Octobre 2022

LES CAHIERS DU LAB

VNF – Programme de Modernisation de l'Exploitation – Atelier du Lab Automates

STANDARD AUTOMATES

Version de travail non validée

VERSION	**0**
NIVEAU DE STANDARD **LEGENDE** Niveau 1 : Stratégique / Défini la cible technique Niveau 2 : Méthodique / Défini les chemins possibles **Niveau 3 : Opérationnel / Précise les solutions techniques** Niveau 4 : Marché nationaux et leur utilisation	**3**
OUVRAGES D'APPLICATION	

OUVRAGES DE NAVIGATION	EPG	X
	EGG	X
	PONT MOBILE	
	TUNNEL	
OUVRAGES DE GH	BARRAGES	
	PRISES D'EAU	
	REJETS	
	BARRAGES RESERVOIR	
POSTE DE COMMANDE CENTRALISEE	REARMEMENT EPG	X
	TELECONDUITE EGG	X
	GESTION HYDRAULIQUE	
	GESTION DU TRAFIC	
	CHEF DE SALLE	

Table des matières

Préambule **5**

I. Démarche de sécurité VNF **6**

I.A. Dangers & analyse de risque 6

I.B. Les 4 types d'arrêts d'une écluses automatisée et les niveaux SIL requis 7

I.C. Les événements redoutés 8

II. Définition des architectures **9**

II.A. Conception de l'installation sécurisée 9

II.B. Architecture d'automatisme standard Ecluse Petit Gabarit 10

II.C. Architecture d'automatisme standard Ecluse Grand Gabarit 12

III. Affectation dynamique des Arrêts d'urgence pour la téléconduite **13**

III.A. Principes d'affectation dynamique des AU pour la téléconduite 13

III.B. Rappel des définitions et standards couleurs 14

IV. Choix du matériel **16**

IV.A. Compatibilité Cybersécurité 16

IV.B. Automate de télégestion 17

IV.C. Contraintes OPC-UA 18

IV.D. Mise à la cible de l'existant - *migration M340 vers M580 Safety* 19

IV.E. Comparatif des solutions 20

V. Standards d'intégration EPG **22**

V.A. Principes de mise en œuvre 22

V.B. Armoire EPG type 23

VI. Méthodes de programmation des automates de sécurité **24**

VII.A. Langages normalisés 24

VII.B. Blocs fonctionnels 25

VII. Annexes **26**

VII.A. Méthodologie standard de projet VNF 26

VII.B. Analyse de risque EPG 27

VII.B.1. Rappels de méthode 27

VII.B.2. Remarques spécifiques à VNF 27

VII.C. Liste des événements redoutés (ER) VNF 29

VII.D. Découpage fonctionnel des EPG selon le modèle ISA S88 30

VII.E. Intégration de la Cybersécurité dans la méthode 31

VII.F. Cybersécurité Opérationnelle 32

VII.G. Définitions cybersécurité : ANSSI, BSI 33

VII.H. Définitions automates de sécurité 35

VII.I. Recommandation SIL - règles de conception et de codage 36

VII.K. Affectation dynamique des AU : diagrammes d'interactions 38

VII.K.1. Diagrammes d'interactions entre le PCC et le sas 40

VII.K.2. Diagrammes d'interactions entre le demi-pupitre et le sas 41

VII.K.3. Glossaire 42

VII.L. Atelier logiciel 43

VII.M. Structure des programmes 43

VII.N. Mnémonique standards E/S ..... **Erreur ! Signet non défini.**

Table des figures

Figure 1 - Schéma standard coupure d'urgence 7
Figure 2 - Fonctions assurées par un automate de sécurité 9
Figure 3 - Architecture d'automatisme standard EPG réarmée à distance, sans barrage – écluse type équipée de BCSF Mini 10
Figure 4 - Architecture d'automatisme standard EPG réarmée à distance, sans barrage – écluse « particulières - dangereuses» équipée de BCSF Complète 10
Figure 5 - Architecture d'automatisme standard EGG double sas avec barrage 12
Figure 6 - Exemple de découpage fonctionnel – non validé 25
Figure 7 - Principe de gestion de la sécurité 25
Figure 8 - Grille d'analyse de risque 27
Figure 9 - Echelle des niveaux SIL 27
Figure 10 - Tableau des ER VNF 29
Figure 11 - Fonctions assurées par un automate de sécurité 35
Figure 12 - Exemple d'installation possible 35
Figure 13 - Entrée de sécurité avec détection de coupure 36
Figure 14 - Sortie de sécurité 36
Figure 15 - Réservation Sas vs PCC 40
Figure 16 – Libération' Sas vs PCC 40
Figure 17 - Affectation Sas vs Poste de Conduite (1/2 – partie AU) 41
Figure 18 - Affectation Sas vs Poste de Conduite (2/2 - Partie Affichage) 41
Figure 19 - Désaffectation Sas vs Poste de Conduite (Affichage+AU) 42

Préambule

Une première vague de quatre ateliers du Lab ont été lancés en décembre 2021 : SCUO, Architecture PCC, Gestion Hydraulique (GH) et Audio & Vidéo.
Une seconde vague de trois ateliers du Lab techniques – sous sponsorat DSIN - a été lancée en juin 2022 : Cybersécurité, Réseaux et Automates

Ces groupes de co-construction fixent une ambition commune de cadrage national sur une thématique. Les principes donnés visent à homogénéiser le fonctionnement et l'utilisation sur tout le territoire et sont définis dans un standard. Ce document est à destination de tous les acteurs de VNF ainsi qu'aux maitres d'œuvres et intégrateurs, afin de le déployer.

Le présent document propose le **standard Automates** dans le cadre de la modernisation de l'exploitation et de la maintenance d'ici fin 2029.

Il couvre les éléments suivants :
- Définition d'un méthodologie standard pour les projets (analyse de risque, analyse fonctionnelle, etc.)
- Définition des architectures automatismes pour le Petit Gabarit
- Définition de l'architecture et du processus d'affectation dynamique des Arrêts d'urgence au PCC pour le Grand Gabarit
- Critère de choix du/des modèle(s) standard(s) national d'automate de sécurité
- Grands principes d'intégration des armoires EPG
- Préconisations concernant les méthodes de programmation des automates de sécurité (langages à utiliser, constitution de blocs fonctionnels, structure des programmes, atelier logiciel)

Il s'agit de définir une vision partagée par l'ensemble de l'établissement (directions territoriales et siège : DIEE, DSIN, DIMOA) et des standards qui permettront d'avoir des outils d'exploitation et de maintenance des ouvrages communs.

Il est à noter que le standard Automates rencontre des connexions et interdépendances avec les autres ateliers du Lab, et prend en compte les préconisations Cybersécurité de la PSSI.

Les participants de l'Atelier du Lab Automates ont été identifiés afin d'avoir une grande expertise sur les sujets et une représentativité de l'ensemble des activités de VNF (technicien, service maintenance-exploitation, informatique).

Représentant DT S et pilote du groupe : Jacques LITZENBURGER
Représentant DT SO et pilote du groupe : Jean-Paul GUERIN
Représentant DT NE : Philippe FLAMMERION
Représentant DT BS : Alain BERLIERE
Représentant DT RS : Sébastien CAMUSET
Représentant DT CB : Jean-Marie FEVRE
Représentant DT NPdC : Cédric FERMENTIN
Responsable technique : Pierre-Emmanuel FLIPPE
Contributeur technique : David MOREL
Contributeur DIMOA : Nathalie MILESI
Sponsor : Christophe LALOYER

Les principes définis et reportés dans ce document ont été retenus car ils constituent une réponse adaptée au champ de contraintes de la majorité des DT.

Ce premier standard automate défini les grands pourtours des automatismes. Il sera à compléter dans un second standard vers une armoire d'automatisme unique pour les écluses à petit gabarit afin de réaliser des gains d'investissement, temps de réalisation des projets, et de maintenabilité des systèmes.

I. Démarche de sécurité VNF

Pour la méthodologie des projets automatisme VNF, voir annexe VII.A. Méthodologie standard de projet VNF

I.A. Dangers & analyse de risque

Les écluses présentent un risque pour l'humain et le matériel, elles sont régies par la directive sur les infrastructures (2008/114/CE) et la norme EN61508 (Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité).
Le niveau de sécurité est mesuré par les niveaux SIL (Safety Integrity Level).

Une analyse de risque pour les écluses à petit gabarit automatisées standards existe, en cas de particularités il convient de compléter l'analyse de sécurité et les actions qui en découlent par un organisme habilité, type Apave, Socotec, etc.

Il est obligatoire de mettre à jour l'analyse de risque à chaque fois qu'on modifie une installation (y compris dans le cadre d'une amélioration, rénovation ou modernisation). L'analyse de risque est à la charge de VNF (qui peut se faire aider par un bureau d'étude spécialisé). La qualification peut se faire par VNF directement avec une méthodologie particulière ou par un bureau d'étude.

En termes de temporalité, l'analyse de risque doit être faite dès que la conception de l'installation est finalisée - avant sa mise en œuvre – pour pouvoir apporter des modifications ou des ajouts si nécessaire.

L'objectif n'est pas de mettre en œuvre des systèmes complexes et difficiles à maintenir/faire évoluer, mais des système simples nécessitant le moins possible de capteurs de sécurité et répondant à des actions de sécurité correctement identifiées, grâce à la connaissance des ouvrages du terrain.
/!\ La mise en œuvre de chaînes de sécurité complète (capteurs de sécurité, traitement de sécurité, contacteurs adaptés) est primordiale. Ce travail doit être réalisé dans les règles de l'art.
/!\ La mise en œuvre d'un automate de sécurité sans mettre en œuvre le reste de la chaîne de sécurité ne sert à rien excepté dépenser de l'argent inutilement.

Pour plus de contexte relatif à l'analyse de risque, voir annexe VII.B. Analyse de risque EPG

I.B. Les 4 types d'arrêts d'une écluses automatisée et les niveaux SIL requis

Les 4 types arrêts doivent être mis en place systématiquement sur les écluses à petit gabarit (EPG) automatisées. **L'arrêt d'urgence** doit être actif quel que soit le mode de fonctionnement et agit de façon contextuelle avec une mise en sécurité des installations en fonction de l'événement **puis** la coupure des énergies. La coupure arrête les mouvements de portes / d'eau puis coupe l'énergie des organes de manœuvre (= ne pilote plus les contacteurs de puissance des moteurs) quand l'écluse est en mode automatique. Il n'est pas réarmable à distance.

La **tirette d'alarme** ne doit fonctionner que pendant le cycle pour éviter que le déclenchement inopportun par des passants en dehors des cycles de bassinée. Elle est réarmable à distance.

La **coupure d'urgence** (CU) déclenche un arrêt immédiat de l'énergie. Il sert à mettre hors tension toute l'écluse (partie commande (PC) et partie opérative (PO)). La coupure ne fait que couper l'énergie mais ne réalise pas mouvements d'écluse (ni porte, ni vanne). Elle ne peut être déclenchée que par les agents de maintenance, en cas de danger physique immédiat d'un collègue. Elle n'est pas réarmable à distance.

La CU est à connecter sur une entrée de l'automate qui coupe l'armoire électrique sauf la TBTS, l'automate et le switch.

L'alimentation de l'automate et du switch doivent être secourue pour pallier les microcoupures : via chargeur 24vDC + batterie, mais pas d'utilisation d'onduleur 230vAC.

Un déplacement sur site sera nécessaire pour alimenter de nouveau l'écluse.

Dans le cas lors d'une coupure locale, si l'automate reste sous tension et si on perd l'alimentation des ilots déportés, un double « acquit » est nécessaire car les sorties de sécurité sont passivées.

Si tout est coupé (API + ilots déportés), un simple acquit suffit.

Dans le cas spécifique d'une EPG avec E/S déportées, des sorties de sécurité doivent permettre des coupures locales.

	Désignation	Type d'organe	Lieu d'implantation	Niveau sécurité requis	Catégorie selon NF EN 60204	Mode de fonctionnement	Actions de sécurité	Observations
Écluse automatisée	**Arrêt d'urgence (BP AU)**	Bouton coup de poing	Pupitre	SIL 2 / PLr = d	1	Mode automatique Mise hors tension des organes de manœuvre coupés par automate de sécu	Mise en sécurité puis mise hors tension de la partie opérative (PO)	Le coup de poing doit être de couleur ROUGE. La collerette du bouton coup de poing doit être de couleur JAUNE et porter la mention « Arrêt d'Urgence »
				SIL 2 / PLr = d	1	Mode manuel	Mise hors tension de la PO	
				SIL 2 / PLr = d	1	Mode maintenance	Mise hors tension de la PO	
	Tirette de sas (alarme)	Tirette rouge ou équivalent	Sas	SIL 2 / PLr = d	1	Mode automatique	Mise en sécurité puis mise hors tension de la PO	La tirette doit être de couleur rouge
				-	-	Mode manuel mode	Aucune action	
				-	-	Maintenance	Aucune action	
	Coupure d'urgence (CU)	Coup de poing	TGBT ou armoire d'automatisme	SIL 2 / PLr = d	0	Tous	Mise hors tension de la PO PO + PC – partie commande. Tout couper sauf TBTS	**Ne doit être utilisée que par les agents de maintenance** Le coup de poing doit être de couleur rouge et porter la mention « Coupure d'urgence »
SCUO v2	**Arrêt cycle**	Bouton poussoir du TPE	Bateau de l'usager	SIL 2	1	Mode automatique	Mise en sécurité puis mise hors tension de la PO	
				-	-	Mode manuel	Aucune action	
				-	-	Mode maintenance	Aucune action	

Figure 1 – détail des 4 arrêts obligatoires pour le Petit Gabarit

I.C. Les événements redoutés

Voir annexe VII.C. Liste des événements redoutés (ER) VNF pour plus de détails

Les ER sont plus compliqués à mettre en place. VNF souhaite déjà en priorité que les DT mettent en place correctement les arrêts de sécurité. Le traitement des événements redouté peut intervenir dans un second temps.

La prévention est privilégiée, en travaillant à limiter les causes de ces événement (via mise en place capteurs, contacteurs adéquats).

II. Définition des architectures

Le standard d'architecture doit être intégré dans les CCTP, pour prise en compte par le maitre d'œuvre, ainsi que pour éviter toute interprétation différente par les entreprises d'exécution.

II.A. Conception de l'installation sécurisée

L'automate de sécurité permet avant tout d'obtenir le niveau de disponibilité souhaité – voir en annexe *VII.H. Définitions automates de sécurité* pour plus de précisions sur le fonctionnement d'un automate de sécurité.

Dans le cadre d'une architecture sécurité, les réseaux doivent être séparés. On compte 3 niveaux :

- Niveau E/S déportées : Sensible car c'est la source d'informations de l'automate pour son fonctionnement, donc doit être impérativement sur un bus ou un réseau dédié qui reste confiné entre la CPU et les modules déportés (aucun échange externe), Profinet, Profinet IO, ASI, ...
- Niveau Automatisme : Si interactions entre 2 automates ou plus pour des interactions process, le réseau doit également être isolé des autres. Pas de SCADA dessus
- Niveau supervision : le protocole retenu est OPC-UA. Un port dédié est nécessaire sur le switch.

En 2022, la communication *backchannel safety* entre CPU n'est pas garantie entre des équipements de sécurité de marque différente, il est obligatoire que les automates soient du même fabricant. L'utilisation de marques différentes impose un automate intermédiaire côté site ou un ilot déporté au niveau du site pour traduire les informations du réseau en informations câblées. Cette solution n'est pas à privilégier mais peut être utilisée temporairement avant une modernisation.

Obligatoire à la cible : un automate de sécurité mixte (qui comporte à la fois la partie sécurité- rouge et la partie process - blanc, voir image ci-dessous) doit être utilisé plutôt qu'une combinaison de 2 ou plus automates rouges et blanc. Cela présente un avantage tant au niveau de la sécurité que du coût.

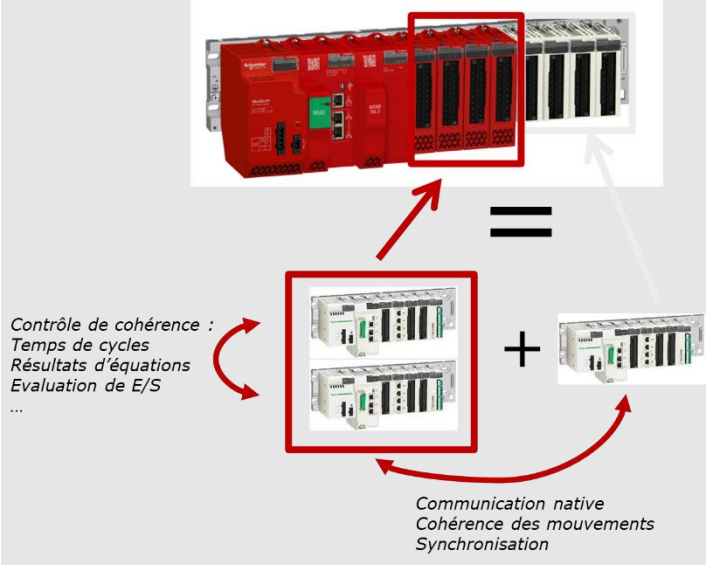


Figure 2 - Fonctions assurées par un automate de sécurité – exemple sur Schneider M580

Obligatoire : en cas de mise en place d'automate de sécurité, les capteurs doivent être compatibles – il faut utiliser des capteurs de sécurité. En cas d'impossibilité il faut respecter les préconisations de câblage du fabricant.

Obligatoire : pour les contrôles process et sécurité, tout ce qui concerne les fonctions de sécurité est câblé côté « rouge », les contrôles process sont câblés côté « blanc ».

Autorisé, mais non recommandé : dans le cas de petite configuration (peu d'entrées sorties) il est possible de câbler l'ensemble des entrées sorties côté sécurité mais le coût peut être élevé et les contraintes de câblage trop importantes. Le coût des cartes d'E/S de sécurité est nettement plus élevé que les celui des E/S standards.

Toutes les connexions locales ou à distance avec le PCC se font au travers du réseau intranet VNF géré par la DSIN. Le réseau fibré propriétaire (cible) donne un large éventail de possibilités de communications.

II.B. Architecture d'automatisme standard Ecluse Petit Gabarit

La cible de modernisation ne prévoit pas d'écluses à petit gabarit téléconduite. La cible est une écluse à petit gabarit automatisée avec des fonctions de réarmement à distance.

Le standard d'architecture illustrée ci-dessous s'applique aux écluses à petit gabarit automatisées avec réarmement à distance :

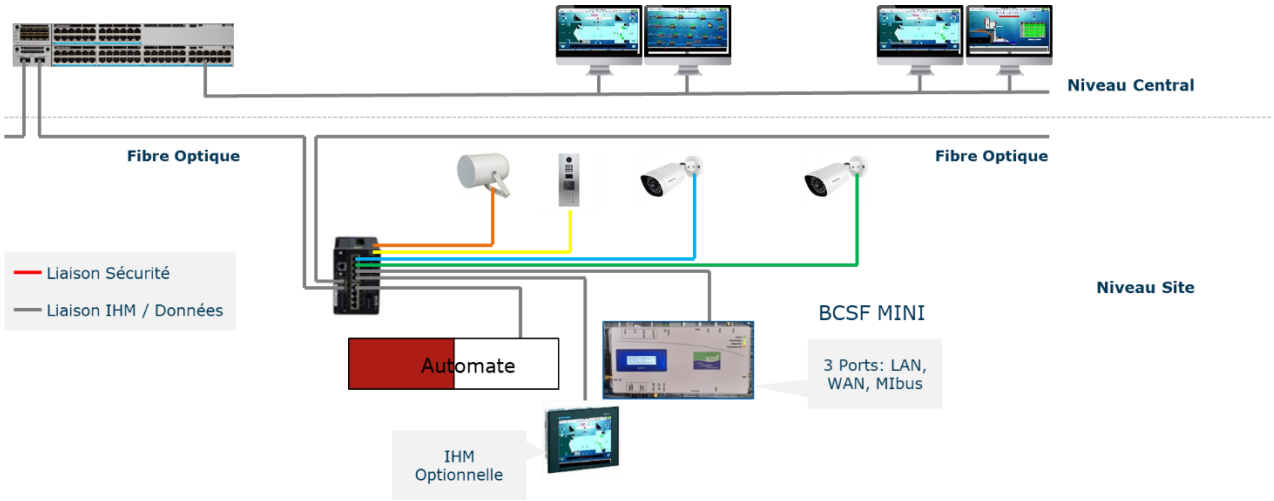


Figure 3 - Architecture d'automatisme standard EPG réarmée à distance, sans barrage – écluse type équipée de BCSF Mini

Pour les écluses équipées de BCSF Complète (écluses particulières - réputées dangereuses), cette BCSF possède un port de sécurité, le schéma de câblage diffère :

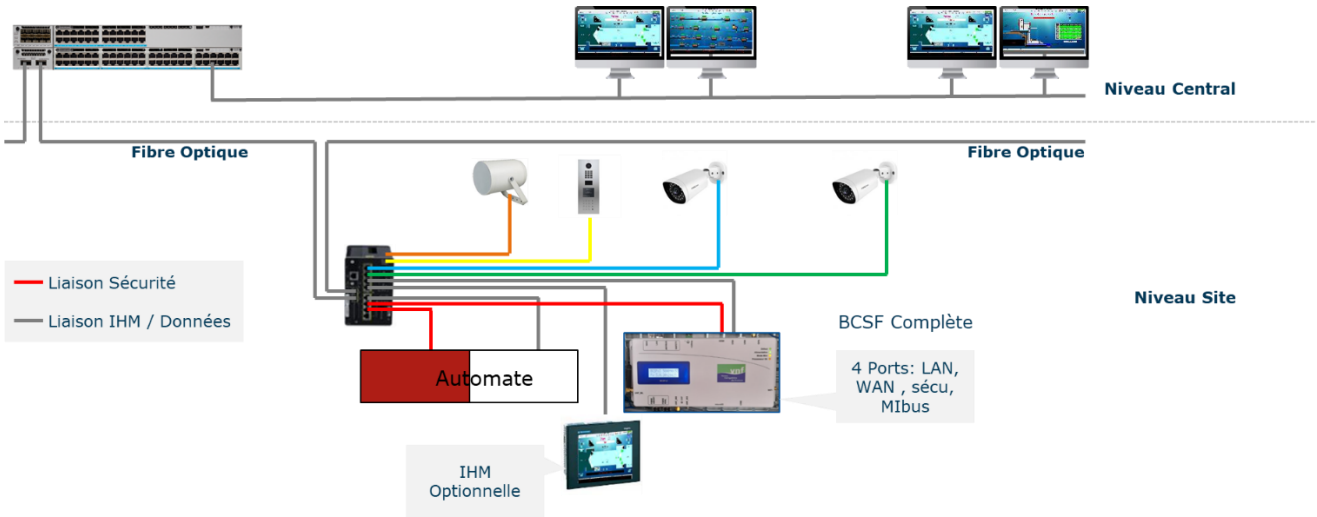


Figure 4 - Architecture d'automatisme standard EPG réarmée à distance, sans barrage – écluse « particulières - dangereuses» équipée de BCSF Complète

Remarques :

- Les modules E/S déportés ne sont pas recommandés sur une EPG car l'objectif est d'avoir le système le plus simple/épuré possible afin de limiter les coûts d'investissement et de maintenance.
- Pour les cas spécifiques où des E/S déportés sont mises en place, cela doit être justifié par un réel intérêt financier.
- L'IHM fixe est en option sur une EPG – pour aide au dépannage. En absence d'IHM fixe, une IHM portable peut être branchée en Ethernet en local pour mainteneurs
- La VRF Safety est locale à l'écluse car il n'y a pas de "bouton d'arrêt d'urgence" déporté au PCC dans le cadre des EPG automatisées avec réarmement
- La liste des ports devient alors :
    - [VRF Voix] - Haut-parleur avec micro intégré
    - [VRF Voix] - Interphone
    - [VRF Vidéo] - Caméra Amont
    - [VRF Vidéo] - Caméra Aval
    - [VRF Industriel Data] - BCSF data
    - [VRF Industriel Data] - IHM
    - [VRF Industriel Data] - Automate Data
    - [VRF Industriel Data] – Maintenance => pour connexion de l'automaticien à l'IHM ou l'automate
    - [VRF Industriel Safety] - BCSF Sécurité => non raccordé au réseau sur EPG « type », mais utilisée sur écluses réputés dangereuse / BCSF complète
    - [VRF Industriel Safety] - Automate Sécurité => non raccordé au réseau sur EPG « type », (fonctionnement local) mais utilisée sur écluses réputés dangereuse / BCSF complète
- En cible une EPG automatisée ne dispose que d'un seul automate par sas permettant de couvrir tous les besoins de navigation et de gestion hydraulique, il n'y aura pas d'autre automate (GH, télégestion ou autre).
    - La liaison permanente entre l'ouvrage et le PCC par la fibre optique VNF (à haut niveau de disponibilité) permet d'échanger directement les informations/consignes avec le terrain de manière fiable.
    - Les PCC vont être équipé d'un système central d'alerte pour les personnels d'astreinte

Avec un total de 8 ports pour une configuration avec BCSF Mini et un total de 10 ports pour une configuration avec BCSF Complète, une extension du switch 8 ports est systématique.

II.C. Architecture d'automatisme standard Ecluse Grand Gabarit

La téléconduite des écluses ne concerne que les Ecluses à Grand Gabarit (EGG). La cible de modernisation de VNF ne comprend pas d'Ecluse à Petit Gabarit téléconduite.

L'architecture standard comporte un automate au PCC, et un automate par sas et par barrage. Des Entrées/sorties déportées sont mises en place au plus près des équipements, au niveau des têtes de portes.

Pour des raisons techniques de compatibilité des protocoles Safety **1 marque unique d'automates doit être utilisée à l'échelle de la DT** (sas d'écluses et PCC nominaux ou de secours)

Au niveau du site, comme évoqué dans un chapitre précédent, il est important de fiabiliser les réseaux dits « Safety ». Il faut donc séparer logiciellement le réseau « Safety PCC » (VRF Safety) des autres réseaux.

Les échanges Safety se font en Modbus, tandis que les échanges process se font en OPCUA.

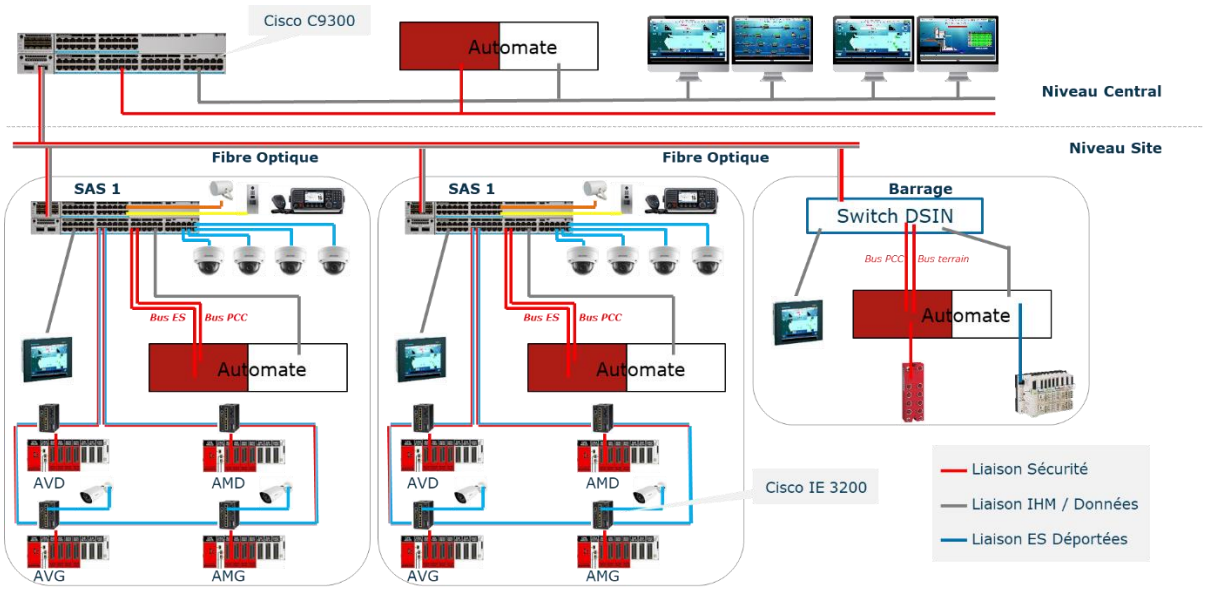


Figure 5 - Architecture d'automatisme standard EGG double sas avec barrage

III. Affectation dynamique des Arrêts d'urgence pour la téléconduite

III.A. Principes d'affectation dynamique des AU pour la téléconduite

Ambitions :

- Permettre l'affectation des écluses entre les différents PCC d'une DT (ou entre PCC de DT différentes) en fonction des conditions d'exploitation (jour/nuit, haute/ basse saison, mode dégradé)
- Utiliser un même pupitre banalisé pour plusieurs fonctions/métiers dans la salle d'exploitation : chef de salle, opérateur de téléconduite, opérateur de réarmement ; probablement gestion hydraulique et gestion du trafic
- En cas de soucis l'opérateur de téléconduite n'a qu'un seul bouton à appuyer et sans se poser de question : un bouton rouge (arrêt d'urgence) par demi-pupitre
- Bouton rouge d'arrêt d'urgence respectant la chaîne de sécurité complète entre le PCC et le sas d'écluse ; un bouton lumineux permettant d'afficher son état : inactif (= éteint), actif (= vert), activé (= rouge)

Contraintes :

- Appairage de l'écluse au PCC : se réalise de manière SIL2 câblée au PCC (BP appairage) et au sas (commutateur local-distant) et protocolaire entre les API sas et API PCC
- Affectation du pupitre à l'écluse : il est réalisé depuis l'IHM d'affectation des sas d'écluses disponible sur le pupitre du chef de salle
- L'écluse doit rester maître de son appairage et de son affectation au PCC
- Avoir un système le plus simple, épuré et compréhensible pour les opérateurs et chefs de salle
- Les sas des EGG doivent disposer des fonctions d'arrêt de sécurité d'un minimum en SIL 2 (réalisé dans les règles de l'art)
- D'après la norme EN 61508-3, il est possible bien que non recommandé en SIL2 (mais pas en SIL3) d'intégrer un élément variable dans chaine de sécurité si cet élément est câblé (pas de virtuel), et si l'équipement est standard SIL2

L'objectif du standard est de définir une architecture et un processus qui permette, dans le respect des règles de sécurité, la téléconduite et l'arrêt d'urgence à distance d'un sas d'une EGG depuis le demi-pupitre de l'opérateur :

Les propositions décrites en <u>Annexe VII.K. Affectation dynamique des AU</u> n'ont pas valeur de standard, elles sont sujettes à évolution à court terme et ne peuvent être mise en place avant d'avoir été certifiée par un organisme extérieur habilité. Cette certification sera engagée par la DSIN en 2023.

Le processus d'affectation se fait en 2 étapes afin de répondre au plus proche des exigences de sécurité SIL2 :

- **1 étape de réservation du sas par le PCC qui se fait intégralement en physique – appui sur boutons raccordés à l'automate de sécurité du PCC, et échange entre automates de sécurité PCC-sas via une liaison sécurisée**
- **1 étape d'affection du sas à un demi-pupitre, à travers le SCADA**

III.B. Rappel des définitions et standards couleurs

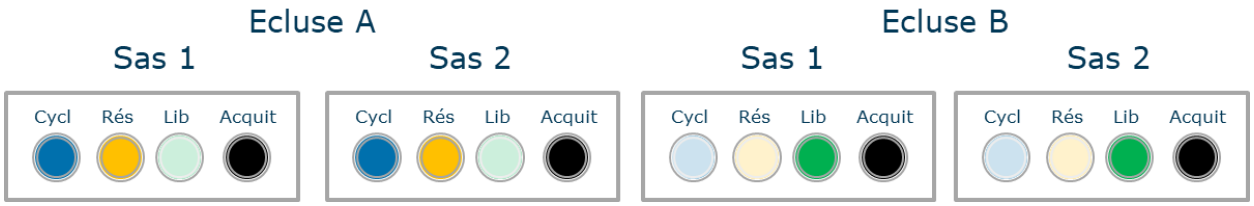
Le **code couleurs pour organes de commande à bouton poussoir** est défini selon la norme ''Sécurité des Machines'' IEC 60204-1 chap. 10 paragraphe 10.2.1 Tableau 2 Page 96 :

- **ROUGE** : Urgence, Application, Arrêt Urgence
- **BLANC** : Marche/Mise sous tension (préférée)
- **NOIR** : Marche/Mise sous tension, Arrêt/Mise Hors Tension (Préférée)
- **JAUNE** : Intervention pour supprimer une condition anormale ou pour remettre en route un cycle automatiquement interrompu
- **VERT** : Actionner pour initier des conditions normales
- **BLEU** : Obligatoire, Fonction de réarmement (acquittement des défauts)
- **GRIS** : Marche/Mise sous Tension, Arrêt/Mise sous Tension

Ce code couleur doit être repris sur l'IHM de supervision

Coffret mural PCC :

- Le coffret mural au PCC devra permettre de sélectionner les sas à réserver par le PCC.
- Des voyants oranges et verts permettront de savoir si le sas est libre ou réservé. (Voir figure 7)
- Un voyant ou une interface visuelle (non présent sur les figures 7 et 8) devra permettre de détecter un éventuel Cycle en Cours au niveau du sas.
- Des boutons poussoirs (avec voyants oranges et verts qui permettront de savoir si le sas est libre ou réservé) permettront de déclencher les actions de réservation, de libération et d'acquittement



- Il est recommandé de regrouper les panneaux par itinéraire pour faciliter le repérage des boutons.

Figure 76 - Exemple non standard, pour illustration : coffrets d'arrêts d'urgence du centre de gestion de la navigation de la CNR

- Il est recommandé d'éclairer le nom de l'ouvrage lors qu'il est affecté. (Voir figure 8)
- Lebouton « test lampes » est à mettre en place par PCC et non pas par coffret.

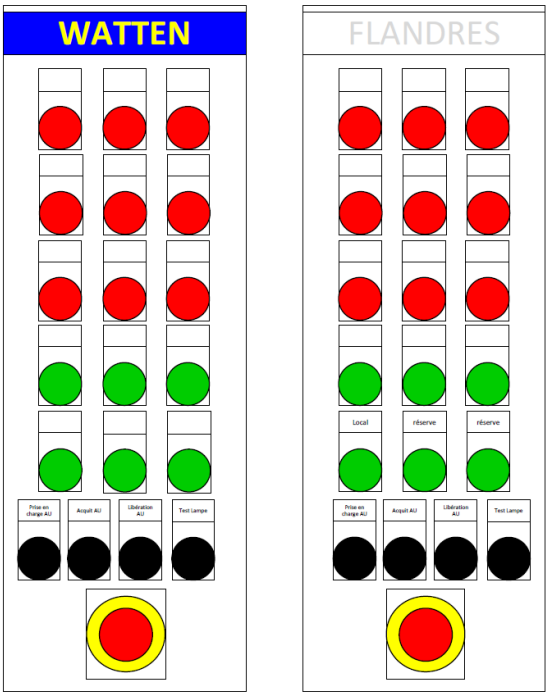


Figure 7 - Exemple non standard, pour illustration - Coffret téléconduite DT NPdC

IV. Choix du matériel

IV.A. Compatibilité Cybersécurité

Références des gammes d'automates autorisés à être déployés dans les écluses :

Fabriquant	**Gamme de matériel autorisée**	**Ecluse Petit Gabarit (EPG)**	**Ecluse Grand Gabarit (EGG)**	**Certification Cybersécurité**
Siemens	S7-1500 ou ET200-SP	*À privilégier :* Config. 100% ET200-SP Safety	*À privilégier :* Config. 100% S7-1500 2PN Safety	ANSSI pour : « ensemble de la gamme d'automates Simatic S7-1500 de Siemens » CPU 1516 et 1518 certifiés
Schneider	M580s	M580s	M580s	ANSSI pour : « Modicon M580 PAC, comportant un module CPU BME P58XXXX1 avec firmware V3.10 et deux modules Ethernet BME NOC 0301 avec firmware V2.17 »
Phoenix Contact	ACXF	AXC F2152+ AXCF XT SPLC 1000	ACX F3152 + AXC F XT SPLC 1000	BSI

Pour plus d'informations concernant ANSSI/BSI, voir annexe *VII.G. Définitions cybersécurité : ANSSI, BSI*

IV.B. Relayage parallèle

Plusieurs modes de marche sont mis en place pour s'adapter aux différents contextes et aux personnes qui manipulent les installations :

- Le mode automatique : les installations fonctionnent seules sans intervention d'un agent ;
- Le mode manuel : ce mode est **dédié aux exploitants**. Il permet le pilotage unitaire des organes de l'écluse mais en conservant l'ensemble des sécurités (fins de courses par exemple) pour éviter toute erreur de manipulation.
- Le mode maintenance : ce mode est dédié à la maintenance. Le pilotage des organes est totalement libre pour permettre aux mainteneurs de travailler sans contraintes.

Le relayage en parallèle de l'automate n'est réellement utile qu'en cas de panne automate (de plus en plus rare compte tenu de la fiabilité de ces équipements). Il ne concernerait dans tous les cas que le mode maintenance et l'automate a tout à fait la capacité de réaliser ces opérations.

D'autre part, la mise en place de fonction de sécurité engendre une augmentation du nombre de contacteurs lorsqu'ils doivent être redondés et la mise en place d'un mode à base de relayage peut selon les méthodes augmenter la taille des armoires de commande.

Le standard automate ne retient donc pas ce mode de fonctionnement par relayage en parallèle de l'automate. Seul le pilotage des organes/équipements par automate est retenu.

IV.C. Automate de télégestion

Un automate de télégestion est un automate qui est capable de communiquer via des technologies sans fil (3G, GPRS, Lora, etc.) et d'envoyer des alertes par SMS ou par appel téléphonique.

Interdit à la cible : les automates de télégestion ne sont plus nécessaires. En effet les automates modernes préconisés ainsi que le réseau haute disponibilité utilisé (FO VNF) permet d'avoir une liaison permanente entre le PCC et les ouvrages.

Pour un PCC ouvert :

- H24 (5 DT sur 7) les alarmes pourront être traitées par un opérateur ;

- H12/H16 reporté dans un PCC H24 d'une autre DT ou utiliser un système de gestion des alarmes (par SMS, mail ou application dédiée). Dans ce cas les alarmes et la gestion d'astreintes sont centralisés au PCC, qui contacte l'agent d'astreinte.

Les alertes remontées au PCC permettent aux opérateurs de prendre connaissance de la situation (SCADA, vidéo, ….), de diagnostiquer, éventuellement résoudre le problème à distance et d'envoyer en dernier temps un agent adapté (itinérant ou mainteneur) sur place. Cette méthode est importante pour éviter d'envoyer systématiquement des agents sur le terrain quelle que soit l'alarme.

Autorisé temporairement : pour les sites isolés, un automate de télégestion peut être conservé avant de passer vers un automate process moderne. Il ne faut en aucun cas doubler les automates (process et télégestion)

IV.D. Contraintes OPC-UA

L'OPC-UA est le protocole d'échanges sécurisé (au sens cyber) retenu par la DSIN et la DIEE pour les échanges automates vers la supervision : API <-> OPC-UA <-> Supervision.
Il ne faut pas confondre ce protocole avec les protocoles Safety (Profisafe, EIP safety).

2 types de supervision sont à utiliser pour la gestion des écluses à distance :

- Petit Gabarit (réarmement) via l'applicatif national SGTf (application du SCADA national) qui va gérer le trafic et les EPG
    - BCSF mini : APIs <- Modbus -> BCSF <- OPC-UA -> SGTf
    - BCSF complète : APIs <- Protocole Safety -> BCSF <- OPC-UA -> SGTf
    - Les fonctions de réarmement dans BCSF et SGTf seront développées à partir de 2023
- Grand Gabarit (téléconduite) via l'IHM téléconduite développé par la DSIN
    - APIs <- OPC-UA -> PCC

L'utilisation d'OPC-UA impose, selon le constructeur, quelques vérifications sur le matériel à utiliser :

Schneider :

- Coupleur de communication spécifique
- Ajout d'une carte spécifique OPC-UA : BMENUA0100
- Obligation (comme pour toute installation Safety) d'avoir des racks Ethernet : BMEXBP
- Interdiction d'utiliser certaines cartes (cartes de comptage par exemple)
- Impossibilité de faire passer les deux protocoles par le même port soit :
    - Un port pour la communication Safety avec PCC
    - Un port pour la communication Safety E/S
    - Un port pour la programmation
- Vérifier la compatibilité SAFETY de la configuration réalisée via l'outil EcoStruxure Control Expert

Siemens :

- OPC-UA Natif
- Préconisation de séparer les réseaux via port/coupleurs dédiés
- Protocole partie process : Profibus, Profinet, Modbus
- Protocole process safety : Profisafe

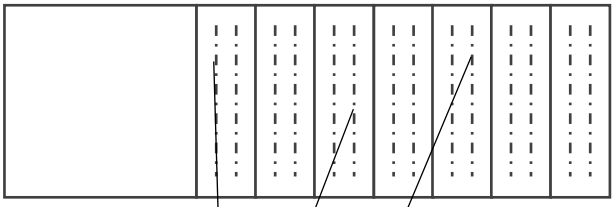
Phoenix Contact :

- OPC-UA Natif
- OPC UA
- Protocole partie process : Profibus, Profinet, Modbus
- Protocole process safety : Profisafe

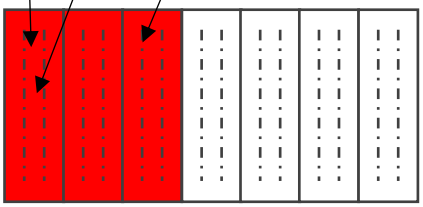
IV.E. Mise à la cible de l'existant - *migration M340 vers M580 Safety*

Les différentes cartes d'entrées sorties « non safety » sont identiques pour les deux plateformes. La migration d'un M340 vers un M580 consiste à :

1. **Redistribuer les E/S :**

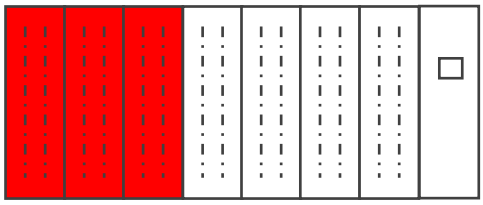


- Reprendre les éléments liés aux fonctions de sécurité à câbler sur des entrées sorties « safety ».

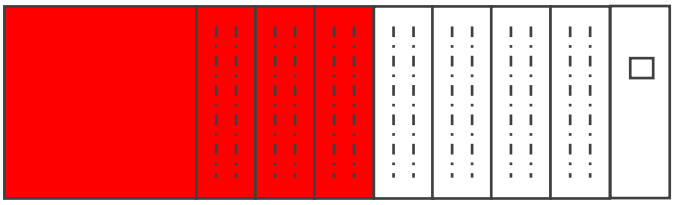


- Les autres entrées sorties peuvent être conservées

2. **Installer les cartes de communication nécessaires (OPC-UA pour Schneider)**



3. **Remplacer le processeur et l'alimentation**



4. **Reprendre le programme pour intégrer les fonctions de sécurité**

IV.F. Comparatif des solutions

L'objectif à terme du groupe de travail, de la DSIN/DIEE est de définir une unique référence matérielle d'automate à l'échelle de l'établissement. Note : Les modèle EPG et modèle EGG pourraient ne pas être les mêmes.

L'ambition pour le Petit Gabarit est la conception nationale, portée par les DT de :

- Un programme national
- Un design d'armoire nationale « plug & play »

Le choix du matériel n'a pas d'impact sur l'opérateur au PCC. Les populations impactées sont les mainteneurs, les automaticiens ainsi que les acheteurs.

Une étude comparative réalisée se base sur les critères suivants dont la pondération reste à définir :

Critères	Questions
Atelier logiciel	**Atelier logiciel**
	Annuaire automaticien interfacé avec l'annuaire d'entreprise de VNF : Dans l'atelier logiciel
	Langages supportés par la norme IEC 61131-3 (grafcet, ladder, DFB, ST, IL)
	Langages évolués (NodeRed,...), fonctionnalités évoluées, ...
Technologies	**Protocoles de communication**
	Serveur web intégré dans l'automate
	Protocoles de communication sécurisés : API-SCADA : OPC-UA : carte spécifique ou natif CPU
	Protocoles de communication sécurisés : APIs écluse <-> APIs PCC : protocole utilisé ?
	Protocoles de communication sécurisés : APIs écluse <-> Module déporté E/S sur le terrain : protocole utilisé
	Protocoles de communication sécurisés : APIs écluse <-> Matériels de process sécurisés : protocoles utilisables
	Matériel
	API : Annuaire automaticien interfacé avec l'annuaire d'entreprise de VNF
	Atelier logiciel : Annuaire automaticien interfacé avec l'annuaire d'entreprise de VNF
	Présence des sources dans la CPU
	Tables d'animations et un simulateur
	Encombrement et la facilité de remplacement des éléments constitutifs de l'automate
Evolutivité	**Gamme : pérennité, évolutivité**
	Intégration de OPC-UA Safety
	Evolutions de l'atelier logiciel (exemple gestion d'utilisateurs)
	Evolutions de la gamme automate
	Pérennité de la gamme
Cybersécurité	**Politique cybersécurité**
	Certification/qualification ANSSI/BSI
	Gestion des certificats
	Stratégie globale de mots de passe
	Stratégie mots de passe atelier logiciel
	Stratégie de mots de passe Automates
Licences	**Licences**
	Récupération des licences actuelles
	Serveurs central de licences (jetons)

	Licence d'entreprise VNF
	Modèle économique OPEX / CAPEX
	Disponibilité à l'UGAP ?
Couts	**Coûts**
	Coût matériel (Ecluse standard PG)
	Remise consentie
	Coût SAV (abonnement, jetons)
	Atelier logiciel API traditionnel : cout licence nationale
	Atelier logiciel API sécurité : cout licence nationale
Support	**SAV & documentation**
	Documentation (accès en ligne, détails techniques, forums…)
	Possibilité de contact via hotline
	Intégration au catalogue de formation VNF
Changement	**Gestion du changement**
	Possibilité d'importation et exportation des données et sources & outils de génération automatique (données automates)
	Outils de gestion de versions des programmes et des blocs fonctionnels
	Maitrise de la solution par VNF (en DT et au siège) / Effort de formation

V. Standards d'intégration EPG

V.A. Principes de mise en œuvre

Le niveau SIL2 est le minimum à atteindre pour les EPG

1. **La mise en œuvre des automates de sécurité, comme toute installation électrique, doit faire l'objet d'attention particulière sur les principes d'installation (sensibilité plus importante qu'un système classique) :** Les mises à la terre des :
    1. Châssis, armoires…
    2. Équipements (capteurs, actionneurs…)
    3. Cheminements
2. La séparation des câbles de puissances et de commandes
3. La longueur des câbles (chutes de tension…)
4. Le câblage des entrées :
    1. Nécessité, dans certains cas, d'ajouter des résistances ou diodes (exemple du capteur avec contact à fermeture pour garantir le contrôle de continuité)
    2. S'assurer de la conformité du raccordement ou de la mise en œuvre avec les préconisations des constructeurs et selon les cas d'usage.
        - Schneider (Safety) : Manuel de sécurité Modicon M580 (Réf QGH46983)
        - Siemens (Fail Safe) : Manuel de sécurité fonctionnelle S7-1500 (Réf A5E38761888-AA)

La protection contre les intrusions doit également être mise en place :

- Protection des locaux
- Protection des câbles
- Protection des armoires

L'exigence de mise en place de badges (traçabilité des accès) doit être clarifiée par l'atelier du Lab « Cybersécurité », une solution nationale sera probablement mise en œuvre.

V.B. Armoire EPG type

L'objectif en 2023 est de définir une armoire d'automate standard à 80%, avec un schéma type à donner aux tableautiers. L'idéal serait même d'avoir un marché national de fourniture d'armoire pour les EPG. Un process de réception après s'installation pour s'assurer du fonctionnement doit être créé.

La coupure d'urgence d'une EPG doit être mise en place dans le général dans le TGBT.

L'armoire doit permettre 3 modes de pilotage de l'écluse : par l'exploitant normal / manuel (surveillé par automates) par le mainteneur maintenance (mouvement non sécurisé)

Il y a 3 types d'organes de manœuvre :

- Crémaillère (électrique)
- Vérin (Hydraulique) : 1, ou 2, ou 3, ou 4 centrales hydrauliques
- Servomoteur – vérin électromécanique

Des configurations spécifiques peuvent être intégrés à l'armoire :

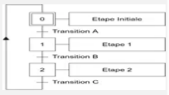
- Dérivation
- Alimentation secourue par groupe électrogène mobile (onduleur/groupe électrogène fixe sont à éviter pour des raisons de coût)
- Exutoire
- Éclairage du site
- Nombre de vannes / ventelles variables

Mode de pose de l'armoire électrique :

- Dans la guérite, avec pupitre spécifique avec vue sur sas
- Dans une armoire extérieure en inox – la qualité d'inox à adapter selon la région et la proximité de la mer, avec systèmes de chauffage et ventilation adaptés pour éviter les problèmes de condensation.

VI. Méthodes de programmation des automates de sécurité

VII.A. Langages normalisés

Langage	Représentation	Avantages	Défaut	Utilisation
Schéma à contacts		• Mise au point et maintenance facile et visuelle	• Non adapté aux programmes complexes	• Gestion de défaut • Processus binaires simples
Liste d'instructions		• Optimisation des temps de cycle	• Proche de langage informatique non structuré comme l'assembleur • Mise au point laborieuse	• Processus simple exigeant en temps de cycle
Diagramme de blocs fonctionnels		• Compacité • Visuel	• Exige une bonne connaissance du comportement des blocs utilisés	• Instanciation (DFB) ou appels (FB) de blocs fonctionnels
Texte Structuré		• Langage de haut niveau • Adapté aux processus complexes • Facilement portable d'une plateforme à une autre • Facile à commenter	• Pas très visuel en mise au point ou maintenance • Fonctions booléennes laborieuses	• Blocs fonctionnels pour une meilleure portabilité
Graphe séquentiel		• Adapté aux processus séquentiels • Visuel	• Gestion des arrêts / reprises de cycle, initiation…	• Processus simple et séquentiel

- Texte structuré à utiliser là où c'est opportun et approprié : par exemple pour le développement des blocs fonctionnels standards de haut niveau (portabilité facilitée entre différentes marques sur les fonctions standard)
- Diagramme de blocs fonctionnels à utiliser là où c'est opportun et approprié : par exemple pour les appels de blocs et asservissements, pour dupliquer les programmes à grande échelle et faciliter la maintenabilité (1 fois pour N blocs)

Remarques :

- L'objectif est de connaitre le fonctionnement des blocs pour ne plus avoir à les ouvrir.
- La bibliothèque de blocs sera à disposition de tous les automaticiens
- Une « plateforme » est un atelier logiciel/une marque automate
- Il est possible de faire du ladder ou du Grafcet dans les blocs, si tout le monde programme dans la même plateforme. Sinon il faut utiliser du texte structuré, ce qui représente un effort d'adaptation
- Le texte structuré à préférer si travail sur plusieurs plateformes. Si une seule plateforme, on peut prendre le langage préféré VNF.
- Le ladder n'est pas du tout adapté aux fonctions qui nécessitent un processus itératif, ou du travail avec des tableaux, des chaines de caractères, tout ce qui relève du traitement informatique pur. En revanche je pense que le ladder est bien adapté à la description des graphes et notamment pour la maintenance (langage visuel).
- Les fonctions de communication sont déjà des blocs
- Une table de visualisation devra être mise à disposition du dépanneur

VII.B. Blocs fonctionnels

Le découpage fonctionnel réalisé – voir annexe *VII.D. Découpage fonctionnel des EPG,* permet de créer des blocs fonctionnels qui soient standardisables et réutilisables sans limitation. Une premier exemple de blocs fonctionnel est présenté ci-dessous, cette proposition devra être détaillée par la suite – Ateliers du Lab 2023

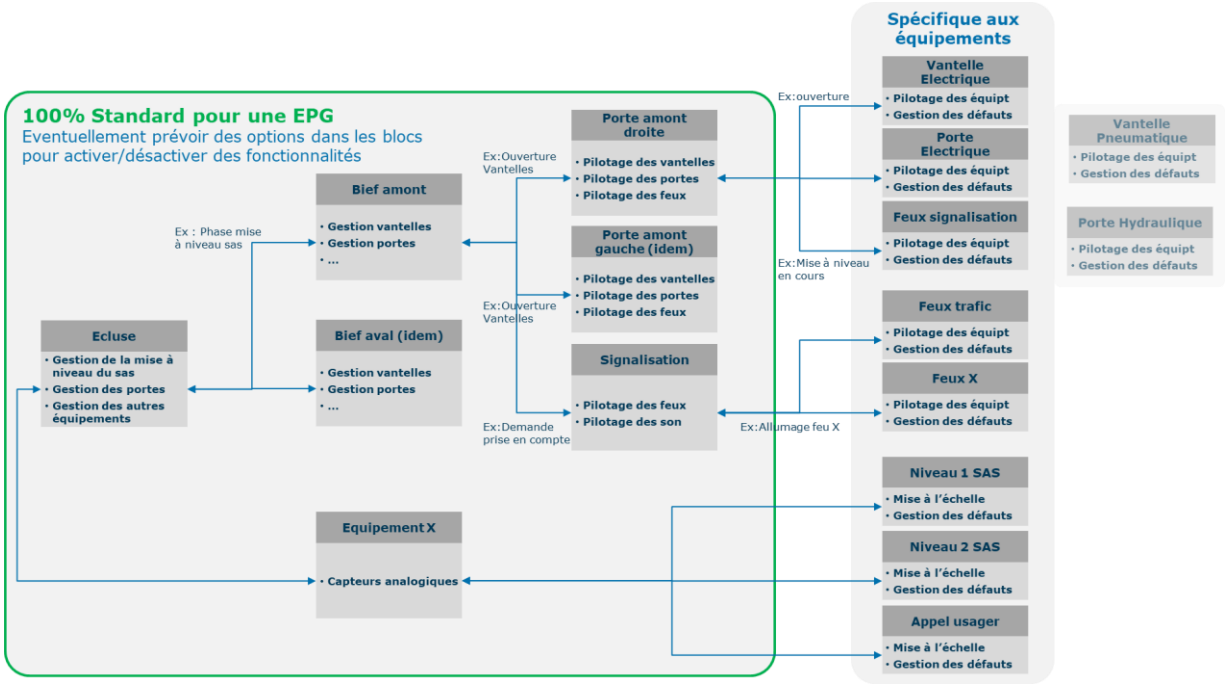


Figure 8 – Proposition de découpage fonctionnel – non validé

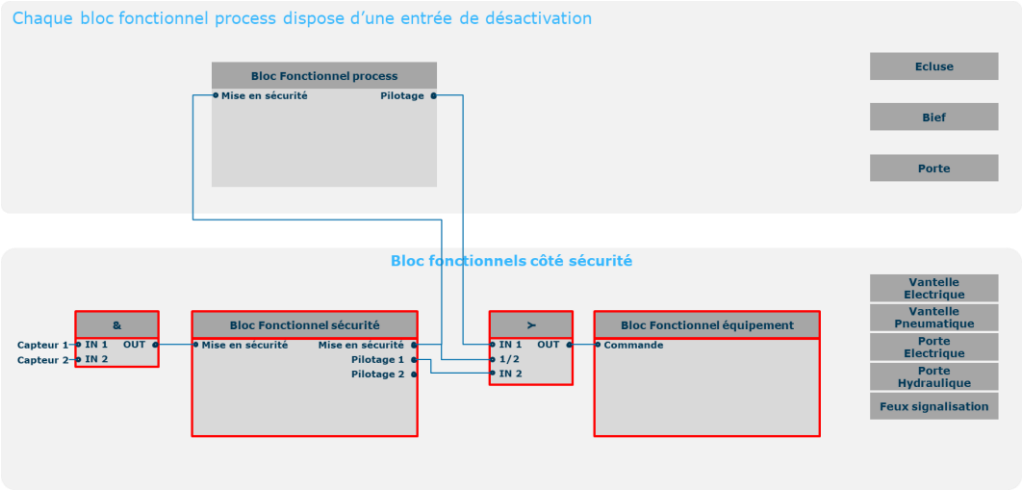


Figure 9 - Principe de gestion de la sécurité

Ce principe permet de couper le bloc process lors du passage en mode sécurité.

La DSIN fournira un bloc fonctionnel pour les APIs aux sas, et un programme complet pour les APIs aux PCC. Cela reste à construire collectivement en 2023, et à améliorer en continu par la suite, cela afin de ne pas réinventer les programmes à chaque fois et d'utiliser partout le meilleur programme possible.

VII. Annexes

VII.A. Méthodologie standard de projet VNF

Les principales étapes de la méthodologie standard sont les suivantes :

1. Analyse de risque
2. L'analyse fonctionnelle
    - Zonage (utiliser la S88)
    - Fonctions automatiques de service / fonctions de sécurité
    - Modes de fonctionnement
    - Le Guide d'Etude des Modes de Marche et d'Arrêt
3. Spécifications techniques
    - Choix du matériel et architecture
    - Agrément matériel
4. L'arbre de défaillances
5. Cahier de tests

Notes :

- Le zonage et la définition des fonctions automatiques de service / fonctions de sécurité sont importants pour la configuration et le choix du matériel (nombre de coupures d'urgence, de cartes d'Entrées/Sorties…), doivent donc être effectués avant.
- Il faut qualifier les défauts en bloquant (réarmement à distance) ou non-bloquant (déblocage sans acquittement, l'usager peut relancer le cycle, par exemple pour un usager qui met du temps à arriver)
- La détection se fait via la surintensité des moteurs (électrique) ou l'augmentation de la pression (hydraulique). L'utilisation de relais thermique est recommandée si pas de variateur de vitesse, pour ne pas avoir de défaut disjonction. Le réglage des pressostats doit être effectué pour éviter la détection intempestive.
- Il est important de bien récupérer la propriété intellectuelle des documents produits par les sous-traitants (Dossier d'Ouvrage Exécuté, éventuelle analyse de sécurité Systema)
- Cette méthodologie doit être appliquée pendant toute la durée de vie de l'ouvrage (création, modifications fonctionnelle, maintenance avec changement de matériel…)
- Elle doit aussi intégrer la notion de Cybersécurité à chaque étape

VII.B. Analyse de risque EPG

VII.B.1. Rappels de méthode

L'analyse de risque est un processus mis en œuvre pour comprendre la nature des phénomènes dangereux et pour déterminer le niveau de risque. Elle se conduit en 5 étapes :

1. Identifier les risques : Lister tous les risques sans se préoccuper de la gravité ou de la probabilité.
2. Evaluer la gravité : Pour chaque risque identifié, on tente de peser les dommages potentiels.
3. Evaluer la survenance : Pour chaque risque identifié, on tente de déterminer la probabilité de survenance.
4. Identifier les points critiques : Pour les risques situés dans la zone chaude, identifier qui/quoi est impacté et à quel moment

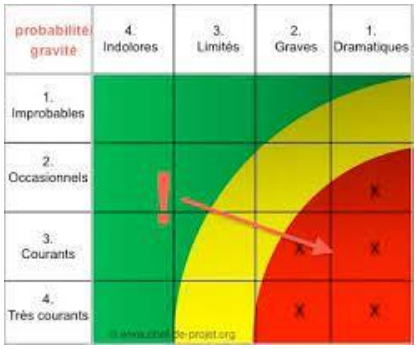


Figure 10 - Grille d'analyse de risque

5. Déterminer le niveau de sécurité à atteindre et à quel niveau de l'installation

L'analyse de risque détermine un niveau de risque appelé SIL, Safety Integrity Level (ou niveau d'intégrité de la sécurité) classé de SIL 1 à SIL 4, SIL 4 correspondant au risque le plus élevé. En fonction de ce niveau de risques, les activités de développement imposées par la norme sont plus contraignantes

Échelle des niveaux SIL

	Sollicitations du SIS		
SIL*	rares PFD**	fréquentes PFH***	Facteur de réduction du risque
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$	10 000 à 100 000
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$	1 000 à 10 000
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$	100 à 1 000
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$	10 à 100

** Safety Integrity level, niveau d'intégrité de la sécurité*

***Probability of Failure on low Demand, probabilité d'avoir une défaillance (pour réaliser la fonction de sécurité prévue) au moment d'une sollicitation*

****Probability of a dangerous Failure per Hour ou Probability of Failure on High demand, probabilité d'une défaillance dangereuse par heure*

Figure 11 - Echelle des niveaux SIL

VII.B.2. Remarques spécifiques à VNF

Concernant l'identification des moyens de mise en sécurité et des moyens de réactions, il est recommandé de se focaliser sur les risques graves et fréquents – en cas d'accident, VNF devra rendre des comptes concernant l'analyse de risque et la justification des moyens mis en œuvre.

La remontée des accidents et presqu'accidents est à faire systématiquement pour permettre de compléter et mettre à jour les analyses de risque.

La totalité des éléments de sécurité doivent être au niveau de risque correspondant au niveau de risque le plus élevé : ce niveau est SIL2 pour une EPG. Par extension l'écluse à grand gabarit répond à ce même niveau SIL2.

Dans le cas des installations télégérées, il est important de tenir compte dans l'analyse de risque liée à la sécurité machine, des éléments susceptibles de modifier les causes d'un risque (contrôle à distance, problème réseau, …) et donc son évaluation et les moyens mis à disposition pour réduire ce risque. La cause peut être un événement réseau de type broadcast non contrôlé qui envoie une mauvaise information à l'automate et déclenche l'événement redouté.

Pour réduire les risques liés à l'interconnexion d'un automate sur les installations, il est important de segmenter les réseaux pour éviter que des équipements dits bureautiques défaillants impacte le réseau industriel.

Les risques sont quantifiés sur 2 échelles correspondant à la méthodologie standard : Gravité et Occurrence.

La quantification de la Détection n'est pas obligatoire.

CRITICITE :

La criticité de la situation dangereuse s'exprime par la combinaison des facteurs de :

Symbole	Désignation	Niveau 1	Niveau 2	Niveau 3	Niveau 4
G (Gravité)	Gravité du dommage pouvant résulter de la situation dangereuse	Lésion légère	Lésion irréversible aux membres supérieurs par exemple	Lésion grave aux membres, au torse, etc...	Perte d'un membre Noyade Chute de plus de 3 m
O (Occurrence)	Ce paramètre caractérise : la fréquence et la durée d'exposition et la probabilité d'occurrence du phénomène dangereux	Rare et / ou Durée d'exposition courte Occurrence supérieure à un an	Peu fréquente et / ou Durée d'exposition moyenne Occurrence de plusieurs fois par an	Fréquente et / ou Durée d'exposition forte Occurrence à la journée	Très fréquente et / ou Durée d'exposition longue Occurrence de l'ordre de bassinée
D (Détection)	Possibilité d'éviter ou de limiter le dommage (probabilité) Caractérise l'efficacité des moyens de prévention	Niveau de protection / prévention élevé	Prévention existe mais probabilité d'incident voisine de 1%	Efficacité des moyens de prévention faible. Probabilité d'incident voisine de 10%	Absence (ou mauvaise efficacité) de moyen de prévention

Pour les EPG, une analyse de risques standard existe déjà, définie avec l'Apave – voir document « CDC_P05_Analyse des risques ».

Cette analyse de risque doit être appliquée, elle peut être adaptée au cas par cas localement pour refléter les spécificités d'un ouvrage.

VII.C. Liste des événements redoutés (ER) VNF

Le tableau des ER redoutés VNF a été réalisé par un organisme externe spécialisé :

ER	Libellé	Gravité des blessures / Fréquence d'apparition	Probabilité de défaillance acceptable	Moyens de réduction à prévoir/ conséquences techniques et organisationnelles
ER1	Ouverture intempestive des vantaux amont et aval	S2 / F1	---	Il est préférable que la chaine de commande passe par l'API/relais de sécurité.
ER2	Ouverture prématurée des vantaux	S2 / F1	10^{-7}/h	La chaine de commande doit passer par l'API de sécurité (**SIL3**).
ER3	Ouverture intempestive ou non fermeture des vantelles	S2 / F1	10^{-7}/h	La chaine de commande doit passer par l'API de sécurité (**SIL3**).
ER4	Fermeture prématurée des vantaux sur un bateau	S2 / F1	10^{-7}/h	Barrière immatérielle au plus près des portes.
ER5	Erreur d'affichage sur les panneaux de signalisation	S2 / F1	10^{-7}/h	Surveillance du fonctionnement du feu rouge grâce à l'utilisation d'un capteur.
ER6	Risque d'électrocution par intervention sur un système non protégé	S2 / F1	---	Conception suivant les règles de l'art notamment NF C15 100. Habilitation électrique des agents (UTE C18-510) Contrôle régulier des installations
ER7	Risque de traumatisme dû aux équipements sous pression hydraulique	S2 / F1	---	Utilisation de composants CE et conception suivant les règles de l'art Habilitation des agents de maintenance Contrôle régulier des installations
ER8	Perte de mise en sécurité de l'écluse sur commande d'arrêt d'urgence	S2/F1	10^{-6}/h	Arrêts de sécurité niveau **SIL2**

FA : Fonction automatique (SCUO V2)
ER : Evénement Redouté (au niveau de l'écluse)
SIL : Safety Integrity Level (IEC 61062)
PLr : Niveau de performance requis (EN ISO 13849)

Figure 12 - Tableau des ER VNF

Dans le cas de la fermeture prématurée des vantaux sur un bateau, détectée visuellement ou par surintensité pour de l'électrique, on peut imaginer rouvrir les portes légèrement pour libérer le bateau - sans les rouvrir entièrement pour ne pas générer d'autre risque.

VII.D. Découpage fonctionnel des EPG selon le modèle ISA S88

L'objectif du découpage fonctionnel selon le modèle ISA S88 est de créer des blocs fonctionnels qui soient standardisables et réutilisables sans limitation. Il s'agit d'un zonage fonctionnel et non géographique. Par exemple, des vantelles qui ne sont pas sur le vantail mais en dérivation peuvent faire partie du même bloc fonctionnel.

La liste des éléments de sécurité doit être estampillé par un organisme externe (contraintes pénales).

Contrôle	Equipement	Unité	Cellule	Sécurité
Actionneur de vantelle / vannage (inclus capteur de surcourse, variateurs)	Vantelle/vannage	-	Navigation	Oui
Capteur de fin de course de vanne / vantelles (min-max) – 2 types de vanne : principale & ajustement	Vantelle/vannage	-	Navigation	Oui en électrique / Non en hydraulique (utilisation de blocs de temporisation -> temps enveloppe = double ou triple du temps normal de fermeture des vannes/vantelles)
Capteur de position de vanne	Vantelle/vannage	-	Navigation	Non
Actionneur de porte (inclus capteur de surcourse, variateurs)	Vantail	Porte**	Navigation	Oui
Capteur de fin de course porte fermée	Vantail	Porte	Navigation	Non
Capteur de fin de course porte ouverte	Vantail	Porte	Navigation	Oui 1 à l'amont et 1 à l'aval côté guérite en cas de BCSF Maxi / complète SIL2 Nondans les autres cas
Capteur de position de porte	Vantail	Porte	Navigation	Non
Feu flash/entrée/mouvement de porte (1 par porte ou 1 par vantailx2)	Vantail	Porte	Navigation	Non
Centrale hydro	Vantail	Porte	Navigation	Non
Capteur pression, température, niveau sur les centrales hydro	Vantail	Porte	Navigation	Non
Capteur débusqueur	-	Porte	Navigation	Non
Capteur de détection de bateau - comptage	-	Porte	Navigation	Non
Tirette d'alarme - déclenchement du cycle de sécurité (différent de CU)	-	-	Navigation	Oui
Arrêt d'urgence (pupitre) – déclenchement du cycle de sécurité (différent de CU)	-	-	Navigation	Oui
Feu de sortie de sas (2x2)	-	-	Navigation	Non
Feux de navigation (4x2)	-	-	Navigation	Non
Feu de tirette (3)	-	-	Navigation	Non
Perche d'annonce	-	-	Navigation	Non
Tirette de sas (départ cycle)	-	-	Navigation	Non Tirette optionnelle en BCSF mini Tirette prohibée en BCSF complète
Capteur de niveau : bief amont, bief aval (sas - pas standard PG, écluses doubles)	-	-	GH / Navigation	Non
Capteur d'alimentation en eau des vannes à jalousie (GH)	-	-	GH	Non

** une porte = 2 vantaux

VII.E. Intégration de la Cybersécurité dans la méthode

Les systèmes VNF étant maintenant interconnectés par la fibre optique, le risque de malveillance Cyber augmente. La segmentation des réseaux bureautique et industriel est primordiale – *voir standard « Réseaux »*

En phase de spécification, les exigences suivantes doivent être intégrées :

- Définir la localisation des équipements afin d'assurer leur sécurité physique en restreignant les accès
- Prévoir la possibilité de changer les configurations par défaut
- Intégrer des mécanismes pour faciliter la requalification d'une installation suite à des modifications
- Exiger, si possible, la non-adhérence des logiciels fournis à une version précise d'une autre brique logicielle (système d'exploitation, système de gestion de bases de données, etc.), à défaut, exiger que le fournisseur assure la compatibilité ascendante avec les évolutions des briques adhérentes ;
- Exiger que les logiciels non indispensables à la conduite des installations soient installés sur d'autres postes ; *Remarque : les automaticiens auront 2 PC distinct : un PC bureautique, et 1 autre PC pour le dev et se brancher sur les écluses.*
- Utiliser un environnement de développement dédié au SI industriel

En phase de conception, les exigences suivantes doivent être intégrées :

- Réduire les interfaces et la complexité du système afin de limiter l'introduction de vulnérabilités lors de l'implémentation ; *Remarque : concernant les EPG avec E/S déportés, cela introduit du risque cyber, les coffrets déportés doivent être protégés ou alors détecter l'intrusion.*
- Sélectionner les composants offrant les meilleures caractéristiques pour répondre aux exigences de cybersécurité (mécanismes d'authentification, ségrégation des droits, etc…) ;
- Distinguer clairement les profils utilisateur et administrateur et appliquer le principe du « moindre privilège », de la ségrégation des droits, et maintenir un principe d'« accès non accordé si non explicitement autorisé » pour les accès au système ;
- Prévoir des mécanismes permettant de généraliser les changements sur un ensemble d'équipements.

En phase d'intégration, les exigences suivantes doivent être intégrées :

- Changer les configurations par défaut (mots de passe par exemple) ;
- Supprimer ou désactiver les fonctions non utilisées mais activées par défaut (*par exemple : mise en STOP de l'automate à distance permet l'arrêt de l'exécution du programme à distance.)*
- Supprimer les fonctions de débogage comme les traces utilisées pour analyser le comportement des installations. (*Remarque : ne conserver que les fonctions de sécurité, qui permet de tracer les événements côté automate de sécurité).*

En phase de test, les exigences suivantes doivent être intégrées :

- Réaliser les tests fonctionnels de sécurité ;
- Dérouler les tests aux limites, les tests d'erreur des fonctions métier et vérifier les exceptions *Remarque : l'utilisation de blocs fonctionnels standards permet de réduire la profondeur des tests*
- Tester des scénarios de menace (tests de pénétration et tentatives de prise de *contrôle). Remarque : à faire par une équipe spécialisée du métier, permet de vérifier que les préconisations ont été appliqués*
- Tester les moyens de réaliser les opérations de maintien du niveau de SSII (déploiement de correctifs, analyse de journaux d'événements…)
- Vérifier les performances du système en termes de sécurité

Un environnement de développement sécurisé à l'état de l'art doit être mis en place, avec au minimum :

- Utilisation d'un environnement de développement dédié au Système d'Information industriel (pré-prod)
- Application de règles de développement de sécurité
- Utilisation d'outils d'analyse statique et des tests de robustesses

- Audit du code (à la vue des schémas SI pour les automates)

VII.F. Cybersécurité Opérationnelle

Catégorie	Règles	Solutions
Documentation	• Mise à jour pour la conformité vis-à-vis des installations • Accessible • Conservée en lieu sûr	• Tous les documents à jour doivent être dans un seul site (atelier) • GMAO unique – dématérialiser
Gestion des changements / évolutions	• Gestion des interventions (autorisations, rapports…) • Traçabilité des modifications	• Dématérialisation • Activer le journal de traçabilité des activités Safety • Journalisation - qui fait quoi quand (faisabilité à confirmer)
Sauvegardes et restaurations	• Traçabilité des sauvegardes • Sauvegarder l'ensemble des données sensibles (paramètres process)	• Sauvegarde automatique des programmes automates – MAJ automatique depuis PC vers central => outil commun national • Sauvegarde automatique des recettes

Configuration	• Sur les automates et les applications industrielles, au minimum, il faut désactiver
	  • Les fonctions de débogage (des intégrateurs et des équipementiers) ;
	  • Désactivation du mode de programmation à distance ;
	  • Protection d'accès au CPU et/ou au programme ;
	  • Restriction des adresses IP pouvant se connecter (Réseau) ;
	  • La prise en charge des mnémoniques et commentaires.
		• Paramétrage à faire lors de la création du projet d'ingénierie (checklist)
		• Protection CPU dépendante de la solution nationale choisie

Sécurisation des protocoles	• Protocoles non sécurisés sont interdits ou encapsulés • Séparer les réseaux (VLAN, VRF…)	• Séparer les réseaux Safety et OPC UA (fonction, comportement, criticité différentes)
Gestion des obsolescences	• Remplacement des équipements obsolètes • Assurer la compatibilité avec les autres équipements	• Logiciel DSIN • Etat des lieux des firmwares automate via autosave • Retour des DT vers le national concernant les évolutions de firmware
Gestion des points d'accès réseau	• Points d'accès clairement identifiés • Ports non utilisés doivent être désactivés • Alerte en cas d'intrusion	• Sujet réseau. Port maintenance local dédié

Protection des automates	• Protection par mot de passe • Accès en lecture seule pour les interventions de niveau 1 • Accès au code protégé • Contrôle du code pour éviter les malveillances (cas de sous-traitance)	• Idéalement contrôle d'accès par badge sur la porte (nécessite un port réseau dispo spécifique • Armoire fermée à clé spécifique • Détection d'intrusion via contact sec (sur une entrée automate) => Un port intrusion existe sur le switch DSIN • Alerte en cas d'intrusion

Consoles de programmation et postes d'administration	• Protection des codes malveillants (antivirus)
	• Matériels mobiles :
	  • Seuls les matériels autorisés peuvent se connecter au réseau
	  • Périmètre d'utilisation définit
	• Médias amovibles (clés USB, disques externes)
	  • À limiter au strict minimum
	  • Sas de décontamination obligatoire
	  • Pas de connexion au réseau industriel
	  • Désactivation des ports
		• Utilisation d'un sas de décontamination
		• Utilisation de clés chiffrées.
		• Reconnaissance de clé autorisées/ carte SD (clé propriété automaticien)
		• 2 PCs par automaticien : PC Indus & PC bureautique
		• Utilisation de bastion type Wallix pour accès au store

Remarques :

- Le logiciel de sauvegarde automates devra cohabiter avec la future GMAO unique pour traçabilité des changements. (Potentielle question de master data/référentiel entre ces 2 outils)
- Concernant le protocole 802.1X, il est peu supporté par les automates et est plutôt destiné à l'authentification des équipements « consommables » changeant plus régulièrement.
- Le PC Indus d'automaticien doit être un PC de programmation suffisamment puissant et adapté aux préconisations des constructeur

VII.G. Définitions cybersécurité : ANSSI, BSI

Qualification ANSSI :

La qualification est la **recommandation par l'État français de produits ou services de cybersécurité** éprouvés et approuvés par l'ANSSI.
Elle atteste de leur conformité aux exigences règlementaires, techniques et de sécurité promues par l'ANSSI en apportant une garantie de robustesse du produit et de compétence du prestataire de service, et d'engagement du fournisseur de solutions à respecter des critères de confiance.

Certification ANSSI :

La certification est **l'attestation de la robustesse d'un produit**, basée sur une analyse de conformité et des tests de pénétration

2 certifications existent :

- La certification critères communs (CC) - Le standard internationalement reconnu avec plusieurs niveaux d'assurance
- La certification de sécurité de premier niveau (CSPN) - L'alternative pour estimer la résistance d'un produit à des attaques de niveau modéré.

Certification BSI :

Il s'agit d'une auto-certification par le fabricant, des produits répondant à la norme BSI (équivalent de l'ANSSI en Allemagne)

Une équivalence existe entre la CSPN (ANSSI) et la certification BSI. Cf site de l'ANSSI : *« Le directeur général de l'ANSSI, et le président du BSI (Bundesamt für Sicherheit in der Informationstechnik), ont signé un accord de reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (Beschleunigte Sicherheitszertifizierung), (…) les certificats valides et publics précédemment délivrés seront reconnus en France comme en Allemagne » (https://www.ssi.gouv.fr/actualite/signature-dun-accord-de-reconnaissance-mutuelle-des-certificats-de-securite-entre-lanssi-et-le-bsi/)*

VII.H. Définitions automates de sécurité

Un automate de sécurité assure deux fonctions en parallèle :

- Contrôle sa propre santé et alerte en cas d'anomalie
- Réaction assurée à un événement

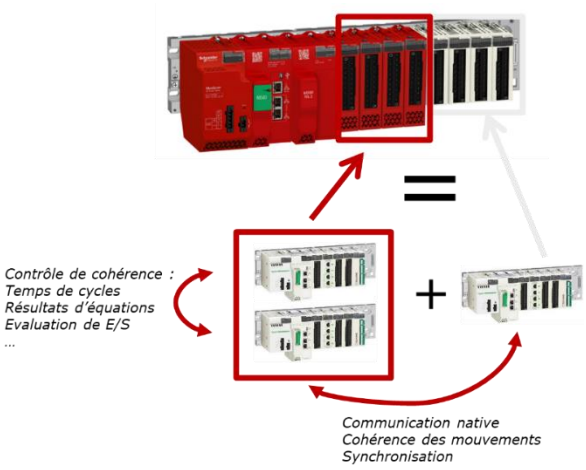


Figure 13 - Fonctions assurées par un automate de sécurité

Dans le cas de l'exemple d'installation ci-dessous :

- Les capteurs, les arrêts d'urgences mais également l'actionneur qui doit agir assurent une réaction sûre.
- Les parties sécurité et process travaillent de concert et garantissent la détection de la moindre anomalie ou événement ainsi que les actions à réaliser.
- Les actions suivantes seront réalisées : coupure d'alimentation pour les portes et action de fermeture si nécessaire, puis coupure d'énergie pour les ventelles.

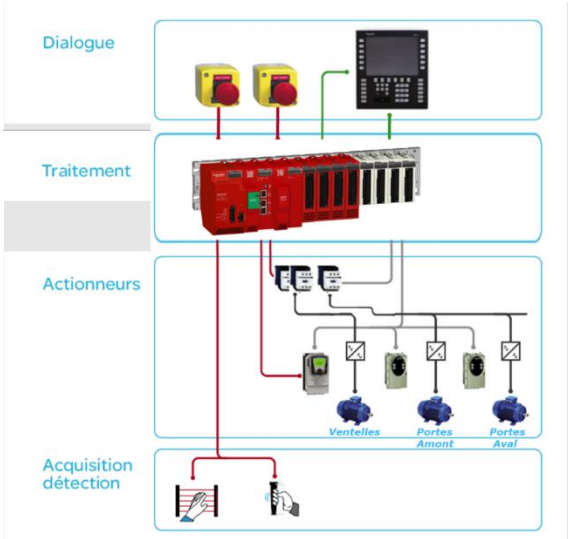


Figure 14 - Exemple d'installation possible

Entrée : La coupure de fil de raccordement, les courts-circuits dans le ou les câbles de liaison (dont ceux entre deux entrées), la mise à la masse des deux entrées, les défauts internes à l'organe de service d'arrêt d'urgence provoquent, en toute circonstance, une réaction sûre.

ATTENTION :

- **Signaux sensibles aux longueurs de câbles (solution E/S déportées avec réseau safe type ASI ou Ethernet)**
- **Capteurs parfois incompatibles**

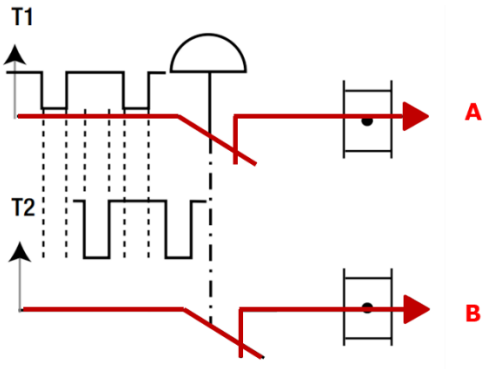


Figure 15 - Entrée de sécurité avec détection de coupure

Sortie : Les sorties ne sont pas très différentes de celles d'un automate « normal ». Il s'agit ici de bien vérifier leur fonctionnement, donc de lier les récepteurs (ici les contacteurs) à un retour d'état, afin que, en toute circonstance, le système ait une réaction sûre par détection d'une discordance.

La documentation du fabricant fait foi et indique comment câbler les capteurs et actionneurs en fonction du niveau de SIL souhaité.

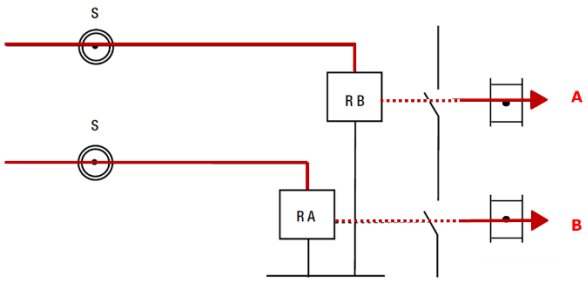


Figure 16 - Sortie de sécurité

Le **bouton d'Arrêt d'urgence** (« bouton rouge ») est un signal qui déclenche une réaction de sécurité qui peut être selon les cas :

- Une coupure d'énergie

Et / ou

- Une action sur les équipements pour réduire les conséquences d'un événement (stopper les mouvements d'eau en fait partie mais pas que, cela peut être aussi un mouvement arrière des portes pour libérer un objet coincé etc…)

VII.I. Recommandation SIL - règles de conception et de codage

Tableau B.1 – Règles de conception et de codage

(Référencées dans le Tableau A.4)

	Technique/Mesure*	réf.	SIL 1	SIL 2	SIL 3	SIL 4
1	Utilisation de règles de codage pour réduire la probabilité d'erreurs	C.2.6.2	HR	HR	HR	HR
2	Pas d'objets dynamiques	C.2.6.3	R	HR	HR	HR
3a	Pas de variables dynamiques	C.2.6.3	---	R	HR	HR
3b	Contrôle en ligne pendant la création de variables dynamiques	C.2.6.4	---	R	HR	HR
4	Utilisation limitée des interruptions	C.2.6.5	R	R	HR	HR
5	Utilisation limitée des pointeurs	C.2.6.6	---	R	HR	HR
6	Utilisation limitée de la récursion	C.2.6.7	---	R	HR	HR
7	Pas de branchements inconditionnels dans les programmes en langages de haut niveau	C.2.6.2	R	HR	HR	HR
8	Pas de conversion de type automatique	C.2.6.2	R	HR	HR	HR

NOTE 1 Mesures 2, 3a et 5. L'utilisation d'objets dynamiques (par exemple, sur la pile d'exécution (stack) ou sur un tas) peut imposer des exigences sur la mémoire disponible et également sur la durée d'exécution. L'application des mesures 2, 3a et 5 n'est pas nécessaire en cas d'utilisation d'un compilateur qui assure a) qu'un espace mémoire suffisant est alloué avant exécution à tous les objets et variables dynamiques, ou qui garantit, en cas d'erreur d'allocation de mémoire, qu'un état de sécurité est obtenu; b) que les temps de réponse satisfont aux exigences.

NOTE 2 Voir Tableau C.11.

NOTE 3 Les références (informatives et non pas normatives) "B.x.x.x", "C.x.x.x" dans la colonne 3 (réf.) désignent des descriptions détaillées de techniques/mesures données dans les Annexes B et C de la CEI 61508-7.

* Les techniques/mesures appropriées doivent être sélectionnées en fonction du niveau d'intégrité de sécurité. Des techniques/mesures équivalentes ou de remplacement sont indiquées à l'aide d'une lettre placée à la suite du numéro. Il convient de satisfaire normalement à une seule des techniques/mesures équivalentes ou de remplacement. Il convient de justifier la sélection d'une technique de remplacement conformément aux propriétés, spécifiées à l'Annexe C, souhaitées pour l'application particulière.

HR	la technique ou mesure est hautement recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure n'est pas utilisée, il convient alors de justifier ce fait avec référence à l'Annexe C pendant la planification de sécurité et après accord de l'évaluateur.
R	la technique ou mesure est recommandée pour ce niveau d'intégrité de sécurité. Il s'agit d'une recommandation de niveau moins élevé qu'une recommandation HR.
---	l'utilisation de la technique ou mesure n'est ni recommandée ni déconseillée.
NR	la technique ou mesure n'est absolument pas recommandée pour ce niveau d'intégrité de sécurité. Si cette technique ou mesure est utilisée, il convient alors de justifier ce fait avec référence à l'Annexe C pendant la planification de sécurité et après accord de l'évaluateur.

VII.K. Affectation dynamique des AU : diagrammes d'interactions

L'objectif du standard est de définir une architecture et un processus qui permette, dans le respect des règles de sécurité, la téléconduite et l'arrêt d'urgence à distance d'un sas d'une EGG téléconduite depuis le demi-pupitre de l'opérateur

Les matériels standards sont :

- 1 seul automate (process + sécurité) par sas d'écluse ; si un site d'écluses à 2 sas alors 2 automates indépendants pour faire fonctionner le site
- 1 seul automate (process + sécurité) par PCC
- Il est obligatoire que l'automate du site et du PCC soient de marque identique
- Les autres parties d'ouvrages (barrage, passe à poisson, …) ne font pas partie du présent standard

Les pupitres banalisés utilisés en PCC sont ceux définis par la DSIN. Ils sont tous identiques quelque-soit le rôle de l'agent (opérateur téléconduite, opérateur réarmement ou chef de salle), l'affectation dynamique des pupitres permet d'apporter de la souplesse dans la gestion de la salle d'exploitation

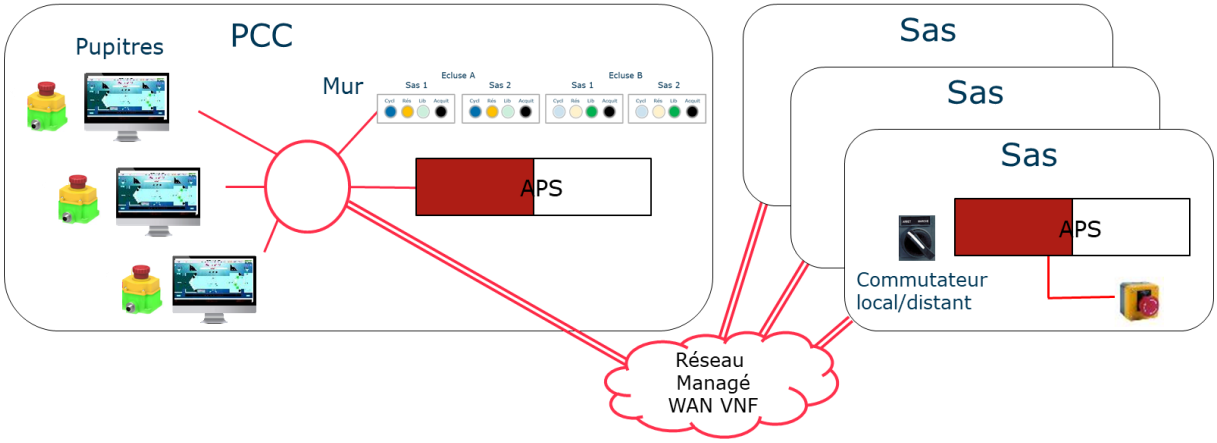


Figure 17 - Schéma de principe communication PCC/Sas

Les propositions ci-après n'ont pas valeur de standard et ne peuvent être mise en place avant d'avoir été certifiée par un organisme extérieur habilité. Cette certification sera engagée par la DSIN en 2023.

En théorie, tous les mécanismes de réservation/affectation/désaffectation/libération doivent être câblés physiquement sur des entrées Safety – en SIL2 - dans la mesure ou les informations correspondantes font partie de la chaine d'affectation dynamique des AU pour laquelle une certification SIL2 est visée. Cependant, il est possible - mais non recommandé - en SIL2 d'avoir une information non sécurisée dans la chaine tant que les bonnes vérifications sont en en place. **Dans le process envisagé, l'action d'affectation d'un sas à un demi-pupitre sera faite dans le SCADA** (variable non Safety) sous réserve de validation d'un organisme certifiant.

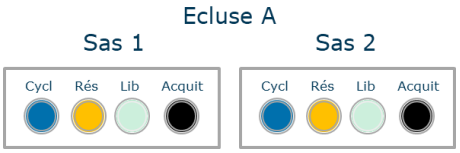
Note pour la spécification à établir : Il faudra également le moment venu, faire la liste détaillée des informations Safety qui doivent faire l'objet des échanges entre le contrôleur PCC et le contrôleur sas, de prime abord on pourrait avoir (cette liste n'est pas exhaustive il faudra creuser) :
* la position de l'AU du pupitre sélectionné
* la demande d'affectation du contrôleur PCC
* la confirmation de la demande d'affectation par le contrôleur de sas
* la position de l'écluse (mode local ou distant)
* information maintenance du contrôleur PCC

Concernant l'information maintenance du contrôleur PCC : lors du passage en Stop du contrôleur PCC (intervention de maintenance, rechargement du programme Safety,..) toutes les liaisons de communication Safety vont tomber. Vu qu'il a été décidé de mettre en sécurité les écluses (cycle arrêt d'urgence) en cas de perte de communication avec le PCC, les contrôleurs de Sas risquent d'enclencher une séquence intempestive

d'arrêt d'urgence à chaque passage en stop du contrôleur du PCC.
Pour éviter ce problème il faudrait prévoir de transmettre une info TOR Safety aux contrôleurs de Sas (bouton tournant dans armoire automate PCC accessible aux seules personnes autorisées), lors des opérations qui nécessitent le passage en stop de l'automate du PCC.

Mode opératoire de l'attribution des sas aux pupitres :

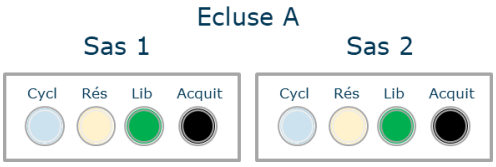
1. A l'**ouverture du PCC** le chef de salle **appaire** physiquement au mur de boutons chaque **sas** d'écluses au **PCC** (bouton orange)



2. Tout au long de son quart, le chef de salle **attribue dynamiquement** les **sas** aux **pupitres** au travers de la console d'administration des sas (page applicative disponible sur un des écrans du chef de salle)
3. Quand un sas est attribué alors le voyant vert du BP AU du pupitre s'allume pour indiquer à l'opérateur que la fonction AU est disponible. La vidéo, l'audio et l'IHM sont également affichés sur pupitre en fonction des données de l'API sas
    a. L'API du sas est maître de la donnée, il gère lui-même les informations : N° PCC, N° sas, état fonctionnel du sas, … le PCC vient consommer ses données pour animer les pupitres
    b. Si le BP AU est percuté quand ce dernier est actif alors le sas se met en sécurité et le BP AU s'allume en rouge

Figure 18 - Exemple de BP à voyant lumineux

4. A à la **fermeture du PCC**, le chef opérateur **supprime les attributions** des sas aux pupitres en fonction du trafic de bateaux puis **supprime les appairages** des sas au PCC via le bouton vert physique sur le mur de boutons



VII.K.1. Diagrammes d'interactions entre le PCC et le sas

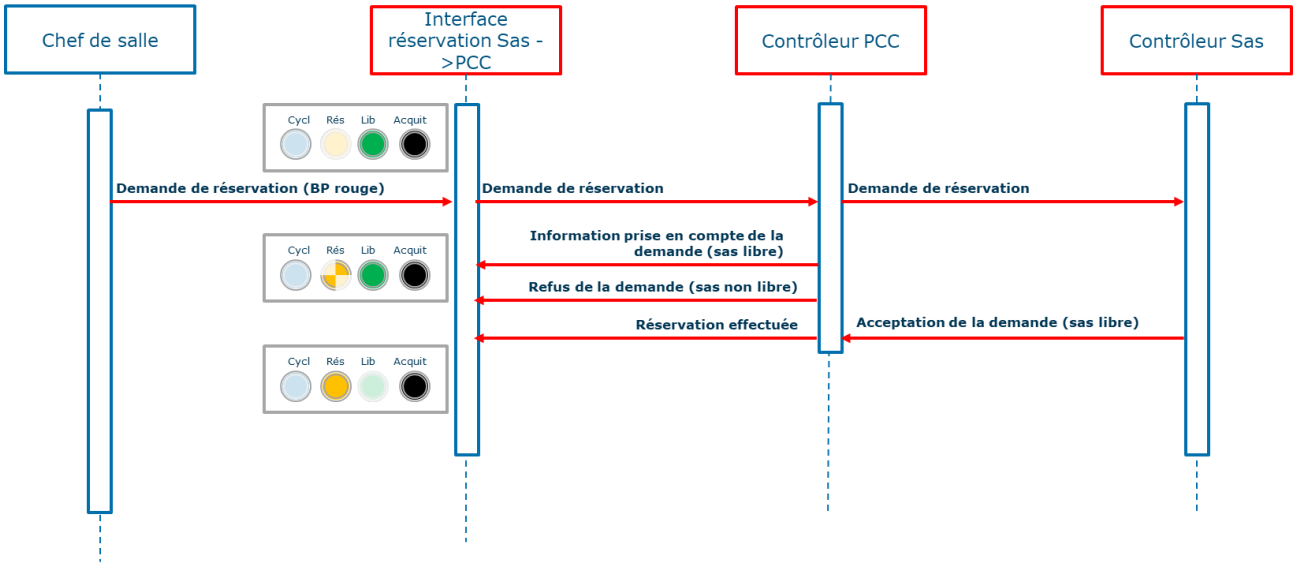


Figure 19 - Réservation Sas vs PCC

Remarque : tous les sas d'une écluse doivent être réservés par le même PCC pour les écluses multi sas.
Le contrôleur PCC doit contacter **individuellement** les 2 ou 3 contrôleurs sas et recevoir 100% de réponses positives pour réserver ou libérer le sas

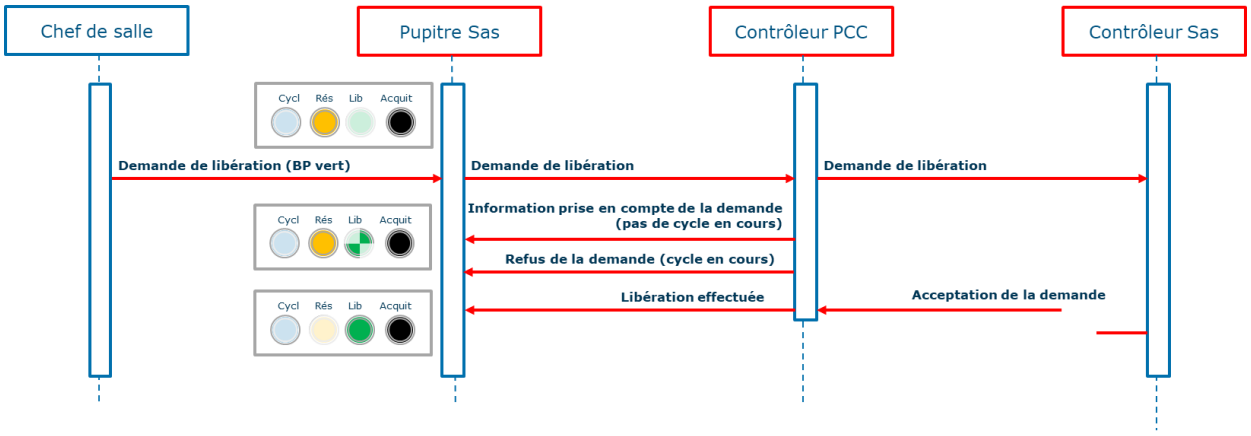


Figure 20 – Libération Sas vs PCC

Remarque : Le contrôleur PCC est en communication permanent avec les contrôleurs des sites, lui permettant de connaitre l 'état et répondre aux demandes

VII.K.2. Diagrammes d'interactions entre le demi-pupitre et le sas

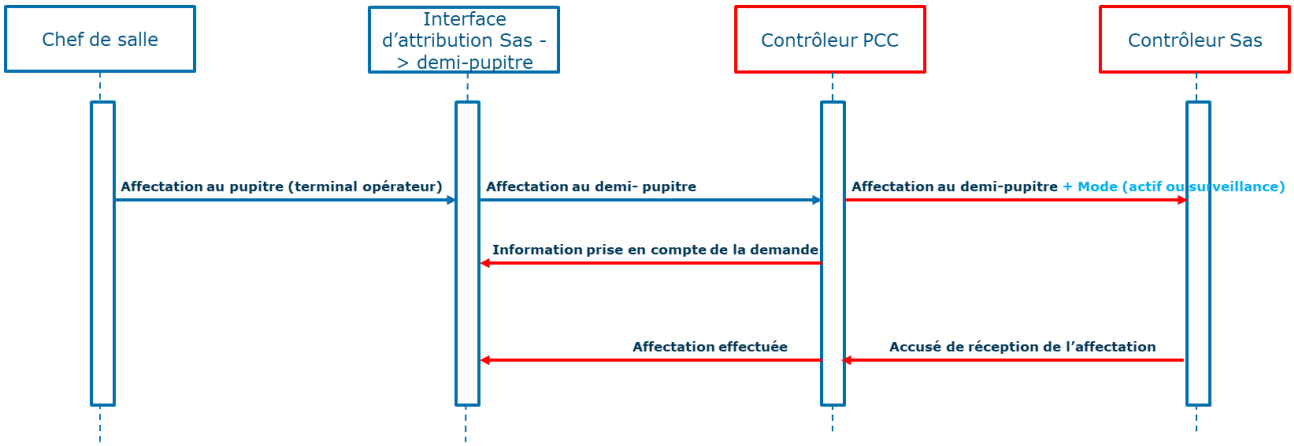


Figure 21 - Affectation Sas vs Poste de Conduite (1/2 – partie AU)

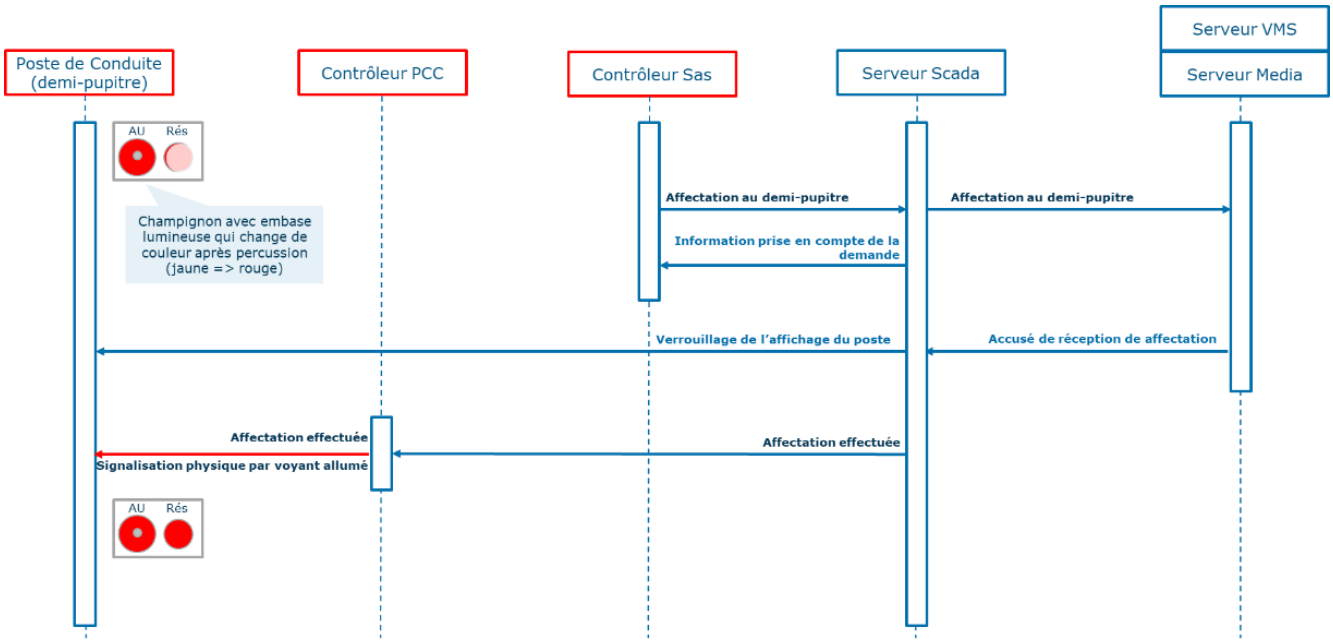


Figure 22 - Affectation Sas vs Poste de Conduite (2/2 - Partie Affichage)

Remarque : Au niveau du pupitre l'opérateur peut travailler sur 1,2 ou 3 sas d'une écluse multi-sas. L'IHM doit vérifier que les autres sas sont libres ou déjà affectés à l'opérateur avant de lancer la demande d'affectation

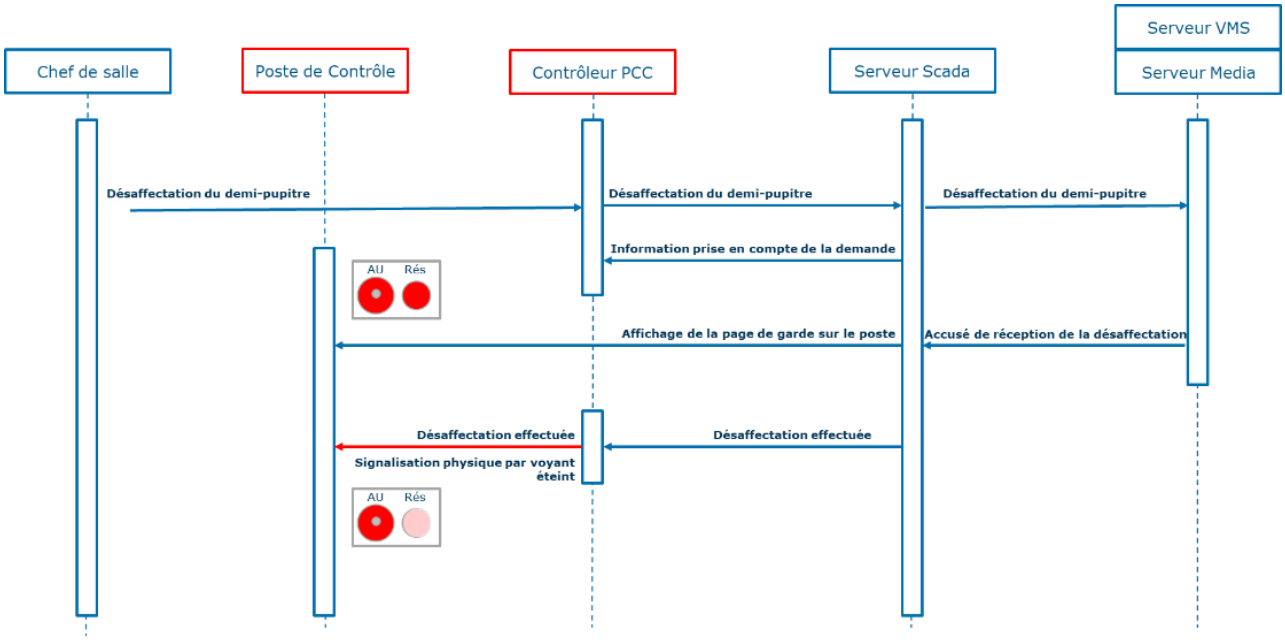


Figure 23 - Désaffectation Sas vs Poste de Conduite (Affichage+AU)

VII.K.3. Glossaire

- **Réservation** : attribution d'un sas d'écluse à un PCC
- **Libération :** arrêt de l'attribution d'un sas d'écluse à un PCC
- **Affectation :** attribution d'un sas d'écluse à un demi-pupitre d'opérateur au PCC
- **Désaffectation :** arrêt de l'attribution d'un sas d'écluse à un demi-pupitre d'opérateur au PCC
- **Demi-pupitre :** poste permettant à l'opérateur de téléconduire un sas
- **Pupitre :** 2 demi-pupitres, permettant à l'opérateur de téléconduire deux sas simultanément
- **Cycle en cours :** lorsqu'un cycle de bassinée est en cours sur le sas. Le sas ne peut être libéré car l'opérateur doit rester en mode actif pour finir de téléconduire
- **Mode Actif :** lorsqu'un opérateur travaille à téléconduire une écluse, ce mode permet d'envoyer des contrôles-commande – le bouton d'arrêt d'urgence est actif.
- **Mode Surveillance :** lorsqu'un opérateur n'est pas en train de téléconduire, celui-ci peut surveiller plusieurs écluses (défilé une à la suite de l'autre) sans possibilité de contrôle-commande ni d'arrêt d'urgence

VII.L. Atelier logiciel

Pour garantir la pérennité des programmes - les automaticiens ayant besoin de divers petits logiciels, il est important de standardiser les ateliers logiciels. Pour cela, il convient de :

- Mettre en place un dépôt partagé (store) avec les logiciels (disponibles rapidement et dans plusieurs versions) nécessaires à la programmation et l'exploitation des automatismes contenant une arborescence du type :
    - Constructeur (Schneider, Siemens, Phoenix Contact, Danfoss…)
        - Logiciel (EcoStruxure, TIA Portal, VLT® Motion Control Tool…)
            - 00_Précédentes
                - Version x.y.z
                - Fichiers d'installation
                - Numéros de licence
                - Procédure d'installation
                - Procédure d'activation
            - 10_Applicable
                - Fichiers d'installation
                - Numéros de licence
                - Procédure d'installation
                - Procédure d'activation
- Mettre en place une gestion des licences centralisée :
    - Automatique si disponible chez le constructeur (serveur de licence)
    - Manuelle sinon :
        - Procédures en cas de crash ou remplacement de PC
        - Traçabilité des installations / activations
- Suivre les compatibilités matériel / logiciel
- Gestion des contrats constructeur (récupération des licences actuelles si possible)

[Action : définir collectivement ce qu'il faut mettre dans le store, pour éviter le 1 besoin = 1 solution (Shadow IT)]

Concernant le transfert des machines intégrateurs vers les machines VNF – un bac à sable (*sandbox pour clé USB à tampon de validation ?)* ou un sas de décontamination doivent être mis en place.

Option alternative : les intégrateurs développent directement depuis les solutions VNF.

VII.M. Structure des programmes

Compte tenu de l'intégration dans les méthodes des principes de l'ISA S88 et des technologies de sécurités il est conseillé de respecter une structure de type fonctionnelle :

- Process
    - Bloc « écluse »
- Phases
    - Blocs « bief »
    - Blocs « équipements X »
    - …
- Opérations
    - Blocs « porte »
    - Blocs « signalisation »
- Actions :

- Blocs actionneurs
- Blocs capteurs

Pour plus de lisibilité, en langage bloc fonctionnel, il est possible de regrouper soit :

- Le process et les phases
- Les phases et les opérations associées

Pour faciliter la standardisation, il est conseillé de conserver les blocs de type Actions à part.

Une étude complémentaire devra être menée pour standardiser les E/S et informations nécessaires au fonctionnement et maintenance.