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-2017/26

Simatic S7 1500 Range
Version 2.1.0

Paris, le 9 octobre 2017

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

[original signé]
Guillaume POUPARD

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-2017/26**
Nom du produit **Simatic S7 1500 Range**
Référence/version du produit **Version 2.1.0**
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**
Développeur **SIEMENS AG** **Gleiwitzer Str. 555** **90475 Nürnberg** **Deutschland**
Centre d'évaluation **AMOSSYS** **4 bis allée du bâtiment** **35000 Rennes** **France**
Fonctions de sécurité évaluées **Gestion des entrées malformées** **Stockage sécurisé des données utilisateur** **Authentification sécurisée à l'interface d'administration** **Politique d'accès** **Signature du firmware** **Intégrité et authentification du programme utilisateur** **Authenticité et intégrité des commandes du mode de fonctionnement** **Communications sécurisées**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

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 CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Les produits évalués sont les automates programmables industriels[1] de la gamme « Simatic S7 1500 Range, version 2.1.0 » développés par *SIEMENS AG.*

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).

La figure ci-dessous explicite l'architecture du produit.

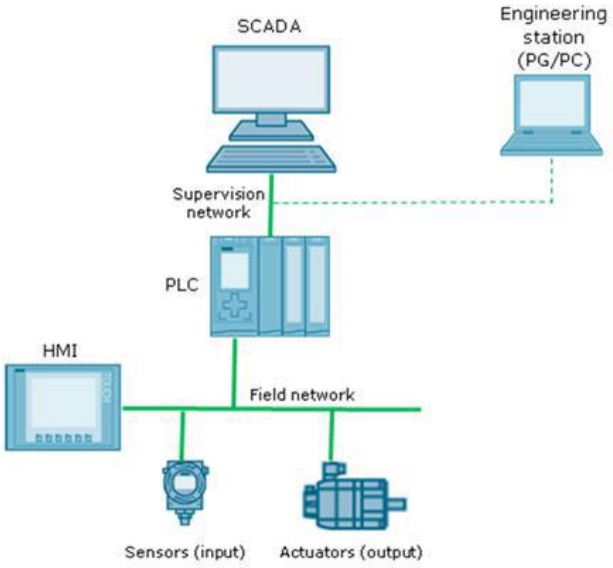

Figure 1 - Architecture Produit.

[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 – pare-feu
☐ 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 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☒ **13 – automate programmable industriel**
☐ 99 – autre

1.2.2. Identification de la gamme de produits

Plusieurs automates programmables industriels sont identifiés pour cette évaluation. Pour les besoins de l'évaluation, et conformément à la [NOTE-21], seules certaines références ont été évaluées. Le CESTI a en effet conclu que les modèles mentionnés dans le Tableau 1 étaient représentatifs de la gamme de produits faisant l'objet de cette certification (Tableau 2).

Type de produit évalué par le CESTI	Référence du produit évalué par le CESTI	Version du *firmware*
CPU 1518-4 PN/DP	6ES7518-4AP00-0AB0	2.1.0
CPU 1517F-3 PN/DP	6ES7517-3FP00-0AB0	2.1.0
CPU 1516F-3 PN/DP	6ES7516-3FN01-0AB0	2.1.0
CPU 1515-2 PN	6ES7515-2AM01-0AB0	2.1.0
CPU 1513F-1 PN	6ES7513-1FL01-0AB0	2.1.0
CPU 1512SP-1 PN	6ES7512-1DK01-0AB0	2.1.0
CPU 1510SP F-1 PN	6ES7510-1SJ01-0AB0	2.1.0

Tableau 1 - Produits de la gamme évalués par le CESTI

Type de produit de la gamme	Référence du produit de la gamme	Version du *firmware*
CPU 1518-4 PN/DP	**6ES7518-4AP00-0AB0**	**2.1.0**
CPU 1518F-4 PN/DP	6ES7518-4FP00-0AB0	2.1.0
CPU 1517-3 PN/DP	6ES7517-3AP00-0AB0	2.1.0
CPU 1517F-3 PN/DP	**6ES7517-3FP00-0AB0**	**2.1.0**
CPU 1516F-3 PN/DP	**6ES7516-3FN01-0AB0**	**2.1.0**
CPU 1516-3 PN/DP	6ES7516-3AN01-0AB0	2.1.0

ET 200pro:CPU 1516PRO-2 PN	6ES7516-2PN00-0AB0	2.1.0
ET 200pro:CPU 1516pro F-2 PN	6ES7516-2GN00-0AB0	2.1.0
CPU 1515F-2 PN	6ES7515-2FM01-0AB0	2.1.0
CPU 1515-2 PN	**6ES7515-2AM01-0AB0**	**2.1.0**
CPU 1513F-1 PN	**6ES7513-1FL01-0AB0**	**2.1.0**
CPU 1513-1 PN	6ES7513-1AL01-0AB0	2.1.0
CPU 1512SP-1 PN	6ES7512-1SK01-0AB0	2.1.0
CPU 1512SP-1 PN	**6ES7512-1DK01-0AB0**	**2.1.0**
CPU 1512C-1 PN	6ES7512-1CK00-0AB0	2.1.0
CPU 1511F-1 PN	6ES7511-1FK01-0AB0	2.1.0
CPU 1511C-1 PN	6ES7511-1CK00-0AB0	2.1.0
CPU 1511-1 PN	6ES7511-1AK01-0AB0	2.1.0
CPU 1510SP F-1 PN	**6ES7510-1SJ01-0AB0**	**2.1.0**
CPU 1510SP-1 PN	6ES7510-1DJ01-0AB0	2.1.0

Tableau 2 - Produits faisant partie de la gamme (en gras les références évaluées)

Le type, la référence ainsi que la version du *firmware* peuvent être identifiés de la manière suivante :

- type de produit :
  - si le produit est équipé d'un écran, le type de produit est imprimé sur le boitier, en haut entre les LED, ou directement par visualisation sur l'écran via le menu [Overview > PLC] ;
  - s'il n'y a aucun écran, le type de produit est imprimé sur le boitier en haut à droite ;
  - dans tous les cas à l'aide du logiciel TIA Portal via les menus [Online & diagnostics > Diagnostics > General],

- référence du produit :
  - si le produit est équipé d'un écran la référence est imprimée sur le boitier, sous l'écran, ou directement par visualisation sur l'écran via le menu [Overview > PLC] ;
  - s'il n'y a aucun écran la référence est imprimée sur le boitier en bas à gauche ;
  - dans tous les cas à l'aide du logiciel TIA Portal via les menus [Online & diagnostics > Diagnostics > General],

- version du *firmware* :
  - directement par visualisation sur l'écran via le menu [Overview > PLC] ;
  - dans tous les cas à l'aide du logiciel TIA Portal via les menus [Online & diagnostics > Diagnostics > General].

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- gestion des entrées malformées ;
- stockage sécurisé des données utilisateur ;
- authentification sécurisée à l'interface d'administration ;
- politique d'accès ;
- signature du *firmware* ;
- intégrité et authentification du programme utilisateur ;
- authenticité et intégrité des commandes du mode de fonctionnement ;
- communications sécurisées.

1.2.4. Configuration évaluée

Tous les automates ont été configurés avec les paramètres par défaut, à savoir :

- désactivation des services suivants :
  - serveur web ;
  - synchronisation NTP ;
  - communication PUT/GET ;
- activation de la protection de l'accès à l'automate par mot de passe.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 adaptée conformément à la procédure [NOTE-21], seuls les tests ayant une adhérence aux caractéristiques distinguant les produits de la gamme ont été joués par le CESTI sur les produits déclinés. Il a également été tenu compte des travaux déjà effectués sur une précédente version du produit, certifiée sous la référence ANSSI-CSPN-2016/05 ([CER]).

2.3. Travaux d'évaluation

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

2.3.1. Installation du produit

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

Les produits étant des *appliances*, il n'y a pas d'installation matérielle à faire. Cependant, l'évaluateur a dû configurer les produits ainsi que développer et installer des applications sur les produits.

2.3.1.3. Durée de l'installation

L'installation de l'ensemble des produits a nécessité 4 jours.

2.3.1.4. 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'évaluateur n'a pas eu directement accès au code source mais a pu obtenir du développeur les éléments nécessaires à son analyse des fonctions de sécurité.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées 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 ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit et en particulier sur la cryptographie.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur a identifié la mise à jour du *firmware* comme pouvant avoir un impact sur la sécurité du produit. Il est en effet possible de revenir sur une version antérieure du *firmware*, notamment une version sur laquelle auraient été découvertes des vulnérabilités (*Downgrade attack*). Cette fonctionnalité doit donc être utilisée par l'administrateur en connaissance des risques et avec toutes les précautions nécessaires.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'évaluateur insiste sur l'importance de respecter les [GUIDES] fournis ainsi que les conditions de déploiement prévues dans la cible de sécurité [CDS] afin de déployer le produit de façon sécurisée.

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur d'aléas du produit a fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

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 la gamme de produits « Simatic S7 1500 Range, version 2.1.0 », contenant les produits listés dans Tableau 2, 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 du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*CSPN Security Target PLC Simatic S7 1500 range* Référence : CSPN-ST-Simatic-S7-1500-Range-1.01 ; Version : *1.01* ; Date : 3 octobre 2017
[RTE]	*CSPN Evaluation Technical Report SIEMENS SIMATIC S7-1500 Controller Family* Référence : ETR-Simatic S7-1500 Controller Family-1.04 ; Version : 1.04 ; Date : 4 octobre 2017
[ANA-CRY]	*Cryptography audit SIEMENS SIMATIC S7-1500 Controller Family* Référence : CRY-Simatic-S7-1500-Controller-Family-1.00 ; Version : 1.00 ; Date : 3 août 2017
[CER]	*Rapport de certification ANSSI-CSPN-2016/05* Siemens Simatic S7 1518-4 Version du micrologiciel 1.83 Référence : ANSSI-CSPN-2016/05 ; Version : 1.0 ; Date : 25 avril 2016
[GUIDES]	*Security recommendations for the use of S7-1500* *S7-1500 security configuration for French certification (CSPN)*

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 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 www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[NOTE-21]	Note d'application - Méthodologie pour l'évaluation d'une gamme de produits, référence ANSSI-CC-NOTE-21/1.0 du 1er février 2017.