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-2020/20

Modicon M580 PAC
Version V3.10/V2.17

Paris, le 24 juin 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]


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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CSPN-2020/20

Nom du produit

Modicon M580 PAC

Référence/version du produit

Module CPU BME P58XXXX avec firmware V3.10
Module Ethernet BME NOC 0301 avec firmware V2.17

Catégorie de produit

Automate programmable industriel

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire / Développeur

Schneider Electric France
35 rue Joseph Monier
92506 Rueil-Malmaison Cedex
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 secrets
Authentification sécurisée à l'interface d'administration
Politique d'accès
Signature du firmware
Intégrité de la configuration et des commandes du mode de fonctionnement
Intégrité et authentification du programme utilisateur
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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 » développé par Schneider Electric France. Elle est composée d'une gamme d'automate idustriel[1] BME P58XXXX[2], aussi appelé module *central processing unit* (CPU) et exécutant le *firmware* V3.10, et du module de communication *Ethernet* BME NOC 0301 avec le *firmware* V.2.17.

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.

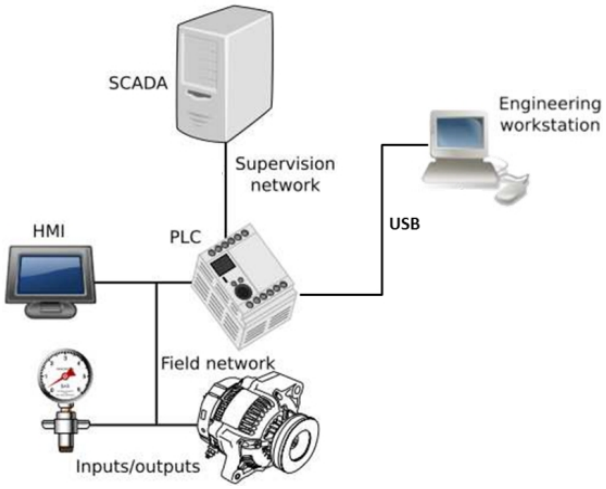

Figure 1 - Architecture Produit.

1 En Anglais *Programmable Logic Controler* (PLC).
2 Voir liste complète des CPU dans le Tableau 2, page 9.

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 produit

Plusieurs automates programmables industriels sont identifiés sous le nom Modicon M580 PAC 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).

Référence du produit évalué par le CESTI	Type de produit évalué par le CESTI	Version du *firmware*
BME P58 2040	CPU	V3.10
BME H58 2040	CPU	V3.10
BME P58 4040S	CPU	V3.10
BME P58 CPROS3	CPU	V3.10
BME NOC 0301	Module de communication *Ethernet*	V2.17

Tableau 1 - Produits de la gamme évalués par le CESTI

Référence du produit de la gamme	Type de produit de la gamme	Version du *firmware*
BME P58 1020	CPU	V3.10
BME P58 1020H	CPU	V3.10
BME P58 2020	CPU	V3.10
BME P58 2020H	CPU	V3.10
BME P58 2040	**CPU**	**V3.10**
BME P58 2040H	CPU	V3.10
BME P58 3020	CPU	V3.10
BME P58 3040	CPU	V3.10
BME P58 4020	CPU	V3.10
BME P58 4040	CPU	V3.10
BME P58 4040S	**CPU**	**V3.10**
BME P58 2040S	CPU	V3.10
BME P58 5040	CPU	V3.10
BME P58 5040C	CPU	V3.10
BME P58 6040	CPU	V3.10
BME P58 6040C	CPU	V3.10
BME H5 82040	**CPU**	**V3.10**
BME H58 2040C	CPU	V3.10
BME H58 4040	CPU	V3.10
BME H58 4040C	CPU	V3.10
BME H58 6040	CPU	V3.10
BME H58 6040C	CPU	V3.10
BME P58 CPROS3	**CPU**	**V3.10**
BME NOC 0301	**Module de communication *Ethernet***	**V2.17**

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

Les versions des *firmwares* exécutés par les produits certifiés peuvent être identifiées au travers de la section paramétrage des modules du logiciel *Control Expert*.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- la gestion des entrées malformées ;
- le stockage sécurisé des secrets ;
- l'authentification sécurisée à l'interface d'administration ;
- la politique d'accès ;
- la signature du *firmware* ;
- l'intégrité de la configuration et des commandes du mode de fonctionnement ;
- l'intégrité et l'authentification du programme utilisateur ;
- les communications sécurisées.

1.2.4. Configuration évaluée

Trois plateformes ont été utilisées pour l'évaluation, correspondant chacune à une configuration différente :
- la configuration de référence ;
- la configuration *HotStandby** (HSBY) ;
- la configuration *Safety**.

*** les caractéristiques propres aux configurations HSBY et *Safety*, à savoir la disponibilité et la redondance des calculs, ne font pas partie du périmètre de l'évaluation.**

La configuration de référence est composée des éléments suivants :
- un *backplane* BMEXBP0800H ;
- un bloc d'alimentation BMX CPS 2000 ;
- un bloc de sorties BMX DDI 1602 ;
- un CPU BME P58 2040 ;
- deux modules de communication *Ethernet* BME NOC 0301.

La configuration HSBY est composée des éléments suivants :
- trois *backplanes* BME XBP 0600 ;
- trois blocs d'alimentation BMX CPS 2000 ;
- un bloc de sorties BMX DDI 1602 ;
- deux CPU BME H58 2040 ;
- deux modules de communication *Ethernet* BME NOC 0301 ;
- un module Remote IO.

La configuration *Safety* est composée des éléments suivants :
- un *backplane* BMEXBP0600 ;
- un bloc d'alimentation BMX CPS 4002S ;
- un bloc de sorties BMX DDI 1602 ;
- un CPU *safety* BME P58 4040S ;
- un *safety coprocessor* BME P58 CPROS3 ;
- deux modules de communication *Ethernet* BME NOC 0301.

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

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

L'installation du produit se fait au travers du logiciel *Control Expert*, 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 :

- le contrôle d'accès par adresse IP doit être activé (ALC) ;
- la modification du mode de fonctionnement (RUN/STOP) ne doit s'effectuer qu'au travers du module d'entrée ;
- la protection de la mémoire doit être activé ;
- les options de sécurité renforcée doivent être mises en œuvre : désactivation des services FTP, TFTP, DHCP/BOOTP, SNMP, EIP et NTP ;
- le protocole IPSEC doit être activé ;
- les logs doivent être activés ;
- aucune information d'*upload* ne doit être stockée sur le CPU ;
- la protection du projet doit être assurée via :
    - l'authentification par login / mot de passe,
    - la protection de la session ;
- le mot de passe par défaut du service FTP doit être changé ;
- les sections d'application doivent être positionnées 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 *Contol Expert*.

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

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

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

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

Sans objet.

2.3.8. Analyse de la facilité d'emploi

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. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier des automates industriels. L'évaluateur insiste également sur

l'importance de respecter les [GUIDES] fournis afin de déployer le produit de façon sécurisée.

2.3.8.3. 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 (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [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 le produit « Modicon M580 PAC, comportant un module CPU BME P58XXXX[1] avec *firmware* V3.10 et deux modules *Ethernet* BME NOC 0301 avec *firmware* V2.17 » 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. Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

Afin de garantir l'utilisation sécurisée du produit, il est impératif que l'utilisateur mette en œuvre les mesures suivantes :

- 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, *Contol Expert* 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 ;
- le contrôle d'accès par adresse IP doit être activé (ALC) ;
- la modification du mode de fonctionnement (RUN/STOP) ne doit s'effectuer qu'au travers du module d'entrée ;
- la protection de la mémoire doit être activée ;
- les options de sécurité renforcée doivent être mises en œuvre : désactivation des services FTP, TFTP, DHCP/BOOTP, SNMP, EIP et NTP ;
- le protocole IPSEC doit être activé ;
- les logs doivent être activés ;
- aucune information d'*upload* ne doit être stockée sur le CPU ;
- la protection du projet doit être assurée via :
    - l'authentification par login / mot de passe,
    - la protection de la session ;
- le mot de passe par défaut du service FTP doit être changé ;
- les sections d'application doivent être positionnées à *no read/write access*.

1 Voir liste complète des CPU dans le Tableau 2, page 9.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Modicon M580 PAC CSPN Security Target* Version : 1.90.
[RTE]	*Rapport Technique d'Évaluation CSPN OLYMPUS4 –Modicon M580* Référence : OPPIDA/CESTI/OLYMPUS4/RTE/1.0 ; Version : 1.0 ; Date : *28 janvier 2020*.
[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, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. 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.