Cible de sécurité CSPN

Gamme commutateurs SCALANCE-XM400

Catégorie « Systèmes Industriels »

Référence : CSPN-ST-SCALANCE_XM400-2.00

Date : 23/11/2015

Code interne : SIE002

Siège : 4 bis allée du Bâtiment ● 35000 Rennes ● France ● www.amossys.fr

SIRET : 493 348 890 00036 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

FICHE D'ÉVOLUTIONS

Révision	Date	Description	Rédacteur
1.00	09/06/2015	Version originale	Antoine COUTANT
2.00	23/11/2015	Mise à jour de la cible de sécurité avec le PP en version 1.0 issu du GT CSI	Antoine COUTANT

Ce document est validé par Siemens.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], de la gamme des commutateurs industriels « *SCALANCE XM400* » développée par la société **Siemens**.

Dans le cadre du groupe de travail sur la cybersécurité des systèmes industriels (GTCSI) sous l'égide de l'ANSSI, deux types de profils de protection ont été rédigés : celui dit à « court terme » et celui dit « à moyen terme ». Le profil de protection à court terme correspond à un niveau de sécurité strictement minimal qui peut être exigé dès à présent dans les équipements. Dans le profil de protection à moyen terme apparaissent des objectifs de sécurité plus ambitieux. Ces objectifs guident les équipementiers afin que leurs produits atteignent le niveau de sécurité requis dans les cinq années à venir.

La présente cible de sécurité a été rédigée sur la base du profil de protection court terme d'un commutateur industriel (version 1.0 du 13 juillet 2015).

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **Siemens**. Les mises à jour de ce document sont effectuées par **AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Editeur	SIEMENS AG OESTLICHE RHEINBRUECKENSTRASSE 50 76187 KARLSRUHE GERMANY
Lien vers l'organisation	http://www.siemens.com
Nom commercial du produit	Gamme SCALANCE XM400
Numéro de la version évaluée	05.00.01
Catégorie du produit	Systèmes Industriels (commutateur industriel)

Tableau 1 - Identification du produit évalué

1.3. RÉFÉRENCES

Pour l'établissement de la présente cible de sécurité, la fiche technique suivante du commutateur à évaluer a été considérée : Data sheet Scalance XM416-4C.

De même, le profil de protection du commutateur industriel est disponible ici : http://www.ssi.gouv.fr/uploads/2015/03/20150713_NP_ANSSI_SDE_commutateur_court_terme_v1.0-fr.pdf.

[1] Certification de Sécurité de Premier Niveau
[2] Agence nationale de la sécurité des systèmes d'information

2. DESCRIPTIF DU PRODUIT

2.1. DESCRIPTIF GÉNÉRAL DU PRODUIT

Un commutateur industriel est 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 (*Virtual Local Area Network*) et permet d'effectuer ainsi du cloisonnement réseau.

La TOE est un commutateur industriel Ethernet managé (couche 3) permettant une grande vitesse de transmission (10, 100 ou 1000 Mbit/s), une grande densité de connexion ainsi que de grandes capacités fonctionnelles en matière de routage. La TOE permet de supporter jusqu'à 255 VLAN selon différents modes (niveaux 1 à 3 de la couche OSI) : port, protocole, IP ou dynamique.

La cible d'évaluation (TOE[3]) considérée est la gamme de commutateurs *SCALANCE XM400* (débit de 1000 Mbit/s) développés par l'équipementier **Siemens**.

La figure suivante est une illustration de son utilisation combinée avec d'autres matériels de l'équipementier **Siemens**.

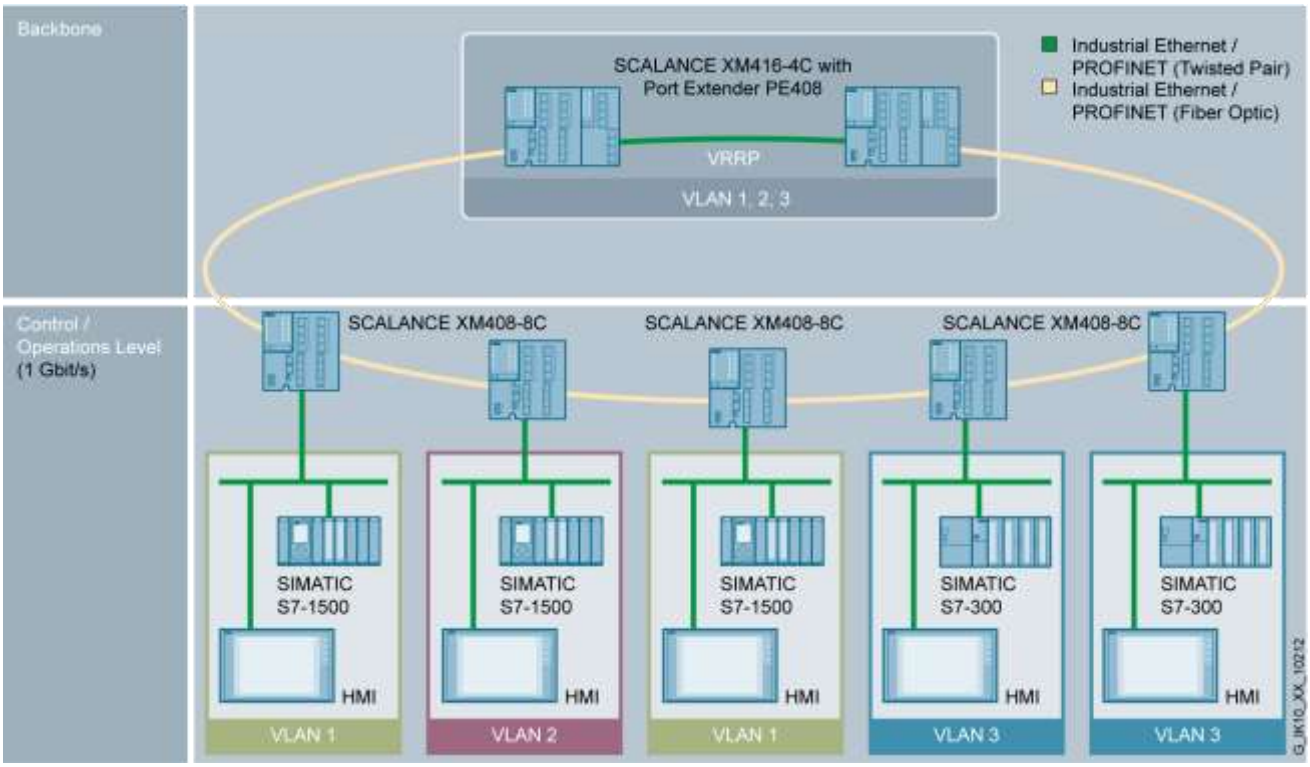

Figure 1 - Illustration d'utilisation de la TOE

[3] Target Of Evaluation

2.2. DESCRIPTIF DE L'UTILISATION DU PRODUIT

Dans un réseau de faible criticité, il est possible d'utiliser les VLAN pour cloisonner différentes fonctions ainsi que l'administration des équipements. Un exemple d'une telle topologie est représenté sur la Figure 2 où le cloisonnement assure que chaque automate ne peut communiquer qu'avec un capteur et un actionneur (VLAN 2 et 3) et empêche la communication entre les deux automates (VLAN 2 et 3 sur le réseau du bas et 4 et 5 sur celui du haut). Enfin, un VLAN permet d'isoler les fonctions d'administration des commutateurs et du poste SCADA (VLAN 1).

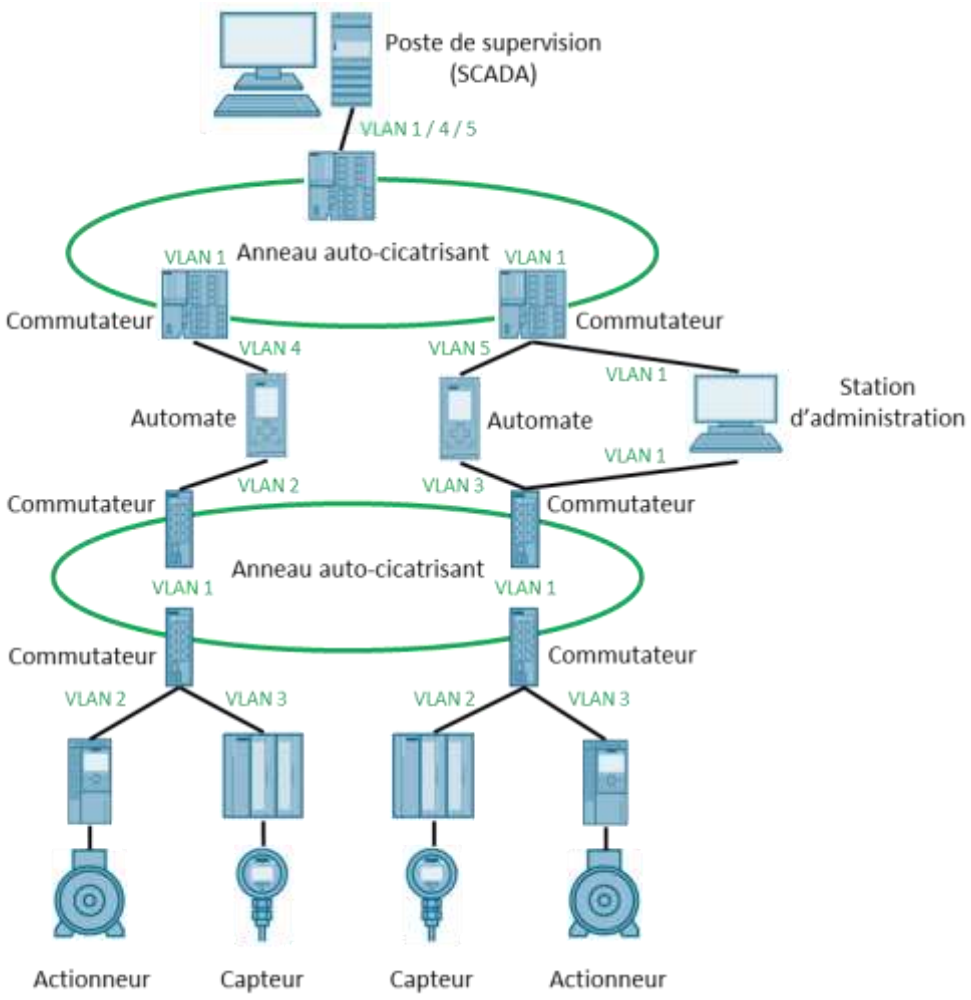

Figure 2 - Réseaux avec cloisonnement par VLAN

Siemens fournit des produits et solutions avec des fonctions de sécurité industrielle qui sont utilisés dans de nombreux secteurs industriels. Ils sont des éléments importants dans un concept de sécurité industrielle globale. Dans cet esprit, les produits et solutions de **Siemens** subissent un développement continu.

Les capacités techniques de la TOE sont disponibles dans les fiches techniques de la gamme des produits *SCALANCE XM400*.

Il est à noter que la TOE permet un accès de diagnostic via NFC (*Near Field Communication*) pour les smartphones et tablettes. Cette fonction est désactivée dans le cadre de l'évaluation.

2.3. DESCRIPTION DES DÉPENDANCES

La TOE est une *appliance* dédiée, il n'y a donc aucune dépendance car elle est livrée préconfigurée avec les éléments nécessaires à son fonctionnement.

2.4. PÉRIMÈTRE DE L'ÉVALUATION

La TOE est livrée sous forme d'*appliance* avec son propre système d'exploitation. La gamme des commutateurs *SCALANCE XM400* est évaluée en tant qu'élément séparateur de deux réseaux VLAN. De même, il sera évalué avec un poste d'administration (sous environnement Windows 7) et de supervision connecté au port local ainsi qu'un serveur d'authentification (RADIUS dans le cadre de l'évaluation) directement accessible.

Le commutateur sera évalué avec des API[4] S7-1500 de **Siemens** positionnés dans les sous-réseaux.

La figure suivante présente la plateforme d'évaluation :

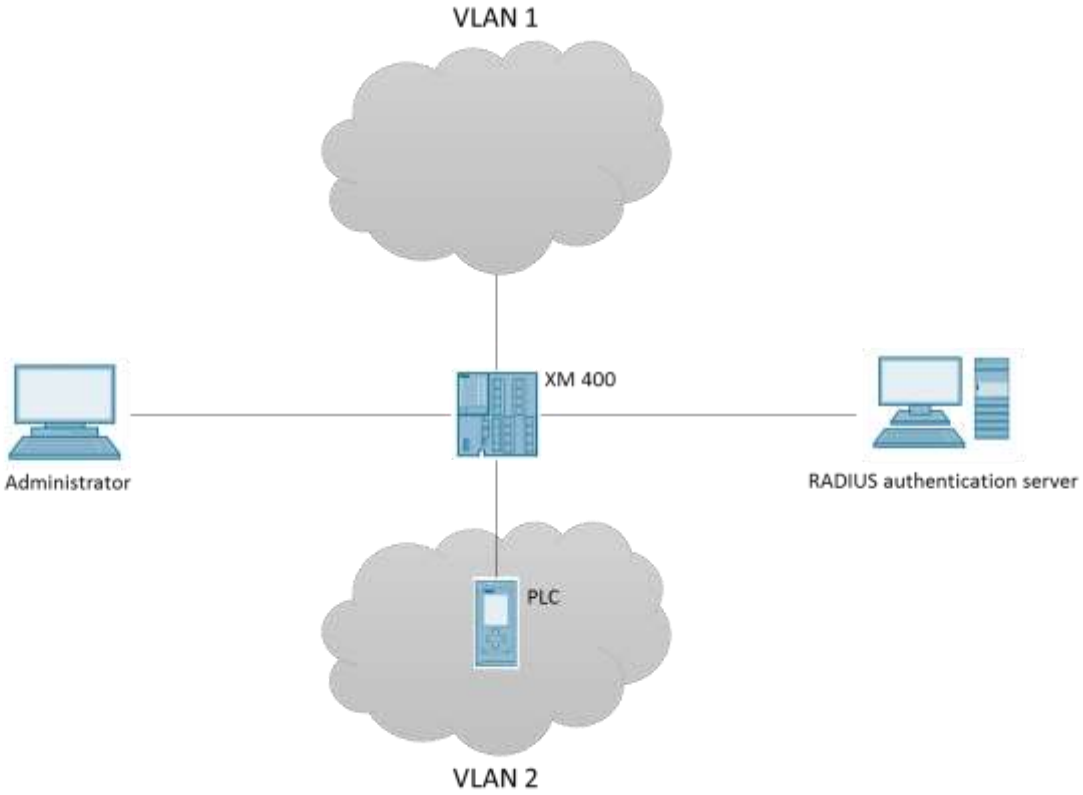

Figure 3 - Plateforme d'évaluation

[4] Automate Programmable Industriel

3.PROBLÉMATIQUE DE SÉCURITÉ

La problématique de sécurité a été établie sur la base du profil de protection court terme d'un commutateur industriel (version 1.0 du 13 juillet 2015).

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Les rôles suivants seront pris en considération dans le cadre de l'analyse :

- ***Administrateur :*** utilisateur ayant les droits de modifier tout ou partie de la configuration de la TOE ;
- ***Utilisateur*** : utilisateur ayant le droit de consulter tout ou partie de la configuration ;
- ***Équipement terminal*** : équipement terminal (API S7 dans le cadre de l'évaluation) connecté directement ou indirectement à la TOE.

Note 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.

Note 2 : le rôle de super-administrateur défini dans le profil de protection a été supprimé car la TOE à évaluer ne gère que les rôles définis précédemment.

3.2. DESCRIPTION DES BIENS SENSIBLES

3.2.1. Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

- **B.TRAMES** : la TOE assure le filtrage et, le cas échéant, la commutation de trames (technologie « *Store & Forward* » mise en œuvre) entre les équipements terminaux.
- **B.CLOISONNEMENT_LOGIQUE :** la TOE assure le cloisonnement logique entre différents sous-réseaux.
- **B.AUTHENT_ÉQUIP_TERMINAUX :** la TOE authentifie les équipements terminaux qui sont directement connectés dessus.

3.2.2. Biens sensibles de la TOE

Les biens sensibles de l'environnement sont les suivants :

- **B.FIRMWARE :** afin d'assurer correctement ses fonctions, le *firmware* de la TOE doit être intègre et authentique.
- **B.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.
- **B.AUTHENT_UTILISATEURS :** la TOE doit protéger l'intégrité et l'authenticité du mécanisme d'authentification des utilisateurs.
- **B.SECRETS_CONNEXION_USERS :** la TOE doit garantir l'intégrité et la confidentialité des identifiants des utilisateurs (mots de passe et certificats).
- **B.POL_GESTION_DROITS :** la TOE doit garantir l'intégrité de la politique de gestion des droits.

3.2.3. Besoins de sécurité des biens sensibles

Les besoins de sécurité de chacun de ces biens sont donnés ci-dessous :

Biens sensibles	Disponibilité	Intégrité	Confidentialité	Authenticité
B.TRAMES	√			
B.CLOISONNEMENT_LOGIQUE	√	√		
B.AUTHENT_ÉQUIP_TERMINAUX	√	√		√
B.FIRMWARE		√		√
B.CONFIGURATION		√	√	
B.AUTHENT_UTILISATEURS		√		√
B.SECRETS_CONNEXION_USERS		√	√	
B.POL_GESTION_DROITS		√		

Tableau 2 - Besoins de sécurité des biens sensibles

3.3. DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la TOE :

- **H.ADMINISTRATEURS :** les administrateurs de la TOE sont compétents, formés et non hostiles.
- **H.LOCAL :** la TOE doit se trouver dans un local sécurisé dont l'accès est restreint à des personnes autorisées considérées comme non hostiles. En particulier, l'attaquant n'aura pas accès aux ports physiques de la TOE. En revanche, des équipements identiques à la TOE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement en vue d'y rechercher des vulnérabilités par tous les moyens à sa disposition pour attaquer la TOE.
- **H.POLITIQUE_CLOISONNEMENT_LOGIQUE :** la politique de cloisonnement configurée sur la TOE est adaptée au cas d'usage.
- **H.DIMENSIONNEMENT :** il est supposé que la TOE est dimensionnée correctement pour les traitements qu'elle doit effectuer.
- **H.SERVEURS_AUTHENTIFICATION :** les serveurs d'authentification utilisés pour authentifier les utilisateurs sont considérés comme sains et configurés correctement.
- **H.SERVICES_DÉSACTIVÉS :** l'ensemble des services présents dans la TOE mais hors de la cible de sécurité sont désactivés dans la configuration par défaut (parfois appelée configuration usine). En particulier, la fonction d'accès de diagnostic via NFC pour les smartphones et tablettes est désactivée pour l'évaluation.

- **H.DOC_SÉCURITÉ :** la TOE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation. L'ensemble des préconisations issues de cette documentation ont été appliquées en vue de l'évaluation :
  - https://support.industry.siemens.com/cs/ww/en/view/109476785
  - https://support.industry.siemens.com/cs/ww/en/view/99897982

3.4. DESCRIPTION DES MENACES

3.4.1. Agents menaçants

Les agents menaçants considérés pour la CSPN sont les suivants :

- **Équipement terminal malveillant :** un équipement terminal connecté à la TOE est contrôlé par l'attaquant.
- **Équipement d'administration malveillant :** 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.

3.4.2. Menaces applicables à la TOE

Les menaces qui portent sur les biens sensibles de l'environnement et de la TOE sont les suivantes :

- **M.DÉFAUT_RÉSILIENCE :** en exploitant un défaut ou une vulnérabilité de la TOE, l'attaquant parvient à empêcher, même temporairement, le changement de topologie en réponse à une panne d'un autre équipement.
- **M.DÉNI_SERVICE :** l'attaquant parvient à effectuer un déni de service sur la TOE en effectuant une action imprévue ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu…). Ce déni de service peut concerner toute la TOE ou seulement certaines de ses fonctions.
- **M.CONTOURNEMENT_CLOISONNEMENT_LOGIQUE :** l'attaquant parvient à violer la politique de cloisonnement logique (par exemple avec des attaques par « saut de VLAN »).
- **M.CORRUPTION_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. Enfin, l'attaquant peut également tenter d'installer une version légitime du *firmware* sans en avoir le droit.
- **M.CORRUPTION_CONFIGURATION :** l'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la TOE.
- **M.COMPROMISSION_CONFIGURATION :** un attaquant parvient à récupérer tout ou partie de la configuration de la TOE de manière illégitime.
- **M.VOL_IDENTIFIANTS :** l'attaquant parvient à récupérer les secrets de connexion d'un utilisateur ou d'un administrateur.
- **M.CONTOURNEMENT_AUTHENTIFICATION :** l'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

- **M.CONTOURNEMENT_POLITIQUE_DROITS :** l'attaquant parvient à obtenir des droits qui ne lui sont pas dévolus. À titre illustratif, un utilisateur déclaré réussit à élever ses droits pour obtenir ceux d'un administrateur.

3.5. DESCRIPTION DES FONCTIONS DE SÉCURITÉ

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- **F.GESTION_ENTRÉES_MALFORMÉES :** la TOE gère correctement les entrées malformées, en particulier en provenance du réseau. En effet, la fonction principale de la TOE est de commuter les paquets.
- **F.POLITIQUE_CLOISONNEMENT_LOGIQUE :** la TOE permet de mettre en place une politique de cloisonnement logique à l'aide de VLAN (par port, par protocole).
- **F.CONNEXION_SERVEUR_AUTHENT :** 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.
- **F.STOCKAGE_SÉCURISÉ_SECRETS :** les secrets de connexion des utilisateurs (et administrateurs) sont stockés de manière sécurisée sur la TOE et la compromission d'un fichier ne permet pas de les récupérer.
- **F.AUTHENT_INTERFACE_ADMIN :** 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.
- **F.POLITIQUE_DROITS :** la politique de gestion des droits est gérée de manière extrêmement stricte. 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.
- **F.SIGNATURE_FIRMWARE :** à chaque installation d'un nouveau *firmware*, l'intégrité et l'authenticité de celui-ci est vérifiée.
- **F.IC_CONFIGURATION :** la politique de gestion des utilisateurs ne permet à une personne non autorisée de modifier tout ou partie de la configuration de la TOE.

3.6. MATRICES DE COUVERTURE

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles :

	B.TRAMES	B.CLOISONNEMENT_LOGIQUE	B.AUTHENT_ÉQUIP_TERMINAUX	B.FIRMWARE	B.CONFIGURATION	B.AUTHENT_UTILISATEURS	B.SECRETS_CONNEXION_USERS	B.POL_GESTION_DROITS
M.DÉFAUT_RÉSILIENCE	**D**							
M.DÉNI_SERVICE	**D**	**DI**	**D**					
M.CONTOURNEMENT_CLOISONNEMENT_LOGIQUE		**I**						
M.CORRUPTION_FIRMWARE				**IA**				
M.CORRUPTION_CONFIGURATION					**I**			
M.COMPROMISSION_CONFIGURATION					**C**			
M.VOL_IDENTIFIANTS							**IC**	
M.CONTOURNEMENT_AUTHENTIFICATION			**IA**			**IA**		
M.CONTOURNEMENT_POLITIQUE_DROITS								**I**

Tableau 3 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F.GESTION_ENTRÉES_MALFORMÉES	F.POLITIQUE_CLOISONNEMENT_LOGIQUE	F.CONNEXION_SERVEUR_AUTHENT	F.STOCKAGE_SÉCURISÉ_SECRETS	F.AUTHENT_INTERFACE_ADMIN	F.POLITIQUE_DROITS	F.SIGNATURE_FIRMWARE	F.IC_CONFIGURATION
M.DÉFAUT_RÉSILIENCE	√							
M.DÉNI_SERVICE	√							
M.CONTOURNEMENT_CLOISONNEMENT_LOGIQUE		√						
M.CORRUPTION_FIRMWARE							√	
M.CORRUPTION_CONFIGURATION					√			√
M.COMPROMISSION_CONFIGURATION					√			√
M.VOL_IDENTIFIANTS				√	√			
M.CONTOURNEMENT_AUTHENTIFICATION			√		√			
M.CONTOURNEMENT_POLITIQUE_DROITS						√		

Tableau 4 - Couverture des menaces par les fonctions de sécurité

Fin du document