Profil de protection d'une diode industrielle et de ses guichets

Version 1.0 moyen-terme

GTCSI

1er juillet 2015

Avant-propos

Dans toute la suite de ce document, l'acronyme ToE (*Target of Evaluation*) désigne le composant qui est l'objet de l'évaluation.

Les passages en rouge sont ceux qui différent de la version de la cible à court terme.

1 Descriptif du produit

1.1 Descriptif général du produit

La ToE considérée dans ce profil de protection est une diode industrielle. Il s'agit d'un équipement qui sert à faire l'interface entre deux réseaux et qui n'autorise la communication que dans un seul sens et ce sans aucun canal retour.

Une diode industrielle sert à faire l'interface entre deux systèmes industriels, éventuellement de criticités différentes ou entre un système industriel critique et un système d'information de gestion. Les flux d'information ne seront alors possibles que depuis le système industriel le plus critique vers le moins critique ; l'objectif étant de protéger l'intégrité et la disponibilité du réseau le plus sensible.

Une diode industrielle doit pouvoir fonctionner dans un environnement hostile avec de l'humidité, de la poussière et des températures habituellement non supportées par des équipements classiques.

La ToE est composée de trois éléments principaux :

— la diode proprement dite qui assure l'unidirectionnalité de la communication de manière physique ;

— le guichet haut qui sert de passerelle et collecte les informations dans le réseau critique en terminant les connexions protocolaires. Par exemple, si des informations sont transmises en utilisant le protocole OPC-UA, le guichet haut doit contenir un client OPC-UA qui va aller chercher les informations auprès des serveurs OPC-UA concernés ;

— le guichet bas qui reçoit les informations transmises par le guichet haut au travers de la diode. Du fait de l'unidirectionnalité de celle-ci, un protocole spécifique doit être utilisé pour transmettre les informations. Ensuite, le guichet présente un serveur adapté aux équipements destinataires finaux de l'information.

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

— **Unidirectionalité des flux :** La ToE assure l'unidirectionnalité des flux entre le guichet haut et le guichet bas.

— **Terminaison protocolaire :** Les guichets de la ToE assurent la terminaison protocolaire dans les réseaux haut et bas. Les protocoles utilisés en haut et en bas ne sont pas nécessairement les mêmes.
— **Fonctions d'administration :** Chacun des guichets de la ToE est muni d'interfaces d'administration qui permettent de le configurer et de consulter et d'extraire les journaux d'évènements générés. Ces interfaces d'administration doivent pouvoir être accédées uniquement sur des réseaux dédiés à l'administration.
— **Journalisation locale d'évènements :** La ToE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration.
— **Journalisation distante d'évènements :** La ToE permet de définir une politique de journalisation distante d'évènements notamment de sécurité et d'administration.

1.3 Descriptif de l'utilisation du produit

En application du guide [1] de l'ANSSI, la ToE sera typiquement utilisée pour faire l'interface entre un réseau de classe 3 et un réseau de classe inférieure ou un réseau de gestion. Les flux vont alors du réseau de classe 3 vers le réseau de classe inférieure. En particulier, on pourra envisager que le guichet bas soit connecté à un réseau non-maîtrisé.

Conformément aux recommandations du guide de mesures détaillées [2], les interfaces d'administration doivent être connectées à des réseaux d'administration dédiés. Dans le cas du réseau de classe 3, ce réseau doit être physiquement disjoint du réseau de production. Dans le cas des réseaux de classe inférieure, le réseau d'administration pourra être isolé logiquement à l'aide de VPN ou, éventuellement, de technologies de type VLAN. Un environnement typique d'utilisation est représenté sur la figure 1.

Dans certains cas, le besoin de disponibilité de la diode est important et un fonctionnement en redondance est nécessaire. Cette redondance peut être gérée au niveau de l'ensemble ou au niveau de chaque guichet.

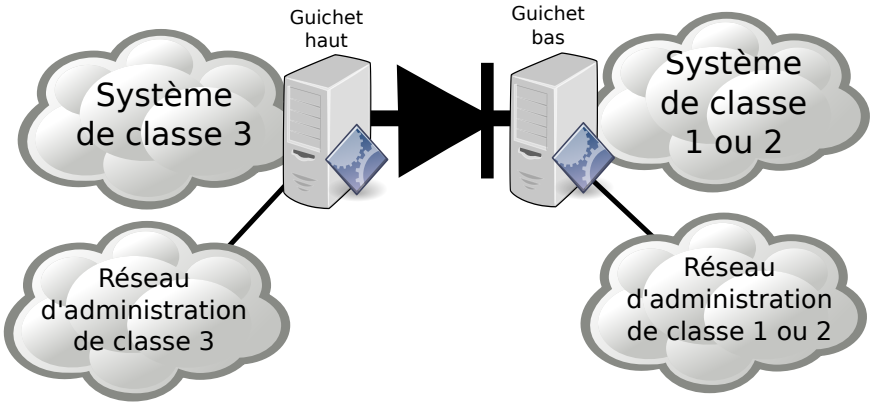

FIGURE 1 – Diode entre des systèmes de classe 3 et de classe inférieure

1.4 Descriptif des différents utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :
— **Administrateur :** Utilisateur ayant les droits de modifier une partie de la configuration de la ToE. Il ne peut cependant pas modifier les comptes des administrateurs.
— **Auditeur :** Utilisateur ayant le droit de consulter tout ou partie des journaux d'évènements produits par la ToE.
— **Super-administrateur :** Utilisateur ayant tous les droits sur la ToE, pouvant en particulier créer, modifier ou supprimer les comptes des administrateurs.

1. *La cybersécurité des systèmes industriels : Méthode de classification et mesures principales*, ANSSI, janvier 2014.
2. *La cybersécurité des systèmes industriels : Mesures détaillées*, ANSSI, janvier 2014.

— **Équipement terminal :** Équipement terminal connecté directement ou indirectement à la ToE.

Note : 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.

1.5 Hypothèses sur l'environnement

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

— **Consultation des journaux :** Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.

— **Administrateurs :** Les administrateurs de la ToE sont compétents, formés et non hostiles.

— **Local :** La ToE n'est pas nécessairement dans un local sécurisé et l'attaquant peut avoir accès à tous les ports de la ToE. De façon similaire, l'attaquant peut arriver à faire brancher un dispositif piégé (par exemple une clé USB ou une carte SD) sur n'importe quel port physique de la ToE. En revanche, il ne peut pas la démonter ou effectuer d'attaque physique dessus.
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.

— **Sens de la diode et guichets :** La ToE est supposée adaptée au cas d'usage. En particulier, la diode est dans le bon sens et les guichets employés proposent des protocoles adaptés.
La diode est également le seul équipement d'interconnexion entre les deux réseaux.

— **Dimensionnement :** Il est supposé que la ToE est dimensionnée correctement pour les traitements qu'elle doit effectuer.

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

— **Services non évalués désactivés par défaut :** 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).

— **Documentation de securité :** 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.

2 Description des biens sensibles à protéger

2.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

— **Réseau critique :** La ToE protège le réseau le plus critique en assurant l'unidirectionnalité des échanges.

— **Échanges au travers de la diode :** La ToE assure la transmission de données entre son guichet haut et son guichet bas.

Les besoins de sécurité pour les biens sensibles de l'environnement sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Réseau critique	X		X	
Échanges au travers de la diode	X		X	
X : obligatoire (X) : optionnel				

2.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :

— **Firmware des guichets :** Afin d'assurer correctement leurs fonctions, les firmwares des guichets de la ToE doivent être intègres. Ceci inclut toute modification temporaire ou permanente.
— **Configuration des guichets :** Les configurations des guichets de la ToE doivent être confidentielles et intègres.
— **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, chacun des guichets de la ToE doit protéger l'intégrité et l'authenticité du mécanisme.
— **Secrets de connexion des utilisateurs :** Il peut s'agir de mots de passe, de certificats, etc. Pour chaque guichet de la ToE, il 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.
— **Politique de gestion des droits :** Pour chacun des guichets de la ToE, cette politique peut être contenue en local 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.
— **Fonction de journalisation locale :** La ToE dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle.
— **Fonction de journalisation distante :** La ToE dispose d'une fonction de journalisation distante qui, une fois configurée, doit rester opérationnelle.
— **Journaux d'évènements locaux :** Les journaux locaux générés par la ToE doivent être intègres.
— **Journaux d'évènements déportés :** Les journaux déportés émis par la ToE doivent être intègres et authentifiés. Un mécanisme doit également permettre au destinataire de détecter l'absence d'un message au sein d'une sequence de messages correctement reçus.

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Firmware des guichets			X	X
Configuration des guichets		X	X	
Mécanisme d'authentification des utilisateurs			X	X
Secrets de connexion des utilisateurs		X	X	
Politique de gestion des droits			X	
Fonction de journalisation locale	X			
Fonction de journalisation distante	X			
Journaux d'évènements locaux			X	X
Journaux d'évènements déportés			X	X
X : obligatoire (X) : optionnel				

3 Description des menaces

3.1 Description des agents menaçants

Les agents menaçants suivants ont été retenus :
— **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.
— **Attaquant avec les droits d'administration :** L'attaquant a réussi à compromettre le compte d'un administrateur. Ce compte peut avoir n'importe quel rôle à l'exception du super-administrateur.

3.2 Menaces retenues

Les menaces suivantes ont été retenues :
— **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 (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.
— **Violation de l'unidirectionnalité des échanges :** L'attaquant parvient à violer l'unidirectionnalité des échanges et à faire transiter des informations du guichet bas vers le guichet haut.
— **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.
Enfin, l'attaquant peut également tenter d'installer une version légitime du firmware sans en avoir le droit.
— **Corruption de la configuration :** L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.
— **Compromission de la configuration :** L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.
— **Vol d'identifiants :** L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.
— **Contournement de l'authentification :** L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.
— **Contournement de la politique de droits :** L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus.
— **Corruption des journaux d'évènements locaux :** L'attaque 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.
— **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.

4 Objectifs de sécurité

Les objectifs de sécurité retenus sont les suivants :
— **Gestion des entrées malformées :** La ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance du réseau.

- **Unidirectionnalité des flux :** L'unidirectionnalité des flux est assurée de manière physique par la ToE.
- **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.
- **Stockage sécurisé des secrets :** Les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la ToE et la compromission d'un fichier ne permet pas de les récupérer.
- **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.
- **Politique de 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.
- **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.
- **Intégrité et confidentialité de la configuration :** La politique de gestion des utilisateurs ne permet à une personne non autorisée, ni de consulter, ni de modifier tout ou partie de la configuration de la ToE.
- **Intégrité des journaux :** Les journaux d'événements générés par la ToE sont intégres et seul le super-adminstrateur peut les modifier.
- **Intégrité des journaux déportés :** La ToE permet de transmettre les journaux déportés à un équipement tiers de manière intègre, authentifiée, et sans rejeu des journaux générés avec détection des événements manquants.

A Couverture des biens par les menaces

	Réseau critique	Échanges au travers de la diode	Firmware des guichets	Configuration des guichets	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Déni de service	D I	D I						D	D		
Violation de l'unidirectionnalité des échanges	D I										
Corruption du firmware			I A								
Corruption de la configuration				I							
Compromission de la configuration				C							
Vol d'identifiants						C I					
Contournement de l'authentification					I A						
Contournement de la politique de droits							I				
Corruption des journaux d'évènements locaux										I A	

D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité

	Réseau critique	Échanges au travers de la diode	Firmware des guichets	Configuration des guichets	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Corruption des journaux d'évènements déportés											I A
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité											

B Couverture des menaces par les objectifs de sécurité

	Déni de service	Violation de l'unidirectionnalité des échanges	Corruption du firmware	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'évènements locaux	Corruption des journaux d'évènements déportés
Gestion des entrées malformées	X									
Unidirectionnalité des flux		X								
Connexion sécurisée avec le serveur d'authentification							X			
Stockage sécurisé des secrets						X				
Authentification sécurisée sur l'interface d'administration				X	X	X	X			
Politique de droits								X		
Signature du firmware			X							
Intégrité et confidentialité de la configuration				X	X					
Intégrité des journaux									X	

	Déni de service	Violation de l'unidirectionnalité des échanges	Corruption du firmware	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'évènements locaux	Corruption des journaux d'évènements déportés
Intégrité des journaux déportés										X

C Liste des contributeurs

Ce profil de protection a été rédigé dans le cadre des travaux du groupe de travail sur la cybersécurité des systèmes industriels (GTCSI) sous l'égide de l'ANSSI.

Les sociétés et organismes suivants ont apporté leur concours à la rédaction de ce document :

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