Cible de sécurité CSPN PANORAMA Serveur et client Court-terme

Cible CSPN

Référence: PANO/CibleCSPN Court-terme-V3.5

Date: 08/10/2019

HISTORIQUE DES REVISIONS

Version	Date	Commentaires
3.0	27/04/2018	Version recentrée sur Panorama E² Ajout de la notion de bulletin de sécurité La fonction Agent SNMP est exclue de la cible Les liaisons HTTP, OPC.TCP et Net.TCP du serveur OPC-UA sont exclues de la cible L'acquisition LON est exclue de la cible
3.1	24/04/2019	La modification des profils en exploitation est exclue de la cible Réactivation partielle du bien sensible bst5 « Certificat de la fonction Serveur de données OPC-UA » et de la fonction de sécurité fs5 « Stockage sécurisé des certificats des fonctions Serveur de données »
3.2	06/06/2019	Mise à jour de l'identification de la cible Mise à jour de la définition des attaquants Éclaircissements sur les biens bst4 et bst5 et les fonctions de sécurité fs4 et fs5
3.3	29/07/2019	Correction du tableau de synthèse des « Biens sensibles de la ToE »
3.4	30/07/2019	Suppression de la notion de clé privée dans bst5
3.5	08/10/2019	Complément dans l'identification du produit (§1.2) Ajout de précisions à hs11

SOMMAIRE

1. INTRODUCTION

1.1 Objet

Ce document décrit la cible pour la Certification de Sécurité de Premier Niveau (CSPN) pour la partie Serveur et Client SCADA de Panorama E².

Ce document a pris pour référence :

- le profil de protection d'un progiciel Serveur SCADA court-terme de l'ANSSI (20151005_NP_ANSSI_SDE_4067_PJ3_serveur_scada_court_terme_PJ3).
- quelques éléments concernant les utilisateurs et les journaux locaux repris de la version moyen terme du serveur (20151005_NP_ANSSI_SDE_4067_PJ4_serveur_scada_moyen_terme_PJ4).
- Le profil de protection d'un progiciel Client MES/SCADA Moyen terme extrapolé en court terme pour le mettre au niveau de la partie serveur (20151005_NP_ANSSI_SDE_4067_PJ9_client_scada_mes_moyen_terme_PJ9).

La description de la cible suit le plan de ces profils.

1.2 Identification du produit

Éditeur	Codra Ingénierie Informatique Immeuble Hélios - 2 rue Christophe Colomb - CS 0851 91300 Massy France
Lien	https://fr.codra.net/panorama/
Produit	Panorama E²
Version	Panorama E² V7.00 intégré à Panorama Suite 2017 (build 17.00.011) + Updates suivants : PS2-1700-01-1086 ; 03-2128 ; 05-1024 ; 06-0348 ; 07-1082; 08-1054 ; 09-1052 ; 13-0348 ; 14-1051 ; 17-1037 ; 18-1157
Catégorie	SCADA

1.3 Documents de référence

Référence	Titre
ANSSI : securite_industrielle_GT_methode_classification-principales_mesures	La cybersécurité des systèmes industriels – Méthode de classification et mesures principales
ANSSI : 20151005_NP_ANSSI_SDE_4067_PJ3_serveur_scada_court_terme_PJ3	Profil de protection d'un progiciel Serveur SCADA court-terme
20151005_NP_ANSSI_SDE_4067_PJ4_serveur_scada_moyen_terme_PJ4	Profil de protection d'un progiciel Serveur SCADA moyen-terme
20151005_NP_ANSSI_SDE_4067_PJ9_client_scada_mes_moyen_terme_PJ9	Profil de protection d'un Client SCADA MES/SCADA moyen- terme
ANSSI-CSPN-CER-P-01/1.1 5/12	Certification de sécurité de premier niveau des produits des technologies de l'information

Référence	Titre
ANSSI-CSPN-CER-I-02.	Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, instruction
ANSSI-CC-NOTE-21/1.0	Note d'application : Méthodologie pour l'évaluation d'une gamme de produits
V7.2 du 6/11/17	Manuel Panorama

1.4 Terminologie et abréviations

1.4.1 Abréviations

AD : Active Directory, service d'annuaire pour les systèmes d'exploitation Windows

API :

Sens 1 : Application Programming Interface

Sens 2 : Automate Programme Industriel, sens non utilisé dans ce document

CIM : computer-integrated manufacturing ou production intégrée par ordinateur, est un concept décrivant l'automatisation complète des procédés de fabrication

CSPN : Certification de Sécurité de Premier Niveau

DCOM : Distributed Component Object Model technologie Microsoft

MES : Manufacturing Execution System ou la gestion des processus industriels, système informatique dont les objectifs sont d'abord de collecter en temps réel les données de production de tout ou partie d'une usine ou d'un atelier

n.a : Non Applicable

OPC : OLE for Process Control, protocole de communication basé initialement sur OLE basé sur COM/DCOM

OPC-DA : OPC basé sur DCOM pour la partie Data Access

OPC-UA : OPC Unified Access, basé sur des web services

SCADA : système de contrôle et d'acquisition de données (anglais : Supervisory Control And Data Acquisition), aussi appelé Système de supervision

ToE : (Target of Evaluation) désigne le composant qui est l'objet de l'évaluation.

1.4.2 Terminologie

Authenticité : Propriété d'une information ou d'un traitement qui garantit son identité, son origine et éventuellement sa destination. *Traduction anglaise :* authenticity
(source securite_industrielle_GT_methode_classification-principales_mesures)

Confidentialité : Caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés. *Traduction anglaise :* confidentiality

(source securite_industrielle_GT_methode_classification-principales_mesures).

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services rendus par ce système.

Le terme cybersécurité sera utilisé dans le document afin d'éviter tout risque de confusion avec le terme « sécurité » qui, dans le monde industriel, peut avoir d'autres significations que celles liées à la sécurité des systèmes d'information comme la sécurité des biens et des personnes par exemple.
(source securite_industrielle_GT_methode_classification-principales_mesures).

Note : ce dernier § n'est pas appliqué partout dans le profil de protection de l'ANSSI. Les textes en provenance de ce document n'ont pas été modifiés pour faciliter la traçabilité. Donc à chaque fois que le terme « sécurité » est rencontré, il faut le traduire en « Cybersécurité ».

Disponibilité : Propriété permettant de rendre le service attendu en temps voulu et dans les conditions d'usage prévues. *Traduction anglaise :* Availability
(source securite_industrielle_GT_methode_classification-principales_mesures).

Intégrité : Propriété de protection de l'exactitude et de la complétude des actifs. *Traduction anglaise :* Integrity (source securite_industrielle_GT_methode_classification-principales_mesures).

Client SCADA : (Poste d'exploitation Panorama) C'est un logiciel installé sur un poste utilisateur permettant à l'opérateur humain d'interagir avec le Serveur SCADA. Le Client SCADA permet à l'opérateur de prendre connaissance des données traitées ou générées par le serveur et d'envoyer des commandes (voir § 2.1Descriptif du produit). Dans le profil de protection, appelé Client Applicatif SCADA ou Client Applicatif.

Serveur SCADA : (serveur fonctionnel Panorama) C'est un logiciel installé sur une machine qui fonctionne sans intervention d'un opérateur et qui permet d'acquérir des données « procédé », passer des commandes, de gérer alarmes, de stocker des valeurs (voir § 2.1Descriptif du produit). Dans le profil de protection, appelé Serveur applicatif SCADA ou Serveur Applicatif.

<u>Définitions issues des autres profils de protection SCADA de l'ANSSI</u> :

Poste d'ingénierie : (Poste de développement Panorama) C'est un logiciel qui permet d'assurer la configuration, le paramétrage, la programmation, les tests de tout ou partie du système de supervision industriel.

Historian : C'est un serveur d'historique, qui utilise une base de données distante et qui permet de stocker les différentes alarmes ou valeurs issues du système de supervision (SCADA) ou du processus industriel. Le serveur d'historique peut être local ou centralisé.

2. DESCRIPTIF DU PRODUIT DE REFERENCE

2.1 Descriptif du produit

2.1.1 Descriptif général du produit

Panorama E² est un SCADA qui est utilisé au sein de réseaux industriels. Il est interconnecté avec des équipements de terrain de niveau CIM 1 et peut s'interfacer avec d'autres équipements et logiciels tiers des niveaux CIM 2 ou CIM 3.

Panorama est constitué de divers composants matériel et logiciel qui utilisent différentes informations pour fonctionner. Le système peut être modélisé sommairement comme sur la figure 1.

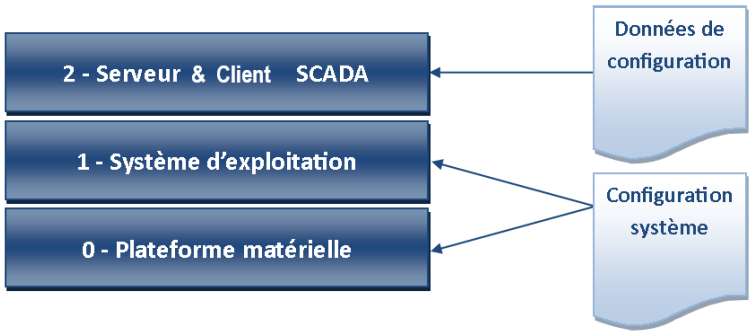

FIGURE 1 – Modélisation d'un système de supervision industrielle

Couche 0 - Plateforme matérielle et 1 – Système d'exploitation Elles constituent la plate-forme d'exécution du produit : Dans le cadre de Panorama, il s'agit de machines sous Microsoft Windows.

Dans la suite de ce document, les briques du système d'exploitation nécessaires au bon fonctionnement du produit sont considérées comme faisant partie de cette plateforme d'exécution du produit. Il en est de même des applicatifs tels qu'un gestionnaire de bases de données, comme SQL Server, assurant des fonctionnalités d'usage général et présentant un certain niveau d'intégration avec le système d'exploitation.

Pour fonctionner, ces couches systèmes nécessitent un certain nombre d'éléments dits de « configuration système ».

Couche 2 – Serveur SCADA et Client SCADA : ils constituent la ToE et assurent les fonctionnalités décrites au paragraphe « 2.1.2 Descriptif des fonctions du produit ».

Pour fonctionner, un Serveur SCADA et le Client SCADA requièrent des données de configuration. Elles sont constituées de l'ensemble des informations nécessaires au paramétrage du SCADA pour adapter son fonctionnement au contexte d'une installation particulière. Les données de configuration typiques comprennent :

- Pour le serveur : la liste des entrées/sorties terrain, la communication avec les équipements, les caractéristiques d'archivage, la configuration des alarmes, des formules, des scripts. . .
- Pour le client : les informations de dessin, de fond de plan, d'animation, de commande des symboles destinés à représenter l'état des installations, des éléments d'IHM standards : textes, boutons, cases à cocher, listes, du paramétrage des courbes, histogrammes…

En plus de ses données de configuration, un Serveur SCADA manipule des données que l'on peut qualifier de « procédé ». Elles sont constituées de l'ensemble des informations en relation directe avec l'installation. On peut y trouver :

- des données issues du terrain et manipulées par le Serveur SCADA. Ces données sont importantes pour permettre à l'utilisateur de contrôler le fonctionnement de l'installation.

- des données types commandes préconfigurées ou recettes qui peuvent, si envoyées aux équipements, impacter le fonctionnement de l'installation.

Le Client SCADA permet à l'opérateur de prendre connaissance des données traitées ou générées par le serveur et d'envoyer des commandes.

En plus de ses données de configuration, un Client SCADA manipule des données qui sont issues des serveurs. Elles sont constituées de l'ensemble des informations en relation avec l'état de l'installation ou élaborées en interne par le serveur.

Panorama E² est un des éléments de Panorama Suite qui comprend aussi Panorama COM (Frontal d'acquisition) et Panorama Historian. Il partage avec ces produits : le kit d'installation, l'environnement de développement et de nombreux éléments techniques pour la partie serveur. Nota : un choix du kit d'installation permet de n'installer que Panorama E².

2.1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

Partie Serveur :

- **Acquisition des données terrain et envoi de commandes :** La ToE comporte des fonctions de communication prenant en charge les échanges avec les équipements de terrain tels que des automates programmables industriels, des contrôleurs, des IED [1]. . . (niveau CIM 1), avec des protocoles tel que OPC-DA, OPC-UA, SNMP V1/V2/V3, BACnet, IEC, Modbus. Le protocole LON est exclu du périmètre.

- **Échanges de données :** La ToE peut envoyer et recevoir des flux d'information en s'appuyant sur des interfaces (serveur OPC DA, Serveur OPC-UA, Agent SNMP) avec des systèmes tels qu'un serveur d'historiques, un MES, une station d'ingénierie, des Serveurs SCADA, des postes clients... La fonction Agent SNMP est exclue du périmètre de la cible. Concernant le serveur OPC-UA, les liaisons de type HTTP, Net.TCP et OPC.TCP sont exclues (seules les liaisons de type HTTPS sont inclues dans le périmètre).

  Ces systèmes peuvent se trouver sur le même niveau CIM 2, sur le niveau CIM 3, ou même être déportés sur un réseau externe.

  La ToE permet aussi d'envoyer des mails, SMS, Fax, de gérer une astreinte vocale, d'échanger en tant que client FTP des fichiers et de vérifier la présence de machines par « Ping ». Ces fonctions sont hors périmètre de la cible.

- **Gestion des alarmes :** La ToE détecte des conditions d'alarmes à partir des informations reçues des équipements de terrain ou de données internes et en assure le traitement et la transmission et leur historisation.

[1] Intelligent Electronic Device, terme utilisé dans le domaine de l'énergie électrique qui regroupe tous les équipements d'automatisme ayant des fonctions de protection ou de pilotage local tels que les disjoncteurs, transformateurs

- **Fonctions d'archivage** : La ToE assure des fonctions d'archivage et de restitution de valeurs.

  Cette fonction peut être rendue soit par :

  - Archivage fil de l'eau ou sélectif qui peut stocker dans un format privé :
    - en local à la machine qui produit les données
    - sur une machine distante en utilisant le « serveur d'archivage ».
  - Un export base de données (format public)

- **Fonctions de redondance :** La ToE permet un fonctionnement en redondance pour assurer la haute disponibilité de ses fonctions.

- **Fonction de persistance dynamique :**

  Cette fonction est constituée deux sous fonctions :

  - Mémorisation des valeurs : La ToE permet de conserver des valeurs de données temps réel entre deux démarrages, par exemple pour ne pas recommencer les comptages ou les comptes à rebours à zéro (fonction disponible en dehors de la redondance). Usage interne.
  - Traçabilité des modifications : Journal des modifications des priorités ajustables, comme les valeurs de seuils d'alarmes : usage externe.

Partie cliente :

- **Interface homme-machine :** La ToE intègre des fonctions d'interface homme-machine **:**
  - Gestion de synoptiques qui permettent de représenter graphiquement l'état de l'installation et de passer des commandes locales à la ToE ou transmises au procédé.
  - Alarmes : Affichage des états, de l'historique des alarmes et des commandes comme l'acquittement, l'inhibition, la saisie de compte-rendu…
  - Affichage de courbes, d'histogrammes…
  - Fonctions GeoScada et Navigateur internet. Ces fonctions sont hors périmètre de la cible.
  - Identification des opérateurs. Seule l'authentification externe des opérateurs est dans le périmètre de la cible. La modification en exploitation de leurs profils est exclue.

- **Compatibilité avec la redondance :** Sélection automatique de serveur actif

Partie commune :

- **Traitement de données, scripting et programmation horaire :** La ToE assure des fonctions de traitement, de calculs et de « Programmation horaire ».

- **Accès générique à une table de base de données :** Interface base de données et recette. La ToE permet d'accéder à une table d'une base de données, pour y lire, écrire, supprimer des enregistrements.

- **Stockage local de secours :** La ToE offre un mécanisme qui permet de stocker en local les écritures pour les fonctions d'archivage et qui accèdent à des bases de données quand le stockage distant est inaccessible. Au retour de la communication il y a un reversement automatique des valeurs stockées localement.

- **Fonctions d'administration :** La ToE comporte plusieurs interfaces pour permettre son administration : gestion de la configuration, gestion des utilisateurs. Nota : ces fonctions d'administration sont utilisées par différentes catégories d'utilisateurs (voir § 4 Descriptif des différents utilisateurs).

- **Fonctions de déploiement configuration :** La ToE comporte une interface permettant d'assurer le déploiement des données de configuration dont la mise la mise à jour a été faite sur le poste d'ingénierie : Architecture générale de l'application, données d'entrée/sortie, communication avec les équipements de terrain, conditions d'alarmes, synoptiques, formules… Nota : certaines de ces données de configuration définies comme ajustables peuvent être adaptées en exploitation, mais en aucun cas la structure de l'application ne peut être modifiée.

  Nota : pour des raisons de sureté de fonctionnement et de cybersécurité, la fonction de pilotage des serveurs associée à la fonction de copie est désactivée.

- **Fonction de diagnostics :** La ToE fournit des fonctions de diagnostics qui permettent de surveiller l'état de son fonctionnement et son état interne (ex : Traceur, Explorateur d'application)

- **Journalisation locale d'évènements :** La ToE fournit une politique de journalisation locale d'évènements de sécurité et d'administration. Les événements journalisés sont décrits dans le manuel « *La sécurité de l'application > Sécurité et fonctionnement en réseau > Utiliser les journaux* ».

Les fonctions suivantes sont hors périmètre de la cible

- L'accès à une base de données autre que SQL Server.
- Serveur d'IHM Mobile et l'accès SmartBMS.
- Export Panorama Historian et le reversement d'archives vers Historian.
- Extension des fonctions métiers Panorama livrées en standard par la notion d'objets utilisateurs développés par les configurateurs en utilisant la même méthodologie d'intégration que les fonctions Panorama.
- Les licences fournies par le serveur de licence Panorama (SLP) : Utilisation de clé spécialisée Safenet sur port USB ou fichier de licence.

Ces fonctions sont nativement désactivées. Pour les activer, il faut les ajouter au paramétrage de l'application.

2.2 Descriptif de l'architecture d'utilisation du produit

Légende des schémas :

- les flux en pointillés sont hors scope de cette CSPN
- les blocs gris représentent les modules concernés par la CSPN

Panorama supporte plusieurs types d'architecture physique de réseau : deux sont typiques

- Client-Serveur, mono réseau
- Client-Serveur, réseau procédé séparé

Seule cette dernière architecture est retenue pour offrir un niveau de sécurité convenable.

Dans ces types d'architecture, les composants logiciels sont déployés sur un ensemble de machines afin de distribuer les traitements, d'être plus proches des équipements de terrain, d'assurer la montée en charge, de redonder certaines fonctions, d'offrir plusieurs postes clients « lourd ».

Nota :

- L'architecture monoposte est aussi supportée : Elle revient à mettre tous les éléments de la ToE sur une seule machine, sans la fonction « serveur d'archivage » qui n'est pas utile dans cette configuration.
- Dans la terminologie Panorama :
    - Le Serveur SCADA est appelé « Serveur fonctionnel »
    - Le Client SCADA est appelé « Poste d'exploitation »
- Le serveur d'IHM mobile est considéré comme un serveur fonctionnel.
- Pour la répartition de charge et la redondance toutes les architecture sont possibles : Par exemple il n'est pas nécessaire d'appairer les serveurs.

Pour les flux logiques, consulter le manuel « *La sécurité de l'application > Sécurité et fonctionnement en réseau > Configuration pour la mise en réseau de Panorama > Annexe : principe des échanges réseau* ».

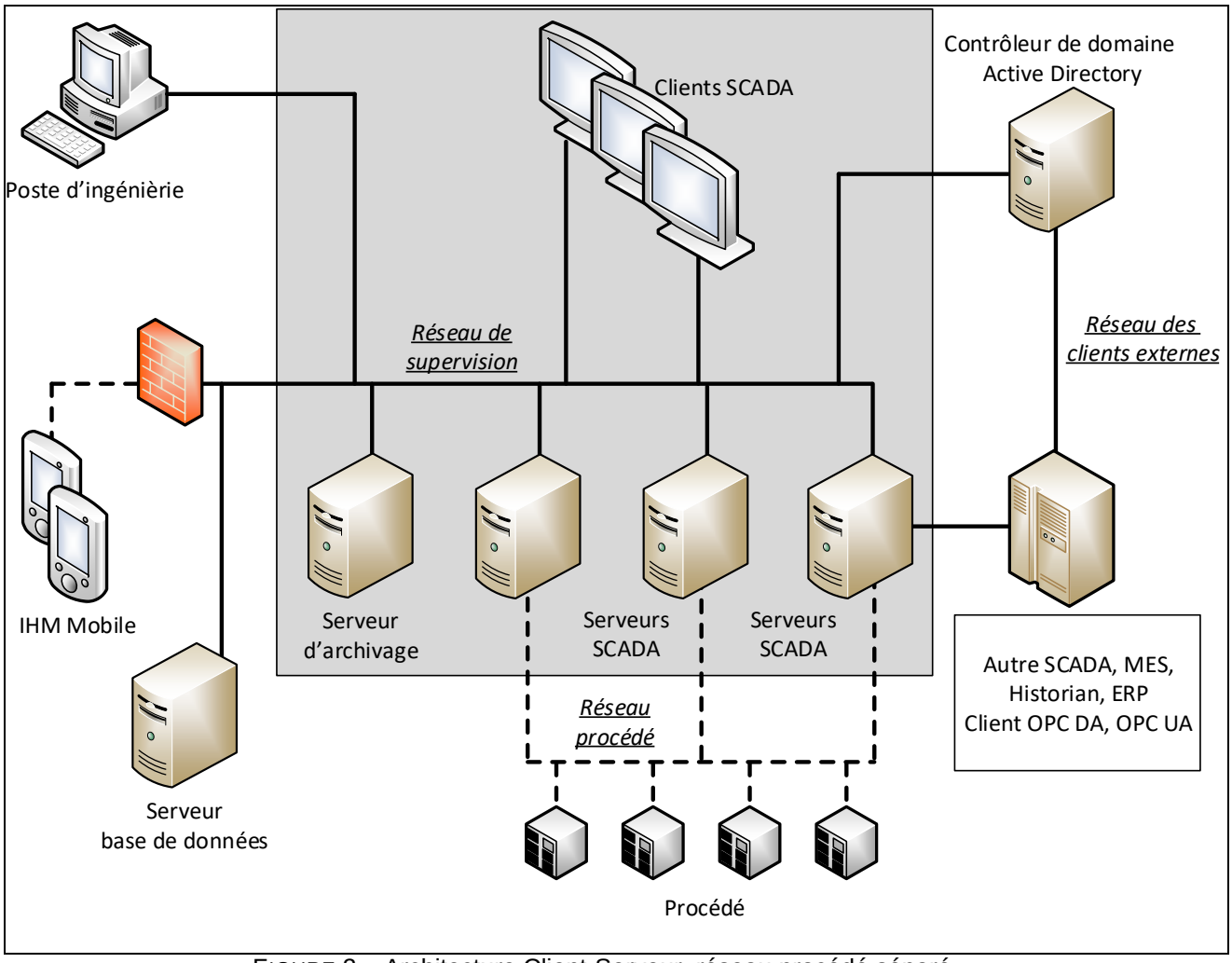

FIGURE 2 – Architecture Client-Serveur, réseau procédé séparé

Trois réseaux :

- Réseau de supervision : réseau interne de la ToE, relié au serveur de base de données dédié et avec le poste d'ingénierie
- Réseau procédé
- Réseau des clients externes (Autre SCADA, MES, ERP …)

3. PERIMETRE D'EVALUATION

3.1 Configuration et mode d'utilisation

- Versions de Windows :
    - Windows 10 (1709)
    - Windows Server 2016 1607

  avec leurs updates de sécurité
- Windows en domaine.
- Configuration avancé DCOM avec configuration des services Panorama dans un compte dédié, voir manuel Panorama.
- Les clients OPC-DA de la fonction « serveur de données » de Panorama sont dans le même domaine que la ToE.
- Les fonctions non utiles à une machine n'y sont pas installées.

3.2 Plateforme d'évaluation

La plate-forme présentée ci-dessous est la plate-forme minimale qui permet de mettre en jeu tous les biens sensibles et les fonctions de sécurité.

La configuration de l'application Panorama doit mettre en jeu :

- Les flux internes : application répartie sur deux serveurs logiques avec des liens entre des données reparties sur les deux serveurs et le poste client contient un synoptique avec, par exemple, une courbe et une fenêtre d'alarme.
- Toutes les fonctions qui utilisent une base de données.
- Les interfaces d'accès aux données d'exploitation et élaborées (voir ci-dessous).
- Le flux avec le poste d'ingénierie

Pour les machines, il faut :

- ToE
    - Deux Serveurs SCADA, un en Windows 10 et l'autre en Windows Server 2016
    - Un poste Client SCADA (Windows 10)
- Hors ToE
    - Un Serveur de domaine (Windows server 2016)
    - Un poste d'ingénierie (Windows 10)
    - Une machine avec Client OPC-DA et OPC-UA (Windows 10)

- Une machine qui simule le procédé (Windows 10)

- Hors et dans ToE
  - Une machine qui contient la base de données (hors ToE) et le serveur d'archivage (ToE) (Windows 10). L'hébergement du serveur d'archivage et SQL Server sur une même machine est un cas très fréquent chez les clients.

4. DESCRIPTIF DES DIFFERENTS UTILISATEURS

Préambule : Sauf indication contraire, les utilisateurs décrits ci-dessous sont gérés par l'Active Directory. Les autres le sont par la ToE.

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :

- **Opérateur :** Ce sont les utilisateurs dont le rôle principal est d'exploiter la ToE depuis le Client SCADA.

  L'opérateur peut au travers des IHM :
  - consulter les données, notamment par navigation dans les vues graphiques,
  - envoyer des commandes (locales à la ToE ou transmises au procédé),
  - consulter les événements et les historiques,
  - consulter et acquitter les alarmes,
  - adapter la partie modifiable dynamiquement de la configuration (voir § 6.2 bst 2)
  - diagnostiquer,
  - arrêter et démarrer l'application.

- **Configurateur/Développeur d'application :** Ce sont les utilisateurs chargés de la création, du développement et de la maintenance (évolutive ou corrective) de l'application de supervision, sans pouvoir modifier le logiciel sous-jacent.
  Dans le cas de la ToE, les développeurs d'application remplissent les fonctions suivantes :
  - la diffusion de la mise à jour des données de configuration,
  - le changement d'application sur la ToE,
  - la gestion de la licence,
  - la gestion de la base de persistance dynamique.
  - la définition de la politique de droits des utilisateurs gérés par la ToE
  - Nota : pour pouvoir mener à bien leurs tâches, ils ont aussi les droits des opérateurs.

- **Opérateur de sauvegarde** : Il est chargé de sauvegarder, les données générées par les applications, par exemple les bases de données ou les fichiers d'archives. Ponctuellement, il est également amené à restaurer les données sauvegardées sur la ToE. Les droits nécessaires à cette dernière tâche sont donnés temporairement par l'administrateur.

- **Administrateur** : Ce sont les utilisateurs chargés de l'administration de la ToE : installation, mises à jour logiciel et possibilité d'activer ou désactiver les journaux.

- **Auditeur :** Utilisateur ayant le droit de consulter tout ou partie des journaux d'évènements produits par la ToE.

- **Super-administrateur :** C'est l'utilisateur dont le rôle est de définir la politique de droits des utilisateurs gérés dans l'AD.

- **Utilisateur d'exécution des services de la ToE :** C'est l'utilisateur sous lequel sont exécutés les processus de type « Service Windows » de la ToE. Il peut être différent pour chaque service.

- **Utilisateurs des interfaces externes :** Ce sont les utilisateurs des applications tierces qui accèdent aux « Données d'exploitation » et aux « Données élaborées » par le flux « Serveur de données » en utilisant les « Flux de collaboration ». Ils peuvent faire les mêmes actions qu'un opérateur sauf le diagnostic. Ils peuvent être limités dans leurs actions suivant l'interface utilisée et la configuration de l'application. On distingue deux types « d'Utilisateurs des interfaces externes » :

  - **Utilisateur de l'interface externe OPC-DA :** Ce type d'utilisateur est géré par l'AD.

  - **Utilisateur des interfaces externes OPC-UA** : Ce type d'utilisateur est géré par la ToE (à l'aide de certificats).

Notes :

Un utilisateur n'est pas forcément une personne physique et peut être un équipement ou un programme tiers. Par ailleurs, une même personne physique peut être titulaire de plusieurs comptes avec des profils d'utilisateur différents.

IMPORTANT : les « utilisateurs Panorama » au sens du manuel utilisateur de Panorama, sont une sur-couche applicative qui permet de discriminer les opérateurs entre eux. Cette notion n'intervient pas au titre de la cible qui se base sur les « Utilisateurs Windows » pour différencier les utilisateurs au sens du profil de protection.

5. HYPOTHESES SUR L'ENVIRONNEMENT

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la ToE :

h 1) **Règles d'hygiène informatique :** Les recommandations du document de l'ANSSI « Guide d'hygiène informatique » sont appliquées quand elles sont applicables.

Dans ce cadre, les comptes et mots de passe Windows nécessaires à l'utilisation de Panorama ne sont fournis qu'aux utilisateurs du profil adéquat.

Pour l'ensemble des machines du domaine, seuls les administrateurs ont le nom du compte et le mot de passe du compte local d'administration de la machine. Seul le super-administrateur a le droit d'inscrire une machine dans le domaine.

Le système mettant en œuvre le produit doit avoir une politique de sécurité applicable, idéalement inspiré par le guide d'hygiène informatique de l'ANSSI. Un responsable SSI en assure la mise en œuvre et le suivi.

Nota : Le manuel dans son chapitre « La sécurité de l'application », cite ce document et décline la majorité de ces points dans le contexte Windows Panorama, sans aller systématiquement jusqu'au mode d'emploi. Il est nécessaire que le client adapte les recommandations à ses spécificités.

h 2) **Consultation des journaux :** Il est considéré que les « auditeurs » consultent régulièrement les journaux locaux générés par l'équipement. Ils les étudient et réagissent le cas échéant en appliquant une procédure de traitement d'incident de cybersécurité.

h 3) **Utilisateurs :** Les utilisateurs définis au chapitre « 4 Descriptif des différents utilisateurs » sont tous compétents, formés et non hostiles.

h 4) **Local :** La ToE doit se trouver dans un local sécurisé dont l'accès est restreint à des personnes autorisées considérées comme non hostiles. En particulier, l'attaquant n'aura pas accès aux ports physiques de la ToE.
En revanche, des équipements identiques à la ToE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement en vue d'y rechercher des vulnérabilités par tous les moyens à sa disposition pour attaquer la ToE.

h 5) **Dimensionnement :** Il est supposé que la ToE est dimensionnée correctement pour les traitements qu'elle doit effectuer.

h 6) **Serveurs d'authentification :** Les serveurs d'authentification utilisés pour authentifier les utilisateurs sont considérés comme sains et configurés correctement, selon les recommandations du guide « Recommandation de sécurité relatives à Active Directory", N°DAT-NT-17/ANSSI/SDE/NP du 10/9/2014 ».

h 7) **Serveurs de base de données :** Les serveurs de base de données sont considérés comme sains et configurés correctement.

h 8) **Système d'exploitation sain :** Le système d'exploitation du système portant la ToE est considéré comme sain au début de l'évaluation et tout au long de l'évaluation sauf en cas de défaillance de la ToE.

h 9) **Système d'exploitation durci :** Le système d'exploitation est supposé avoir été configuré et durci selon les recommandations du fabricant de la ToE.
En particulier :

- Le système d'exploitation est supposé à jour.
- Le domaine est configuré pour que seul l'administrateur du domaine (super-administrateur) puisse ajouter une machine dans le domaine et les serveurs DNS associés.
- Seuls les comptes qui ont besoin d'ouvrir une session sur une machine de la TOE, peuvent

le faire (utilisation d'un GPO au niveau du serveur de domaine par exemple).

h 10) **Services non évalués absents :** L'ensemble des services fournis par Panorama mais hors de la cible de sécurité ne sont pas paramétrés/ajoutés dans l'application Panorama par le développeur.

h 11) **Documentation de sécurité :**

- La ToE est fournie avec un manuel détaillé sur l'utilisation sécurisée, confère son chapitre « La sécurité de l'application ». En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation.
- Des bulletins de sécurité sont publiés :
  - Dès la découverte d'une faille de sécurité avec fourniture d'une solution ou de consignes d'utilisation
  - Dès la disponibilité d'une amélioration de la sécurité, par exemple suite à des évolutions de normes.

L'ensemble des préconisations issues de cette documentation et des bulletins de sécurité ont été appliquées en vue de l'évaluation, y compris sur d'autres machines que celles qui hébergent la ToE et qui sont sur le réseau ou non : L'exemple type est : « les règles de protection de l'application Panorama sont appliquées sur toutes les machines où elle est recopiée ».
En particulier, comme indiqué dans le Bulletin de Sécurité Pano/BS-010, il convient de mettre en place une politique de surveillance de l'état d'expiration des certificats et de mise à jour de la liste pour retirer les empreintes des certificats expirés pour OPC-UA et les remplacer par celles des certificats renouvelés.

h 12) **Module externe :** Il est supposé qu'aucun module externe[2] n'est installé sur la ToE. Par exemple les objets utilisateurs sont clairement exclus de la cible.

h 13) **Non-adhérence logicielle :** La ToE a été développée de telle sorte à ne pas être adhérente à une version donnée d'un composant externe[3] (système d'exploitation, logiciel, bibliothèque). En particulier, l'utilisateur doit avoir la possibilité d'appliquer les mises à jour de sécurité de tout composant externe.
Dans le cas contraire, ce composant doit être intégré à la ToE.

h 14) **Activation des journaux :** La fonction de journalisation locale basée sur les journaux d'évènements Windows est supposée activée, fonctionnelle, intègre et authentique.

[2] Un module externe est un élément logiciel apportant de nouvelles fonctionnalités à la ToE mais qui n'est pas indispensable à son fonctionnement. Exemple : « objet utilisateur Panorama »

[3] Un composant externe est un élément logiciel nécessaire au fonctionnement de la ToE

6. DESCRIPTION DES BIENS SENSIBLES A PROTEGER

6.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

bse 1) **Flux vers la station d'ingénierie :** il s'agit d'un flux de copie de fichiers par SMBv3 et l'utilisation d'un partage accessible aux seuls configurateurs. Quand la copie est déclenchée depuis le poste d'ingénierie, il y a un flux UDP et DCOM complémentaires si le pilotage des serveurs est utilisé. Ces flux n'existent pas si la copie est déclenchée depuis la ToE.

Les flux entre la ToE et la station d'ingénierie doivent être protégés en intégrité, en confidentialité et en authenticité.

Nota : la confidentialité du flux de la station d'ingénierie ne s'appuie pas sur le fait que l'application est chiffrée par Panorama.

bse 2) **Flux vers un serveur d'historique :** Les flux entre la ToE et un serveur d'historique doivent être protégés en intégrité et en authenticité, flux SQL Server.

bse 3) **Flux de collaboration :** Les flux de collaboration doivent être protégés en intégrité et en authenticité. Ils sont constitués de l'ensemble des flux entre la ToE et d'autres composants du système :

I) Flux de surveillance de l'état de la ToE : il permet savoir si un serveur est accessible, si une application est chargée et laquelle, et savoir l'état des « serveurs logiques » de l'application. Ce flux est basé sur UDP et un protocole propriétaire. Utilisé conjointement avec le flux pilotage, voir ci -dessous

II) Flux de pilotage de l'application depuis l'outil « Administration & Configuration » utilisé depuis une machine hors ToE, flux DCOM.

III) Flux avec la fonction serveur d'archivage « fil de l'eau », flux DCOM, pour la restitution par API depuis une machine hors ToE.

IV) Flux des outils de diagnostic utilisés en distant comme « l'explorateur d'application » (flux DCOM) et le traceur (Pipe), depuis une machine hors ToE.

V) Flux « serveur de données » OPC-DA et OPC-UA qui permettent d'accéder aux données d'exploitation et/ou de passer des commandes.

bse 4) **Données d'exploitation** : Les données d'exploitation sont constituées de l'ensemble des informations utiles au bon fonctionnement du système de supervision en phase opérationnelle. Cet ensemble comprend notamment des valeurs instantanées, des alarmes, des commandes.

Elles sont mises à disposition d'applications tierces (Extensions applicatives, autres SCADA, Hypervision, MES, ERP) par la ToE au travers d'interfaces standards décrites ci-dessous.

Ces données doivent être protégées en intégrité et authenticité.

L'accès à ces données est régi par la politique de droit de la ToE ou par les services offerts par le système d'exploitation ou le serveur base de données. Il est utile de savoir comment sont accédées ces données :

I) Depuis les flux internes (voir § 6.2 Biens sensibles de la ToE bst10)

II) Depuis les flux de collaboration bse3

III) Données archivées par le serveur d'archivage, flux DCOM
Accessible par DCOM via un objet de restitution soit depuis le poste Client soit depuis un outil qui utilise l'API publique de cet objet.

bse 5) **Mécanisme d'authentification des utilisateurs gérés par l'AD :** L'intégrité et l'authenticité du mécanisme doivent être protégées par la ToE.

bse 6) **Secrets de connexion des utilisateurs gérés par l'AD :** La ToE doit garantir l'intégrité et la confidentialité de ces identifiants.

Les besoins de sécurité pour les biens sensibles de l'environnement sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Flux vers la station d'ingénierie		X	X	X
Flux vers un serveur d'historique			X	X
Flux de Collaboration			X	X
Données d'exploitation			X	X
Mécanisme d'authentification des utilisateurs gérés par l'AD			X	X
Secrets de connexion des utilisateurs gérés par gérés par l'AD		X	X	

6.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :

bst 1) **Logiciel(s) :** Afin d'assurer correctement ses fonctions, le logiciel doit être protégé en intégrité en toutes circonstances et en authenticité à l'installation ou la mise à jour.

Le logiciel comprend ce qui est installé par le kit d'installation Panorama et qui sert lors de l'exécution de la ToE : les binaires, les descripteurs de classes et les applications de référence.

bst 2) **Configuration :** La configuration de la ToE doit être confidentielle et intègre. Dans le cadre de Panorama tout utilisateur de la TOE peut avoir accès à l'application en lecture. L'attaquant ne doit pas pouvoir découvrir cette configuration autrement que par l'observation de l'activité de la ToE.

La configuration provient pour partie du poste d'ingénierie. Une autre partie est faite en local sur chaque machine, comme par exemple la configuration du stockage local de secours, de la surveillance réseau…

La partie en provenance du poste d'ingénierie peut être modifiée dynamiquement sur la ToE par les opérateurs. Seules les valeurs des propriétés « ajustables » sont concernées. Les adaptations sont mémorisées par la ToE avec le même niveau de confidentialité et d'intégrité que le reste de la configuration.

bst 3) **Mécanisme d'authentification des utilisateurs gérés par la ToE :** L'intégrité et l'authenticité du mécanisme doivent être protégées.

bst 4) **Certificats des utilisateurs des interfaces externes OPC-UA de la ToE** : Il s'agit des certificats présentés par les utilisateurs des interfaces externes OPC-UA pour permettre leur identification par la ToE. La ToE doit garantir l'intégrité de ces identifiants.

bst 5) **Certificats des Serveurs de données OPC-UA de la ToE** : Dans le cadre de cette version de la cible, il s'agit d'un certificat utilisé par la fonction Serveur de données OPC-UA. La ToE doit garantir l'intégrité de ces éléments.

bst 6) **Secrets de connexion aux bases de données :** la ToE doit garantir l'intégrité et la confidentialité de ces identifiants.

bst 7) **Politique de gestion des droits :** Cette politique de gestion des droits doit être intègre.

bst 8) **Fonction de journalisation locale :** La ToE dispose d'une fonction de journalisation locale qui, une fois activée, doit rester opérationnelle.

bst 9) **Journaux d'évènements locaux :** Les journaux locaux générés par la ToE doivent être intègres.

bst 10) **Flux internes :** Ils sont constitués de l'ensemble des flux internes entre les différentes machines de la ToE, ils doivent être protégés en intégrité et en authenticité :

I) Flux de surveillance de l'état de la ToE : il permet de savoir si un serveur est accessible, si une application est chargée et laquelle, et savoir l'état des « serveurs logiques » de l'application. Ce flux est basé sur UDP et un protocole propriétaire.

II) Flux de pilotage de l'application, depuis l'application Panorama ou depuis l'outil « Administration & Configuration », flux DCOM.

III) Flux d'échange de données, y compris alarmes, flux DCOM. Cela comprend aussi bien les flux entres les serveurs qu'entre les serveurs et les clients.

IV) Flux avec la fonction serveur d'archivage « fil de l'eau », flux DCOM.

V) Flux des outils de diagnostic utilisés en distant comme « l'explorateur d'application » (flux DCOM) et le traceur (Pipe).

VI) Flux pour accéder à la référence du paramétrage des opérateurs. Il s'agit d'un flux de copie de fichiers par SMBv3 et l'utilisation d'un partage accessible aux opérateurs et aux configurateurs.

bst 11) **Données élaborées** : Les « données élaborées » sont constituées de l'ensemble des informations utiles au bon fonctionnement du système de supervision en phase opérationnelle et élaborée en interne par la ToE, par exemple à partir des données d'exploitation. Cet ensemble comprend notamment les valeurs des compteurs, les résultats des formules, les propriétés des objets panorama…

Elles sont accessibles et traitées comme les données d'exploitation « § 6.1 Biens sensibles de l'environnement bse 4 ».

bst 12) **Données archivées :** Les données archivées sont constituées par les données stockées par la fonction « Archivage fil de l'eau ou sélectif ». Nota : La fonction peut stocker aussi bien des « données d'exploitation » que des « données élaborées ».

Elles doivent être stockées de manière intègre et authentique et à tout moment (disponibilité).

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Logiciel(s)			X	X
Configuration		X	X	
Mécanisme d'authentification des utilisateurs gérés par la ToE			X	X
Certificats des utilisateurs des interfaces externes OPC-UA de la ToE			X	
Certificats des Serveurs de données OPC-UA de la ToE			X	
Secrets de connexion aux bases de données		X	X	
Politique de gestion des droits			X	
Fonction de journalisation locale	X			
Journaux d'évènements locaux			X	
Flux internes			X	X
Données élaborées			X	X
Données archivées	X		X	X

7. DESCRIPTION DES MENACES

7.1 Description des agents menaçants

Les agents menaçants suivants ont été retenus :

am1) **Utilisateur malveillant Niveau 1 :** Un attaquant disposant d'un compte utilisateur géré par l'AD mais qui n'est pas un compte utilisateur défini au « 4 Descriptif des différents utilisateurs ». Il cherche à utiliser la TOE.

am2) **Utilisateur malveillant Niveau 2 :** Un attaquant disposant d'un compte utilisateur géré par l'AD et qui est un compte utilisateur défini au « 4 Descriptif des différents utilisateurs » sans privilèges d'administration (administrateur ou super-administrateur). Il cherche à outrepasser les droits du compte qu'il a compromis.

am3) **Attaquant dans le système industriel :** Tout attaquant n'ayant aucun compte cherchant à attaquer la ToE.

Aucun de ces attaquants n'est situé sur le réseau « procédé ».

7.2 Menaces retenues

Les menaces suivantes ont été retenues (le § 9 Tableau de couverture « Biens/Menaces/Sécurité » indique à quels biens s'appliquent ces menaces) :

m 1) **Déni de service :** L'attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu…).

m 2) **Altération des flux :** L'attaquant parvient à modifier des échanges sans que cela ne soit détecté.

m 3) **Compromission des flux :** Pour les flux requérant la confidentialité, l'attaquant parvient à récupérer des informations en interceptant des échanges entre la ToE et un composant externe.

m 4) **Corruption du logiciel :** L'attaquant parvient à modifier, de manière temporaire ou permanente le logiciel de la ToE. L'attaquant réussit à exécuter du code illégitime sur la ToE.

m 5) **Corruption de la configuration :** L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.

m 6) **Compromission de la configuration :** L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.

m 7) **Vol d'identifiants :** L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur ou aux bases de données.

m 8) **Contournement de l'authentification :** L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

m 9) **Contournement de la politique de droits :** L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus.

m 10) **Corruption des journaux d'évènements locaux :** L'attaque parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé par la politique de droits de la ToE.

8. FONCTIONS DE SECURITE

Les fonctions de sécurité sont les suivants (le $ 9 Tableau de couverture « Biens/Menaces/Sécurité » indique à quelles menaces s'appliquent ces objectifs) :

fs 1) **Gestion des entrées malformées :** La ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance du réseau.

fs 2) **Communications sécurisées :** La ToE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité pour les flux décrits au chapitre « 6.1 Biens sensibles de l'environnement ».

fs 3) **Non divulgation des secrets de connexion des utilisateurs gérés par l'AD** : La ToE ne permet pas de retrouver les secrets de connexions d'un utilisateur authentifié par l'AD.

fs 4) **Intégrité des certificats des utilisateurs des interfaces externes OPC-UA de la ToE** : La ToE doit pouvoir protéger ces certificats de façon à ce que seuls les utilisateurs autorisés puissent modifier ceux-ci.

fs 5) **Intégrité des certificats des Serveurs de données OPC-UA de la ToE** : La ToE doit pouvoir protéger ces certificats de façon à ce que seuls les utilisateurs autorisés puissent modifier ceux-ci.

fs 6) **Accès aux bases de données par Sécurité Intégrée :** La ToE permet de d'accéder aux bases de données en utilisant la « Sécurité Intégrée », évitant ainsi de stocker des secrets de connexion aux bases de données.

fs 7) **Authentification sécurisée :** L'utilisation de la ToE nécessite une authentification des utilisateurs ce qui permet de les différencier et donc de protéger des biens comme la configuration et les divers secrets de connexions.

fs 8) **Politique de droits :** La politique de gestion des droits est gérée de manière extrêmement stricte. L'implémentation de cette politique permet en particulier de garantir l'authenticité des opérations critiques, c'est-à-dire pouvant porter atteinte aux biens sensibles identifiés.

fs 9) **Signature du logiciel :** Le kit d'installation, les mises à jour sont tous signés avec un certificat au nom de Codra, fourni par une autorité de certification reconnue.

Nota : cela permet à l'administrateur de vérifier l'authenticité et l'intégrité des composants logiciels lors de leur installation ou de leur mise à jour.

fs 10) **Intégrité et confidentialité de la configuration :** La politique de gestion des utilisateurs ne permet pas à une personne non autorisée, ni de consulter, ni de modifier tout ou partie de la configuration de la ToE. Elle se base sur l'utilisation de compte Windows et la mise en place de droits adéquats sur le répertoire contenant l'application.

fs 11) **Intégrité des journaux :** Panorama enregistre ses journaux avec des droits tels que seuls les administrateurs et le super-administrateur puissent désactiver les journaux Panorama, effacer un de ces journaux ou l'un de leurs événements.

9. TABLEAU DE COUVERTURE « BIENS/MENACES/SECURITE »

Il est intéressant d'associer les lignes qui ont des croix dans une même colonne, ce qui permet de voir par **quelle(s) fonction(s) de sécurité est couvert un bien**, en passant de la partie A à la partie B).

Exemples :

- Partie A) Logiciel(s) est couvert par « Signature logiciel »se la partie B) en passant par la colonne « Corruption du logiciel »
- « Mécanisme d'authentification des utilisateurs » est couvert par « Stockage sécurisé des secrets » et « Authentification sécurisée avec le serveur d'authentification ».

MENACES	Déni de service	Altération des flux	Compromission des flux	Corruption du logiciel	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'évènements locaux
A) BIENS										
bse1) Flux vers et de la station d'ingénierie		IA	C			C				
bse2) Flux vers un serveur d'historique		IA								
bse3) Flux de collaboration		IA								
bse4) Données d'exploitation		IA							IA	
bse5) Mécanisme d'authentification des utilisateurs gérés par l'AD								IA		
bse6) Secrets de connexion des utilisateurs gérés par l'AD							CI			
bst1) Logiciel(s)				IA						
bst2) Configuration					I	C				
bst3) Mécanisme d'authentification des utilisateurs gérés par la ToE								IA		
bst4) Certificats des utilisateurs des interfaces externes OPC-UA de la ToE								I		
bst5) Certificats des Serveurs de données OPC-UA de la ToE					I					
bst6) Secrets de connexion aux bases de données							CI			
bst7) Politique de gestion des droits									I	
bst8) Fonction de journalisation locale	D									
bst9) Journaux d'évènements locaux										I
bst10) Flux internes		IA								
bst11) Données élaborées		IA							IA	
bst12) Données archivées	D	IA							IA	
B) Fonctions de sécurité										
fs1 : Gestion des entrées malformées	X									
fs2 : Communications sécurisées		X	X							
fs3 : Non divulgation des secrets de connexion des utilisateurs gérés par l'AD							(2)			
fs4 : Intégrité des certificats des utilisateurs des interfaces externes OPC-UA de la ToE								(3)		
fs5 : Intégrité des certificats des Serveurs de données OPC-UA de la ToE					(5)					
fs6 : Accès aux bases de données par Sécurité Intégrée							(4)			
fs7 : Authentification sécurisée		(1)			X	X	X	X		
fs8 : Politique de droits									X	
fs9 : Signature du logiciel				X						
fs10 : Intégrité et confidentialité de la configuration					I	C				
fs11 : Intégrité des journaux										X

(1) Participe à l'authenticité du flux « vers et de la station d'ingénierie »
(2) Pour le bien « Secrets de connexion des utilisateurs définies dans l'AD ».
(3) Pour le bien « Certificats des utilisateurs des interfaces externes OPC-UA de la ToE ».
(4) Pour le bien « Secrets de connexion aux bases de données ».
(5) Pour le bien « Certificats des Serveurs de données OPC-UA de la ToE ».