

**Institut Universitaire de Technologie,
Aix-Marseille Université**

**RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité**

Projet IOT et Hypervision

Ethan LASSELLE

DELTA SERTEC

Responsable entreprise : Marc Martinez

Responsable académique : Eric Wurbel

2024

Table des matières

1	Introduction.....	5
2	Présentation de l'entreprise.....	6
2.1	Présentation générale	6
2.2	Son offre.....	6
2.3	Son organisation	7
2.3.1	Direction.....	7
2.3.2	Equipe Commerciale.....	8
2.3.3	Administration	8
2.3.4	Equipe Technique	8
3	Projet IOT	9
3.1	Contexte	9
3.2	LoRaWAN	10
3.3	Maquette et Tests.....	10
3.3.1	Configuration de la Passerelle	10
3.3.2	Configuration des capteurs.....	12
3.3.3	Configuration de Kheiron.....	13
3.3.4	Tests	13
3.4	Déploiement de la solution	15
4	Prysm.....	17
4.1	Hypervision	17
4.1.1	Caractéristiques.....	17
4.1.2	Avantages	18
4.1.3	Applications.....	18
4.2	Présentation Générale	18
4.2.1	Fonctions et Capacités	19
4.2.2	Avantages	19
4.3	Formation.....	20
4.4	Missions	23
5	Conclusion	25
6	Glossaire	29
7	Sitographie	31

1 Introduction

Delta Sertec est une entreprise de sécurisation des bâtiments par le biais de systèmes électroniques dit de « courants faibles ». L'entreprise conçoit, réalise et maintient des systèmes de sécurité électroniques et réseau de communication. Ils interviennent aussi bien sur les nouveaux chantiers que sur les chantiers déjà en activité.

Créé depuis environ un an et demi, le service d'hypervision et développement conçoit des applications graphiques pour que chaque système puisse remonter vers l'utilisateur et qu'il puisse gérer sa sécurité installée de la manière la plus simple possible. Ce service effectue aussi de l'implémentation de nouveaux systèmes comme de l'internet des objets.

Mes missions durant ce stage ont été :

- Mise en place d'un projet IOT
- Formation sur le logiciel d'intégration de solutions PRYSM
- Soutien sur des projets d'hypervision

Je commencerai ce rapport par la présentation de l'entreprise, son offre et des organigrammes de ses équipes. Je continuerai par le développement du projet IOT que j'ai mené puis de ma formation sur le logiciel PRYSM ainsi que de mes missions sur des projets en cours avec ce dernier. Enfin je conclurai.

2 Présentation de l'entreprise

2.1 Présentation générale

DELTA SERTEC est une entreprise experte dans les technologies dites « courant faibles » qui regroupe différentes briques technologiques. L'entreprise détient une équipe de techniciens qualifiés et détenant de multiples compétences répondant aux briques technologiques de l'entreprise et du marché de l'électricité.

Fondée en 1979 par Jean-Louis BROUQUIER, l'entreprise familiale est aujourd'hui dirigée par Arnaud BROUQUIER



PDG : Arnaud BROUQUIER

En plus de 40 ans, DELTA SERTEC est devenue une référence du marché du « courant faible » et est un des leaders de la sécurisation et la connectivité des bâtiments. DELTA SERTEC, est une PME de plus de 50 salariés.

DELTA SERTEC, est une entreprise à orientation de la responsabilité sociétale des entreprises fortes. La RSE se définit comme la prise en compte par les entreprises, sur une base volontaire, et parfois juridique, des enjeux environnementaux et du développement durable. DELTA SERTEC est une filiale de DELTA SMART TECHNOLOGIE, tout comme DELTA PHARMA et DELTA TELECOM.

2.2 Son offre

DELTA SERTEC propose des offres globales sur les 4 piliers de son offre. Cela permet une meilleure flexibilité sur les problématiques rencontrés et projet dans leurs globalités, tout en étant un interlocuteur unique de leurs clients. DELTA SERTEC met également en place des architectures de sûreté éprouvées, répondant au besoin en matière de contrôle d'accès, de vidéosurveillance, de systèmes anti-intrusion, de sonorisation et de détection anti-incendie. De l'étude de site à la maintenance préventive et curative en passant par la conception et le déploiement, DELTA SERTEC est un partenaire unique pour tous les projets de réseau en courant faible.

Après l'étude complète de la demande du client via un cahier des charges si le projet est déjà bien rodé ou via le site internet en cas de réflexion nouvelle DELTA SERTEC proposera une offre sur mesure. L'entreprise vient réaliser des chantiers dans deux secteurs distincts, le premier pour ce qui concerne l'habitat (collectivité, habitat et bâtiments etc.) et le second pour la partie tertiaire (chantier pour de grands groupes, EHPAD, hôtellerie etc.).

Voici les 4 piliers technologiques DELTA SERTEC :

-CABLAGES ET EQUIPEMENT NUMERIQUE DE BATIMENTS :

Étant la brique la plus historique de 40 ans savoir-faire. DELTA SERTEC propose d'installer des systèmes d'interphonie et de télévision collective. À la suite du développement de nouvelles techniques, l'entreprise installe tout ce qui concerne : réseaux informatiques filaires, Wi-Fi, ponts

radio, capteurs IoT (Internet of Things), IRVE (Infrastructures de Recharge pour Véhicules Électriques), supervision technique....

-SURETE DES LOCAUX ET DES PERSONNES :

La sécurisation des biens et des personnes est primordiale aujourd'hui. DELTA SERTEC recherche les solutions les plus adaptées aux besoins des clients et aux enjeux de ces derniers. L'entreprise adresse toutes les composantes de la sûreté et sécurité électronique : Contrôle d'accès, vidéoprotection, alarme anti-intrusion, système de sécurité incendie.

-DIGITALISATION DES ESPACES :

La liaison entre l'informatique, la télécoms et de l'électronique permet de toutes nouvelles perspectives. Les nouveaux outils digitaux permettent d'apporter simplicité et « éco-responsabilité », en limitant notamment les déplacements superflus. Plusieurs outils collaboratifs font partie de l'usage quotidien : Ecrans d'affichage dynamique, IPTV (Internet Protocol Television), salle de réunion digitale, visioconférence, sonorisation.

L'entreprise propose de multitude de solutions télécoms allant des accès Internet et abonnement téléphoniques : Téléphonie fixe et mobile, abonnements Internet, Fibre Haut-Débit, Communications unifiées

Le Service Technique de Maintenance :

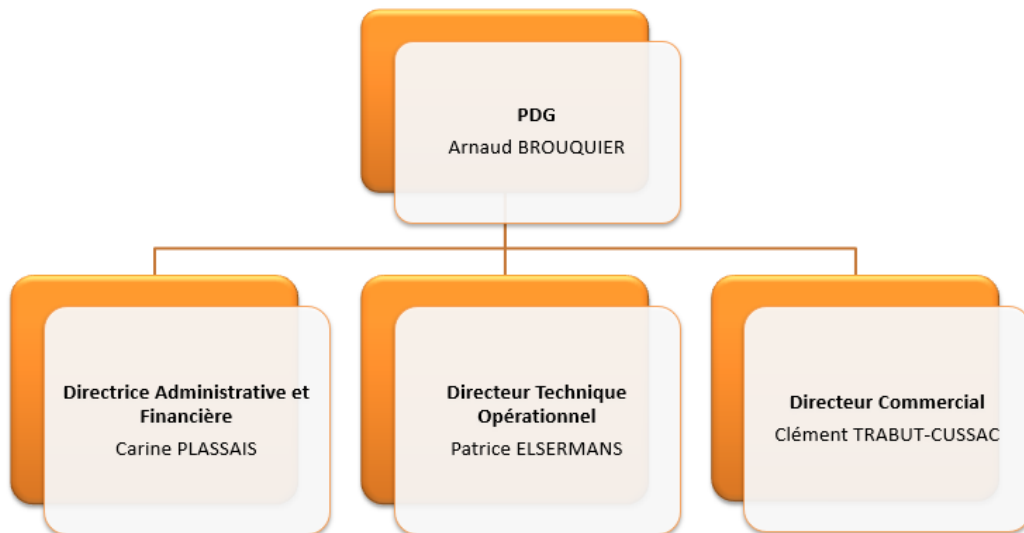
DELTA SERTEC propose également un service de maintenance pour la partie tertiaire et habitat. Selon son contrat, le client bénéficie d'un service après-vente en cas de panne ou de maintenance nécessaire. L'entreprise interviendra selon des degrés différents. Cela peut être une platine qui ne fonctionne plus correctement dans un habitat, l'entreprise étudiera le problème rencontré par le client afin de lui proposer la meilleure offre possible. L'entreprise va alors déployer des techniciens qui viendront remplacer ou réparer le matériel.

2.3 Son organisation



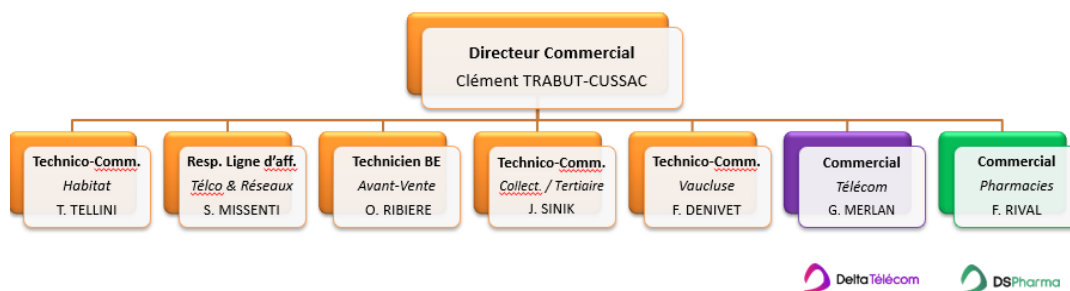
Structure du groupe Smart Technologies

2.3.1 Direction



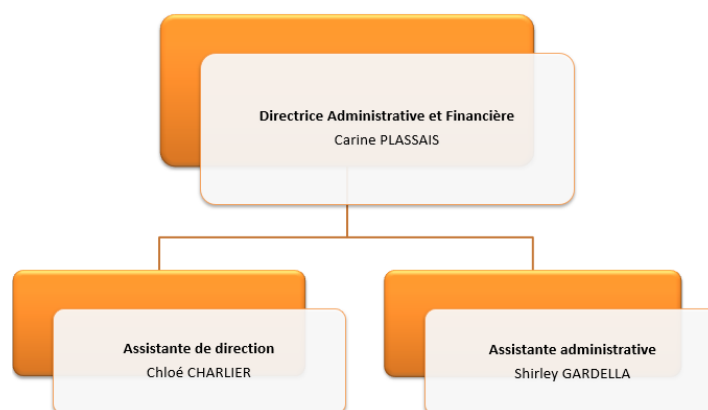
Organigramme de la Direction de Deltac Sertec

2.3.2 Equipe Commerciale



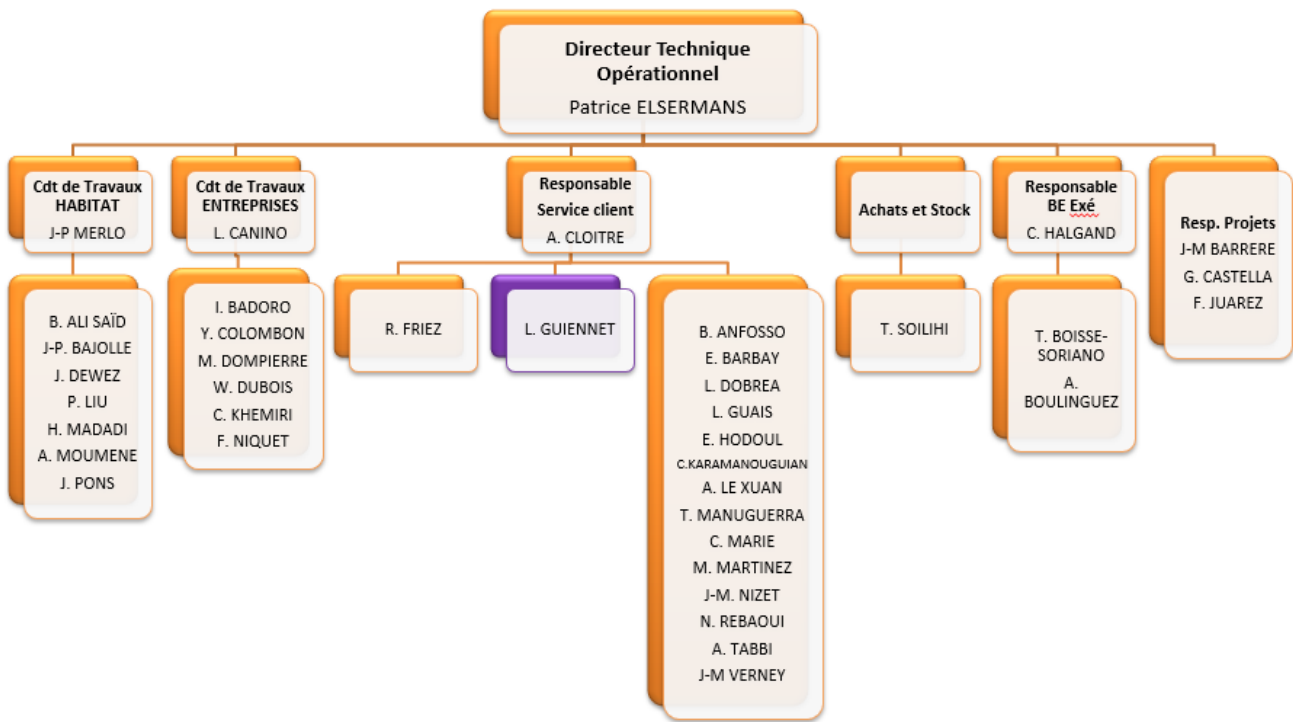
Organigramme de l'équipe commerciale

2.3.3 Administration



Organigramme de l'Administration

2.3.4 Equipe Technique



Organigramme de l'équipe technique

3 Projet IOT

3.1 Contexte

Ce projet est une réponse à un appel d'offre d'un bailleur social pour la mise en place de poteaux de vidéosurveillance dans la résidence du Charrel à Aubagne.

Le client souhaitait sécuriser la résidence via l'installation de 12 mâts de vidéosurveillance répartis dans le quartier.

Chaque mât est composé de plusieurs caméras de différents types comme les caméras dômes, les caméras fictives et caméras de surveillance IP (Internet Protocol). Les caméras fictives sont des caméras non-alimentées servant à dissuader de potentiels vols ou infractions.

Chaque mât est relié à un lampadaire qui n'est alimenté que la nuit. Le jour, les mâts fonctionnent sur batteries.



Plan de déploiement des mâts et de la passerelle

Il y a, sur chacun, un capteur Wattecoo Tout ou rien Sens'O LoRaWAN servant à vérifier l'alimentation du mât mais aussi sur le relais lora et la passerelle donc il y a 14 capteurs en tout. Les capteurs possèdent trois entrées mais seulement deux seront utilisées pour ce projet. Elles seront reliées à un contacteur de part et d'autre d'un disjoncteur. En fonction de la localisation du problème d'alimentation, ce système permet de remonter une alarme qui engendrera une intervention soit du distributeur d'électricité si cette dernière est située avant le disjoncteur, soit de Delta Sertec.

Les capteurs auront un lien LoRaWAN avec une passerelle UG67 de la marque Milesight. La passerelle recevra les trames des capteurs et les renverra vers la plateforme Kheiron qui permet une supervision du site. La plateforme traitera les trames et enverra des mails d'alertes sur l'adresse mail du client.

Tout le matériel et la solution ont été définis par le client et les commerciaux dans le cahier des charges du projet.

3.2 LoRaWAN

Avant de décrire mon travail sur ce projet, je vais définir ce qu'est le LoraWAN.

LoRaWAN (Long Range Wide Area Network) est un protocole de communication pour les réseaux de capteurs sans fil de basse puissance. Il est conçu pour permettre la communication à longue portée avec une consommation d'énergie minimale, ce qui le rend idéal pour les applications de l'Internet des objets (IoT). Voici les principales caractéristiques et concepts liés à LoRaWAN :

Longue portée :

- Permet la communication sur des distances de plusieurs kilomètres en milieu rural et jusqu'à quelques kilomètres en milieu urbain.

Faible consommation d'énergie :

- Conçu pour que les dispositifs IoT puissent fonctionner sur des batteries pendant plusieurs années.

Topologie en étoile :

- Les capteurs ou dispositifs IoT (nœuds) communiquent directement avec des passerelles (gateways), qui relaient les messages vers un serveur réseau.

Adaptation au débit de données :

- Peut ajuster dynamiquement le débit de données en fonction de la qualité du signal et de la distance entre le nœud et la passerelle.

3.3 Maquette et Tests

Avant de déployer la solution des capteurs et de la communication, avec mon binôme Clément Marie, nous avons monté une maquette du projet.

J'ai commencé à configurer la passerelle.

3.3.1 Configuration de la Passerelle

Avant de se connecter à la passerelle, j'ai relié mon ordinateur portable au port rj45 de l'adaptateur de cette dernière. Il est composé de deux port rj45, l'un servant pour les données et l'autre pour l'alimentation PoE (Power over Ethernet).

Pour pouvoir avoir la transmission de données vers la plateforme Kheiron hébergée sur internet, il faut que la passerelle ait une connexion. Pour se faire, j'ai pu obtenir une carte SIM (subscriber identity/identification module) que j'ai inséré dans le port adéquat.

J'ai ensuite modifié mes paramètres de connexion réseau car la passerelle utilise l'adresse 192.168.23.150 avec le masque 255.255.255.0. Je me suis donc mis dans le même réseau avec l'adresse 192.168.23.10 avec le même masque.

La passerelle UG67 possède un interface web préconfigurée pour pouvoir la paramétrer depuis un navigateur.

J'ai ouvert un navigateur et j'ai rentré dans la barre de recherche <https://192.168.23.150>. Je me suis connecté grâce à la page de connexion.

J'ai débuté le paramétrage de la partie carte SIM. Je suis allé dans le menu Network/Interface puis dans l'onglet Cellular (cellulaire). J'ai rempli les champs APN (Access Point Name) avec les informations données par le constructeur de la carte, le nom d'utilisateur avec le mot de passe défini par Delta Sertec ainsi que le code PIN.

Pour pouvoir transmettre les informations à Kheiron, j'ai dû créer le lien avec la plateforme. Pour se faire, je suis allé dans le menu Network Server dans l'onglet Applications. J'ai pu mettre en place le type de transmission de données vers la plateforme. Il s'agit de MQTT (Message Queuing Telemetry Transport) qui est un protocole de messagerie largement utilisé dans le domaine de l'internet des objets.

Pour faire fonctionner le lien, j'ai dû remplir les champs du broker qui est un lien vers un serveur distant qui m'a été mis à disposition par le prestataire Kheiron, son port, son identifiant client. La connexion se fait grâce à une identification grâce à un mot de passe et un nom d'utilisateur.

La sécurisation est prise en charge par un échange de certificats TLS (Transport Layer Security) autosignés.

Pour que les données soient bien traitées par le serveur, j'ai dû remplir les Topic (sujets) Uplink (lien montant) et Downlink (lien descendant). Les topics permettent de catégoriser et d'organiser les messages pour que les clients puissent s'abonner aux catégories d'informations qui les intéressent.

Je dois maintenant paramétrer le type de capteur qui enverra les données. Je vais donc dans l'onglet Profiles. Les capteurs sont de type Classe A OTAA (Over-The-Air Activation) c'est-à-dire qu'il s'agit de capteur ayant une très basse consommation d'énergie fonctionnant sur piles ainsi qu'une communication bidirectionnelle (montante et descendante) par ondes de très hautes fréquences entre 863 et 870 MHz et non par câbles.

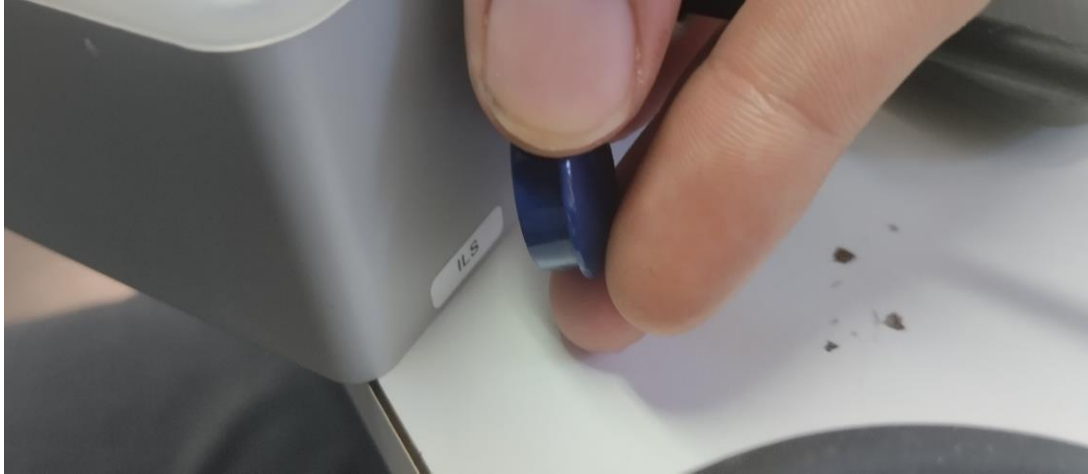
Ensuite, je dois appareiller les capteurs avec la passerelle. Je vais donc dans l'onglet Devices puis j'ajoute un capteur. Il convient de noter que pour le moment les capteurs ne sont toujours pas allumés.

Pour ajouter un capteur, je remplis les champs du nom, de sa description, son EUI (Extended Unique Identifier) c'est-à-dire son identifiant unique, l'Application que j'ai définie, nommé Kheiron, le numéro de port avec lequel je ferais la communication entre la passerelle et le capteur. Dans mon cas, il s'agit du port prédéfini numéro 125. Il ne me restera qu'à rentrer la clé applicative du capteur pour le chiffrement des données de bout en bout. La clé et l'EUI ont été donné par le constructeur et répertorié dans un fichier Excel lors de la livraison du matériel.

3.3.2 Configuration des capteurs

Avant de pouvoir configurer les capteurs, j'ai d'abord associé chaque capteur avec son mât dans le tableau Excel.

Pour allumer un capteur, j'ai passé un aimant assez puissant sur le bas du capteur, comme sur la photo ci-dessous :



Placement de l'aimant

J'ai maintenu l'aimant pendant environ 3 secondes puis une led s'est mise à clignoter rapidement en rouge pendant environ 1 seconde signifiant que le capteur vient de s'allumer. Elle clignota ensuite en vert avec un clignotement toutes les 5 secondes. Cela signifie que le capteur recherche la passerelle avec laquelle il a préalablement été attribué grâce à son EUI et sa clé. Une fois la passerelle trouvée, la lumière deviendra verte pendant environ 3 secondes avant de s'éteindre.

Pour pouvoir configurer le capteur pour qu'il remonte les bonnes informations, il faut lui transmettre des trames codées en hexadécimal. Pour se faire, j'ai d'abord regardé sur la page web de la passerelle dans le menu Network Server dans l'onglet Packets qui montre toutes les trames reçues par la passerelle. Sur ces dernières, on peut voir l'EUI du capteur qui a envoyé la trame.

Avant de transmettre les trames de configuration, j'ai dû passer les capteurs en mode test c'est-à-dire dans un mode qui met le capteur sur écoute de la passerelle et qui attend les trames de configuration.

Pour entrer dans ce mode, il faut laisser l'aimant pendant quelques petites secondes jusqu'à ce que la led se mette à clignoter lentement environ toutes les 3 secondes. Je devais cependant faire attention à ne pas laisser trop longtemps car sinon la led se mettait à clignoter très rapidement pendant 5 secondes puis à clignoter pendant 3 secondes. Dans ce cas le capteur a été éteint et il faut le rallumer.

Un fois le passage en mode test réussi, toujours dans l'onglet Packet sur la passerelle, je devais remplir une trame préremplie par la passerelle avec l'EUI du capteur, le type de données que j'envoie vers le capteur, c'est-à-dire de l'hexadécimal. Puis je remplis les données par la trame hexadécimale de configuration qui m'a été fourni par le fournisseur. Enfin, je renseigne le numéro de port soit le 125 dans mon cas et je coche la case qui permet de stipuler qu'un acquittement est attendu.

Les trames de configuration doivent être envoyés une à une et il faut bien attendre la trame d'acquiescement envoyée par le capteur.

Les trames à envoyer sont les suivantes :

-La première est 1106000f00005510000085a001

Cette trame permet de configurer l'entrée 1 du capteur en mode tout ou rien c'est-à-dire soit l'entrée est alimentée soit non.

-La seconde est 3106000f00005510000085a001

Cette trame permet de configurer l'entrée 2 du capteur en mode tout ou rien.

- La troisième est 1106005000000641a760a7600700050000000000

- La quatrième est 1105000f00541001

Cette trame permet de configurer l'entrée 1 du capteur avec une inversion polarité, cela signifie que l'on utilise le capteur de façon inverse c'est-à-dire qu'il ne doit envoyer que les changements d'états de l'entrée et non un rapport tous les x secondes.

-La cinquième est 3105000f00541001

Cette trame permet de configurer l'entrée 2 du capteur avec une inversion polarité.

-La sixième est 115000500202

Cette trame permet de supprimer l'ancienne configuration de comptage, c'est-à-dire que le capteur ne va plus compter le nombre de fois qu'il a changé d'état.

3.3.3 Configuration de Kheiron

La configuration de Kheiron se fait directement sur la plateforme web <https://kheiron-sp.io>. Le fournisseur de la plateforme m'a ouvert une session avec mon adresse mail et un mot de passe que j'ai dû changer à ma première connexion.

Une fois connecté, une arborescence a été paramétrée cependant les capteurs n'ont pas encore leurs noms simplifiés et il ne s'agit à ce moment-là que de leur EUI. Pour les renommer, je suis allé dans les paramètres, dans l'onglet Digital Twins et j'ai cliqué sur l'outil de modification.

Dans ce dernier, j'ai pu renommer le capteur mais j'ai mis en description l'EUI du capteur pour éviter un oubli ou que l'on recherche à quel EUI correspond quel capteur sur quel mât. J'ai sélectionné le fuseau horaire de Paris ainsi que les droits d'accès, le canal de diffusion pour les alertes par mails ainsi que le projet.

Pour les alertes, je suis allé dans l'onglet Astreintes et j'ai créé une astreinte la nuit avec le bon fuseau horaire.

Puis je suis retourné sur la page d'accueil et je suis allé sur le projet dans lequel tous les capteurs ont été référencés et renommés à la suite de la modification des paramètres. J'ai cliqué sur le symbole d'œil pour voir les détails sur le capteur puis j'ai cliqué sur les paramètres de ce dernier.

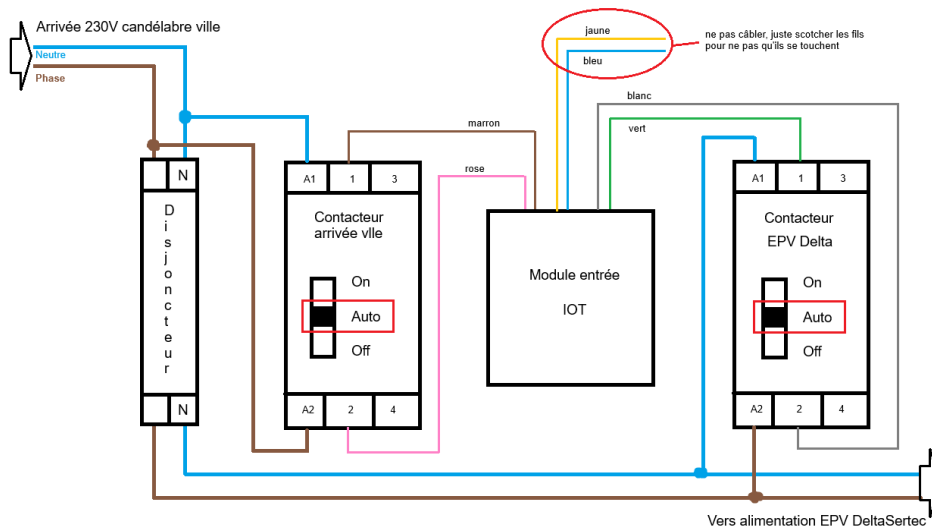
Dans cette page, j'ai rentré les coordonnées géographiques du capteur pour que l'intervention soit plus facile.

J'ai défini les deux entrées du capteur comme utilisées avec un état normalement fermé, c'est-à-dire que le mât doit être normalement alimenté.

Les alarmes ont été activées sur les deux entrées et ces dernières ont été renommées Alimentation Ville et Alimentation Delta.

3.3.4 Tests

Avant de déployer la solution sur le site, mon tuteur, Mr Martinez, m'a aidé à monter une maquette de tests.



Maquette de test

J'ai effectué le câblage me permettant de brancher ou non une arrivée électrique classique de 230V. Ce système est composé du capteur qui est en bas à droite de l'image, relié à un contacteur par entrée avec chaque contacteur de part et d'autre du disjoncteur. Avant le premier contacteur, il y a une prise d'alimentation male et après le second contacteur, il y a une prise femelle qui permet de fermer le circuit électrique.

Le premier test a été de voir si le capteur remontait bien les changements d'états. Pour se faire, j'avais connecté mon ordinateur à la passerelle dans l'onglet Packets pour voir le trafic de trames entre le capteur et cette dernière. En parallèle, j'étais aussi sur la plateforme Kheiron.

Lors d'un changement d'état, la valeur d'une des entrées ou des deux dans le cas où tout le système n'est pas alimenté. J'ai donc branché le système et laissé le disjoncteur sur l'état armé, c'est-à-dire qu'il laissera passer le courant. Les deux entrées sont alimentées et j'ai vu une trame passée par la passerelle. J'ai ensuite vérifié si le changement avait eu lieu. Ce dernier a bien été effectué sur les deux entrées.

Le second test a été de voir lorsque le disjoncteur n'est pas armé, c'est-à-dire lorsqu'il y a une ouverture dans le circuit, et que le courant passe bien dans le circuit avant ce dernier, si l'entrée du capteur reliée au contacteur qui se situe après le disjoncteur transmet bien l'information d'une perte de courant. Lors de l'opération, je vis bien la trame être transmise à la passerelle. Cependant lorsque j'ai vérifié le résultat sur la plateforme Kheiron, j'ai remarqué que l'on avait inversé les entrées lors du paramétrage de ce dernier, c'est-à-dire que l'entrée alimentation ville était vue comme non-alimentée alors que cela devait être l'inverse.

J'ai donc corrigé mon erreur en reparamétrant correctement les entrées sur la plateforme puis j'ai refait le test. Ce dernier fut concluant.

Le troisième test fut la vérification de l'envoi de mail d'alerte lors d'un changement d'état anormal. Pour pouvoir tester, j'ai modifié les horaires d'envoi d'alarmes pour que ces derniers se fassent le jour. Je suis aussi allé dans les paramètres pour modifier mon profil en le reliant avec la notification d'alarme qui j'ai préalablement défini comme étant un mail.

J'ai donc débranché le système. J'ai vérifié le passage de la trame et le changement sur la plateforme. Le processus n'a montré aucune erreur. J'ai donc vérifié sur ma boîte mail. Ce dernier est bien arrivé quelques minutes après.

Le dernier test a été de voir qu'elle est le rayon d'action de la passerelle et à partir de quelle distance, cette dernière perdrait la communication avec un capteur. Pour faire ce test, j'ai placé la passerelle dans des conditions non optimales, c'est-à-dire que cette dernière était couchée, au rez-de-chaussée du siège

de Delta Sertec en pleine ville donc avec beaucoup d'obstacles (immeubles, maisons, ...) et d'interférences. J'ai ensuite pris un capteur qui a été préalablement paramétré et testé puis je suis parti en ville avec un repère GPS (Global Positioning System) sur mon téléphone qui mesurait la distance à vol d'oiseaux entre mon repère et ma position. Mon binôme Clément Marie est resté dans les locaux et observait les trames ainsi que la plateforme Kheiron.

Pour voir si l'information parvenait bien, j'ai pris les deux fils d'une entrée et je les collais. J'étais en même temps au téléphone avec mon binôme pour savoir si tout se passait bien. Puis je décollais les fils et j'attendais de nouveau avant de continuer à marcher. Nous avons continué le test jusqu'à ce qu'il n'y ait plus aucun passage de trame entre le capteur et la passerelle. La distance obtenue fut d'environ 175 mètres.

Sur le plan, le capteur le plus loin est à environ 180 mètres. Cependant, la passerelle sera montée droite sur le toit d'un immeuble de 10 étages et assez haut sur ce dernier pour avoir une vue directe sur chaque mât avec très peu d'interférences. À la suite des retours de mon tuteur et du commercial en charge du projet sur le résultat du test, ce dernier fut considéré comme concluant.

3.4 Déploiement de la solution

Après une démonstration auprès de mon tuteur et du commercial en charge du projet, j'ai obtenu la validation pour le déploiement de ce dernier dans la résidence du Charrel à Aubagne.

J'ai donc accompagné une équipe sur place.

Ma tâche fut de monter la passerelle sur le toit. J'étais au début accompagné d'un technicien pour pouvoir apporter tout le matériel sur le toit. Puis ce dernier à percer plusieurs trous dans le mur pour pouvoir y attacher le socle qui servirait à maintenir la passerelle. Pendant ce temps, je montais les deux antennes sur cette dernière. Il fallait faire très attention car ces dernières contiennent du verre assez fragile. J'ai dû éviter le moindre choc violent et de ne pas trop forcer sur le connecteur pour éviter d'abimer le connecteur entre les deux éléments. Les photos ci-dessous montrent la passerelle prête et l'installation sur le toit terminée.



Passerelle prête à l'installation



Installation terminée sur le toit

Pour pouvoir alimenter la passerelle, elle fut reliée à un commutateur (Switch) possédant des port rj45 PoE assez puissant pour fournir 48V en courant continu, c'est-à-dire sans fluctuation de la tension comme dans les maisons par exemple.

Pour se faire, j'ai dû faire l'ajout de connecteurs sur un câble comme lors des cours de Monsieur Depeyre en début de première année. J'ai donc dû dénuder le câble puis enlever le blindage de ce dernier pour avoir le résultat suivant :



Câble dénudé

Je devais faire attention à ne pas abimer les câbles de cuivre colorés sinon je devais recommencer. Un fois le connecteur installé, ce dernier fut branché à la passerelle et protégé par un système en plastique et en caoutchouc de la passerelle avant de passer le câble dans une gaine qui arrive en dessous du coffret contenant le commutateur et un capteur. Il n'y a qu'un seul capteur et contacteur dans le coffret car le seul problème d'alimentation ne peut être que dans le bâtiment puisque la passerelle est alimentée par le commutateur qui est lui-même alimenté par l'immeuble.

La gaine permet de protéger le câble des intempéries.

Un fois le câble tiré, je devais faire le deuxième embout pour le connecter au commutateur. J'ai ensuite vérifié que le courant passait bien en regardant les leds sur le commutateur mais aussi en me connectant à l'adresse publique de la passerelle fournie par la carte SIM. Le résultat fut concluant.

Pour l'installation des capteurs, je ne pus les faire car ils devaient être au sommet des mâts qui font plus de 5 mètres. Le technicien a utilisé une nacelle pour pouvoir le faire.

4 Prysm

4.1 Hypervision

L'hypervision en termes de sécurité désigne une approche avancée et centralisée de la surveillance et de la gestion des systèmes de sécurité. Elle intègre et centralise les données et les contrôles de multiples systèmes de sécurité dans une interface unique, permettant une surveillance plus efficace et une gestion optimisée des ressources et des incidents.

4.1.1 Caractéristiques

Je vais décrire les principales caractéristiques de l'hypervision.

La première est la centralisation des systèmes, c'est-à-dire l'intégration multi-système sur une interface unifiée.

L'intégration multi-système combine des systèmes de vidéosurveillance, de contrôle d'accès, d'alarme incendie, de détection d'intrusion, et d'autres dispositifs de sécurité dans une seule plateforme. Chacun de ces systèmes possède le plus souvent un protocole de communication qui lui est propre.

L'interface unifiée est définie par une interface utilisateur unique pour surveiller et gérer tous les systèmes de sécurité de manière cohérente.

La seconde est la visualisation avancée des systèmes de sécurité en d'autres termes, une interface graphique personnalisées en fonction des besoins et une cartographie interactive du lieu hypervisé.

L'interface graphique affiche les données en temps réel à travers des tableaux de bord et une navigation personnalisable.

La cartographie interactive utilise des cartes et des plans interactifs pour représenter visuellement la localisation des dispositifs de sécurité et des incidents.

La troisième est la gestion des incidents qui regroupe la détection et la notification automatique en cas d'incident ou de contrôle ainsi que des flux de travail pour la gestion de ces derniers.

La détection et la notification permettent l'identification automatique des incidents et alerte les opérateurs via des notifications en temps réel.

Les flux de travail pour la gestion des incidents fournissent des outils pour suivre, gérer et documenter les incidents depuis leur détection jusqu'à leur résolution.

Le quatrième point est l'analyse et l'automatisation. Cette caractéristique regroupe l'analyse de données et l'automatisation de réponses aux incidents.

L'analyse de donnée utilise des algorithmes d'analyse pour détecter les anomalies, prévoir les incidents potentiels et fournir des perspectives sur la sécurité.

L'automatisation des réponses permet la réaction automatique face à certains types d'alerte comme le verrouillage des portes ou l'activation des alarmes.

La dernière caractéristique est l'interopérabilité et l'évolutivité du système d'hypervision en fonction des changements effectués dans une structure.

L'interopérabilité signifie la compatibilité avec divers fournisseurs. Les plateformes d'hypervision sont le plus souvent conçues pour être compatibles avec une variété de dispositifs et de systèmes provenant de différents fabricants.

L'évolutivité désigne la possibilité d'intégrer de nouveaux dispositifs et systèmes à mesure que les besoins de sécurité évoluent.

4.1.2 Avantages

L'hypervision possède des nombreux avantages que je vais lister.

L'un des plus important avantage est l'efficacité couplée à la réactivité. Cela signifie la réduction du temps de réponse dû à la centralisation des systèmes et la visualisation en temps réel permettant une détection plus rapide des incidents et une réponse plus coordonnée mais aussi de la prise de décision informée. En effet, les opérateurs disposent de toutes les informations nécessaires pour prendre des décisions éclairées et rapides en cas d'incident.

Un autre avantage est l'optimisation des ressources. Elle comprend l'efficacité opérationnelle et la réduction des coûts.

L'efficacité opérationnelle réduit la désorganisation et permet une utilisation plus efficace des ressources humaines et technologiques.

La réduction des coûts touche les coûts de maintenance et de gestion car plusieurs systèmes sont intégrés dans une seule plateforme.

Le dernier avantage est non des moindre. Il s'agit de l'amélioration de la sécurité globale par l'implication de la détection proactive, c'est-à-dire d'une approche de sécurité où les menaces et les incidents potentiels sont identifiés avant qu'ils ne causent des dommages significatifs, ainsi que par la coordination améliorée dû à la vue unifiée entre les différents éléments de sécurité installés et de leur localisation.

4.1.3 Applications

L'hypervision peut être utilisé dans différents secteurs.

On peut la retrouver dans la sécurité urbaine et dans les innovations dites de « villes intelligentes ». En effet, elle est utilisable dans les centres de commandement pour superviser la sécurité publique, la gestion du trafic, et les services d'urgence en intégrant la surveillance des infrastructures urbaines et des espaces publics pour améliorer la sécurité et l'efficacité des opérations municipales.

L'hypervision peut être utilisée sur des installations critiques et/ou industrielles. Elle surveille et gère la sécurité des sites industriels, des infrastructures critiques comme les centrales électriques, les raffineries, et les usines. Elle comporte aussi la surveillance des processus industriels et la gestion des alarmes pour prévenir les pannes et optimiser la production.

Il est possible d'installer de l'hypervision dans des bâtiments commerciaux et les résidences. Dans ce cas, elle surveillera les systèmes de sécurité des bâtiments, y compris les contrôles d'accès, les alarmes incendie, et les caméras de surveillance tout en facilitant la gestion des incidents de sécurité et l'optimisation des systèmes de gestion des bâtiments.

L'hypersion peut jouer un rôle majeur dans le secteur des transports et de la logistique. En effet, elle assure la sécurité des aéroports, des gares, et des infrastructures de transport en surveillant les mouvements des personnes et des marchandises en gérant les systèmes de sécurité en temps réel pour garantir la sûreté et l'efficacité des opérations de transport.

4.2 Présentation Générale

Prism est une solution de supervision et de gestion centralisée qui intègre divers systèmes de sécurité et de gestion d'installations dans une interface unifiée. Elle est conçue pour améliorer la visibilité, la coordination et le contrôle des infrastructures complexes, notamment dans les domaines de la sécurité, de la gestion des bâtiments, et des opérations industrielles.

Prysm possède plusieurs concurrents sur ce marché comme PCvue entre autres.

4.2.1 Fonctions et Capacités

Prysm reprend toutes les caractéristiques demandées pour « hyperviser » un site.

En effet, Prysm intègre divers systèmes comme la vidéosurveillance, les contrôles d'accès, les systèmes de détection d'incendie, les systèmes de gestion des alarmes, et les capteurs IoT. Il offre une interface centralisée pour surveiller et contrôler tous ces systèmes de manière cohérente.

Prysm permet une grande personnalisation de tableaux de bord ou de navigation sur un site en ayant la possibilité d'utiliser différents types de format pour les plans ainsi que la superposition d'éléments pour permettre de voir les différents systèmes de sécurité installés.

Il est possible grâce à Prysm de pré paramétrer la manière de gérer et remonter les alarmes. Je peux prendre comme exemple le fait que sur certains sites, il est demandé, dès qu'il y a une alarme, d'afficher sur un mur d'images les caméras ayant un angle de vision sur l'endroit de déclenchement de cette dernière ou si l'opérateur veut avoir un autre angle de vision qu'il lui semble plus approprié, il peut sélectionner une caméra en particulier.

Prysm intègre une solution d'automatisation de tâches mais aussi de personnalisation de scripts en langage C#. L'automatisation de certaines tâches de supervision et de gestion regroupe en parti l'activation des alarmes ou la gestion des accès. Prysm permet la création de scripts pour des actions automatisées spécifiques.

4.2.2 Avantages

Le premier avantage que j'ai pu observer est l'amélioration de la réactivité d'un opérateur grâce à la détection rapide des incidents et d'alerte permettant une réponse rapide et efficace ainsi qu'une coordination optimisée dû à la vue centralisée entre différents systèmes et le personnel.

La vue centralisée permet de réduire la complexité de gestion de systèmes disparates.

Un autre avantage non négligeable est la possibilité, comme dit précédemment d'automatiser des tâches répétitives et critiques à l'aide de scripts, ce qui augmente drastiquement l'efficacité opérationnelle.

Un avantage supplémentaire est la sécurité et la conformité grâce à l'option d'enregistrement, d'analyse et de résilience de Prysm. En effet, il fournit des enregistrements détaillés et des capacités d'analyse pour les audits et la conformité réglementaire. La résilience est améliorée grâce à une surveillance continue et une gestion proactive des incidents.

L'un des plus gros avantages de Prysm est qu'il possède une grande base de pilote pour une large gamme de matériel. Dans la plupart de ces derniers, il y a un programme nommé witcher c'est-à-dire que lors de l'installation du pilote, il va s'exécuter et créer toutes les variables permettant l'utilisation d'un système.

Je peux citer comme exemple l'utilisation d'un pilote pour une centrale d'alarmes. Une centrale est un dispositif centralisé utilisé pour surveiller, contrôler et gérer un système d'alarme. Elle est au cœur des systèmes de sécurité et de détection d'intrusion, assurant la coordination et le traitement des signaux provenant de divers capteurs et dispositifs de sécurité installés dans un bâtiment ou une zone protégée. Cette dernière possède de nombreux systèmes interconnectés avec elle telle que des détecteurs de mouvement, infrarouges et autres, ce qui signifie donc de nombreux flux de données.

Une centrale d'alarmes peut posséder des milliers de variables car il existe celles qui sont renvoyées contenant un changement d'état, une mise en défaut ainsi que plein d'autres types qui lui sont propres,

mais aussi des variables que l'on doit utiliser pour envoyer des commandes de réaction ou de changement de configuration. Il y a donc en tout plusieurs centaines de variables pour une seule centrale avec un fonctionnement particulier ou un type précis, par exemple de type énumération qui permet de passer plus de 2 états à une variable.

Le witcher contenu dans le pilote va créer toutes les variables adéquates avec la bonne arborescence concernant le matériel utilisé.

4.3 Formation

Prysm possède plusieurs solution comme AppControl et AppVision.

AppControl de Prysm est un logiciel de gestion et de supervision centralisée conçu pour optimiser la surveillance et le contrôle des infrastructures critiques et des systèmes de sécurité. Ce logiciel fait partie de la suite de solutions de Prysm pour l'hypervision, permettant une gestion unifiée des différents sous-systèmes de sécurité et des dispositifs de contrôle d'accès, de vidéosurveillance, d'alarme, et plus encore.

AppVision est un logiciel conçu pour la supervision, le contrôle et la gestion intégrée de divers systèmes de sécurité et de gestion des bâtiments. Ce logiciel de type PSIM (Physical Security Information Management) permet de centraliser et d'unifier la surveillance et le contrôle de différents systèmes disparates au sein d'une interface unique et cohérente.

Delta Sertec utilise la solution AppVision pour créer ces interfaces HUD (Heads Up Display) c'est-à-dire l'environnement de l'application d'hypervision, ainsi que leur IHM (Interface Homme-Machine).

AppVision est composé de 3 logiciels, AppVision Server, AppVision Configurator et AppVision Client.

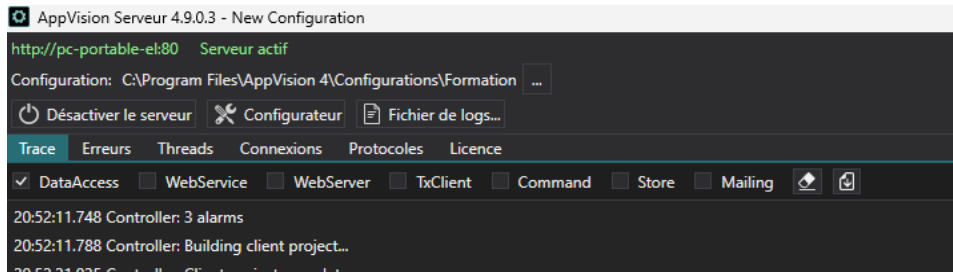
AppVision Server est une composante essentielle de leur suite logicielle de gestion de la sécurité et de la supervision des infrastructures. Il sert de moteur central pour la plateforme AppVision, permettant de centraliser, traiter, gérer les données et les protocoles provenant de divers systèmes de sécurité et de gestion des bâtiments.

AppVision Configurator est un outil essentiel conçu pour faciliter la configuration et la personnalisation des solutions de gestion centralisée de la sécurité et des infrastructures. Cet outil permet aux administrateurs et aux intégrateurs de systèmes de définir, configurer et ajuster les paramètres et les comportements des systèmes supervisés par AppVision.

AppVision Client est conçue pour permettre aux utilisateurs finaux d'interagir avec le système de supervision et de gestion centralisée. Ce logiciel client offre une GUI (Interface Utilisateur Graphique) qui permet de surveiller, contrôler et gérer divers systèmes de sécurité et d'infrastructure à partir d'un point centralisé. Avant de rendre la solution finale au client, il est possible d'organiser et de fixer le nombre et la taille de différents conteneurs dans lesquels pourront se glisser par exemple un menu de navigation ou des plans.

Je vais maintenant passer à une brève présentation graphique des différents logiciels.

Voici une vue du logiciel AppVision Server :



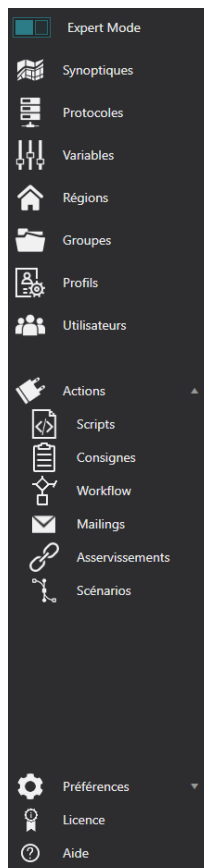
Accueil de APPVision Server

Dans cette interface, on peut voir sur la ligne Configuration, le chemin vers le projet chargé par le serveur. Il est possible de modifier ce chemin pour ouvrir d'autres projets. Cependant, il faut redémarrer le logiciel car ce dernier va aussi charger et vérifier le bon lancement des protocoles de communications des systèmes raccordés et paramétrés.

Sur la deuxième ligne, il y a la désactivation possible du serveur, l'accès au logiciel AppVision Configurator traduit ici par Configurateur ainsi que l'accès aux fichiers journaux qui répertorie toutes les opérations et les erreurs rencontrées. Lors du lancement du configurateur par ce biais, ce dernier va déjà être sur le projet chargé par le serveur mais il est tout à fait possible de se connecter sur un serveur contenant un autre projet hébergé sur une machine distante et de continuer à distance.

Sur la dernière ligne du menu, il y a Trace qui affiche tout ce qui est fait par le serveur en temps réel, Erreurs, Threads (Fils en anglais) qui fait un récapitulatif des services lancés ou en attente, Connexions qui retrace comme son nom l'indique les connexions de configurateurs ou de clients au server, qu'elles soient distantes ou non, Protocoles qui regroupe tous les protocoles programmés et lancés par le serveur, ainsi que Licence qui détaille tout ce qui est contenu dans cette dernière soit le nombre de protocoles autorisés, le nombre de variables et autres.

Sur le configurateur, voici les différents menus :



Vu des menus du configurateur

Le premier menu est celui des synoptiques. Ce menu est une fonctionnalité clé qui permet de créer, visualiser et interagir avec des représentations graphiques des systèmes supervisés. Ces représentations, appelées "synoptiques", sont des diagrammes ou des plans visuels qui illustrent les différents composants et dispositifs du système de sécurité ou de gestion des bâtiments de manière intuitive et interactive en offrant des outils de dessin et des bibliothèques d'icônes pour représenter différents types de dispositifs.

Ce menu facilite la configuration des dispositifs directement à partir du synoptique en associant des icônes et des éléments graphiques aux dispositifs réels connectés au système en permettant de définir des propriétés et des comportements de dispositifs, comme les zones de couverture des caméras ou les points de contrôle d'accès.

Les synoptiques permettent une visualisation en temps réel de l'état des dispositifs et des systèmes. Les utilisateurs peuvent voir les alarmes, les événements et les états des dispositifs directement sur la carte synoptique tout en offrant la possibilité de paramétrer un zoom, des déplacements et des interactions avec les éléments du synoptique pour obtenir des informations détaillées.

Il est possible de définir des scénarios d'automatisation basés sur les interactions avec le synoptique. Par exemple, un double-clic sur un détecteur de fumée peut déclencher une séquence d'actions prédéfinies, comme l'activation des alarmes et l'envoi de notifications.

Les synoptiques peuvent être personnalisés pour répondre aux besoins spécifiques de chaque installation. Les utilisateurs peuvent ajouter des couches, des annotations et des marqueurs pour améliorer la clarté et l'efficacité de la visualisation.

Ils peuvent évoluer avec le système, permettant d'ajouter de nouveaux dispositifs et de modifier la configuration au fil du temps.

Le deuxième menu est celui des Protocoles est un composant clé pour la gestion des communications entre AppVision et les dispositifs ou systèmes externes qu'il supervise. Les protocoles sont des ensembles de règles qui définissent la manière dont les données sont échangées entre les différents systèmes. Ce menu permet aux administrateurs de configurer, gérer et intégrer divers protocoles de communication pour assurer une interopérabilité fluide entre AppVision et les dispositifs tiers.

Le troisième menu est le menu Variables. Comme son nom l'indique c'est dans ce dernier que l'on peut permettre de définir, gérer et utiliser des variables dans le cadre de la configuration et de l'automatisation des systèmes supervisés. Les variables jouent un rôle crucial dans la création de scénarios automatisés, la personnalisation des réponses aux événements, et l'intégration de différents systèmes.

Le quatrième menu regroupe les Régions. Il sert à organiser, structurer et gérer les différents éléments et zones au sein d'une installation supervisée. Ce menu permet de définir des espaces géographiques ou logiques, facilitant ainsi la gestion centralisée des dispositifs et des événements associés à ces régions.

Il ne faut pas le confondre avec le menu Groupe qui lui, cependant, va servir à regrouper des éléments en fonctions de leur type, par exemple pour un groupe que de cameras ou de détecteurs de mouvements.

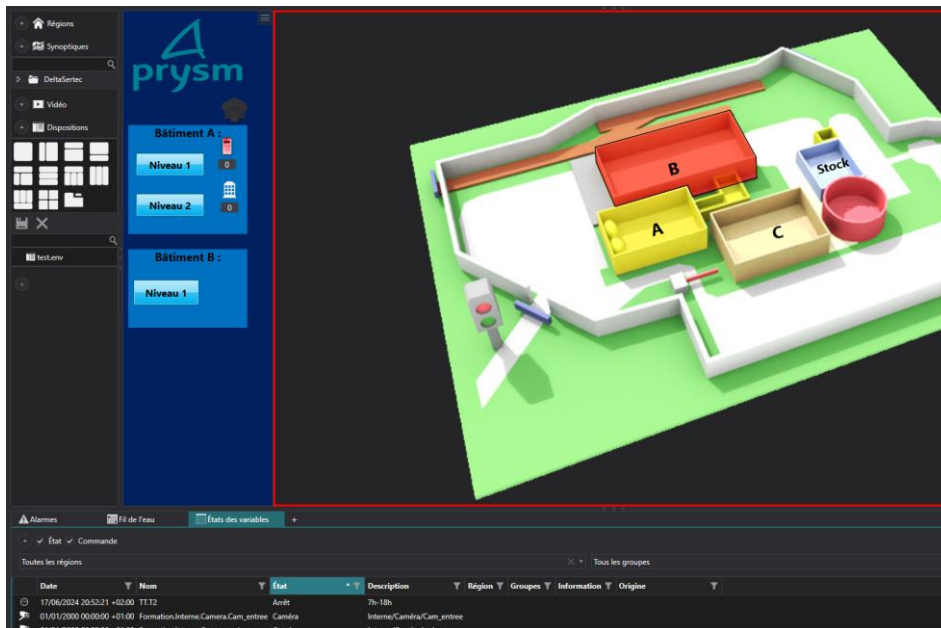
Le cinquième est le menu Profils. Il permet de définir, gérer et appliquer différents profils de configuration et de sécurité pour les utilisateurs et les dispositifs intégrés dans le système de gestion.

Le sixième est le menu Utilisateur. Il est utilisé pour gérer les comptes individuels des utilisateurs, incluant la création, la modification, et la suppression des comptes et permet de définir les informations spécifiques à chaque utilisateur, telles que le nom, le rôle, les informations de contact, et les identifiants

de connexion ainsi que des permissions et des accès spécifiques à chaque utilisateur, qui peuvent être basés sur des profils prédéfinis mais ajustés individuellement si nécessaire.

Le septième est un groupe de menus. Dans ce groupe, je n'ai utilisé que celui nommés Scripts. Il s'agit d'une fonctionnalité avancée qui permet aux utilisateurs de créer, gérer et exécuter des scripts pour automatiser et personnaliser divers aspects du système de gestion centralisée. Cette fonctionnalité est essentielle pour les intégrateurs et les administrateurs système souhaitant augmenter la flexibilité et les capacités de la plateforme AppVision en fonction de leurs besoins spécifiques. Ces derniers ne sont exécutés que par le serveur.

Je vais maintenant donner des explications sur le logiciel AppVision Client.



Interface Client avec mon projet Formation

Tout d'abord, le panneau de droite et celui du bas peuvent être retirés. Je les ai juste affichés pour aider à la compréhension.

Au centre, il y a l'interface où l'on dispose les containers c'est-à-dire à une structure logique utilisée pour organiser, afficher et gérer divers éléments d'information ou de contrôle dans l'interface utilisateur. Leur comportement est similaire à ceux utilisés par la distribution Linux.

Le panneau de droite comporte différentes parties. Il y a la partie région qui est la même que celle du configurateur. La partie synoptique qui permet de disposer les plans ou les visualisations faites dans le configurateur dans les différents containers.

Ce qui nous amène à la partie disposition, dans cette dernière, on y retrouve comme son nom l'indique différentes dispositions déjà faites mais il est possible d'en créer soi-même en allant dans les fichiers pour en copier une existante et la modifier selon nos besoins.

Le panneau du bas peut contenir différents onglets pouvant servir au débogage ou au test comme l'onglet états des variables qui permet de modifier l'état d'une variable pour déclencher une alarme, un fil de l'eau pour voir les modifications ou encore un onglet préprogrammé pour les alarmes dont l'acquiescement est possible depuis ce dernier.

4.4 Missions

Mes missions sur Prysm ont été la création d'une disposition de containers pour l'interface graphique d'un gros projet, la création d'une navigation entre différents plans et menus, l'intégration d'une

partie du visuel ainsi que du nettoyage de plans donnés par le client pour les afficher dans le logiciel AppVision Client.

Pour la disposition des containers, j'ai dû créer un fichier dans lequel je définis le nombre, le nom et la taille en pixels de ces dernier.

La navigation entre les différentes vues se fait par le biais de plusieurs boutons pour changer entre les différents étages, vues globales ou menu de gestions.

L'intégration du visuel a été faite par l'utilisation d'une gamme de couleurs similaires mais aussi par la création de synoptiques taillés au pixel près pour être insérés dans les containers qui leurs sont attribués. J'ai aussi créé différentes couches pour pouvoir faire apparaître des éléments suite à une action précise sur le plan central.

Enfin la partie qui n'est certes pas la plus intéressante mais qui est l'une des plus importantes et chronophage, il s'agit du nettoyage au pixel des plans architecturaux envoyés soit par le client soit par l'architecte.



Partie de plan avec un début de nettoyage

Comme on peut le remarquer sur la figure, cette partie de plan zoomée n'est pas très nette ni très visible sur le fond de couleur bleu foncé.

Je vais donc effacer les pixels qui font cette imprécision ainsi que l'ajout d'un calque où je vais venir repasser dans des tons bleu clair plus visibles au-dessus des murs tout en les simplifiant pour le regard.

Le résultat est le suivant :



Plan nettoyé

5 Conclusion

Je vais maintenant conclure sur mon expérience durant ce stage. J'ai pleinement apprécié découvrir de nouveaux domaines qui m'étaient complètement inconnus comme tout le domaine de la sûreté et de sécurité d'un site ainsi que l'hypervision, son utilité et sa mise en œuvre.

J'ai pu durant ce stage faire l'ajout d'une « brique » IOT sur un projet en cours. Cette expérience fut très enrichissante car j'ai travaillé en partie en autonomie mais aussi en équipe sur ce dernier.

Le seul « regret » que j'ai par rapport à ce stage est le fait que je n'ai pas pu faire beaucoup de réseau dû aux retards de livraisons de matériels pour la mise en place de maquettes réseaux pour des gros projet en court. Cependant, je continuerai mon parcours dans cette entreprise durant mon année d'alternance. J'ai vraiment hâte de voir de nouvelles choses et d'être confronté à de nouveaux projets ainsi qu'à la suite de certains que je suivais lors de mon passage dans le pôle hypervision.

Remerciements

En premier lieu, je tiens à remercier BROUQUIER Arnaud, PDG de l'Entreprise DELTA SERTEC pour son accueil chaleureux au sein de l'entreprise.

Je tiens à remercier vivement mon maitre d'apprentissage, MARTINEZ Marc, responsable du service Hypervision et développement au sein de l'entreprise DELTA SERTEC. Je suis extrêmement reconnaissant quant à sa bienveillance et à tous les conseils qu'il a pu me fournir au quotidien.

Par ailleurs, je voudrais remercier MARIE Clément, Alternant sous la tutelle de Mr MARTINEZ, pour son aide lors de nos travaux en binôme.

Je remercie également CHARLIER Chloé de m'avoir accueilli dès le premier jour très chaleureusement au sein de l'entreprise et d'avoir su me renseigner à chaque fois que j'en avais besoin.

Sans oublier Mathieu Rialland, camarade de formation, pour son sérieux, sa curiosité, sa bonne humeur, son assistance et sa persévérance durant ce stage.

J'aimerais également remercier tous les membres de l'équipe DELTA SERTEC pour leur bienveillance.

6 Glossaire

BUT, Bachelor Universitaire de Technologie

IOT, Internet of Things

IRVE, Infrastructures de Recharge pour Véhicules Électriques

IPTV, Internet Protocol Television

IP, Internet Protocol

PoE, Power over Ethernet

SIM, Subscriber Identity/Identification Module

GPS, Global Positioning System

PSIM, Physical Security Information Management

HUD, Heads Up Display

IHM, Interface Homme-Machine

GUI, Interface Utilisateur Graphique

7 Sitographie.

Présentation de Delta Sertec :

<https://www.deltasertec.com>

Documentation sur la gateway Milesight:

<https://www.milesight.com/iot/product/lorawan-gateway/ug67>

Sur ce lien, rechercher dans la partie Download

Documentation sur les capteur Sens'o Watteco :

<https://support.watteco.com/>

<https://www.watteco.fr/produit/capteur-pulse-senso-ip55-ip68-atex-zone-1-lorawan/>

<https://www.watteco.com/download/fiche-technique-capteur-pulse-senso-lorawan-50-70-039/>

Présentation de Prysm:

<https://prysm-software.com/>

Documentation sur Prysm :

<https://prysm-software.com/notre-solution/appvision/specifications-techniques>

Assistance sur Prysm :

<https://prysm-software.com/frequently-asked-questions?lang=en>