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-2017/25

Modicon M580 PAC
Version V2.20/V2.11

Paris, le 9 octobre 2017

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

Guillaume POUPARD
[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-2017/25

Nom du produit

Modicon M580 PAC

Référence/version du produit

Module CPU BME P58 2040 avec firmware V2.20

Module Ethernet BME NOC 0301.4 avec firmware V2.11

Catégorie de produit

Automate programmable industriel

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Schneider Electric France
35 rue Joseph Monier
92506 Rueil-Malmaison Cedex
France

Développeur

Schneider Electric France
1ère avenue
06510 Carros
France

Centre d'évaluation

Oppida
4-6 avenue du vieil étang, Bâtiment B
78180 Montigny le Bretonneux
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 **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 CSPN 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 la solution « Modicon M580 PAC » développée par *SCHNEIDER ELECTRIC FRANCE*. Elle est composée de l'automate programmable industriel[1] BME P58 2040, aussi appelé module *central processing unit* (CPU), et du module de communication Ethernet BME NOC 0301.4.

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 (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, les modifications du *firmware* et du programme utilisateur se font au travers de son port USB vers la station d'ingénierie (*Engineering workstation* sur la Figure 1).
La figure ci-dessous explicite l'architecture du produit.

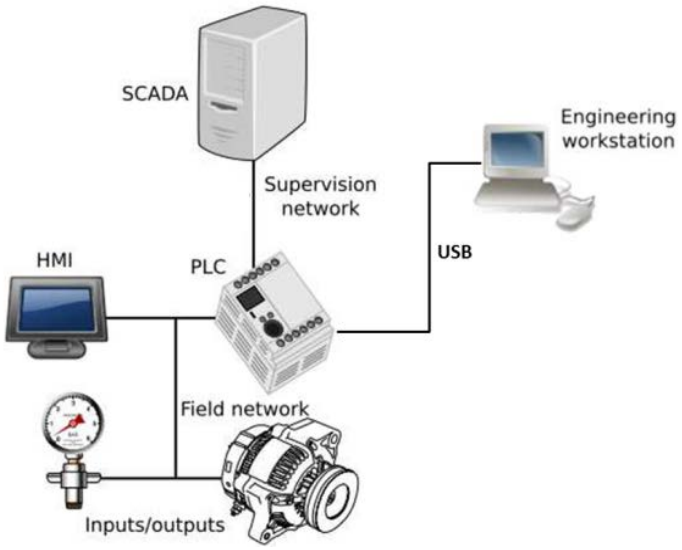

Figure 1 - Architecture Produit.

[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 du produit

Le Modicon M580 PAC est la combinaison des deux modules suivants :

Référence du module CPU	BME P58 2040
Numéro de la version du *firmware* du module CPU évaluée	V2.20
Référence du module Ethernet	BME NOC 0301.4
Numéro de la version du *firmware* du module Ethernet évaluée	V2.11

Les versions des *firmware* exécutés par les produits certifiés peuvent être identifiées au travers de la section paramétrage des modules du logiciel Unity Pro.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

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

1.2.4. Configuration évaluée

La configuration évaluée correspond aux modules CPU et Ethernet listés en section 1.2.2.

Le logiciel Unity Pro en version 12, développé par *SCHNEIDER ELECTRIC FRANCE*, est utilisé sur la station d'ingénierie afin de communiquer avec le produit.

Le patch UnityPro_V120_HF_BMENOC0301-311_CSPN doit être installé afin de pouvoir configurer et communiquer avec le module Ethernet BME NOC 0301.4. L'empreinte SHA256 de ce patch est :

- ccf635f8f43870cba48da5aae524e0fbc9b6fe6d5bfc4fc36f8c9135792e199a.

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 est 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, 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

L'installation du produit se fait au travers du logiciel Unity Pro, installé sur la station d'ingénierie. La connexion entre le produit et cette station doit obligatoirement être effectuée en point à point en utilisant le port USB du module CPU.

L'utilisateur devra s'assurer qu'il configure le produit en respectant le guide « *Cyber Security Reference Manual* » (voir [GUIDES]), à savoir, en utilisant les paramètres suivants :

- activation du protocole IPSec ;
- utilisation d'une clé partagée ;
- activation du paramètre « Enable DH 2048 » ;
- activation du paramètre « Enable Confidentiality » ;
- activation du contrôle d'accès par adresse IP (ACL) ;
- activation du mode « Run/Stop par entrée uniquement » ;
- protection de la mémoire ;
- désactivation des services FTP, TFTP, DHCP/BOOTP, SNMP, EIP et NTP ;
- activation des logs :
- pas d'information d'upload stockée sur le CPU ;
- protection du projet Unity Pro :
    - authentification par login / mot de passe ;
    - protection de la session,
- positionnement des sections d'application à *no read/write access*.

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

La configuration initiale de sécurité selon les recommandations de la cible et du guide nécessite un temps important et une bonne maitrise de l'outil Unity Pro.

2.3.1.3. Durée de l'installation

L'installation et la configuration nécessitent plusieurs heures.

2.3.1.4. Notes et remarques diverses

L'évaluateur note qu'un assistant de configuration pourrait être utile afin de configurer correctement le produit dans la version sécurisée.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace 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

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

Des vulnérabilités ont été identifiées, mais se sont révélées inexploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Des recommandations ont été formulées par l'évaluateur afin d'améliorer la sécurité du produit sur le long terme. L'évaluateur insiste également sur l'importance de respecter les [GUIDES] fournis afin de déployer le produit de façon sécurisée.

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

Le produit est globalement bien documenté, mais sa mise en œuvre peut présenter des difficultés pour un utilisateur non formé.

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 a identifié une non-conformité au RGS, mais considérée comme non bloquante. Aucune vulnérabilité exploitable n'a été identifiée.

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 le produit « Modicon M580 PAC, comprenant le Module CPU BME P58 2040 avec firmware V2.20 et le module Ethernet BME NOC 0301.4 avec firmware V2.11 » 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 le paramétrage défini dans la section 2.3.1.1.

Cependant l'évaluation a mis en avant les restrictions d'usage additionnelles suivantes à respecter pour une utilisation sécurisée du produit :

- pendant la phase d'installation et de configuration du produit, la station d'ingénierie doit obligatoirement être connectée au port USB local du module ;
- dans le cas nominal d'utilisation, lorsque la station de supervision (SCADA) est connectée par le réseau de supervision, Unity Pro ne doit jamais être connecté au produit ;
- toute modification de la configuration ou du *firmware* doit obligatoirement être faite sur le port local USB du module CPU.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Modicon M580 PAC CSPN Security Target* Version : 1.5 ; Date : *1 août 2017*
[RTE]	*Rapport Technique d'Evaluation CSPN OLYMPUS2 - Modicon M580 PAC* Référence : OPPIDA/CESTI/OLYMPUS2/RTE/1.2 ; Version : 1.2; Date : *12 septembre 2017*
[GUIDES]	*Cyber Security Reference Manual* Date : *juillet 2017*

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.