PREMIER MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2025/08

Cyber Fence Link

Version 1.0

Paris, le 12/8/2025 | 10:48 CEST

Vincent Strubel

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-2025/08**
Nom du produit **Cyber Fence Link**
Référence/version du produit **Version 1.0**
Catégorie de produit **Matériel et logiciel embarqué**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SERPE** Parc d'activité Technellys – Bâtiment E 165, rue de la Montagne du Salut 56600 Lanester France
Centre d'évaluation **CEA - LETI** 17 avenue des martyrs 38054 Grenoble Cedex 9, France
Accord de reconnaissance applicable fixed time certification Ce certificat est reconnu dans le cadre du [BSZ_CSPN]
Fonctions de sécurité évaluées Remontée vers la supervision de messages capteurs authentifiés, intègres, déchiffrés et à jour uniquement. Composants stockée vierges, programmation à la mise en service par personnel habilité puis passage du microprocesseur en exécution seule Chiffrement du bus capteurs en AES128 mode GCM, utilisation d'un Tag et d'un compteur anti-rejeux
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

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 cyber.gouv.fr.

TABLE DES MATIERES

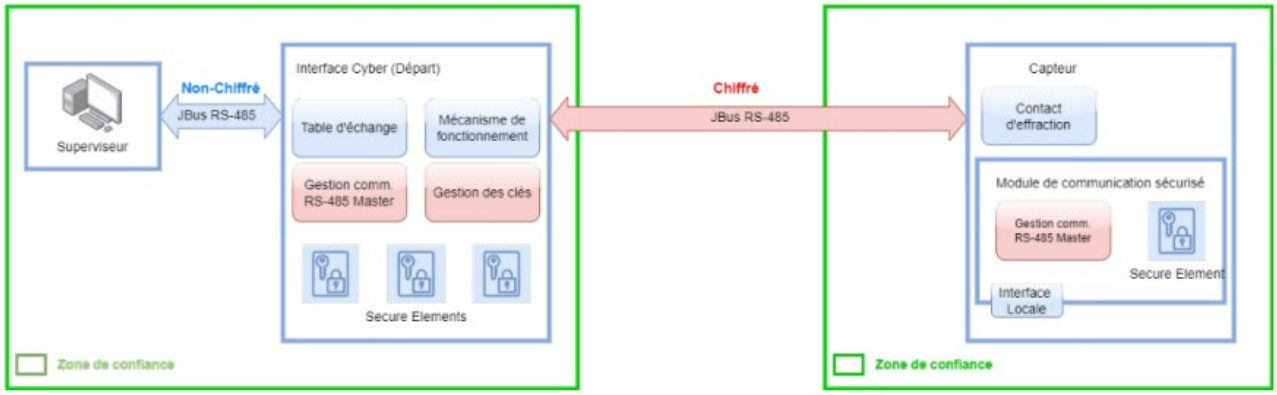
1 Le produit

1.1 Présentation du produit

Le produit évalué est « Cyber Fence Link, Version 1.0 » développé par SERPE.

Ce produit est un protocole permettant le chiffrement d'une liaison JBus/Modbus. Il est implémenté par : Un module de communication sécurisé intégré à un capteur du catalogue SERPE (MCS – S996) et une interface de communication sécurisée vers le superviseur, pouvant être redondée (ICS – S995).

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



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*

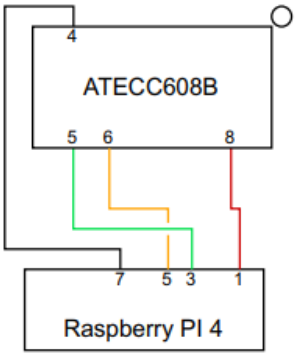
Produit	
Nom du produit	Cyber Fence Link
Numéro de la version évaluée	Version 1.0

La version certifiée du produit peut être identifiée de la manière suivante :

Sur l'ICS comme pour le MCS, les versions des PCB (circuit imprimé) et du STM32 (microcontrôleur) sont identifiables en regardant les cartes électroniques.

Pour identifier les éléments sécurisés, le centre d'évaluation a dû mettre en place sa propre procédure :

Le composant ATECC608B doit être connecté à un Raspberry Pi 4 selon le schéma ci-dessous



- L'utilitaire atecc-util (branche feature/atecc608b-id-support) doit être installé selon les instructions du projet ;

- Un correctif sur l'outil du CESTI-Leti a été appliqué pour réveiller le composant correctement ;

Le numéro de révision du composant sécurisé identifié par U23 sur le PCB vaut 00006003 : le composant est conforme à la cible de sécurité.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- Remontée par l'ICS des messages capteur correctement authentifiées, déchiffrées et à jour uniquement.
- Composants stockée vierges, programmation à la mise en service par personnel habilité puis passage du microprocesseur en exécution seule.
- Utilisation de l'AES128 en mode GCM, utilisation d'un Tag et d'un compteur anti-rejeux

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à

- Une carte électronique SERPE S995D : interface de communication sécurisée (ICS) ;

- Un module de protection périmétrique (module 1) composé de : Un coffret de type "détecteur maillage" avec un détecteur d'ouverture ; Une carte électronique SERPE S993B : capteur type

détecteur 4 boucles ; Une carte électronique SERPE S996D : module de communication sécurisée (MCS).

- Un module de protection périmétrique (module 2) composé de : Une carte électronique SERPE S993B : capteur type détecteur 4 boucles ; Une carte électronique SERPE S983C : module de communication RS485.

- Un boitier de commandes relié aux modules 1 et 2 pour modifier l'état des capteurs ;

- Un système de supervision avec les droits d'administration sur Windows 11 (version 10.0.22621 build 22624). Le rapport des informations systèmes du superviseur est donné en annexe, chapitre 10. Les logiciels (propriétaires développeur) suivants ont été installés et configurés par le développeur : EryVision : logiciel de supervision ; EryCapt : logiciel de configuration des capteurs ; EryModBusMaster : logiciel de simulation ModBus.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]

2.2 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].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

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

2.2.1.2 Description de l'installation et des non-conformités éventuelles

La plateforme d'évaluation a été installée et configurée selon la procédure décrite dans [CJB_COMM_USER_D] dont les étapes sont les suivantes :

- Connexion de la carte S995D (ICS) avec le superviseur

- Connexion de la carte S996D (MCS) avec le capteur

- Réinitialisation de l'ICS

- Configuration des capteurs : (L'adresse du capteur dans le boitier 1 (sécurisé) vaut 10 ; L'adresse du capteur dans le boitier 2 (non-sécurisé) vaut 2)

- Encodage des MCS : (Génération des clés de chiffrement ; Enrôlement de l'ICS et du MCS)

- Alimentation du capteur.

2.2.1.3 Notes et remarques diverses

La plateforme ne reflète pas l'entièreté des hypothèses d'environnement : il y pas d'alimentation électrique secourue. Le périmètre de l'évaluation qui a été défini ne tient pas compte de ces mesures.

2.2.2 *Analyse de la documentation*

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

Les documents fournis permettent de mettre en place la communication entre un ICS et un MCS. Ils ne permettent pas de mettre en place la communication entre la station de supervision (hors cible) et l'ICS. Le développeur a indiqué que ces informations sont spécifiques à la supervision utilisée. Les informations (tables d'échanges) sur les capteurs sont fournis à la demande pour des installations avec des supervisions tierces.

L'évaluateur a eu accès à des documents internes de conception dans le cadre de cette évaluation.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'ICS et du MCS.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 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.

2.2.7.2 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. Cependant, La documentation d'installation a permis au CESTI d'installer le produit dans la configuration couverte par l'évaluation en moins d'une heure.

2.2.7.3 Notes et remarques diverses

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

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 « Cyber Fence Link, Version 1.0 » 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.

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 suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- Les capteurs utilisés qui fonctionnent avec le produit doivent se trouver à l'intérieur de la zone de confiance à protéger et ne doivent pas être accessibles physiquement par un attaquant.

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (Beschleunigte Sicherheitszertifizierung ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Sécurisation communication JBus-RS485 Cible de sécurité, référence DOC23017G, version G, 23 septembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Sécurisation communication JBus-RS485 Cible de sécurité, référence DOC23017I, version I, 8 juillet 2025.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'évaluation CSPN – TOLKIEN, référence LETI.CESTI.TOL.RTE.001 - V1.1, version 1.1, 4 juin 2025.
[GUIDES]	Guide d'utilisation du produit : - ICS/MCS - Manuel utilisateur, référence DOC23035, version D, 28 juin 2019 Guide cryptographique : - Sécurisation communication JBus-RS485 - Spécification cryptographique, référence DOC23018D_Specification_Crypt ographique_CyberJBus.pdf, version D, 21 mars 2024.

ANNEXE B. Références liées 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, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, juillet 2024. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0,1er septembre 2024.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence bsz_cspn_mutual_recognition_agreement,version 2.0, mai 2024.