Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2016/05

Siemens

Simatic S7 1518-4

Version du micrologiciel 1.83

Paris, le 25 avril 2016

Le directeur général adjoint de l'agence nationale
de la sécurité des systèmes d'information

Contre-amiral Dominique RIBAN
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2016/05

Nom du produit

Simatic S7 1518-4

Référence/version du produit

Version du micro-logiciel 1.83

Référence de la cible de sécurité

Cible de sécurité

Référence : CSPN-ST-Simatic-S7-1518-4-1.02 en date du 18 avril 2016.

Catégorie de produit

Automate programmable industriel

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Siemens S.A.S
40, Avenue des Fruitiers
93527 Saint-Denis
France

Centre d'évaluation

Amossys
4 bis allée du bâtiment, 35000 Rennes, France

Fonctions de sécurité évaluées

Gestion des entrées malformées
Authentification sécurisée sur l'interface d'administration
Politique de droits
Signature du firmware
Intégrité et confidentialité de la configuration
Authenticité, intégrité du programme utilisateur
Confidentialité du programme utilisateur
Authenticité et intégrité des commandes du mode de fonctionnement
Communications sécurisées

Fonctions de sécurité non évaluées

Stockage sécurisé des secrets

Restrictions d'usage

Oui (cf. §3.2)

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'automate programmable industriel[1] Simatic S7 1518-4, version 1.83 développé par *SIEMENS*.
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 de capteurs, l'automate envoie des ordres vers ses sorties, les actionneurs.

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

Un automate programmable industriel peut s'inscrire dans un grand nombre d'architectures distinctes. Cependant un cadre général de déploiement ressort (Figure 1).
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 (*Field network* sur la Figure 1).
Les échanges vers la supervision (IHM SCADA) se font au travers d'une interface de communication dédiée sur le réseau de supervision (*Supervision network* sur la Figure 1).
L'administration de l'automate programmable industriel se fait à partir d'une station d'ingénierie ayant accès au réseau de supervision. Les modifications du *firmware* et du programme utilisateur peuvent être envoyées sur l'automate par le réseau de supervision, par un lien série ou à l'aide de supports amovibles (cartes SD ou clés USB par exemple).

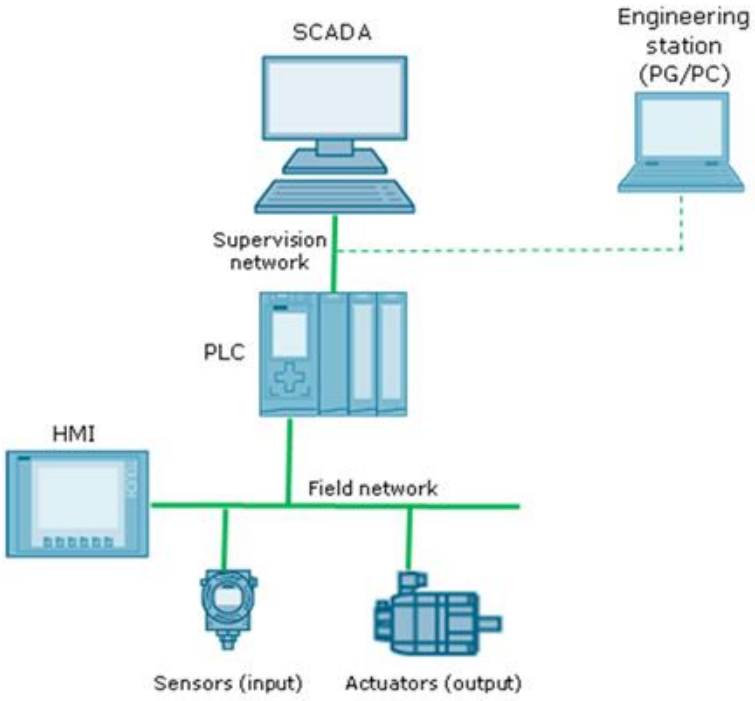

Figure 1 – Cadre général de déploiement.

[1] En Anglais *Programmable Logic Controler (PLC).*

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☐ 6 – identification, authentification et contrôle d'accès
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ **9 – stockage sécurisé**
☐ 10 – environnement d'exécution sécurisé
☐ 11 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☒ **13 – automate programmable industriel**

1.2.2. Identification du produit

Nom du produit	Simatic S7 1518-4
Numéro de la version analysée	1.83

La version certifiée du produit peut être identifiée de deux manières différentes :

- directement par visualisation de l'écran de celle-ci en via le menu [overview > PLC] ;
- à l'aide du logiciel TIA Portal via les menus [Online & diagnostics > Diagnostics > General].

1.2.3. Configuration évaluée

Conformément à la cible de sécurité [CDS], la configuration évaluée se base sur les options suivantes :

- désactivation des services suivants (ces services sont désactivés par défaut) :
  - serveur web ;
  - synchronisation NTP ;
  - communication PUT/GET.
- activation des options suivantes (ces options ne sont pas activées par défaut)
  - *« No Access (complete protection) » ;*
  - *« know how protection ».*

Les tests de l'évaluation ont été réalisés uniquement sur la plateforme matérielle du S7 1518-4.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et à la note d'application [NOTE-3]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

La plateforme de test est constituée des éléments suivants :

- un automate programmable industriel Simatic S7 1518-4 ;
- une station d'ingénierie et de supervision *Windows 7 Professional* équipée du logiciel « TIA Portal » en version V13+SP1 ;
- un module « d'entrées-sorties » permettant les interactions avec le réseau de terrain ;
- une machine connectée au réseau de supervision dans le rôle de l'attaquant, fonctionnant selon les tests sur les systèmes d'exploitation suivants : Debian 7 64 bits, Kali 64 bits ou Windows 8 64 bits.

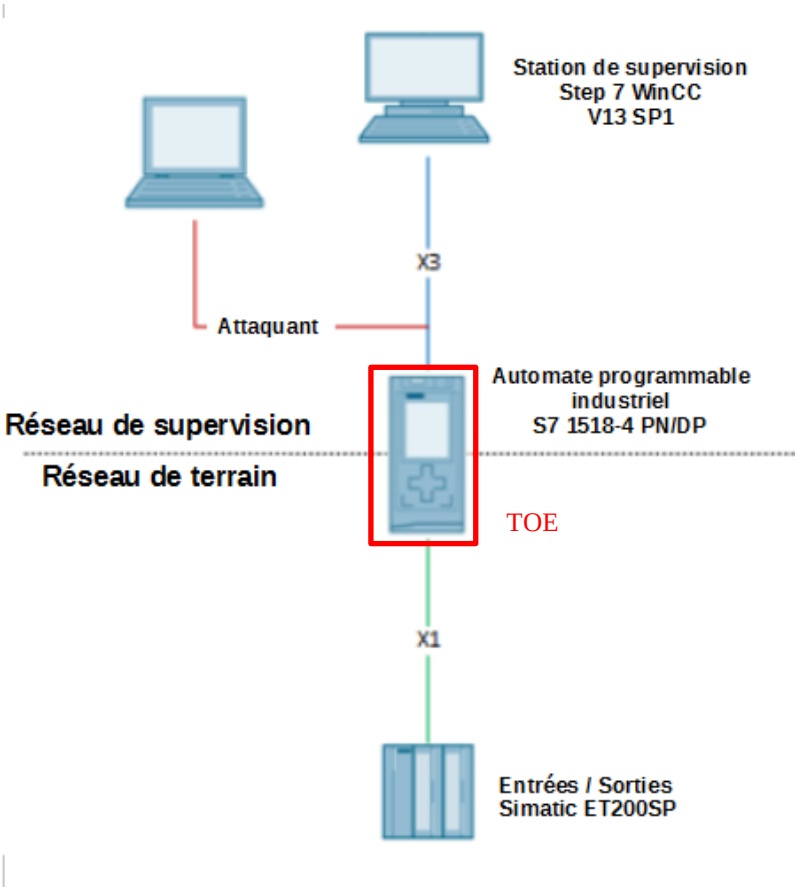

Figure 2 – Plateforme de test.

2.3.1.2. Particularités de paramétrage de l'environnement et options d'installation

L'automate a été évalué dans la configuration précisée au paragraphe 1.2.3.

2.3.1.3. Description de l'installation et des non-conformités éventuelles

Néant

2.3.1.4. Durée de l'installation

L'installation a nécessité une journée.

2.3.1.5. Notes et remarques diverses

Néant

2.3.2. Analyse de la documentation

La documentation est claire et permet d'appréhender l'ensemble des dépendances logiques du produit.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

2.3.4. Analyse de la conformité des fonctions de sécurité

La fonction de sécurité « Authentification sécurisée sur l'interface d'administration » requiert lorsque la politique de droits est modifiée la déconnection de tous les utilisateurs afin de garantir la prise en compte des nouveaux droits.
Le « stockage sécurisé des secrets » compte tenu du type d'évaluation en boite noire n'a pas pu faire l'objet de tests.
La fonction de sécurité « signature du *firmware* » a bien fait l'objet de tests qui ont montré qu'un *firmware* malformé est rejeté par la cible, et n'a pas ainsi été mise en défaut. Cependant compte tenu de l'évaluation en boite noire, il n'est pas possible de démontrer la présence d'un mécanisme de protection de l'intégrité du *firmware*.

Les autres fonctions de sécurité ont été testées et sont conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité testées ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation de la cible d'évaluation.

2.3.6. Analyse des vulnérabilités (conception, construction…)

2.3.6.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues et exploitables sur ce produit dans sa version évaluée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit ou son implémentation pouvant remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Comme exposé au paragraphe 2.3.4, il convient de déconnecter tous les utilisateurs après une modification des droits et permissions.
Le *timeout* d'un programme utilisateur doit être configuré avec une marge suffisante.

2.3.8.3. Avis d'expert sur la facilité d'emploi

L'utilisateur devra être particulièrement attentif aux correspondances entre les rôles et les droits associés sur TIA Portal et sur l'automate.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit *Simatic S7 1518-4, version 1.83* soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur de ce certificat devra s'attacher à employer la configuration énoncée au paragraphe 1.2.3. Cependant l'évaluation a mis en avant des restrictions d'usage à respecter pour une utilisation sécurisée du produit décrites ci-après :

- après une modification des droits et permissions, tous les utilisateurs doivent être déconnectés ;
- le temporisateur (*timeout*) d'un programme utilisateur doit être configuré avec une marge conséquente.

Enfin les règles de défense en profondeurs doivent être appliquées et notamment dans le cas d'une administration par le réseau, il est recommandé d'utiliser un réseau séparé physiquement ou, au minimum, logiquement. Il est également recommandé que la station d'ingénierie ne soit pas branchée en permanence mais uniquement en cas de besoin.

Annexe 1. Références documentaires du produit évalué

[CDS]	*CSPN Security Target Simatic S7-1518-4* Référence : CSPN-ST-Simatic-S7-1518-4-1.02 ; Version : 1.02 ; Date : *18 avril 2016*
[RTE]	*CSPN Evaluation Technical Report Product Simatic S7 1518-4* Référence : CSPN-ETR-S7-1518-4-2.01; Version : 2.02 ; Date : *18 avril 2016*
[GUIDES]	*Security recommendations for the use of S7-1500* Référence : *S7-1500_SEC_RECO_EXTR_V1.0*; Version : 1.0.
[CONF]	*S7-1500 security configuration for French certification (CSPN)* Référence : *S7-1500_SEC_CONF_CSPN_V1.0*; Version : 1.0.

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur http://www.ssi.gouv.fr/
[NOTE-3]	Méthodologie pour l'évaluation logicielle d'automates programmables industriels en vue d'une certification de sécurité de premier niveau ANSSI-CSPN-NOTE-03/1 du 30 juillet 2015. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 2.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03. Documents disponibles sur http://www.ssi.gouv.fr/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.