
Profil de protection d'un progiciel serveur applicatif SCADA

Version 1.0 moyen-terme

GTCSI

1^{er} 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 diffèrent de la version de la cible à court terme.

1 Descriptif du produit

1.1 Descriptif général du produit

Un système de supervision industrielle permet d'acquérir et de traiter un grand nombre de données : télémessures, télésignalisations et téléalarmes. Il permet également de contrôler des équipements industriels — automates, capteurs, actionneurs — en leur envoyant des télécommandes et des téléajustages.

Un tel système est utilisé au sein de réseaux industriels. Il est interconnecté avec des équipements de terrain de niveau CIM 1 et peut s'interfacer avec d'autres équipements et logiciels tiers des niveaux CIM 2 ou CIM 3.

Un système de supervision industrielle est constitué de divers composants matériel et logiciel qui utilisent différentes informations pour fonctionner. Le système peut être modélisé sommairement comme sur la figure 1.

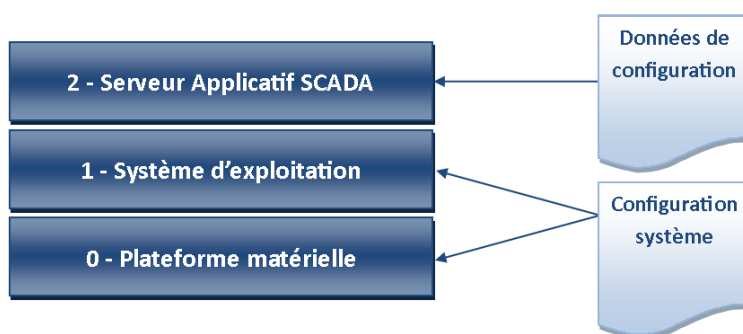


FIGURE 1 – Modélisation d'un système de supervision industrielle

Couches 0 - Plateforme matérielle et 1 – Système d'exploitation Elles constituent la plateforme d'exécution du produit. Il s'agit de machines de type station de travail ou serveur, sous Microsoft Windows, Solaris, l'une des nombreuses distributions Linux ou tout autre

système d'exploitation dit « classique » (par opposition à des plateformes d'exécution spécifiques constructeur). Dans la suite de ce document, les briques du système d'exploitation nécessaires au bon fonctionnement du produit sont considérées comme faisant partie de cette plateforme d'exécution du produit. Il en est de même des applicatifs tels qu'un gestionnaire de bases de données ou un serveur web assurant des fonctionnalités d'usage général et présentant un certain niveau d'intégration avec le système d'exploitation.

Pour fonctionner, ces couches systèmes nécessitent un certain nombre d'éléments dits de « configuration système ».

Couche 2 – Serveur Applicatif SCADA Elle constitue la ToE et assure les fonctionnalités décrites au paragraphe 1.2.

Pour fonctionner, un Serveur Applicatif SCADA requiert des données de configuration. Elles sont constituées de l'ensemble des informations nécessaires au paramétrage du Serveur Applicatif SCADA pour adapter son fonctionnement au contexte d'une installation particulière. Les données de configuration typiques d'un produit SCADA comprennent : la liste des entrées/sorties terrain, la communication avec les équipements, les caractéristiques d'archivage. . .

En plus de ses données de configuration, un Serveur Applicatif SCADA manipule des données que l'on peut qualifier de « procédé ». Elles sont constituées de l'ensemble des informations en relation directe avec l'installation. On peut y trouver :

- des données issues du terrain et manipulées par le Serveur Applicatif SCADA. Ces données sont importantes pour permettre à l'utilisateur de contrôler le fonctionnement de l'installation.
- des données types commandes préconfigurées ou recettes qui peuvent, si envoyées aux équipements impacter le fonctionnement de l'installation.

Note : La mise en œuvre d'un système SCADA peut requérir l'usage d'extensions tierces. Il s'agit d'un ensemble de composants logiciels, usuellement basés sur un SDK ou des interfaces du Serveur Applicatif SCADA. De telles extensions sont parfois développées de façon à assurer des besoins particuliers tels que l'interfaçage avec des composants tiers, des traitements de données métier spécifiques. . .

Elles n'entrent pas dans le périmètre de ce profil de protection, mais devraient l'être si l'on traitait le cas d'une installation particulière faisant usage de tels composants. Etant de même nature que le produit SCADA en lui-même, elles présentent potentiellement les mêmes risques, sont sujet aux mêmes menaces et peuvent également apporter des fonctions de sécurité.

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

- **Acquisition des données terrain et envoi de commandes** : La ToE peut comporter un frontal de communication prenant en charge les échanges avec les équipements de terrain tels que des automates programmables industriels, des contrôleurs, des IED¹. . . (niveau CIM 1).
- **Échanges de données** : La ToE peut envoyer et recevoir des flux d'information en s'appuyant sur des interfaces avec des systèmes tels qu'un serveur d'historiques, un MES, un serveur de paramétrage, une station d'ingénierie, des serveurs applicatifs SCADA, des postes clients. . .
Ces systèmes peuvent se trouver sur le même niveau CIM 2, sur le niveau CIM 3, ou même être déportés sur un réseau externe.
- **Gestion des alarmes procédé** : La ToE détecte des conditions d'alarmes sur le procédé à partir des informations reçues des équipements de terrain et en assure le traitement et la transmission.
- **Fonctions d'administration** : La ToE comporte une ou plusieurs interfaces pour permettre son administration, notamment la gestion des utilisateurs et de la politique de droits.

1. *Intelligent Electronic Device*, terme utilisé dans le domaine de l'énergie électriques qui regroupe tous les équipements d'automatisme ayant des fonctions de protection ou de pilotage local tels que les disjoncteurs, transformateurs

- **Fonctions de configuration** : Le serveur comporte une ou plusieurs interfaces permettant d'assurer la mise à jour et le déploiement des données de configuration : données d'entrée/sortie, communication avec les équipements de terrain, conditions d'alarmes.
- **Traitement de données et scripting** : La ToE peut assurer des fonctions de traitement et de calcul de variables dérivées.
- **Fonctions de redondance** : La ToE peut permettre un fonctionnement en redondance pour assurer la haute disponibilité d'une ou plusieurs de ses fonctions.
- **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 Serveur Applicatif SCADA peut être mis en œuvre dans deux types d'architectures principales :

- un poste SCADA tout-en-un ;
- des architectures client-serveur.

Dans les schémas qui suivent, les éléments en pointillés — composants et flux — sont hors scope de ce profil de protection.

1.3.1 Poste SCADA tout-en-un

Dans cette architecture, l'ensemble des composants logiciels SCADA sont déployés sur une machine unique :

- le (ou les) composants serveur(s) applicatif(s) assurant les fonctions de frontal de communication, de gestion d'alarmes, de traitement de données, etc ;
- le client graphique.

C'est l'architecture habituelle des pupitres opérateurs représentée sur la figure 2.

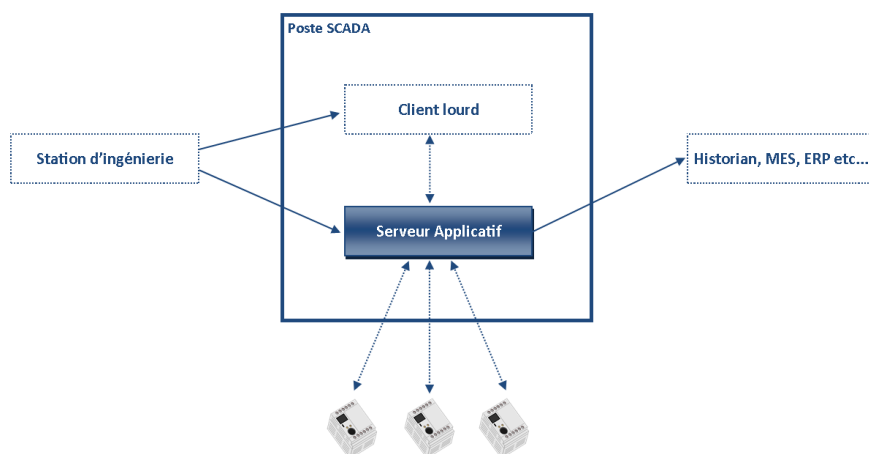


FIGURE 2 – Exemple d'architecture type pupitre opérateur

1.3.2 Architecture client-serveur

Dans ce type d'architecture, les composants logiciels SCADA sont déployés sur un ensemble de machines afin de distribuer les traitements et de redonder certaines fonctions :

- les frontaux de communication ;
- la gestion d'alarmes ;
- le traitement de données ;

- les fonctions métiers spécifiques ;
 - les interfaces Web ;
 - les clients graphiques locaux ;
 - les clients graphiques déportés.
- Cette architecture est représentée sur la figure 3.

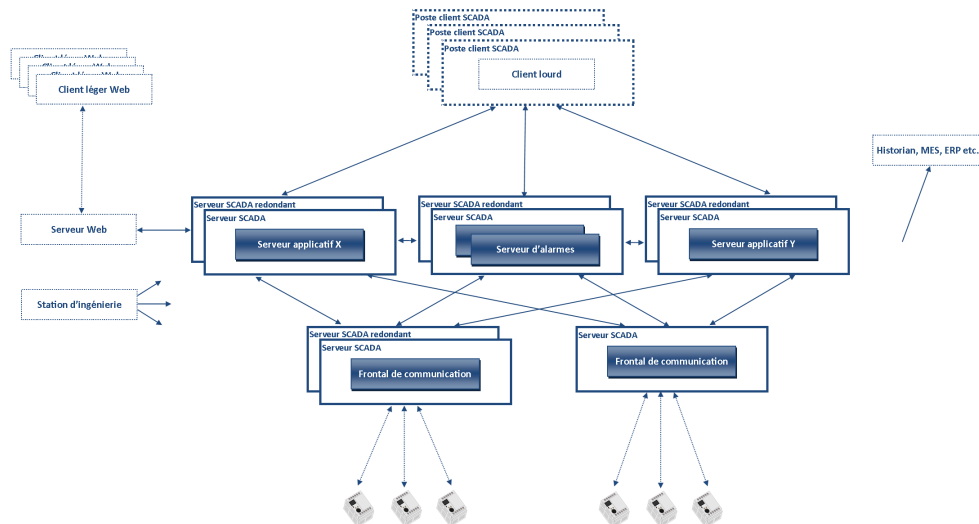


FIGURE 3 – Exemple d'architecture type Client-Serveur

Une variante de ce type d'architecture constitue les architectures distribuées comprenant des liaisons inter-sites :

- les frontaux de communication locaux ;
- les clients déportés ;
- etc.

1.4 Descriptif des différents utilisateurs

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

- **Opérateur** : Ce sont les utilisateurs légitimes de la ToE dans son mode de fonctionnement nominal.
L'opérateur peut, en fonction des droits qui lui sont attribués, au travers des IHM :
 - consulter les données, notamment par navigation dans les vues graphiques ;
 - envoyer des commandes ;
 - consulter les événements et les historiques ;
 - consulter et acquitter les alarmes.
- **Configureur/développeur** : Ce profil permet de modifier la configuration voire de reprogrammer certaines parties de la ToE sans pouvoir modifier le logiciel sous-jacent.
- **Administrateur** : Ce profil permet d'installer, de mettre à jour le logiciel de base de la ToE. Il permet également de définir la politique de droits des utilisateurs à l'exception des droits d'administration.
- **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.

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.
- **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.
- **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.
- **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 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.
- **Module externe** : Il supposé qu'aucun module externe² 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 externe³ (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.

2 Description des biens sensibles à protéger

2.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

- **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.
- **Flux vers un serveur d'historique** : Les flux entre la ToE et la station d'ingénierie doivent être protégés en intégrité, en confidentialité et en authenticité.
- **Flux de collaboration** : Ils sont constitués de l'ensemble des flux entre la ToE et d'autres composants du système. Il s'agit par exemple des flux entre un frontal de communication et un autre serveur applicatif.
Les flux de données de collaboration doivent être protégés en intégrité et en authenticité.

2. Un module externe est un élément logiciel apportant de nouvelles fonctionnalités à la ToE mais qui n'est pas indispensable à son fonctionnement.

3. Un composant externe est un élément logiciel nécessaire au fonctionnement de la ToE.

Ils pourraient également être protégés en confidentialité pour des raisons de secret industriel mais ceci n'est pas considéré ici.

- **Flux de données avec les équipements terrain** : Les flux de données entre la ToE et les équipements de terrain (par exemple, les automates) doivent être protégés en authenticité et intégrité.
- **Données d'exploitation** : Les données d'exploitation sont constituées de l'ensemble des informations utiles au bon fonctionnement du système de supervision en phase opérationnelle. Cet ensemble comprend notamment des valeurs instantanées, des alarmes, des commandes. . .
Elles peuvent être mises à disposition d'applications tierces (Extensions applicatives, MES, ERP. . .) par la ToE au travers d'interfaces : API, SDK ou interfaces standard telles qu'OPC ou SNMP.
Ces données doivent être protégées en intégrité et authenticité. L'accès à ces données est régi par la politique de droit de la ToE.

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

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Flux vers la station d'ingénierie		(X)	X	X
Flux vers un serveur d'historique			X	X
Flux de collaboration			X	X
Flux de données avec les équipements terrain			X	X
Données d'exploitation			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.
- **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 mécanisme⁴.
- **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.

4. 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.

- **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

Les agents menaçants suivants ont été retenus :

- **Utilisateur malveillant** : L'attaquant a réussi à compromettre un compte sans privilèges d'administration et cherche à outrepasser les droits de son compte.
- **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.
- **Attaquant dans le système industriel** : Tout attaquant ayant pris le contrôle d'un composant du système industriel et cherchant à attaquer la ToE.

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.
- **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'événements locaux** : L'attaque parvient à supprimer ou modifier une entrée dans les journaux d'événements locaux sans y avoir été autorisé par la politique de droits de la ToE.
- **Corruption des journaux d'événements 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 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 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 intègres et seul le super-administrateur 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

	Flux vers la station d'ingénierie	Flux vers un serveur d'historique	Flux de collaboration	Flux de données avec les équipements terrain	Données d'exploitation	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'événements locaux	Journaux d'événements déportés
Déni de service											D	D		
Altération des flux	IA	IA	IA	IA	IA									
Compromission des flux	(C)													
Corruption du logiciel						IA								
Corruption de la configuration							I							
Compromission de la configuration							(C)							
Vol d'identifiants									CI					
Contournement de l'authentification								IA						
Contournement de la politique de droits					IA					I				
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité														

	Flux vers la station d'ingénierie	Flux vers un serveur d'historique	Flux de collaboration	Flux de données avec les équipements terrain	Données d'exploitation	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'événements locaux	Journaux d'événements déportés
Corruption des journaux d'événements locaux													I A	
Corruption des journaux d'événements 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	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
Gestion des entrées malformées	X										
Communications sécurisées		X	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 logiciel				X							
Intégrité et confidentialité de la configuration					X	X					
Intégrité des journaux										X	

Déni de service	
Altération des flux	
Compromission des flux	
Corruption du logiciel	
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	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