elsylog
Parc d'activités des Berges de Seine 3
10-12 rue Marcel Paul - 95870 Bezons
Fax : +33 (0)1.39.61.57.59 - accueil@elsylog.com
+33 (0)1.39.61.05.80 www.elsylog.com

Cible de sécurité CSPN V1.4

UTL « SYRIUS-2P2L-IP-EXT version 1660f »

13/02/2020

Date	Version	Motif	Rédacteur
01/08/2018	V1.0	Version initiale	OPPIDA
25/10/2018	V1.1	Correction des versions des logiciels	OPPIDA
04/07/2019	V1.2	Mise à jour des version logiciels Ajout d'une hypothèse manquante sur la protection en intégrité,confidentialité et authenticité de la clé diversifiée stockée dans le badge desfire. Ajout d'une hypothèse manquante sur les exploitants. Retrait, du dialogue badge desfire / lecteur, du périmètre de certification Ajout d'une protection en intégrité sur la fonction F.PROTEC_COM_RS485 Ajout de traçabilité entre menaces,biens et fonctions de sécurité. Ajout d'une hypothèse H_INJECTION_CLE_SSCPV2 et de la fonction F_PROTECT_FIRMWARE. Modification de F_PROTECT_CODE_PIN, F_PROTECT_UTL et M.PHYS_UTL	ELSYLOG
28/01/2020	V1.3	Modification de la version (devient 1660f) du firmware utl dans le tableau "Configuration évaluée". Nouveau firmware pour parer au problème de l'attaque relai.	ELSYLOG
13/02/2020	V1.4	Modification de l'entête , du titre, de l'identification du produit (page 5) et du tableau paragraphe 3.2 pour indiquer que l'évaluation concerne l'UTL Syrius	ELSYLOG

Liste de diffusion

Nom	Prénom	Société	Contact
-	-	ANSSI	-
MARY	Olivier	OPPIDA	olivier.mary@oppida.fr
ZAHM	Vincent	ELSYLOG	vincent.zahm@elsylog.com
PELLERIN	Philippe	ELSYLOG	philippe.pellerin@elsylog.com

Table des matières

1 IDENTIFICATION DU PRODUIT

Ce document constitue la cible de sécurité pour une évaluation **CSPN de l'utl Syrius** intégrée au système de contrôle d'accès SYRACUSE 6.01.01 développé par la société ELSYLOG.

Editeur	ELSYLOG
Site de l'éditeur	www.elsylog.com
Nom commercial du produit	SYRIUS
Version évaluée	1660f
Catégorie de produit	Identification, authentification pour le contrôle d'accès physique

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GÉNÉRALE DU PRODUIT

Le système de contrôle d'accès SYRACUSE est composé de :

- Badges Mifare Desfire EV1/EV2, norme ISO 14443

- lecteurs de Proximité MIFARE DESFIRE (Modèle SYL123-S-ARCDES), compatibles avec tous les identifiants Mifare sécurisé Classic - Mifare Plus - Desfire EV1/EV2 ISO 14443 A et B ISO 18092 - Portée de lecture 5 cm environ.

  Dans le cadre de l'évaluation la cible sera constituée avec des lecteurs de badges DESFIRE (SY-DES4ko) et badges MIFARE DESFIRE EV1/EV2.

- raccordés sur des unités de traitement SYRIUS 2P2L-IP-EXT : Gestion de 2 têtes de lecture en entrées/sorties

  Ces UTL acceptent en standard, le raccordement sur un réseau TCP/IP

- Les unités de traitement embarquent une carte SAM AV2 NXP permettant la gestion et la sécurisation des clés utilisées dans le cadre des communications avec le badge, ainsi que celles nécessaires à la communication avec le serveur.

- Les informations enregistrées par les unités de traitement sont centralisées par notre logiciel SYRACUSE, configuré en multiposte et gérant jusqu'à 2048 lecteurs.

  Un certain nombre de modules peuvent être ajoutés dans le logiciel SYRACUSE afin de gérer des éléments particuliers (Ascenseurs, Personnalisation de badges, …)

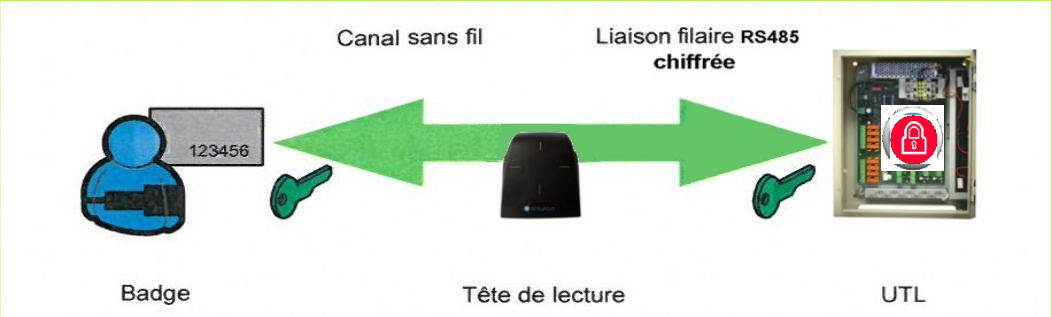
- Le système est administré via des postes clients équipés d'un lecteur encodeur / enrôleur (Modèle OMNIKEY 5422 compatible PCSC) permettant aux opérateurs, outre d'encoder les badges, d'accéder, sur simple lecture de leur badge, au logiciel de façon rapide, d'effectuer les fonctions d'activation et de rendu de badge, d'identifier un badge du site trouvé (numéro de série des badges non sérigraphié).

Le lecteur encodeur/enrôleur utilise une carte SAM assurant la sécurité des clés d'accès aux badges DESFIRE.

2.2 DESCRIPTION FONCTIONNELLE DU PRODUIT

2.2.1 Le mode transparent.

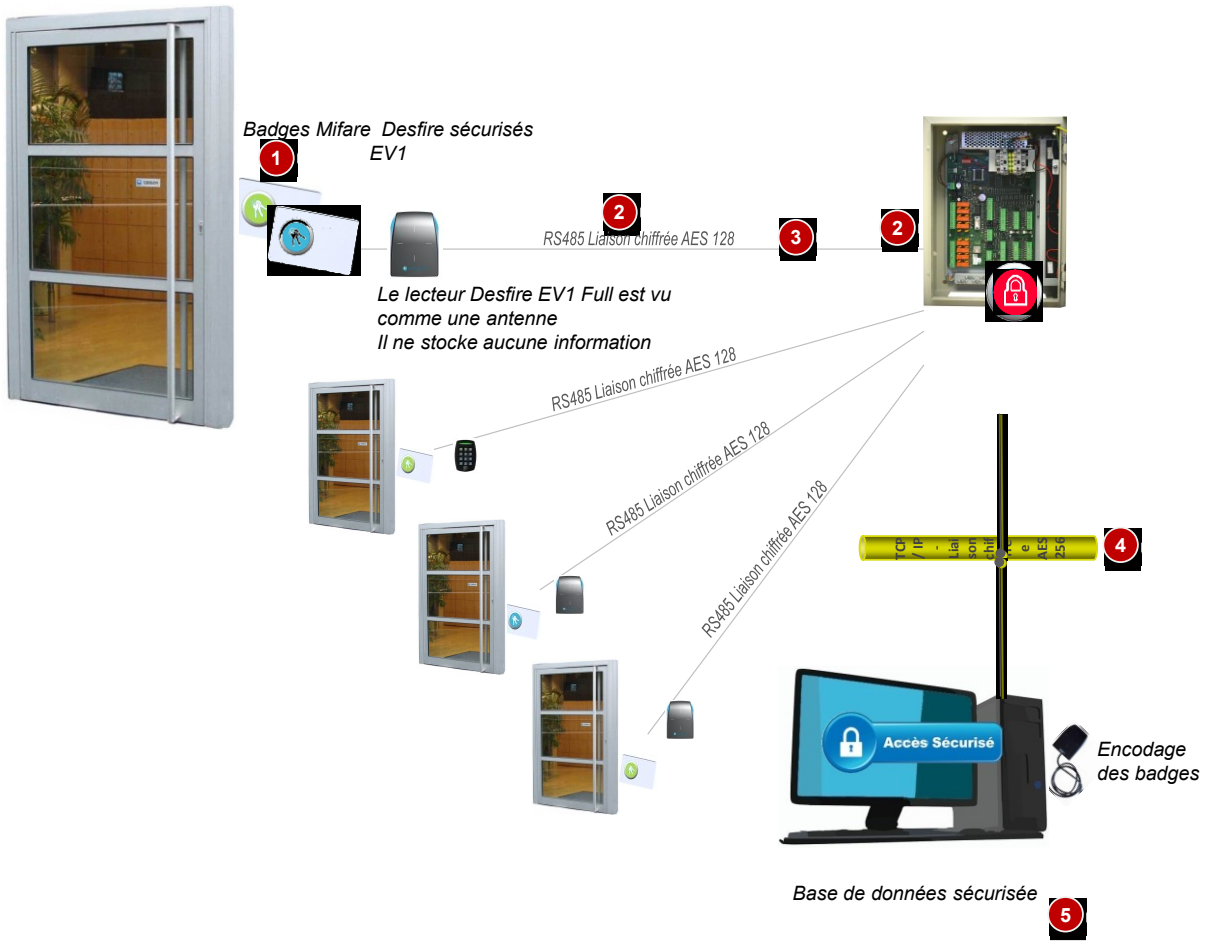
Le système de contrôle d'accès SYRACUSE repose sur l'utilisation du mode transparent des lecteurs de badges. Ce mode de fonctionnement est préconisé par l'ANSSI.



Dans ce mode de fonctionnement, les clés de chiffrement de la communication entre le badge et l'UTL ne sont pas stockées dans la tête de lecture mais dans l'UTL. En l'occurrence dans la carte SAM pour le cas qui nous concerne.

2.2.2 Architecture générale

Le schéma ci-dessous présente l'architecture générale du système SYRACUSE



1 **Badge Mifare Desfire EV1, norme ISO 14443,**

2 **Maillon Lecteur / UTL :** Le lecteur transparent garantit que les clefs d'accès aux données des badges ne se trouvent pas dans le lecteur lui-même, mais stockées dans la carte SAM de l'UTL (Unité de Traitement Locale) placée en zone sécurisée à l'intérieur du bâtiment. Le risque de se voir dérober un lecteur contrôlant un accès périmétrique du site contenant des informations sensibles n'existe plus.

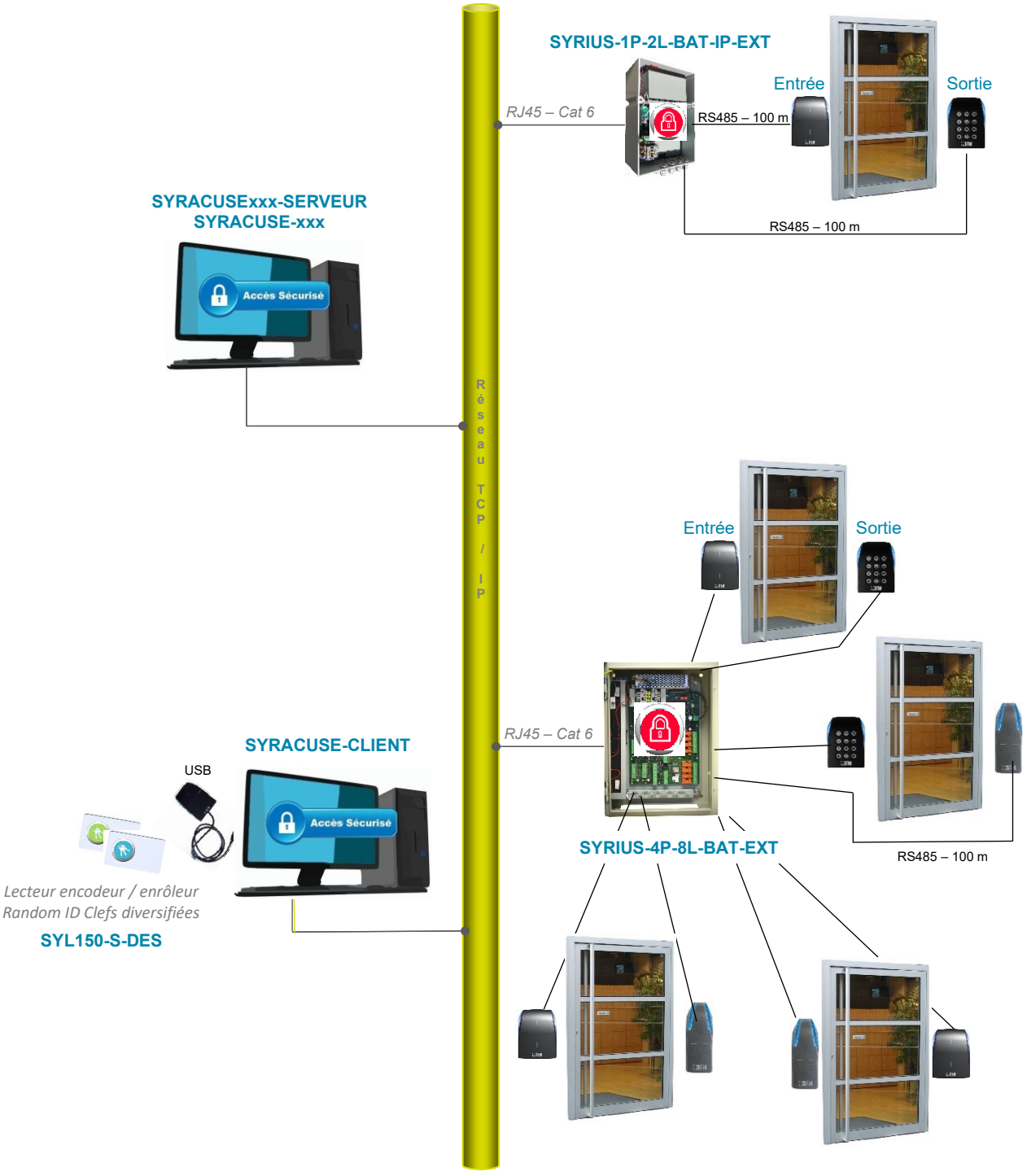
3 **Maillon communication entre le lecteur et l'UTL :** La liaison entre le lecteur et l'UTL est assurée via une interface RS485. Sur cette liaison est mis en œuvre un chiffrement des données en AES128 (voir protocole SSCPV2 Stid).

4 **Maillon Réseau IP :** autre liaison chiffrée impérative aujourd'hui, le réseau IP étant devenu un standard de communication dont les multiples moyens d'écoute représentent une vulnérabilité certaine : afin de résoudre cette faille de sécurité

potentielle, ELSYLOG chiffre toutes les données entre les UTL et le serveur (chiffrement AES 128, 256 …) et intègre un mécanisme d'anti-rejeu.

5. **Maillon Serveur :** nous préconisons l'installation du logiciel sur une machine virtuelle et assurons une exploitation avec une base de données sécurisée compatible SQL.

Le schéma ci-après présente l'implantation logique d'une installation typique de SYRACUSE



 SYL123-S-ARC1-DESF

 SYL123-S-ARCDESF

 SYL123-S-ARCDESF-C

2.2.3 Tête de lecture 13,56 MHz Stid – RS485 - Architect

- Tête de lecture déportée de l'électronique de gestion de l'accès (UTL) évolutive (option faces multifonctions interchangeables)
  Réf. Modèle standard : SYL123-S-ARCDESF
  Réf. Modèle de faible encombrement pour montants de porte : SYL123-S-ARC1-DESF
- Lecture de tous les identifiants normés 13,56 MHz Mifare Classic, Mifare Plus et Desfire EV1/EV2, ce qui peut assurer le basculement progressif d'une technologie à l'autre
- Lecteur de Très Haut Niveau de Sécurité (AES de Desfire EV1/EV2)
- Numéro de badge encodé avec des clefs de sécurité privées et transmis par l'UTL sur une liaison sécurisée RS485 (confidentialité des données transmises par chiffrement et authentification)
- Portée de l'ordre de 5 cm selon le type d'identifiant et d'environnement
- Fonctions Badgez, Accès autorisé, Accès refusé, Position de la porte (ouverte / fermée) et Mode de gestion de l'accès (libre, interdit) matérialisées par 1 buzzer et 1 leds à 3 couleurs
- Solution d'autoprotection et d'anti-arrachement intégrée
- Modèle robuste et protégé des intempéries pour intégration dans tous types d'environnement
- Boîtier compact : capot démontable et interchangeable (option faces multifonctions interchangeables) – IP 65 hors connectique – IK 10
- Excellente résistance à la poussière, à l'humidité et au vandalisme grâce à sa coque en polycarbonate renforcée et sa carte électronique tropicalisée
- Raccordement aisé par bornier à vis débrochable
- Arrachement détecté par un accéléromètre configurable par badge (sortie contact sec)

2.2.4 Tête de lecture 13,56 MHz Stid – RS485 – Architect avec clavier

- Têtes de lecture déportées de l'électronique de gestion de l'accès (UTL) avec clavier : Boîtier compact et résistant (antenne et contrôleur / décodeur totalement encapsulés dans de la résine)
  Réf SYL123-S-ARCDESF-C
- Fonctionnement possible sur plages horaires en Badge + Code secret pour augmenter le niveau de sécurité dans l'identification du porteur de badge :
  Badge seul pour tous Code seul pour tous Badge ou code seul selon.
- Proximité 13,56 MHz Mifare sécurisé Classic - Mifare Plus - Desfire EV1/EV2 ISO 14443 A et B ISO 18092 (NFC) pour projets multi-applicatifs
- Portée 4 à 6 cm selon l'identifiant et l'environnement
- Lecteur de Très Haut Niveau de Sécurité (AES de Desfire EV1/EV2)
- Numéro de badge encodé avec des clefs de sécurité privées et transmis par l'UTL sur une liaison sécurisée RS485 (confidentialité des données transmises par chiffrement et authentification)
- Fonctions Badgez, Accès autorisé, Accès refusé, Position de la porte (ouverte / fermée) et Mode de gestion de l'accès (libre, interdit) matérialisées par 1 buzzer et 3 Leds
- Grande robustesse en environnements intérieurs ou extérieurs et haut niveau de résistance au vandalisme (boîtier compact, clavier étanche, coque autoextinguible, antenne et contrôleur / décodeur encapsulés dans de la résine)
- Raccordement aisé par bornier à vis
- Arrachement détecté par un accéléromètre configurable par badge (sortie contact sec)

2.2.5 Unité de traitement 1 à 8 lecteurs – RS422 ou IP

- Réf. SYRIUS-4P8L-EXT-BAT Gestion de 1 à 4 lecteurs avec des mémoires locales par lecteur adaptées à chaque configuration :
  - ❖ 1 lecteur : 20 000 badges autorisés et 1 024 événements
  - ❖ 2 lecteurs : 12 000 badges autorisés et 1 024 événements
  - ❖ 3 à 8 lecteurs ; 5 000 badges autorisés et 1 024 événements

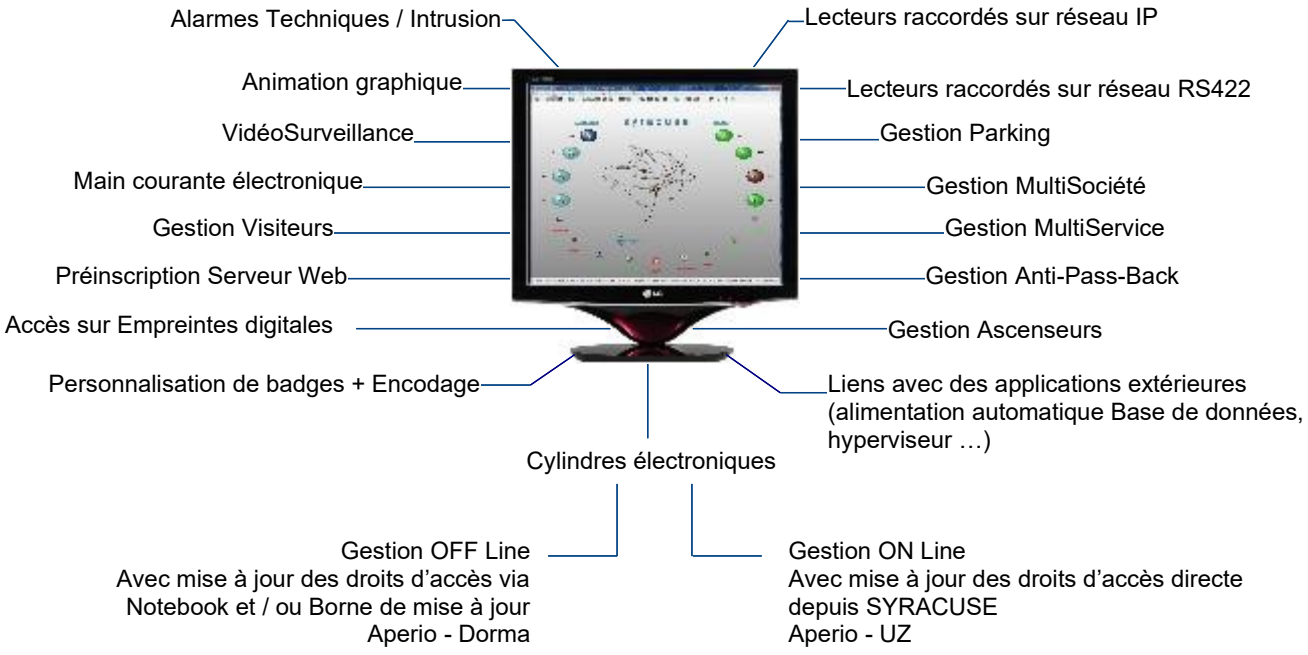
Photo non contractuelle

- Temps de traitement d'un badge : < 0,10 seconde
- Alim. 220 V à découpage + bat. 12V 12Ah (3 A dispo sous 12 V)
- Prise de décision locale, sans dégradation du niveau de sécurité en cas de rupture de dialogue avec le système de gestion
- Génération de l'événement correspondant et diffusion au système de gestion en temps réel
- Raccordement au système de gestion via IP
- Gestion classique ou évoluée des accès (sas, ascenseur, parking …)
- Armoire métallique fermée à clef - IP 55-9
- Plaque support presse étoupes prédécoupées pour sorties de câbles (12 presse étoupes ø 9, 11, 13 mm)
- Raccordements par borniers à vis embrochables
- Circuit horloge calendaire sauvegardé
- Contact d'autoprotection du coffret

Ces UTL peuvent gérer en standard jusqu'à 8 têtes de lecture en mode 4 portes entrée/sortie. Dans cette configuration, elles permettent de mémoriser localement jusqu'à 5 000 badges autorisés et 1 024 événements par tête raccordée.
Le même modèle permet un raccordement au système de gestion via bus terrain RS422 ou via réseau TCP / IP

2.2.6 Contrôle d'accès SYRACUSE

- Solution haut de gamme de Contrôle d'accès multiposte (jusqu'à 40 postes Client)
- Ergonomie intuitive accompagnée d'une aide en ligne (touche F1)
- Environnement Windows 64 bits
  Principe réseau : support Ethernet avec protocole TCP/IP pur (architecture Client / Serveur).
- Conception modulaire :
  - ❖ Licences pour 8, 16, 32, 64, 128, 512, 896 ou 2 048 lecteurs gérés
  - ❖ Nombreuses fonctionnalités :



2.2.7 Caractéristiques des serveurs et des postes d'exploitation

	< 16 lecteurs – 300 badges	< 128 lecteurs – 1 000 badges		> 128 lecteurs – 1 000 badges	
	Monoposte	**Serveur**	**Client**	**Serveur**	**Client**
Processeur	**Intel I3** ou équivalent et >	**Intel I5** ou équivalent et >	**Intel I3** ou équivalent et >	**Intel I7** ou équivalent et >	**Intel I3** ou équivalent et >
Mémoire RAM	**4 Go et >**				
Disque dur	**500 Go et >**				
Ecran	**Pour SYRACUSE seul : 17 pouces et >** **Pour SYRACUSE et SYGAL (intrusion, synoptiques) : 21 pouces et Résolution selon les plans**				
Périphériques	**USB, COM1, COM2** – Fonction des équipements retenus pour le poste : **concentrateur (RS232C**), **lecteur enrôleur (USB ou RS232C)**, imprimante Rapports etc… ***Prévoir une unité de sauvegarde (données, historique) : Disque dur externe, graveur, clef USB …***				

	Poste Serveur 64 bits	Poste Client 64 bits
Environnement Windows	**Seven Pro** **Windows 8.1** **Windows serveur 2008 R2** **Windows Serveur 2012** **Windows Serveur 2016**	**Seven Pro** **Windows 8 8.1** **Windows 10**

3 CONTEXTE D'EVALUATION

3.1 PÉRIMÈTRE D'ÉVALUATION

La ToE est composée des éléments physiques suivants :

- Badges Mifare Desfire EV1/EV2, norme ISO 14443.
- Lecteurs de Proximité MIFARE DESFIRE (Ref Esylog : SYL123-S-ARCDESF – Ref Stid : ARCW33APH57AD1), (Ref Elsylog : SYL123-S-ARCDESF-C -Ref Stid : ARCW33BPH57AD1) raccordées sur des unités de traitement SYRIUS via une liaison RS485.
- UTL SYRIUS (Modèle SYRIUS-2P2L-IP-EXT et SYRIUS-4P8L-BAT) raccordée au serveur SYRACUSE via un réseau de terrain IP. L'UTL dispose d'un module de sécurité SAM AV2 de la société NXP. Ce module hérite d'une certification Critères Communs EAL5+.

La carte **SAM**, le **serveur SYRACUSE** le **poste d'exploitation** et le **badge DESFIRE** ne font pas partie du périmètre d'évaluation.

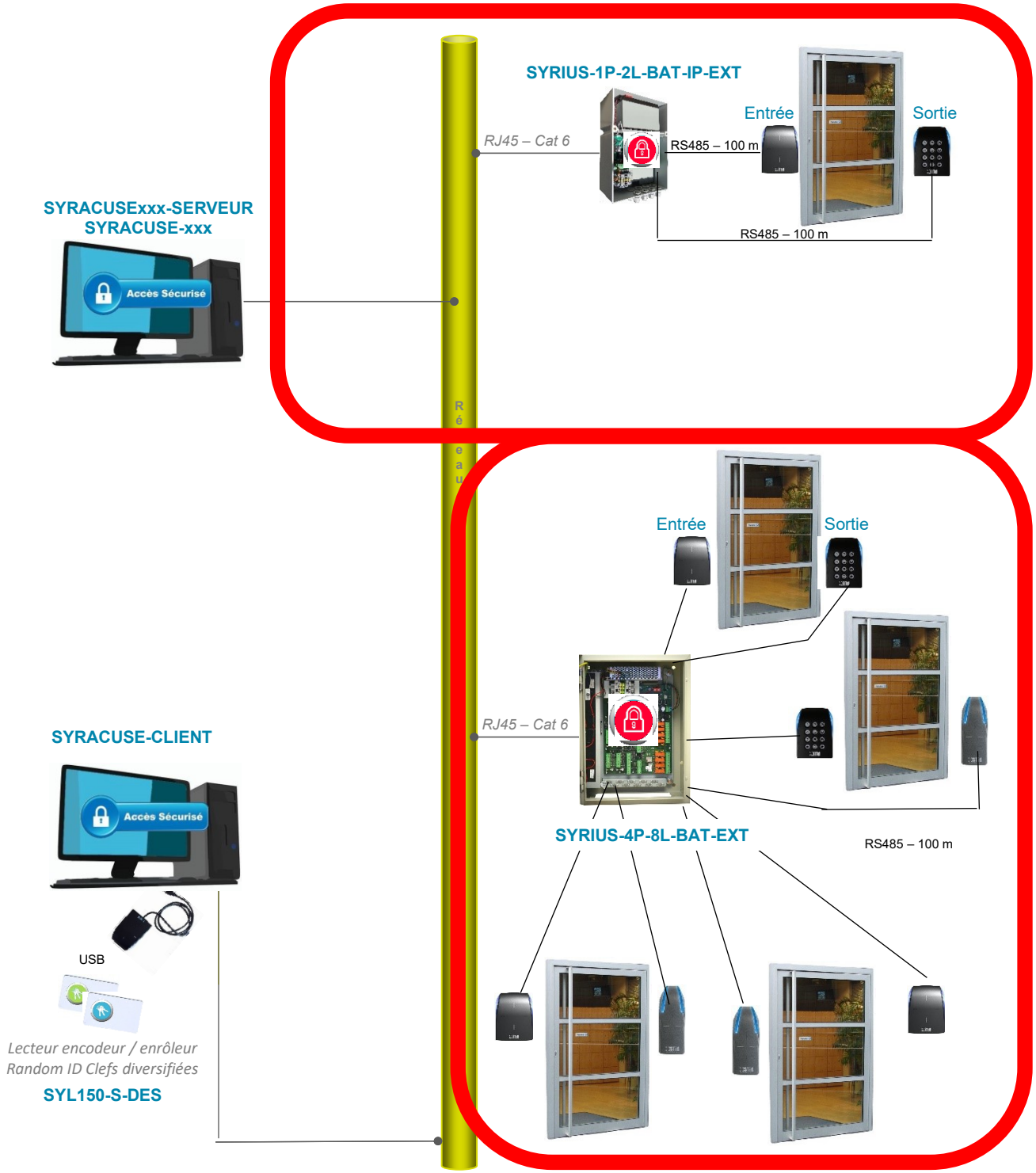
L' interface de la ToE suivante ne fait pas partie du périmètre de l'évaluation :

- Interface de communication entre les badges et les lecteurs.

Les interfaces de la ToE suivantes font partie du périmètre de l'évaluation :

- Interface de communication entre les lecteurs de proximité et l'UTL (RS485).
- Interface de communication entre l'UTL et le serveur SYRACUSE (réseau IP).

Le périmètre d'évaluation est représenté sur le schéma ci-dessous :



3.2 CONFIGURATION ÉVALUÉE

La configuration évaluée est détaillée au sein des tableaux ci-dessous :

Solution	SYRIUS-2P2L-IP-EXT
Version	1660f

Nomenclature des composants retenus pour l'évaluation :

Description	Nom	Fabricant	Modèle / Version
Lecteur de proximité	Lecteur simple	STID	ARCW33APH57AD1
	Lecteur avec clavier	STID	ARCW33BPH57AD1
Unité de traitement	SYRIUS 2 Portes	ELSYLOG	Firmware: SYRIUS-2P2L-IP-EXT version 1660f PCB: 181101 ind. C
Badges		NXP	Mifare Desfire EV1/EV2
SAM		NXP	SAM AV2

4 DEFINITION DU PROBLEME DE SECURITE

4.1 UTILISATEURS DU PRODUIT

Usager porteur de badge

Il s'agit de l'utilisateur final du système de contrôle d'accès. L'usager porteur de badge interagit avec le lecteur de badges et se voit octroyer des droits d'accès en fonction de son profil. L'interaction avec le lecteur de badge peut se faire de deux manières : présentation simple du badge ou présentation du badge avec saisie d'un code PIN.

Exploitant

L'exploitant configure et exploite le système de contrôle d'accès à partir d'une station d'exploitation. Il configure notamment les droits d'accès des usagers. Les exploitants n'ont pas d'accès aux UTL.

Installateur/Mainteneur

Il s'agit des personnels qui mettent en œuvre le système à son installation et qui en assurent la maintenance. Ce sont ces personnels qui ont accès aux UTL.

Officier de sécurité

Ces personnels ont le plus haut niveau de droits d'accès au système. Ils possèdent les privilèges maximums sur le serveur et ils paramètrent également les données de sécurité du système (clés de gestion du badge, profils des exploitants, injections de clés dans les cartes SAM).

4.2 HYPOTHÈSES SUR L'ENVIRONNEMENT D'UTILISATION DU PRODUIT

4.2.1 Hypothèses sur l'environnement physique

H.UT_SECU

Les UTL sont installées dans un local sécurisé à accès contrôlé. Seuls les personnels autorisés ont accès aux UTL (installateur/mainteneur & officiers de sécurité).

H.LECTEUR_SECU

Les lecteurs sont reliés aux UTL via une interface RS485 qui est considérée comme directe et non accessible facilement (câbles non exposés).

H.LAN_SUP_SECU

Les machines et le serveur SYRACUSE sont installés dans un local sécurisé à accès contrôlé. Seuls les exploitants, les officiers de sécurité et les installateurs/mainteneurs sont autorisés à accéder à ce local.

H.STATION_PERSO_SECU

La machine servant à la personnalisation des badges et à l'initialisation des UTL (mise à la clé) est située dans un local à accès contrôlé uniquement accessible aux officiers de sécurité et aux exploitants. Toutefois on peut imaginer d'avoir la base de données sur un pc portable et d'effectuer la mise en service sur l'UTL in situ. La base de données dans ce cas sera restreinte aux informations d'installations seules et administrée par un officier de sécurité.

4.2.2 Hypothèses sur les intervenants

H.OFF_CONFIANCE

Les officiers de sécurité sont formés à l'utilisation du système et sont considérés de confiance.

H.INST_CONFIANCE

Les installateurs et les mainteneurs sont formés à l'utilisation du système et sont considérés de confiance.

H.PORTEUR_SENSIBILISATION

Les porteurs de badges (les usagers) sont sensibilisés à l'utilisation de leur badge et des accès qu'il leur permet. En particulier, ils sont sensibilisés au fait de ne pas prêter, échanger leur badge ainsi que de ne pas divulguer leur code PIN lorsque l'installation en prévoit un en plus du badge individuel. Les porteurs sont censés prévenir les exploitants en cas de perte de leur badge.

H.EXPLOITANT_CONFIANCE

Les exploitants sont chargés de l'attribution ou de la définition des droits d'accès sur l'ensemble des portes et obstacles physiques contrôlés, ils sont supposés être compétents, formés et de confiance. Les exploitants ne se connectent jamais physiquement sur les coffrets (UTL).

4.2.3 Hypothèse sur l'environnement technique

H.INJECTION_CLE_SAM

L'injection des clés mères (B.K_MERE_COM_BADGE_UTL, B.K_BI-CLE_UTL_COM_UTL_SERVEUR et B.K AUTH SAM) nécessaires à la sécurité des communications entre lecteur/UTL et UTL/Serveur est faite dans un module de sécurité SAM AV2 de la société NXP, module intégré dans l'UTL. Ce module de sécurité hérite d'une certification Critères Communs EAL5+. La cérémonie d'injection de clés est réalisée par l'officier de sécurité ou pour plus de confiance par deux officiers de sécurité. La cérémonie de clés est assurée dans un local sécurisé. La clé B.K AUTH SAM est transférée chiffrée en AES 256 directement sur l'UTL via une liaison série. La carte SAM protège en intégrité et confidentialité les éléments stockés par elle.

H.INJECTION_DONNES DESFIRE EV1/EV2

Le badge DESFIRE EV1/EV2 protège en intégrité et confidentialité les éléments stockés par lui.

H.INJECTION_CLE SSCPV2

Le changement de la clé par défaut du protocole SSCPV2 dans les lecteurs est protégé en intégrité, confidentialité, authenticité par un badge SKB unique par site.

4.3 BIENS SENSIBLES

B.K_MERE_COM_BADGE_UTL

Il s'agit de la clé AES mère qui permet de générer des clés diversifiées utilisées dans les communications UTL / Badge. Cette clé est injectée dans la carte SAM par l'officier de sécurité à l'aide du logiciel de gestion des cartes SAM fourni par Elsylog ou celui en place dans l'entreprise.

B.K_DIVERSIFIEE_COM_BADGE_UTL

Il s'agit d'une clé qui permet d'authentifier un badge et de générer les clés de sessions nécessaires à la communication entre l'UTL et le badge. Cette clé propre au badge est initialisée à l'enrôlement d'un badge. Elle est stockée dans le badge uniquement. Il s'agit d'une clé dérivée de B.K_MERE_COM_BADGE_UTL

B.K_SESSION_COM_BADGE_UTL

Il s'agit des clés de session utilisées pour protéger les communications en mode transparent entre badge/UTL. Ces clés sont générées à partir de la clé diversifiée B.K_DIVERSIFIEE_COM_BADGE_UTL correspondant à un badge donné.

B.FICH_ID

Il s'agit du fichier contenant l'identifiant du badge.

B.PINCODE

Il s'agit du code d'accès à 4 chiffres de l'usager lorsqu'il le rentre sur le lecteur-clavier. Ce code est associé à l'identifiant pour valider une authentification de l'usager.

B.FIRMWARE

Il s'agit du firmware de l'UTL.

B.DROITS_PORTEURS

Il s'agit des droits d'accès d'un usager sur les dispositifs de contrôle d'accès de l'installation. Ces droits sont transmis et stockés dans l'UTL.

B.K_DEVERROUILLAGE_SAM_UTL_SESSION

Il s'agit de la clé utilisée pour chiffrer le secret qu'envoie l'UTL au serveur SYRACUSE à l'initialisation. Si le secret est correct, le serveur accepte d'envoyer la clé B.K_AUTH_SAM (de déverrouillage la carte SAM de l'UTL) chiffrée par cette clé de session.

B.K_AUTH_SAM

Il s'agit d'une clé AES128 d'authentification de la carte SAM. Cette clé permet de déverrouiller la carte SAM. Elle est saisie lorsqu'on initialise l'UTL et également stockée de manière sécurisée dans la base de données du serveur SYRACUSE. Elle est envoyée à l'UTL soit au moyen d'une liaison série à l'initialisation dans une salle sécurisée, soit par un officier de sécurité muni d'un PC portable connecté sur l'UTL une fois installée. Cette phase ne sera jamais accessible par réseau IP. Cette clé est utilisée pour autoriser la génération des clés publiques et privées de l'UTL.

B.K_BI-CLE_UTL COM_UTL_SERVER

Bi-clé générée après authentification dans la carte SAM. La partie publique est transférée chiffrée en AES-256 à la base de données.

B.K_BI-CLE_SERVER_COM_UTL_SERVER

Bi-clé du serveur pour les communications entre serveur et UTL. Une commande à partir du logiciel Syracuse (sur le serveur uniquement) permettra le calcul d'une nouvelle bi-clé. Une commande permettra sa diffusion vers les UTL.

B.K_SESSION_COM_UTL_SERVER

Clé de session AES256 calculée pour les communications entre UTL et serveur. Une commande à partir du logiciel Syracuse pourra à tout moment calculer une nouvelle clé de session et l'envoyer au travers du canal précédemment sécurisé. Sur acquittement de l'UTL, le chiffrement prendra cette nouvelle clé comme référence.

Le tableau ci-dessous présente les besoins de sécurité de chaque bien sensible

Bien sensible	Confidentialité	Disponibilité	Intégrité	Authenticité
B.K_MERE_COM_BADGE_UTL	X		X	X
B.K_DIVERSIFIEE_COM_ BADGE _UTL	X		X	X
B.K_SESSION_COM_BADGE_UTL	X		X	X
B.FICH_ID	X			
B.PINCODE	X			
B.FIRMWARE	X		X	X
B.DROITS_PORTEURS			X	
B.K_AUTH_SAM	X		X	X
B.K_DEVERROUILLAGE_SAM_UTL_SESSION	X		X	X
B.K_BI-CLE_UTL COM_UTL_SERVER	X		X	X
B.K_BI-CLE_SERVER_COM_UTL_SERVER	X		X	X
B.K_SESSION_COM_UTL_SERVER	X		X	X

4.4 MENACES

4.4.1 Profil des attaquants

Les attaquants potentiels peuvent mener des attaques logiques ou physiques sur les constituants de la ToE. Les attaquants ont un accès physique aux UTL rendu difficile de par le fait que les équipements sont en zone à accès contrôlé. Les attaquants peuvent être des usagers porteurs de badge ou des individus malveillants ne possédant pas de badge.

Pour les attaques logiques, on distingue les points d'accès suivants :

- Le réseau entre le Serveur et l'UTL
- La liaison RS485 entre une UTL et un lecteur de badges

- Le lecteur de badges

Les attaques physiques sont considérées sur les équipements suivants :

- Le lecteur de badges
- L'UTL

4.4.2 Liste des menaces

M.FIRMWARE_CORRUPT

Un attaquant tente de corrompre le firmware d'un UTL en utilisant soit une mise à jour malveillante fournie à l'insu d'un utilisateur autorisé soit en tentant de l'injecter lui-même.

M.INTERCEP_UTL_SERVEUR

Un attaquant tente d'intercepter les communications entre une UTL et le serveur afin de pouvoir compromettre, modifier, rejouer des communications. L'impact de cette menace peut être l'interception de biens sensibles (ex : code PIN) ou l'octroi de droits d'accès par modification/rejeu de commandes.

M.INTERCEP_LECT_UTL

Un attaquant tente d'intercepter les communications entre un lecteur et un UTL afin de pouvoir compromettre, modifier, rejouer des communication. L'impact de cette menace peut être l'interception de biens sensibles (ex : code PIN) ou l'octroi de droits d'accès par modification/rejeu de commandes.

M.PHYS_LECTEUR

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but de modifier le comportement des lecteurs de badges. L'attaquant peut tenter d'ouvrir ou de substituer le lecteur.

M.PHYS_UTL

Cette menace couvre les attaques physiques pouvant être menées par un attaquant dans le but de modifier le comportement des UTL. L'attaquant peut tenter d'ouvrir ou de substituer l'UTL.
Il peut tenter d'isoler une UTL pour empêcher la remonté d'évènements.

5 FONCTIONS DE SECURITE

F_PROTECT_COM_RS485

La protection des communications entre le lecteur et l'UTL est assurée selon la norme ISO 14443-A-B . La norme met en œuvre un protocole de sécurité qui s'appuie sur :

- Une phase d'authentification mutuelle utilisant les clés diversifiées (B.K_DIVERSIFIEE_COM_BADGE_UTL)
- La génération d'une clé de session AES 128 bits qui protège alors les communications (B.K_SESSION_COM_BADGE_UTL).

La protection des communications en dehors de l'authentification mutuelle et du chiffrement, inclus également une protection contre le rejeu et assure la gestion de l'intégrité des données dans les phases de lecture/écriture , essentiel dans un mécanisme de contrôle d'accès physique. Le détail des mécanismes cryptographiques mis en œuvre est fourni dans le document de spécifications cryptographiques [CRYPTO].
Pour rappel la clé mère B.K_MERE_COM_BADGE_UTL permettant de générer les clés diversifiées B.K_DIVERSIFIEE_COM_BADGE_UTL est protégée par un module SAM AV2 de la société NXP. Ce module de sécurité hérite d'une certification critères commun EAL5+. La clé est injectée dans la carte SAM par l'officier de sécurité à l'aide du logiciel de gestion des cartes SAM fourni par Elsylog ou celui en place dans l'entreprise.

F_PROTECT & AUTHENCOM_UTL_SERVEUR

La protection des communications entre l'UTL et le serveur SYRACUSE est assurée par un protocole établissant un canal sécurisé entre l'UTL et le Serveur SYRACUSE.

Ce protocole se base sur les bi-clés des deux équipements (B.K_BI-CLE_UTL_COM_UTL_SERVER et B.K_BI-CLE_SERVEUR_COM_UTL_SERVER) Il permet la réalisation d'une authentification mutuelle et le chiffrement d'aléas, générés de part et d'autres, servant à la création d'une clé de session

B.K_SESSION_COM_UTL_SERVER. La construction de celle-ci (voir document de cryptographie) démarrera le chiffrement des échanges sécurisés.

Pour rappel le bi-clé B.K_BI-CLE_UTL_COM_UTL_SERVER est protégé par un module SAM AV2 de la société NXP. Ce module de sécurité hérite d'une certification Critères Communs EAL5+. La clé est injectée dans le SAM à l'initialisation de l'UTL.

Le protocole assure l'authentification mutuelle, l'échange de clés de session ainsi que l'intégrité des communications. Concernant la protection contre le rejeu un mécanisme propriétaire est mis en œuvre associant un champ aléatoire aux commandes passées. Le générateur d'aléa est identifié dans le document de spécifications cryptographiques de SYRACUSE [CRYPTO] .

F_PROTECT_CODE PIN

Lorsque le code PIN est saisi par le porteur de badge sur le lecteur, le code PIN est envoyé chiffré à l'UTL via le protocole SSCPv2. La comparaison du code saisie sur le lecteur est faite dans l'UTL et ne remonte pas vers le serveur. Sauf dans un cas, si le porteur du badge fait son changement de code PIN à partir du lecteur de badge muni d'un clavier. Dans ce cas il est envoyé au serveur via le canal sécurisé de la fonction F_PROTECT&AUTHEN_COM_UTL_SERVEUR.Le code pin est stocké chiffré dans l'UTL et la base données côté serveur.

F_PROTECT_UTL

L'UTL dispose d'une fonction de détection d'ouverture sous la forme d'un contact sec qui remonte une alarme vers le serveur SYRACUSE en cas de détection d'effraction ou d'arrachement. Ne recevant plus de trame en vie, la perte de dialogue est quant à lui signalé par le logiciel d'exploitation.Le passage sur alimentation secourue (batterie) est remonté vers le serveur ainsi que « Batterie basse » lorsque celle-ci arrive au seuil critique. En cas de coupure complète les informations sont sauvegardées plusieurs jours, permettant ainsi un redémarrage et la reprise immédiate de la sécurisation de l'accès.

F_PROTECT_LECTEUR

Les lecteurs de badges disposent d'un mécanisme de détection d'ouverture et d'un mécanisme de détection d'arrachement. En cas de détection, une alarme est remontée au niveau du SERVEUR SYRACUSE.

F_PROTECT_FIRMWARE

Les fichiers de mise à jour firmware sont protégés en confidentialité par du chiffrement AES 256 , en intégrité par une empreinte numérique et en authenticité par une signature numérique. Le fichier de mise à jour contient une clé maitre. Reçue par l'UTL elles sera ensuite dérivée pour obtenir la clé de déchiffrement. L'authenticité réside sur la connaissance de l'algorithme de dérivation et la signature numérique. La reprogrammation ne sera possible qu'une fois les vérifications effectuées et correctes.

Le tableau ci-dessous présente la couverture des menaces par les fonctions de sécurité

	M.FIRMWARE_CORRUPT	M.INTERCEP_UTL_SERVEUR	M.INTERCEP_LECT_UTL	M.PHYS_LECTEUR	M.PHYS_UTL
F_PROTECT_COM_RS485			X		
F_PROTECT_ & AUTHENCOM_UTL_SERVEUR	X				
F_PROTECT_CODE PIN		X	X		
F_PROTECT_UTL					X
F_PROTECT_LECTEUR				X	
F_PROTECT_FIRMWARE	X				