Profil de protection d'un automate programmable industriel

Version 1.1 moyen-terme

GTCSI

13 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

Un automate programmable industriel est un équipement qui permet de réaliser, de façon continue et sans intervention humaine, la commande de processus industriels (machine ou processus continu). En fonction de ses données d'entrées, reçues des capteurs, l'automate envoie des ordres vers ses sorties, les actionneurs.

En plus des modèles standard, il existe deux types d'automates programmables :

— les systèmes redondants, pour augmenter la disponibilité des installations, et

— les systèmes de sécurité, utilisés pour assurer la protection des biens et des personnes (sécurité fonctionnelle). L'ensemble relève de la sûreté de fonctionnement.

L'automate programmable industriel doit pouvoir fonctionner dans un environnement hostile. En particulier, il doit pouvoir fonctionner en présence d'humidité ou de poussière ou avec des températures inhabituelles pour des équipements informatiques.

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

— **Exécution d'un programme automate :** La ToE exécute un programme fourni par l'utilisateur. Ce programme lit les entrées de la ToE, effectue son traitement et met à jour ses sorties.

— **Gestion des éntrées/sorties :** La ToE est capable de communiquer pour lire ou écrire sur des entrées/sorties déportées ou non. Ces entrées/sorties peuvent être numériques, analogiques ou de type « tout ou rien ». Elles permettent à la ToE de contrôler et de commander le processus industriel.

— **Communication avec la supervision :** La ToE peut communiquer avec la supervision (SCADA) pour recevoir des ordres et remonter des informations sur le processus industriel.

— **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

Un automate programmable industriel peut s'inscrire dans un grand nombre d'architectures. Mais un schéma directeur ressort. L'automate est relié à ses entrées-sorties et à son interface homme machine locale (pupitre opérateur) via une même interface de communication, sur le réseau de terrain. Les échanges vers la supervision (IHM SCADA) se font au travers d'une interface de communication dédiée sur le réseau de supervision.

L'administration de l'automate programmable industriel se fait avec une station d'ingénierie. Les modifications du firmware et du programme utilisateur peuvent être généralement envoyées sur l'automate par le réseau, par un lien série ou à l'aide de supports amovibles (cartes SD ou clés USB par exemple).

Dans le cas d'une administration par le réseau, il est recommandé d'utiliser un réseau séparé physiquement ou, au minimum, logiquement. En pratique, une station d'ingénierie est souvent présente sur le réseau de supervision. Il est recommandé que celle-ci ne soit pas branchée en permanence mais uniquement en cas de besoin.

Cette architecture basique est représentée sur la figure 1.

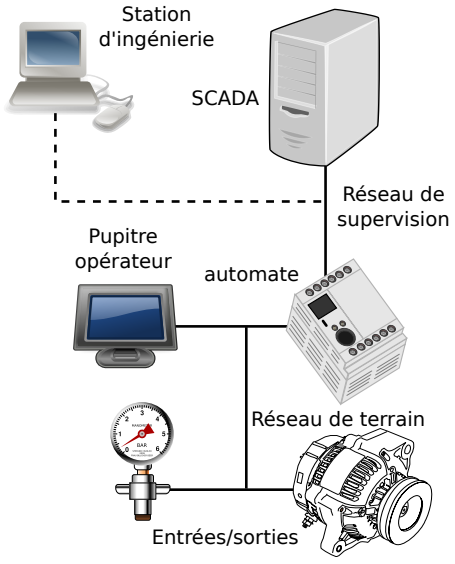

FIGURE 1 – Architecture type d'un réseau pour un automate programmable industriel

1.4 Descriptif des différents utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :
— **Opérateur d'exploitation :** Cet utilisateur n'a accès aux informations contenues dans la ToE qu'en lecture simple et ne peut rien modifier.
— **Technicien :** Cet utilisateur a les mêmes droits que l'utilisateur précédent mais il peut également modifier certaines variables dans la ToE.
— **Automaticien/administrateur :** Cet utilisateur a tous les droits et peut en particulier modifier le programme automate et mettre à jour le firmware de la ToE. Dans certains contextes, le terme « programmeur » est utilisé pour désigner ce type d'utilisateur.

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.
- **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 :

- **Commande du procédé industriel :** La ToE participe à la commande et au contrôle d'un processus industriel en lisant des entrées et en envoyant des ordres aux actionneurs. Ces actions doivent être protégées en disponibilité et en intégrité.
- **Échanges entre la ToE et la supervision :** Les échanges entre la supervision et la ToE sont nécessaires au bon fonctionnement du système industriel dans son ensemble et doivent être intègres et authentiques.
- **Flux vers la station d'ingénierie :** Les flux entre la ToE et la station d'ingénierie doivent être protégés en intégrité, en confidentialité et en authenticité.
- **Échanges entre la ToE et un autre automate :** Pour les communications entre la ToE et un autre automate, l'utilisation d'entrées/sorties dédiées devrait être privilégiée. Néanmoins, dans le cas où ces communications doivent transiter sur un réseau mutualisé, elles doivent être protégées en intégrité et en authenticité.

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

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Commande du procédé industriel	X		X	
Échanges entre la ToE et la supervision			X	X
Flux vers la station d'ingénierie		(X)	X	X
Échanges entre la ToE et un autre automate			X	X
X : obligatoire (X) : optionnel				

2.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :

— **Firmware :** Afin d'assurer correctement ses fonctions, le firmware de la ToE doit être intègre et authentique.

— **Programme utilisateur :** La ToE exécute un programme écrit et chargé par l'utilisateur et décrivant son fonctionnement. Il doit être protégé en confidentialité [1] , en intégrité et en authenticité.

— **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.

— **Mode de fonctionnement de la ToE :** Le mode de fonctionnement de la ToE (run ou stop par exemple) doit être protégé en intégrité et authenticité.

— **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 [2].

— **Secrets de connexion des utilisateurs :** Il peut s'agir de mots de passe, de certificats, etc. Ils peuvent être contenus dans la ToE 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 :

1. La confidentialité n'est pas primordiale pour protéger un système industriel, il s'agit d'une mesure de défense en profondeur. Cette propriété peut également être recherchée à des fins de protection du secret industriel.
2. 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.

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Firmware			X	X
Programme utilisateur		(X)	X	X
Configuration		(X)	X	
Mode de fonctionnement de la ToE			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 :

— **Attaquant sur le réseau de supervision :** L'attaquant a la maîtrise d'un équipement sur le réseau de supervision de l'automate.

— **Attaquant sur le réseau de terrain :** L'attaquant a la maîtrisie d'un équipement sur le réseau de terrain.

— **Utilisateur malveillant :** L'attaquant a réussi à compremettre un compte sans privilèges d'administration et cherche à outrepasser les droits de son compte.

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.

— **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 du mode de fonctionnement :** L'attaquant parvient à modifier le mode de fonctionnement de la ToE sans en avoir le droit (envoi d'une commande stop par exemple) ;
- **Compromission du programme utilisateur :** L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE par d'autres moyens que l'observation de l'activité de la ToE [3].
- **Corruption du programme utilisateur :** L'attaquant parvient à modifier, de façon temporaire ou permanente, le programme utilisateur.
- **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.
- **Injection de commandes ou paramètres :** L'attaquant parvient à modifier des paramètres à l'intérieur de la ToE ou de lui passer des commandes sans y être autorisé.

- **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.

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.
- **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

3. Cette menace n'est considérée que lorsque la confidentialité du programme utilisateur est un besoin de sécurité identifié.

la configuration de la ToE.

— **Authenticité, intégrité du programme utilisateur :** La ToE doit pouvoir protéger le programme utilisateur de façon à ce que seuls les utilisateurs autorisés puissent modifier celui-ci.
— **Confidentialité du programme utilisateur :** La ToE assure la confidentialité du programme utilisateur de telle sorte que seuls les utilisateurs autorisés y aient accès.
— **Authenticité et intégrité des commandes du mode de fonctionnement :** La ToE doit garantir que le mode de fonctionnement ne pourra être modifié que par des personnels autorisés et donc authentifiés.
— **Communications sécurisées :** La ToE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et, éventuellement, en confidentialité avec des composants externes.
— **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

	Commande du procédé industriel	**Échanges entre la ToE et la supervision**	**Flux vers la station d'ingénierie**	**Échanges entre la ToE et un autre automate**	**Firmware**	**Programme utilisateur**	**Configuration**	**Mode de fonctionnement de la ToE**	**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'événements locaux**	**Journaux d'événements déportés**
Déni de service	D											D	D		
Corruption du firmware					I A										
Corruption du mode de fonctionnement								I							
Compromission du programme utilisateur						(C)									
Corruption du programme utilisateur	I					I A									
Corruption de la configuration							I								
Compromission de la configuration							(C)								
Vol d'identifiants										C I					
Contournement de l'authentification									I A						

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

	Commande du procédé industriel	Échanges entre la ToE et la supervision	Flux vers la station d'ingénierie	Échanges entre la ToE et un autre automate	Firmware	Programme utilisateur	Configuration	Mode de fonctionnement de la ToE	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
Injection de commandes ou paramètres	D I	I A													
Altération des flux	D I	I A	I A	I A											
Compromission des flux			(C)												

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

B Couverture des menaces par les objectifs de sécurité

	Déni de service	Corruption du firmware	Corruption du mode de fonctionnement	Compromission du programme utilisateur	Corruption du programme utilisateur	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	Injection de commandes ou paramètres	Altération des flux	Compromission des flux
Gestion des entrées malformées	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								
Authenticité, intégrité du programme utilisateur					X										
Confidentialité du programme utilisateur				X											

	Déni de service	Corruption du firmware	Corruption du mode de fonctionnement	Compromission du programme utilisateur	Corruption du programme utilisateur	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	Injection de commandes ou paramètres	Altération des flux	Compromission des flux
Authenticité et intégrité des commandes du mode de fonctionnement			X												
Communications sécurisées													X	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
— Belden
— DGA/MI
— Gimelec
— Oppida
— Phoenix Contact
— RATP
— Schneider Electric
— Siemens
— Sogeti
— Stormshield
— Thales