



Service de l'énergie opérationnelle

Référentiel automatisme



Version
RA 07/2024

SOMMAIRE

I. Préambule.....	4
II. Généralités	4
1. Présentation des automatismes et des fonctions prises en compte	4
2. Utilisateurs des automatismes et les droits d'interactions	7
a) Utilisateurs nationaux	7
b) Utilisateurs locaux.....	7
3. Définition des principes de fonctionnement de l'automatisme.....	10
a) Capacités induites en dépôt au regard de ces états de fonctionnement	10
III. Spécifications techniques et fonctionnelles	11
1. Exigences fonctionnelles.....	11
a) Exigences fonctionnelles d'exploitation	11
b) Exigences fonctionnelles de sécurité	12
2. Exigences techniques	12
a) Automate	12
b) Ilots d'entrées / sorties déportés.....	12
c) IHM/SCADA	12
d) Lecteur NFC.....	13
e) Bibliothèque des briques IHM/SCADA et automate.....	14
f) Équipements informatiques.....	14
g) Matériels cyberactifs et hébergement.....	15
h) Éléments de sécurité.....	16
IV. Mode maintenance	18
V. Continuité de service.....	18
1. Description générale et périmètre.....	18
2. Déclenchement du mode continuité de service et modalités de reprise.....	18
a) Déclenchement du mode continuité de service	Erreur ! Signet non défini.
3. Exigences fonctionnelles et techniques pour la continuité de service.	19
VI. Réseaux et systèmes informatiques.....	20
1. Cadre de cohérence technique	Erreur ! Signet non défini.
2. Connexions internes automatismes	20
3. Architecture type.....	21
4. Parc à risque cybersécurité.....	21
5. Interconnexions entre le SEO et TRAPIL	22
6. Gestion du mécanisme de mot de passe manuel ou par carte « SCALP » :	23

7. Sauvegardes et restauration	23
8. Accessibilité et authentification.....	23
9. Traçabilité.....	24
VII. Réception des ouvrages, formation des utilisateurs et garantie	26
1. Réception des ouvrages	26
2. Homologation par déploiement.....	Erreur ! Signet non défini.
3. Notice de fonctionnement et formation.....	27
a) Notice de fonctionnement et d'entretien	27
b) Formation	27
4. Phase de garantie	27
Annexes	28
A. Documents de référence et textes réglementaires	28
B. Matrice de sécurité type	29
C. Actions à réaliser par le prestataire pour répondre au certificat d'usage de conformité (CUC).....	31
D. Règles relatives aux mots de passe et à l'authentification.....	33
E. Protocole de sauvegarde et de restauration (fourni en juillet 2024)	34
F. Fiche de non-conformité.....	35

I. Préambule

Le présent document est un référentiel technique qui définit les prescriptions générales et techniques relatives à la conception, l'installation et l'équipement des automatismes métiers au sein des installations pétrolières spécialisées (IPS) du service de l'énergie opérationnelle (SEO).

Il s'applique strictement aux automatismes métier du SEO sur les parties matérielles et logicielles. Il est adossé aux marchés d'infrastructure pour la partie des installations pétrolières spécialisées.

Ce document fait partie d'un corpus documentaire appartenant au SEO, et contribue à atteindre et à maintenir une cible d'harmonisation des automatismes métiers au sein des IPS.

Ce document est systématiquement utilisé lors de la passation des marchés infrastructure relatifs à la rénovation des systèmes automatismes du SEO ou plus largement lors de la rénovation des dépôts.

Tout écart avec ce référentiel doit être identifié dans l'annexe F (fiche de non-conformité) et doit être soumis à validation du chef du bureau infrastructure du centre de soutien technique et administratif (CSTA).

Tout écart jugé majeur au référentiel devra être validé par l'exploitant des installations.

II. Généralités

1. Présentation des automatismes et des fonctions prises en compte

Le service de l'énergie opérationnelle est responsable de *l'approvisionnement*, du *stockage* et de la *distribution* des produits pétroliers au sein des forces armées. Pour ce faire, les SEO dispose de dépôts pétroliers en France métropolitaine, en outre-mer et à l'étranger.

Ces dépôts sont considérés comme des sites industriels pétroliers pouvant être définis de la manière suivante:

- **le dépôt** : site industriel fonctionnant en autonomie et comprenant un ou plusieurs parcs.
- **le parc** : site clôturé contenant des IPS dont le fonctionnement n'est pas autonome.

Au sein d'un même dépôt, les installations prendront la dénomination suivante :

- parc principal ;
- parc secondaire.

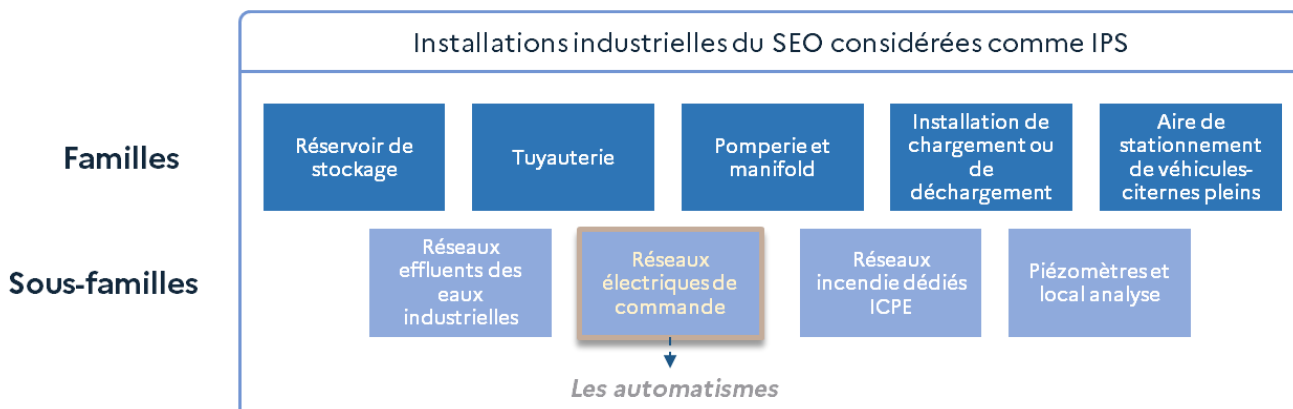
Les parcs secondaires pourront varier de 1 à 4 et seront ainsi dénommés en ajoutant le nombre à leur dénomination.

Pour chaque installation industrielle du SEO, l'infrastructure est scindée en deux parties distinctes :

- les installations pétrolières spécialisées (IPS) sous la responsabilité¹ du SEO ;
- les installations non pétrolières (INP) sous la responsabilité¹ d'un service interne au ministère des armées (MinArm).

¹ Pour la construction et la maintenance.

Les IPS sont implantées sur tous les parcs du SEO et sont regroupées au sein de 5 familles pétrolières et 4 sous-familles transverses :



Les automatismes métier du SEO se positionnent dans la sous-famille des réseaux électriques de commande.

L'automatisme métier du SEO se compose des organes suivants :

- automates,
- interfaces homme /machine (IHM) et systèmes de contrôle et d'acquisition de données (SCADA),
- actionneurs, capteurs et réseaux associés ...).

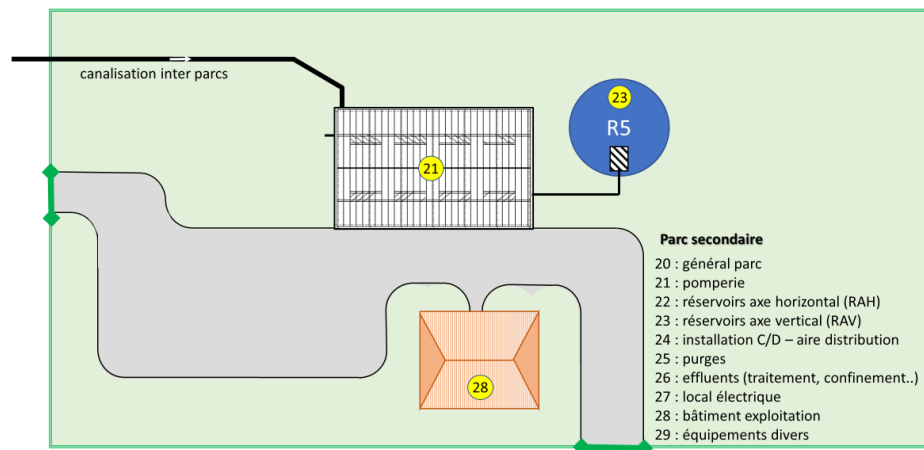
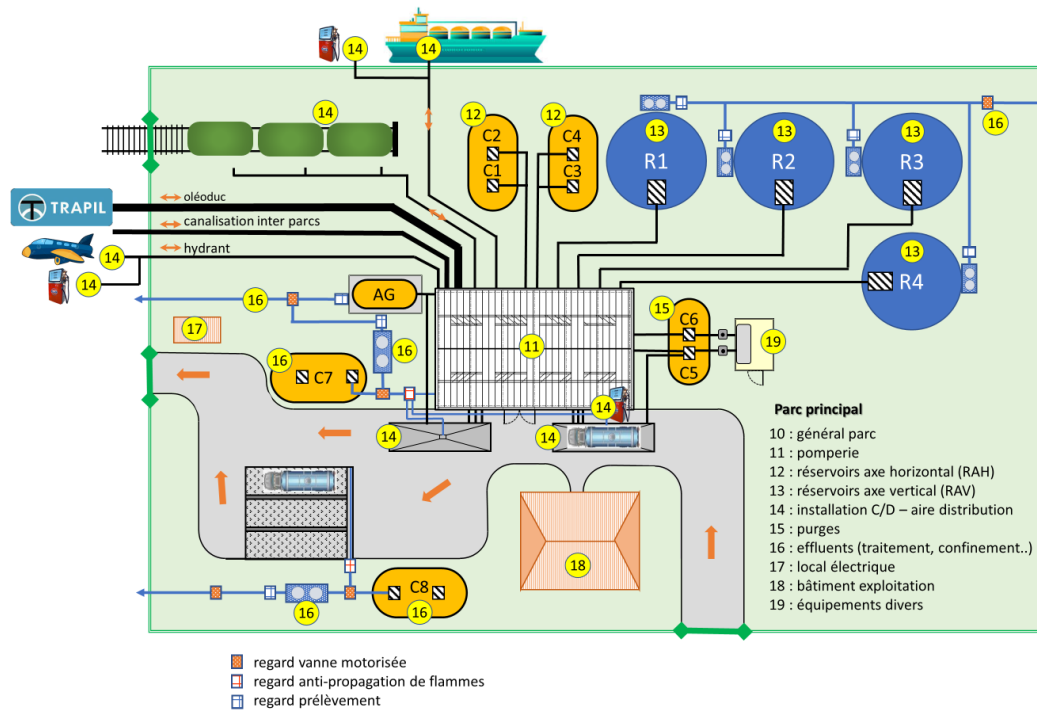
Initialement, le SEO a équipé ses dépôts d'automatismes métier en vue d'assurer les fonctions de sécurité liées aux installations classées pour la protection de l'environnement (ICPE). Depuis, ces automatismes métier couvrent de plus en plus des fonctions d'exploitation.

Le SEO a fait le choix d'automatiser certaines opérations à l'aide de systèmes informatiques et d'automatismes tout en répondant aux exigences fonctionnelles et de sécurité des dépôts.

Ces automatismes permettent entre autres :

- de concourir à la sécurité industrielle des opérations d'exploitation pétrolière ;
- d'améliorer l'efficacité opérationnelle ;
- de limiter les erreurs humaines ;
- d'harmoniser les règles métier.

Le schéma ci-dessous permet, par l'intermédiaire d'un dépôt exhaustif (dépôt théorique réunissant l'ensemble des fonctionnalités de tous les dépôts du SEO), de décrire les équipements automatismes **interconnectés en filaire uniquement** :



2. Utilisateurs des automatismes et les droits d'interactions

Les utilisateurs des automatismes sont répartis en deux familles :

- les utilisateurs nationaux qui disposent de prérogatives globales sur tous les sites du SEO ;
- les utilisateurs locaux qui disposent des prérogatives sur un site industriel unique du SEO. Ce site unique peut disposer de plusieurs parcs.

a) Utilisateurs nationaux

Principalement attachés au centre de maintenance des automatismes (CMA) de Nancy, ils se répartissent en trois niveaux particuliers :

- **Automaticien** : accès utilisateur au bastion, qui lui ouvre les droits suivants :
 - administration fonctionnelle sur les logiciels automatismes (ECE et EMSE) des sites ;
 - droits utilisateur sur la partie système d'exploitation des ordinateurs ;
 - droits suffisants pour effectuer des restaurations (firmware automate, configuration ECE/EMSE) via les sauvegardes logicielles prévues.
- **Administrateurs système** : accès utilisateur au bastion, qui lui ouvre les droits suivants :
 - droits administrateur sur les serveurs (hors bastion et partition de logs) et éléments actifs de réseau (EAR, pare-feu), système d'exploitation ;
 - droits d'administration système (OS, couche applicative socle type antivirus) sur les PC.
- **Administrateur de sécurité** :
 - droits d'administration du bastion et des partitions contenant les logs ;
 - droits utilisateur des autres postes ;
 - création des utilisateurs et attribution des droits accordés (utilisateurs locaux - niveaux 5 et 6, cf. ci-dessous - et utilisateurs nationaux).

Pour ces trois niveaux nationaux, des mots de passe de 14 caractères dont au moins une majuscule, une minuscule, un caractère non alphanumérique sont nécessaires.

b) Utilisateurs locaux

La déclinaison des différents rôles sur le personnel du dépôt est :

- fonctionnelle (le personnel montant la permanence est à plus forte raison du niveau cadre) ;
- ajustable au besoin par le chef de dépôt en particulier pour l'exploitant terrain.

Ils se répartissent en 7 rôles permettant de définir différents droits d'interaction avec les automatismes en fonction d'un niveau de responsabilité ou d'un niveau de rôle.

Les rôles sont présentés ci-dessous :

Niveau de rôle	Dénomination	Description
rôle 0 (R0)	visiteur (sans accès nominatif)	Interaction des alarmes et vue du plan de masse de l'emprise concernée avec affichage dynamique des mouvements de produit et certaines fonctionnalités.
rôle 1 (R1)	client (nominatif - identification matériel logistique)	Droits du rôle 0 et interactions avec les bornes d'avitaillement.
rôle 2 (R2)	exploitant terrain (nominatif)	Droits du rôle 1 et interactions avec l'automate au travers de l'IHM pour l'exploitation du dépôt (ordres + validation si <100m³) + utilisation des stations de distribution.
Hors présence exploitant, sur une plage horaire définie par le chef de dépôt, les ordres de mouvement pour le chargement des vecteurs, l'utilisation de l'hydrant et des stations de distribution sont autorisés à hauteur de 100 m³ sans validation.		
rôle 3 (R3)	exploitant bureau (nominatif)	Droits du rôle 2 et interactions avec l'automate au travers de l'IHM pour l'exploitation du dépôt (ordre et demande de validation si >100m³).
rôle 4 (R4)	maintenancier infrastructure (nominatif)	Droit du rôle 3 interactions avec l'automate au travers de l'IHM pour dérivation des automates et paramétrage des capteurs et actionneurs.
rôle 5 (R5)	cadre de permanence de dépôt (nominatif)	Droits du rôle 4 et utilisation des fonctions actives de l'automate au travers de l'IHM + droits de modification paramètres automatismes + validation de tous mouvements >100m³
rôle 6 (R6) *	chef de dépôt et adjoint(s) (nominatif)	Seulement pour gestion des utilisateurs et des droits. Rôle à destination du chef de dépôt et de 1 à 3 adjoints.

* Selon les possibilités liées au développement de la solution en cours. Le rôle pourra être dédié à la seule gestion des comptes.

	R0 : Visiteur	R1 : Client	R2 : Exploitant terrain	R3 : Exploitant bureau	R4 : Mainteneur infrastructure	R5 : Cadre de permanence de dépôt	R6 : Chef de dépôt et adjoint(s)
Identifiant (trigramme)	Non	Non	Oui				
Mot de passe	Non	NFC + Code à 4 chiffres	NFC + Code à 4 chiffres ou 8 Alphanum + 1 non alphanum				
Ecran de veille							
Vue générale schéma du parc principal	X	X	X	X	X	X	X
Vue générale schéma du/des parcs secondaires	X	X	X	X	X	X	X
Approvisionnement							
déchargement camion-citerne			O + V	O + V	O + V	O + V	O + V
déchargement wagon-réservoir				O	O	O + V	O + V
déchargement navire pétrolier				O	O	O + V	O + V
réception oléoduc				O	O	O + V	O + V
réception par fût pour additif			O + V	O + V	O + V	O + V	O + V
Stockage							
fabrication produit				O	O	O + V	O + V
transfert réservoir				O	O	O + V	O + V
vidange réservoir				O	O	O + V	O + V
Reprise / Remise - Bateau /Avion				O	O	O + V	O + V
Distribution							
chargement camion-citerne *			O + V	O + V	O + V	O + V	O + V
chargement wagon-réservoir				O	O	O + V	O + V
chargement navire pétrolier				O	O	O + V	O + V
distribution via hydrant système *			O + V	O + V	O + V	O + V	O + V
reprise via hydrant système *			O + V	O + V	O + V	O + V	O + V
station distribution (terre, air, mer) 24/7 *		O + V	O + V	O + V	O + V	O + V	O + V
Générale							
Présence/Absence exploitant				O + V	O + V	O + V	O + V
Acquiescement Alarme:							
Homme mort (deux niveaux d'alarme)			A	A	A	A	A
liaison équipotentielle			A	A	A	A	A
alarmes sonore et visuelle technique (jaune)				A	A	A	A
alarmes sonore et visuelle environnement (bleu)				A	A	A	A
alarmes sonore et visuelle incendie (rouge)				A	A	A	A
Mode continuité de service						O	O
Mode maintenance					O + V	O + V	O + V
Gestion mot de passe							O
Eclairage			O	O	O	O	O
Maintenance							
Capteur:							
Shunt					O + V	O + V	O + V
Réglage					O + V	O + V	O + V
Matériel:							
Hors service					O + V	O + V	O + V
Maintenance					O + V	O + V	O + V
Automate:							
Sauvegarde					protocole	protocole	protocole
Restauration					protocole	protocole	protocole
local automate					accès	accès	accès
Pc de programmation					accès	accès	accès
Baie Cybersécurité							
Maintenance					accès	accès	accès
Sauvegarde log					protocole	protocole	protocole
Ordre	O						
Validation	V						
Acquiescement	A						
* = opérations autorisées en absence exploitant							

3. Définition des principes de fonctionnement de l'automatisme

Pour l'exploitation d'un site industriel équipé d'automatisme, 3 modes de marche existent. Ces 3 modes apportent une certaine flexibilité au dépôt face aux différentes circonstances.

	Mode nominal	Mode maintenance *	Mode continuité de service **
État de l'automatisme	Standard	Maintenance (partiellement défaillant ou non)	Hors service
Principe de fonctionnement	Ce mode de fonctionnement normal du dépôt s'appuie sur l'ensemble des fonctionnalités offertes par l'automatisme pour les fonctions de sécurité et d'exploitation.	Ce mode de fonctionnement permet de piloter spécifiquement une partie de l'automatisme (d'un capteur / actionneur jusqu'au groupe fonctionnel*).	Ce mode de fonctionnement hors automatisme permet de garantir la disponibilité des fonctions minimales (exploitation pétrolière + sécurité ICPE) et essentielles du dépôt pour assurer <i>a minima</i> la distribution du produit.
Modalité de bascule	-	Depuis l'IHM	Depuis un commutateur 2 positions dans l'armoire automate
Niveau de responsabilité associé	Tous les rôles	R4, R5 & R6	R5 & R6
Conséquence pour l'exploitation	-	Commande actionneur par actionneur ²	Commande actionneur par actionneur

* le paragraphe V est dédié au mode maintenance.

** le paragraphe IV est dédié au mode de continuité de service.

1: Un groupe fonctionnel se compose d'actionneurs physiquement présents dans un même circuit et concourants à la même finalité métier, interdépendants les uns des autres. La définition des groupes fonctionnels fait partie de l'analyse fonctionnelle initiale du dépôt et doit tenir compte des spécificités du dépôt et de l'installation pétrolière.

2: En cas de partage d'un élément actif, pouvant éventuellement faire l'objet d'une défaillance, d'un shunt ou d'un mode continuité d'activité (actionneur – exemple une vanne motorisée), entre au moins deux groupes fonctionnels, un scénario alternatif est admissible. L'élément actif en question peut être exclu des groupes fonctionnels pour limiter cette dépendance et devra déclencher une alarme nécessitant acquittement par le cadre du dépôt toutes les 24 heures.

Le choix de ce scénario doit être explicitement mentionné et justifié, en tenant compte de sa criticité, dans le cadre de l'analyse fonctionnelle initiale du dépôt. Certains scénarios spécifiques peuvent faire l'objet d'un traitement particulier pour permettre de ne pas neutraliser l'ensemble de l'installation ou du circuit (ex. : installation C/D).

a) Capacités induites en dépôt au regard de ces états de fonctionnement

En conséquence, les dépôts seront dotés :

Au niveau des IHM (en numérique)	Au niveau des armoires automates (en physique)
- un tableau d'indicateur du mode de marche en cours sur les différents groupes fonctionnels ; - une capacité de bascule en mode maintenance et nominal ; - une capacité de dérivation (shunt) des capteurs de niveau bas (NB).	- une capacité de bascule en mode continuité de service par commutateur en façade d'une armoire automate du local automate ; - une capacité de dérivation (shunt) des capteurs de niveau très haut (NTH) par commutateur en façade d'une armoire automate du local automate *.

*Il existe un commutateur par réservoir.

² Certains cas d'usage peuvent être dérogatoires au sein d'un dépôt et doivent être décrit dans l'analyse fonctionnelle du dépôt concerné (utilisation modulaire des installations C/D, etc.).

III. Spécifications techniques et fonctionnelles

1. Exigences fonctionnelles

L'exploitation des dépôts consiste en trois tâches distinctes que sont :

- l'approvisionnement,
- le stockage,
- la distribution.

Chacune de ces missions possède des fonctions d'exploitation propres qui peuvent être plus ou moins automatisées. Les fonctions de sécurité industrielle sont listées en annexe B (matrice de sécurité). Cette liste est évolutive et sera mise à jour dès qu'une nouvelle fonction aura été automatisée.

a) Exigences fonctionnelles d'exploitation

Ce tableau permet d'identifier toutes les fonctions d'exploitation aujourd'hui automatisées pour le SEO. Concernant les IPS, chaque marché d'infrastructure fera l'objet d'une analyse fonctionnelle dès le début du projet qui détaillera le niveau d'automatisation attendue en cible en rapport avec les fonctions ci-dessous :

Fonction	Sous-fonction	Effet à obtenir
Ouverture de l'exploitation	• présence/absence exploitant	Maîtrise de l'exploitation du site
Mouvement de produit	• déchargement, • transfert, • fabrication, • chargement.	Gestion des volumes mouvementés Gestion des débits Gestion des stocks Gestion des ouvertures de réseaux Gestion des pompes
Niveaux de réservoirs		Gestion des stocks

La « présence exploitant » autorise les mouvements bilatéraux de produits pétroliers (des infrastructures et vers les infrastructures du dépôt.) L'« absence exploitant » les interdit formellement à l'exception :

- du chargement de camion-citerne ;
- de l'utilisation de l'hydrant ;
- de l'utilisation des stations de distribution.

Toutes ces opérations, autorisées lors de l'absence exploitant, sont strictement limitées au maximum à 100 m³.

b) Exigences fonctionnelles de sécurité

Les fonctions de sécurité liées aux dépôts sont les suivantes (cf. annexe B : matrice de sécurité):

Fonction	Effet à obtenir
Mise à la terre	Ouverture des réseaux
Protection travailleur isolé et prévention débordement citerne (dispositif homme-mort)	Arrêt des pompes et activation des alarmes sonores et visuelles
Dispositif d'alarme lié au déclenchement de la détection d'hydrocarbure (SDH) dans les DSOA hors réservoirs	Ouverture des vannes de dérivation Confinement Activation des alarmes sonores et visuelles Fermeture du réseau d'effluents
Barrière mixte	Coupage de l'approvisionnement
Détection de niveau très haut (NTH)	Coupage de l'électricité de l'exploitation Activation des alarmes sonores et visuelles
Détection de niveau haut (NH)	Activation des alarmes sonores et visuelles Arrêt de la pompe de remplissage et fermeture de la vanne motorisée du circuit utilisé.
Détection de niveau d'exploitation maximal (NEM)	Coupage de l'électricité de l'exploitation Activation des alarmes sonores et visuelles
Détection de niveau bas (NB)	Arrêt des pompes et activation des alarmes sonores et visuelles
Détection d'hydrocarbure (SDH) dans les encuvements	Coupage des pompes de relevage activation des alarmes sonores et visuelles
Dispositif d'alarme lié au déclenchement de la détection d'hydrocarbure (SDH) en point bas de la pomperie	Coupage de l'exploitation
Détection humaine en zone critique	Bascule des organes d'exploitation en mode manuel

2. Exigences techniques

a) Automate

Le matériel de référence est l'automate type M580 (ou équivalent) de référence BMEP582010 ou supérieur selon le besoin. Si nécessaire, en cas de besoin, des variantes pourront être proposées à la validation du SEO. Les automates déployés doivent respecter les exigences fonctionnelles de la pile logicielle disponible dans la version DR du référentiel automatisme papier.

b) Ilots d'entrées / sorties déportés

Le logiciel de référence est « ADVANTYS » pour configurer les ilots d'Entrées / Sorties déportées de la famille « STB » gérés par l'automate M580 ou équivalent. Ces ilots seront installés hors zone ATEX.

c) IHM/SCADA

Le logiciel de référence est Ecostruxure Machine SCADA Expert ainsi qu'une configuration IHM/IPC Harmony P6 de référence :

- HMIP63A10N15AN3N00 (écran 22"W) ou équivalent pour installation en bureau exploitation uniquement ;
- Coffret ACIER - H600XL800XP300 - porte pleine, Enveloppe : acier, couleur poudre époxy-polyester - gris (RAL 7035) (Spacial S3D, référence Schneider-Electric : NSYS3D6830P) ;
- HMIP63G10N15AN3N00 (écran 19"W) ou équivalent pour le reste ;
- Coffret ACIER - H600XL600XP200 - porte pleine, Enveloppe : acier, couleur poudre époxy-polyester - gris (RAL 7035).

Un coffrage sera mis en place dans une finalité de sécurité (blocage des ports de communication). La connexion fibre optique – RJ45 s'effectuera avec un boîtier de type TP_Link MC100CM ou équivalent et inséré dans le coffrage de l'IHM.

En complément, pour les IHM installées en zone ATEX (positionnement final déterminé lors de l'analyse

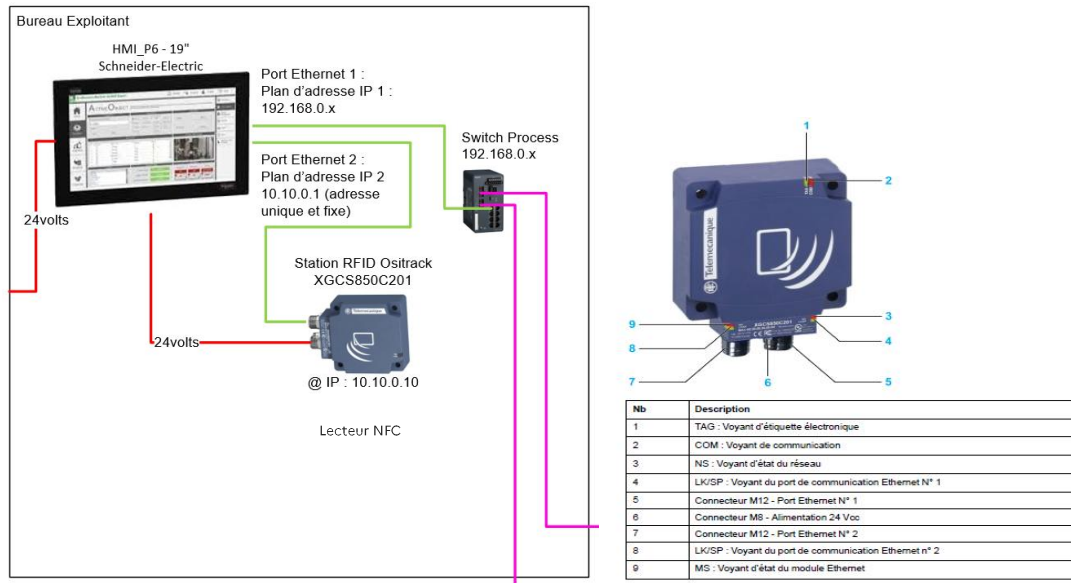
fonctionnelle du dépôt), le coffrage utilisé doit répondre à la norme ATEX (CE xxxx  II 3 G EEX/EX xx IIA T3) Catégorie 3 (Zone ATEX 2/22).

Ce coffrage devra prévoir 6 passages de câbles normés ATEX.

De plus, le lecteur NFC (pour authentification utilisateurs) associé sera également installé dans un autre boîtier répondant à la même exigence ATEX et raccordé à l'IHM.

d) Lecteur NFC

Un lecteur NFC de type station RFID sera utilisé. Ce lecteur NFC est raccordé à l'HMI-P6 (avec ou sans sur coffrage en fonction du positionnement final déterminé lors de l'analyse fonctionnelle du dépôt.



L'identification du personnel sur l'application est réalisée à l'aide d'une carte SCALP (carte d'accès au logiciel du SEO) par protocole « MIFARE ». Pour ce faire, l'opérateur doit présenter son badge devant un lecteur type «NFC». L'identification du personnel est automatique et entraîne une demande de saisie de son mot de passe à 4 chiffres.

Le matériel de référence est :

- OsiSense XG - station RFID - 13,56Mhz - 2 ports de communication Ethernet de référence XGCS850C201;
- OsiSense XZ - connecteur Alimentation pré-câblé - droit femelle - M8 - 4 broches - 2m de référence XZCP0941L2 ;
- Câble Ethernet, connexion en cuivre, 1 connecteur IP67 - M12 (4 broches) et 1 connecteur RJ45, longueur 1m de référence TCSECL1M3M1S2.

En complément, pour les lecteurs NFC installés en zone ATEX (positionnement final déterminé lors de l'analyse fonctionnelle du dépôt), le coffrage utilisé doit répondre à la norme ATEX zone 2 « CE xxxx  II 3 G EEX/EX xx IIA T3 ».

³Les fournisseurs aujourd'hui connus pour ces boîtiers ATEX sont Pepperl-fuchs (référence : GUBW1) et TEKMA .

³ (Plus de précision seront apportées fin juillet)

e) Bibliothèque des briques IHM/SCADA et automate.

Ces briques fonctionnelles sont regroupées dans une bibliothèque « procédé SEO » livrée en annexe informatique. Elles devront être utilisées pour exécuter les programmes mis en œuvre au sein des sites industriels du SEO.

En cas de besoin d'évolution ou d'ajout, il sera obligatoire de faire une demande auprès du bureau des services numériques du CSTA.

Les briques fonctionnelles IHM/SCADA consisteront en une standardisation de la représentation des organes d'exploitation, de l'affichage des alarmes, de la navigation dans l'application et de la conduite (pop-up de paramétrage standard, pages standards pour les transferts, les purges, etc.).

Les briques fonctionnelles doivent respecter les normes de programmation suivantes :

- **Nom du DFB** : Les noms des DFB doivent être descriptifs et refléter la fonction principale de la DFB. Le cas échéant, la convention de nommage prescrite par le SEO doit être utilisée.
- **Commentaires** : Chaque DFB doit inclure des commentaires clairs et concis expliquant la fonction, les entrées, les sorties, et tout autre aspect important.
- **Structure modulaire** : Le DFB doit pouvoir être divisé en modules logiques, chacun responsable d'une fonction spécifique.
- **Gestion des erreurs** : Des mécanismes de gestion des erreurs appropriés doivent être intégrés, comme des messages d'erreur ou des retours de valeurs spécifiques.
- **Tests automatisés** : Des tests automatisés pour vérifier le bon fonctionnement du DFB doivent être intégrés. Il sera nécessaire d'utiliser des assertions ou des bibliothèques de test pour garantir la qualité au sein de la plateforme d'intégration.

f) Équipements informatiques baie cyber

Le PC de programmation prévu (PC complet) devra disposer *a minima* des caractéristiques suivantes :

- compatibilité avec Windows 10 et Windows 11 ;
- 32 Go de RAM ;
- 500 Go de stockage ;
- processeur Intel i3 (10e génération) ou AMD Ryzen 3 (série 3000) ;
- disposer d'une garantie de fonctionnement pendant 5 ans ;
- écran 27" (seul équipement présent hors de la baie cyber).

UCSCADA (UC) devra disposer *a minima* des caractéristiques suivantes :

- compatibilité avec Windows 10 et Windows 11 ;
- 16 Go de RAM ;
- 500 Go de stockage ;
- processeur Intel i3 (10e génération) ou AMD Ryzen 3 (série 3000) ;
- disposer d'une garantie de fonctionnement pendant 5 ans.

g) Matériels cyberactifs et hébergement

L'hébergement des équipements de connexion au réseau est réalisé dans le local automate du parc principal. En cas d'impossibilité technique d'hébergement dans le local automate, une étude sera diligentée pour envisager une solution alternative respectant à minima l'exigence de contrôle d'accessibilité.

La liste des équipements cyberactifs et leurs caractéristiques est définie ci-dessous :

Baie pour le parc principal		Baie pour les parcs secondaires à risque	
Équipement	Modèle ou équivalent	Équipement	Modèle ou équivalent
Baie informatique	18/22/24 U	Baie informatique	6/4 U
Système de ventilation rackable	KIMEX 110-0205	Système de ventilation rackable	KIMEX 110-0205
Bandeau rackable PDU	L8 RM	Bandeau rackable PDU	L8 RM
Pare-feu rackable Stormshield	SN720	Système de ventilation rackable	KIMEX 110-0205
Serveur de LOGS	Combinaison ELK	Pare-feu rackable Stormshield	SN220
Commutateur de desserte	CISCOC9200L		
Onduleur	GROWATT 1015		
Tiroir à documentation rackable	Thon Rack Drawer 2U		

Les matériels Stormshield seront équipés du pack de sécurité « basique ».

Les routeurs Cisco disposent également du pack inclus dans le perpetual licencing.

h) Éléments de sécurité

Alarmes sonores et visuelles	
Les alarmes visuelles et sonores seront installées sur un mât à hauteur du local électrique et à une altitude suffisante pour être visible et entendues de la zone pétrolière et des bureaux.	
Gyrophare 1 - environnement	Couleur bleue
	Alarmes environnement, détecteurs de fuite et d'hydrocarbures
	Mise en marche à l'apparition d'un défaut et à l'apparition d'un autre défaut après acquittement du premier, etc.,
	S'arrête à l'acquittement du défaut (défaut toujours signalé sur synoptique), et à l'acquittement d'un autre défaut, etc....
Gyrophare 2 – technique	Couleur jaune
	Alarmes exploitation, détecteurs de niveaux, homme mort
	Mise en marche à l'apparition d'un défaut et à l'apparition d'un autre défaut après acquittement du premier, etc.
	S'arrête à l'acquittement du défaut (défaut toujours signalé sur synoptique), et à l'acquittement d'un autre défaut, etc.
Gyrophare 3 - incendie	Couleur rouge
	Alarme incendie
	Mise en marche sur action d'un boîtier d'alarme incendie (déclencheur manuel)
Sirène	Un son différent par type d'alarme de +/- 120 dB
	S'arrête à l'acquittement du défaut (défaut toujours signalé sur synoptique), et à l'acquittement d'un autre défaut, etc....
	Mise en marche à l'apparition d'un défaut et à l'apparition d'un autre défaut après acquittement du premier, etc.,

Transfert d'alarme		
Le SEO a choisi un transmetteur industriel de type ETIC TELECOM E220 ou équivalent *.		
Ce boîtier sera relié à l'automate principal selon une liaison Ethernet assurera le report des alarmes vers le téléphone portable de permanence et report vers les pompiers (pour les alarmes incendie)		
Chaîne de sécurité	1	Transmission d'au maximum 7 SMS répartis sur 55 minutes à destination du cadre de permanence fournissant la nature de l'alarme (ex. : « détection HC dans séparateur »).
		Si pas d'acquittement <i>in situ</i> réalisé après 60 minutes
	2	Transmission d'au maximum 3 SMS « alarme dépôt XXX » à destination de l'officier d'astreinte CLEO/CSTA.

* les configurations du transmetteur devront répondre aux exigences suivantes :

- pas de contrôle distant RAS ;
- pas de communication ADSL, VDSL, XDSL;
- pas de WIFI ni de BLUETOOTH ;
- a minima 4 entrées ANA/NUM ou I/O ;
- a minima 1 sortie I/O sur relais ;
- a minima 1 redondance d'alimentation (par batterie ou pile).

Arrêts d'urgence	
Les arrêts d'urgence exploitation (AUE), arrêt incendie (AI) et arrêts pompiers (AP) seront placés conformément au plan de masse donné dans le CCTP et leur emploi déclenchera les actions décrites ci-après.	
AUE	Alarme sonore et visuelle. Le volume sonore devra être de 120 dB. En cas de nécessité, une seconde alarme pourra être installée.
	Un buzzer doit être installé dans les bureaux
	Coupage de l'alimentation électrique de la zone exploitation (l'automate, les portails électriques, les locaux, les vannes motorisées du réseau EP et l'éclairage demeurant alimentés)
	Fermeture des vannes à sécurité positive HC
	Fermeture des vannes motorisé du réseau EP: vannes d'isolement et regards de dérivation
	Report téléphone portable de permanence
AI	Alarme sonore et visuelle. Le volume sonore devra être, au minimum, de 120 dB
	Coupage de l'alimentation électrique de la zone concernée. L'automate, les portails électriques, le bâtiment administratif, les vannes motorisées du réseau EP et l'éclairage demeurant alimentés
	Fermeture des vannes à sécurité positive HC
	Fermeture des vannes à sécurité positive du réseau EP (regards de dérivation et vanne d'isolement)
	Report de l'information vers l'ESIS/SSIS et sur le téléphone portable de permanence
AP⁴	Coupage totale de l'alimentation électrique du dépôt
	Report téléphone portable de permanence

⁴ Hors automatisme.

IV. Mode maintenance

Ce mode de fonctionnement permet de piloter spécifiquement une partie de l'automatisme (d'un capteur / actionneur jusqu'au groupe fonctionnel) sous condition de sécurité et sous la responsabilité maintenancier/cadre du dépôt.

Dans certains cas dérogatoires de fonctionnement avec des défaillances au sein d'un groupe fonctionnel, le mode de maintenance peut être mis en œuvre et permettre :

- un shunt numérique des niveaux bas ;
- un shunt par commutateur du NTH.

Dans ces cas spécifiques, l'utilisation du mode de maintenance doit être soumise à validation du cadre du dépôt pour garantir une utilisation de l'installation dans les conditions de sécurité nécessaires.

V. Continuité de service

1. Description générale et périmètre

L'implémentation du mode de continuité de service prescrit dans ce présent référentiel doit permettre au commandement du site de basculer volontairement en mode continuité de service pour répondre à une défaillance de l'automatisme et permettre une résilience du dépôt.

Le passage dans ce mode assurera la dérivation électrique de l'automate par un commutateur positionné dans une armoire électrique du local automate et doit être issu d'une action anthropique à la suite d'une décision de commandement.

Cette continuité de service s'intègre dans le plan de continuité d'activité (PCA) du dépôt et doit assurer *a minima* la continuité de 3 fonctions de sécurité et d'exploitation :

- fonction de sécurité industrielle (ICPE) : maintien du fonctionnement des capteurs de niveau très haut, maintien en fonction des renvois d'alarmes sonores et visuelles ; maintien en fonction de tous les arrêts d'urgences (arrêt d'urgence exploitation et incendie) ;
- fonction d'exploitation de stockage : le maintien en fonctionnement du système d'additivation ;
- fonction d'exploitation de distribution : le maintien en fonctionnement du système de distribution hydrant ; le maintien en fonctionnement des pompes et des vannes.

Le mode de continuité de service ne prévoit pas de transfert d'alarmes.

2. Déclenchement du mode continuité de service et modalités de reprise

Le passage en mode continuité de service doit pouvoir être utilisé volontairement après décision du commandement du dépôt et aussi longtemps que nécessaire par exemple lors d'un défaut majeur de l'automatisme du site (HS). Toutefois, les causes de la mise en œuvre du mode de continuité de service doivent rapidement être diagnostiquées et corrigées afin de remettre en service le fonctionnement normal du site (voir annexe B – matrice de sécurité).

Le déclenchement de ce mode doit être assuré suite à un ordre de commandement par un commutateur 2 positions situé dans le local automate du site. Lors de la panne majeure d'un automate et/ou d'une IHM, un protocole d'échange IHM-automate doit permettre de confirmer à l'utilisateur la nécessité de passage en mode continuité de service. Elles doivent décrire le plan d'actions à mener pour assurer le service du site en sécurité.

Le protocole de déclenchement du mode continuité de service sera défini localement par chaque chef de dépôt avec une mise en œuvre lors d'exercice annuel.

3. Exigences fonctionnelles et techniques pour la continuité de service.

Les tâches qui permettent de couvrir la continuité de service sont décrites ci-dessous et doivent être mises en œuvre.

Selon l'existant, les orientations techniques peuvent évoluer :

Fonction	Effet final recherché	Orientation technique
Bascule en mode continuité de service	Le circuit électrique dérive l'automate pour l'exploitation du dépôt	Mise en place d'un commutateur dans le local automate.
Arrêt et démarrage des pompes	Maintien en fonctionnement des pompes	Mise en place d'un boîtier de commande à chaque pompe
		Si déjà présent, l'utilisation d'un pupitre de commande centralisé est admise
Ouverture et fermeture des vannes	Maintien en fonctionnement des vannes	Mise en place d'un volant de manœuvre manuel à chaque vanne
		Selon faisabilité, mise en place d'une vanne avec servomoteur
Sécurité ICPE	Maintien du fonctionnement des capteurs de NTH de chacune de capacités de stockage du site	La gestion des sécurités (NTH, AUE, AI) ne doit pas être assurée par des automates de sécurité. Les sécurités doivent être câblées sur relai électrique dans la chaîne de sécurité de l'installation.
	Maintien en fonction d'une alarme sonore (ton discontinue) et visuelle (rouge)	
	Maintien en fonction de tous les arrêts d'urgences (AUE, AI)	
Actionneurs d'additivat⁵	Maintien en fonctionnement du système d'additivat	En cours d'étude
Réseau hydrant	Maintien en fonctionnement du système de distribution hydrant	A définir

En cas de déclenchement d'un capteur/actionneur câblé (NTH + AUE + AI) alors une alarme sonore (ton discontinue) et visuelle (rouge) sera activée en logique câblée.

⁵ Solution à fournir par S4

VI. Réseaux et systèmes informatiques

La pile logicielle utilisée doit être conforme à la pile logicielle présente dans le dossier d'homologation (DR). Toute évolution de version ou changement de produit doit être soumis à validation du RSSI qui s'assurera :

- de la conformité de la proposition au cadre de cohérence technique (CCT) du ministère (document mis à jour par la DGNUM) dans sa dernière version validée ;
- d'obtenir une dérogation si nécessaire à ce CCT par le sous-comité cohérence des architectures (SC²A).

De même la solution antivirus doit être conforme à la directive DARMA de l'AND (agence numérique de la défense) et suivre ses évolutions, à savoir :

- pour les PC : Office Scan Apex One v14 ;
- pour le serveur : Deepsecurity v12.

Ces documents sont de mention « diffusion restreinte » et disponibles sur demande :

- sur l'Intradef pour les personnes disposant d'un accès ;
- par transmission sur une adresse courriel hors Intradef dans une archive ACID (le destinataire doit donc être possesseur d'une clé ACID).

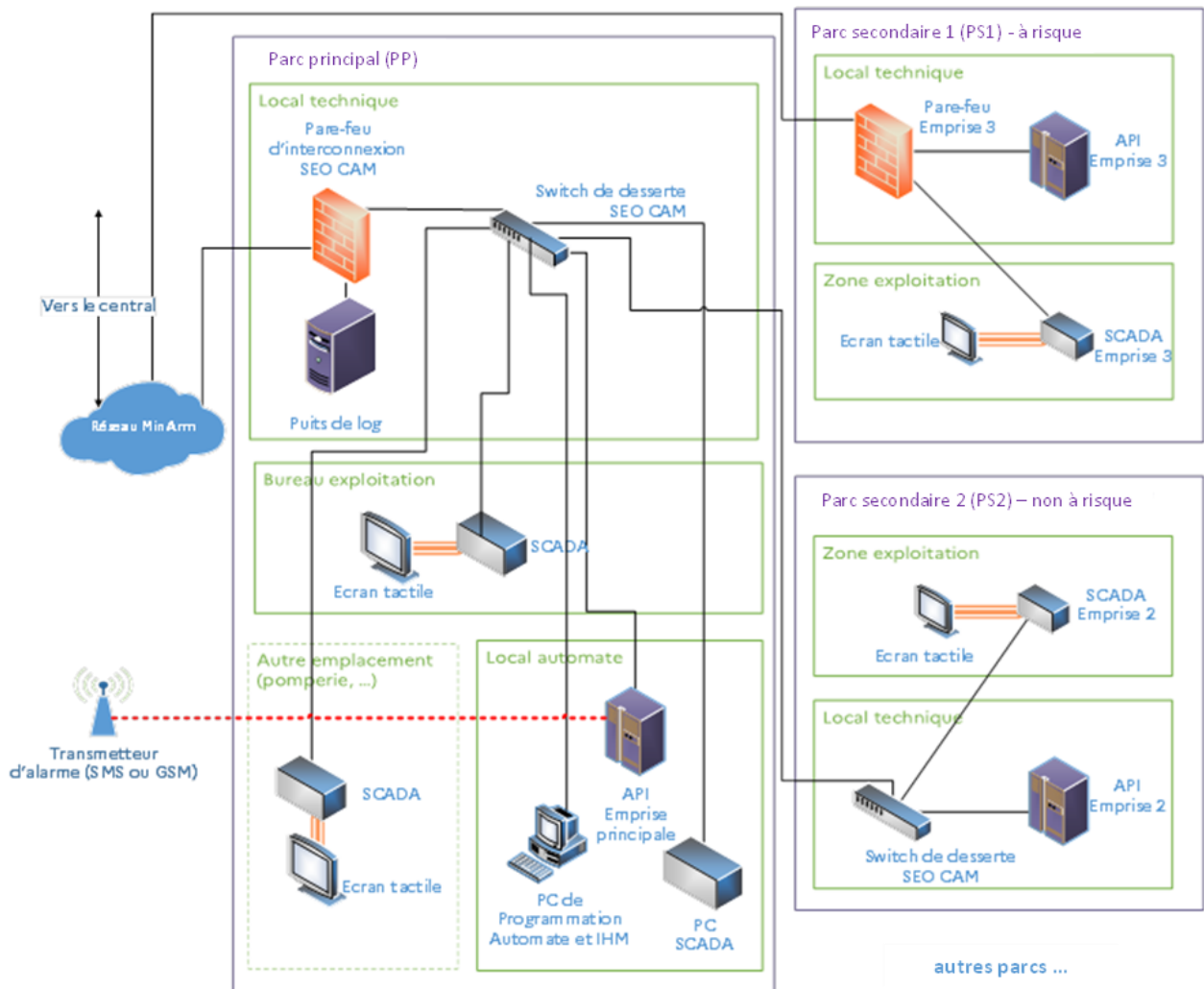
1. Connexions internes automatismes

La connexion filaire exclusive est obligatoire pour toutes les communications inter-automatismes.

Par ailleurs, tous les ports de communication des matériels installés doivent respecter les exigences suivantes :

Niveau de sécurité	Mesures techniques	Cas de figure
Ports verrouillés	• bloqueur de ports	Tous ports de communication inutilisés situés dans un local fermé à clé
Ports bloqués	• sur coffrage • bloqueur de ports	Tous ports de communication inutilisés situés dans un parc militaire hors local automate.
Ports inertés	• sur coffrage • bloqueur de ports • déconnexion interne du port	Tous ports de communication inutilisés situés hors emprises militaire.

2. Architecture type



3. Parc à risque cybersécurité

Un parc secondaire est considéré à risque cybersécurité si la liaison avec le commutateur du parc principal n'est pas une liaison directe en fibre optique (obligation de passer par des routeurs / relais / autres éléments actifs de réseau).

En conséquence, ce type de parc sera systématiquement équipé d'un pare-feu de type STORMSHIELD SN220 ou équivalent reliant le parc principal.

Pour les parcs considérés comme non à risque, il n'y a pas de baie cybersécurité à déployer, le commutateur administrable prévu sera placé dans la baie automate.

Toutes les connexions sont réalisées en fibre optique hors contre-indication du SEO jusqu'au commutateurs convertisseurs. Des alternatives seront systématiquement envisagées pour des distances inférieures à 60 m et mises en œuvre avec accord du SEO.

4. Interconnexions entre le SEO et TRAPIL

Certains dépôts du SEO sont connectés logistiquement à l'oléoduc de défense commune (ODC) opéré par la société externe TRAPIL.

Dans une démarche de cybersécurisation, les principes directeurs relatifs à l'interconnexion entre les automates SEO et TRAPIL doivent être appliqués selon les solutions d'interconnexion suivantes :

- solution cible : une interconnexion en logique câblée entre les automates ;
- solution alternative : pas d'interconnexion entre les automates SEO et TRAPIL.

Si la solution cible est appliquée alors les données échangées entre les automates SEO et TRAPIL doivent être à *minima* celles-ci-dessous :

Données écrites par l'automate TRAPIL dans l'automate SEO		Données lues par l'automate TRAPIL dans l'automate SEO	
Désignation	Typologie	Désignation	Typologie
Transfert en cours	Tout ou rien (TOR)	Arrêt d'urgence SEO	TOR
Arrêt d'urgence TRAPIL	TOR	Autorisation de livraison	TOR

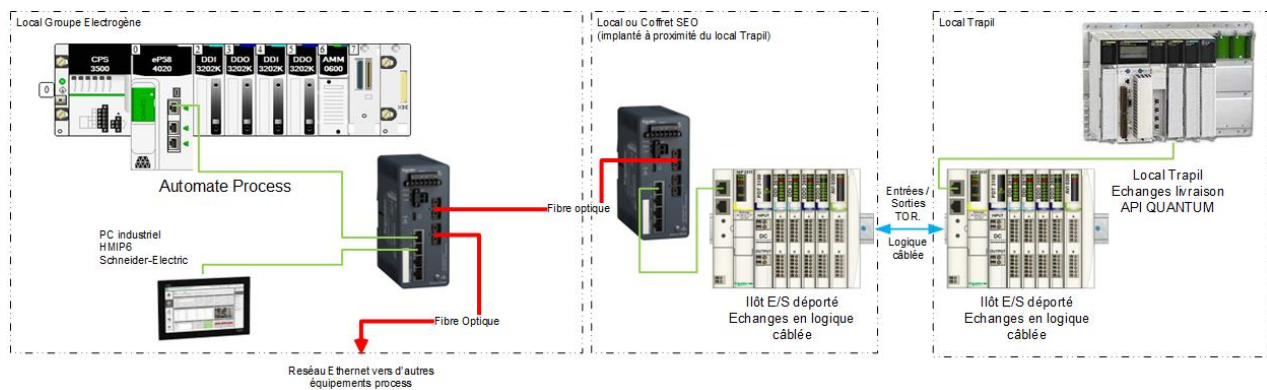
En cas de besoin d'échanges d'informations numériques entre les deux automates TRAPIL et SEO, la connexion en logique câblée est obligatoire, mais nécessite des ajustements en particulier dans la proximité.

Pour ce faire, un ilot d'Entrées/Sorties déporté sera positionné au plus près de l'automate TRAPIL.

Le raccordement entre cet ilot et l'automate TRAPIL s'effectuera en logique câblée. Le raccordement entre l'ilot STB et l'automate métier du SEO s'effectuera au travers d'un commutateur (administrable) « Cuivre / Fibre Optique » à la fibre optique « process pétrolier » du site.

L'ilot déporté sera installé dans un local annexe fermé du SEO accolé au local TRAPIL.

Schéma de principe pour le raccordement des automates du SEO et TRAPIL :



5. Gestion du mécanisme de mot de passe des utilisateurs :

5.1 utilisateurs nationaux⁶

5.2 utilisateurs locaux soit en manuel soit par carte SCALP

Le mécanisme de gestion des mots de passe locaux est défini ci-dessous. L'annexe D appuie ce principe.

- création par le chef de dépôt, d'une liste d'intervenants avec chacun :
 - UID de la carte SCALP utilisée ;
 - mot de passe temporaire (4 chiffres) associé à l'UID ;
 - rôle ;
 - trigramme d'identification ;
 - mot de passe temporaire (9 caractères dont 8 alphanumériques et 1 non alphanumérique) associé au trigramme ;
 - nom ;
 - type de débit (exclusivement pour les clients = R1).
- l'utilisateur modifie ses mots de passe, lors de la première connexion sur un des postes de supervision (connexion manuelle ou par badge).

6. Sauvegardes et restauration

Un protocole de sauvegarde et de restauration est proposé en annexe E. Les éléments sauvegardés devront être stockés à plusieurs endroits :

- sur un disque dur externe ;
- sur le serveur de sauvegarde à Nancy ;
- en local sur le PC console de programmation.

Les éléments à sauvegarder sont à fournir suite à la réception des installations et des travaux et sont les suivants (liste non exhaustive) :

- les programmes automate et IHM ;
- les logiciels de programmation automate et IHM ;
- les configurations des équipements réseau ;
- les configurations des serveurs et des postes de travail (peut être facilité si ces équipements sont déployés à partir d'un Master).

Une procédure de sauvegarde et de restauration sera livrée par le titulaire en fin de marché.

7. Accessibilité et authentification

Pour chaque élément pouvant disposer d'authentification, différents comptes sont créés et ont des privilèges différents, selon les principes de *besoin d'en connaître* et de *moindre privilège*. Les différents comptes envisagés sont indiqués ci-dessous.

Comptes des postes de travail :

- Compte administrateur (pour les administrateurs système) ;
- Compte utilisateur individuel.

⁶ Paragraphe à écrire par S7

Comptes de la supervision (IHM SCADA) :

- Conformes au §2.b, rôles R1 à R6.
- La gestion des comptes est faite par les comptes de niveau R6.

Comptes sur éléments actifs de réseau (pare-feu, routeur) :

- Compte d'administrateur national.

Le mot de passe de protection des automates est activé et paramétré.

Le code par défaut de la carte SIM du report d'alarme est modifié ainsi que tous les mots de passe par défaut présents (équipements ou logiciels).

« Les droits d'accès aux ressources doivent être gérés suivant les principes du besoin d'en connaître et du moindre privilège. Ces droits d'accès doivent être attribués à travers des profils d'accès et s'appuyer sur des processus formalisés. Les processus d'affectation, de révision et de suppression des droits d'accès applicables aux utilisateurs et administrateurs sont décrits dans la documentation du système. » [PSSI-M-T]

De plus, des contraintes sur la configuration de l'authentification sont mises en place, de manière proportionnelle à la criticité des accès. Les règles détaillées sont disponibles en annexe D.

En plus des différents comptes créés, des règles sur la gestion de ces droits sont mises en place. Ces règles doivent être respectées dès que le matériel le permet.

8. Traçabilité

L'architecture de la solution propose un élément permettant de conserver des journaux (serveur puits de logs). Différentes directives et bonnes pratiques permettent de définir les éléments et événements devant être enregistrés.

Les logs doivent indiquer :

- l'identité de l'émetteur de la requête ;
- l'horodatage de la tentative ;
- le résultat de la tentative ;
- le nombre de connexions ;
- les commandes passées.

De plus, la conservation des journaux doit être d'un an minimum. Les événements devant être enregistrés et conservés sont les suivants :

Événements à logger	Logiciels industriels	Postes Windows	Équipements réseau
Echec d'authentification compte à privilège	X	X	X
Réussite authentification compte à privilège	X	X	X
Echec connexion distante	X	X	X
Réussite connexion distante	X	X	X
Echec d'authentification compte classique	X	X	X
Réussite d'authentification compte classique	X	X	X
Mises à jour des programmes liés à la programmation des automates	X		
Mises à jour des programmes liés à la programmation des IHM	X		
Modifications apportées à la configuration des équipements réseau			X
Mises à jour antivirus		X	X
Détection antivirus		X	X
Echec mise à jour antivirus		X	X
Calcul d'empreinte non valide	X	X	X
Requête traitée par le pare-feu local		X	
Connexions de médias amovibles	X	X	X
Déconnexions de médias amovibles	X	X	X
Connexion d'éléments sur le réseau			X
Déconnexion d'éléments sur le réseau			X
Réussite application mise à jour système		X	X
Echec application mise à jour système		X	X
Echec téléchargement mise à jour système		X	X

VII. Réception des ouvrages, formation des utilisateurs et garantie

1. Réception des ouvrages

La réception des ouvrages se fera en 3 temps décrits ci-dessous :

1. Temps 1 : le titulaire du marché :

À l'issue de tous les travaux, l'industriel indiquera les modalités pratiques de réalisation des essais au maître d'œuvre et fournira une liste complète des épreuves et essais à exécuter ainsi qu'un planning d'essai (en lien avec l'analyse fonctionnelle du site). Chaque épreuve ou essai fera l'objet d'une procédure de mise en œuvre. Par ailleurs, à la fin du chantier, l'industriel s'assurera de remettre à niveau, en local, tous les blocs fonctionnels utilisés pour le dépôt au regard de la dernière version du standard.

Ces documents devront être transmis au maître d'œuvre au moins dix jours ouvrables avant les essais de réception.

2. Temps 2 : le maître d'œuvre :

- valide les épreuves, essais et contrôles des installations ;
- est responsable de la coordination des épreuves, essais et contrôles ;
- décide d'éventuels essais complémentaires.

3. Temps 3 : le chef d'établissement :

Le chef d'établissement est responsable de la sécurité incendie et du respect des dispositions réglementaires en matière d'hygiène et sécurité du travail ainsi que de la protection de l'environnement.

Les essais minimaux à réaliser sont listés ci-dessous :

Essais	Localisation	Compétence	Précisions
Validation des procédés (programmation locale des automates et IHM) sur la plateforme d'intégration du CMA	Au CSTA	Automatisme	
Suivi du protocole d'essai automatisme proposé par le titulaire et validé par le SEO	Sur site	Automatisme	
Vérification des sauvegardes applicatives	Sur site et au CSTA	Automatisme	3 niveaux de sauvegarde : • au CMA ; • sur un média amovible local ; • sur la console de programmation locale.
Création du stockage en local des logs cyber	Sur site	Informatique	Vérifier que chaque équipement pouvant créer des logs le fait, les envoie, et ce pour tous les événements à logger (cf. référentiel)
Vérification de l'adressage réseau local	Sur site	Informatique	Vérifier que chaque équipement a la bonne adresse IP
Vérification de la connexion vers Nancy	Sur site et au CSTA	Informatique	
Vérification de la configuration du pare-feu	Sur site	Informatique	Grille DIR39 et matrice de flux
Vérification des configurations / durcissement des postes Windows	Sur site	Informatique	Grille DIR39
Vérification des comptes Windows et SCADA/IHM	Sur site	Informatique	Accès, comptes avec et sans privilèges
Vérification des comptes équipements réseau	Sur site	Informatique	Accès, comptes avec et sans privilèges
Vérification antivirus	Sur site	Informatique	Test EICAR
Vérification envoi et réception des logs en central	Sur site et au CSTA	Informatique	
Vérification réception mise à jour	Sur site	Informatique	

2. Notice de fonctionnement et formation

a) Notice de fonctionnement et d'entretien

Au plus tard à la demande de réception, exprimée par le titulaire, les documents suivants seront remis au maître d'œuvre et au chef du dépôt :

- les notices de fonctionnement et d'entretien ;
- les procédures de mise en œuvre ;
- le planning de maintenance de tous les matériels installés.

b) Formation

Deux formations, portant sur la mise en œuvre et l'entretien des installations livrées, seront assurées au profit du personnel de l'établissement avec :

Participants (rôles)	Objet de la Formation	Contenu	Durée
R2, R3, R4, R5 et R6	Droits et fonctionnalités associées au rôle 2	○ Présentation IHM ○ Ordre chargement /déchargement ○ Usage des lumières	1/2 journée
R3, R4, R5 et R6	Droits et fonctionnalités associées au rôle 3	○ Toutes les fonctionnalités du R3	1/2 journée
R4, R5 et R6	Droits et fonctionnalités associées au rôle 4	○ Toutes les fonctionnalités du R4	1/2 journée
R5 et R6	Droits et fonctionnalités associées au rôle 5	○ Toutes les fonctionnalités du R5 sur IHM ○ Sauvegarde et restauration système	1/4 journée
R6	Droits et fonctionnalités associées au rôle 6	○ Modalité de création/suppression de compte ○ Gestion des droits des comptes (affectation des rôles) ○ Passage en mode continuité de service	1/4 journée

Tous les supports de formation seront fournis à la réception des travaux.

3. Phase de garantie

La garantie, d'une durée légale (2 ans) n'est employée qu'à la suite d'un dysfonctionnement.

Elle comprend toutes les actions nécessaires aux résolutions des problèmes tant d'un point de vue matériel que d'un point de vue programmation/logiciel.

Pour la mise en œuvre de cette garantie, les actions nécessaires à la résolution du problème peuvent être menées soit localement soit à distance par l'usage du centre de maintenance automatisme (CMA) présent au sein du CSTA à la caserne Thiry de Nancy. Quel que soit le mode d'intervention nécessaire, un accord officiel du SEO devra être obtenu.

Annexes

A. Documents de référence et textes réglementaires

Les documents de référence et textes réglementaires complémentaires à ce document sont :

- la directive 39 relative à la sécurité des systèmes industriels ;
- la cadre de cohérence technique des systèmes d'information et de communication du ministère des armées ;
- la directive 27 portant sur l'homologation des systèmes d'information du ministère des Armées ;
- la directive 29 portant sur les traces et leur gestion au sein du ministère de la Défense ;
- le guide relatif aux mesures de maître des risques instrumentées (MMRI) ;
- toutes les directives ATEX ;
- les normes françaises et européennes d'électricité ;
- l'analyse fonctionnelle exhaustive du dépôt du SEO

B. Matrice de sécurité type

Désignation du capteur	Action déclenchée via automate	Affichage sur la supervision	Enregistrement des données	Environnement gyrophare bleu	Technique gyrophare jaune	Incendie gyrophare rouge	Alarme sonore incendie	Autre alarme sonore	Report téléphone
NB jaugeur	Arrêt de la pompe de soutirage	X	X		X			X	
NEM jaugeur	Alarme	X	X		X			X	
Delta H jaugeur	Alarme	X	X		X			X	X
NH jaugeur	Arrêt de la pompe de remplissage et fermeture de la vanne motorisée du circuit utilisé	X	X		X			X	
NTH	AUE	X	X		X			X	X
NH espace annulaire	Mise en route pompe de relevage correspondante	X	X						
NB puisard périphérique	Arrêt de la pompe de relevage correspondante	X	X						
Détecteur HC puisard périphérique	Arrêt de la pompe de relevage correspondante	X	X	X				X	X
Détecteur HC point bas pomperie	Asservissement à un AUE	X	X	X				X	X
Sonde détectrice HC DSOA	Fermeture vanne d'isolement réseau EP et vanne de dérivation confinement	X	X	X				X	X
Sonde détectrice (eau +HC DSOA) réservoir	Fermeture vanne d'isolement réseau EP et vanne de dérivation confinement et si nécessaire arrêt de la pompe de relevage	X	X	X				X	X
Détecteur fuite double enveloppe		X	X	X				X	X
Détecteur de présence de liquide confinement		X	X	X				X	X

Désignation du capteur	Action déclenchée via automate	Affichage sur la supervision	Enregistrement des données	Environnement gyrophare bleu	Technique gyrophare jaune	Incendie gyrophare rouge	Alarme sonore incendie	Autre alarme sonore	Report téléphone
Détecteur débit nul pompe	Arrêt de la pompe correspondante	X	X						
Capteur de fin de course vanne	Autorisation mise en route pompe sur réseau correspondant	X	X						
Connexion liaison équipotentielle	Autorisation de chargement/déchargement	X	X						
Homme mort	Arrêt de la pompe	X	X						
Présence exploitant automate	Activation des commandes d'exploitation	X	X						
Absence exploitant	Désactivation des commandes d'exploitation et fermeture des vannes motorisées HC	X	X						
AUE	Coupage de l'alimentation électrique de la zone d'exploitation pétrolière (tous moyens exceptés l'éclairage, le portail d'accès et le local automate)	X	X		X			X	X
AI	Coupage de l'alimentation électrique de la zone concernée	X	X			X	X		X
AP ⁷	Coupage générale électricité					X			X

⁷ hors automatisme

C. Actions à réaliser par le prestataire pour répondre au certificat d'usage de conformité (CUC)

- Tester la connexion inter-emprise ;
- Configurer le BIOS de chaque poste de travail du système industriel de telle sorte que ce dernier n'autorise pas d'autre démarrage depuis un disque dur interne local ;
- S'assurer que tous les postes de travail et les serveurs informatiques du dépôt se verrouillent automatiquement après un maximum de 10 mn d'inactivité. Le déverrouillage nécessite alors une nouvelle authentification de l'utilisateur ;
- S'assurer que toutes les stations de travail et tous les serveurs disposent d'un antivirus validé par le Ministère des Armées, fonctionnel et à jour, avec un processus de mise à jour fonctionnel.
- S'assurer que seuls les services utiles au fonctionnement, à la qualité, à la sécurité et à la supervision des automatismes hébergés sont activés ;
- S'assurer que les traces des actions de gestion et d'administration et MCO/MCS sont protégées en intégrité, soit par un stockage sur un système informatique séparé dont les comptes à privilèges sont détenus par un administrateur de sécurité, soit par un enregistrement dans un "coffre-fort numérique" ;
- S'assurer que sur les intranets, un réseau dédié à l'administration et MCO/MCS des équipements ou au moins un réseau logiquement séparé de celui des utilisateurs doit être utilisé pour les actions d'administration et MCO/MCS
- S'assurer que les traces de ces actions de gestion et d'administration et MCO/MCS des SI industriels du SEO sont stockées pour une durée minimale de 12 mois ;
- S'assurer que les mises à jour et modifications apportées à l'automatisme sont tracées ;
- S'assurer qu'un processus de journalisation et sauvegarde des configurations de l'automatisme est mis en œuvre ;
- S'assurer que les couches logicielles de l'automatisme sont sauvegardées (pour restauration) ;
- S'assurer que les sauvegardes de données et configurations sont testées avant la mise en service opérationnelle (test de restauration) ;
- S'assurer que les mots de passe par défaut des équipements sont modifiables et changés avant la mise en service opérationnelle ;
- S'assurer que le changement du mot de passe initial est imposé par le système à la première connexion ;
- S'assurer que le mot de passe utilisateur est composé au minimum de 9 caractères pour les utilisateurs (14 pour les administrateurs), hors code PIN carte opérateur ;
- S'assurer que le mot de passe inclut au moins trois des catégories : lettre majuscule, lettre minuscule, chiffre, caractère spécial (sous réserve que le SI le permette), hors code PIN carte opérateur ;
- S'assurer que le mot de passe ne contient pas l'identifiant, le nom de l'utilisateur, sa fonction, son grade ;
- S'assurer que le mot de passe est différent des 6 derniers mots de passe utilisés.
- S'assurer que la durée de validité du mot de passe utilisateur est fixée de 7 jours minimum à 90 jours maximum, hors code PIN carte opérateur ;
- S'assurer que les comptes par défaut ou non utilisés sont supprimés ou à défaut désactivés ;
- S'assurer que tous les comptes non utilisés et/ou anonymes, ainsi que les comptes créés systématiquement par les systèmes du type "invité" doivent être systématiquement supprimés, à défaut désactivés ;
- S'assurer qu'aucun mot de passe n'est en clair sur le réseau ou affiché dans le bureau ou sur l'automatisme ;
- S'assurer que les mots de passe des administrateurs et des EAR sont protégés par un moyen agréé, ou à défaut, conservés dans le coffre de l'OSSI/CSSI de l'organisme, sous enveloppe cachetée ;
- S'assurer que les échecs d'authentification et les authentifications réussies des comptes à privilèges à l'automatisme sont enregistrés ;
- S'assurer que le personnel intervenant sur les systèmes industriels est formé à la SSI et doit le démontrer avant toute intervention ;
- S'assurer que la documentation du système local est fournie au SEO ;

- S'assurer que les comptes fonctionnels sont limités au strict nécessaire, ne possèdent pas de droits privilégiés et sont désactivés en dehors des périodes autorisées d'utilisation ;
- S'assurer que les protocoles sécurisés garantissant confidentialité, intégrité et authenticité des points communicants (https, sftp, etc.) sont obligatoirement privilégiés au détriment des protocoles non sécurisés de type ftp, tftp, http, telnet, etc ;
- S'assurer qu'une mise en œuvre de test + 1 mis en œuvre de formation de la continuité de service sera réalisée avant la mise en service opérationnelle ;
- S'assurer que l'automatisme est obligatoirement cloisonné physiquement ou à défaut logiquement en interne et externe ;
- S'assurer que qu'il n'y a pas de compilateurs, codes sources, binaires instrumentés ou de toute autre ressource spécifique au développement sur un automatisme en environnement de production ;
- S'assurer que les services non indispensables (service web par exemple) sont désactivés sur les équipements de l'automatisme ;
- S'assurer que les lecteurs optiques et les ports USB sont obligatoirement désactivés ou clairement identifiés lorsque leur ouverture est nécessaire ;
- S'assurer que les réseaux sur lesquels sont connectés les automatismes à des mécanismes physiques (type actionneurs, robots, etc.) sont cloisonnés de l'intradef ;
- S'assurer qu'aucun périphérique sans fil n'est utilisé sur l'automatisme ;
- S'assurer que lorsque des flux non-IP doivent transiter entre deux zones distinctes, un filtrage est réalisé sur les identifiants source et destination, ou sur les protocoles autorisés ;
- S'assurer qu'une vérification en intégrité et authenticité est obligatoirement effectuée au chargement des logiciels et programmes SCADA ;
- S'assurer que les composants logiciels et programmes commerciaux disposent d'une licence valide ;
- S'assurer que les équipements de type automate ont obligatoirement activé une liste blanche d'adresses IP et désactivé la programmation à distance ;
- S'assurer que les équipements de type automate possèdent obligatoirement une protection d'accès de type CPU active (mot de passe) ;
- Les programmes exécutables des équipements de type automate possèdent obligatoirement une protection d'accès (mots de passe)
- S'assurer que cartes opérateurs sont enrôlées dans le système et la procédure d'enrôlement est donnée ;
- S'assurer que chaque utilisateur possède un compte personnel pouvant être lié à une carte ;
- S'assurer que tous les services et fonctionnalités non nécessaire au report d'alarme sont désinstallés et/ou inhibés ;
- S'assurer que le report d'alarme est fonctionnel pour l'ensemble des alarmes prévues ;
- S'assurer que la configuration des EAR permet le passage des flux nécessaires à l'administration et à la maintenance depuis le CMA.

D. Règles relatives aux mots de passe et à l'authentification

Règle de gestion des mots de passe

En l'absence de mécanismes techniques permettant d'interdire les mots de passe faibles, des campagnes de recherche régulières de mots de passe faibles doivent être conduites sur les SI par l'opérateur. La découverte d'un mot de passe faible doit conduire au changement de mot de passe dans les 5 jours ou au verrouillage du compte.

Le nombre maximal de tentatives de saisie de mot de passe autorisées avant blocage du compte ne doit pas dépasser 10 tentatives.

A la création du compte, le gestionnaire associe un mot de passe initial aléatoire avec l'identifiant et sélectionne l'option « première connexion ». L'opérateur se connecte et ne peut faire autrement que de changer son mot de passe par celui qu'il désire.

Dans le cas où un opérateur oublie son mot de passe, le gestionnaire régénère un mot de passe temporaire et coche la case « première connexion ». L'opérateur se connecte et ne peut faire autrement que de changer son mot de passe par celui qu'il désire.

Les mots de passe utilisateur doivent faire a minima 9 caractères et contenir 3 des 4 types de caractères (minuscule, majuscule, chiffres, caractères spéciaux)

Les mots de passe administrateur doivent faire a minima 14 caractères et être complexes (au moins 3 des 4 types de caractères et avoir une forte entropie si le système permet de l'imposer).

L'authentification multi facteurs est autorisé avec l'emploi d'une carte à puce et d'un code PIN associé (code à 4 chiffres minimum).

E. Protocole de sauvegarde et de restauration (en cours de développement)

[illegible]

REFERENTIEL AUTOMATISME

Fiche de non-conformité par rapport au référentiel automatisme

Site industriel concerné			
Non-conformité identifié		Date de création	

Contexte

Indiquez ici le contexte dans lequel la non-conformité survient

--

Définition de la non-conformité

Précisez l'écart à la cible, ses différents aspects, la cause de cette non-conformité

--