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

Commutateur industriel
Modèle de cible de sécurité

Version 1.1 moyen-terme

GTCSI

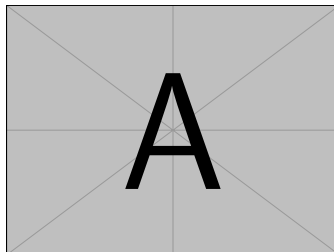


Table des matières

1	Introduction	3
1.1	Objet du document	3
1.2	Identification du produit	3
1.3	Acronymes	3
1.4	Documents applicables	3
2	Description du produit	4
2.1	Description générale du produit	4
2.2	Description de la manière d'utiliser le produit	4
2.3	Description de l'environnement prévu pour son utilisation	5
2.4	Description des dépendances à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit	6
2.5	Description des utilisateurs typiques concernés	7
2.6	Description du périmètre de l'évaluation	7
3	Description des hypothèses sur l'environnement	8
4	Description des biens sensibles	9
5	Description des menaces	11
5.1	Profils des attaquants	11
5.2	Menaces	11
6	Description des fonctions du produit	13
6.1	Fonctions métier	13
6.2	Fonctions de sécurité	13
	Annexe A Liste des tâches associées aux utilisateurs	15
	Annexe B Matrices de couverture	16
	B.1 Menaces et biens sensibles	16
	B.2 Fonctions de sécurité	18
	Annexe C Liste des tâches	19
	Annexe D Liste des contributeurs	21

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 court 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	Commutateur industriel

1.3 Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

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

La TOE considérée est un commutateur industriel, destiné à fonctionner dans des environnements hostiles où des commutateurs classiques pourraient ne pas fonctionner du fait de la chaleur, de l'humidité ou de la poussière par exemple.

D'un point de vue fonctionnel, le commutateur industriel permet d'interconnecter différents équipements ou segments de réseaux communiquant en Ethernet. Il supporte les VLAN et permet d'effectuer ainsi du cloisonnement réseau.

2.2 Description de la manière d'utiliser le produit

Les commutateurs industriels peuvent être utilisés dans de nombreux contextes différents. Néanmoins, on peut dégager deux grandes catégories avec les réseaux de « terrain » qui relient les entrées/sorties déportées aux automates, et les réseaux de supervision qui connectent les automates aux stations SCADA.

Dans des réseaux de faible criticité, il est possible d'utiliser les VLAN pour cloisonner les différentes fonctions et l'administration des équipements. Un exemple d'une telle topologie est représenté sur la figure 1. On peut voir sur cette figure que le cloisonnement assure que chaque automate ne peut communiquer qu'avec un capteur et un actionneur (VLAN 102 et 103) et empêche la communication entre les deux automates (VLAN 102 et 103 sur le réseau du bas et 104 et 105 sur celui du haut). Enfin, un VLAN permet d'isoler les fonctions d'administration des commutateurs (VLAN 101).

2.3 Description de l'environnement prévu pour son utilisation

[Raffinement : ce schéma est à refaire par le rédacteur de la cible de sécurité]

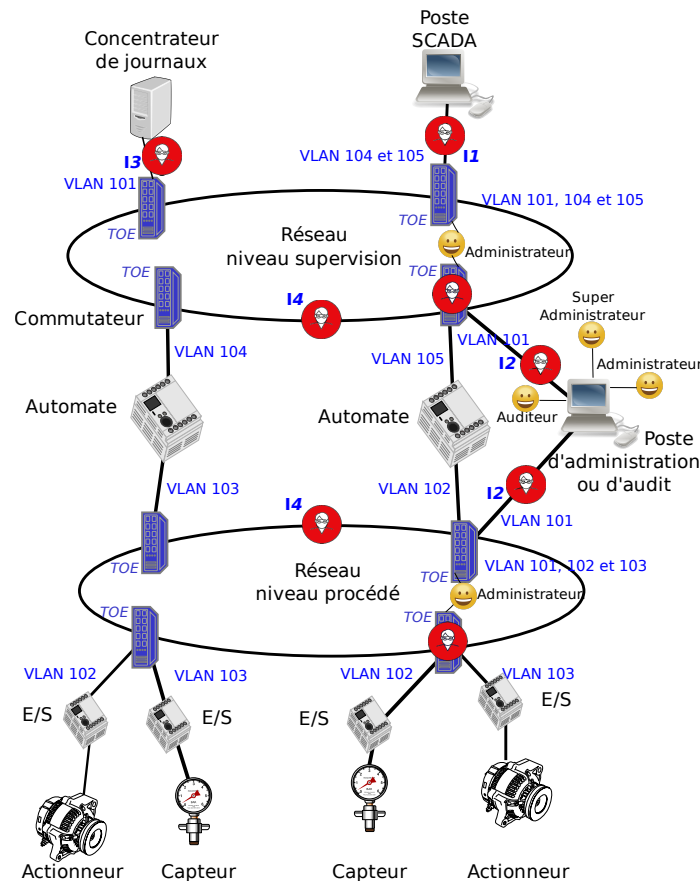


FIGURE 1 – TOE dans un système industriel

Légende :  Attaquant

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

- **I1.** Interface de raccordement aux outils métier, par exemple un client SCADA.
- **I2.** Interface du réseau d'administration et raccordée aux consoles d'administration ou de supervision et d'audit. Cette interface permet l'accès aux rôles super-administrateur, Administrateur et Auditeur.
- **I3.** Interface de raccordement aux outils de journalisation, par exemple un concentrateur de journaux.
- **I4.** Interface de raccordement des équipements réseaux adjacents, par exemple un commutateur, un routeur ou un pare-feu.

Le périmètre de l'évaluation est constitué de la TOE et de ses [Affectation : nombre d'interfaces réseau] interfaces réseau.

[Affectation : compléter la liste des interfaces si besoin par exemple par des interfaces systèmes tels que USB, VGA, etc.]

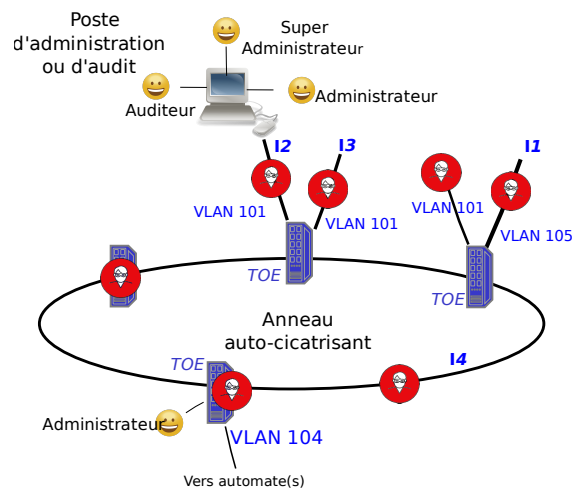


FIGURE 2 – Environnement de la TOE

Légende :  Attaquant

Le périmètre de l'évaluation est représenté sur la figure 2.

[Affectation : compléter la description du périmètre de l'évaluation si besoin]

2.4 Description des dépendances à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit

[Affectation : description des dépendances à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit]

2.5 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 utilisateurs¹ suivants :

- Administrateur ;
 - Auditeur ;
 - Super-administrateur ;
- [Affectation : autres rôles si besoin]

2.6 Description du périmètre de l'évaluation

Le périmètre de l'évaluation est constitué de la TOE et de ses [Affectation : nombre d'interfaces réseau] interfaces réseau.

[Affectation : 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.

[Affectation : compléter la description du périmètre de l'évaluation si besoin]

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

3 Description des hypothèses sur l'environnement

Les hypothèses sur l'environnement de la TOE sont les suivantes :

H1 Consultation des journaux

Il est considéré que les auditeurs consultent régulièrement ou accèdent automatiquement² aux journaux locaux ou déportés générés par la TOE.

H2 Super-administrateurs

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

H3 Politique de cloisonnement logique

La politique de cloisonnement configurée sur la TOE est adaptée au cas d'usage.

H4 Dimensionnement

Il est supposé que la TOE est dimensionnée correctement pour les traitements qu'elle doit effectuer.

H5 Serveurs d'authentification

Le cas échéant, les serveurs d'authentification utilisés pour authentifier les utilisateurs sont considérés comme sains et configurés correctement.

H6 Documentation de sécurité

Les utilisateurs se conforment aux préconisations issues de la documentation de sécurité de la TOE. La documentation inclut :

- la désactivation de l'ensemble des services présents dans la TOE mais hors de la cible de sécurité ;
- l'ensemble des secrets de connexion présents par défaut pour permettre leur personnalisation.

[Affectation : autres hypothèses si besoin]

2. 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 Trames

Les trames d'un sous-réseau ne doivent pas être accessibles (visibles ou modifiables) par un acteur résidant sur un autre sous-réseau. Les trames doivent être protégées en disponibilité par la TOE sur une panne d'un équipement distant.

B2 Authentification des équipements terminaux

Aucun équipement terminal non autorisé ne doit être présent sur le réseau. Les éléments permettant d'authentifier un terminal raccordé sur la TOE doivent être transmis en authenticité, intégrité et confidentialité au serveur D'authentification.

B3 Firmware

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

B4 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.

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 mécanisme³.

B6 Secrets de connexion des utilisateurs

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

B7 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.

B8 Fonction de journalisation locale

La TOE dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle.

B9 Fonction de journalisation distante

La TOE dispose d'une fonction de journalisation distante qui, une fois configurée, doit rester opérationnelle.

B10 Journaux d'évènements locaux

Les journaux locaux générés par la TOE doivent être intègres.

B11 Journaux d'évènements déportés

L'émission du journal par la TOE doit être intègre et authentifié. 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.

[Affectation : autres biens sensibles si besoin]

3. 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.

		Disponibilité	Confidentialité	Intégrité	Authenticité
B1	Trames	X		X	
B2	Authentification des équipements terminaux	X	X	X	X
B3	<i>Firmware</i>			X	X
B4	Configuration		X	X	
B5	Mécanisme d'authentification des utilisateurs			X	X
B6	Secrets de connexion des utilisateurs		X	X	
B7	Politique de gestion des droits			X	
B8	Fonction de journalisation locale	X			
B9	Fonction de journalisation distante	X			
B10	Journaux d'évènements locaux			X	X
B11	Journaux d'évènements déportés			X	X

X : obligatoire (X) : optionnel

TABLE 1 – Biens sensibles de la TOE

5 Description des menaces

5.1 Profils des attaquants

Les attaquants⁴ à considérer pour l'évaluation sont :

- **Équipement terminal malveillant**
Un équipement terminal connecté à la TOE est contrôlé par l'attaquant.
- **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.
- **Attaquant avec les droits d'utilisateur(s)**
L'attaquant a réussi à compromettre le compte d'un utilisateur. Ce compte peut avoir n'importe quel rôle à l'exception de ceux définis éventuellement en hypothèse au chapitre 3.
[Affectation : autres profils parmi les rôles listés au chapitre 2.5 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 Contournement de la politique de filtrage d'équipement

L'attaquant parvient à connecter un équipement terminal à la TOE et à faire transiter du trafic en dépit de la politique de filtrage.

M3 Corruption du *firmware*

L'attaquant parvient à injecter et faire exécuter un *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.

M4 Corruption de la configuration

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

M5 Compromission de la configuration

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

M6 Vol d'identifiants

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

M7 Contournement de l'authentification

L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

M8 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 *firmware* sans en avoir le droit.

M9 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.

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

M10 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.

[Affectation : 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 » sont données à titre indicatifs et ne font pas l'objet d'une évaluation de sécurité.**

6.1 Fonctions métier

FM1 Cloisonnement logique

L'équipement permet d'effectuer du cloisonnement logique (à l'aide de VLAN par exemple) qu'il est possible de configurer.

FM2 Gestion des ports de communication

La TOE permet de désactiver les ports physiques non utilisés.

FM3 Filtrage par adresse MAC

La TOE permet de définir des listes blanches d'adresses MAC pour chaque port Ethernet.

FM4 Authentification des terminaux connectés

La TOE permet d'authentifier les équipements terminaux connectés avec un protocole tel que celui décrit dans la norme 802.1x.

FM5 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.).

FM6 Fonctions de redondance

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

FM7 Journalisation locale d'évènements

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

FM8 Journalisation distante d'évènements

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

[Affectation : autres fonctions métier]

6.2 Fonctions de sécurité

FS1 Gestion des entrées malformées et résilience du réseau

La TOE gère correctement les entrées malformées, en particulier 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.). La TOE change la topologie de ses interfaces réseau afin de continuer à transmettre les trames en cas de blocage d'un équipement réseau différent de la TOE.

FS2 Politique de cloisonnement logique

La TOE met en œuvre une politique de cloisonnement logique configurable par l'administrateur (à l'aide de VLAN et PVLAN).

FS3 Application du filtrage des équipements

La TOE permet la mise en place d'une politique de filtrage des équipements par adresse MAC.

FS4 Connexion sécurisée avec le serveur d'authentification

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

FS5 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.

FS6 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. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.

FS7 Politique de droits

La politique de gestion des droits est gérée de manière extrêmement stricte. 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.

FS8 Signature du *firmware*

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

FS9 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.

FS10 Intégrité des journaux

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

FS11 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.

[Affectation : autres fonctions de sécurité si besoin]

Annexe A Liste des tâches associées aux utilisateurs

Administrateur

- 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 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.).
- Mise à jour du système d'exploitation de la TOE.
- Redémarrage de la TOE.
[Affectation : autres tâches définies dans la liste en Annexe C]

Auditeur

- Consultation des statistiques de fonctionnement de la TOE : [Affectation : lister les statistiques].
- Consultation des journaux d'évènements générés par la TOE.
[Affectation : autres tâches définies dans la liste en Annexe C]

Super-administrateur

- Création des comptes associés aux rôles [Affectation : liste des rôles].
- Suppression des comptes associés aux rôles [Affectation : liste des rôles].
- Modification des comptes associés aux rôles [Affectation : liste des rôles].
- Consultation des attributs [Affectation : liste des attributs] des comptes associés aux rôles [Affectation : liste des rôles].
[Affectation : autres tâches définies dans la liste en Annexe C]

[Affectation : autres rôles si besoin]

[Affectation : autres tâches définies dans la liste en Annexe C]

Annexe B Matrices de couverture

B.1 Menaces et biens sensibles

	B1 Trames	B2 Authentification des équipements terminaux	B3 Firmware	B4 Configuration	B5 Mécanisme d'authentification des utilisateurs	B6 Secrets de connexion des utilisateurs	B7 Politique de gestion des droits	B8 Fonction de journalisation locale	B9 Fonction de journalisation distante	B10 Journaux d'événements locaux	B11 Journaux d'événements déportés
M1	Déni de service	DI DIA						D	D		
M2	Contournement de la politique de filtrage d'équipement	I									
M3	Corruption du <i>firmware</i>		IA								
M4	Corruption de la configuration			I							
M5	Compromission de la configuration			C							
M6	Vol d'identifiants					CI					
M7	Contournement de l'authentification				IA						
M8	Contournement de la politique de droits	CIA					I				
M9	Corruption des journaux d'événements locaux									IA	
M10	Corruption des journaux d'événements déportés										IA

TABLE 2 – Atteintes aux biens sensibles en fonction des menaces

Légende : Disponibilité (D), Intégrité (I), Confidentialité (C), Authenticité (A)

B.2 Fonctions de sécurité

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
	Déni de service	Contournement de la politique de filtrage d'équipement	Corruption du <i>firmware</i>	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'événements locaux	Corruption des journaux d'événements déportés
FS1	Gestion des entrées malformées et résilience du réseau	X								
FS2	Politique de cloisonnement logique	X								
FS3	Application du filtrage des équipements	X								
FS4	Connexion sécurisée avec le serveur d'authentification					X				
FS5	Stockage sécurisé des secrets				X					
FS6	Authentification sécurisée sur l'interface d'administration			X	X	X	X			
FS7	Politique de droits		X					X		
FS8	Signature du <i>firmware</i>		X							
FS9	Intégrité et confidentialité de la configuration			X	X					
FS10	Intégrité des journaux								X	
FS11	Intégrité des journaux déportés									X

TABLE 3 – Couverture des menaces par les fonctions de sécurité

Annexe C Liste des tâches

[Raffinement : 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 règles de filtrage.
- Modification des règles de filtrage.
- Suppression des règles de filtrage.
- Consultation des règles 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.

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 [Affectation : liste des rôles].
- Suppression des comptes associés aux rôles [Affectation : liste des rôles].
- Modification des comptes associés aux rôles [Affectation : liste des rôles].
- Consultation des attributs [Affectation : liste des attributs] des comptes associés aux rôles [Affectation : liste des rôles].
- Edition des attributs [Affectation : liste des attributs] des comptes associés aux rôles [Affectation : liste des rôles].

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 : [Affectation : lister les statistiques].

Equipement terminal

- Néant

[Affectation : autres tâches si besoin]

Annexe D Liste des contributeurs

La version 1.1 de ce profil de protection a été rédigé avec le concours des sociétés et organismes suivants :

- Amossys
- Belden
- DGA/MI
- Oppida
- Siemens
- Stormshield