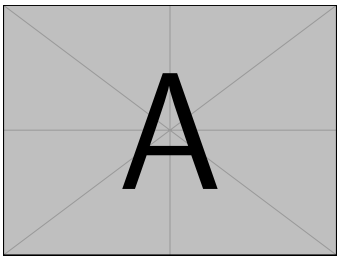
[AFFECTATION : NOM DE L'ÉDITEUR]
[AFFECTATION : NOM DU PRODUIT]

Automate programmable industriel
Modèle de cible de sécurité

Version 1.2 court-terme

GTCSI



14 juin 2023

Table des matières

Avant-propos

Ce document doit être instancié ou complété par l'utilisateur (industriel ou commanditaire du visa de sécurité).
Les passages en rouge sont ceux qui diffèrent de la version de la cible à moyen terme.

La cible moyen terme a un objectif de sécurité plus ambitieux intégrant, entre autres, l'intégrité des journaux distants.

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	Automate programmable industriel

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

SD
: Secure digital

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://www.ssi.gouv.fr`
[R2]	Recommandations relatives à l'administration sécurisée des systèmes d'information, n° DAT-NT-22/ANSS/SDE/NP. Disponible sur `https://www.ssi.gouv.fr`
[R3]	Guide de sélection d'algorithmes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version en vigueur. Disponible sur `https://www.ssi.gouv.fr`

2 Description du produit

2.1 Description générale du produit

Un automate programmable industriel (API) ou Programmable logic controller (PLC) en anglais, est un équipement conçu pour commander un processus industriel. Il est pour cela connecté au système physique par des entrées et des sorties, respectivement reliées aux capteurs (pression, position, température) et aux actionneurs (verins, moteurs, pompes). La connexion à ces entrées/sorties peut être réalisée soit directement via des contacts électriques, soit par l'utilisation d'un module d'entrées/sorties déporté. L'automate communique avec des serveurs de supervisions (SCADA) et peut communiquer avec d'autre(s) automate(s) ou des entrées/sorties déportées.

Types d'automate En plus des modèles standard, un API peut se décliner sous différentes formes pour répondre à des contraintes fonctionnelles spécifiques. On retrouve de ce fait :

- des automates en redondance, permettant d'améliorer la disponibilité des installations ;
- des automates de sûreté, permettant d'assurer la protection des biens et des personnes (sécurité fonctionnelle). Utilisés pour assurer la sûreté de fonctionnement, l'objectif est de positionner le système dans un état sûr en cas de détection d'une situation dangereuse sur la fonction « métier » (dysfonctionnement ou perte d'un équipement, état du système anormal, etc.).

Si les fonctionnalités de l'automate peuvent être étendues par l'ajout de modules complémentaires (communication, borniers d'entrées/sorties), il est dit modulaire et les différents éléments communiquent via un bus de communication dit de fond de panier. Dans le cas contraire, il est dit compact, et sa connectivité est figée pour le modèle concerné. Si des modules additionels sont utilisés pour augmenter la connectivité de l'automate, les fonctionnalités apportées devront être couvertes par l'ajout d'exigences correspondantes, tirées de profils de protections si ces derniers existent.

Un API répond à des contraintes matérielles strictes et se doit de fonctionner dans des environnements hostiles. Ces conditions peuvent se caractériser par des températures ou des niveaux d'humidité inhabituels pour des équipements informatiques ou par la présence de poussières, de composés explosifs ou encore de fortes vibrations. Cela implique des performances de calcul et une quantité de mémoire limitée (étant intégrée dans des boîtiers ne permettant pas de refroidissement mécanique).

2.2 Description de la manière d'utiliser le produit

La mise en œuvre d'un système industriel étant spécifique à chaque situation (géographique, métier, etc.), un API peut être utilisé dans différentes configurations d'architectures. Il se détache cependant un cadre d'utilisation classique qui sera pris comme référence dans ce profil et illustré en figure 1.

L'administration de l'API est réalisée avec une station d'ingénierie. Les modifications du micrologiciel (*firmware*) et de la configuration peuvent être généralement effectuées au travers d'un réseau, d'une interface USB ou à l'aide de supports amovibles (carte SD ou clés USB par exemple).

Dans le cas d'une administration de l'API par le réseau, il est recommandé que ce dernier soit dédié (physiquement ou logiquement). Ce réseau d'administration est également utilisé pour la configuration du système SCADA ainsi que par le poste d'audit. Il est également recommandé que la station d'ingénierie ne soit pas branchée en permanence mais uniquement en cas de besoin.

Il est recommandé de séparer le réseau terrain (I1), réalisant le contrôle du procédé physique aux autres réseaux (I2 à I4).

Dans le cas d'interconnexion(s) avec d'autre(s) automate(s) (I4), la communication peut transiter par une interface dont l'usage correspond à la nature de ces échanges afin de garder le cloisonnement entre réseau de terrain et de supervision.

2.3 Description de l'environnement prévu pour son utilisation

[***A compléter par le rédacteur de la TOE : ce schéma est à refaire***]

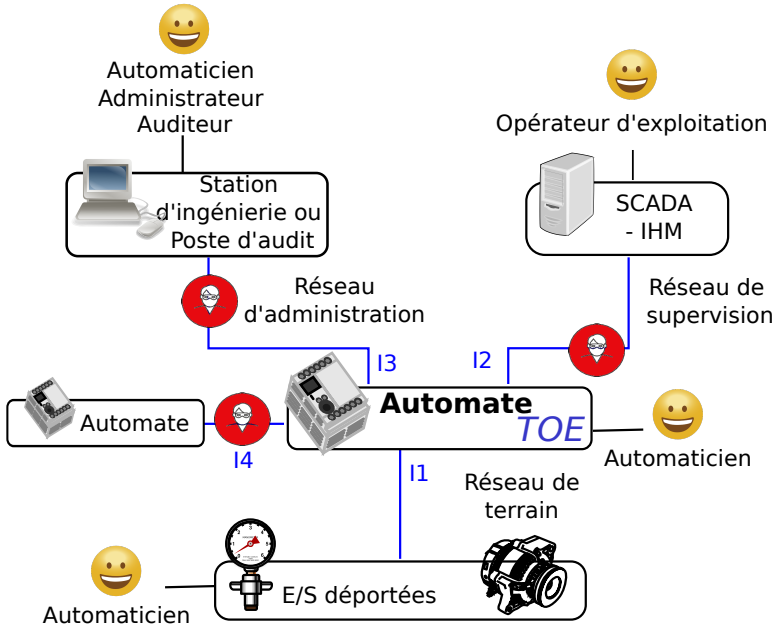


FIGURE 1 – Interfaces de communications virtuelles de la TOE et présence de l'attaquant

Légende : Attaquant

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

- **I1.** Interface de communication avec le réseau de terrain lorsque celles-ci sont déportées. Cette connexion constitue le réseau terrain sur lequel transitent les flux de contrôles et de commandes de l'installation.
- **I2.** Interface de communication dédiée à la supervision métier. Cette interface peut être connectée à un poste de maintenance locale (pupitre ou IHM locale) ainsi qu'à une station de supervision métier plus globale : le SCADA.
- **I3.** Interface de communication avec le réseau d'administration et de maintenance de l'automate industriel vers une station d'ingénierie ou un système de configuration centralisé. Les modifications du micrologiciel *firmware*, du programme de l'automate ou son paramétrage, sont transférés sur ce réseau. Le poste d'audit est également raccordé sur cette interface au travers du réseau d'administration. Sur certaines architectures plus anciennes, ce peut être une interface de type série ou une interface vers un périphérique amovible (USB, carte SD, etc.).
- **I4.** Interface de raccordement vers un ou plusieurs autre(s) automate(s). Cette interface est utilisée pour la synchronisation des traitements distribués entre différents automates ou lorsque l'automate est utilisé en redondance avec un second équipement.

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 composants tiers intégrés au produit (bibliothèque(s) en source ouverte, COTS, etc.) et de justifier que ces derniers sont encore maintenus par leur développeur originel, s'il existe des versions plus récentes, et quels correctifs ou modifications ont été appliqués sur ces composants tiers.* [1]]

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 [2] suivants :

- Opérateur d'exploitation ;
- Administrateur ;
- Auditeur ;
- Super-administrateur ;
- Automaticien ;

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

2.7 Description du périmètre de l'évaluation

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

[*A compléter par le rédacteur de la TOE : liste des interfaces actives et protocoles utilisées (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*]

1. Pour des contraintes de confidentialité cette liste sera annexée au profil de protection.
2. 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 [3] aux journaux locaux ou déportés générés par la TOE.

H2 Administrateurs
Les administrateurs (et les super-administrateurs) de la TOE sont compétents, formés et non hostiles.

H3 Local
La TOE n'est pas nécessairement dans un local sécurisé et l'attaquant peut avoir accès à ses ports. En particulier, l'attaquant aura accès aux ports physiques de la TOE (par exemple une clé USB ou une carte SD) pour une courte durée. En revanche, il ne peut ni démonter, modifier ou effectuer d'attaque physique sur la TOE (soudure, etc.) ;

Deux cas de figure :

1. la TOE est protégée par des mesures organisationnelles.
   [A compléter par le rédacteur de la TOE : décrire ici les mesures (local sécurisé, coffret fermé avec détection et remontée(s) d'évènement(s) sur ouverture de ce dernier, mesures de vidéoprotection, etc.)]
2. aucun coffret sécurisé : une protection physique de l'équipement est mise en place.
   [L'évaluateur mesurera la résistance de l'équipement à une attaque physique : accès au JTAG, effacement des secrets lors de l'ouverture de l'équipement, etc. Le degré de résistance nécessaire pour obtenir la CSPN sera cependant variable selon le degré de protection organisationnel offert par cette hypothèse.]

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.

H4 Documentation de sécurité
Les utilisateurs se conforment aux préconisations issues de la documentation de sécurité de la TOE.

3. Un auditeur n'est pas forcément une personne physique et peut être un équipement terminal ou un programme ou système tiers.

4 Description des biens sensibles

Les biens sensibles de la TOE sont les suivants :

B1 Commande du procédé industriel
La TOE participe à la commande et au contrôle d'un processus industriel en lisant des entrées et en envoyant des ordres aux actionneurs. Ces actions doivent être protégées en disponibilité et en intégrité.

B2 Échanges entre la TOE et la supervision
Les échanges entre la supervision (SCADA) et la TOE sont nécessaires au bon fonctionnement du système industriel dans son ensemble et doivent être intègres et authentiques (confidentialité de façon optionnelle).

B3 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).

B4 Micrologiciel (*firmware*)
Afin d'assurer correctement ses fonctions, le micrologiciel (*firmware*) de la TOE doit être intègre et authentique.

B5 Programme utilisateur
La TOE exécute un programme écrit et chargé par l'utilisateur et décrivant son fonctionnement. Il doit être protégé en confidentialité [4] , en intégrité et en authenticité.

B6 Configuration
La configuration de la TOE doit être confidentielle et intègre. L'attaquant ne doit pas pouvoir découvrir cette configuration autrement que par l'observation de l'activité de la TOE (observation de l'état des organes « terrain »).

B7 Mode de fonctionnement de la TOE
Le mode de fonctionnement de la TOE (run ou stop par exemple) doit être protégé en intégrité et authenticité.

B8 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 [5].

B9 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.

B10 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.

B11 Fonction de journalisation locale
La TOE dispose d'une fonction de journalisation locale [6] qui, une fois configurée, doit rester opérationnelle.

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

4. La confidentialité n'est pas primordiale pour protéger un système industriel, il s'agit d'une mesure de défense en profondeur. Cette propriété peut également être recherchée à des fins de protection du secret industriel.

5. 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.

6. 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.

7. 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.

B13 Journaux d'évènements locaux
Les journaux locaux générés par la TOE doivent être intègres et authentifiés.

B14 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	Commande du procédé industriel	✗		✗	
B2	Échanges entre la TOE et la supervision		(✗)	✗	✗
B3	Flux avec la station d'ingénierie		(✗)	✗	✗
B4	Micrologiciel (*firmware*)			✗	✗
B5	Programme utilisateur		(✗)	✗	✗
B6	Configuration		(✗)	✗	
B7	Mode de fonctionnement de la TOE			✗	
B8	Mécanisme d'authentification des utilisateurs			✗	✗
B9	Secrets de connexion des utilisateurs		✗	✗	
B10	Politique de gestion des droits			✗	
B11	Fonction de journalisation locale	✗			
B12	Fonction de journalisation déportée	✗			
B13	Journaux d'évènements locaux			✗	✗
B14	Journaux d'évènements déportés			✗	✗

✗ : obligatoire (✗) : optionnel

TABLE 1 – Biens sensibles de la TOE

5 Description des menaces

5.1 Profils des attaquants

Les attaquants [8] à considérer pour l'évaluation sont :

- **Attaquant présent sur le réseau de supervision**
  L'attaquant a la maîtrise d'un équipement sur le réseau de supervision de l'automate.
- **Attaquant présent sur le réseau d'administration**
  Un équipement présent sur le réseau d'administration de la TOE est contrôlé par l'attaquant sans que ce dernier ne dispose nécessairement d'identifiants d'authentification valides auprès de la TOE.
- **Utilisateur malveillant**
  L'attaquant possède un compte sans droits d'administration et cherche à outrepasser les droits de son compte (vers un autre utilisateur non privilégié ou un compte administrateur).

  [*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 Corruption du micrologiciel (*firmware*)
L'attaquant parvient à injecter et faire exécuter un micrologiciel (*firmware*) corrompu sur la TOE. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.

L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans la TOE par des moyens légitimes.

M3 Corruption du mode de fonctionnement
L'attaquant parvient à modifier le mode de fonctionnement de la TOE sans en avoir le droit (envoi d'une commande stop par exemple) ;

M4 Compromission du programme utilisateur
L'attaquant parvient à récupérer tout ou partie de la configuration de la TOE par d'autres moyens que l'observation de l'activité de la TOE [9].

M5 Corruption du programme utilisateur
L'attaquant parvient à modifier, de façon temporaire ou permanente, le programme utilisateur de la TOE.

M6 Corruption de la configuration
L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la TOE.

M7 Compromission de la configuration
L'attaquant parvient à récupérer tout ou partie de la configuration de la TOE de manière illégitime.

M8 Vol d'identifiants
L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

8. Sauf mention contraire, le terme « attaquant » regroupe l'ensemble des profils d'attaquants listés ci-dessous.
9. Cette menace n'est considérée que lorsque la confidentialité du programme utilisateur est un besoin de sécurité identifié.

M9 Contournement de l'authentification
L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

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.

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.

M12 Injection de commandes ou paramètres
L'attaquant parvient à modifier des paramètres à l'intérieur de la TOE ou de lui passer des commandes sans y être autorisé.

M13 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.

M14 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.

M15 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.

[*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 Exécution d'un programme automate
La TOE exécute un programme fourni par l'utilisateur. Ce programme lit les entrées de la TOE, effectue son traitement et met à jour ses sorties.

FM2 Gestion des entrées/sorties
La TOE est capable de communiquer pour lire ou écrire sur des entrées/sorties déportées ou non. Ces entrées/sorties peuvent être numériques, analogiques ou de type « tout ou rien ». Elles permettent à la TOE de contrôler et de commander le processus industriel.

FM3 Communication avec la supervision métier
La TOE peut communiquer avec la supervision (SCADA) pour recevoir des ordres et remonter des informations sur le processus industriel.

FM4 Fonctions d'administration
La TOE dispose de fonctions permettant de configurer ou, dans certains cas, de programmer l'ensemble des autres fonctionnalités. Différentes interfaces d'administration sont envisageables :

- des clients lourds (appelés également, en fonction du contexte, consoles d'administration, de programmation ou de configuration),
- des clients légers comme des clients web,
- des supports amovibles (cartes SD, clés USB, etc.).

FM5 Journalisation locale d'évènements
La TOE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration.

FM6 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.).

FS2 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.

FS3 Authentification sécurisée sur l'interface d'administration
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 [10]. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.

FS4 Politique de droits
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.

10. Selon le type de session web utilisée.

FS5 Signature du micrologiciel (*firmware*)
À chaque installation d'un nouveau micrologiciel (*firmware*), l'intégrité et l'authenticité de celui-ci est vérifiée. L'intégrité et l'authenticité sont également vérifiées au chargement du micrologiciel (*firmware*) lors du démarrage de l'équipement.

FS6 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.

FS7 Authenticité, intégrité du programme utilisateur
La TOE doit pouvoir protéger le programme utilisateur de façon à ce que seuls les utilisateurs autorisés puissent modifier celui-ci.

FS8 Confidentialité du programme utilisateur
La TOE assure la confidentialité du programme utilisateur de telle sorte que seuls les utilisateurs autorisés y aient accès.

FS9 Authenticité et intégrité des commandes du mode de fonctionnement
La TOE doit garantir que le mode de fonctionnement ne pourra être modifié que par des personnels autorisés et donc authentifiés.

FS10 Communications sécurisées
La TOE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.

FS11 Intégrité des journaux
Les journaux d'événements générés par la TOE sont intègres et seul le super-administrateur peut les modifier.

FS12 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*]

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 nécessaire au pilotage de la TOE.

[*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 ou modification des comptes administrateur de la TOE.

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

Automaticien

- 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.

[*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 Commande du procédé industriel	B2 Échanges entre la TOE et la supervision	B3 Flux avec la station d'ingénierie	B4 Micrologiciel (*firmware*)	B5 Programme utilisateur	B6 Configuration	B7 Mode de fonctionnement de la TOE	B8 Mécanisme d'authentification des utilisateurs	B9 Secrets de connexion des utilisateurs	B10 Politique de gestion des droits	B11 Fonction de journalisation locale	B12 Fonction de journalisation déportée	B13 Journaux d'évènements locaux	B14 Journaux d'évènements déportés
M1	**Déni de service**	**D**										**D**	**D**		
M2	**Corruption du micrologiciel (*firmware*)**				**I A**										
M3	**Corruption du mode de fonctionnement**							**I**							
M4	**Compromission du programme utilisateur**					**(C)**									
M5	**Corruption du programme utilisateur**	**I**				**I A**									
M6	**Corruption de la configuration**						**I**								
M7	**Compromission de la configuration**						**(C)**								
M8	**Vol d'identifiants**									**C I**					
M9	**Contournement de l'authentification**								**I A**						
M10	**Corruption des journaux d'évènements locaux**													**I A**	
M11	**Corruption des journaux d'évènements déportés**														**I A**
M12	**Injection de commandes ou paramètres**	**D I**	**I A**												
M13	**Contournement de la politique de droits**										**I**				
M14	**Altération des flux**	**D I**	**(C) I A**	**I A**											
M15	**Compromission des flux**			**(C)**											

TABLE 2 – Atteintes aux biens sensibles en fonction des menaces

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

B.2 Fonctions de sécurité

		M1 Déni de service	M2 Corruption du micrologiciel (*firmware*)	M3 Corruption du mode de fonctionnement	M4 Compromission du programme utilisateur	M5 Corruption du programme utilisateur	M6 Corruption de la configuration	M7 Compromission de la configuration	M8 Vol d'identifiants	M9 Contournement de l'authentification	M10 Corruption des journaux d'événements locaux	M11 Corruption des journaux d'événements déportés	M12 Injection de commandes ou paramètres	M13 Contournement de la politique de droits	M14 Altération des flux	M15 Compromission des flux
FS1	Gestion des entrées malformées	X														
FS2	Stockage sécurisé des secrets								X							
FS3	Authentification sécurisée sur l'interface d'administration						X	X	X	X						
FS4	Politique de droits													X		
FS5	Signature du micrologiciel (*firmware*)		X													
FS6	Intégrité et confidentialité de la configuration						X	X								
FS7	Authenticité, intégrité du programme utilisateur					X										
FS8	Confidentialité du programme utilisateur				X											
FS9	Authenticité et intégrité des commandes du mode de fonctionnement			X												
FS10	Communications sécurisées												X		X	X
FS11	Intégrité des journaux										X					
FS12	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 est à supprimer une fois l'Annexe A complétée.*]

Configuration réseau

- Consultation de la configuration de l'interface d'admin
  - 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.

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*)

- Met à jour les micrologiciels (*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

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 nécessaire 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.

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.

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

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

Annexe D Liste des contributeurs

La version 1.2 de ce profil de protection a été rédigé avec le concours des sociétés et organismes suivants :

- Amossys
- ARC Informatique
- Belden
- DGA/MI
- Gimelec
- Oppida
- Phoenix Contact
- RATP
- Schneider Electric
- Siemens
- Sogeti
- Stormshield
- Thales