Profil de protection d'un progiciel serveur applicatif MES

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

Un logiciel de MES *(Manufacturing Execution System)*regroupe et organise sous une forme cohérente (système) les opérations qui se déroulent au sein de l'usine et de l'atelier (on parle parfois aussi de *Manufacturing Operation Management*).

Le MES couvre en particulier les fonctions de planification détaillée ou d'ordonnancement, de définition fine des produits, de répartition en tâches des ordres de fabrication, d'exécution, et de collecte de données permettant d'assurer la traçabilité du procédé, la traçabilité des produits et l'analyse de performance des installations.

Comme le périmètre couvert par ce type de logiciel peut varier considérablement d'un logiciel à l'autre, on se référera au standard ISA-95 pour le positionner quant à sa couverture des différentes fonctions :

- la gestion des ressources ;
- l'ordonnancement ;
- le cheminement des produits et des lots et le suivi des opérations ;
- la gestion des documents de l'atelier ;
- la collecte et acquisition de données ;
- la gestion du personnel ;
- la gestion de la qualité ;
- le processus de conformité libératoire ;
- la gestion ou le pilotage du procédé d'allocation des ressources machine ;
- la gestion de la maintenance ;
- la traçabilité ascendante et descendante du produit et la généalogie ;
- l'analyse des performances.

À titre purement informatif, l'éditeur du logiciel pourra s'il le souhaite présenter ce positionnement sous forme de diagramme radial comme dans la figure 1.

Ce système se situe au niveau 3 du CIM (Computer Integrated Manufacturing), soit entre les niveaux 1-2 du CIM (contrôle-commande / supervision) et le niveau 4 (progiciels intégrés de gestion / ERP).

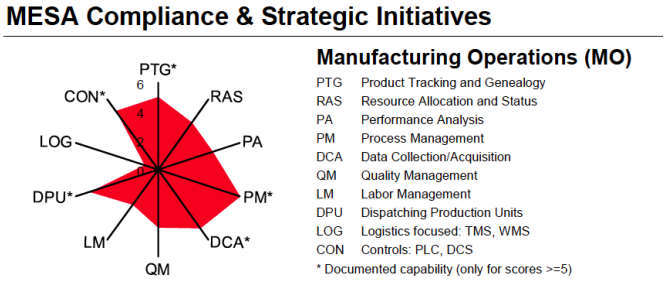

FIGURE 1 – Diagramme radial des grandes fonctions d'un logiciel MES (source MESA International)

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 IED [1]... (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.

— **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.

— **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.

— **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

L'architecture sur laquelle s'appuie un logiciel MES est le plus souvent du type représenté sur la figure 2. Une partie complémentaire, qui fait généralement partie de la périphérie de ce logiciel (douchettes code-barres, lecteurs de badges, terminaux dédiés, etc.) n'est pas représentée ici. Dans la pratique, cette périphérie est connectée soit aux automates programmables industriels (ou équipements équivalents, dont deux sont représentés), soit au serveur d'application, soit directement aux ordinateurs clients (douchettes ou lecteurs de badges par exemple).

Le découpage en composants, pour sa part, va dépendre en grande partie de la technologie utilisée pour la réalisation du logiciel MES. De par la vocation d'infrastructure d'un logiciel MES, on peut considérer que l'architecture est au minimum de type Client/Serveur. Par la suite, on va trouver deux grandes familles technologiques :

— les architectures de type « client lourd » : un ou plusieurs modules sont installés côté serveur et une application au minimum (parfois plusieurs dans le cas de plusieurs modules)

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

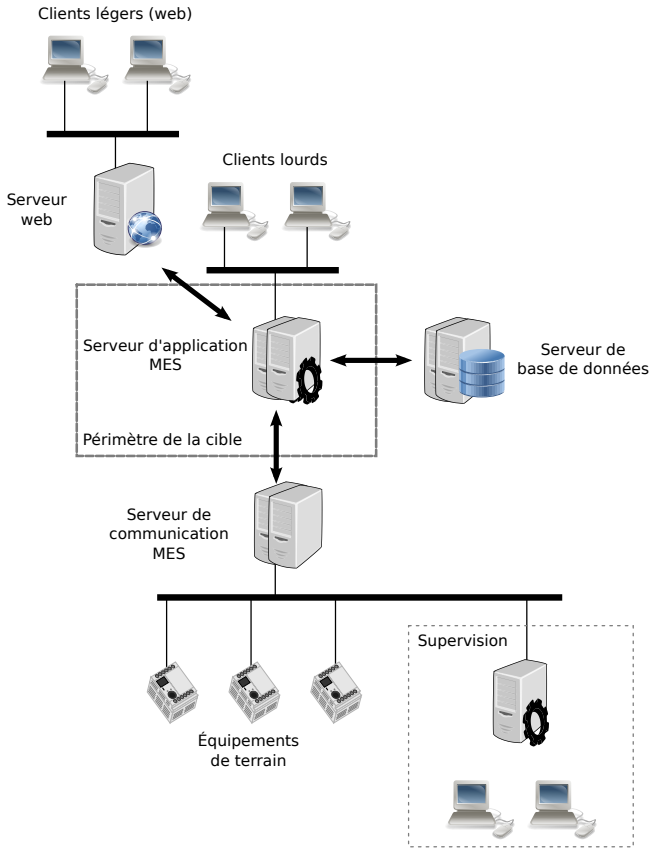

FIGURE 2 – Architecture non sécurisée d'un système MES avec clients lourds et clients web.

est installée sur chaque client.

— les architecture de type « web » : le ou les modules sont installés côté serveur et sont accédés par le client au moyen d'un navigateur standard ou d'une application d'accès générique.

Certaines solutions pourront être hybrides par rapport à ces deux grandes familles.

Ces composants seront souvent complétés par un (ou plusieurs) composants « Configurateur » ou « Environnement de développement » permettant de créer l'application. Ces éléments correspondent à ce que l'on appelle une station d'ingénierie dans le cas d'un système de supervision (SCADA). Mais cette configuration peut également être un mode particulier de l'exploitation, réservé à un profil d'utilisateur spécifique.

Sauf cas exceptionnels, les différents composants du logiciel MES s'appuient sur :

— un OS (généralement Windows ou Linux) ;

— les services d'une base de données tierce (SQL Server, Oracle, MySQL, etc.).

Ce profil de protection ne porte que sur le serveur d'application comme on peut le voir sur la figure 2. Néanmoins, ce profil de protection peut être adapté pour porter sur le serveur de communication.

1.4 Descriptif des différents utilisateurs

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

— **Opérateur :** Ce type de profil permet d'utiliser la ToE sans en modifier la configuration.

— **Configurateur/développeur :** Ce profil permet de modifier la configuration voire de reprogrammer certaines parties de la ToE sans pouvoir modifier le logiciel sous-jacent.

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

— **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.
— **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.
— **Bases de données saines :** Les bases de données sont supposées saines et les informations contenues sont correctes au début de l'évaluation. Il en restera de même au cours de l'évaluation sauf du fait d'une défaillance de la TOE.
— **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.
— **Non-adhérence logicielle :** La ToE a été développée de telle sorte à ne pas être adhérente à une version donnée d'un composant externe [2] (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.
— **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.

2. Un composant externe est un élément logiciel nécessaire au fonctionnement 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.

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. 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.

— **Description de l'installation et état des équipements :** Directement ou indirectement, soit au travers des informations fournies aux automatismes et aux opérateurs, le logiciel MES est amené à piloter, contrôler et réguler un système de production physique. En particulier, les équipements doivent être dans l'état voulu (vanne ouverte ou fermée, bonne valeur de débit, température de consigne correcte, etc.)

— **Définition des matières premières et produits :** La ToE doit garantir l'identification, et la connaissance de la quantité disponible et de la qualité des matières premières, matières intermédiaires et stocks produits mis en jeu dans l'atelier de production. Dans certains cas, la nature des matières premières employées est confidentielle.

— **Définition du personnel de production :** La ToE doit garantir l'identification, et le niveau de qualification requis si nécessaire du personnel de production.

— **Définition des recettes, gammes et formulations :** Une mauvaise exécution de la production peut conduire à une détérioration des matières mises en jeu, et à la fabrication d'articles ou de produits non conformes, défectueux, voire toxiques ou dangereux. Les informations associées sont généralement confidentielles.

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
Description de l'installation et état des équipements	X		X	X
Définition des matières premières et produits	X	X	X	X
Définition du personnel de production	X	X	X	X
Définition des recettes, gammes et formulations	X	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.

— **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 [4].

— **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.

— **Tracabilité des opérations :** La traçabilité des opérations et transferts de matières effectués, des contrôles qualités réalisés, des différentes mesures effectuées durant l'exécution du procédé et des alertes éventuelles associées. L'absence de cette traçabilité pouvant conduire soit à l'ignorance d'un risque potentiel sur les fabrications, soit à une destruction de ces fabrications en raison du principe de précaution.

— **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

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.

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	
Tracabilité des opérations	X	X	X	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 compremettre 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 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.
— **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'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 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.
— **Développement sécurisé :** La ToE est développée de manière sécurisée afin d'assurer le respect du modèle d'information et de la politique de droits.
— **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

	Flux vers la station d'ingénierie	Flux vers un serveur d'historique	Flux de collaboration	Flux de données avec les équipements terrain	Description de l'installation et état des équipements	Définition des matières premières et produits	Définition du personnel de production	Définition des recettes, gammes et formulations	Logiciel(s)	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Tracabilité des opérations	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évè-
Déni de service					D	D	D	D						D			
Altération des flux	I A	I A	I A	I A		I A		I A							D	D	
Compromission des flux	C					C	C	C									
Corruption de données					I A	I A	I A	I A						I A			
Compromission de données							C	C						C			
Corruption du logiciel									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

	Flux vers la station d'ingénierie	Flux vers un serveur d'historique	Flux de collaboration	Flux de données avec les équipements terrain	Description de l'installation et état des équipements	Définition des matières premières et produits	Définition du personnel de production	Définition des recettes, gammes et formulations	Logiciel(s)	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Tracabilité des opérations	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évè
Contournement de la politique de droits													I				
Corruption des journaux d'évènements locaux																	I A
Corruption des journaux d'évènements déportés																	

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 de données	Compromission de données	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'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				
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					
Développement sécurisé				X	X								

	Déni de service	Altération des flux	Compromission des flux	Corruption de données	Compromission de données	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'évènements locaux	Corruption des journaux d'évènements déportés
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