165, Rue de La Montagne du Salut
56 600 LANESTER (France)
Tél : +33 2 56 37 10 00
www.serpe-surete.com

Sécurisation communication JBus-RS485

Cible de sécurité

DOC23017I

Rédigé par	Signature	Vérifié par	Signature	Approuvé par	Signature	Date	Indice
HOUITTE Pierre-Yves ERYMA	HOUITTE Pierre-Yves Signature numérique de HOUITTE Pierre-Yves Date : 2025.07.08 11:42:15 +02'00'	BOUSSEMART Luc ERYMA	BOUSSEMART Luc Signature numérique de BOUSSEMART Luc Date : 2025.07.08 11:44:09 +02'00'	BARBIER Florian ERYMA	Florian BARBIER	08-juil.-25	I

Suivi des modifications	
Indice	**Objet de la modification**
I	Suppression des références aux composants logiciels tiers et de l'historique de révisions pour publication, changement de catégorie.

Sécurisation communication JBus-RS485

Cible de sécurité

DOC23017I

Sommaire

1 Objet du document

Ce document décrit la cible de sécurité « kit de communication série JBus-RS485 au protocole SERPE CFL V1.0 » nécessaire à une CSPN des produits des technologies de l'information (**ANSSI-CSPN-CER-P-01_v5.0**) pour ce produit SERPE.

1.1 Documents de référence :

- **[1]** ANSSI-CSPN-CER-P-01 (Certification de sécurité de premier niveau des produits des technologies de l'information).
- **[2]** ANSSI-CSPN-NOTE-09 (Contenu et structure de la cible de sécurité CSPN)
- **[11]** Guide des mécanismes cryptographiques référence ANSSI-PG-083 Version 2.04
- **[13]** Spécifications du protocole JBus référence DOC97069 dernier indice.
- **[18]** Manuel d'installation Mygale 4S+ référence DOC18042C03.
- **[19]** Manuel d'installation Jaguar 400 référence DOC13098E
- **[20]** Manuel d'installation Lynx 400 référence DOC19065B.
- **[21]** Manuel d'installation S993 référence DOC19014B.
- **[22]** Manuel utilisateur Mygale 4S+ référence DOC18043C01.
- **[23]** Manuel utilisateur Jaguar 400 référence DOC12081O.
- **[24]** Manuel utilisateur Lynx 400 référence DOC19066A.
- **[25]** Manuel utilisateur S993 référence DOC17019D.

1.2 Abréviations - définitions :

- ADU : A Définir Ultérieurement (lors de ou des revues de spécifications).
- AES : Advanced Encryption Standard qui est un algorithme de chiffrement symétrique. Recommandé par l'ANSSI en version 128 bits ou plus.
- CSPN : Certification de Sécurité de Premier Niveau
- GCM : Galois/Counter Mode qui est un algorithme de chiffrement authentifié conçu pour fournir à la fois l'intégrité et l'authenticité des données, ainsi que la confidentialité. Il est utilisé couplé avec AES. Recommandé par l'ANSSI à partir de la TLS2.1. Voir plus en détail en Annexe **Annexe B**
- Habilité : Reconnu par l'employeur pour effectuer les opérations en question (programmation, installation et mise en service des équipements MCS et ICS).
- ICS, MCS : Interface, Module de communication sécurisée
- NIST: National Institute of Standards and Technology (Technology administration US department of Commerce).
- S.O. : Sans Objet.
- S995 : code produit de l'ICS
- S996 : code produit du MCS

1.3 Objectif du document :

L'objectif principal de ce document est de :

- Rappeler les spécifications de sécurité génériques à la communication série JBus-RS485 sécurisée avec les capteurs SERPE (protocole SERPE CFL V1.0).
- Décrire la cible de sécurité relative à ce produit SERPE « communication série JBus-RS485 au protocole SERPE CFL V1.0 ».

La cible de sécurité sert à la fois de spécification des fonctions dédiées à la sécurité, par rapport à laquelle le produit est évalué, et de description des liens entre le produit et l'environnement dans lequel celui-ci est exploité. Sont donc intéressés par la cible de sécurité, non seulement le développeur du produit et les responsables de son évaluation, mais également les personnes chargées de sa gestion, de son achat, de son installation, de sa configuration, de son exploitation et de son emploi.

2 Produit à évaluer

2.1 Identification du produit

Catégorie :	Matériel et logiciel embarqué.
Société éditrice / fabricant :	ERYMA (https://www.eryma.com/).
Marque commerciale :	SERPE (https://www.serpe-surete.com/).
Nom commercial :	Cyber Fence Link.
Type de produit :	Communication série JBus-RS485 au protocole SERPE V1.0 pour capteurs de protection périmétrique.

Versions :

Module ICS	Version matérielle (carte) S995D. Version logicielle YLP5101A00
Modules MCS	Version matérielle (carte) S996D. Version logicielle YLP5102A00

2.2 Identification des concepteurs du produit

Personnes physiques :

- Dominique JUTEL, Eryma, concepteur du protocole CFL et de l'architecture matérielle.
- Luc BOUSSEMART, Eyrma, conception électronique et développement logiciel.
- Pierre-Yves HOUITTE, Eryma, développement logiciel.

2.3 Argumentaire du produit

2.3.1 Description générale du produit

Le produit, appelé « Kit Cyber Fence Link» (composé d'une interface de communication sécurisée et de modules de communication sécurisés) dans la suite de ce document est un protocole permettant le chiffrement d'une liaison JBus/Modbus. Celui-ci est implémenté par à minima :

- Un module de communication sécurisé intégré à un capteur du catalogue SERPE (MCS – S996)
- Une interface de communication sécurisée vers le superviseur, pouvant être redondée (ICS – S995)

Chaque MCS est installé à l'intérieur du coffret du capteur SERPE et est connecté sur sa carte électronique principale. Ce module communique :

- D'un côté, avec le capteur via une liaison série type SPI non chiffrée.
- Et de l'autre côté avec une ICS via une liaison série cyber-sécurisé (protocole SERPE CFL V1.0) de type RS485.

L'ICS « départ » est installée près du superviseur et communique à la fois avec lui via une liaison série RS485 selon le protocole JBus en clair et à la fois avec les capteurs via une liaison série RS485 et le protocole cyber sécurisé SERPE CFL V1.0. Le protocole permet le mixage de capteurs chiffrés et non chiffrés.
Une seconde interface, appelée « retour », assure la sûreté de fonctionnement du bus RS485 pour le cas de coupure physique de ce bus ou de dysfonctionnement de l'interface de départ ou de son alimentation. Elle est capable de prendre le relais pour les communications avec les capteurs situés après la coupure ou pour leur totalité. Elle est également placée en zone de confiance mais est séparée physiquement de l'interface de départ et est alimentée séparément.

L'ensemble « MCS / ICS » offre au superviseur une acquisition rapide et sécurisée des alarmes, des informations et défauts techniques des capteurs et lui permet un téléréglage sécurisé des capteurs sous son contrôle et sa surveillance.
Le superviseur intègre les fonctions principales suivantes :

- Affichage sur un synoptique des alarmes, informations et défauts techniques des capteurs.
- Historisation de ces données.
- Configuration et paramétrage du système et des capteurs : téléréglage et sauvegarde.

La communication JBus-RS485 est primordiale pour le système de protection. Elle nécessite d'être sécurisée. Cette nécessité est solutionnée par l'utilisation du JBus-RS485 cyber sécurisé associant interfaces et modules cyber-sécurisés au protocole SERPE CFL V1.0.

2.3.1.1 Architecture globale de la solution « CFL RS485 »

Ci-dessous un diagramme représentant le périmètre d'évaluation que l'on souhaite adopter.

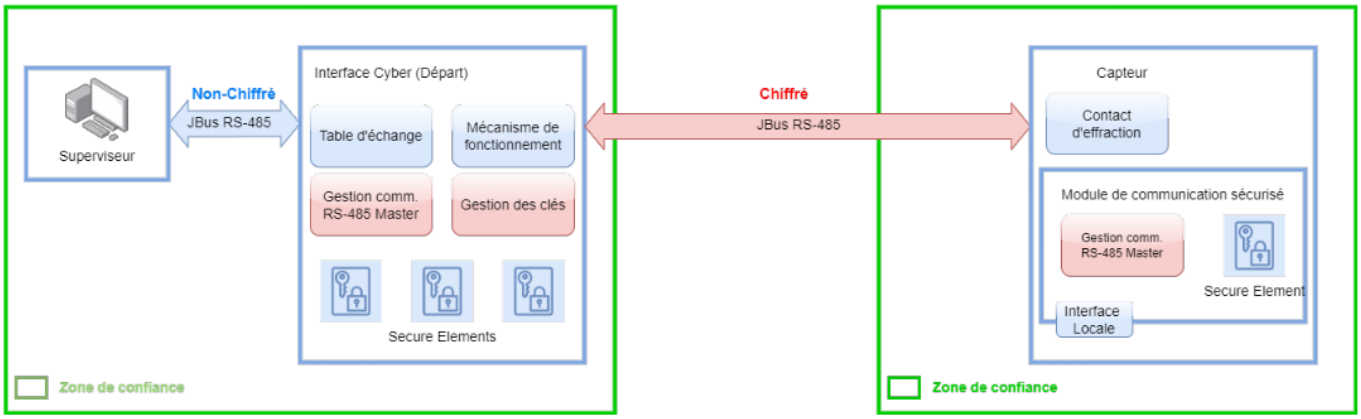


Figure : Architecture globale de la solution « CFL RS485 »

2.3.1.2 Les capteurs périmétriques

Leur rôle est de détecter les intrus sur tout périmètre de site sensible. Certains peuvent également générer un effet dissuasif pour rendre plus difficile l'intrusion.
Le plus souvent ils sont associés à des obstacles sur lesquels leur principe détecteur est installé.
Exemples : clôture, bavolet, portail, portillon, porte, …
Télé-alimentés, ils sont distribués le long du périmètre à surveiller en extérieur ou dans des armoires techniques. Ils peuvent gérer une ou plusieurs zones du périmètre total.
Leur coffret offre une protection physique à leur électronique et au module de communication sécurisé. Il est équipé d'un contact anti-sabotage pour détecter leur ouverture. L'intérieur des coffrets est ainsi une zone de confiance.
Ils communiquent avec un superviseur via le protocole JBus (Dérivé de Modbus) et une table d'échange dont les 8 premiers mots concernent leur état (alarme, défaut technique, information de fonctionnement).

Les capteurs concernés par cette cible de sécurité sont ceux du catalogue SERPE :

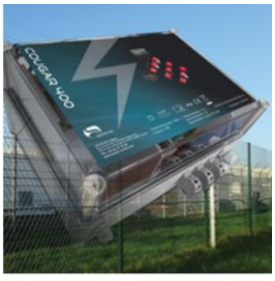
- Mygale 4S+ : Détection par câble piézoélectrique. Gestion jusqu'à 4 zones.
- Lynx 400 : Détection par mesure capacitive d'un fil électrique tendu et isolé. Gestion d'une zone.
- Jaguar 400 : Dissuasion par HT impulsionnelle et détection par mesure capacitive d'un fil électrique tendu et isolé. Gestion d'une zone.
- Couguar 400 : Dissuasion par HT impulsionnelle et détection par mesure de la présence de la HT impulsionnelle. Gestion d'une zone.
- Détecteur 4 boucles S993 : Détection par surveillance de la continuité et de l'isolation électriques d'un câble électrique. Gestion jusqu'à 4 zones.

Capteurs	**Mygale 4S+**	**Lynx 400**	**Jaguar 400**	**Cougar 400**	**Détecteur 4 bl.**
Versions logicielle	YLP8112B04	YLP6303A02	YLP7301B08	YLP7301B08	YLP6202B05
Versions matérielle	S959E	S982B	S980A00	S980A00	S993B
Processeur	ADSP-BF538BBCZ-5A	STM32F105VCT6	ATmega128	ATmega128	STM32L476RGT6


MYGALE 4S +

LYNX 400

JAGUAR 400



COUGAR 400


Détecteur 4 boucles - S993

2.3.1.3 Le module de communication sécurisé (MCS)

Il se présente sous la forme d'une carte électronique (S996D) à installer dans les capteurs :

- Dimensions : 82 x 47 x 22
- Fonction : Interfacer la communication JBus-RS485 cyber-sécurisée (protocole SERPE CFL V1.0) côté interface avec la communication SPI en clair côté capteur.
- Alimentation à partir du 5 VDC du capteur.
- Communication SPI avec le processeur du capteur : 1Mbit/s.
- Communication JBus-RS485 cyber sécurisée : 19200 bauds / 8 bits / 1 stop bit / parité paire.
- 1 élément sécurisé ATECC608B de Microchip pour :
  - La sauvegarde sécurisée de la clef de chiffrement symétrique
  - La sauvegarde de l'Aad et de l'adresse JBus du module
  - Le chiffrement / déchiffrement selon le standard AES128 GCM.
- 1 microcontrôleur (STM32L442KC)
- Son logiciel pour :
  - La gestion de la communication avec le capteur.
  - La gestion de la communication sécurisée avec l'ICS via la liaison RS485 et à l'aide de l'élément sécurisé.

Fonctionnement :

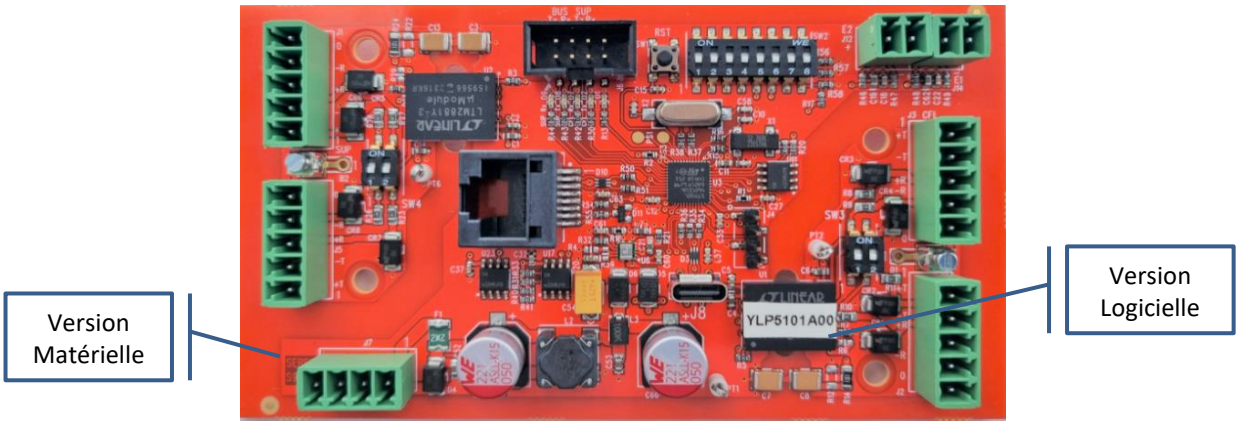
Le MCS interface la communication JBus cyber sécurisée du bus RS485 (protocole SERPE CFL V1.0) avec la communication JBus clair de la liaison SPI du capteur.

La mise en service des cartes MCS, de la programmation de leur micrologiciel jusqu'à leur installation dans les capteurs, zones de confiances, est effectué par un opérateur habilité. Ceci garanti l'intégrité du micrologiciel.

La programmation de la clé d'un MCS se fait par une opération manuelle de raccordement sur l'ICS, effectuée par un opérateur habilité en zone de confiance.

2.3.1.4 L'interface de communication sécurisée

Elle se présente sous la forme d'une carte électronique (S995 D) à installer sur rail DIN près du superviseur en zone de confiance dans un coffret ou une baie informatique :



- Dimensions : 146 x 72 x 40.
- Fonctions :
  - Interfacer la communication JBus-RS485 en clair du côté superviseur avec la communication JBus RS485 cyber sécurisée (protocole SERPE CFL V1.0) côté capteurs.
- Alimentation : 19 VDC à fournir.
- Communication JBus-RS485 avec le superviseur : 115200 bauds / 8 bits / 1 stop bit / parité paire.
- Communication JBus-RS485 cyber sécurisée : 19200 bauds / 8 bits / 1 stop bit / parité paire.
- 3 éléments sécurisés ATECC608B de Microchip assurant :
  - La sauvegarde sécurisée de la clef de chiffrement de chacun des capteurs.
  - La sauvegarde des Aad de chacun des capteurs.
  - Le chiffrement / déchiffrement selon le standard AES128 GCM.
  - Jusqu'à 32 capteurs par ICS avec adresse de 1 à 32.
- 1 microcontrôleur (STM32L462CEU6 en boitier UFQFPN48_7X7_050).
- Son logiciel pour :
  - La gestion de la communication avec le superviseur.
  - La gestion de la communication JBus-RS485 cyber sécurisée avec les capteurs
  - La gestion des clefs.

Fonctionnement :

L'interface chiffre la communication JBus-RS485 du superviseur avec les capteurs via le protocole SERPE CFL V1.0.

Pour cela elle gère de manière « automatique » la création et la sauvegarde aux modules de communication sécurisés des clefs nécessaires aux chiffrement / déchiffrement symétrique utilisé (AES128 GCM). La fourniture des clés générées aux modules doit être réalisée manuellement par un opérateur habilité.

Son rôle est de rendre transparente la communication entre le superviseur et les capteurs cyber sécurisés ou non.

La mise en service des cartes ICS, de la programmation de leurs micrologiciels jusqu'à leurs installations en zones de confiances, est effectué par un opérateur habilité. Ceci garanti l'intégrité du micrologiciel.

2.3.1.5 Le superviseur

Le superviseur qui peut être un simple PC est équipé d'un logiciel de supervision apte à gérer le système complet de protection périmétrique. Pour cela il a besoin de communiquer selon le standard JBus-RS485 avec les capteurs pour à minima :

- Acquérir et afficher leur état.
- Les télécontrôler.
- Historiser leurs évènements.

La capacité du superviseur est variable. Il peut gérer jusqu'à plusieurs centaines de capteurs. Ces derniers sont alors organisés par bus de communication comportant chacun jusqu'à 16 capteurs au maximum.
Pour le superviseur cette cyber sécurisation est transparente.
Il peut ainsi communiquer directement avec les capteurs selon le protocole standard JBus. L'interface et son logiciel rendent la cyber-sécurisation transparente par « encapsulation » des requêtes et des réponse JBus (protocole SERPE CFL V1.0).

2.3.2 Description de l'environnement d'utilisation du produit

Cette solution de protection périmétrique cyber sécurisée est destinée à assurer la sécurité physique des sites de types OIV et OSE. Ces organismes sensibles concernent les secteurs d'activité de l'industrie, du tertiaire, du bancaire, de la défense, de l'énergie, du traitement et de la distribution de l'eau, de l'espace, …
Pour cela la protection périmétrique apporte, selon le niveau de menaces, retardement, dissuasion, détection et alerte pour intervention.
Les technologies de retardement, de dissuasion et de détection sont ainsi choisies au regard du niveau de protection nécessaire.
Par exemples :

- Concertina : détection en isolation et continuité (S993).
- Grille détectrice : détection en isolation et continuité (S993).
- Bavolet détecteur : détection en isolation et continuité (S993).
- Fil tendu détecteur : détection en isolation et continuité (S993) ou détection de toucher capacitive (Lynx 400).
- Clôture électrique : dissuasion HT impulsionnelle et détection de toucher capacitive (Jaguar 400) ou détection coupure ou court-circuit (Cougar 400).
- Clôture grillagée : détection des chocs, grimpés, découpes et sabotage du câble détecteur (Mygale 4S+).

Plusieurs peuvent être associées pour augmenter la qualité de la protection et de la surveillance.

Pour remplir leur mission, les capteurs sont installés au plus près de la périmétrie soit sur la clôture elle-même, soit sur un support ou soit dans une armoire technique. Ils sont télé-alimentés et communiquent en temps réel avec le superviseur par liaison série type RS485 à travers un câble multi paires qui coure de coffret en coffret. Cette liaison RS485 supporte le protocole cyber sécurisé SERPE CFL V1.0 qui protège du piratage la communication et donc évite à la protection périmétrique d'être inhibée partiellement ou totalement.

2.3.3 Description de l'utilisation courante du produit

L'objectif principal d'une protection périmétrique est d'alerter le plus rapidement possible et ce de manière certaine les intervenants de la sécurité du site qu'un évènement anormal est en cours d'occurrence à tel endroit du périmètre. Cette rapidité associée au retard apporté par la sécurité physique de la clôture donne le temps nécessaire aux intervenants pour intercepter le ou les intrus. L'information doit être transmise sans piratage ni inhibition.
Pour cette transmission entre capteurs et superviseur, la sécurité est basée sur le protocole SERPE CFL V1.0 associé à un ICS et des MCS. Clefs et algorithmes de chiffrement sont fournis par un élément sécurisé de marque Microchip et de modèle ATECC608B déclaré conforme au standard de chiffrement symétrique AES128 GCM recommandé par le NIST et l'ANSSI. Chaque ICS utilise trois éléments sécurisés dans lesquelles les informations de chiffrement sont stockées et le MCS des capteurs s'appuie sur son propre élément sécurisé. Ainsi chaque capteur possède une clef unique.

2.3.4 Description des hypothèses sur l'environnement du produit

2.3.4.1 Hypothèses sur l'environnement physique du produit

Les équipements sont installés par des techniciens habilités et formés aux spécificités du système de protection périmétrique et de sa sécurité.

Le superviseur est installé dans un local technique ou un centre de télésurveillance en zone de confiance c'est-à-dire à accès physiques contrôlés et limités aux exploitants et techniciens habilités.

L'interface départ est installée dans la même baie que le superviseur ou dans un coffret situé dans un local technique en zone de confiance c'est-à-dire à accès physiques contrôlés et limités aux exploitants et techniciens habilités.

La liaison JBus-RS485 entre le superviseur et les interfaces sont physiquement sécurisées, en zone de confiance à accès physiques contrôlés et limités aux exploitants et techniciens habilités.

La liaison Cyber JBus-RS485 entre la ou les interfaces et les capteurs utilise un support cuivre ou optique situé en zone non sécurisée.

L'installation des modules MCS et ICS comprenant de la programmation de leurs micrologiciels respectif et la distribution des clés de chiffrement, jusqu'à leur mise en service sont réalisées en zone de confiance par des techniciens SERPE (fabriquant) habilités.

Les capteurs et leur principe de détection sont installés par des techniciens habilités et formés aux spécificités du système de protection périmétrique et de sa sécurité. Ils sont installés à l'intérieur de la zone sécurisé selon leur manuel d'installation respectif (voir [18] à [21]) et réglés selon leur manuel utilisateur respectif ([22] à [25]).
Les capteurs sont intégrés avec leur module de communication cyber sécurisé dans un coffret protégé par un contact d'effraction. Les coffrets sont installés à l'intérieur de la zone de sécurisé, soumise à un accès contrôlé et limité aux exploitants et techniciens habilités, et sont donc en zone de confiance. Les clefs de chiffrement stockées au sein du MCS sont donc protégées en intégrité et en disponibilité par cette hypothèse.

L'alimentation électrique de chacun des équipements est secourue pour une continuité de service définie.

2.3.4.2 Hypothèses sur les exploitants du produit

L'exploitation du système de protection périmétrique s'effectue principalement à partir du superviseur.
Trois profils d'exploitants sont disponibles :

- L'opérateur qui observe l'IHM au quotidien :
  - Il alerte l'équipe d'intervention lors de l'occurrence d'une alarme puis acquitte l'alarme en précisant le résultat de l'intervention.
  - Il s'assure du bon fonctionnement du système en vérifiant qu'aucun défaut technique n'apparaît.
- L'administrateur qui gère le système d'un point de vue administratif et sécuritaire :
  - Il affecte les personnes au regard des profils et de leurs prérogatives.
  - Il limite les accès au regard des prérogatives de chacun.
  - Il gère l'historique et les sauvegardes.
  - Il maîtrise les configurations matérielle et logicielle des équipements du système
  - Il ajuste les niveaux de sensibilités de détection au besoin.
  - Il suit les mises à jour nécessaires des différents logiciels et matériels.
- Le technicien de maintenance qui intervient pour régler les défauts techniques ou modifier les paramètres techniques de fonctionnement lorsque nécessaire. Il peut être amené à intervenir in situ sur les capteurs ou leur principe de détection pour maintenance préventive (mise à jour matérielle, nettoyage, vérification fonctionnement, …) ou corrective. Pour cela il dispose d'un logiciel de configuration sur PC portable et d'une connexion USB surveillée dans chacun des capteurs.

A chacun de ces 3 profils correspond une habilitation avec prérogatives. Ils peuvent bien entendu être affectés à une même personne pour les petits systèmes.
Basé sur une identification par login + mot de passe, la gestion des comptes exploitant s'appuie sur les « Recommandations de sécurité relatives aux mots de passe » rédigées par l'ANSSI (voir : [11] Mécanismes d'authentification référence RGS_B_3).
Ces exploitants de la solution de protection périmétrique sont supposés appartenir à l'organisation interne de gestion de la sûreté du client ou d'un mandataire sous contrôle et autorité de ce service. Ils ont suivi une formation spécifique à leurs attributions et aux tâches qui leurs sont confiées.

2.3.4.3 Hypothèses sur l'environnement technique du produit

Le superviseur intègre le ou les logiciels nécessaires à son rôle de supervision de la protection périmétrique. Il peut fonctionner sous Windows ou sous un autre système d'exploitation. Les comptes administrateur, opérateur et technicien de maintenance sont créés avec les privilèges de chacun et sauvegardés.

Le superviseur doit être capable de détecter les coupures de communication avec les capteurs. La perte de communication avec un capteur doit entraîner une levée d'alarme par timeout sur le superviseur.

Afin d'optimiser les temps de réponse, deux mécanismes de cache des données est mis en œuvre :

Entre MCS et capteur

- Les MCS interrogent à rythme régulier les capteurs pour mise en mémoire tampon et pré-chiffrent ces données.

Entre ICS et MCS

- Le superviseur interroge les capteurs à leur adresse.
- Si l'ICS a la donnée à jour dans sa mémoire tampon, il la retourne directement sans interroger le capteur. Sinon il passe l'interrogation au capteur et retourne se réponse.
- L'ICS maintien sa mémoire tampon par ses interrogations propres des capteurs. Ce mécanisme d'interrogation périodiques est activé et maintenu par les requêtes superviseur/capteur.

La communication avec les capteurs est sécurisée grâce aux chiffrement / déchiffrement effectués par l'interface et les modules (protocole SERPE CFL V1.0).
L'interface départ gère aussi les clefs de chiffrement symétriques. Elle est la seule, avec l'interface de maintenance qui est renseignée par l'interface départ, à connaître les clefs opérationnelles. Chaque clef est sauvegardée, de manière sûre, dans l'élément sécurisé relatif à chacun des capteurs dans les interfaces et les modules.

Les capteurs sont télé-réglés pour offrir une détection optimale au regard de l'environnement de l'installation et du type de menace. Par leur construction ils fournissent via leur table d'échange leur état et leurs variables de fonctionnement à l'interface après chiffrement par le module cyber sécurisé.

2.3.5 Description du périmètre d'évaluation

La présente cible de sécurité prévoit l'évaluation des équipements suivants :

- Les ICS pour leurs parties communication avec les « éléments sécurisés » et gestion de la communication RS485-JBus cyber-sécurisée (protocole SERPE CFL V1.0).
- Le lien « CFL V1.0 » entre interfaces et modules.
- Les MCS connectés aux capteurs pour leurs communication avec l'élément sécurisé et leur gestion de la communication RS485-JBus cyber-sécurisée (protocole SERPE CFL V1.0).

Ainsi l'évaluation porte sur la communication CFL RS485 inter capteurs au protocole SERPE v1.0 à l'exception des équipements et des fonctions situés en zone de confiance entourés de vert sur la figure du § Architecture globale de la solution. Ces zones de confiance concernent :

- Le boitier ICS localisé dans une armoire protégée de l'ouverture et avec détection.
- Le boitier MCS – Capteur protégé par une détection d'ouverture et installé à l'intérieur de la zone sécurisée.

Le domaine d'agrément CSPN de l'évaluation est « Matériel et logiciel embarqué ».

2.4 Environnement Technique

L'évaluation est menée sur une plateforme semblable à celle du § Architecture globale de la solution. Elle intègre au moins un de chaque capteur du catalogue SERPE (Jaguar 400, Cougar 400, Lynx 400, Mygale 4S+ et S993), 1 ICS et un superviseur. Le Cougar utilisant la même carte que le Jaguar n'est pas inclus dans l'environnement d'évaluation.

L'interface communique via une liaison JBus-RS485 avec le superviseur. Elle est paramétrée pour un fonctionnement normal avec les capteurs et avec le superviseur.

Une opération d'initialisation et de fourniture des clés de chiffrement aux capteurs, doit être manuellement réalisée selon le manuel utilisateur avant la mise en service.

Chaque capteur est relié au bus CFL par le biais d'un module MCS qui lui et intégré. Leur paramétrage est standard. Leurs principes détecteurs sont simulés par :

- 1 résistance de 3 kΩ pour chacune des boucles de la S993.
- 1 résistance de 330 kΩ pour chacun des segments du Mygale 4S+.
- 1 circuit HT de type RC 1kΩ – 10 nF pour le Jaguar 400 et le Lynx 400.
- 1 fil simple pour le Cougar 400.

Le superviseur est au choix du client, le produit ne modifiant pas l'API de communication avec les capteurs. Le superviseur doit assurer la remonté d'information sur perte de communication des capteurs.

Le superviseur, le Jaguar 400, le Cougar 400 et le Lynx sont alimentés par le secteur 230 VAC. Le Mygale 4S+ et la S993 sont alimentés par une alimentation de laboratoire 230 VAC / 14 VDC. Les interfaces sont alimentées par une alimentation 230 VAC / 5VDC.

L'ensemble est sous tension et opérationnel :

- L'interface ICS communique périodiquement avec les capteurs.
- Le superviseur via l'interface départ interroge périodiquement les capteurs pour acquérir, signaler et historiser leurs états.
- Le superviseur via l'interface interroge en direct (de manière transparente à travers l'ICS) les capteurs pour en connaître les paramètres de fonctionnement et pour en vérifier leur intégrité.
- Le superviseur affiche les statistiques des défauts de communications.

Synthèse des éléments d'environnement des composants évalués.

Composant du système Global			Inclus dans le produit évalué	Non évalué (Environnement du produit)	
				Supposé de confiance	Attaquant éventuel
Communs ICS et MCS	C_A.1	Matériel et micrologiciel (respectivement MCS et ICS)	X		
	C_A.2	Composant cryptographique et librairie	X		
	C_A.3	BUS CFL	X		
Environnement MCS	C_A.4	Capteur		X (zone de confiance)	
Environnement ICS	C_A.5	BUS Supervision		X (zone de confiance)	
	C_A.6	Interface PERLE (RS485-IP)		X (zone de confiance)	
	C_A.7	Supervision		X (zone de confiance)	

3 Problème de sécurité

3.1 Biens sensibles

Les biens sensibles pour le système de communication cyber sécurisé SERPE V1.0 sont de plusieurs natures :

Réf.	Description
B1	Les paramètres de fonctionnement des capteurs (hors adresse et clé). Ils doivent être intègres et disponibles.
B2	Les paramètres de fonctionnent ICS et MCS. Ils doivent être intègres et disponibles. Ces paramètres sont stockés localement dans la mémoire de configuration (table d'échange) et accessible par requête.
B3	Les clefs de chiffrement symétrique AES128 GCM. Elles doivent être intègres et disponibles, et protégées en confidentialité : • Dans les interfaces. • Dans les modules.
B4	La donnée circulant sur le bus de terrain CFL – RS485 (protocole SERPE CFL V1.0). Elle doit être confidentielle, intègre, authentifiable, protégée contre l'anti-rejeux et disponible.
B5	Les microcodes de l'ICS ainsi que du MCS doivent être protégés en confidentialité et en intégrité.

3.2 Matrice de couverture entre les biens et les protections associées

Protections / Biens	Confidentialité	Intégrité	Authentification	Disponibilité
B1		X		X
B2		X		X
B3	X	X		X
B4	X	X	X	X
B5	X	X		

3.3 Utilisateurs

Les utilisateurs du produit sont :

Description de l'acteur		Degré de confiance
A.1 Personnel et Techniciens fabriquant (SERPE) habilités	Gestion du stock, Expédition, Installation, Mise en service, Maintenance	De confiance car habilités.
A.2 Exploitants habilités	Maintenance	De confiance car habilités.
A.3 Logiciel de supervision	Client 'logique' de supervision.	De confiance.
A.4 Capteur hôte	Client 'logique' terminal.	De confiance.

Le produit est en distribution directe (par de chaîne logistique/revente), installé et configuré (programmation FW et première attribution de clés) par un technicien SERPE habilité.

3.4 Mesures environnementales

Comme indiqué sur la figure du § Architecture globale de la solution, le superviseur et ses ICS ainsi que les capteurs équipés de MCS sont à installer en zone de confiance accessible uniquement par les personnes habilitées : opérateur(s), administrateur(s) et technicien(s) de maintenance.
Le bus de terrain peut être hors zone de confiance. Son accès n'est donc pas nécessairement contrôlé.

Ces mesures font partie des « bonnes pratiques ». Selon l'organisation de l'organisme utilisateur, elles sont à porter à la connaissance des personnes en charge de la sécurité du site. Elles se présentent sous forme de consignes, circulaires, notes ou documents confidentiels.

Synthèse des mesures environnementales

Type de mesure	Description de la mesure	Acteurs en charge de la mesure
Organisationnelle	Mise en service (dont programmation microcode) par un technicien fabriquant habilité.	A.1
	Maintenance par technicien de maintenance habilité.	A.2
	Exploitation (signalement et gestion des alarmes et défauts techniques) par l'opérateur.	A.2
	Effectuer une mise à jour des accès pour chaque évolution du personnel.	A.2
Logistique	Les pièces détachées nécessaires à la maintenance sont stockées en zone de confiance à accès contrôlé. Chaque entrée et sortie est tracée (date, heure, nom du technicien, référence, configuration avec version du logiciel …).	A.2

Méthodologique	Des tests de détection en grandeur réelle sont à réaliser périodiquement et après chaque intervention sur les zones de protection concernées. Ils permettent de s'assurer du bon fonctionnement des équipements après la fermeture de leur coffret et donc après la fin de l'alarme « effraction coffret ».	A.2
	Traiter toutes les remontées d'information qu'elles soient de type alarme ou défaut technique.	A.2
	Enregistrer toutes les interventions qu'elles soient sécuritaires ou techniques.	A.2
	Toute intervention technique sur les capteurs demande une autorisation de l'opérateur et est limitée dans le temps.	A.2
	Les alarmes « effraction » ou « branchement outil de maintenance » demandent une attention particulière quant à leur suivi. Elles doivent correspondre à une intervention autorisée.	A.3

3.5 Menaces

Les menaces concernant la communication CFL - RS485 SERPE objet de la cible de sécurité sont catégorisées en 2 types :

- Les attaques physiques sur le matériel durant leur exploitation ou leur maintenance.
- Les attaques logiques pendant l'exploitation du système.

Les menaces sont des évènements volontaires (attaque) ou involontaires :

- Exemple de menace involontaire : erreur de saisie d'un paramètre de réglage de sensibilité lors d'une intervention de maintenance).

Seuls les équipements du système de protection périmétrique situés hors zone de confiance sont pris en compte dans la description des menaces.

Les menaces peuvent demander des moyens d'attaque évoluées voire sophistiquées : préméditation, personnes initiées, fortement équipée, renseignées à partir de connaissances confidentielles sur la conception et l'exploitation du système et en possession de matériel spécifique de cryptanalyse conçu spécialement pour neutraliser la sûreté en place.
Seules les menaces jugées probables et impactantes sont retenues.

3.5.1 Menaces physiques et logiques

ID	Description	Menace	Impact
M1	Un attaquant ayant accès physique au bus peut le couper.	Mise hors service partielle de la communication avec les capteurs.	Plus de communication avec les capteurs situés après la coupure. Protection partiellement interrompue.
M2	Un attaquant ayant accès physique au bus peut le court-circuiter.	Mise hors service complète de la communication avec les capteurs.	Plus de communication avec les capteurs. Protection complètement interrompue.
M3	Un attaquant ayant accès physique au bus d'alimentation des capteurs peut le court-circuiter ou le couper.	Mise hors service complète des capteurs.	Arrêt complet de la protection.

M4	Un attaquant ayant accès au stock peut lire et/ou falsifier le microcode des MCS/ICS	Fraude par falsification du microcode dans le stock de maintenance	Détection rendue inopérante ou perturbée avec risque d'interruption de la protection.
M5	Un attaquant ayant accès au bus peut falsifier l'état des capteurs.	Atteinte à l'intégrité des données échangées.	Communication sabotée et/ou fonctionnement détection perturbée avec risque d'interruption de la protection.
M6	Un attaquant ayant accès au bus terrain peut cloner/rejouer des messages.	Clonage / rejeux de messages	Communication sabotée et/ou fonctionnement détection perturbée avec risque d'interruption de la protection.
M7	Un attaquant ayant accès au bus terrain peut saturer le bus par envoi de messages intempestifs et/ou falsifiés.	Déni de service.	Communication sabotée et/ou fonctionnement détection perturbée avec risque d'interruption de la protection.
M8	Un attaquant ayant accès au bus terrain peut extraire par cryptanalyse la clef de chiffrement.	Extraction par cryptanalyse de la clef de chiffrement symétrique pour clonage.	Chiffrement et communication corrompus. Clonage et donc inhibition partielle ou complète de la protection.
M9	Un attaquant peut déchiffrer un message par cryptanalyse sans connaitre la clef de déchiffrement	Déchiffrement d'un message par cryptanalyse	Perte de confidentialité des données transitant sur le bus. Le système reste opérationnel.
M10	Un attaquant ayant accès au bus peut extraire les données transitant sur le bus.	Interceptions des données sur le bus	Perte de confidentialité des données transitant sur le bus. Le système reste opérationnel.

3.5.2 Matrice de couverture entre les menaces et les biens impactés

Biens / Menaces	B1	B2	B3	B4	B5
M1	X	X		X	
M2	X	X		X	
M3	X	X		X	
M4					X
M5	X	X		X	
M6	X	X		X	
M7	X	X		X	
M8			X		
M9				X	
M10				X	

4 Fonctions évaluées

Les fonctions de sécurité de la communication CFL RS485 SERPE offrent une sécurisation de son fonctionnement par empêchement des conséquences des attaques et/ou par signalisation de l'impact des attaques.

4.1.1 Fonctions de sécurité en réponse aux menaces physiques et logiques

ID	Description	Attaque	Biens
F1	Remontée par l'ICS des messages capteurs correctement authentifiées, déchiffrées et à jour uniquement.	Coupure du bus.	B1 – B2 – B4
		Court-circuit du bus.	
		Coupure ou court-circuit sur le bus d'alimentation du capteur	
		Saturation du bus par envoi de messages intempestifs et/ou falsifiés	
F2	Composants stockée vierges, programmation à la mise en service par personnel habilité puis passage du microprocesseur en exécution seule pour éviter toute relecture/réécriture.	Réécriture du code source du microcode pour falsifier le fonctionnement du capteur	B5
F3	Utilisation de l'AES128 en mode GCM pour s'assurer de la confidentialité des messages mais aussi de leur intégrité. L'utilisation d'un Tag permet d'authentifier le message et un compteur unique, qui permet, lui, l'anti-rejeux.	Homme du milieu (écoute du bus) ou clonage de carte existante. Rejeux des messages écoutés.	B4
		Cryptanalyse pour usurper la clef de chiffrement	B3
		Cryptanalyse pour déchiffrer un message.	B4

4.1.2 Matrice de couverture entre les fonctions de sécurité et les menaces

Menaces / Fonctions de sécurité	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
F1	X	X	X				X			
F2				X						
F3					X	X		X	X	X

5 Surface d'attaque : synthèse des interfaces vers les fonctions du produit

Type de surface d'attaque	Interfaces (accessibles ou non accessibles)	Acteurs ayant accès aux interfaces
Interfaces physiques	Surface PCB (pistes, composants) Ports : • 'CI' vers capteur (Alimentation, SPI) • Bus RS485 • Port USB • Port prog SWIO / JTAG • Prise RJ45 (non ethernet)	A.1 A.2
Interfaces logiques	Port capteur SPI	A.4 Capteur
	Bus CFL (RS485)	A.4 Capteur
	Port Supervision	A.3 Supervision

Les interfaces physiques résident en zones de confiance et ne sont accessibles que par des acteurs de confiance.
Les interfaces logiques non chiffrées sont en zones de confiance.
L'interface logique chiffrée est l'élément à protéger, hors zone de confiance.