AUTORITÉ DES MARCHÉS FINANCIERS

ANNEXE 1

DEFINITION DE L'EXISTANT - ARCHITECTURE DE SECURITE

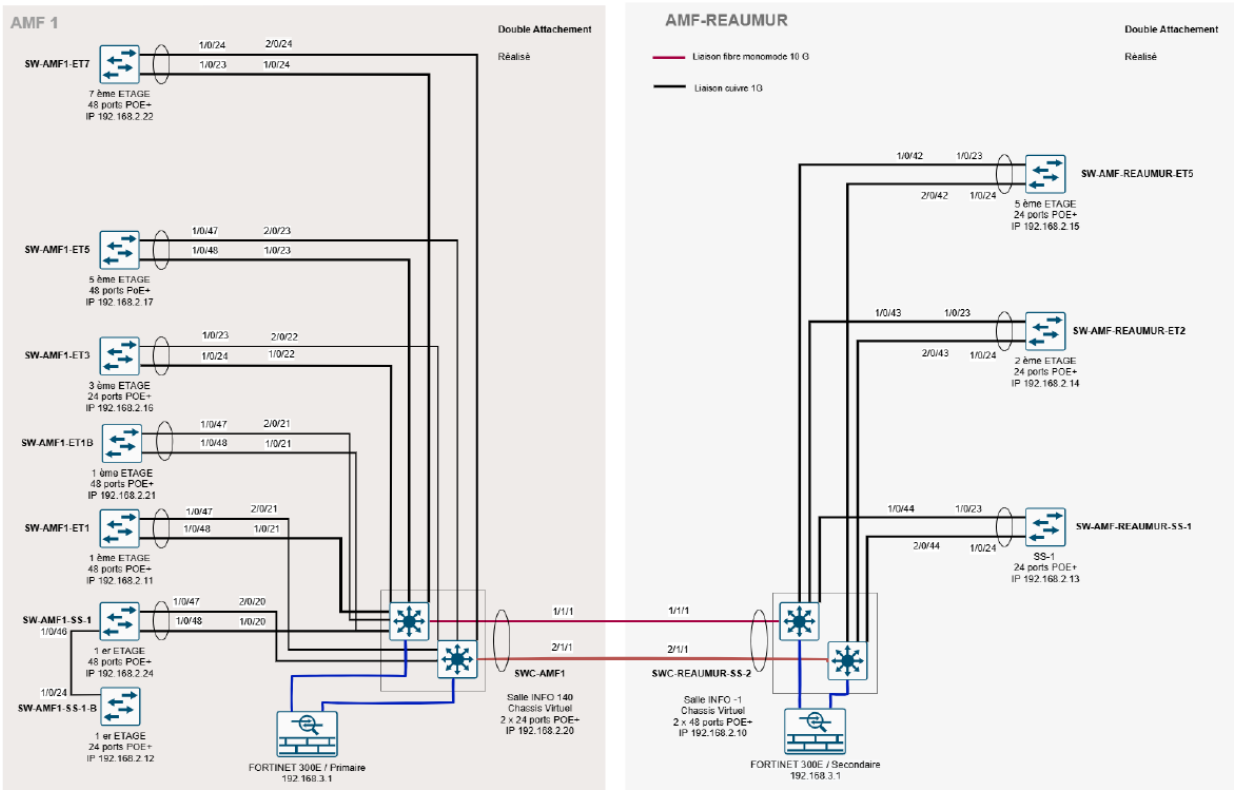
L'AMF dispose d'une documentation à jour. Elle est notamment constituée :

- Des DOE câblage sureté pour ses deux bâtiments ;
- Des schémas d'architecture physique ou logique ;
- D'une politique de sauvegarde ;
- D'un plan de reprise et de continuité ;

Le Titulaire, au titre de la maintenance forfaitaire, devra la maintenir à jour. L'AMF donnera les accès à cette documentation qui ne doit pas sortir du SI de l'AMF.

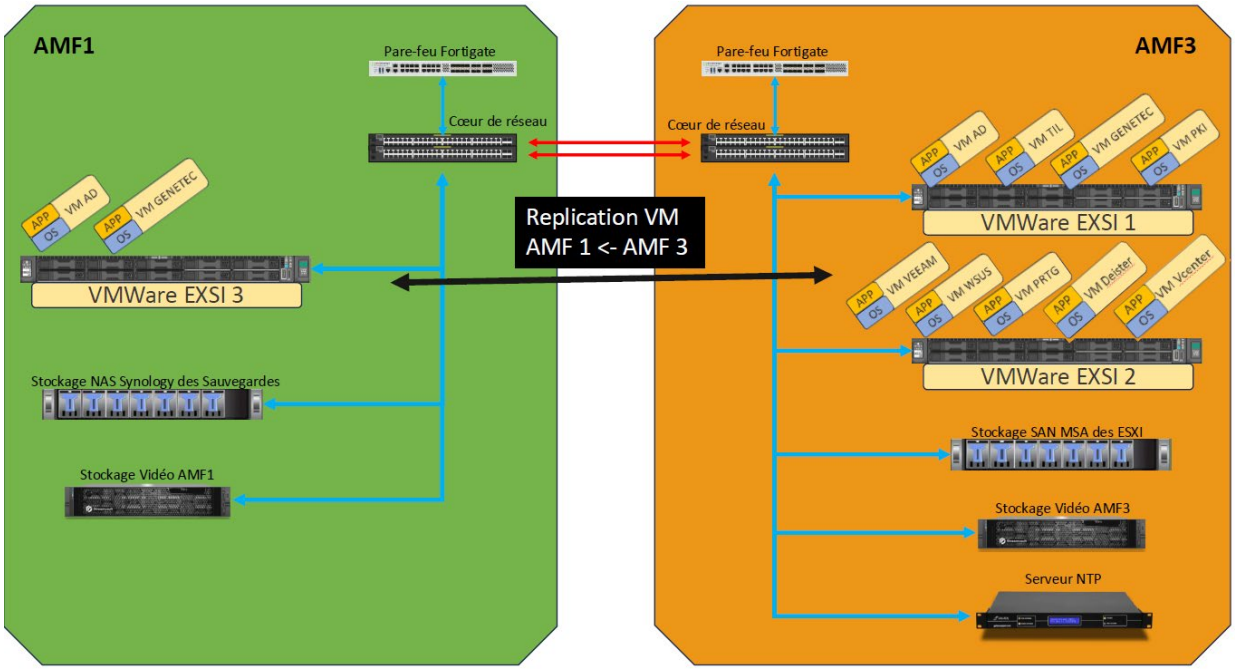
1.1. SYNOPTIQUE GENERAL

L'architecture est de haute disponibilité et est basée sur des redondances matérielles et des mécanismes de bascules logicielles (VMware). L'architecture physique est décrite dans le schéma ci-dessous :



L'ensemble des composants de cette architecture sont décrits dans les deux schémas ci-dessous et dans le fichier CMDB (annexe 2)

Infrastructures



Le système de contrôle d'accès et détection d'intrusion est de marque TIL Technologies, type Micro-Sésame avec base de données SQL Server.

Le système de vidéosurveillance est de marque GENETEC, type OMNICAST.

1.2. EXPLOITATION DU SYSTEME DE SURETE

L'exploitation des installations est réalisée sur des postes informatiques dédiés à la Sûreté :

- ☐ Postes informatiques dédiés à l'exploitation d'AMF1.
- ☐ Postes informatiques dédiés à l'exploitation d'AMF3.

Les fonctions d'administration sont assurées sur deux postes dédiés à l'administration.

Les fonctions de gestion et d'attribution des droits et des profils de badges sont assurées sur le poste dédié au PC Sécurité d'AMF1, pourvu d'un lecteur enrôleur et d'une imprimante de personnalisation de badges. Le poste d'administration AMF situé dans le bureau du cadre Sûreté (RdC AMF1).

Les fonctions d'exploitation temps réel sont réalisées sur des postes informatiques dédiés à la Sûreté (contrôle d'accès et vidéosurveillance) au PC AMF1 et au PC AMF3.

Le PC AMF1 reçoit la totalité des informations (AMF1 et AMF3), le PC AMF3 reçoit aussi la totalité des informations (AMF3 et AMF1).

Les informations remontées ne sont pas filtrées. Tout événement est remonté à l'exploitation (exemple : badge valide, badge invalide, porte maintenue ouverte, porte forcée, etc.).

La gestion des visiteurs est réalisée par les hôtesses d'accueil des bâtiments AMF1 au moyen de badges spécifiques.

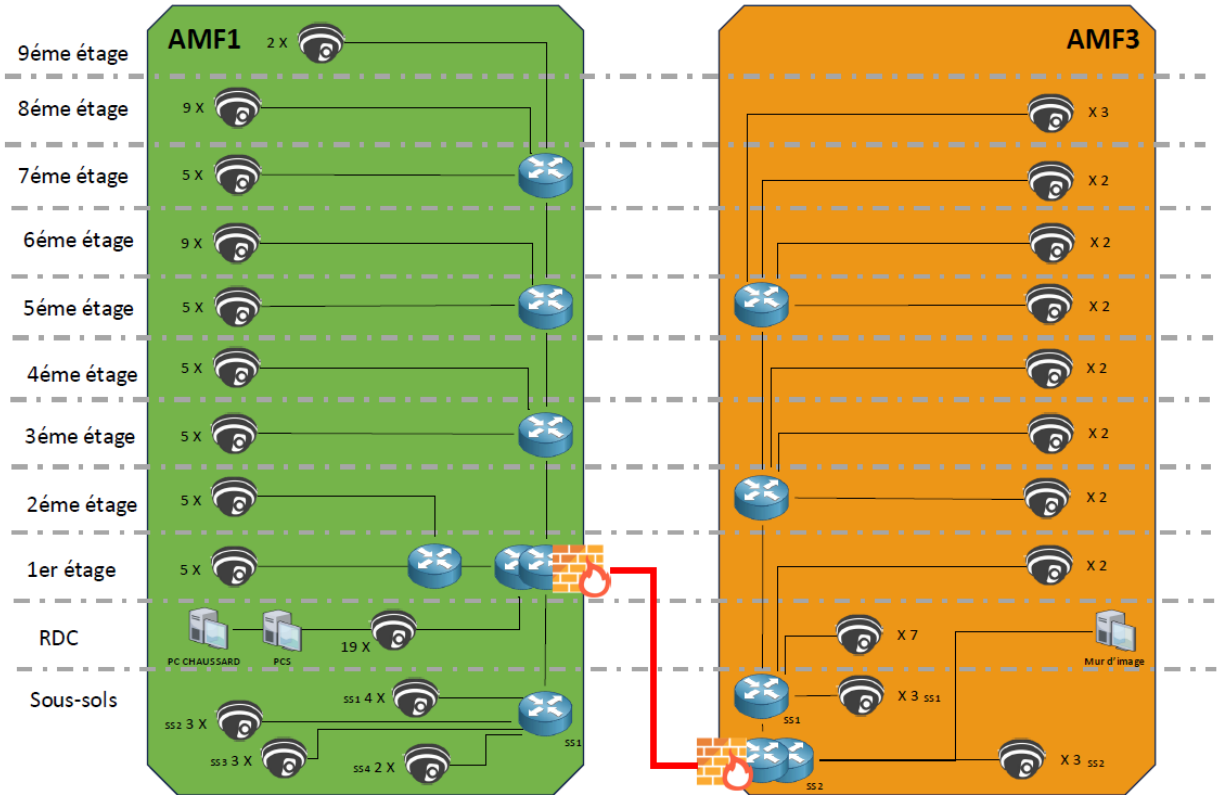
La délivrance d'un badge visiteur est réalisée sur présentation d'une pièce d'identité par le visiteur. Le badge est restitué en sortie.

La supervision technique des composants est réalisée par la solution Paessler PRTG, qui interroge des métriques et reçoit des alertes via le protocole SNMPv3.

1.3. SYSTEME DE VIDEO SURVEILLANCE

Quantitatif existant

Voir fichier CMDB (annexe 2)



Architecture technique

Les caméras numériques d'AMF1 et d'AMF3 sont reliées aux switches de chaque étage. Les flux vidéo sont acheminés à l'hébergeur secondaire et son espace de stockage.

Le VMS utilisé est Genetec Security Center.

Caméras et encodage

Les sites bénéficient d'un total de 115 caméras numériques.

Sur AMF1 et AMF3, les flux sont directement en MPEG4.

Les caméras sont redondées vers les serveurs de secours via des licences « failover caméra connexion ».

Enregistrement

Une fois les flux encodés au format Mpeg4, les fonctions d'enregistrement et de visualisation sont réalisées au travers du logiciel OMNICAST

L'enregistrement se déclenche sur alarme via la vidéo-détection ou via le dispositif de détection d'intrusion à proximité.

Les images enregistrées sur chaque site sont dupliquées et enregistrées sur l'autre site. Concrètement chaque site dispose d'un espace de stockage

1.4. SYSTEME DE CONTROLE D'ACCES ET DETECTION D'INTRUSION

Quantitatif existant

Voir fichier CMDB (annexe 2)

Système

Le système de contrôle d'accès et de détection d'intrusion est de marque TIL Technologies, type Micro-Sésame sous base de données SQL Server.

Ce système est susceptible de migration vers la solution Genetec Security Center.

Ce système permet la supervision globale des accès contrôlés sur AMF1 et AMF3, en termes de :

- Gestion sécurisée des personnes (fabrication de badges d'accès, gestion des données relatives aux personnes en lien avec le lieu, les horaires, le niveau hiérarchique, etc..) ;
- Gestion des identifiants pour les personnes ;
- Gestion sécurisée du bâtiment (centralisation des alarmes intrusion liées au contrôle d'accès, programmation d'automatismes, commandes à distance activées par des programmes horaires, des événements, des décisions d'opérateurs).

Les UTL sont raccordées directement sur le réseau Ethernet. Sur ce réseau sont raccordés le serveur, et les postes clients.

Unités de Traitement Local (UTL)

Voir fichier CMDB (annexe 2)

Module d'extension

Voir fichier CMDB (annexe 2)

Lecteur de badges

Le système de contrôle d'accès implémente le modèle de configuration n°1 préconisé par l'ANSSI (cf. R41 de https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection) c'est-à-dire que tous les flux sont chiffrés au moyens d'algorithmes et protocoles cryptographiques robustes, et que les lecteurs de badge sont en fonctionnement « transparents » : il ne contiennent aucun secret cryptographique, ces derniers étant uniquement stockés dans les UTL.

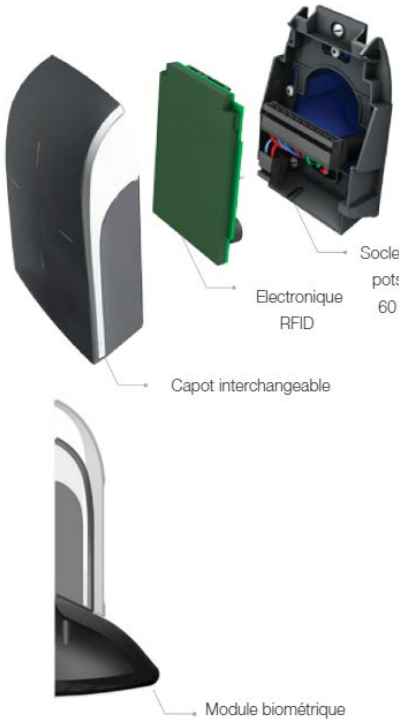
Les lecteurs de badge sont tous des STiD Evolution, au format « standard », sans clavier :

Voir fichier CMDB (annexe 2)

ANNEXE 1

LECTEURS EVOLUTION

Montage et Modularité



Caractéristiques détaillées

- Alimentation : 12 VDC
- Consommation moyenne : 100 mA
- Fréquence d'émission : 13.56 MHz - ISO14443 A & B, ISO18092 (NFC). *Gamme Bluetooth : voir fiche spécifique*
- Distance max. entre le module et le lecteur : 100 m (Wiegand/Dataclok), 600m en RS485, et 300m en RS485 crypté
- Interface de communication : Data/clock ISO2, Wiegand, RS485, RS485 crypté AES128
- Connectique : Bornier débrochable 10 points (5mm)
- Protection : Détection de l'arrachement par accéléromètre + possibilité d'effacement des clefs
- Dimensions :
  - » 111 x 42 x 22 mm (lecteur étroit pour montants de portes)
  - » 107 x 80 x 26 mm (lecteur standard et lecteur-clavier à touches)
  - » 128 x 80 x 31 mm (lecteur-afficheur couleur)
- Fixation : Murale en applique ou sur pots électriques entre-axes 60 et 62 mm (sauf lécteur étroit). Sur tout type de support y compris métal, sans entretoise
- Distance de lecture : Entre 4 et 8 cm selon technologie de badge et forme du lecteur
- Signalisation paramétrable :
  - » 2 LEDs RVB - 360 couleurs
  - » Buzzer intégré (pilotable avec automates NG / V3 uniquement)
- Matériaux :
  - » ABS-PC UL-V0 (noir)
  - » ASA-PC-UL-V0 UV (blanc)
- Résistance / étanchéité : IK10, IP65 (hors connectique)
- Température de fonctionnement :
  - - 20°C à + 70°C (lecteur simple et clavier à touches)
  - - 10°C à + 60°C (lecteur avec afficheur)
  - - 10°C à + 50°C (lecteur avec capteur biométrique)
- Poids : 0,150 à 0,250 kg selon modèles (hors capteur biométrique)

Programmation de la lecture sécurisée

- Si le client utilisateur ne souhaite pas gérer les clés de cryptage nécessaires à la lecture sécurisée des badges, il recevra des lecteurs déjà programmés par TIL.
- Si le client souhaite maîtriser ses clés de cryptage, il devra acheter un kit de programmation qui lui permettra d'encoder ses badges et de configurer ses lecteurs. TIL livrera des lecteurs non programmés.

Compatibilités identifiants 13,56MHz

- ISO14443 A & B, ISO18092 (NFC)
- MIFARE® Ultralight & Ultralight C, MIFARE Classic, MIFARE Plus, MIFARE DESFire EV1 & EV2 émulé V1, NFC, SMART MX, CPS3, Moneo, iCLASS, PicoPass

Badge d'identification

L'AMF dispose d'un badge d'identification multiservice qui permet :

- Le contrôle des accès ;
- L'accès aux copieurs multifonctions ;
- L'utilisation de solde de paiement sur les machines à café (terminal de lecture Nayax GTI).

La technologie d'identification est de type « proximité », technologie passive (pas d'alimentation embarquée), la puce étant alimentée lorsqu'elle est placée dans un champ sur la porteuse 13,56 MHz (distance de lecture 5 cm). La technologie DESFire EV2 est utilisée de façon exclusive dans l'infrastructure de contrôle d'accès.

Un secteur est affecté au contrôle d'accès et l'AMF est propriétaire de ses clés d'accès aux secteurs.

L'AMF dispose d'une population de :

- 1 500 badges actifs avec fiches profils et autorisations d'accès suivant les habilitations ;
- Population de badges permanents : l'attribution est nominative et les autorisations d'accès sont attribuées en fonction de profil type hiérarchisés et du rôle et fonction de chacun ;
- Population de badges titulaires : un badge provisoire est affecté suivant les devoirs et attentes du titulaire avec des droits d'accès définis ;
- Population de badges visiteurs : un badge éphémère est affecté auprès de l'accueil avec des droits d'accès réduits au besoin du personnel visité.

Détection d'intrusion

Des détecteurs volumétriques ont été déployés dans les circulations généralement à proximité des caméras ainsi que dans les locaux sensibles, avec un asservissement au contrôle d'accès.

La mise en route de la détection d'intrusion est réalisée sur des plages horaires

En cas d'alarme, des diffuseurs sonores sont activés.

Voir fichier CMDB (annexe 2)

Dispositifs de verrouillage et de contrôle des issues de secours

Toute issue de secours est asservie au Système de Sécurité Incendie et automatiquement déverrouillée sur alarme incendie.

La typologie de l'issue de secours peut également prévoir une ouverture par lecteur de badge en sortie voire en entrée/sortie.

Deux typologies de verrouillage des issues de secours sont déployées sur le site :

- Verrouillage via barre antipanique motorisée,
- Verrouillage via verrou électromagnétique ou ventouse.

Voir fichier CMDB (annexe 2)

1.5. SYSTEME DE RADIOCOMMUNICATION MOBILE PTI

L'AMF dispose d'un système de radiocommunication mobile avec fonction PTI (marque MOTOROLA).

L'installation comprend :

- 1 base radio sur chacun des PCS (DM 4600e) ;
- 1 relais numérique (SLR1000) avec antenne sur AMF1 ;
- 1 relais numérique (SLR1000) avec antenne sur AMF3 ;
- 1 coffret télé transmetteur alarme PTI sur AMF3 ;
- 15 portatif UHF / PTI avec écran/clavier (DP3661e) dont 4 avec fonctionnalité GSM).

1.6. SYSTEME D'INTERPHONIE DE SURETE

AMF1 et AMF3 disposent de systèmes d'interphonie de la marque CASTEL (sur AMF1, chaque pallier d'étage dispose d'un système d'interphonie).

Le dispositif est complété par une installation de vidéophonie (1 vidéo portier à l'entrée visiteur pour AMF1 et un pour AMF3, 1 en entrée parking AMF1).

1.7. RESEAU SURETE

Les installations de Sûreté bénéficient d'un réseau dédié au protocole TCP/IP permettant la communication entre les équipements centraux (serveurs / UTL / postes d'exploitation dédiés Sûreté). La liaison réseau inter-bâtiments est assurée par une fibre optique dédiée constituée de 2 câbles de 12 brins en monomode. Sur chaque câble, 2 brins sont dédiés à la Sûreté et 8 autres brins sont utilisés pour le transport Data, voix, etc.

Le schéma ci-dessous décrit le réseau Sûreté :

