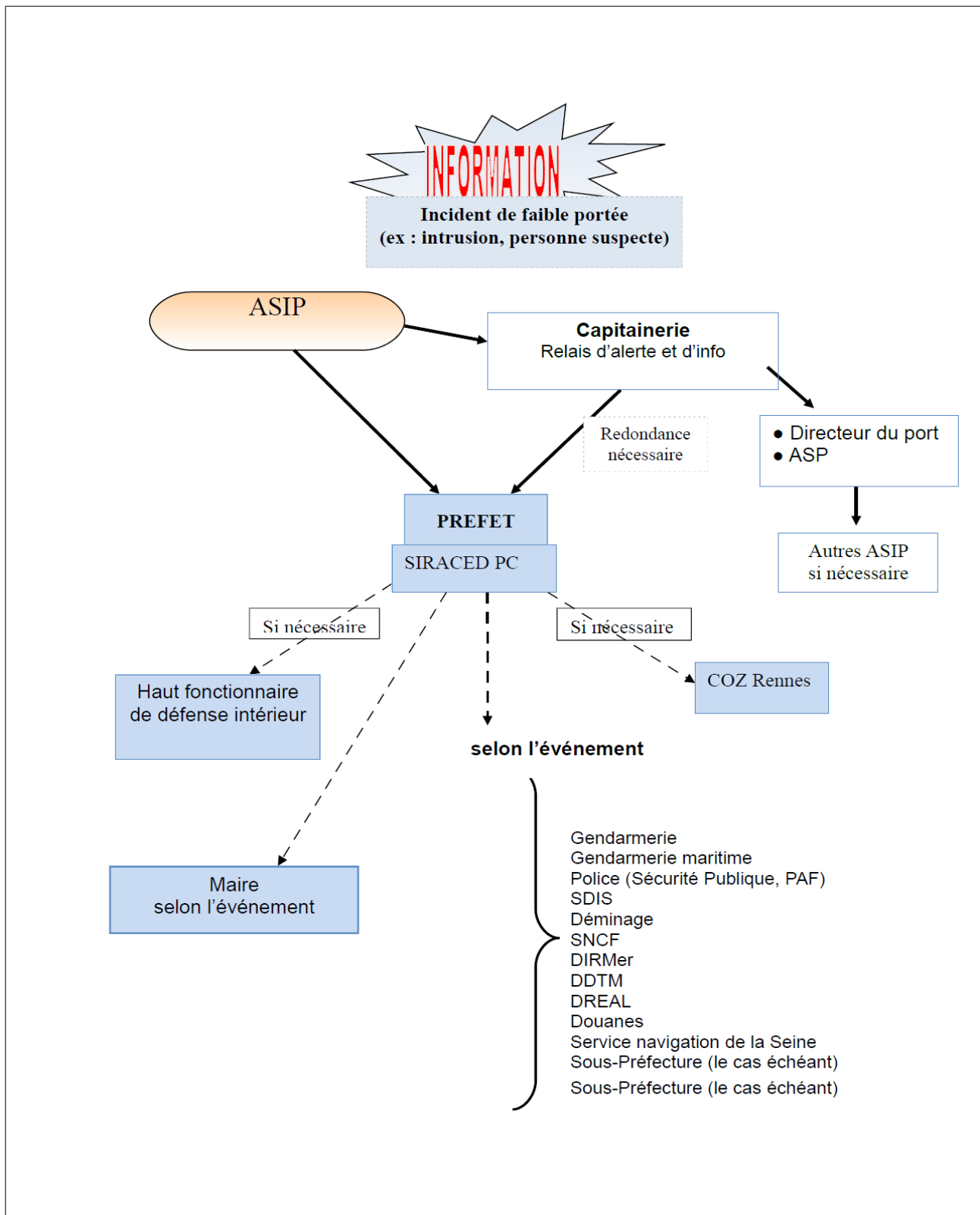
En réalité, si l'exploitant ne fixe pas de délai de mise en œuvre, c'est qu'il est capable de réagir de manière immédiate en cas de passage aux niveaux 2 et 3 ISPS.

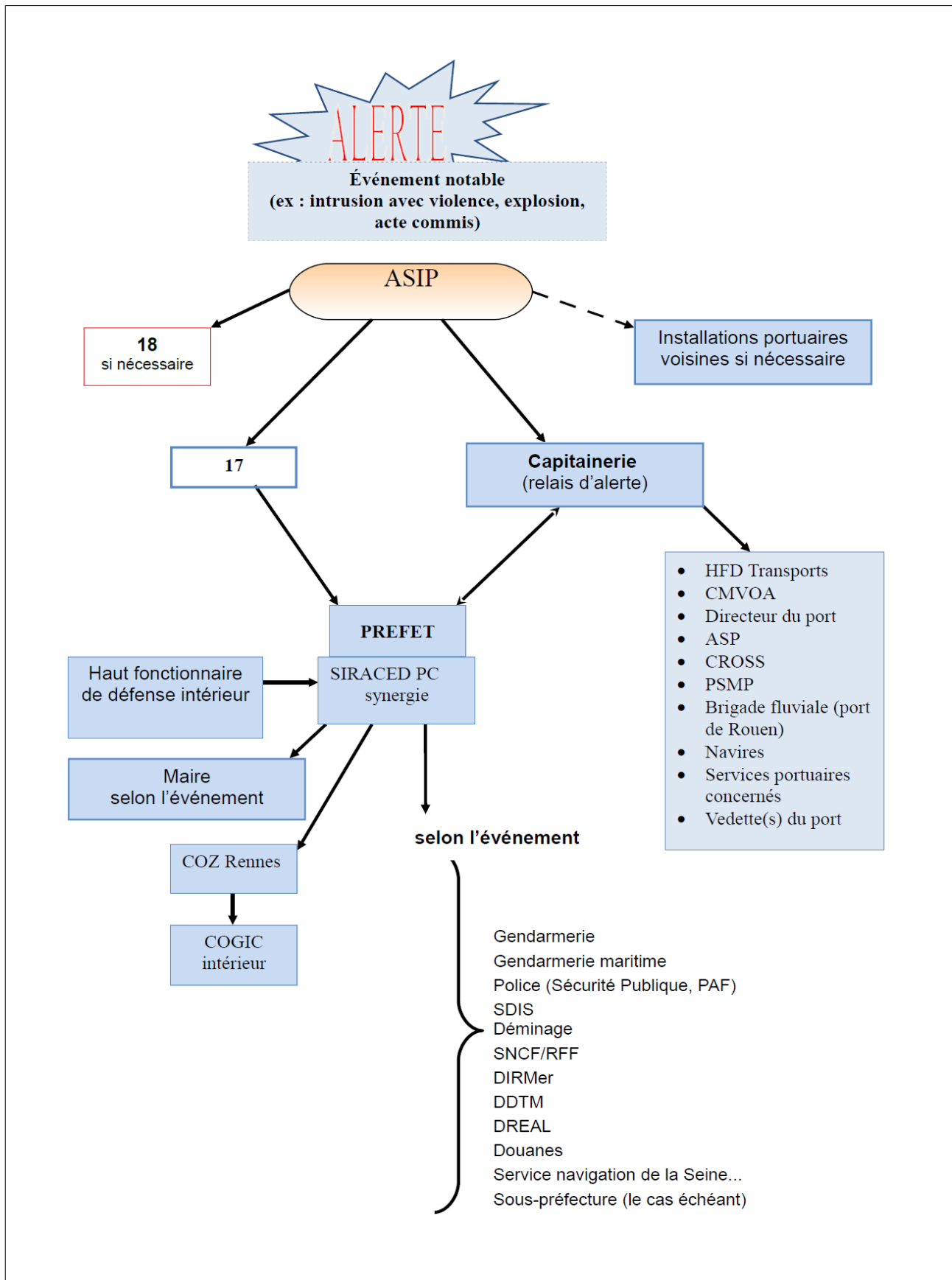
Si le niveau ISPS s'élève, l'exploitant doit réfléchir aux mesures de sûreté qu'il peut mettre en œuvre. Par exemple :

- de manière immédiate : l'ASIP intensifie ses rondes ;
- sous 24h – 48h : un prestataire de sûreté prend le relais, la prestation est définie dans un contrat ;
- au-delà de 48h : les moyens sont encore intensifiés...

Les temps d'intervention des prestataires de sûreté sont à préciser dans le cahier des charges techniques et particulières. Si le délai d'intervention du prestataire de sûreté est trop long, l'exploitant devrait préciser s'il peut mettre en place des mesures palliatives en attendant l'arrivée de renforts.

Annexe 9 – Exemple de schémas type de transmission d'alerte





Annexe 11 – Exemples de fiches réflexes

A L'OCCASION DU SERVICE, VOUS POUVEZ ETRE DESTINATAIRE D'UN APPEL ANONYME DE MENACE CONTRE LES BIENS OU LES PERSONNES

CE PEUT-ETRE :

- *UNE ALERTE A LA BOMBE INDIQUANT LE LIEU ET L'HEURE DE L'EXPLOSION*
- *UNE PRISE D'OTAGE*
- *UNE ATTAQUE EXTERIEURE*
- *UN DETOURNEMENT DE NAVIRE*
- *UNE AUTRE MENACE*
- *UNE INFORMATION SUR UNE PERSONNE OU UN OBJET SUSPECT*

VOUS DEVEZ IMPERATIVEMENT et IMMEDIATEMENT :

RENDRE COMPTE DE CET APPEL

➤ **A L'ASIP OU A SON SUPPLEANT (06 XX XX)**

Qui déclenche l'alerte.

Qui avise les services de Police.

SANS OUBLIER DE :

- **NOTER PRECISEMENT LA DATE ET L'HEURE L'APPEL**
- **NOTER LE MAXIMUM D'INDICATIONS SUR L'INTERLOCUTEUR :**
 - *(HOMME OU FEMME, TIMBRE DE VOIX, ACCENT, ETC...)*
- **NOTER LE MAXIMUM D'INDICATIONS SUR L'OBJET DE L'APPEL :**
 - *(LIEU ET HEURE DE LA MENACE ANNONCEE, ETC...)*
- **RENDRE COMPTE EVENTUELLEMENT DES DIFFICULTES RENCONTREES**
- **ETABLIR A L'ISSUE UN RAPPORT CIRCONSTANCIE**

DECOUVERTE D'UN COLIS SUSPECT

Sécurité = 100 m

**A L'OCCASION DU SERVICE OU SUR APPEL D'UN TIERS, VOUS
POUVEZ ETRE EN PRESENCE D'UN OBJET SUSPECT**

(BAGAGE, CAISSE A OUTIL, OU COLIS ABANDONNE...)

IL DOIT ETRE SYSTEMATIQUEMENT CONSIDERE COMME DANGEREUX !

VOUS DEVEZ IMPERATIVEMENT :

ALERTER

- **L'ASIP ou son suppléant (06 XX XX)**

Qui déclenche l'alerte.

Qui avise les services de Police.

- COMMUNIQUER SA LOCALISATION
- LE DECRIRE (*FORME - ASPECT EXTERIEUR - DIMENSIONS APPROXIMATIVES...*) POUR FACILITER L'INTERVENTION DES ARTIFICIERS
- NE PAS LE TOUCHER, LE MANIPULER OU LE DEPLACER
- NE PAS UTILISER D'APPAREILS DE RADIOCOMMUNICATION A PROXIMITE
- NE PAS PRODUIRE DE VIBRATIONS SONORES, THERMIQUES OU MECANIQUES A PROXIMITE
- RESTER ELOIGNE DE L'OBJET : **100 m**
- BALISER L'ENDROIT (*en utilisant tout matériel disponible sur place : barrière, chaises, rubalise, etc. à 100m du bagage ou de l'objet*)
- INTERDIRE L'ACCES AUX PERSONNES NON-AUTORISEES (*mise en place d'un périmètre de sécurité provisoire. Il sera ensuite adapté selon les prescriptions des services du déminage*)
- EMPÊCHER LES RASSEMBLEMENTS DE CURIEUX
- RECHERCHER L'EVENTUEL PROPRIETAIRE, *si possible par annonces sonores (gare maritime)*
- PREPARER L'EVACUATION DE L'IP ou de la gare maritime
- RENDRE COMPTE DES DIFFICULTES RENCONTREES
- ETABLIR A L'ISSUE UN RAPPORT CIRCONSTANCIE (*indiquer chronologiquement les mesures mises en place*).

DECOUVERTE D'UN VEHICULE SUSPECT EN STATIONNEMENT

Sécurité = 200 m

**A L'OCCASION DU SERVICE OU SUR APPEL D'UN TIERS, VOUS POUVEZ
ETRE EN PRESENCE DE CE TYPE DE VEHICULE RESTE EN
STATIONNEMENT D'UNE FACON INSOLITE**

IL DOIT ETRE SYSTEMATIQUEMENT CONSIDERE COMME DANGEREUX

VOUS DEVEZ IMPERATIVEMENT :

ALERTER

- **L'ASIP ou son suppléant (06 XX XX)**

Qui déclenche l'alerte.

Qui avise les services de Police.

- **COMMUNIQUER SA LOCALISATION**
- **LE DECRIRE (TYPE, CARACTERISTIQUE, NUMERO MINERALOGIQUE...)**
- **RESTER ELOIGNE DU VEHICULE : 200 m**
- **BALISER L'ENDROIT**
- **INTERDIRE L'ACCES AUX PERSONNES NON-AUTORISEES (*mise en place d'un périmètre de sécurité provisoire. Il sera ensuite adapté selon les prescriptions des services du déminage*)**
- **EMPÊCHER LES RASSEMBLEMENTS DE CURIEUX**
- **RENDRE COMPTE DES DIFFICULTES RENCONTREES**
- **ETABLIR A L'ISSUE UN RAPPORT CIRCONSTANCIE (*indiquer chronologiquement les mesures mises en place*).**

DECOUVERTE D'UNE PERSONNE SUSPECTE PENETRANT OU SE TROUVANT DANS UNE ZONE NON LIBREMENT ACCESSIBLE AU PUBLIC (IP OU ZAR)

**A L'OCCASION DU SERVICE OU SUR APPEL D'UN TIERS, VOUS POUVEZ
ETRE EN PRESENCE D'UNE PERSONNE SUSPECTE**

ELLE DOIT ETRE CONSIDEREE COMME

« INTRUS POSSIBLE »

VOUS DEVEZ IMPERATIVEMENT :

ALERTER

- **L'ASIP ou son suppléant (06 XX XX)**

Qui déclenche l'alerte.

Qui avise les services de Police.

MENTIONNER LE LIEU ET LES CIRCONSTANCES DE LA DECOUVERTE

EFFECTUER DES RECHERCHES :

- **S'ASSURER QU'IL N'Y A PERSONNE D'AUTRE**
- **S'ASSURER QU'IL N'Y A PAS DE COLIS SUSPECT**

RASSEMBLER LE MAXIMUM D'INFORMATION

- **Enregistrer l'incident**
- **Informers les autorités**

DECOUVERTE D'UN INTRUS

L'INTRUSION PEUT AVOIR POUR BUT :

- *L'ÉMIGRATION CLANDESTINE*
- *L'ACTE MALVEILLANT*
- *L'ACTE DE TERRORISME*

LA LUTTE CONTRE L'INTRUSION PASSE AVANT TOUT PAR DES CONTRÔLES RENFORCÉS AU MOMENT DES ÉCHANGES PORTUAIRES

**LAISSER L'INTRUS À L'ENDROIT OÙ IL A ÉTÉ DÉCOUVERT, OU POUR SA
SÉCURITÉ, L'ISOLER DANS UN LOCAL GARDÉ**

RELEVER L'IDENTITÉ DE L'INTRUS

SURVEILLER L'INTRUS JUSQU'À L'ARRIVÉE DES FORCES DE L'ORDRE

ALERTER :

- **L'ASIP (06 XX XX)**

ESSAYER DE SAVOIR :

- *S'IL EST SEUL*
- *SI D'AUTRES INTRUS SONT SUR LA ZONE PORTUAIRE.*
- *COMMENT IL EST ENTRÉ.*

SI LES RÉPONSES SONT DOUTEUSES :

- *EFFECTUER DES RECHERCHES.*
- *FAIRE UN CONTRÔLE DES CLOTURES*

AVISER LES AUTORITES

- **REMETTRE L'INTRUS AUX FORCES DE L'ORDRE**
- **LEUR DEMANDER DE FAIRE DES PATROUILLES EN ZONE
PORTUAIRE**

EVACUATION

ALERTER LES SERVICES DE POLICE ET DE SECOURS

**L'ÉVACUATION EST DÉCIDÉE PAR L'EXPLOITANT OU PAR L'ASIP APRES
AVIS DES SERVICES DE SECOURS**

AVISER

- *LA CAPITAINERIE (02 XX XX)*
- *LE BORD SI UN NAVIRE EST À QUAI.*
 - *LE PERSONNEL DE L'IP, PAR RADIO ET PAR TÉL, AFIN QU'IL SE DIRIGE
VERS LA SORTIE.*
 - *LES AUTORITES, DE L'ÉVACUATION ET DES MOTIFS DE CETTE OPÉRATION*

**LE PERSONNEL DÉSIGNÉ PAR L'ASIP SE REND EN VÉHICULE SUR TOUTE
L'IP AFIN D'INVITER LE PERSONNEL RECENSE À REJOINDRE LES SORTIES**

LES BÂTIMENTS SONT ÉVACUÉS

**L'ASIP OU LE PERSONNEL DESIGNÉ PAR SES SOINS S'ASSURE QUE LES
BÂTIMENTS SONT VIDES. IL INVITE LE PERSONNEL À QUITTER LES LIEUX
ET SORT EN DERNIER**

LES PORTES DES BÂTIMENTS RESTENT OUVERTES

**LE PERSONNEL ET LES VISITEURS RECENSÉS SONT REGROUPÉS SUR LES
POINTS DE RALLIEMENTS POUR VÉRIFICATION ET COMPTAGE**

**LES RESPONSABLES SÉCURITÉ ET SÛRETÉ DU SITE RESTENT À
DISPOSITION DES SERVICES D'INTERVENTION**

**LES FILTRAGES ET INTERDICTIONS SUR LES VOIES PUBLIQUES
PORTUAIRES SONT À LA CHARGE DES SERVICES DE POLICE ET DE
GENDARMERIE**

PRISE D'OTAGES

INFORMER L'ASIP (06 XX XX) ET LA CAPITAINERIE (02 XX XX)

FACE AU(X) PRENEUR(S) D'OTAGES :

- **OPPOSER LE PLUS GRAND CALME A L'AGRESSIVITE**
- **PRENDRE EN COMPTE LES EXIGENCES SANS DISCUTER**
- **LAISSER PARLER LES AGRESSEURS**
- **DONNER LE MINIMUM D'INDICATIONS EN RETOUR**
- **NE PAS FIXER D'ULTIMATUM**
- **NE PAS PROPOSER DE SOLUTION DE RECHANGE**
- **NE RIEN OFFRIR, NE RIEN PROMETTRE**
- **NE PAS ESSAYER DE MENTIR NI TROMPER**
- **NE JAMAIS DIRE NON**

PREMIER INTERVENANT :

- **NE PAS RECHERCHER LE CONTACT D'INITIATIVE**
- **EVITER D'AGGRAVER LA SITUATION**
- **ESSAYER DE COLLECTER DES RENSEIGNEMENTS**
- **NE PAS IMPLIQUER DES TIERS ET/OU DES AUTORITES**
- **NE PAS CHERCHER A NEGOCIER (C'EST L'AFFAIRE DES SPECIALISTES)**
- **ETRE UN TRAIT D'UNION ENTRE LES RAVISSEURS ET LES NEGOCIATEURS**
- **NE PAS PANIQUER ET ETRE ATTENTIF AUX PROPOS TENUS**
- **N'ECARTER AUCUNE REVENDICATION**
- **RENDRE COMPTE AUX AUTORITES ET AUX NEGOCIATEURS**

A L'EXTERIEUR DE L'ACTION :

- **ISOLER LA ZONE DE LA PRISE D'OTAGES**
- **PREVENIR LES FORCES DE L'ORDRE DES QUE POSSIBLE**
- **PLACER LES VOIES D'ACCES SOUS CONTROLE**
- **RASSEMBLER LES PLANS ET AUTRES INFORMATIONS UTILES SUR LA ZONE**
- **AVERTIR LES NAVIRES A QUAI (RELEVAGE DES COUPEES, PERSONNE SUR LE PONT)**
- **SUSPENDRE LES ACTIVITES PORTUAIRES ET PREPARER LES MESURES D'EVACUATION**
- **PREPARER LE TERRAIN POUR LES EQUIPES SPECIALISEES (NEGOCIATEURS)**

Annexe 12 – Exemples pour les entraînements et les exercices

Préalablement à l'organisation d'exercices et d'entraînements, l'exploitant devrait examiner la liste des menaces possibles listées dans la section B/15.11 du Code ISPS annexé au RE N° 725/2004.

Quelques exemples de mise en œuvre de simulation d'entraînement :

Il s'agit de mettre en situation le personnel contrôlé à partir de thèmes préparés pour lesquels des réponses précises sont attendues.

- « Il est demandé à l'ACVS de procéder à l'accueil et à la mise en œuvre des contrôles de sûreté (fouille/palpation) d'une personne ; vous conservez dissimulé dans votre poche un couteau ou autres articles prohibés factices » ;
- « Deux individus suspects se présentent au niveau de la clôture (ou poste de contrôle) et font un signe à l'ACVS. À l'approche de l'ACVS, l'un des deux hommes le menace avec un pistolet factice et exige de pénétrer dans la ZAR » ;
- « La femme du commandant d'un navire se présente au poste d'inspection filtrage de la ZAR et demande à accéder au navire » ;
- « L'ACVS reçoit un appel téléphonique, l'interlocuteur précise qu'une bombe a été posée à proximité du navire/sur le quai/...une musique est perceptible en fond, l'interlocuteur se revendique d'un groupe terroriste » ;
- « Un feu se déclenche sur les quais à proximité des navires (réaliser une photo « montage » avec des flammes pour permettre de visualiser l'incident), le feu est violent et nécessite l'intervention des secours » ;
- « Un mécanicien se présente à l'entrée de la ZAR afin de procéder à un dépannage sur un navire à quai. Une arme factice est dissimulée sous son blouson, l'ACVS est pris en otage » ;
- « Faire déclencher réellement un système d'alarme à l'insu du personnel en charge d'agir (prendre les mesures de sécurité pour éviter un effet de panique), apprécier la prise en compte de l'alarme et la mise en œuvre des actions réflexes » ;
- « Deux personnes se revendiquant fonctionnaires de police se présentent à l'entrée de la ZAR afin de procéder à un contrôle sur le navire à quai » ;
- « Un homme se présente à l'entrée de la ZAR et souhaite accéder au navire pour des contrôles. Il ne parle pas français » ;
- « Des personnes suspectes sont présentes dans la ZAR (clandestins ?, voleurs ?..., apprécier les actions des personnes en charge d'agir ?) » ;
- « Signaler la présence d'un colis suspect (déposé à l'insu des personnes), des fils sortent avec un interrupteur ».

Exemple de mise en situation théorique d'entraînement :

Il s'agit d'interviewer la personne contrôlée à partir des éléments du plan de sûreté, des fiches réflexes ou procédures de contrôle du PSIP. Pour exemple, les thèmes de questionnement :

- Conditions d'accès et de circulation en zone d'accès restreint ;
- Règles applicables aux véhicules ; Personnels navigants et autres personnels travaillant à bord des navires ;
- Relèves d'équipage, des personnels navigants des navires accueillis et des personnes se trouvant à bord des navires pour y effectuer des tâches professionnelles liées à l'exploitation du navire ;
- Conditions d'accès du personnel du site, des entreprises extérieures ;

- Condition d'accès des visiteurs ;
- Conditions d'accès des personnes titulaires d'un titre de circulation permanent ou temporaire (R. 5332-37 du code des transports), fonctionnaires et agents publics exerçant des missions d'évaluation ou de contrôle en matière de sûreté ou de sécurité munis d'un titre national mentionné à l'article R. 5332-38 du même code ;
- Conditions d'accès des agents et véhicules des services de police, de sécurité et de secours dans le cadre d'une intervention d'urgence ;
- Conditions des avitaillements du navire « matériel et marchandise » ;
- Conditions d'accès pour les avitaillements du navire « chargement/déchargement d'huile » ;
- Contrôle test des équipements de sûreté ;
- Palpation, fouilles, inspection ;
- Déontologie des visites de sûreté ;
- Comportement vis-à-vis des personnes réfractaires ;
- Découverte d'un article prohibé ;
- Refus de se soumettre à la palpation, fouille, inspection ;
- Présence de clandestins ou intrusion illicite ;
- Présence d'individus ou véhicules suspects ;
- Présence en ZAR d'une petite embarcation, nageur, plongeur ;
- Découverte d'un objet suspect ;
- Découverte d'une rupture dans la clôture ;
- Incident de fonctionnement du système de contrôle d'accès ;
- Panne du détecteur de métaux, radio, contrôleur de ronde ;
- Panne d'un dispositif d'éclairage de la ZAR ;
- Déclaration d'une perte d'un titre de circulation ;
- Principes généraux et objectifs de la sûreté ;
- Mesures élémentaires et de vigilance de sûreté ;
- Les correspondants privilégiés en cas d'incidents de sûreté ;
- Incident lors d'un avitaillement d'un navire ;
- Incident lors d'une relève d'équipage ;
- Alerte à la bombe ;
- Conduite à tenir en cas de plan d'opération interne / évacuation ;
- Prise d'otage de l'Agent Chargé des Visites de Sûreté au poste de sûreté ;
- Prise d'otage du navire ;
- Déclenchement de l'alarme intrusion ;
- Incident de fonctionnement du système de vidéoprotection ;
- Connaissance du volume 2 du PSIP ;
- Modalité d'application du taux de contrôle de sûreté imposé par le préfet ;
- Changement de niveau de sûreté après la diffusion d'un message provenant des autorités françaises suite à une menace importante.

Quelques exemples de mise en œuvre d'exercice :

Il peut s'agir de simuler un exercice à partir d'une menace (qui peut être choisie parmi les thèmes de l'entraînement) mais qui imposera de mettre en œuvre des actions transversales en impliquant les services internes de l'IP, et/ou le navire et/ou l'ASP et/ou les services de l'État (préfecture, forces de police, douane...)

Pour éviter toute interprétation, toutes les actions verbales, écrites (fax ou courriel) ou appels téléphoniques doivent être précédés de la mention « ENTRAÎNEMENT ou EXERCICE DE SURETE » répétée trois fois.

L'exercice peut également prendre la forme d'un séminaire ou réunion autour des thématiques de sûreté regroupant les ASIP des IP avec l'ASP et/ou les services de l'État. Pourront être examinés à cette occasion, les retours d'expérience des entraînements et exercices réalisés par les ASIP, les incidents de sûreté, les difficultés particulières en matière de sûreté, les leçons à tirer, l'évolution réglementaire...

Tableau d'enregistrement des modifications ou compléments apportés au document

Numéro de la modification ou du complément	Date de la modification ou du complément	Dispositions avant modifications ou complément / n° de fiche	Dispositions après modifications ou complément / n° de fiche

Sigles et abréviations

a - Sigles et abréviations nationaux

ACVS : agent chargé des visites de sûreté

AIPPP : autorité investie du pouvoir de police portuaire qui désigne le représentant de l'État responsable des opérations de police sensibles

Art. : article

ASC : agent de sûreté de la compagnie

ASIP : agent de sûreté de l'installation portuaire

ASN : agent de sûreté du navire

ASP : agent de sûreté portuaire

Audit : expertise par un agent compétent et impartial aboutissant à un jugement sur le plan de sûreté portuaire et sur les mesures de sûreté mise en place

Autorité portuaire : autorité responsable des questions de sûreté à terre dans un port donné

CCTP : cahier des clauses techniques particulières

CD : Confidentiel Défense

CE : commission européenne

CEZAR : contrôle d'entrée en zone d'accès restreint

CLSP : comité local de sûreté portuaire

CMVOA : centre ministériel de veille opérationnelle et d'alerte

Code ISPS : (*International Ship and Port Facility Security Code*) code international pour la sûreté des navires et des installations portuaires

COGIC : centre opérationnel de gestion interministérielle des crises

COZ : centre opérationnel zonal

CPM : code des ports maritimes (comme cela a été le cas pour sa partie législative, sa partie réglementaire a vocation à être intégrée au code des transports)

CROSS : centre régional opérationnel de surveillance et de sauvetage

DAM : direction des affaires maritimes de la direction générale des infrastructures, des transports et de la mer

DCPAF : direction centrale de la police aux frontières

DDTM : direction départementale des territoires et de la mer

DGITM : direction générale des infrastructures, des transports et de la mer au sein du ministère de l'écologie, de l'énergie, du développement durable et de la mer. C'est l'autorité maritime compétente au sens de l'article 2.7 du Règlement (CE) N° 725/2004. La DGITM a en charge l'ensemble des sujets relatifs aux transports terrestres et maritimes.

DIRMer : direction interrégionale de la mer

DoS : acronyme anglais désignant la Déclaration de sûreté. C'est un document contresigné dans des cas particuliers par le capitaine du navire ou l'ASN et l'ASIP afin de préciser les obligations incombant au navire, d'une part, et à l'IP, d'autre part, en matière de sûreté.

DST : direction des services de transport de la direction générale des infrastructures, des transports et de la mer

DREAL : direction régionale de l'environnement, de l'aménagement et du logement

DSûT : département de la sûreté dans les transports, a repris notamment les missions de la mission sûreté défense (MSD)

DTMPL : direction du transport maritime, des ports et du littoral

EEI : engin explosif improvisé

ESIP : évaluation de sûreté de l'installation portuaire

ESP : évaluation de sûreté portuaire

Exploitant : exploitant d'une installation portuaire ou d'un port, responsable notamment du plan de sûreté de son installation et de sa mise en œuvre

GISIS : Global Integrated Shipping Information System

GISTMOP : groupe Interministériel de sûreté du transport maritime et des opérations portuaires

HFD : haut fonctionnaire de défense

IGA : inspection générale de l'administration

Installation portuaire : cela désigne un emplacement tel que défini par le Représentant de l'État dans le Département où a lieu l'interface navire/port (terminal)

Installation : installation portuaire ou Port

IF : inspection filtrage

IG : instruction générale

IP : installation portuaire

ISO : international standards organisation

ISPS : nternational Ship and Port Security

ISSC : (*International Ship Security Certificate*) certificat de sûreté d'un navire, à valeur internationale et délivré par un État partie à la convention SOLAS ou une société de classification reconnue par l'État

MEDDE : Ministère de l'Écologie, du Développement durable et de l'Énergie

MSC: Maritime Safety Committee

OIV : opérateur d'importance vital

OSH : organisme de sûreté habilité, tel que défini dans le code ISPS sous le vocable « organisme de sûreté reconnu »

OMI: organisation maritime internationale

PIV : point d'importance vital

PIF: postes d'inspection filtrage

plan POLMAR : plan pollution maritime

Port : abri naturel ou artificiel pour les bâtiments de navigation, muni des installations portuaires nécessaires à l'embarquement et au débarquement des marchandises et des passagers

PPP : plan particulier de protection

PREMAR : préfecture maritime

Procédure : manière spécifiée de réaliser une action, une activité

PSIP : plan de sûreté de l'installation portuaire

PSMP : peloton de sûreté maritime et portuaire

PSP : plan de sûreté du port

RE : règlement européen

RoPax : chargement mixte roulier passager

RoRo : chargement roulier

SDSIE : service de défense, de sécurité et d'intelligence économique

SIDPC : service interministériel de défense et de protection civile

SIRACEDPC : service interministériel régional des affaires civiles et économiques de défense et de la protection civile

SDIS: service départemental d'incendie et de secours

SSAS : (*Ship Security Alert System*) système d'alerte de sûreté du navire

Système d'alerte de sûreté du navire : Cela désigne un système installé sur tous les navires (selon la Règle 6 du Chapitre XI-2 de la Convention SOLAS), leur permettant d'envoyer -via satellite- une alerte discrète en cas de problème majeur de sûreté, type détournement, prise d'otage, attaque du navire ou autre au point de contact de l'État du pavillon.

UHF: ultra hautes fréquences

VHF:very high frequency

ZAR : zone d'accès restreint

ZNLA : zone non librement accessible

ZPS : zone portuaire de sûreté au sens de l'article L. 5332-1 du code des transports : elle est délimitée par l'autorité administrative et comprend le port dans ses limites administratives et les zones terrestres contiguës intéressant la sûreté des opérations portuaires.

b - Sigles et abréviations internationaux

AIS : Automatic Identification System

CSO : Company Security Officer

DoS : Declaration of Security

IMDG : International Maritime Dangerous Goods

IMO : International Maritime Organisation

ISPS : International Ship and Port Facility Security (Code)

PF : Port Facility

PFSA : Port Facility Security Assessment

PFSO : Port Facility Security Officer

PFSP : Port Facility Security Plan

PSA : Port Security Assessment

PSO : Port Security Officer

PSP : Port Security Plan

RSO : Registered Security Office

SOLAS : Safety Of Life At Sea

SSA : Ship Security Assessment

SSAS : Ship Security Alert System

SSO : Security Ship Officer

SSP : Ship Security Plan

UHF : Ultra High Frequency

VHF : Very High Frequency

VTS : Vessel Traffic Services

Liste des textes réglementaires

Textes internationaux :

Convention SOLAS (Safety Of Life At Sea) de 1974 modifiée en 2002 afin d'inclure les nouvelles dispositions du chapitre XI-2 annexé relatif aux mesures spéciales pour renforcer la sûreté maritime

Code ISPS (International Ships and Port facilities Security Code) relatif à la sûreté des navires et des installations portuaires de l'OMI

Textes européens :

Règlement (CE) N° 725/2004 du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires

Directive européenne 2005/65/CE du 26 octobre 2005, relative à l'amélioration de la sûreté portuaire des ports

Textes généraux français :

Décret n° 2004-290 du 26 mars 2004 portant publication des amendements à l'annexe à la Convention Internationale de 1974 pour la sauvegarde de la vie humaine en mer, ensemble un code international pour la sûreté des navires et des installations portuaires (Code ISPS), adoptés à Londres le 12 décembre 2002 (1)

Décret n° 2014-1670 du 30 décembre 2014 relatif aux dispositions du livre III de la cinquième partie réglementaire du code des transports et à leur adaptation à l'outre-mer (Décrets en Conseil d'Etat et décrets simples)

Décret n° 2007-937 du 15 mai 2007 relatif à la sûreté des navires

Circulaire 922 du 19 décembre 2003 relative au renforcement de la sûreté des installations portuaires

Textes français relatifs aux évaluations et aux plans de sûreté :

Arrêté du 22 avril 2008 définissant les modalités d'établissement des évaluations et des plans de sûreté portuaires et des installations portuaires

Circulaire du 18 novembre 2008 méthodologie de l'évaluation de sûreté

Textes français relatifs aux zones d'accès restreint :

Arrêté du 20 mai 2008 fixant la liste des équipements et systèmes intéressant la sûreté portuaire et maritime mis en œuvre dans les zones d'accès restreint, tels que définis par l'article R. 5332-44 du code des transports

Arrêté du 4 juin 2008 relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation

Arrêté du 18 juin 2008 relatif à la délivrance d'un agrément nécessaire pour l'exercice de missions de sûreté ou d'une habilitation nécessaire pour l'accès permanent à une zone d'accès restreint

Arrêté du 15 avril 2009 portant création d'un traitement de données à caractère personnel relatif à la délivrance d'habilitations, d'agréments et au suivi de la validité des titres de circulation des personnes

exerçant une activité dans les zones d'accès restreint des ports maritimes dénommé « CEZAR (Contrôle d'entrée en zone d'accès restreint) »

Arrêté du 1^{er} avril 2015 modifiant l'arrêté du 4 juin 2008 relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation

Textes français relatifs aux formations :

Arrêté du 17 juin 2004 relatif à la délivrance de l'attestation de formation d'agent de sûreté de l'installation portuaire (formation de 32 heures)

Arrêté du 23 septembre 2009 relatif à la formation des agents chargés des visites de sûreté (ACVS)

Arrêté du 12 mai 2011 relatif aux agréments des prestataires délivrant une formation professionnelle maritime

Autres textes français :

Arrêté du 27 octobre 2006 fixant la liste des ports maritimes relevant des collectivités territoriales et de leurs groupements où l'autorité investie du pouvoir de police portuaire est le représentant de l'État

Arrêté du 10 avril 2007 fixant la liste des ports mentionnée à l'article R. 5332-18 du code des transports

Arrêté du 26 juillet 2007 relatif à l'habilitation des organismes de sûreté

Arrêté du 3 mars 2008 complétant l'arrêté du 10 avril 2007 fixant la liste des ports mentionnée à l'article R. 5332-18 du code des transports

Arrêté du 2 juin 2008 fixant les conditions d'organisation des exercices et entraînements de sûreté dans les ports et les installations portuaires