Profil de protection d'un logiciel d'ingénierie

Version 1.0 moyen-terme

GTCSI

11 septembre 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.

1 Descriptif du produit

1.1 Descriptif général du produit

La ToE considérée dans ce profil de protection est un logiciel d'ingénierie. Celui-ci permet d'assurer la configuration, le paramétrage, la programmation, les tests et les diagnostics de tout ou partie d'un système d'automatisme et de supervision industriel.

Pour fonctionner, un logiciel d'ingénierie requiert des données de configuration. Elles sont constituées de l'ensemble des informations nécessaires à l'adaptation de son fonctionnement au contexte d'une installation particulière. Le type de données dépend du contexte considéré.

- Les données typiques d'un système d'automatisme comprennent : la configuration matérielle, les entrées/sorties terrain, le paramétrage, les programmes utilisateurs...
- Les données de configuration typiques d'un produit SCADA comprennent : les tables d'échanges avec les équipements d'automatisme, la communication avec les équipements, les vues graphiques, les caractéristiques d'archivage...

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

- **Programmation et configuration :** La ToE permet de programmer et de configurer tout ou partie d'un système d'automatisme ou de supervision industriels.
  A cette fin, la ToE permet la création, la gestion et la consultation des programmes utilisateurs.
- **Diagnostic :** La ToE permet d'effectuer du diagnostic sur tout ou partie d'un système d'automatisme ou de supervisionindustriels.
- **Gestion de version :** La ToE permet la gestion des différentes versions de configuration et de programmes utilisateurs pour un système d'automatisme ou de supervision industriels donné.
- **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).
- **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

Dans certains cas, le poste contenant la ToE peut être connecté directement aux équipements d'automatismes ou au système de supervision, auquel cas les données du procédé industriel peuvent être issues de l'installation réelle. Dans d'autres cas, la ToE peut être utilisée dans un environnement de test, auquel cas le procédé est simulé, et les données ne sont pas issues de l'installation réelle.

Lorsque le poste contenant la ToE est connecté au système de production, conformément aux recommandations du guide de l'ANSSI [1], il doit être éteint et stocké dans un endroit sécurisé lorsqu'il n'est pas utilisé. La mise en œuvre d'une architecture sécurisée d'administration comme celles qui sont décrites dans le guide publié par l'ANSSI [2] peut également être envisagée.

1.4 Descriptif des différents utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :

— **Configurateur/programmeur/automaticien :** Ce profil permet de modifier la configuration et les programmes utilisateurs des équipements d'automatisme et de supervision. Dans le cas d'équipements embarqués comme des automates, il peut également mettre à jour le firmware de l'équipement. Dans la suite, du fait de ses privilèges élevés, ce profil est également appelé administrateur.

— **Super-administrateur :** Utilisateur ayant tous les droits sur la ToE, pouvant en particulier créer, modifier ou supprimer les comptes des administrateurs.

— **Auditeur :** Utilisateur ayant le droit de consulter tout ou partie des journaux d'évènements produits par 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.

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

— **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.

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

— **Système d'exploitation sain :** Le système d'exploitation du système portant la ToE est considéré comme sain au début de l'évaluation et tout au long de l'évaluation sauf en cas de défaillance de la ToE.

— **Système d'exploitation durci :** Le système d'exploitation est supposé avoir été configuré et durci selon les recommandations du fabricant de la ToE.
En particulier, le système d'exploitation est supposé à jour.

1. La cybersecurité pour les systèmes industriels : Mesures détaillées, ANSSI, janvier 2014.
2. Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, février 2015

— **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.
— **Module externe :** Il supposé qu'aucun module externe [3] n'est installé sur la ToE sauf si celui-ci fait partie du périmètre d'évaluation.
— **Non-adhérence logicielle :** La ToE a été développée de telle sorte à ne pas être adhérente à une version donnée d'un composant externe [4] (système d'exploitation, logiciel, bibliothèque). En particulier, l'utilisateur doit avoir la possibilité d'appliquer les mises à jour de sécurité de tout composant externe.
Dans le cas contraire, ce composant doit être intégré à la ToE.
— **Poste dédié :** Le poste sur lequel la ToE est installée est dédié à l'ingénierie et n'a notamment pas accès à Internet.

2 Description des biens sensibles à protéger

2.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :
— **Flux avec les systèmes et équipements configurés ou programmés :** La ToE protège en intégrité, authenticité et éventuellement en confidentialité les échanges avec les systèmes dont elle assure la configuration et la programmation.
— **Versions des configurations et programmes utilisateurs :** La ToE doit assurer l'intégrité, l'authenticité et éventuellement la confidentialité des différentes versions des éléments de configuration et des programmes utilisateurs récupérés ou destinés à être déployés sur les équipements d'automatisme ou systèmes de supervision.

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

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Flux avec les systèmes et équipements configurés ou programmés		(X)	X	X
Versions des configurations et programmes utilisateurs		(X)	X	X
X : obligatoire (X) : optionnel				

2.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :
— **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 la mise à jour.
— **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.

3. Un module externe est un élément logicel apportant de nouvelles fonctionnalités à la ToE mais qui n'est pas indispensable à son fonctionnement.
4. Un composant externe est un élément logiciel nécessaire au fonctionnement de la ToE.

— **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].
— **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.
— **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.
— **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
Logiciel(s)			X	X
Configuration		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

L'agent menaçant suivant a été retenu :
— **Attaquant dans le système industriel :** Tout attaquant ayant pris le contrôle d'un composant du système industriel et cherchant à attaquer la ToE.

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.

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.
— **Altération des flux :** L'attaquant parvient à modifier des échanges entre la ToE et un composant externe sans que cela ne soit détecté.
— **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.
— **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.
— **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.
— **Corruption de données :** L'attaquant parvient à modifier des données, sans en avoir le droit, en exploitant une faille de la ToE.
— **Compromission de données :** L'attaquant parvient à exploiter une faille dans la ToE pour accéder des informations auxquelles il ne devrait pas avoir accès.
— **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.
— **Communications sécurisées :** La ToE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.
— **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 et la compromission d'un fichier ne permet pas de les récupérer.
— **Stockage sécurisé :** La ToE permet d'assurer le stockage sécurisé en assurant la confidentialité et l'intégrité d'informations stockées en local à l'aide de mécanismes cryptographiques.
— **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 programme utilisateur :** Afin de se protéger contre l'injection d'un programme utilisateur ou d'une configuration illégitime, la ToE permet de signer et de vérifier la signature d'éléments venant de l'extérieur avant mise à jour du système administré [6].
— **Signature du logiciel :** Un mécanisme de signature est utilisé par la ToE pour permettre la vérification par l'administrateur de l'authenticité et de l'intégrité des composants logiciels lors de leur installation.
— **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.

6. Des outils standard doivent être privilégiés à cet effet (PKCS#7, par exemple). Les mécanismes cryptographiques choisis doivent être conformes au RGS.

A Couverture des biens par les menaces

	Flux avec les systèmes et équipements configurés ou programmés	**Versions des configurations et programmes utilisateurs**	**Logiciel(s)**	**Configuration**	**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	D		
Altération des flux	I A										
Compromission des flux	(C)										
Corruption du logiciel			I A								
Corruption de la configuration				I							
Compromission de la configuration				C							
Corruption de données		I A									
Compromission de données		(C)									
Vol d'identifiants						C I					
Contournement de l'authentification					I A						
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité											

	Flux avec les systèmes et équipements configurés ou programmés	Versions des configurations et programmes utilisateurs	Logiciel(s)	Configuration	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
Contournement de la politique de droits							I				
Corruption des journaux d'évènements locaux										I A	
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	Altération des flux	Compromission des flux	Corruption du logiciel	Corruption de la configuration	Compromission de la configuration	Corruption de données	Compromission de données	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												
Communications sécurisées		X	X										
Connexion sécurisée avec le serveur d'authentification										X			
Stockage sécurisé des secrets									X				
Stockage sécurisé							X	X					
Authentification sécurisée sur l'interface d'administration					X	X			X	X			
Politique de droits											X		
Signature du programme utilisateur							X						
Signature du logiciel				X									

	Déni de service	Altération des flux	Compromission des flux	Corruption du logiciel	Corruption de la configuration	Compromission de la configuration	Corruption de données	Compromission de données	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 et confidentialité de la configuration					X	X							
Intégrité des journaux												X	
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
— Areal
— Codra
— DGA/MI
— EDF
— Gimelec
— Oppida
— Ordinal Software (représentant le club MES)
— RATP
— Schneider Electric
— Siemens
— Sogeti
— Stormshield
— Thales