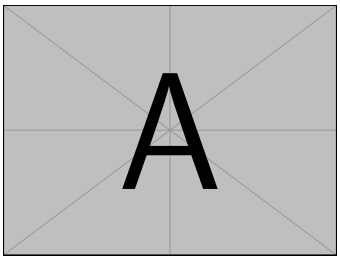
[AFFECTATION : NOM DE L'ÉDITEUR]
[AFFECTATION : NOM DU PRODUIT]

Serveur et client applicatif SCADA
Modèle de cible de sécurité

Version 1.1 moyen-terme

GTCSI



1er octobre 2024

Table des matières

Avant-propos

Ce document doit être instancié ou complété par l'utilisateur (industriel ou commanditaire du visa de sécurité).

1 Introduction

1.1 Objet du document

Le présent document constitue la cible de sécurité du produit [Affectation : nom du produit] dans sa version [Affectation : version du produit] développé par [Affectation : nom de l'éditeur] dans le cadre d'une Certification de Sécurité de Premier Niveau (CSPN).

1.2 Identification du produit

Éditeur	[Affectation : nom de l'éditeur]
Site Web de l'éditeur	[Affectation : lien vers le site Internet de l'éditeur]
Nom commercial du produit	[Affectation : nom du produit]
Numéro de la version du produit	[Affectation : version du produit]
Catégorie de produit	Serveur et client applicatif SCADA

1.3 Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

API
: Automate programmable industriel

COTS
: *Commercial off-the-shelf*

IHM
: Interface Homme Machine

SCADA
: Système d'acquisition et de contrôle de données

SDK
: Kit de développement logiciel

TOE
: *Target of evaluation*

USB
: Bus série universel

VLAN
: Réseau local virtuel

1.4 Documents applicables

Référence	Document
[R1]	Prestataires de détection des incidents de sécurité, référentiel d'exigences, version en vigueur. Disponible sur `https://cyber.gouv.fr`
[R2]	Recommandations relatives à l'administration sécurisée des systèmes d'information, n° ANSSI-PA-022. Disponible sur `https://www/cyber.gouv.fr`
[R3]	Guide de sélection d'algorithmes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, n° ANSSI-PG-083. Disponible sur `https://cyber.gouv.fr`
[R4]	Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, n° ANSSI-CSPN-CER-P02. Disponible sur `https://cyber.gouv.fr`

2 Description du produit

2.1 Description générale du produit

Un système de supervision industrielle permet d'acquérir et de traiter un grand nombre de données : télémesures, télésignalisations et téléalarmes. Il permet également de contrôler des équipements industriels — automates, capteurs, actionneurs — en leur envoyant des télécommandes et des téléréglages.

Un tel système est utilisé au sein de réseaux industriels. Il est interconnecté avec des équipements de terrain de niveau 1 [1] et peut s'interfacer avec d'autres équipements et logiciels tiers des niveaux 2 ou 3.

Un système de supervision industrielle est constitué de divers composants matériels et logiciels qui utilisent différentes informations pour fonctionner. Le système peut être modélisé sommairement comme présenté figure 1.

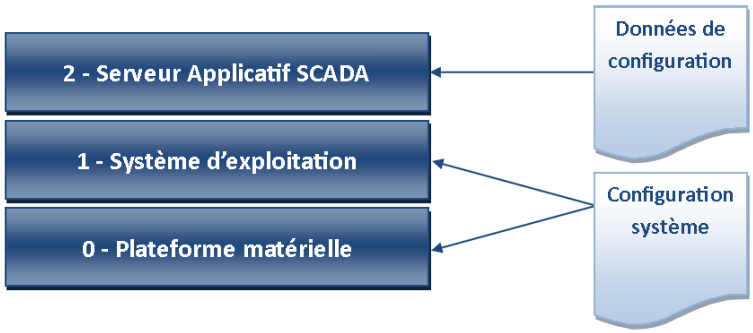


FIGURE 1 – Modélisation d'un système de supervision industrielle

Couche 0 - Plateforme matérielle et couche 1 – Système d'exploitation Elles constituent la plateforme d'exécution du produit. Il s'agit de machines de type station de travail ou serveur, utilisant un système d'exploitatio de type Microsoft Windows, Solaris, l'une des nombreuses distributions Linux ou tout autre système d'exploitation dit « classique » (par opposition à des plateformes d'exécution spécifiques constructeur). Dans la suite de ce document, les composants 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 ou un serveur web assurant des fonctionnalités d'usage général et présentant un certain niveau d'intégration avec le système d'exploitation.

Pour fonctionner, ces couches systèmes nécessitent des éléments dits de « configuration système ».

Couche 2 – Serveur Applicatif et client SCADA Cette couche constitue la TOE.

Pour fonctionner, un serveur applicatif SCADA requiert des données de configuration. Elles sont constituées de l'ensemble des informations nécessaires au paramétrage du serveur applicatif SCADA pour adapter son fonctionnement au contexte d'une installation particulière. Les données de configuration typiques d'un produit SCADA comprennent : la liste des entrées/sorties terrain, la communication avec les équipements, les caractéristiques d'archivage, etc.

En plus de ses données de configuration, un Serveur Applicatif 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 Applicatif 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.

Un client applicatif SCADA est un logiciel installé sur un poste utilisateur permettant à l'opérateur humain d'interagir avec les serveur SCADA. Le client applicatif permet à l'opérateur de prendre connaissance des données traitées ou générées par le serveur et d'envoyer des télécommandes ou des téléréglages.

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

- les informations de dessin de fond de plan,
- les informations de dessin, d'animation, de commande des symboles destinés à représenter l'état des installations ;
- les caractéristiques graphiques d'affichage des alarmes ;
- des éléments d'IHM standards : textes, boutons, cases à cocher, listes.

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

Note : La mise en œuvre d'un système SCADA (serveur(s) et client(s)) peut requérir l'usage de composants tiers. Il s'agit d'un ensemble de composants logiciels, usuellement basés sur un SDK ou des interfaces du serveur applicatif SCADA. De tels composants sont parfois développés de façon à assurer des besoins particuliers tels que l'interfaçage avec d'autres composants tiers, des traitements de données métier spécifiques, etc.

Elles n'entrent pas dans le périmètre de ce profil de protection sauf s'il s'agit d'une installation particulière faisant usage de tels composants. Etant de même nature que le produit SCADA en lui-même, elles présentent potentiellement les mêmes risques, sont sujet aux mêmes menaces et peuvent également apporter des fonctions de sécurité. .

2.2 Description de la manière d'utiliser le produit

Un serveur applicatif SCADA peut être mis en œuvre selon deux types d'architectures principales :

- un poste SCADA tout-en-un (*standalone*) ;
- une architecture distribuée.

Dans les schémas qui suivent, seuls les éléments en pointillés — composants et flux — font partie du périmètre de ce profil de protection.

2.2.1 Poste SCADA tout-en-un (*standalone*)

Dans cette architecture, l'ensemble des composants logiciels SCADA sont déployés sur une machine unique :

- le (ou les) composants serveur(s) applicatif(s) assurant les fonctions de frontal de communication, de gestion d'alarmes, de traitement de données, etc ;
- le client graphique (client lourd ou léger).

C'est l'architecture habituelle des pupitres opérateurs représentée sur la figure 2.

1. Purdue Reference Model – ANS/ISA95 – Norme internationale pour l'intégration des systèmes d'entreprise et de contrôle

2.2.2 Architecture distribuée

Dans ce type d'architecture, les composants logiciels SCADA sont déployés sur un ensemble de machines afin de distribuer les traitements et de redonder certaines fonctions :

- les frontaux de communication ;
- la gestion d'alarmes ;
- le traitement de données ;
- les fonctions métiers ;
- les interfaces Web ;
- les clients graphiques locaux ;
- les clients graphiques déportés.

Cette architecture est représentée sur la figure 3.

Une variante de ce type d'architecture constitue les architectures distribuées comprenant des liaisons inter-sites :

- les frontaux de communication locaux ;
- les clients déportés ;
- etc.

2.3 Description de l'environnement prévu pour son utilisation

[***A compléter par le rédacteur de la TOE : ce (ces) schéma(s) est (sont) à modifier/compléter***]

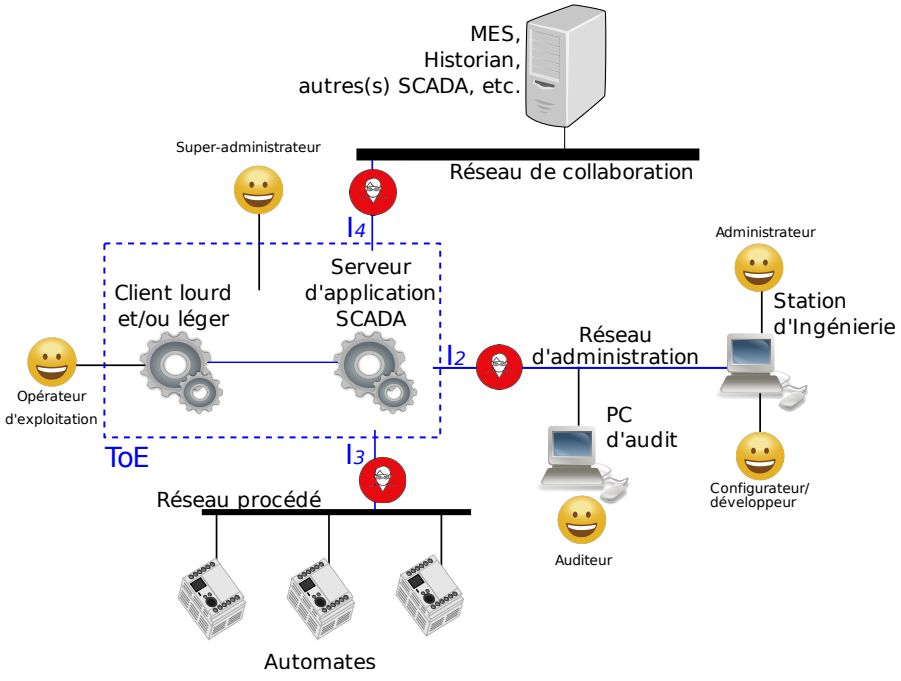


FIGURE 2 – Exemple d'architecture type tout-en-un (*standalone*)

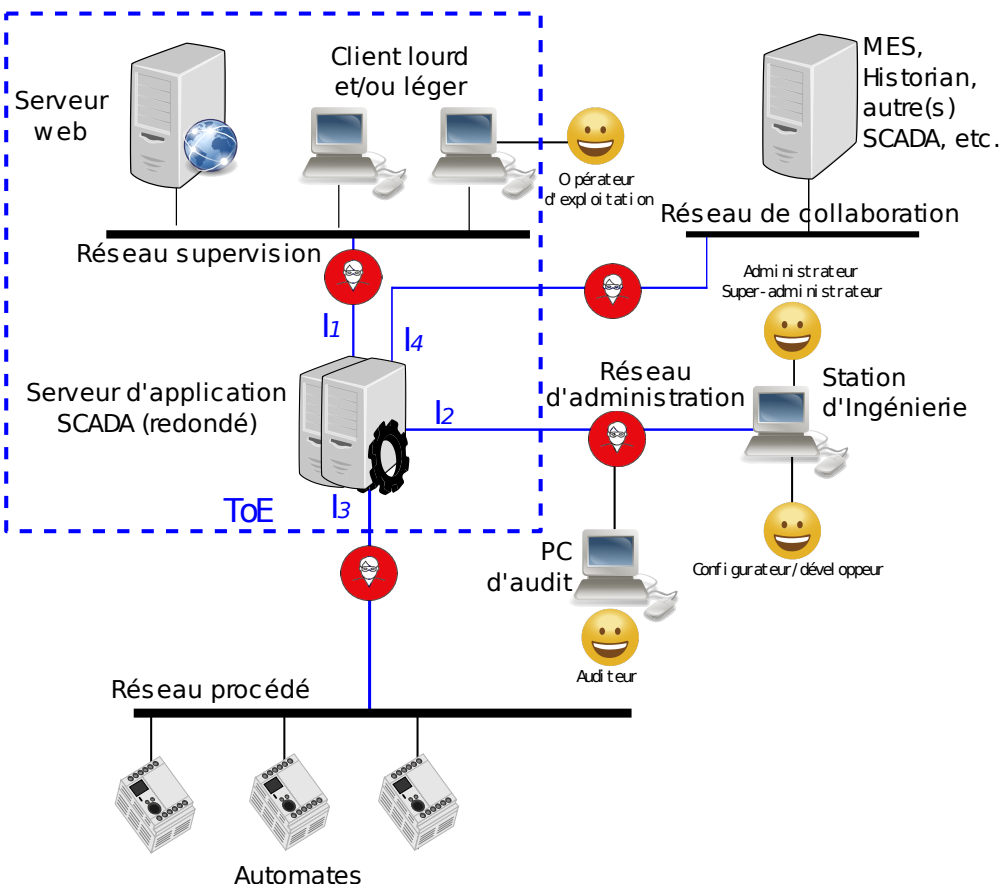


FIGURE 3 – Exemple d'architecture distribuée

Légende : Attaquant

La TOE dispose de plusieurs interfaces réseau physiques différentes qui sont listées ci-dessous :

- **I1.** Interface de raccordement au réseau de supervision (au(x) client(s) lourd(s) ou léger(s) dans le cas de l'architecture distribuée) ;
- **I2.** Interface du réseau d'administration et raccordée aux consoles d'administration ou d'audit. Cette interface permet l'accès aux rôles Super administrateur, Administrateur et Auditeur ;
- **I3.** Interface de raccordement au réseau procédé (automates, RTU, etc.) ;
- **I4.** Interface de raccordement au réseau de collaboration (autre(s) SCADA, MES, Historian, clients OPC DA, OPC UA, etc).

2.4 Description des dépendances

[*A compléter par le rédacteur de la TOE : description des dépendances à des matériels, des logiciels et/ou des micrologiciels du système non fournis avec le produit (versions des logiciel(s), bibliothèque(s), matériel(s), etc.)*]

2.5 Description des bibliothèques tierces

[*A compléter par le rédacteur de la TOE : description des bibliothèques tierces sur lesquelles reposent la TOE. Il s'agit de lister les identifiants et versions de l'ensemble des librairies tierces intégrées au produit (bibliothèque(s) en source ouverte, COTS, etc.) et de justifier que ces dernières sont encore maintenues par leur développeur originel, s'il existe des versions plus récentes, et quels correctifs ou modifications ont été appliqués sur ces bibliothèques tierces.* [2]]

2.6 Description des utilisateurs typiques concernés

Pour des raisons de simplification, le terme « **utilisateur** » regroupe indifféremment les rôles listés.

L'association des utilisateurs avec la liste des tâches qu'ils sont autorisés à réaliser est donnée en Annexe A .

La TOE gère les utilisateurs [3] suivants :

- Opérateur d'exploitation ;
- Configurateur/développeur ;
- Administrateur ;
- Auditeur ;
- Super-administrateur ;

  [*A compléter par le rédacteur de la TOE : autres rôles si besoin*]

2.7 Description du périmètre de l'évaluation

L'évaluation concerne le serveur SCADA dans sa globalité. Les interfaces suivantes sont actives sur le produit soumis à l'évaluation et sont testées en robustesse :

[*A compléter par le rédacteur de la TOE : liste des interfaces actives et protocoles utilisés (compléter la liste des interfaces si besoin par exemple par des interfaces systèmes tels que USB, VGA, etc.)*]

Le périmètre de l'évaluation est représenté au chapitre 2.3.

[*A compléter par le rédacteur de la TOE : compléter la description du périmètre de l'évaluation si besoin*

2. Pour des contraintes de confidentialité cette liste sera annexée au profil de protection.
3. 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 distincts avec des profils d'utilisateur différents.

3 Description des hypothèses sur l'environnement

H1 Consultation des journaux
Il est considéré que les auditeurs consultent régulièrement ou accèdent automatiquement [4] aux journaux locaux ou déportés générés par la TOE.

H2 Utilisateurs légitimes
Les utilisateurs légitimes de la TOE sont compétents, formés et non hostiles.

H3 Administrateurs
Les administrateurs (et les super-administrateurs) de la TOE sont compétents, formés et non hostiles.

H4 Super-administrateurs
Les super-administrateurs de la TOE sont compétents, formés et non hostiles.

H5 Local
Deux cas de figure :

1. La TOE se trouve dans un local sécurisé dont l'accès est restreint à des personnes autorisées considérées comme non hostiles et l'attaquant ne peut pas avoir accès aux ports physiques de la TOE.
2. La TOE n'est pas dans un local sécurisé. Dans ce cas, la TOE est protégée par des mesures organisationnelles ou physiques.
   [A compléter par le rédacteur de la TOE : décrire ici les mesures organisationnelles ou physiques (détection et remontée(s) d'évènement(s) sur déconnexion d'un port Ethernet, mesures de vidéoprotection, etc.)]

On peut également noter que des équipements identiques à la TOE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement afin d'y rechercher des vulnérabilités par tous les moyens à sa disposition.

H6 Installation physique du système conforme
L'utilisateur s'assure que l'installation physique du système de la TOE respecte les règles d'installation fournies par le constructeur.

H7 Serveurs d'authentification
L'utilisateur s'assure que les serveurs d'authentification hors de la TOE utilisés pour authentifier les utilisateurs sont sains et configurés correctement.

H8 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.

H9 Documentation de sécurité
Les utilisateurs se conforment aux préconisations issues de la documentation de sécurité de la TOE.

H10 Module externe
L'utilisateur s'assure que les modules externes [5] considérés comme désactivés dans cette cible sont bien désactivés en pratique.

4. Un auditeur n'est pas forcément une personne physique et peut être un équipement terminal ou un programme ou système tiers.
5. Un module externe est un élément logiciel apportant de nouvelles fonctionnalités à la TOE mais qui n'est pas indispensable à son fonctionnement.

4 Description des biens sensibles

Les biens sensibles de la TOE sont les suivants :

B1 Flux avec la station d'ingénierie
Les flux entre la TOE et la station d'ingénierie doivent être protégés en intégrité et en authenticité (confidentialité de façon optionnelle).

B2 Flux vers un serveur d'historique
Les flux entre la TOE et le serveur d'historique doivent être protégés en Intégrité et en authenticité (confidentialité optionnelle).

B3 Flux de collaboration
Ils sont constitués de l'ensemble des flux entre la TOE et d'autres composants du système. Il s'agit par exemple des flux entre un frontal de communication et un autre serveur applicatif (SCADA, Historian, client(s) OPC, etc).

Les flux de données de collaboration doivent être protégés en intégrité et en authenticité (confidentialité optionnelle).

B4 Flux de données avec les équipements terrain
Les flux de données entre la TOE et les équipements de terrain (par exemple, les automates) doivent être protégés en authenticité et intégrité (confidentialité optionnelle).

B5 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, etc.

Elles peuvent être mises à disposition d'applications tierces (Extensions applicatives, MES, ERP, etc.) par la TOE au travers d'interfaces : API, SDK ou interfaces standard telles qu'OPC ou SNMP.

Ces données doivent être protégées en intégrité et authenticité. L'accès à ces données est régi par la politique de droit de la TOE.

B6 Flux du client lourd/léger avec le serveur
Tous les flux entre le client lourd/léger et le serveur applicatif doivent être protégés en confidentialité, intégrité et authenticité.

B7 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 à la mise à jour.

B8 Configuration
La configuration de la TOE doit être intègre (confidentialité optionnelle).

B9 Mécanisme d'authentification des utilisateurs
Ce mécanisme peut s'appuyer sur une base de données locale ou sur un connecteur avec un annuaire distant. Dans les deux cas, la TOE doit protéger l'intégrité et l'authenticité du mécanisme [6].

B10 Secrets de connexion des utilisateurs
Il peut s'agir de mots de passe, de certificats, etc. Ils peuvent être contenus localement à la TOE ou être échangés avec un serveur distant. Dans tous les cas, la TOE doit garantir l'intégrité et la confidentialité de ces secrets de connexion.

B11 Politique de gestion des droits
Cette politique peut être contenue en local sur la TOE ou être obtenue à partir d'un annuaire distant. Dans les deux cas, la TOE doit garantir l'intégrité de cette politique de gestion des droits.

6. Tous les mécanismes d'authentification présents dans la TOE ne doivent pas nécessairement être présents dans la cible de sécurité. Néanmoins, il doit y en avoir au moins un et ceux qui ne sont pas inclus doivent être désactivés par défaut.

B12 Fonction de journalisation locale
La TOE dispose d'une fonction de journalisation locale [7] qui, une fois configurée, doit rester opérationnelle (disponible).

B13 Fonction de journalisation déportée
La TOE dispose d'une fonction de journalisation déportée [8] qui, une fois configurée, doit rester opérationnelle (disponible).

B14 Journaux d'évènements locaux
Les journaux locaux générés par la TOE doivent être intègres et authentifiés.

B15 Journaux d'évènements déportés
L'émission du journal par la TOE lui permet d'être intègre et authentifiée. Un mécanisme doit également permettre au destinataire de détecter la perte d'un ou plusieurs messages au sein d'une séquence de messages correctement reçus.

[*A compléter par le rédacteur de la TOE : autres biens sensibles si besoin*]

		Disponibilité	Confidentialité	Intégrité	Authenticité
B1	Flux avec la station d'ingénierie		(✗)	✗	✗
B2	Flux vers un serveur d'historique		(✗)	✗	✗
B3	Flux de collaboration		(✗)	✗	✗
B4	Flux de données avec les équipements terrain		(✗)	✗	✗
B5	Données d'exploitation			✗	✗
B6	Flux du client lourd/léger avec le serveur		✗	✗	✗
B7	Logiciel(s)			✗	✗
B8	Configuration		(✗)	✗	
B9	Mécanisme d'authentification des utilisateurs			✗	✗
B10	Secrets de connexion des utilisateurs		✗	✗	
B11	Politique de gestion des droits			✗	
B12	Fonction de journalisation locale	✗			
B13	Fonction de journalisation déportée	✗			
B14	Journaux d'évènements locaux			✗	✗
B15	Journaux d'évènements déportés			✗	✗

✗ : obligatoire (✗) : optionnel

TABLE 1 – Biens sensibles de la TOE

7. Capacité à générer des évènements enregistrés dans des journaux, possibilité d'horodater ces évènements grâce à une source de temps commune et dimensionnement adéquat du stockage des journaux sur les équipements.
8. Capacité à générer des évènements enregistrés dans des journaux, possibilité d'horodater ces évènements grâce à une source de temps commune et à les transfèrer au travers du réseau sur un serveur du SI.

5 Description des menaces

5.1 Profils des attaquants

Les attaquants [9] à considérer pour l'évaluation sont :

- **Utilisateur malveillant**
  L'attaquant possède un compte sans privilège d'administration et cherche à outrepasser les droits de son compte **(vers un autre utilisateur non privilégié ou un compte administrateur)**. Ce compte peut avoir n'importe quel rôle à l'exception de ceux définis éventuellement en hypothèse au chapitre 3.
- **Attaquant dans le système industriel**
  Tout attaquant ayant pris le contrôle d'un composant du système industriel et cherchant à attaquer la TOE.

  [*A compléter par le rédacteur de la TOE : autres profils parmi les rôles listés au chapitre 2.6 si besoin*]

5.2 Menaces

Les menaces à considérer pour l'évaluation sont :

M1 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. Par exemple, envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu, perturbation, même temporairement, du changement de topologie en réponse à une panne d'un autre équipement. Ce déni de service peut concerner toute la TOE ou seulement certaines de ses fonctions.

M2 Altération des flux
L'attaquant parvient à modifier des échanges entre la TOE et un composant externe ou interne à celle-ci sans que cela ne soit détecté.

M3 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 ou interne à celle-ci.

M4 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.

M5 Corruption de la configuration
L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la TOE.

M6 Compromission de la configuration
L'attaquant parvient à récupérer tout ou partie de la configuration de la TOE de manière illégitime.

M7 Vol d'identifiants
L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

M8 Contournement de l'authentification
L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

M9 Contournement de la politique de droits
L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus. L'attaquant peut également tenter d'installer une version légitime du micrologiciel (*firmware*) sans en avoir le droit.

M10 Corruption des journaux d'évènements locaux
L'attaquant 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.

9. Sauf mention contraire, le terme « attaquant » regroupe l'ensemble des profils d'attaquants listés ci-dessous.

M11 Corruption des journaux d'évènements déportés
L'attaquant parvient à modifier une entrée de journal distant émise par la TOE sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte.

[*A compléter par le rédacteur de la TOE : autres menaces si besoin*]

6 Description des fonctions du produit

Deux types de fonctions composent la TOE. Les fonctions dites « métier » et les fonctions de sécurité. **Les fonctions « métier » ne sont pas évaluées en *conformité* dans le cadre de la CSPN. En revanche, l'évaluateur va vérifier la possibilité pour un attaquant d'utiliser l'une de ces fonctions pour compromettre un bien sensible**.

6.1 Fonctions métier

FM1 Acquisition des données terrain et envoi de commandes
La TOE peut comporter un frontal de communication prenant en charge les échanges avec les équipements de terrain tels que des automates programmables industriels, des contrôleurs, des IED [10], etc. (niveau 1 du modèle de PURDUE).

FM2 Échanges de données
La TOE peut envoyer et recevoir des flux d'information en s'appuyant sur des interfaces avec des systèmes tels qu'un serveur d'historiques, un MES, un serveur de paramétrage, une station d'ingénierie, des serveurs applicatifs SCADA, des postes clients, etc.

Ces systèmes peuvent se trouver sur le même niveau 2, sur le niveau 3 du modèle de PURDUE 3, ou même être déportés sur un réseau externe.

FM3 Gestion des alarmes procédé
La TOE détecte des conditions d'alarmes sur le procédé à partir des informations reçues des équipements de terrain et en assure le traitement et la transmission.

FM4 Interface homme-machine
La TOE intègre des fonctions d'interface homme-machine. Par exemple, dans le cas des alarmes, elle permet un affichage des états et la prise en compte de commandes (acquittement par exemple). Cette interface permet de visualiser le fonctionnement du procédé industriel.

FM5 Fonctions d'administration
La TOE comporte une ou plusieurs interfaces pour permettre son administration, notamment la gestion des utilisateurs et de la politique de droits.

FM6 Fonctions de configuration
La TOE comporte une ou plusieurs interfaces permettant d'assurer la mise à jour et le déploiement des données de configuration.

FM7 Traitement de données et scripting
La TOE peut assurer des fonctions de traitement et de calcul de variables dérivées.

FM8 Fonctions de redondance
La TOE peut permettre un fonctionnement en redondance pour assurer la haute disponibilité d'une ou plusieurs de ses fonctions.

FM9 Journalisation locale d'évènements
La TOE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration.

FM10 Journalisation distante d'évènements
La TOE permet de définir une politique de journalisation distante d'évènements notamment de sécurité et d'administration.

[*A compléter par le rédacteur de la TOE : autres fonctions métier*]

6.2 Fonctions de sécurité

FS1 Gestion des entrées malformées
La TOE gère correctement les entrées malformées en provenance du réseau, afin d'éviter qu'un attaquant puisse la positionner dans un état non souhaité pour l'exploiter (injection de code, etc.).

10. *Intelligent Electronic Device*, terme utilisé dans le domaine de l'énergie éléctrique qui regroupe tous les équipements d'automatisme ayant des fonctions de protection ou de pilotage local tels que les disjoncteurs, les transformateurs.

FS2 Communications sécurisées
La TOE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.

FS3 Connexion sécurisée avec le serveur d'authentification
La TOE permet une connexion sécurisée avec le serveur d'authentification en assurant l'authenticité des deux extrémités, l'intégrité et la confidentialité des échanges, ainsi que le non-rejeu.

FS4 Stockage sécurisé des secrets
Les secrets de connexion des utilisateurs sont stockés de manière sécurisée et la compromission d'un fichier ne permet pas de les récupérer.

FS5 Authentification sécurisée sur l'interface d'administration
La TOE identifie et authentifie les administrateurs avant d'accorder l'accès. Les jetons de session sont protégés contre le vol et contre le rejeu. Les jetons de session ont une durée de vie limitée et sont générés aléatoirement ou authentifiés [11]. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.

FS6 Gestion des autorisations
La TOE restreint les privilèges des utilisateurs comme décrit dans l'annexe A. 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.

FS7 Vérification de la signature du logiciel
Un mécanisme de vérification de signature est utilisé par la TOE pour s'assurer de l'authenticité et de l'intégrité des composants logiciels lors de leur installation et de leur exécution.

FS8 Intégrité et confidentialité de la configuration
La politique de gestion des utilisateurs interdit à une personne non autorisée de consulter ou modifier tout ou partie de la configuration de la TOE.

FS9 Intégrité des journaux
Les journaux d'événements générés par la TOE sont intègres et seul le super-administrateur peut les modifier.

FS10 Intégrité des journaux déportés
La TOE permet de transmettre les journaux à un équipement tiers de manière intègre, authentifiée, et sans rejeu des journaux générés avec détection des événements manquants.

[*A compléter par le rédacteur de la TOE : autres fonctions de sécurité si besoin*]

6.3 Fonctions désactivées

[*A compléter par le rédacteur de la TOE : description des fonctionnalités présentes sur la TOE mais désactivées*]
L'évaluateur vérifiera l'impossibilité pour un attaquant de pouvoir réactiver une fonction désactivée.

11. Selon le type de session web utilisée.

Annexe A Liste des tâches associées aux utilisateurs

Opérateur d'exploitation

- Consultation en lecture seule des données métiers disponibles sur la TOE.
- Écriture d'un ensemble limitée de données nécessaires au pilotage de la TOE.

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

Configurateur/développeur

- Configuration de l'application métier SCADA (développement, évolution ou correction)
- Gestion des licences, gestion de la base de données, etc.
- Définition de la politique de droits des utilisateurs (comptes, rôles, etc.).

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

Administrateur

- Gestion (création, import, export, destruction, etc.) des éléments cryptographiques de la TOE.

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

Auditeur

- Consultation des statistiques de fonctionnement de la TOE : [*A compléter par le rédacteur de la TOE : lister les statistiques*].
- Consultation des journaux d'évènements générés par la TOE.

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

Super-administrateur

- Gestion (création, import, export, destruction, etc.) des éléments cryptographiques de la TOE.
- Création des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Suppression des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Modification des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Consultation des attributs [*A compléter par le rédacteur de la TOE : liste des attributs*] des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

[*A compléter par le rédacteur de la TOE : autres rôles si besoin*]

[*A compléter par le rédacteur de la TOE : autres tâches définies dans la liste en Annexe C*]

Annexe B Matrices de couverture

B.1 Menaces et biens sensibles

		B1 Flux avec la station d'ingénierie	B2 Flux vers un serveur d'historique	B3 Flux de collaboration	B4 Flux de données avec les équipements terrain	B5 Données d'exploitation	B6 Flux du client lourd/léger avec le serveur	B7 Logiciel(s)	B8 Configuration	B9 Mécanisme d'authentification des utilisateurs	B10 Secrets de connexion des utilisateurs	B11 Politique de gestion des droits	B12 Fonction de journalisation locale	B13 Fonction de journalisation déportée	B14 Journaux d'évènements locaux	B15 Journaux d'évènements déportés
M1	**Déni de service**												**D**	**D**		
M2	**Altération des flux**	**(C) I A**	**(C) I A**	**(C) I A**	**(C) I A**	**I A**	**C I A**									
M3	**Compromission des flux**	**(C)**	**(C)**	**(C)**	**(C)**		**C**									
M4	**Corruption du logiciel**							**I A**								
M5	**Corruption de la configuration**								**I**							
M6	**Compromission de la configuration**								**(C)**							
M7	**Vol d'identifiants**										**C I**					
M8	**Contournement de l'authentification**									**I A**						
M9	**Contournement de la politique de droits**					**I A**						**I**				
M10	**Corruption des journaux d'évènements locaux**														**I A**	
M11	**Corruption des journaux d'évènements déportés**															**I A**

TABLE 2 – Atteintes aux biens sensibles en fonction des menaces

Légende : **D :** Disponibilité, **I :** Intégrité, **C :** Confidentialité, **A :** Authenticité - **(x) :** optionnel

B.2 Fonctions de sécurité

		M1 Déni de service	M2 Altération des flux	M3 Compromission des flux	M4 Corruption du logiciel	M5 Corruption de la configuration	M6 Compromission de la configuration	M7 Vol d'identifiants	M8 Contournement de l'authentification	M9 Contournement de la politique de droits	M10 Corruption des journaux d'événements locaux	M11 Corruption des journaux d'événements déportés
FS1	Gestion des entrées malformées	x										
FS2	Communications sécurisées		x	x								
FS3	Connexion sécurisée avec le serveur d'authentification								x			
FS4	Stockage sécurisé des secrets							x				
FS5	Authentification sécurisée sur l'interface d'administration					x	x	x	x			
FS6	Gestion des autorisations									x		
FS7	Vérification de la signature du logiciel				x							
FS8	Intégrité et confidentialité de la configuration					x	x					
FS9	Intégrité des journaux										x	
FS10	Intégrité des journaux déportés											x

TABLE 3 – Couverture des menaces par les fonctions de sécurité

Annexe C Liste des tâches

[*A préciser par le rédacteur de la TOE : une même tâche peut être affectée à plusieurs profils d'utilisateur. Cette annexe*[12] *est à supprimer une fois l'Annexe A complétée.*]

Configuration réseau

- Consultation de la configuration de l'interface d'administration
  - Adresses IP
  - Port / VLAN / Isolation des flux d'administration
  - ACL
- Edition de la configuration de l'interface d'administration
  - Adresses IP
  - Port / VLAN / Isolation des flux d'administration
  - ACL
- Consultation du cloisonnement logique
  - Séparation des flux métiers
  - Gestion des VLAN métiers, quarantaine, défaut, natif...
- Edition du cloisonnement logique
  - Séparation des flux métiers
  - Gestion des VLAN métiers, quarantaine, défaut, natif...
- Consultation de la configuration des ports de communication
  - Mode attribué aux ports (trunk, access, etc.).
  - Activation/désactivation des ports non utilisés.
- Edition de la configuration des ports de communication
  - Mode attribué aux ports (trunk, access, ...) ;
  - Activation/Désactivation des ports non utilisés.
- Consultation des fonctions de redondances niveau 2.
- Edition des fonctions de redondances niveau 2.
- Consultation de la configuration système (politique de sauvegarde, etc.).
- Edition de la configuration système (politique de sauvegarde, restauration de la Configuration, etc.).

Configuration de sécurité

- Consultation des mécanismes de sécurité (Port security, rate limit, Authentification du poste terminal, DAI, adresse MAC,etc.).
- Edition des mécanismes de sécurité (Port security, rate limit, Authentification du poste terminal, DAI, adresse MAC, etc.).
- Création des régles de filtrage.
- Modification des régles de filtrage.
- Suppression des régles de filtrage.
- Consultation des régles de filtrage.

Gestion des éléments cryptographiques

- Gestion (création, import, export, destruction, etc.) des éléments cryptographiques de la TOE.

12. Liste générique à tous les profils de protection

Version

- Consultation de la version de la TOE.
- Consultation de la version du système d'exploitation de la TOE.

Mise à jour du système

- Mise à jour du système d'exploitation de la TOE.

Mise à jour du micrologiciel (*firmware*)

- Mise à jour du (ou des) micrologiciel(s) (*firmware*) de la TOE.

Gestion du temps de référence

- Consultation du temps de référence de la TOE.
- Edition du temps de référence de la TOE.

Journaux d'évènements

- Configuration des journaux d'évènements (niveau de log, serveurs distants, rétention, etc.).
- Consultation des journaux d'évènements générés par la TOE.
- Suppression des journaux d'évènements générés par la TOE.

Gestion des utilisateurs

- Création des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Suppression des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Modification des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Consultation des attributs [*A compléter par le rédacteur de la TOE : liste des attributs*] des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].
- Edition des attributs [*A compléter par le rédacteur de la TOE : liste des attributs*] des comptes associés aux rôles [*A compléter par le rédacteur de la TOE : liste des rôles*].

Usager

- Utilisation du badge qui lui a été délivré pour accéder aux différentes zones protégées suivant ses droits d'accès

Configuration du superviseur SCADA

- Définition de la politique de droits des utilisateurs (comptes, rôles, etc.).
- Configuration de l'application métier SCADA (développement, évolution ou correction)
- Gestion des licences, gestion de la base de données, etc.

Arrêt et démarrage

- Arrêt de la TOE.
- Démarrage de la TOE.
- Redémarrage de la TOE.

Comptes administrateur

- Création ou modification des comptes administrateur de la TOE.

Contrôle complet hormis les données cryptographiques et les comptes administrateurs

- Toutes les tâches affectées à la TOE hormis la création ou modification des données cryptographiques de la TOE et la création ou modification de comptes administrateurs.

Écriture limitée

- Écriture d'un ensemble limitée de données nécessaires au pilotage de la TOE.

Consultation des données métiers

- Consultation en lecture seule des données métiers disponibles sur la TOE.

Supervision du fonctionnement

- Consultation des statistiques de fonctionnement de la TOE : [*A compléter par le rédacteur de la TOE : lister les statistiques*].

Maintien en conditions opérationnelles du centre de gestion des contrôles d'accès

- Maintien en conditions opérationnelles du centre de gestion des contrôles d'accès.

Maintien en conditions de sécurité du centre de gestion des contrôles d'accès

- Maintien en conditions de sécurité du centre de gestion des contrôles d'accès.

Intégration de nouveaux dispositifs de contrôle d'accès dans le réseau

- Intégration de nouveaux dispositifs de contrôle d'accès dans le réseau.

Intégration de nouveaux dispositifs de contrôle d'accès dans le centre de gestion des contrôles d'accès.

- Intégration de nouveaux dispositifs de contrôle d'accès dans le centre de gestion des contrôles d'accès.

Consultation de l'historique d'accès des porteurs de badge.

- Consultation de l'historique d'accès des porteurs de badge.

Ajout, suppression et modification des droits d'accès des porteurs de badge.

- Ajout, suppression et modification des droits d'accès des porteurs de badge.
- Ajout, suppression et modification des droits d'accès aux caméras.

Affectation des droits d'accès des porteurs de badge sur les ouvrants.

- Mise à jour des droits d'accès des porteurs de badge dans le système.
- Affectation des droits d'accès des porteurs de badge sur les ouvrants.

Déploiement et maintenance des équipements de contrôle d'accès (unité de traitement local et lecteur de badge).

- Déploiement et maintenance des équipements de contrôle d'accès (unité de traitement local et lecteur de badge).

Équipement terminal

- Néant

Maintien en conditions opérationnelles du centre de gestion vidéo.

- Maintien en conditions opérationnelles du centre de gestion vidéo.

Maintien en conditions de sécurité du centre de gestion vidéo.

- Maintien en conditions de sécurité du centre de gestion vidéo.

Intégration de nouveaux dispositifs dans le système.

- Intégration de nouveaux dispositifs de vidéo IP dans le réseau.

Déploiement des caméras.

- Déploiement des caméras.

Maintenance des caméras.

- Maintenance des caméras.

Traitement des événements.

- Traitement des événements.

Visualisation en direct ou a posteriori des vidéos.

- Visualisation en direct ou à posteriori des vidéos.

[*A compléter par le rédacteur de la TOE : autres tâches si besoin*]

Annexe D Liste des contributeurs

La version de ce profil de protection a été rédigé avec le concours des sociétés et organismes suivants :

- Amossys
- ARC Informatique
- Areal
- Codra
- DGA/MI
- EDF
- Gimelec
- Oppida
- Ordinal Software (représentant le club MES)
- RATP
- Schneider Electric
- Siemens
- Sogeti
- Stormshield
- Thales