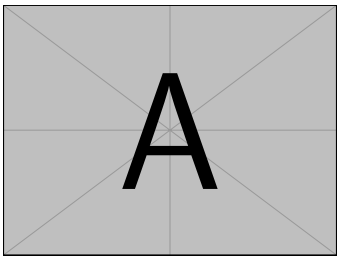
[AFFECTATION : NOM DE L'ÉDITEUR]
[AFFECTATION : NOM DU PRODUIT]

Système de contrôle d'accès physique
Modèle de cible de sécurité

Version 1.1 court-terme

GTCSI



21 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	Système de contrôle d'accès physique

1.3 Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

COTS
Commercial off-the-shelf

GAC
Centre de gestion des contrôles d'accès

OSI
Open Systems Interconnection model

SAM
Secure access module

SCADA
Système d'acquisition et de contrôle de données

SD
Secure digital

TOE
Target of evaluation

USB
Bus série universel

UTL
Unité de traitement local

VLAN
Réseau local virtuel

VMS
Centre de gestion vidéo

1.4 Documents applicables

Référence	Document
[R1]	Guide de recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de videoprotection. Disponible sur `https://www.ssi.gouv.fr/`

2 Description du produit

2.1 Description générale du produit

La TOE considérée dans ce profil de protection est un système de contrôle d'accès physique qui est un dispositif ayant pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local. Il est constitué de moyens permettant d'autoriser les entrées et sorties de zones contrôlées aux seules personnes qui ont le droit d'y accéder.

Un système de contrôle d'accès physique assure quatre fonctions primaires :

- l'identification et l'authentification ;
- le traitement des données ;
- le déverrouillage ;
- la tracabilité des passages.

Ces fonctions sont assurées en chaque point où l'accès est contrôlé. Dans le cas d'un système de contrôle d'accès utilisant des technologies sans contact, quatre éléments supports principaux interviennent :

- le badge ;
- le lecteur (tête de lecture) ;
- l'unité de traitement local (désignée par UTL, également connue sous le nom d'unité de traitement et de contrôle) ;
- le centre de gestion des contrôles d'accès (GAC). Il inclut les éléments suivants :
  - — un logiciel de gestion du système, qui communique avec les UTL,
  - — des ressources de type base de données ou annuaire, qui permettent de gérer les données essentielles au système, comme les droits, utilisateurs, groupes, ou encore identifiants de badges. Ces ressources peuvent appartenir à un système d'information extérieur à la TOE.

2.2 Description de la manière d'utiliser le produit

Le fonctionnement d'un système de contrôle d'accès physique est géré par le centre de gestion des contrôles d'accès (GAC). Ce centre est une infrastructure centralisée assurant les fonctions suivantes :

- la centralisation des journaux d'événements ;
- l'affichage et la notification des événements à l'opérateur ;
- l'hébergement et la mise à jour de la base de données centrale (droits, utilisateurs, groupes, identifiants de badge, etc.) ;
- le pilotage de l'ensemble des UTL ainsi que la transmission périodique de la base de données nécessaire au traitement local des demandes d'accès.

A l'usage, trois phases sont identifiables dans le fonctionnement d'un système de contrôle d'accès physique :

- l'identification et l'authentification. Cette phase inclut l'identification, l'authentification du badge et éventuellement l'authentification du porteur ;
- le traitement des demandes d'accès. Celui-ci est assuré en premier lieu par l'UTL. Cette unité assure la gestion de toutes les demandes d'accès en provenance des têtes de lecture qui lui sont rattachées, analyse ces demandes vis-à-vis d'un ensemble de droits d'accès stocké dans sa base de données locale et délivre les commandes de déverrouillage. En deuxième lieu le GAC peut assurer cette gestion dans le cas où il est fait usage de fonctionnalités qui nécessitent une vue d'ensemble du système (anti pass-back physique, etc.) ;
- le verrouillage et le déverrouillage. Le dispositif de verrouillage permet de réaliser le blocage mécanique d'un point d'accès pour empêcher le passage des personnes non autorisées. Le contrôle d'accès permet le déverrouillage.

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 refaire***]

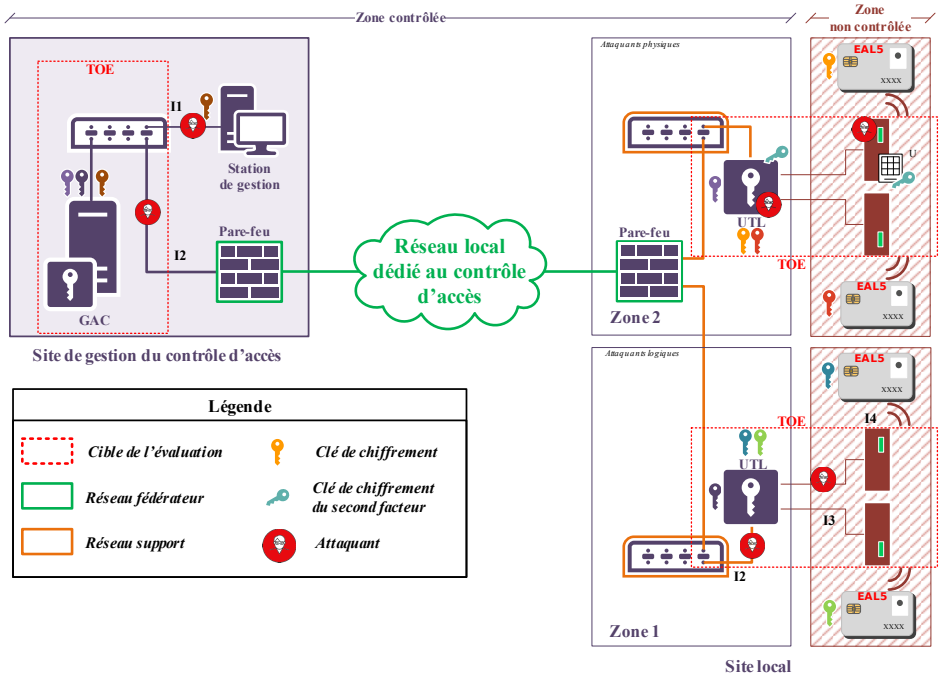


FIGURE 1 – Architecture type d'un réseau de contrôle d'accès

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

- **I1** : Interface de raccordement du serveur de gestion des contrôles d"accès (GAC) à la station de gestion ;
- **I2** : Interface de raccordement du serveur de gestion des contrôles d'accès (GAC) à l'unité de traitement local (UTL) ;
- **I3** : Interface de raccordement de l'unité de traitement local (UTL) au lecteur de badge ;
- **I4** : Interface sans contact entre le lecteur de badge et le badge.

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.*[1]]

1. Pour des contraintes de confidentialité cette liste sera annexée au profil de protection.

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 :

- Super-administrateur ;
- Administrateur technique ;
- Administrateur métier ;
- Opérateur du GAC ;
- Opérateur d'exploitation des journaux d'évènements des systèmes ;
- Mainteneur de matériel physique ;
- Porteur de badge ou usager ;

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

2.7 Description du périmètre de l'évaluation

L'évaluation concerne les éléments du système de contrôle d'accès physique listés ci-dessous :

- le GAC :
  - système d'exploitation ;
  - applicatifs ;
  - fonctions cryptographiques ;
  - base de données et annuaires.
- les UTL :
  - système d'exploitation ;
  - applicatifs ;
  - fonctions cryptographiques ;
  - SAM .
- les lecteurs de badges :
  - lecteurs simples ;
  - lecteurs-clavier.

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. 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 Badges évalués
L'utilisateur s'assure que les badges, ainsi que leur interface radio, ont déjà été évalués a minima critères communs EAL5. Dans ce cas les badges seront considérés comme sûrs.

H2 Module externe
L'utilisateur s'assure que les modules externes [3] considérés comme désactivés dans cette cible sont bien désactivés en pratique.

H3 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.

H4 Bases de données saines
L'utilisateur s'assure que les bases de données hors de la TOE sont saines et les informations contenues sont correctes.

H5 Documentation de sécurité
Les utilisateurs se conforment aux préconisations issues de la documentation de sécurité de la TOE.

H6 Administrateurs
Les administrateurs techniques et métiers de la TOE sont compétents, formés et non hostiles.

H7 Super-administrateurs
Les super-administrateurs de la TOE sont compétents, formés et non hostiles.

H8 Consultation des journaux
Il est considéré que les opérateurs d'exploitation des journaux d'évènements des systèmes consultent régulièrement ou accèdent automatiquement aux journaux locaux ou déportés générés par la TOE.

H9 Système d'exploitation du centre de gestion vidéo sain
Le système d'exploitation, hors TOE, portant le VMS est considéré comme sain au début et tout au long de l'évaluation sauf en cas de défaillance du VMS.

H10 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.

H11 Local
L'UTL 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 l'UTL (par exemple une clé USB ou une carte SD) pour une courte durée. En revanche, il ne peut ni modifier ni effectuer d'attaque physique sur l'UTL (soudure, etc.) ;

Deux cas de figure :

1. l'UTL 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.

3. 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 Droit d'accès des porteurs de badge
Les droits d'accès des porteurs de badge sont constitués de l'ensemble des informations permettant de vérifier qu'un porteur possède les autorisations d'accès à une zone. Selon ces droits, l'action de badger peut mener à l'autorisation d'accès ou non à la zone concernée. La TOE doit maintenir une cohérence de ses droits à l'échelle du système. Ces droits doivent être protégés en confidentialité et en intégrité.

B2 Données d'exploitation du système de contrôle d'accès physique
Les données d'exploitation sont constituées de l'ensemble des informations utiles au bon fonctionnement du système de contrôle d'accès 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, SI RH, etc.) par la TOE au travers d'interfaces de programmation. Ces données doivent être protégées en intégrité et authenticité. L'accès à ces données est régi par la politique de droit de la TOE.

B3 Échanges entre les UTL et le GAC
Le GAC pilote les UTL et assure une transmission périodique de la base de données nécessaire au traitement local des demandes d'accès. Ces flux doivent être protégées en confidentialité, en intégrité et en authenticité.

B4 Échanges entre le lecteur de badge et l'UTL
Les UTL assurent la gestion de toutes les demandes d'accès en provenance des têtes de lecture qui lui sont rattachées. Les flux entre les UTL et les têtes de lecture doivent être protégées en confidentialité, en intégrité et en authenticité.

B5 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 [4].

B6 Secrets de connexion
Il peut s'agir de mots de passe, de clés, de certificats (format intégrant la clef privée), 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.

B7 Micrologiciel (*firmware*)
Afin d'assurer correctement ses fonctions, le micrologiciel (*firmware*) de la TOE doit être intègre et authentique.

B8 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.

B9 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.

B10 Fonction de journalisation locale
La TOE dispose d'une fonction de journalisation locale [5] qui, une fois configurée, doit rester opérationnelle (disponible).

4. 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.

5. 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.

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

B12 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.

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

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

		Disponibilité	Confidentialité	Intégrité	Authenticité
B1	Droit d'accès des porteurs de badge		✗	✗	
B2	Données d'exploitation du système de contrôle d'accès physique		(✗)	✗	✗
B3	Échanges entre les UTL et le GAC		✗	✗	✗
B4	Échanges entre le lecteur de badge et l'UTL		✗	✗	✗
B5	Mécanisme d'authentification des utilisateurs			✗	✗
B6	Secrets de connexion		✗	✗	
B7	Micrologiciel (*firmware*)			✗	✗
B8	Logiciel(s)			✗	✗
B9	Politique de gestion des droits			✗	
B10	Fonction de journalisation locale	✗			
B11	Fonction de journalisation déportée	✗			
B12	Journaux d'évènements déportés		(✗)	✗	✗
B13	Journaux d'évènements locaux		(✗)	✗	✗

✗ : obligatoire (✗) : optionnel

TABLE 1 – Biens sensibles de la TOE

6. 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 [7] à considérer pour l'évaluation sont :

- **Attaquant à l'extérieur du bâtiment protégé**
  Attaquant ayant accès uniquement au lecteur de badge et au badge situé dans une zone non protégée.
- **Attaquant ayant accès à l'UTL** [8]
  Attaquant ayant accès à l'UTL.
- **Attaquant ayant la main sur le réseau du centre de gestion des contrôles d'accès**
  Attaquant se situant sur le réseau du centre de gestion des contrôles d'accès (GAC).
- **Attaquant ayant la main sur le réseau support** [9]
  Attaquant se situant sur le réseau support.
- **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 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.

M4 Vol d'identifiants
L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

M5 Contournement de l'authentification
L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

M6 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.

7. Sauf mention contraire, le terme « attaquant » regroupe l'ensemble des profils d'attaquants listés ci-dessous.
8. Dans le cadre de la certification, la cotation doit donc prendre en compte l'effort requis pour accéder aux UTL, mais les attaques physiques ne sont pas exclues par principe.
9. Un réseau support désigne les équipements de niveau 2 et inférieur (modèle OSI) sur lesquels sont connectés des UTL.

M7 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.

M8 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.

M9 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.

M10 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.

M11 Corruption de données
L'attaquant parvient à modifier des données, sans en avoir le droit, en exploitant une faille de la TOE.

M12 Compromission de données
L'attaquant parvient à exploiter une faille dans la TOE pour accéder à des informations auxquelles il ne devrait pas avoir accès.

[*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 Paramétrage des droits d'accès
La TOE doit permettre l'hébergement et la mise à jour de la base de données centrale (droits, utilisateurs, groupes, identifiants de badge, etc.)

FM2 Notifications des événements à l'opérateur
La TOE doit permettre l'affichage et la notification des événements à l'opérateur.

FM3 Pilotage des ouvrants et des lecteurs
La TOE doit permettre la gestion de plusieurs têtes de lecture ainsi que la commande et le contrôle de plusieurs ouvrants.

FM4 Fonctions de configuration
La TOE comporte une ou plusieurs interfaces permettant d'assurer la mise à jour et le déploiement des données de configuration.

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
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 [10]. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.

FS4 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.

FS5 Vérification de la signature du micrologiciel (*firmware*)
À chaque installation d'un nouveau micrologiciel (*firmware*), l'intégrité et l'authenticité de celui-ci sont vérifiées.

FS6 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.

10. Selon le type de session web utilisée.

FS7 Communications sécurisées
La TOE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.

FS8 Authentification des équipements terminaux
La TOE permet la mise en place d'une authentification des équipements terminaux.

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.

FS11 Stockage sécurisé
La TOE stocke en local les informations de manière sécurisée en assurant la confidentialité et l'intégrité d'informations stockées en local à l'aide de mécanismes cryptographiques.

FS12 Protection contre les attaques par relais
Afin de se protéger contre les attaques par relais, la TOE intègre un mécanisme permettant de s'en prémunir.

[*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.

Annexe A Liste des tâches associées aux utilisateurs

Super-administrateur

- 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*]

Administrateur technique

- Intégration de nouveaux dispositifs de contrôle d'accès dans le réseau.
- 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.
- Mise à jour du (ou des) micrologiciel(s) (*firmware*) 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*].
- Arrêt de la TOE.
- Démarrage de la TOE.
- Redémarrage de la TOE.

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

Administrateur métier

- Consultation des statistiques de fonctionnement de la TOE : [*A compléter par le rédacteur de la TOE : lister les statistiques*].
- Ajout, suppression et modification des droits d'accès des porteurs de badge.
- Intégration de nouveaux dispositifs de contrôle d'accès dans le centre de gestion des contrôles d'accès.
- 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*]

Opérateur du GAC

- Consultation de l'historique d'accès des porteurs de badge.
- Mise à jour des droits d'accès des porteurs de badge dans le système.

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

Opérateur d'exploitation des journaux d'évènements des systèmes

- 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*]

Mainteneur de matériel physique

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

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

Porteur de badge ou usager

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

  [*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 Droit d'accès des porteurs de badge	B2 Données d'exploitation du système de contrôle d'accès physique	B3 Échanges entre les UTL et le GAC	B4 Échanges entre le lecteur de badge et l'UTL	B5 Mécanisme d'authentification des utilisateurs	B6 Secrets de connexion	B7 Micrologiciel (*firmware*)	B8 Logiciel(s)	B9 Politique de gestion des droits	B10 Fonction de journalisation locale	B11 Fonction de journalisation déportée	B12 Journaux d'évènements déportés	B13 Journaux d'évènements locaux
M1	**Déni de service**										**D**	**D**		
M2	**Corruption du micrologiciel (*firmware*)**							**I A**						
M3	**Corruption du logiciel**								**I A**					
M4	**Vol d'identifiants**						**C I**							
M5	**Contournement de l'authentification**					**I A**								
M6	**Contournement de la politique de droits**									**I**				
M7	**Corruption des journaux d'évènements locaux**													**I A**
M8	**Corruption des journaux d'évènements déportés**												**I A**	
M9	**Altération des flux**			**I A**	**I A**									
M10	**Compromission des flux**			**C**	**C**									
M11	**Corruption de données**	**I**	**I A**											
M12	**Compromission de données**	**C**	**(C)**										**(C)**	**(C)**

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 Corruption du micrologiciel (*firmware*)	M3 Corruption du logiciel	M4 Vol d'identifiants	M5 Contournement de l'authentification	M6 Contournement de la politique de droits	M7 Corruption des journaux d'événements locaux	M8 Corruption des journaux d'événements déportés	M9 Altération des flux	M10 Compromission des flux	M11 Corruption de données	M12 Compromission de données
FS1 Gestion des entrées malformées	X											
FS2 Stockage sécurisé des secrets				X								
FS3 Authentification sécurisée sur l'interface d'administration				X	X							
FS4 Gestion des autorisations						X						
FS5 Vérification de la signature du micrologiciel (*firmware*)		X										
FS6 Vérification de la signature du logiciel			X									
FS7 Communications sécurisées									X	X	X	X
FS8 Authentification des équipements terminaux									X		X	
FS9 Intégrité des journaux							X					
FS10 Intégrité des journaux déportés								X				
FS11 Stockage sécurisé											X	X
FS12 Protection contre les attaques par relais					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*[11] *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.

11. 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*]