Octobre 2022

LES CAHIERS DU LAB

VNF – Programme de Modernisation de l'Exploitation –

Atelier du Lab Cybersécurité

STANDARD CYBERSÉCURITÉ

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	**1**

Table des matières

Préambule **4**

Glossaire **5**

1. Introduction **7**

1.1 Périmètre du document 7

1.2 Contexte réglementaire 7

1.3 Contexte des menaces actuelles 7

1.4 Conséquences de l'attaque de 2021 8

2. Mesures applicables immédiatement **9**

2.1 Mesures extraites du PSSI 9

2.2 Gestion des accès physiques 9

2.3 Séparation des PC industriel et bureautique 10

3. Préconisations pour le futur SI **11**

3.1 Actions de renforcement 11

3.2 Nouvelles fonctions 12

3.3 Fonctionnement en mode nominal 12

3.4 Fonctionnement en mode crise 14

4. Approche du risque par typologie de site **15**

5. Annexes **16**

5.1. Mesures cybersécurité à implémenter immédiatement 16

5.2. Approche par le risque : échelle DICT 27

5.3. Autres propositions 28

5.4. Analyse générale des risques et plan d'actions 28

5.4.1. Plan d'action 28

5.4.2. PSSI Opérationnelle (Politique de Sécurité des Systèmes d'Information) 29

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 Cybersécurité** dans le cadre de la modernisation de l'exploitation et de la maintenance d'ici fin 2029.

Il couvre les éléments suivants :

- Définitions et contexte des menaces cybersécurité VNF
- Mesures cybersécurité à appliquer immédiatement
- Organisation efficiente de la Cybersécurité
- Qualification des risque selon l'approche DICT
- Gestion des accès physiques
- Segmentation des PC Indus-bureautique

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

Il est à noter que le standard Cybersécurité rencontre de fortes connexions et interdépendances avec les autres ateliers du Lab.

Les participants de l'Atelier du Lab Réseaux 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 : Dominique ROZIER
Représentant DT NPdC et pilote du groupe : Didier GRAVE
Représentant DT NE : Alexandre KONGS
Représentant DT BS : Alain BONY
Représentant DT RS : Alain BERNARD
Représentant DT CB : Romaric GROS
Représentant DT SO : Renaud MARTIN-DAROCHA
Contributeur DSIN : Sylvain BART
Contributeur DSIN : David MOREL
Contributeur DIEE : Olivier DISSAUX
Contributeur DIMOA : Sébastien PLANTIER
Sponsor : Christophe LALOYER

Glossaire

Abréviation	Signification	Définition
AD	Active Directory	Un service d'annuaire qui fonctionne sur Microsoft Windows Server. Sa fonction principale consiste à permettre aux administrateurs de gérer les permissions et de contrôler l'accès aux ressources du réseau
AQSSI	Autorité Qualifiée pour la Sécurité des Systèmes d'Information	Il s'agit de l'autorité légalement responsable de la sécurité des systèmes d'information dans les administrations, services et établissements publics.
CMDB	Configuration Management DataBase	Une base de données unifiant les composants d'un système informatique. Elle permet d'en comprendre l'organisation et d'en modifier la configuration.
DICT	Disponibilité, Intégrité, Confidentialité, Traçabilité	Ces critères se retrouvent souvent en sécurité des SI, quand il faut identifier et valoriser l'information (en jargon « cartographier les actifs informationnels »), ou quand on veut faire une analyse de risques
GMAO	Gestion de la Maintenance Assistée par Ordinateur	Une méthode / outil de gestion de la maintenance par le biais d'un logiciel permettant de gérer les différentes tâches de maintenance des équipements au sein d'une entreprise
LPM	Loi de Programmation Militaire	Une loi visant à établir une programmation pluriannuelle des dépenses que l'État français consacre à ses forces armées
NIS	Network and Information Security	Cette directive a pour objectif d'atteindre un niveau commun élevé de sécurité des réseaux et des systèmes d'informations dans toute l'Union Européenne
MFA	MultiFactor Authentication	Une méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN
PSO	Plan de Sécurité d'Opérateur	Il s'agit d'un document obligatoire pour les OIV qui décrit l'organisation et la politique de sécurité de l'opérateur.
PSSI	Politique de Sécurité des Systèmes d'Information	Le guide PSSI a pour objectif de fournir un support aux responsables SSI pour élaborer une politique de sécurité du ou des systèmes d'information (PSSI) au sein de leur organisme.
RACI	Réalisateur, Approbateur, Consulté, Informé	La matrice RACI est un outil de communication. Elle permet de visualiser les rôles de chacun dans un projet et donc de répondre aux questions « Qui fait quoi ? »

RSSI	Responsable de la Sécurité des Systèmes d'Information	Le responsable de la sécurité des systèmes d'information définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi.
SIIV	Système d'Information d'Importance Vitale	Ce sont les « systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation »
SOC	Security Operation Center	Le SOC est l'équipe en charge de contrôler et d'analyser régulièrement le dispositif de sécurité de l'entreprise.
VPN	Virtual Private Network	C'est un service qui achemine le trafic web de l'internaute vers un serveur distant sécurisé avant de le rediriger vers la requête initiale (site web, applications…)
XDR	eXtended managed Detection and Response	Une solution qui collecte et met automatiquement en corrélation des données sur plusieurs couches de sécurité (email, Endpoint, serveur, charge de travail sur le Cloud et réseau). Cela permet une détection plus rapide des menaces ainsi qu'une amélioration des temps d'enquête et de réponse lors de l'analyse de sécurité

1. Introduction

La mise en œuvre des mesures techniques et organisationnelles préconisées dans ce document a pour objectif de limiter l'impact d'un incident de sécurité touchant l'établissement (accès frauduleux, code malveillant, etc.).

Ces mesures doivent être présentées, comprises et intégrées par l'ensemble des collaborateurs de VNF, elles s'appliquent à toutes les utilisations de systèmes informatisés, à la fois dans les domaines bureautiques et industriels.

1.1 Périmètre du document

Ce document présente le contexte de la cybersécurité et les mesures à appliquer au moment de sa rédaction.

Son contenu et sa portée peuvent évoluer dans le temps en fonction de l'évolution des menaces et des technologies. **Ce document doit faire l'objet d'une amélioration continue** tant qu'il reste applicable. Il doit être complètement remplacer à long terme par le document de la PSSI.

1.2 Contexte réglementaire

- La **Loi de Programmation Militaire (LPM)** est un plan stratégique voté tous les 5 ans qui impose des règles de sécurité très contraignantes. En tant que fournisseur d'installations jugées indispensables pour la survie de la Nation, VNF a été désigné opérateur d'importance vitale **(OIV)** en 2008 et entre donc depuis cette date dans le champ d'application de cette loi.

  A ce titre, VNF doit assurer la conformité de ses systèmes d'information critiques **(SIIV)** par la mise en œuvre de mesures de sécurité spécifiques et contraignantes.

- Un **SIIV** est un système pour lequel l'**atteinte à la sécurité ou au fonctionnement** risquerait de diminuer d'une façon importante le **potentiel économique, la sécurité** ou pourrait présenter un **danger grave pour la population**.
- **Une attention est à porter aux réglementations futures**, nationales et européennes : risque de règles encore plus contraignantes (directive NIS : Network and Information Security, décret de 2018).

1.3 Contexte des menaces actuelles

L'Internet a révolutionné la façon de travailler mais il a aussi permis l'émergence de nouvelles menaces : les cyber-attaques.

Ces attaques sont de plus en plus fréquentes et communes, et peuvent avoir des impacts désastreux sur les entreprises et les organismes. L'augmentation de la fréquence de ces attaques est due à de nombreux facteurs :

1. L'Internet permet de lancer et synchroniser des attaques depuis partout dans le monde ;
2. L'augmentation du nombre d'appareils connectés augmente la probabilité de découvrir des failles dans les systèmes ;
3. La confiance dans l'outil informatique ainsi que le manque de sensibilisation des utilisateurs ralentissent la mise en œuvre des règles fondamentales de cybersécurité.

L'exposition médiatique d'évènements, notamment les J.O. de Paris en 2024, ou encore l'augmentation des conséquences du réchauffement climatique (phénomènes tels que la raréfaction de l'eau) font de VNF une cible privilégiée pour tout organisme souhaitant nuire à la France.

Ces attaques sont de différents types avec des impacts et conséquences spécifiques :

- Les ransomwares ou rançongiciels bloquent l'accès à des données vitales jusqu'au versement d'une rançon ;
- L'espionnage industriel, dans lequel des outils sont déployés sur le réseau pour accéder et transmettre des données confidentielles voire vitales ;
- Le blocage ou la destruction de systèmes permet d'empêcher le bon fonctionnement d'un système dans le but de nuire à une entreprise, un organisme ou un état.

Toutes ces attaques se basent sur des combinaisons de nombreuses techniques (attaque par déni de service, attaque Man in the Middle, hameçonnage, cassage de mots de passe, élévation de privilèges, injections SQL, ...) dont il faut savoir se protéger.

Exemples de cyberattaques récentes :

- 2017 : ransomware WannaCry dans l'usine Renault de Douai bloquant toute la production pendant une semaine pour un coût estimé à 140 millions d'euros ;
- 2018 : attaque sur le ministère des affaires étrangères via la messagerie électronique afin de dérober des listes de contacts ;
- 2022 : sabotage des câbles de liaison radio visant à bloquer le trafic ferroviaire dans le nord de l'Allemagne.

1.4 Conséquences de l'attaque de 2021

En 2021 le réseau VNF a subi une cyberattaque. Les analyses ont démontré qu'il s'agissait d'une attaque étatique et opportuniste. Bien qu'il n'y eût pas de volonté de nuire, les conséquences ont été nombreuses :

- 380 jours de charge interne pour l'analyse et la remédiation ;
- Investissements de plus de 350 k€ pour le projet de remédiation (hors matériels et prestations d'installation) ;
- Déploiements de nouveaux services de sécurité pour un coût annuel de 120 k€ ;
- Décalage de nombreux projets.

Les mesures suivantes ont depuis été mises en œuvre :

- Déploiement d'un XDR sur environ 5000 assets ;
- Mise en œuvre d'un Micro-SOC pour le traitement des alertes XDR ;
- Déploiement du MFA sur l'ensemble des accès VPN ;
- Mise en œuvre d'un modèle d'administration de type « Tiering » (hiérarchisation des données en fonction de leur importance) ;
- Revue complète des procédures d'administration.

2. Mesures applicables immédiatement

Ce document vise à définir des mesures techniques et organisationnelles pour le SI à venir. Mais le contexte actuel impose la mise en œuvre d'une partie de ces mesures dès que possible afin d'augmenter le niveau de protection du SI actuel.

2.1 Mesures extraites du PSSI

Des mesures primordiales ont été extraites du document de la PSSI, elles sont applicables immédiatement. Elles sont listées en annexe de ce document.

2.2 Gestion des accès physiques

En 2018, une analyse de risque effectuée par le cabinet Wavestone a indiqué la nécessité de lancer un chantier de restriction et de contrôle d'accès physique aux locaux abritant des équipements supports du SI industriel. Ces actifs doivent être protégés physiquement contre l'intrusion, les malveillances, le dommage, la perte accidentelle, etc.

Des mesures de contrôle d'accès physique doivent être mises en œuvre pour protéger les équipements sensibles contre les accès non autorisés.

Attention : la gestion des accès physique de point de vue cyber n'est que complémentaire de la mise en place des basiques de la sureté : sécurisation des ouvertures, des câbles, etc.

Pour cela, l'approche suivie pour cette gestion physique est la suivante :

1. Définir le niveau de protection physique nécessaire.
2. Définir le niveau de traçabilité requis.
3. Déduction du type de contrôle d'accès physique à mettre en place. Le choix de la technologie de restriction d'accès physique dépend des exigences de sécurité liées à la criticité d'ouvrage.

Criticité	Exemples	Niveau de protection	Niveau de Traçabilité	Types d'accès
Critique	PCC, EGG, EPG fort trafic, Autres ouvrages fort trafic (tunnel, pont mobile, etc.), Barrages critiques (classe A).	**Fort** (Accès et armoires fermées)	Traçabilité obligatoire	**A la cible :** Contrôle d'accès sur entrée site, et sur armoires / équipements **Transitoire :** Contrôle d'accès sur entrée site, clé ou digicode sur armoires et équipements
Non-critique	EPG, Autres ouvrages faible trafic		Inventaire des clés mais pas de traçabilité des accès	Clé, digicode

	(tunnel, pont mobile, etc.), Déversoirs, Barrages non critiques (classe B).			

Clés :

- Il est important de tenir un inventaire de clés avec une gestion des entrées/sorties ;
- Au-delà des portes, toutes les ouvertures doivent être sécurisées, via barreaudage des fenêtres notamment ;
- Certains équipements installés chez des hébergeurs utilisent des serrures et cadenas utilisant des clefs type "Locken" pour la gestion des accès physiques. Ce type de clé est compliqué à mettre en œuvre pour un nombre important d'ouvrages du fait de la logistique imposée par sa gestion.

Badges :

- L'implémentation du badge sur l'ensemble des ouvrages connectés au réseau nécessite du temps et des moyens conséquents ;
- Les PCC, les nouveaux bâtiments et les bâtiments rénovés seront les premiers à être dotés d'un contrôle d'accès par badge ;
- Un marché national pour le contrôle d'accès doit être lancé ;
- Dans le cas de perte de d'alimentation électrique, le contrôle d'accès par badge continue de fonctionner grâce à sa batterie de secours permettant ainsi l'accès et le traçage aux sites.

2.3 Séparation des PC industriel et bureautique

Le réseau global de VNF est segmenté logiquement en deux sous-réseaux indépendants : le réseau industriel et le réseau bureautique.

Un PC configuré pour se connecter sur le réseau industriel (i.e. configuré avec les applications d'exploitation) ne doit pas pouvoir se connecter sur le réseau bureautique.

De la même façon un PC configuré pour le réseau bureautique (i.e. disposant de la boîte mail, des navigateurs web et des applications non directement liées à l'exploitation) ne doit pas pouvoir se connecter sur le réseau industriel.

Certains postes (opérateurs, mainteneurs, …) nécessiteront l'utilisation simultanée de 2 PC distincts : un pour l'industriel et l'autre pour la bureautique.

3. Préconisations pour le futur SI

3.1 Actions de renforcement

Au regard de l'état des lieux de la menace cyber touchant l'ensemble des acteurs privés et publics en France, VNF doit impérativement renforcer la prise en compte et l'application des mesures de sécurité, en particulier sur les systèmes en charge de l'exploitation, plus communément nommés "informatique industrielle".

Ce résultat ne peut être atteint qu'en appliquant strictement les préconisations de sécurité de ce document, et en faisant en sorte que ces mesures soient portées et acceptées par l'ensemble des acteurs de VNF, de la direction générale jusqu'à l'agent d'exploitation.

Définir les responsabilités	**Former les acteurs**	**Réaliser un inventaire**	**Tracer la mise en application**
Objectif : s'assurer que la prise de décisions et la réalisation d'actions soient faites par les bonnes personnes au bon moment	**Objectif :** faciliter l'acceptation des mesures cybersécurité	**Objectif :** améliorer le suivi des connexions sur le réseau VNF	**Objectif :** s'assurer de la mise en œuvre des mesures cybersécurité
▪ Construction d'un RACI des actions de cybersécurité entre les différents acteurs (DSIN, AQSSI, RSSI, DT, exploitants, …) ▪ Mise en place des nouvelles fonctions Cybersécurité au siège et en DT	▪ Formation initiale à la cybersécurité ▪ Mise à niveau et rappels annuels ▪ Harmonisation des pratiques ▪ Mise à disposition des manuels, guides et outils	▪ Mise en place d'une CMDB commune indus/gestion, interconnectée avec la GMAO ▪ Mise à jour des assets ▪ Mise à jour de l'inventaire, incluant les entrées et sorties de toutes machines ayant une IP, y compris les machines isolées ▪ Respect des règles lors de la connexion d'une machine au réseau	• Contrôles continus, audits, tests d'intrusions, analyse de risques et interventions sur site • Veille de la réglementation • Matrice de traçabilité pour le suivi de la mise en œuvre des règles • Adaptation des règles si nécessaire • A plus long terme : challenges/certifications internes (norme ISO 27000 - SMSI)

En cybersécurité la connaissance complète du parc informatique est primordiale. Le cycle de vie complet du matériel (ajout, mise-à-jour, suppression) est de la responsabilité du gestionnaire de parc au siège ou en DT. Selon les cas, il peut s'agir de la DSIN, de la DIEE, d'un responsable local en DT, etc. Le gestionnaire de parc est aussi responsable de la mise à jour de l'inventaire de son parc.

3.2 Nouvelles fonctions

La définition des responsabilités cybersécurité constitue une étape importante dans la sécurisation des SI de l'entreprise face aux différentes menaces qu'elle affronte aujourd'hui. Il s'agit d'avoir une idée claire sur les rôles et responsabilités de chaque entité impliquée dans la gouvernance cybersécurité.

Les travaux réalisés dans le cadre de l'atelier cyber ont conclu de l'intérêt de nouvelles fonctions clés :

- Un pôle expertise « central », rattaché au siège, dans un rôle **d'acteur et prescripteur** ;
- Un animateur de communauté cyber, rattaché au siège, dans un rôle **d'acteur et d'animateur** ;
- Une communauté de **correspondants terrain** regroupant à minima un **profil métier indus et un profil SI**, en DT, pour avoir à la fois une vision transverse au sein de cette direction mais aussi une vision d'échange avec les prescriptions qui arrive du central, dans un rôle de **contributeur et d'animateur** ;
- Des acteurs terrain (mainteneur, informaticien…), au sein de chaque DT, dans un rôle de **contributeur et de mise en œuvre des bonnes pratiques cyber**.

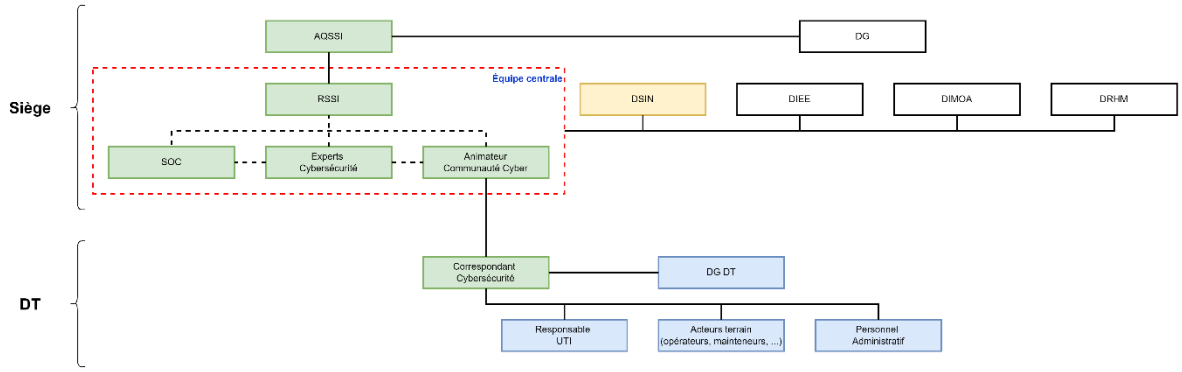


Figure 1 : nouvelle organisation cybersécurité

La recommandation est d'avoir des ressources internes VNF, formées et capables d'occuper le rôle d'experts cybersécurité dans la nouvelle organisation mais il reste possible de recruter des ressources externes compte tenu de la complexité du rôle (nécessite la compréhension des menaces et les techniques de défense).

Les acteurs de l'organisation présentés dans le précédent chapitre ont des rôles divers et variés concernant la cybersécurité. La définition du périmètre de chaque acteur est essentielle Le paragraphe ci-après présente d'une manière détaillée ces rôles et responsabilités.

Une modification des fiches de postes des acteurs terrain pour intégrer les dimensions cyber est nécessaire étant donné qu'aucun nouveau poste terrain ne sera créé.

3.3 Fonctionnement en mode nominal

Acteurs		Responsabilités	Charge
	AQSSI	▪ Porte la responsabilité légale	Partie intégrante du poste DG adjoint
	RSSI	▪ Gère le pôle d'expertise central ▪ Pousse les chartes utilisateur via la DRHM ▪ Effectue un état des lieux annuel	1 ETP

Pôle expertise central		▪ Définit, en lien avec les experts et animateurs, les modules de sensibilisation et de formation ▪ Met en place les certifications et habilitations à destination des administrateurs.	
	Experts cyber	▪ Définissent avec l'animateur les points d'attention ▪ Procèdent aux tests et audits ▪ Effectuent des visites de conformité sur le terrain ▪ Réalisent une veille technique et réglementaire ▪ Appliquent toutes les mesures nécessaires à la résolution d'un incident au niveau national.	3 ETP (continuité)
	Animateur de communauté	▪ Fait le lien avec les correspondants terrains ▪ Anime et informe la direction et les DT	1 ETP
	SOC (Security Operations Center)	▪ Surveille activement les SI ▪ Analyse les logs	Partie intégrante du poste
Correspondants terrain		▪ S'assurent de l'application de la PSSI sur le terrain ▪ Remontent les problématiques ▪ Transmettent les inventaires ▪ Sensibilisent tous les acteurs terrain	Dépendant du nombre d'ouvrage 1 ETP de charge répartie sur 2 personnes
Acteurs terrains - UTI		▪ Appliquent les consignes liées à la cybersécurité ▪ Appliquent les règles définies par la PSSI ▪ Sont à jour de leurs formations, certifications et habilitations liées à la cybersécurité	Partie intégrante du poste
DRHM		▪ Met à disposition les modules de formation et de certification obligatoires ▪ Effectue le suivi des formations et certifications des collaborateurs	Partie intégrante du poste

3.4 Fonctionnement en mode crise

Le standard de l'atelier « Réseaux » a établi une méthodologie de traitement des incidents en fonction de leur criticité et de leur ampleur. Elle a pour but de déterminer la chaîne de réaction précise à mettre en place pour résoudre un incident ; elle définit une chronologie d'actions à réaliser au bon moment par des acteurs identifiés, de la détection du problème jusqu'à sa résolution. 4 niveaux d'ampleur et de criticité sont définis, aboutissant à l'identification de 16 scénarios types avec leurs chaînes de réaction associées.

Cette méthodologie doit être appliquée également aux incidents de cybersécurité afin de garantir l'intervention des bons acteurs aux bons moments via l'application d'un processus connu et maîtrisé.

Ces scénarios et chaînes de réaction associées sont définis dans le document de la PSO et sont peut-être à préciser.

4. Approche du risque par typologie de site

Certains éléments de ce premier standard cybersécurité, notamment l'analyse de risques, seront complétés ultérieurement dans le cadre d'une mission avec un cabinet d'expertise en cybersécurité.

Cette approche par le risque a uniquement valeur de proposition en l'état présent. Elle sera utilisée pour prioriser le déploiement de mesures de cybersécurité par typologie de site et alimenter l'étude de risques détaillée par typologie d'ouvrage qui sera faite par Wavestone en 2023.

Les critères DICT sont des indicateurs de sécurité informatique standard qui permettent d'évaluer les besoins de sécurité associés à une ressource/application donnée.

Typologie de site	Criticité	Exemples	Disponibilité	Intégrité	Confidentialité	Traçabilité
			Note	**Note**	**Note**	**Note**
Gestion de trafic	Critique	PCC, Ecluses téléconduites, autres ouvrages fort trafic (pont mobile, etc.), tunnels longs	3 Tenir compte mode dégradés et impact orga PCC	2 Contrôle-commande Automates	2 CDE, données usagers, données AIS	1
	Non-critique	Écluses RAD et autres ouvrages faible trafic (pont mobile, etc.), tunnels courts	0	1 Doit être capable de détecter modifications	2	1
Ouvrage GH	Critique	PCC, Barrages classe A/critiques, barrages soumis à arrêtés	3 Besoin de réaction rapide	2 Information hauteur barrage à impact. Pas toujours de caméras	2 Certaines données publiques (AGHYRE)	1 Pas d'obligation à stocker
	Non-critique	Déversoirs, Barrages classe B/moins critiques, capteurs GH (non lié au trafic)	0	1	2 Certaines données publiques (AGHYRE)	1

Remarques complémentaires :

- **Disponibilité** : Le fonctionnement en mode dégradé doit être pris en compte dans l'estimation de la disponibilité de l'ouvrage. La notation donnée pour la disponibilité des ouvrages tient compte du fait que VNF s'engage auprès des organismes à ce que certains ne soient pas indisponibles pour une durée fixée par des réglementations.
- **Traçabilité** : Il est important de faire la différence entre une sauvegarde des données et une journalisation d'évènements qui constitue un réel intérêt pour les investigations et les analyses statistiques. De ce fait, une précision du périmètre à l'accès à ces données doit être faite.

5. Annexes

5.1. Mesures cybersécurité à implémenter immédiatement

Catégorisation des sites				Responsabilité DT	Responsabilité siège
Organisation de la cybersécurité des systèmes d' information industriels	Prise en compte de la SSII dans les projets (début ou évolution)	ORG-5	Une évaluation du niveau de sensibilité et une analyse de risques et de l'identification de mesures de traitement des risques doivent être réalisées	✓	✓
	Prise en compte de la SSII dans la maintenance	ORG-11	Les plans de maintenance des installations des sites doivent intégrer la maintenance des systèmes d'information industriels associés.	✓	×
	Prise en compte de la SSII dans la sous-traitance	ORG-15	Les prestations externalisées au sein de chaque DT et de chaque UTI doivent être identifiées.	✓	×
		ORG-16	Les clauses de sécurité industrielle types doivent être listées et intégrées dans les contrats de sous-traitance.	✓	×
		ORG-19	Les échanges d'information avec des organisations externes dans le cadre de la sous-traitance doivent être contrôlés.	✓	✓
	Prise en compte de la SSII dans les appels d'offres	ORG-20	Le cahier des charges doit intégrer des exigences de cybersécurité a minima pour respecter la présente politique.	✓	✓
	Prise en compte de la SSII dans les contrats de fournisseurs VNF	ORG-27	Les contrats de fournisseurs doivent intégrer les exigences de sécurité des SI Industriels de la présente politique opérationnelle.	✓	✓

	Suivi permanent de la sécurité	ORG-37	Des reportings doivent être formalisés régulièrement (au minimum trimestriellement) par chaque DT afin de suivre le niveau de la sécurité des Systèmes d'Information Industriels SSII	✓	×
		ORG-38	Un reporting global de la SSII doit être formalisé régulièrement (au minimum trimestriellement) afin de suivre le niveau de sécurité sur ces systèmes.	×	✓
Organisation de la cybersécurité des systèmes	Cartographie des installations	GAC-1	Les équipements SI industriels de VNF doivent être clairement identifiés et un inventaire doit être établi et tenu à jour en permanence. Il doit en particulier permettre de gérer et d'anticiper l'obsolescence.	✓	✓
		GAC-4	L'inventaire du parc, la cartographie et la documentation doivent être mises à jour à chaque modification de l'installation.	✓	✓
	Gestion des intervenants internes et externes	CSR-5	L'intervention de tout individu externe doit être au préalable notifiée à la direction territoriale concernée.	✓	×
		CSR-7	Un processus de gestion des compétences doit être mis en place afin de s'assurer que les intervenants disposent des compétences nécessaires pour leurs missions. Ce processus doit intégrer le transfert de compétences en cas de départ ou de changement de poste des personnes en charge des systèmes.	×	✓
		CSR-8	Une revue régulière des intervenants et de leurs comptes doit être effectuée, au minimum une fois par an.	✓	×
		CSR-9	Les responsabilités en termes de sécurité doivent être formalisées dans la fiche de poste de chaque agent.	×	✓

		CSR-10	Une charte d'utilisation des systèmes d'information industriels doit être formalisée et inclure les sanctions disciplinaires encourues pour traiter le cas des infractions à la sécurité de ces systèmes. Cette charte doit être signée par tout nouvel arrivant (internes ou tierces parties).	×	✓
		CSR-11	En cas de départ, les habilitations et les droits d'accès du personnel sortant (internes ou tierces parties) doivent être retirés.	×	✓
Contrôle des accès	Contrôle d'accès physique	ACC-1	L'accès physique aux sites abritant les actifs du SI industriel doit être restreint et contrôlé par badge ou clé.	✓	✓
		ACC-2	La gestion quotidienne des clés et des badges doit être assurée par une personne nommée au préalable pour chaque site ou UTI.	✓	✓
		ACC-3	Un inventaire des clés et des badges d'accès doit être réalisé au minimum chaque semestre et en cas de perte, de vol ou de casse pour chaque site ou UTI.	✓	✓
		ACC-6	L'accès en cas d'urgence doit être assuré.	✓	✓
	Compte d'accès utilisateurs ou administrateurs	ACC-8	Chaque utilisateur doit être identifié de manière unique.	×	✓
		ACC-11	Les comptes disposant de privilèges importants, comme les comptes administrateur, doivent être distincts des comptes utilisateurs et ne pas être des comptes par défaut ou génériques.	×	✓
		ACC-14	Une revue annuelle des comptes doit être mise en place.	×	✓
		ACC-15	Une revue semestrielle des comptes administrateurs doit être mise en place.	×	✓

		ACC-19	Les mots de passe utilisés doivent être robustes au regard de ce qui est possible : • Les mots de passe par défaut doivent être changés ; • Les mots de passe ne doivent pas être conservés sur des supports papiers ; • Les mots de passe ne doivent pas pouvoir être trouvés dans un dictionnaire ; • Si possible, les mots de passe doivent contenir un mélange de caractères alphanumériques et de caractères spéciaux ; • La complexité technique des mots de passe doit être vérifiée.	×	✓
		ACC-20	Les mots de passe doivent faire au moins 10 caractères pour les comptes utilisateurs.	×	✓
		ACC-21	Les mots de passe doivent faire au moins 14 caractères pour les comptes d'administration.	×	✓
		ACC-22	Les mots de passe des comptes utilisateurs doivent être renouvelés tous les ans avec impossibilité d'utiliser les 10 derniers mots de passe.	×	✓
		ACC-23	Les mots de passe des comptes administrateurs doivent être renouvelés tous les 6 mois (3 mois pour les sites sensibles) avec impossibilité d'utiliser les 10 derniers mots de passe.	×	✓
		ACC-24	Les mots de passe sont confidentiels et ne doivent pas être communiqués à des tiers, ni être affichés.	×	✓
		ACC-25	L'échange de mot de passe doit se faire via des protocoles de chiffrement conformes à l'état de l'art. Le login et le mot de passe doivent être communiqués via deux canaux différents.	×	✓

		ACC-26	L'envoi de mots de passe par mail est strictement interdit sauf s'il y a utilisation d'un moyen de chiffrement autorisé.	×	✓
		ACC-27	Un même mot de passe ne doit pas être utilisé sur plusieurs systèmes. En particulier, il est strictement interdit de réutiliser le même mot de passe pour les comptes administrateurs locaux des systèmes (Windows ou autre) : ceux-ci doivent être spécifiques et unique à chaque machine et doivent être générés aléatoirement.	×	✓
		ACC-28	Les mots de passes ou leur empreinte doivent être stockés de façon sécurisée par les mécanismes de chiffrement autorisés pour assurer leur confidentialité et leur intégrité.	×	✓
		ACC-29	Une procédure sécurisée de réinitialisation des mots de passe doit être définie.	×	✓
		ACC-30	Les logiciels et navigateurs doivent être configurés de façon à ne pas mémoriser les données d'authentification.	×	✓
	Gestion des comptes des automates ou génériques	ACC-34	Une personne responsable des comptes des automates ou génériques de chaque site doit être définie.	✓	×
		ACC-35	Les comptes par défaut et génériques doivent être désactivés sauf dérogation (ORG-4). Dans ce cas, leur utilisation devra être limitée à des usages précis, documentés et tracés.	×	✓

		ACC-36	Lorsque cela est possible, les mots de passe doivent faire au moins 16 caractères pour les comptes de services ou en cas de compte génériques après dérogation nécessaire (ORG-4). Ils doivent être générés aléatoirement et différent sur chaque installation avec 3 des 4 catégories de caractères différent (majuscules, minuscules, numériques, caractères spéciaux).	✗	✓
		ACC-37	Chaque mot de passe doit être stocké de manière sécurisée.	✗	✓
		ACC-38	Les comptes des automates ou génériques doivent être revus annuellement.	✓	✗
Cybersécurité des réseaux	Interconnexion avec un fournisseur	CRX-1	Si une interconnexion doit être mise à disposition d'un fournisseur / prestataire, celle-ci devra être conforme à la politique de sécurité de VNF (VPN et authentification multifacteur).	✓	✓
	Sécurisation au sein d'un site	CRX-2	Les systèmes industriels doivent être découpés par zones fonctionnelles ou zones techniques cohérentes. Ces zones doivent être cloisonnées entre elles.	✗	✓

		CRX-3	Une politique de cloisonnement et filtrage entre les zones doit être mise en place. Au minimum : • Un cloisonnement physique doit être privilégié ; • Lorsqu'une séparation physique n'est pas possible, un cloisonnement logique doit être mis en place (par exemple VLAN) ; • Le réseau d'administration des équipements doit être considéré comme une zone distincte du réseau industriel ; • Le réseau de gestion doit être considéré comme une zone distincte du réseau industriel ; • Les connexions internet doivent se faire via des postes de travail cloisonnés physiquement et logiquement du réseau industriel ; • Seuls les flux nécessaires doivent être autorisés.	×	✓
		CRX-7	Le SI Industriel ne peut être connecté au SI de gestion qu'au travers d'au moins un pare-feu.	×	✓
	Sécurisation de l'exposition d'un site	CRX-8	Toute autre interconnexion que celles décrites dans le PSSI est interdite.	✓	✓
		CRX-10	Les automates doivent être isolés d'un point de vue réseau et n'être visibles que du SCADA (Supervisory Control and Data Acquisition), aucune exposition directe sur Internet n'est autorisée.	✓	✓
		CRX-14	Site interconnecté via un filtrage simple qui assure les exigences suivantes : • Limitation flux autorisés au strict minimum et à des flux standard.	✓	✓

	Réseaux sans fil	CRX-16	Avant l'installation d'un réseau sans fil (Wifi, radio…), une étude doit être menée pour déterminer les emplacements et la puissance des bornes afin de limiter l'exposition du réseau.	✓	×
	Télégestion	CRX-20	La téléassistance n'est possible que dans le respect des règles actuellement en vigueur (VPN + MFA + Bastion)	✓	✓
		CRX-22	La télégestion doit se baser sur des protocoles sécurisés avec les mécanismes de chiffrement autorisés.	✓	✓
		CRX-23	Tout intervenant réalisant de la téléassistance doit être authentifié de façon forte.	✓	✓
Cybersécurité opérationnelle	Documentation	CSO-1	La documentation doit être maitrisée pour disposer d'une image exacte des installations afin d'éviter des erreurs d'exploitation.	×	✓
		CSO-2	La diffusion de la documentation doit être maitrisée afin d'assurer sa confidentialité et que seules les personnes ayant besoin des informations soient les destinataires.	×	✓
		CSO-3	Une politique de gestion de la documentation (processus de mise à jour, durée de conservation, liste de diffusion, stockage…) doit être définie et mise en œuvre pour assurer la confidentialité de la documentation sensible.	×	✓
		CSO-4	La documentation relative à un SI industriel ne doit pas être conservée sur le SI industriel lui-même.	×	✓

		CSO-5	Des versions papiers des documents d'exploitation doivent être disponibles afin d'en assurer l'accès en cas d'urgence.	✖	✓
	Gestion des changements	CSO-9	Une procédure de gestion des interventions doit être mise en place afin d'identifier : • L'intervenant et le donneur d'ordre ; • La date et l'heure de l'intervention ; • Le périmètre d'intervention ; • Les actions à réaliser ; • Les équipements concernés, et en cas de retrait ou remplacement, la liste des numéros d'identification ; • Les modifications apportées et leur impact.	✓	✓
	Configuration	CSO-20	Les systèmes d'exploitation de chaque équipement doivent être durcis suivant les recommandations des constructeurs et des éditeurs.	✖	✓
		CSO-21	La gestion de configuration doit limiter la surface d'exposition aux attaques, au minimum, il faut désactiver : • Les comptes par défaut ; • Les ports physiques et équipements radios inutilisés ; • Les supports amovibles ; • Le boot sur un disque externe ; • Les services non indispensables (service web par exemple).	✓	✓
	Protection contre les codes malveillants	CSO-50	Une politique antivirale doit être définie pour se prémunir des attaques par virus.	✖	✓
		CSO-51	Si le poste de travail ou le serveur le permet, la solution de sécurité centralisée doit être déployée	✖	✓

		CSO-53	Tout équipement d'intervention (stations portables, postes de télémaintenance, station d'ingénierie…) doit disposer de la solution de sécurité VNF centralisée	×	✓
		CSO-54	Le processus de livraison de l'ensemble des logiciels, programmes et éléments de configuration ainsi que le processus de livraison de leurs mises à jour doit intégrer un mécanisme de vérification de l'intégrité et de l'authenticité (signature). Les éléments concernés sont en particulier : • Les firmwares ; • Les systèmes d'exploitation et logiciels standards ; • Les progiciels industriels ; • Les programmes d'automates et du Système de contrôle et d'acquisition de données ; • Les fichiers de configuration des équipements réseau.	×	✓
	Gestion des matériels mobiles personnels	CSO-55	La charte d'utilisation des SI doit spécifier les modalités d'utilisation des matériels mobiles.	×	✓
		CSO-56	Les équipements autorisés à se connecter aux systèmes doivent être clairement identifiés et validés.	×	✓
		CSO-58	Un processus d'attribution des matériels mobiles doit être mis en place. Il doit permettre, au minimum : • De valider l'attribution du matériel par le responsable hiérarchique ; • D'assurer la traçabilité entre le matériel et ses utilisateurs ; • De sensibiliser l'utilisateur aux règles d'usage en vigueur.	×	✓

	Gestion des points d'accès réseau	CSO-61	Les points d'accès réseau doivent être clairement identifiés et recensés.	✓	✓
		CSO-62	Les points d'accès réseau non utilisés (commutateurs, hubs, baies de brassage, prises de maintenance sur les bus de terrain, etc.) doivent être désactivés.	✓	✓
	Protection des automates	CSO-74	L'accès aux automates doit être protégé par un mot de passe (ACC-18).	✓	×

5.2. Approche par le risque : échelle DICT

Niveau	Disponibilité	
0	**Limité**	Elle ne gêne pas l'activité : une durée d'indisponibilité supérieure à 24h est acceptable.
1	**Modéré**	Elle perturbe l'activité : une durée d'indisponibilité d'au plus 24 heures mais supérieure à 4h est acceptable.
2	**Important**	Elle nuit à l'activité : une durée d'indisponibilité d'au plus 4 heures mais supérieure à 1h est acceptable.
3	**Majeur**	Elle nuit gravement à l'activité : la durée d'indisponibilité doit rester d'au maximum une heure.

Niveau	Intégrité	
0	**Faible**	Elle ne gêne pas l'activité : les données sont altérables.
1	**Détection**	Elle perturbe l'activité : les altérations doivent être détectées (ex : les données non fiables sont ignorées ou un nouvel import de données est déclenché).
2	**Correction**	Elle nuit à l'activité : les altérations doivent être détectées et corrigées.
3	**Exactitude permanente**	Elle nuit gravement à l'activité : aucune altération n'acceptée.

Niveau	Confidentialité	
0	**Public**	Les données sont publiques ou pourraient être diffusées sans conséquences.
1	**Interne**	Les données sont internes ou réservées à l'administration ou à des partenaires identifiés.
2	**Restreint**	Les données sont sensibles et ne doivent être accessibles que de par les personnes identifiées. Certaines données sont à caractère personnel ordinaires.
3	**Confidentiel**	Les données nécessitent une protection particulière. Certaines données sont à caractère personnel sensibles.

Niveau	Traçabilité	
0	**Faible**	Aucune traçabilité n'est nécessaire.
1	**Détectable**	Seule une traçabilité des connexions est nécessaire.
2	**Imputable**	Toutes ou certaines actions doivent être attribuées à leur auteur, ou certaines actions ou échanges doivent être horodatés.

Niveau	Traçabilité	
3	**Valeur probante**	Toutes les actions ou certaines actions sensibles doivent pouvoir être attribuées sans équivoque à leur auteur. Ce niveau est également retenu lorsque les actions des administrateurs doivent être tracées.

5.3. Autres propositions

- Les modules de formation doivent être mis à jour en les rendant plus attractifs
- Bloquer les clés USB ou les disques durs externes ? borne de décontamination dans le PCC
- Crypter les données sur le disque à l'aide d'un outil type Cryhod primx
- Travailler sur la transparence des utilisateurs en cas de phishing ?
- Utiliser un outil de gestion des mots de passe type Keypass pour augmenter la protection des systèmes
- Cortex (XDR) doit être déployé sur la totalité du parc / systèmes
- Travail à faire de sécurisation des flux de connexion (VPN, partage de connexion, box ADSL…)
- S'assurer d'inventorier les machines « orphelines » car les attaques opportunistes visent les éléments oubliés de l'organisation
- Lister les IP et rechercher les ports ouverts (RDP inclus)
- Mettre en place une newsletter cyber mensuelle ?
- Organiser des demos d'attaques et des conférences pour sensibiliser les directions ?
- Rechercher des abaques de dimensionnements d'autres entreprises ?

5.4. Analyse générale des risques et plan d'actions

5.4.1. Plan d'action

À la suite de l'analyse de risques effectuée par Wavestone en 2018, un plan d'action a été défini. Pour **minimiser** autant que possible **la criticité, les impacts et la probabilité d'occurrence des risques** identifiés, de plan d'action détaille **56 mesures qui ont été construites et qualifiées** selon :

1. **Un classement par chantiers**

   Chantier 01 : Continuité d'activité

   Chantier 02 : Dimensionnement

   Chantier 03 : Gestion de la maintenance, des tests et des mises à jour

   Chantier 04 : Gestion des accès

   Chantier 05 : Gestion des matériels

   Chantier 06 : Gestion des ressources humaines

   Chantier 07 : Gestion des sauvegardes

   Chantier 08 : Gouvernance sécurité

   Chantier 09 : Sécurité des réseaux

Chantier 10 : Sécurité physique

Chantier 11 : Sensibilisation SSI

2. **Le coût** de la mise en œuvre de l'action
3. **La charge** de travail nécessaire à la mise en œuvre de l'action
4. **L'opportunité** que représente l'action. L'opportunité correspond à un ratio Priorité / Coût permettant de déterminer les impacts de la mise en œuvre :
    - Action d'envergure : action coûteuse mais importante
    - Quick Win : action peu coûteuse et importante
    - Action mineure : action peu importante
    - Arbitrage : la mise en œuvre reste à décider en fonction des bénéfices par rapport aux coûts

Parmi les 56 mesures, ***10*** *sont des « Quick Wins », des* ***actions faciles à mettre en œuvre avec une nette amélioration de la cybersécurité*** *:*

	Mesure de sécurité	Charge de travail	Coût	Priorité
Chantier 04 : Gestion des accès	Réaliser une revue des droits sur l'ensemble des comptes (utilisateurs et administrateurs, personnels et génériques) : attribuer aux comptes uniquement les droits dont ils ont besoin	■□□	■□□	■■■
	Dans la mesure du possible, fournir des comptes personnels au lieu de comptes génériques	■□□	■□□	■■■
	Changer les mots de passe par défaut	■□□	■□□	■■■
	Protéger l'accès aux automates par un mot de passe	■□□	■□□	■■■
Chantier 06 : Gestion des ressources humaines	Mettre en place une procédure pour informer des départs, en amont	■□□	■□□	■■□
	Mettre en place une procédure pour, au moment du départ d'une personne : retirer ses droits d'accès au SI, récupérer ses badges d'accès aux locaux, récupérer les équipements qu'elle possède, changer les mots de passe des comptes génériques qu'elle aurait pu connaitre	■□□	■□□	■■□
Chantier 07 : Gestion des sauvegardes	Réaliser des sauvegardes des configurations des équipements afin d'être en mesure de redémarrer un site après un désastre	■□□	■□□	■■□
	Réaliser des sauvegardes des configurations des équipements afin d'être en mesure de redémarrer un site après une attaque	■□□	■□□	■■□
Chantier 10 : Sécurité physique	Réaliser un inventaire des clés et des badges d'accès pour chaque site	■□□	■□□	■■■
Chantier 11 : Sensibilisation SSI	Sensibiliser les utilisateurs sur le stockage des mots de passe	■□□	■□□	■■■

5.4.2. PSSI Opérationnelle (Politique de Sécurité des Systèmes d'Information)

Prenant en compte l'analyse générale des risques de Wavestone et les recommandations ANSSI, **la PSSI Opérationnelle est le document de référence de la cybersécurité VNF.**

La PSSI présente **239 recommandations** classées selon **8 grandes catégories :**

- Organisation de la cybersécurité des systèmes d'information industriels
- Gestion des actifs
- Cybersécurité et ressources humaines
- Contrôles des accès
- Cybersécurité des réseaux
- Cybersécurité opérationnelle
- Gestion des incidents de cybersécurité
- Conformité

Remarques :

Il est envisagé de remplacer la classification SIIV (Système Très Critique, Système Critique et Système à Criticité Faible) par une classification basée sur la typologie d'ouvrage pour bien focaliser les efforts de mise en œuvre des mesures.