

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Bureau Qualification et Agrément

Paris, le 09 NOV. 2017
N° 5479 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU ELEMENTAIRE

SIMATIC S7 1500 version 2.1.0

SIEMENS S.A.S

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions de la qualification.

Fiche 3 : Base documentaire de la qualification.

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

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale [LPM] ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1^{er} ;

Vu le décret du 27 mars 2017 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Décide :

Art. 1^{er} – La famille de produits SIMATIC S7 1500 version 2.1.0 fournie par *SIEMENS* respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 ainsi que le processus de qualification d'un produit et est qualifié au niveau élémentaire sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La présente décision est valable pour une durée de 3 ans.

Art. 3 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le chapitre VII du processus de qualification d'un produit [PROCESS_QUALIF_PROD].

Guillaume POUPARD
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information



Fiche 1

Description du produit.

Désignation et versions

Le produit qualifié est la solution « SIMATIC S7 1500, version 2.1.0 » développée par *SIEMENS*.



Figure 1. Illustration du produit SIMATIC S7 1500, version 2.1.0

Présentation générale

La famille de produits SIMATIC S7 1500 est une famille d'automates industriels programmables. Chacun d'eux permet de réaliser, de façon continue et sans intervention humaine, la commande de processus industriels (machine ou processus continu). En fonction de données d'entrée 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.

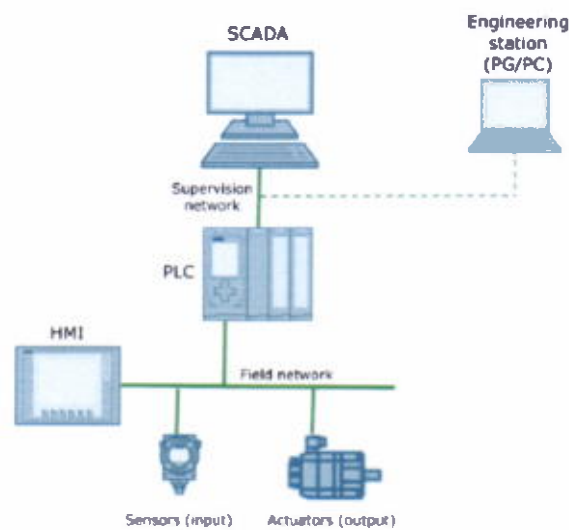
Les fonctions de sécurité offertes par l'automate et couvertes par la présente décision de qualification sont les suivantes :

- 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.

Un automate programmable industriel peut s'inscrire dans un grand nombre d'architectures distinctes. Cependant un cadre général de déploiement 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 (*Field network*) ;
- les échanges vers la supervision (IHM, SCADA) se font au travers d'une interface de communication dédiée sur le réseau de supervision (*Supervision network*) ;
- 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 une architecture de déploiement type du produit :



Fiche 2

Conditions de la qualification.

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit ainsi s'assurer que :

- C1.** Les restrictions d'usage figurant au chapitre 2.3.8.2 du rapport de certification [CERTIF] soient bien respectées ;
- C2.** Le guide de sécurité [GUIDE] soit bien mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie ;
- C3.** L'utilisateur du produit s'assure du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS].

Fiche 3

Base documentaire de la qualification

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, version 1.0 du 06 janvier 2017. Disponible sur http://www.ssi.gouv.fr .
[LPM]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur http://www.legifrance.gouv.fr .

Documents rédigés par le centre d'évaluation

[RTE]	CSPN Evaluation Technical Report SIEMENS SIMATIC S7-1500 Controller Family Référence : ETR-Simatic S7-1500 Controller Family-1.04 ; Version : 1.04 ; En date du: 4 octobre 2017
-------	--

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence : ANSSI-CSPN-2017/26 En date du : 9 octobre 2017
----------	---

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE]	Security recommendations for the use of S7-1500 S7-1500 security configuration for French certification (CSPN)
[CDS]	CSPN Security Target PLC Simatic S7 1500 range Référence : CSPN-ST-Simatic-S7-1500-Range-1.01 ; Version : 1.01 ; En date du : 3 octobre 2017