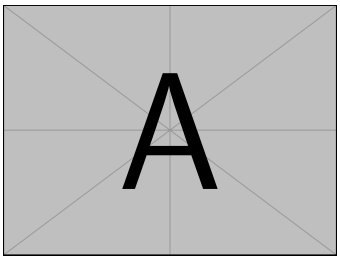
[AFFECTATION : NOM DE L'ÉDITEUR]
[AFFECTATION : NOM DU PRODUIT]

Système vidéo IP : VMS
Modèle de cible de sécurité

Version 1.0 court-terme

GTCSI



10 février 2025

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 vidéo IP : VMS

1.3 Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

COTS
Commercial off-the-shelf

SCADA
Système d'acquisition et de contrôle de données

TOE
Target of evaluation

USB
Bus série universel

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.cyber.gouv.fr/`

2 Description du produit

2.1 Description générale du produit

Un système de vidéo IP est constitué de moyens permettant de capturer des flux vidéo, audio ou les deux, de les analyser, de les enregistrer et d'interagir avec d'autres systèmes de sûreté. Un système vidéo IP assure plusieurs fonctions :

- la captation vidéo et/ou audio ;
- la sauvegarde des données captées ;
- le traitement des données ;
- le déclenchement d'actions ;
- la génération d'évènements ;
- la gestion des évènements ;
- la configuration et la gestion de caméra à distance ;
- la visualisation de la vidéo en direct.

Dans le cas d'un système vidéo IP, deux éléments supports principaux interviennent :

- les caméras ;
- le centre de gestion vidéo (Centre de gestion vidéo (VMS)) qui inclut les éléments suivants :
  - un logiciel de gestion vidéo qui communique avec les caméras IP ;
  - des ressources de type base de données ou annuaire, qui permettent de gérer les données essentielles au système comme les utilisateurs, les groupes ou les enregistrements provenants des capteurs. Ces ressources peuvent appartenir à un système d'information extérieur à la *Target of evaluation* (TOE).

2.2 Description de la manière d'utiliser le produit

Le fonctionnement d'un système vidéo IP est géré par le centre de gestion vidéo (VMS). Ce centre est une infrastructure centralisée assurant les fonctions suivantes :

- la gestion et l'analyse des évènements ;
- la visualisation des flux vidéo en direct ;
- l'enregistrement des flux vidéo des caméras ;
- l'administration et la gestion des caméras.

À l'usage, quatre phases sont identifiables dans le fonctionnement d'un système de vidéo IP :

- la captation de flux vidéo et/ou audio par les caméras ;
- l'analyse des images par le centre de gestion vidéo ;
- le déclenchement d'alarmes à l'opérateur et aux systèmes métiers auxquels il est connecté ;
- la consultation des vidéos en direct ou à posteriori.

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***]

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

- I1 : Interface de raccordement du serveur de gestion vidéo (VMS) à la station de gestion [1].
- I2 : Interface de raccordement du serveur de gestion vidéo (VMS) aux caméras.

1. Une station de gestion désigne le poste de travail à partir duquel l'opérateur du VMS effectue les opérations d'exploitation et d'administration du système de vidéo IP. Des dispositifs d'orientation des caméras de type joystick sont souvent associés à la station de gestion.

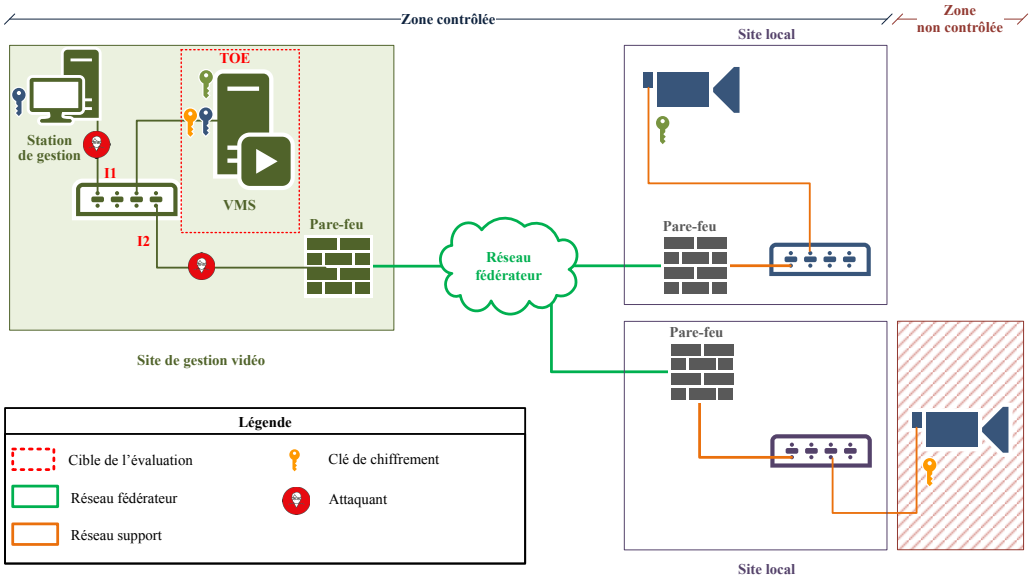


FIGURE 1 – Architecture type d'un réseau de vidéo IP

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, Commercial off-the-shelf (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 :

- Super-administrateur ;
- Administrateur technique ;
- Administrateur métier ;
- Opérateur du VMS ;
- Opérateur d'exploitation des journaux d'évènements des systèmes ;

[*A compléter par le rédacteur de la TOE : autres rôles 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.

2.7 Description du périmètre de l'évaluation

L'évaluation concerne les éléments du système vidéo IP listés ci-dessous :

- le VMS :
  - le système d'exploitation ;
  - applicatifs (hors traitement d'image) ;
  - fonctions cryptographiques ;
  - base de données et annuaires.

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 Bus série universel (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*]

3 Description des hypothèses sur l'environnement

H1 Module externe
Les utilisateurs s'assurent que les modules externes [4] considérés comme désactivés dans cette cible sont bien désactivés en pratique.

H2 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.

H3 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.

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

H5 Administrateurs
Les administrateurs techniques et métiers de la TOE sont compétents, formés et non hostiles.

H6 Super-administrateurs
Les super-administrateurs de la TOE sont compétents, formés et non hostiles.

H7 Consultation des journaux
Les opérateurs d'exploitation des journaux d'évènements des systèmes consultent régulièrement ou accèdent automatiquement aux journaux locaux ou déportés générés par la TOE.

H8 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.

4. 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 Données capturées
Les données capturées et enregistrées doivent être protégées en confidentialité, intégrité et authenticité.

B2 Données de configuration
Les données de configuration sont constituées de l'ensemble des informations utiles au bon fonctionnement du système vidéo IP en phase opérationnelle. Cet ensemble comprend notamment des configurations, des valeurs instantanées, des alarmes, des commandes etc. Elles peuvent être mises à disposition d'applications tierces par la TOE au travers d'interfaces de programmation. Ces données doivent être protégées en confidentialité, intégrité et authenticité. L'accès à ces données est régi par la politique de droit d'accès de la TOE.

B3 Échanges entre le VMS et les caméras
Les flux de contrôle et multimédia doivent être protégés en confidentialité, en intégrité et en authenticité.

B4 Échanges entre le VMS et la station de gestion
Les flux entre la station gestion et le VMS doivent être protégés 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 [5].

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 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 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.

B9 Fonction de journalisation locale
La TOE dispose d'une fonction de journalisation locale [6] qui, une fois configurée, doit rester opérationnelle (disponible).

B10 Fonction de journalisation déportée
La TOE dispose d'une fonction de journalisation déportée [7] qui, une fois configurée, doit rester opérationnelle (disponible).

B11 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.

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.

B12 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	Données capturées		✗	✗	✗
B2	Données de configuration		✗	✗	✗
B3	Échanges entre le VMS et les caméras		✗	✗	✗
B4	Échanges entre le VMS et la station de gestion		✗	✗	✗
B5	Mécanisme d'authentification des utilisateurs			✗	✗
B6	Secrets de connexion		✗	✗	
B7	Logiciel(s)			✗	✗
B8	Politique de gestion des droits			✗	
B9	Fonction de journalisation locale	✗			
B10	Fonction de journalisation déportée	✗			
B11	Journaux d'évènements déportés		(✗)	✗	✗
B12	Journaux d'évènements locaux		(✗)	✗	✗

✗ : 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 ayant compromis le réseau du centre de gestion vidéo**
  Attaquant se situant sur le réseau du centre de gestion vidéo (VMS).
- **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 temporaire, due à un 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 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.

M3 Vol d'identifiants
L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

M4 Contournement de l'authentification
L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

M5 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.

M6 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.

M7 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.

M8 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.

M9 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.

M10 Corruption de données
L'attaquant parvient à modifier des données, sans en avoir le droit, en exploitant une faille de la TOE.

M11 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*]

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

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 Visualisation des vidéos
La TOE doit permettre l'affichage et l'écoute des flux audio et vidéo.

FM2 Génération d'événements
La TOE doit permettre de générer des événements.

FM3 Gestion et analyse d'événements
La TOE doit permettre la gestion et l'analyse d'événements.

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, afin d'éviter qu'un attaquant puisse la positionner dans un état non souhaité pour l'exploiter (injection de code, fuzzing, etc.).

FS2 Stockage sécurisé des secrets
La TOE stocke les secrets de connexion des utilisateurs 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 utilisateurs avant d'accorder l'accès. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée [9].

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 logiciel
La TOE vérifie la signature des composants logiciels pour s'assurer de leur authenticité et de leur intégrité lors de l'installation, de la mise à jour et de l'exécution.

FS6 Communications sécurisées
La TOE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.

FS7 Authentification des équipements terminaux
La TOE permet la mise en place d'une authentification des équipements terminaux.

FS8 Intégrité des journaux
La TOE génére des journaux d'événements intègres.

9. Dans le cadre d'authentification faisant intervenir des jetons de session, ceux-ci sont protégés contre le vol et contre le rejeu. De plus ils ont une durée de vie limitée et sont générés aléatoirement ou authentifiés.

FS9 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.

FS10 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.

[*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 et configuration de nouveaux dispositifs de vidéo IP dans le réseau.
- Maintien en conditions opérationnelles du centre de gestion de la TOE.
- Maintien en conditions de sécurité du centre de gestion de la TOE.
- 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 aux caméras.
- 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 VMS

- Visualisation en direct ou à posteriori des vidéos.
- Traitement des événements.

  [*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*]

[*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 Données capturées	B2 Données de configuration	B3 Échanges entre le VMS et les caméras	B4 Échanges entre le VMS et la station de gestion	B5 Mécanisme d'authentification des utilisateurs	B6 Secrets de connexion	B7 Logiciel(s)	B8 Politique de gestion des droits	B9 Fonction de journalisation locale	B10 Fonction de journalisation déportée	B11 Journaux d'évènements déportés	B12 Journaux d'évènements locaux
M1	**Déni de service**									**D**	**D**		
M2	**Corruption du logiciel**							**I A**					
M3	**Vol d'identifiants**						**C I**						
M4	**Contournement de l'authentification**					**I A**							
M5	**Contournement de la politique de droits**								**I**				
M6	**Corruption des journaux d'évènements locaux**												**I A**
M7	**Corruption des journaux d'évènements déportés**											**I A**	
M8	**Altération des flux**			**I A**	**I A**								
M9	**Compromission des flux**			**C**	**C**								
M10	**Corruption de données**	**I A**	**I A**										
M11	**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 logiciel	M3 Vol d'identifiants	M4 Contournement de l'authentification	M5 Contournement de la politique de droits	M6 Corruption des journaux d'événements locaux	M7 Corruption des journaux d'événements déportés	M8 Altération des flux	M9 Compromission des flux	M10 Corruption de données	M11 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 logiciel		X									
FS6 Communications sécurisées								X	X	X	X
FS7 Authentification des équipements terminaux								X		X	
FS8 Intégrité des journaux						X					
FS9 Intégrité des journaux déportés							X				
FS10 Stockage sécurisé										X	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. Cette liste est générique à tous les profils de protection.*]

Configuration réseau

- Consultation de la configuration de l'interface d'administration
  - Adresses IP
  - Port / Réseau local virtuel (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*)

- 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 Système d'acquisition et de contrôle de données (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.

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

Maintien en conditions opérationnelles du centre de gestion de la TOE.

- Maintien en conditions opérationnelles du centre de gestion de la TOE.

Maintien en conditions de sécurité du centre de gestion de la TOE.

- Maintien en conditions de sécurité du centre de gestion de la TOE.

Intégration et configuration de nouveaux dispositifs dans le système.

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

Ajout, suppression et modification des droits d'accès aux caméras.

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

Traitement des événements.

- Traitement des événements.

Pilotage de la TOE.

- Pilotage de la TOE.

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*]