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

Analyses et études au sein d'un progiciel de gestion de la sécurité de sites industriels

Nolan BEN YAHYA

EDF CNEPE

Responsable entreprise : Clément HERVE

Responsable académique : Ivan MADJAROV

2023

Table des matières

1 Introduction

Au sein du CNEPE (Centre National d'Equipement de Production d'Electricité), division de la DIPNN (Direction Ingénierie et Projets Nouveau Nucléaire) d'EDF, mon stage avait pour but de réaliser des études et analyses au sein d'un progiciel de gestion de la sécurité de sites industriels au sein du groupe IIS (Informatique Industrielle Sécuritaire).

L'objectif était pour moi de tester les diverses fonctionnalités du progiciel et de vérifier qu'elles soient en cohérence avec les exigences d'EDF en me basant sur une matrice fonctionnelle. Au fil de ces tests, j'ai eu pour objectif de réaliser une documentation et des préconisations d'exigences. J'ai aussi été force de proposition dans la sélection de solutions du marché sur la gestion des visiteurs. J'ai pu également organiser des réunions avec les fournisseurs afin d'éclaircir certains points et partager quelques retours.

Je commencerais par présenter EDF, la DIPNN, le CNEPE et le groupe IIS, puis je contextualiserais ma mission, je présenterais ensuite mon travail et les problèmes que j'ai pu rencontrer avant de conclure.

2 Présentation de l'entreprise

2.1 EDF

EDF est une entreprise publique de production et de fourniture d'électricité. Elle s'appuie sur ses filiales afin de réaliser ses différents rôles d'intérêts nationaux avec, par exemple : EDF Renouvelables, Dalkia et EDF DPNT pour la production ; Enedis et RTE pour la distribution.

Premier producteur mondial d'électricité neutre en CO_2 (Annexe 1), EDF profite de son expérience dans les divers moyens et infrastructures de production et de distribution d'énergie bas carbone pour s'exporter et piloter des projets à l'international. Ainsi, ses 171 490 collaborateurs, répartis sur 5 continents dans environ 30 pays font d'EDF un acteur majeur dans le choix et la diversification du mix énergique de la planète.

2.1.1 La DIPNN

La DIPNN ou la Direction Ingénierie et Projets Nouveau Nucléaire est en charge depuis 2015, avec ses 4 300 ingénieurs et techniciens, de piloter les projets de conception de nouvelles infrastructures nucléaires et de réaliser la maintenance des centrales en cours de fonctionnement, aussi bien en France qu'à l'étranger.

La gestion de deux centres d'ingénierie (le CNEPE et Edvance), lui permet de déléguer les différentes tâches d'étude, de réalisation et de maintenance des projets et sites en fonction de leurs spécificités.

En 2022, 6 projets de réacteurs de type EPR2 voient le jour en France pour un début de construction en 2028 et une mise en service aux environs de 2035. Gérés par la DIPNN, ces projets doivent permettre d'accroître considérablement la part du nucléaire dans le mix énergétique français.

L'organigramme de la DIPNN est disponible en annexe (Annexe 2).

2.1.2 Le CNEPE

Le CNEPE ou le Centre National d'Equipement de Production d'Electricité, est l'un des deux centres d'ingénierie de la DIPNN. Basé à Tours, le centre pilote 1 400 chantiers par an et compte plus de 1 260 salariés.

Depuis 2008, le projet du « Grand carénage » visant à effectuer des travaux dans le but d'allonger la durée de vie du parc nucléaire existant est suivi par le CNEPE dans 10 grands projets, tels que : l'évacuation d'énergie, le groupe turbo alternateur et la protection des sites.

Le CNEPE est aussi exportateur de savoir-faire, puisqu'au-delà des projets de nouveaux réacteurs en France tels que l'EPR2 (European Pressurized Reactor) et le SMR (Small Modular Reactor), le centre contribue également au développement de réacteurs au Royaume-Uni (Hinkley Point C et Sizewell C), mais aussi en Inde avec le JNPP (Jaitapur Nuclear Power Plant), la plus grande centrale nucléaire du monde.

Pour bien cerner le champ d'action du CNEPE, il faut d'abord comprendre ce qui constitue une centrale nucléaire (Figure 1). En effet, une centrale est composée de deux parties : l'îlot nucléaire et l'îlot conventionnel. L'îlot nucléaire, comme son nom l'indique, est la partie nucléaire de la centrale dans laquelle on retrouve : le bâtiment réacteur et le bâtiment combustible par exemple. L'îlot conventionnel englobe tout le reste de la centrale, c'est-à-dire : la source froide, la salle des machines et l'aéroréfrigérant par exemple, avec, en plus, la protection de site.

Figure 1 – Les principales composantes d'une centrale nucléaire

La sécurisation d'une centrale et les enjeux de sa mise en place, sont d'autant plus complexes quand on considère les différentes zones de sécurité qui compose un site, leurs aspects techniques et leurs contraintes spécifiques (Figure 2).

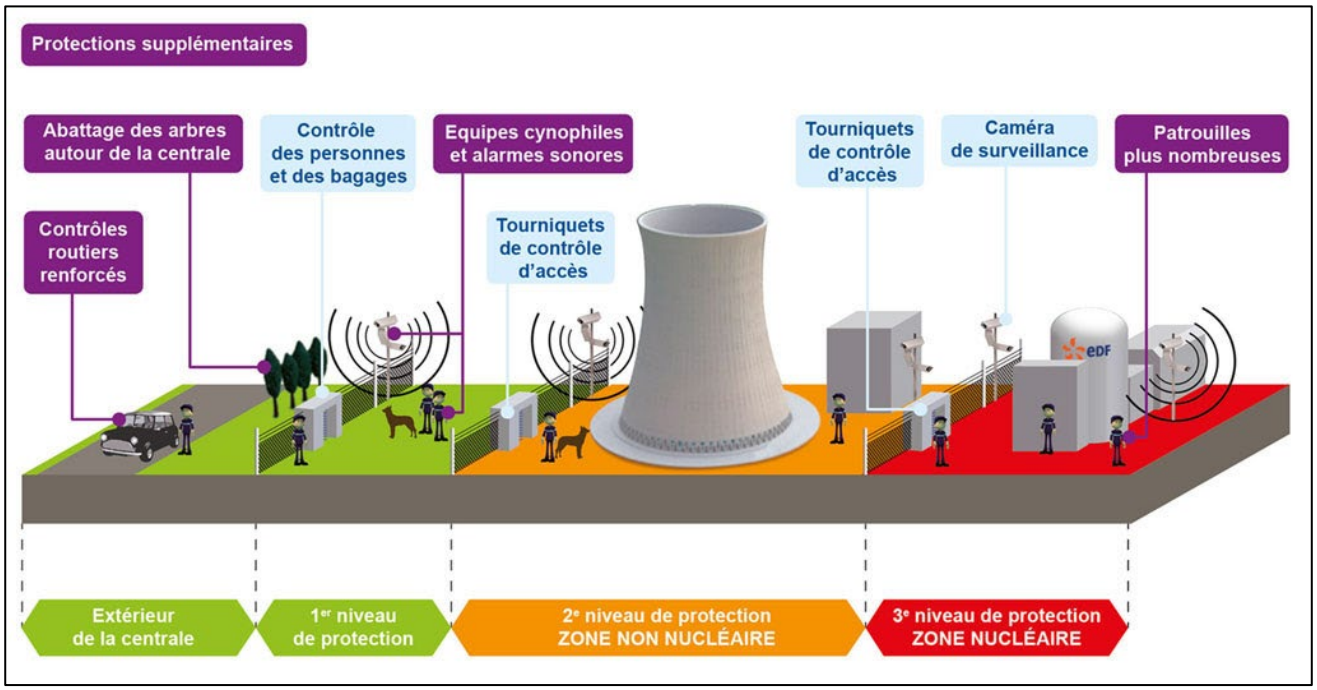


Figure 2 - Les différentes zones de sécurité d'une centrale nucléaire

L'organigramme détaillé du CNEPE est disponible en annexe (Annexe 3).

2.1.3 Le groupe IIS

Le groupe IIS ou Informatique Industrielle Sécuritaire est l'une des multiples branches du département études (DETU) du CNEPE organisée sous le service CIS (Contrôle Commande et Installations Electriques de Surveillance).

Ce groupe a pour mission d'étudier, analyser et proposer des solutions de protection de site industriel, notamment en réalisant des cahiers de préconisations pour une solution de vidéosurveillance ou de gestion des accédants.

On retrouve ainsi plusieurs domaines dans le groupe allant du développement pur, à la gestion et au déploiement de VMS (Video Management System).

Le groupe s'appuie sur les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et sur l'IGI 1300 (Instruction Générale Interministérielle) portant sur la protection du secret de la défense nationale, afin de réaliser ses travaux qui doivent scrupuleusement respecter ces normes du fait du caractère extrêmement sensible des informations qu'ils protègent et manipulent.

En effet, le CNEPE faisant parti d'un OIV (Opérateur d'Importance Vitale) et ayant accès à des lieux et ressources stratégiques relatives à la défense et à la souveraineté nationale, tous les systèmes et surtout les systèmes de sécurité des sites doivent être performants et encadrés par des normes strictes en commençant par les employés qui doivent se soumettre à une enquête préliminaire en vue de l'obtention d'un poste.

3 Contextualisation

3.1 Conduite de projets

Les projets EPR2 ou European Pressurized Reactor 2ème génération n'ont débuté leur développement que très récemment. Pour bien cerner les objectifs et enjeux de mes missions, il est d'abord primordial de connaître les différentes étapes de réalisation d'une centrale nucléaire (Figure 3).

Premièrement, il y a la phase d'opportunité où le client (ici l'Etat Français) commande des centrales en fonction de ses besoins. Des concepts sont alors élaborés et des coûts sont dressés.

Ensuite, la faisabilité du projet fait intervenir la mise en place d'exigences techniques, d'éléments industriels et la validation des concepts définis lors de la phase d'opportunité.

Puis, la conception générale du projet, l'établissement des spécifications, la ratification des contrats et l'élaboration du Databook interviennent dans une phase dite de « développement ».

Finalement, la phase de réalisation est amorcée et se compose du design des détails du projet, de la validation des fabrications, de l'organisation des chantiers, de la vérification des sites et enfin, de la mise en service et de la clôture finale du projet.

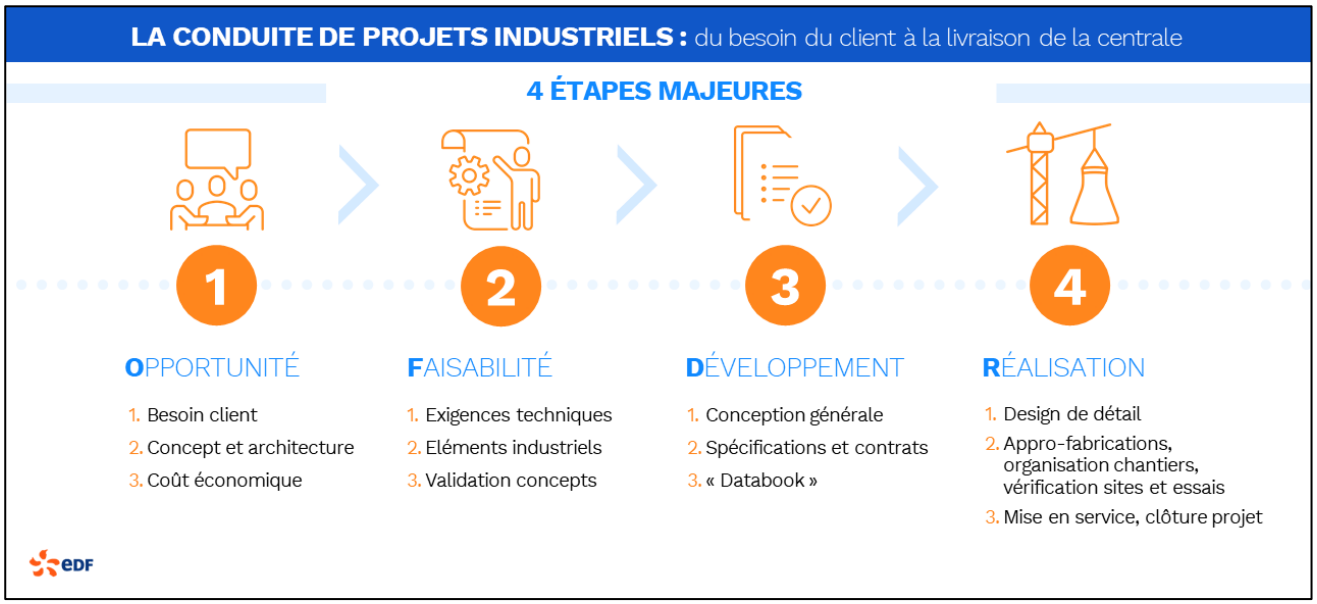


Figure 3 – Les étapes majeures de la conduite de projets industriels

Mes missions intervenaient dans la phase de Développement et plus particulièrement au niveau de la mise en place et la validation des spécifications juste avant le lancement de la phase de réalisation.

3.2 Construction d'une centrale

La construction d'une centrale nucléaire est un processus complexe et comporte plusieurs grandes étapes.

Tout d'abord, une fois que le terrain a été choisi puis préparé, il est nécessaire de monter une ZAC ou Zone d'Accès Chantier, c'est-à-dire enfermer toute la zone de chantier de la future centrale à l'intérieur d'un périmètre protégé par des clôtures et un système informatisé de protection de site.

Cette ZAC se doit d'être accessible aux agents, ingénieurs, techniciens et contractuels qui travaillent à l'élaboration de la centrale. Un PAC ou Poste d'Accès Chantier, c'est-à-dire un bâtiment en béton hébergeant l'accueil du site, des accès piétons et véhicules, est érigé temporairement le temps de la durée du chantier.

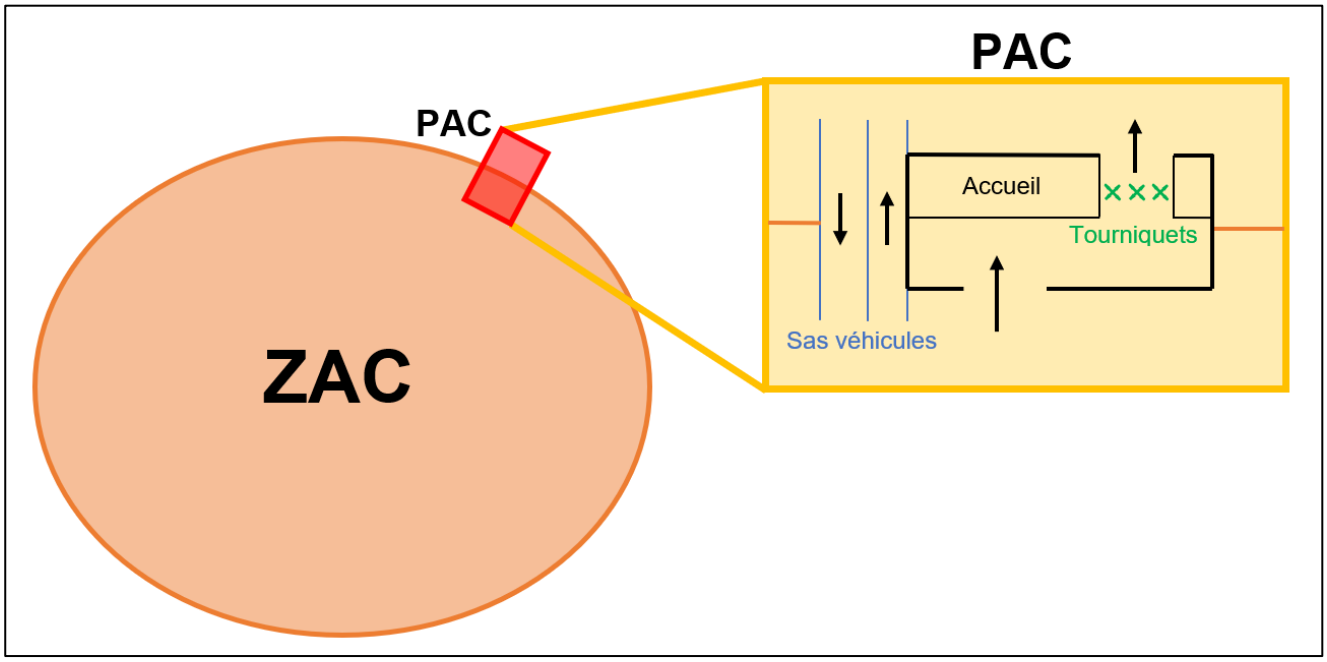


Figure 4 – Schéma ZAC et PAC avec détails

La sécurisation du chantier est d'autant plus importante qu'elle doit assurer l'intégrité de l'infrastructure finale et éviter la perturbation du déroulé de la construction.

Dans l'optique où ma mission découle du projet nouveau nucléaire, il est nécessaire de réaliser un référentiel pour les nouveaux systèmes.

Ainsi, EDF a lancé un travail d'analyse du marché afin de trouver des solutions de sécurité provenant du marché, de les tester suivant un cahier des charges établi (la matrice fonctionnelle) et de mettre en commun les points des exigences validées par toutes les solutions testées, ce qui donnera naissance à un nouveau référentiel. Les solutions choisies ou développées dans le futur devront alors obligatoirement répondre au minimum aux nouvelles exigences contenues dans le référentiel.

17	ACCES PORTIQUE	Contrôle d'accès renforcé	Le système est capable d'identifier, de remonter des alarmes et de proposer des actions opérateurs face à des comportements anormaux et des scénarios de fraude élaborés

Figure 5 – Exemple d'exigence présente dans la matrice fonctionnelle

Il est ici question de mettre en place un cahier des charges afin de pouvoir choisir une solution de sécurité qui sera opérationnelle le temps du chantier. A la fin de celui-ci, le PAC sera déconstruit, remplacé par une structure permanente et le système de sécurité changé.

3.3 Solutions

Au terme de l'étude du marché, EDF retient deux fournisseurs : **Secure** et **Genetec**.

C'est donc en se basant sur les deux solutions retenues et sur les exigences définies par EDF que l'on pourra, au terme des différents tests menés, créer un nouveau référentiel.

On appelle les tests réalisés sur une solution en vue de vérifier si elle se conforme à un cahier des charges, un POC ou Proof Of Concept.

3.3.1 Secure

Figure 6 – Logo de Secure Systems & Services

Secure Systems & Services est un acteur français dans le domaine du contrôle d'accès. Branche de Vinci Energies et basée à Aix-en-Provence, Secure reste une entité indépendante et s'exporte peu à peu à l'étranger avec notamment des nouveaux pôles en Amérique du Nord.

Secure est développeur de plusieurs solutions logicielles et matérielles de gestion d'accès. La solution EvolynxNG est le produit phare de Secure permettant la centralisation et l'intégration de solutions matérielles produites par Secure ou par des tiers, afin de gérer par exemple, des caméras, des portiers et des automates. C'est cette solution que j'ai été amenée à tester dans le cadre de mon stage.

D'autres solutions, plus limitées, sont également proposées par Secure comme uDemand et uHost, permettant conjointement d'exploiter des bornes et des postes d'enregistrement pour la gestion des visiteurs.

Il est important de noter que certaines fonctionnalités d'EvolynxNG ne sont disponibles qu'après l'utilisation d'un hyperviseur comme Prysm. De ce fait, il n'est pas possible, par exemple, d'utiliser le VMS d'une société existante sans passer par l'hyperviseur, bien que la solution de Secure supporte les solutions VMS de Milestone et de Genetec.

Fort d'un grand catalogue de projets à son actif, Secure est déjà intervenu dans le processus de sécurisation d'OIVs. On retrouvera dans ses projets : la sécurisation de 4 sites de l'ESA (Agence Spatiale Européenne) dont le site de lancement à Kourou et la sécurisation des hautes sphères européennes.

3.3.2 Genetec

Figure 7 – Logo de Genetec

Genetec est un autre acteur connu de la sécurité de sites. Entreprise canadienne, Genetec est néanmoins présent dans divers sites à travers le monde et notamment au sein de certains CNPE (Centre Nucléaire de Production d'Electricité, soit des centrales) en tant que solution de VMS.

Majoritairement présent aux Etats-Unis, Genetec est également bien implanté en Europe notamment dans diverses administrations publiques et sites de grande envergure comme les Aéroports de Paris dont le système de vidéosurveillance est géré par un produit Genetec : Security Center Omnicast.

Secure et Genetec peuvent fonctionner en synergie et ainsi permettre aux clients de profiter du meilleur des deux environnements. En effet, la solution de VMS de Genetec peut s'interfacer avec Evolynx, la solution de gestion d'accès de Secure. Néanmoins, la mise en place d'un hyperviseur est nécessaire afin de faire cohabiter les deux solutions et permettre à Secure de communiquer avec le système de Genetec. Cela n'est pas forcément le cas avec Genetec qui intègre un grand panel de solutions de manière native.

Les tests de conformité aux exigences pour la solution proposée par Genetec ont été réalisés par des alternants en parallèle des tâches que j'ai pu effectuer sur la solution de Secure.

3.4 Environnement de travail

Afin de tester les solutions par rapport aux exigences d'EDF, il est nécessaire de pouvoir travailler avec du matériel physique disposé de manière à se rapprochant de la réalité du terrain. Ainsi, le CNEPE dispose d'une plateforme qui permet les tests de solutions et de matériel en plus d'avoir la capacité de réaliser de la téléopération.

Cette pièce, disposant de baies de serveur hébergeant notamment les bases de données et les services qui composent les systèmes proposés par Secure et Genetec est aussi un espace de démonstration. En effet, un espace de « Showroom » y est installé, reproduisant l'intérieur d'un PCP (Photo 1) soit un Poste de Commande Principale, le centre névralgique de la sécurité au sein d'une centrale.

Photo 1 – Illustration d'un Poste de Commande Principal (PCP)

Ce showroom permet notamment de visualiser les systèmes de gestion de la sécurité dans un environnement réel et ainsi pouvoir mieux orienter les essais et avoir une meilleure vision du rendu final.

C’est dans cette pièce que les maquettes de test pour les systèmes de Secure et Genetec sont installées et c’est sur la plateforme que j’ai passé la majeure partie de mon stage.

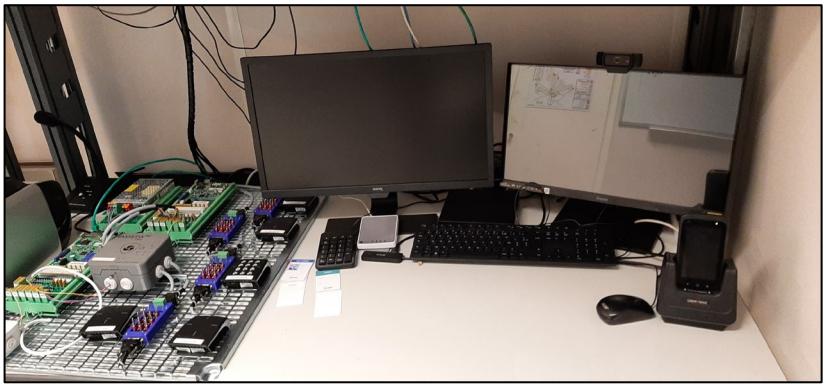


Photo 3 – Mon poste de travail sur la plateforme

Photo 2 – La maquette de test de Secure

4 Travail effectué

4.1 Prise en main

Durant les premières semaines de mon stage, je me suis donc familiarisé avec la solution Evolynx de Secure, en commençant par lire les documentations que j'avais à ma disposition. Ces documentations étaient majoritairement des documents marketing et assez peu d'informations techniques qui m'auraient permis de réellement comprendre le fonctionnement de la solution et de la maquette installée étaient disponibles.

En lisant les différentes plaquettes concernant les solutions installées par Secure (Evolynx, uDemand et uHost), je me suis rapidement posé la question de la nécessité et du fonctionnement concret des deux derniers logiciels (uDemand et uHost). Cette partie de manque de clarté reviendra quelques semaines plus tard et annoncera la naissance d'une nouvelle mission.

Après quelque temps de recherche, de tests et de réflexion, j'ai pu identifier et comprendre les différents modules qui composent la maquette et le système Evolynx. Le schéma fournit par Secure, sur lequel ils repasseront lors d'une réunion portant sur un projet différent auquel j'ai pu assister, m'aura également permis de comprendre quelques subtilités (Figure 8).

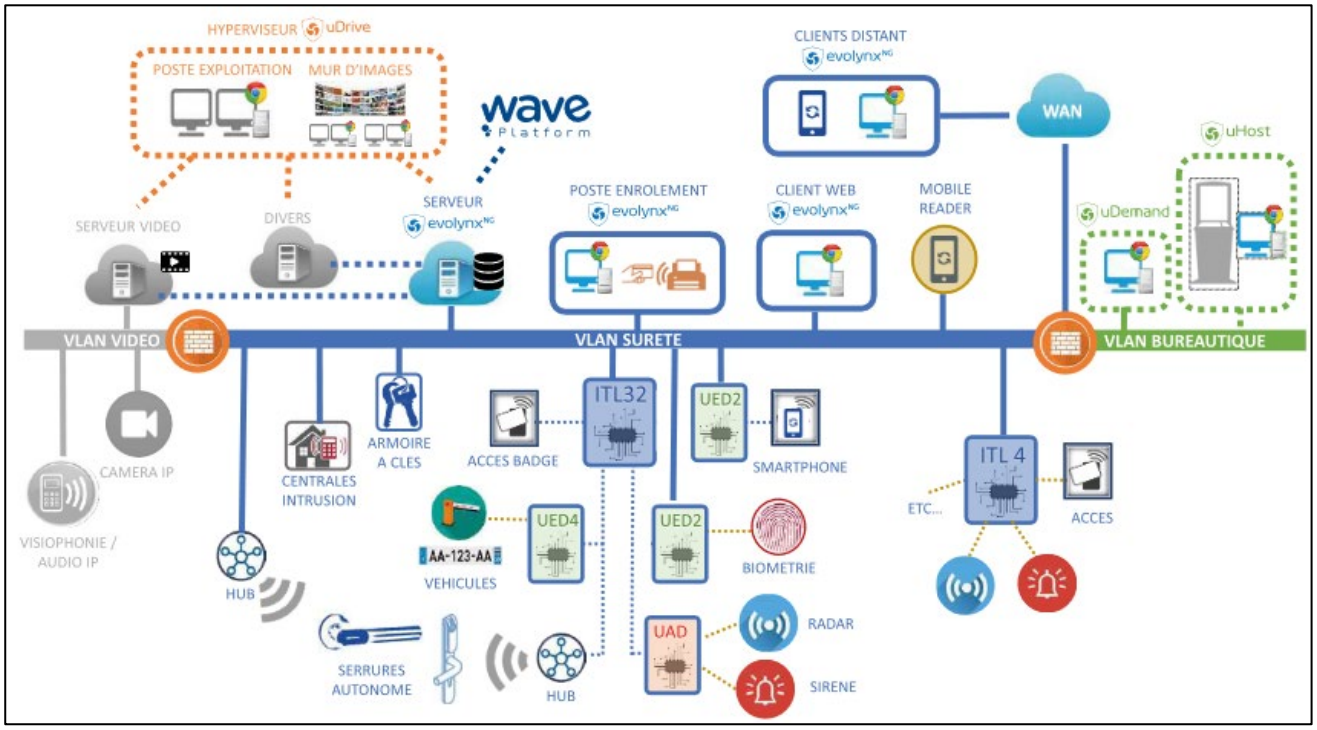


Figure 8 – Plan de l'architecture des solutions de Secure

4.1.1 Matériel

J'ai d'abord pu identifier les principaux composants physiques de la maquette et leurs fonctions (Figure 10).

Premièrement, la maquette est composée d'un module d'alimentation étant donné que le courant arrive en 230 V et que la maquette fonctionne sous 24 V, il est nécessaire de diminuer la tension.

Ensuite, j'ai identifié l'unique ITL 32 (Intelligence de Traitement Local) de la maquette. Cet élément permet de gérer 32 antennes à elle seule (d'où le numéro 32) de manière locale. Cela signifie que les vérifications d'identité sont réalisées sur la carte sans passer par le serveur. Ce mode de fonctionnement permet une plus grande rapidité de vérification et d'autorisation, mais peut également être source de faille de sécurité. En effet, si les vérifications de badges sont effectuées sur cet équipement, cela signifie que l'équipement doit être en mesure de déchiffrer les informations du badge. Ainsi, si une personne malintentionnée s'empare de l'ITL, il lui serait alors possible de réaliser un appareil de récupération des données de badges et ainsi usurper l'identité d'accédants.

Figure 9 – Une carte SAM

Afin de contrôler ce problème, il est possible, et même fortement recommandé par l'ANSSI voir obligatoire, d'installer une carte SAM (Secure Access Module) (Figure 9) sur l'ITL. Ainsi, les données des badges seront chiffrées et n'apparaîtront plus en clair dans l'ITL. Il sera seulement indispensable de sécuriser de manière physique, le poste d'encodage des cartes SAM.

La maquette est en plus composée d'une UED 4 et d'une UED 2 (Unité d'Equipement Déporté). Suivant le même principe que l'ITL, le chiffre suivant l'acronyme de l'équipement définit le nombre d'antennes que l'équipement peut gérer. Il est également possible d'ajouter une carte SAM à une UED afin de renforcer la sécurité des informations des badges qui transitent sur le système.

Enfin, 5 lecteurs de badge dont un lecteur avec clavier pour la tabulation d'un code pin sont reliés aux UED et à l'ITL. Ces lecteurs permettent de simuler des entrées/sorties de zone selon différentes configurations (il est par exemple possible de tester la mise en place et le fonctionnement de sas). Les lecteurs peuvent aussi ne pas servir de point d'accès, mais simplement d'antennes permettant la vérification d'informations qui peuvent être affichées sur des écrans déportés à l'attention, par exemple, d'un opérateur de sas ou d'un agent de sécurité, on appelle alors cela une IHM ou Interface Homme-Machine. Cette IHM permettra notamment à l'opérateur d'effectuer des actions directement sur l'accédant venant de badger. On retrouvera ce fonctionnement dans les sas piétons et véhicules.

Quatre boîtes à boutons sont également présentes sur la maquette et permettent de simuler des ouvertures/fermetures de porte. En effet, n'ayant pas de réelles portes à disposition, il est nécessaire d'actionner les interrupteurs manuellement afin de faire comprendre au système qu'une personne venant de badger a « emprunté » l'accès.

Je disposais également d'un encodeur et d'une imprimante de badges dont je ne me suis que très peu servi (Annexe 4 & Annexe 5).

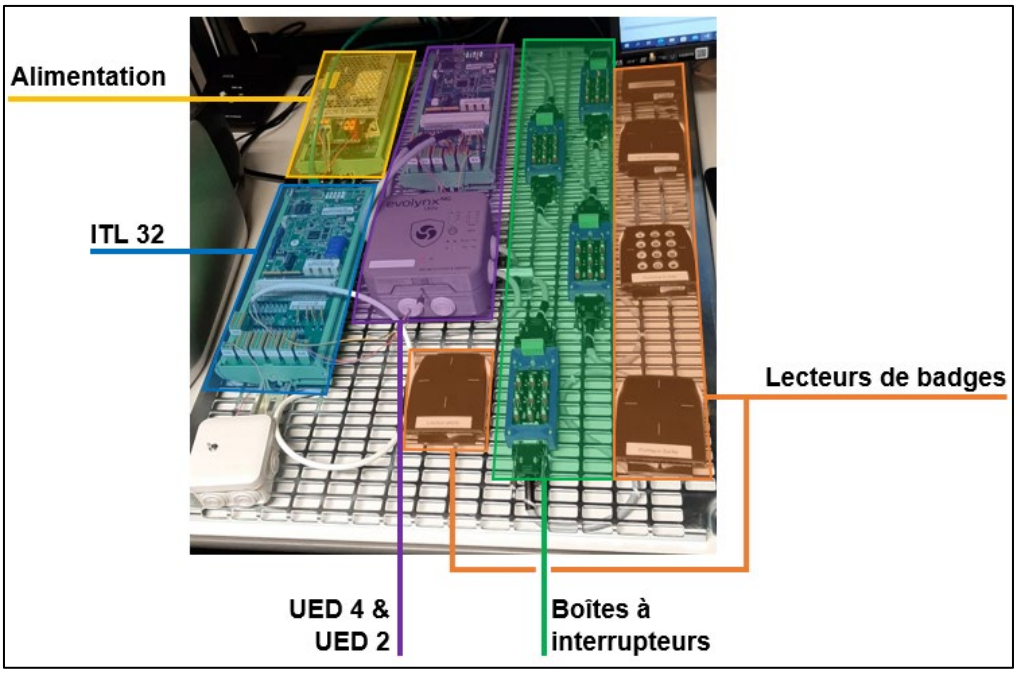


Figure 10 – Maquette de la solution Evolynx avec identification des composants

4.1.2 Logiciel

Concernant la partie logicielle, j'ai d'abord pu constater de manière quasi-immédiate qu'Evolynx gérait une grande partie de la sécurité d'un site de manière autonome.

Ce qui a ensuite été un critère majeur dans la différenciation des deux solutions (Secure et Genetec) n'est autre que la partie graphique. J'ai tout de suite remarqué que l'interface Secure (Figure 11), parce qu'elle est réalisée en HTML 5 et mettant le confort de l'utilisateur au premier plan, était plus sympathique à regarder, mais aussi qu'elle offrait une facilité de prise en main conséquente par rapport à l'interface de Security Center de Genetec (Figure 12). Ce point est important et dispose de sa propre exigence dans la matrice fonctionnelle.

En effet, bien qu'un hyperviseur auquel sera vraisemblablement raccordée la future solution choisie sur les nouveaux sites nucléaires, dispose de sa propre patte graphique, il faut s'imaginer que des opérateurs utilisent l'une des deux solutions tous les jours. Une interface épurée et moderne, permet non seulement de prodiguer aux équipes un environnement de travail plus plaisant, mais aussi d'économiser du temps précieux lors de la réalisation de tâches.

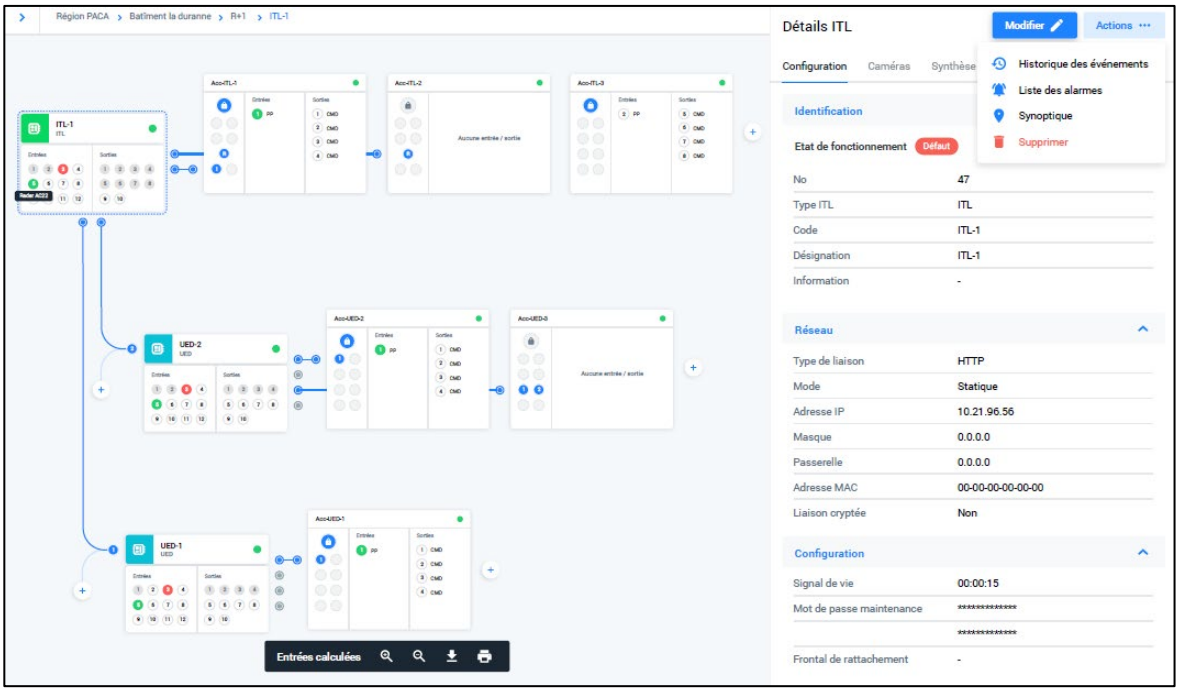


Figure 11 – Interface de création et d'attribution d'équipements d'accès d'Evolynx

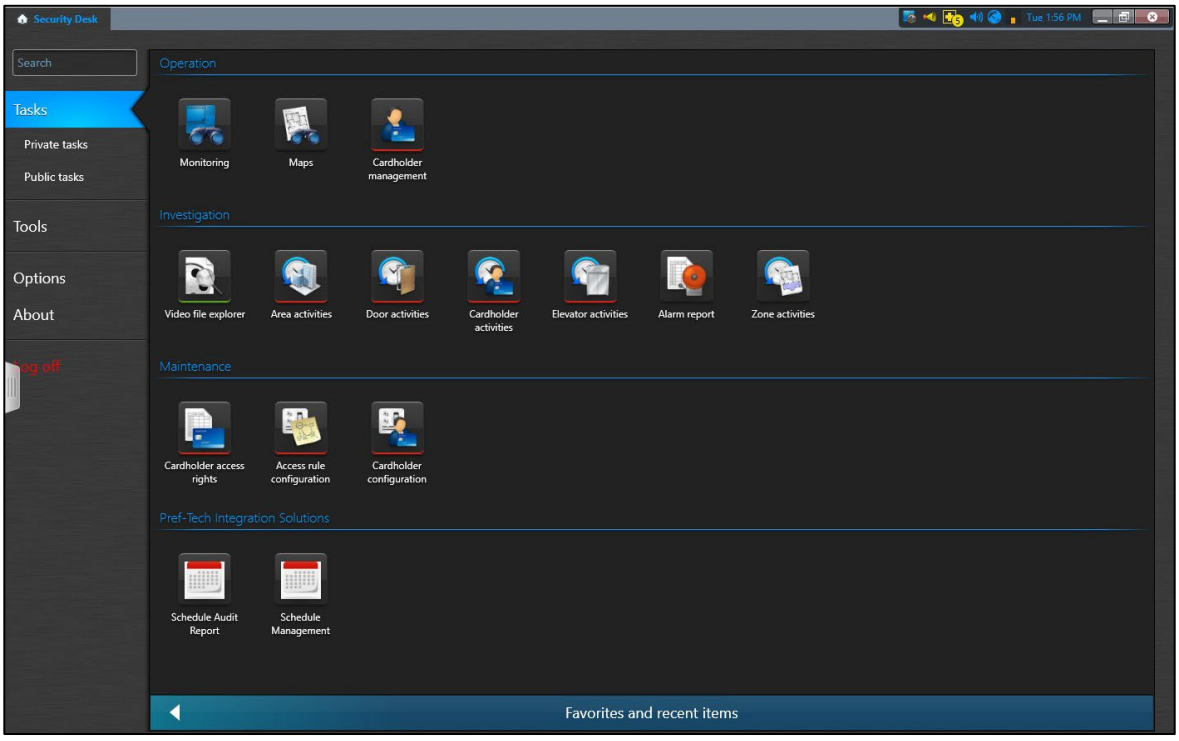


Figure 12 – Interface du Security Center de Genetec

4.2 Tests et vérifications de conformité aux exigences

Après avoir cerné la solution, tant d'un point de vue matériel que d'un point de vue logiciel, j'ai pu commencer à effectuer quelques tests afin de réellement m'approprier la maquette et, par la suite, de pouvoir effectuer les réels tests en vue de la validation ou l'invalidation des exigences de la matrice fonctionnelle.

J'ai ainsi pu ajouter des accédants, créer des badges et effectuer des demandes de visites.

Dès le début de ces tests, après un redémarrage de la maquette, le seul lecteur relié à l'ITL, permettant simplement d'afficher les informations d'un badge sur un écran déporté, s'est mis en échec. Il était donc devenu impossible de l'utiliser correctement. J'y ai vu l'opportunité de refaire de zéro le paramétrage d'un lecteur depuis l'interface graphique d'Evolynx et ainsi mieux comprendre le fonctionnement de l'interface d'ajout d'équipement.

Sur la page de création et d'attribution d'équipement d'Evolynx, j'ai dû ajouter un instrument directement connecté à l'ITL, configurer le type d'instrument (un lecteur) et lui attribuer une zone. En effet, si une personne badge sur le lecteur, mais que la zone dans laquelle il se trouve est hors des autorisations d'accès de la personne alors le lecteur refusera « l'accès » et un message notifiant l'opérateur du refus d'accès sera affiché en plus des informations de l'accédant sur l'écran déporté.

Au moyen de Use Case ou Cas d'Utilisation définis pour des parties importantes des exigences, j'ai pu structurer ma documentation et élaborer des cheminements logiques au sein même de la solution.

4.2.1 Gestion des accédants

Certaines exigences portaient sur la gestion des visiteurs et des accédants par le poste d'accueil. Elles stipulent notamment que « le système doit pouvoir octroyer des droits d'accès […], imprimer et encoder un badge ». Il est nécessaire que ces actions soient effectuées avec un double contrôle afin d'éviter la complicité interne, c'est-à-dire qu'une personne malintentionnée puisse obtenir un badge à l'aide d'un complice seul ayant des droits de création et de distribution de badge.

J'ai vite remarqué, au cours de mes tests, mais aussi en réponse à mes questions de la part de Secure lors des réunions de mise au point, que la gestion des accédants et l'attribution de droits en plus, à destination des personnes possédant un BNU (Badge National Unique) et souhaitant rentrer sur un site, ne pourrait pas passer par un double contrôle et que celui-ci était uniquement possible pour les demandes de visite. Il n'est pas possible d'attribuer des demandes de visite à des BNU et ainsi pouvoir utiliser le double contrôle pour l'attribution de nouveaux droits d'accès, tout simplement car seuls les badges non attribués peuvent être appairés à des demandes de visite.

Ainsi, j'ai commencé la manipulation des paramètres de la solution Evolynx afin de monter un système de double contrôle pour les demandes de visite, servant notamment à la vérification des informations de visiteurs temporaires ne disposant pas de badge.

Etant donné la manière dont les permissions des utilisateurs d'Evolynx sont pensées, j'ai pu dissocier la validation des demandes de visite à leur création et à l'encodage de badge.

J'ai donc réalisé un diagramme résumant le processus logique d'obtention d'un badge lié à une demande de visite avec un double contrôle des informations (Figure 13).

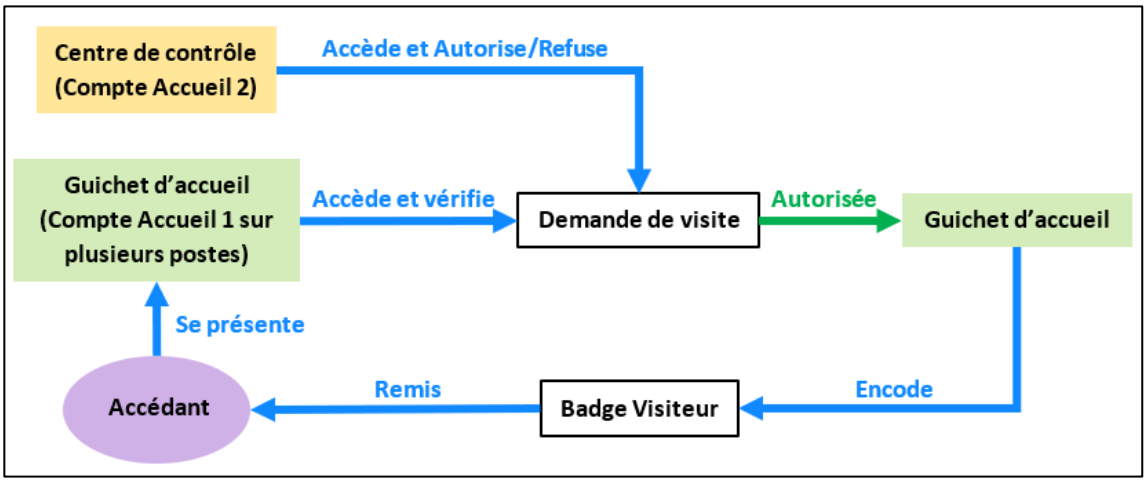


Figure 13 – Diagramme d'obtention de badge avec double contrôle

Ce double contrôle n'est pas parfait puisqu'il ne permet pas la vérification de la correspondance entre la pièce d'identité et l'accédant par une tierce personne. Néanmoins, il permet de s'assurer qu'une personne seule ne puisse pas accueillir un visiteur et lui fournir des accès. En effet, la demande de visite est soit créée par l'accueil, soit déjà enregistrée dans le système Evolynx suite à son importation depuis APS (Accueil Protection de Site). Ensuite, pour pouvoir attribuer un badge libre à une demande de visite, il est nécessaire que celle-ci soit autorisée. Or, seul le centre de contrôle peut autoriser ou refuser les demandes de visite et seul l'accueil peut attribuer des badges et les encoder avec les informations de l'accédant et les droits liés à la demande de visite.

De ce fait, le centre de contrôle seul ne peut pas attribuer des badges à des accédants et il en est de même pour le guichet d'accueil.

Lors des tests effectués avec la gestion des accédants et le double contrôle, je me suis rendu compte que dans certains cas, le compte destiné au centre de contrôle se faisait brutalement déconnecter. Je me suis alors penché sur le système des permissions et j'ai commencé à en ajouter et à en retirer successivement afin de trouver l'origine du problème. En effet, la déconnexion ne survenait que dans un cas très précis : lorsque le compte tentait de visualiser les informations d'un visiteur rattaché à une demande de visite.

Après quelque temps à passer et repasser sur les permissions, j'ai finalement trouvé la source du problème. Il n'est pas nécessaire que le centre de contrôle puisse créer des demandes de visites étant donné que celles-ci sont soit créées par l'accueil ayant un contact direct avec l'accédant, soit importées automatiquement depuis APS à partir d'un fichier CSV (Comma-Separated Values). Ainsi, je n'avais pas activé la permission permettant de créer des demandes de visites pour le compte du centre de contrôle. Dès lors que je l'eusse activée, le problème n'est plus survenu.

Ce que je trouvais curieux dans ce problème, c'est que la permission permettant à un utilisateur de simplement consulter les informations d'un visiteur ou d'une demande de visite existe bel et bien et permettrait en toute logique d'autoriser seule la fonction qu'elle décrit.

J'ai donc contacté les responsables du produit Evolynx pensant avoir manqué quelque chose dans la configuration de la solution. Je leur ai ainsi fourni ma démarche et les permissions utilisées afin qu'ils puissent tenter de reproduire le problème sur leur plateforme.

Il s'est avéré que c'était bel et bien un problème, qui plus est, inconnu de leur part. Mon signalement et les informations que j'ai pu leur communiquer leur permettront de corriger ce bogue lors de leur prochaine mise à jour corrective.

4.2.2 Sas

Certains accès d'un site industriel, se doivent de fonctionner sous la forme de sas, et ce, afin de protéger au mieux les zones accessibles. On pourra par exemple trouver un sas véhicule dans le PAC et un sas piéton au niveau de la ZV (Zone Vitale) de la centrale ou juste avant le PCP.

Afin de m'aider à bien cerner le fonctionnement des sas et ainsi mieux appréhender leur technicité et leur intégration dans la solution proposée par Secure, j'ai réalisé plusieurs diagrammes montrant les différentes configurations de sas.

Les sas véhicules présents sur le PAC ne permettent pas, comme cela est le cas pour certains accès piéton, de contrôler les portails directement via un lecteur. C'est en effet le poste de contrôle et les opérateurs qui actionnent eux-mêmes l'ouverture et la fermeture des portails (Figure 14).

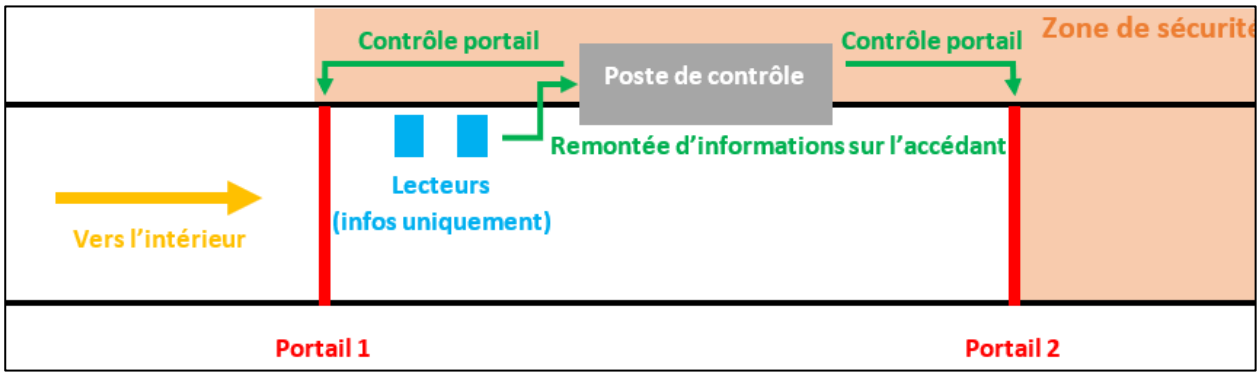


Figure 14 – Schéma d'un sas véhicule

Concernant les sas piétons, les choses se compliquent un peu. En effet, il peut y avoir des sas à deux voire, trois portes, disposant d'autant de zones de sécurité différentes. Ainsi, le fonctionnement des sas piétons est plus technique, car, tantôt, les lecteurs fonctionnent comme des ouvre-portes, tantôt comme simples interfaces servant à remonter des informations sur l'IHM de l'opérateur comme cela est déjà le cas d'office pour les lecteurs de sas véhicule.

Ainsi la configuration d'un sas piéton à deux portes et deux zones de sécurité (la zone extérieure est aussi comptée comme étant une zone de sécurité) est ce qui se rapproche le plus du fonctionnement d'un sas véhicule (Figure 15).

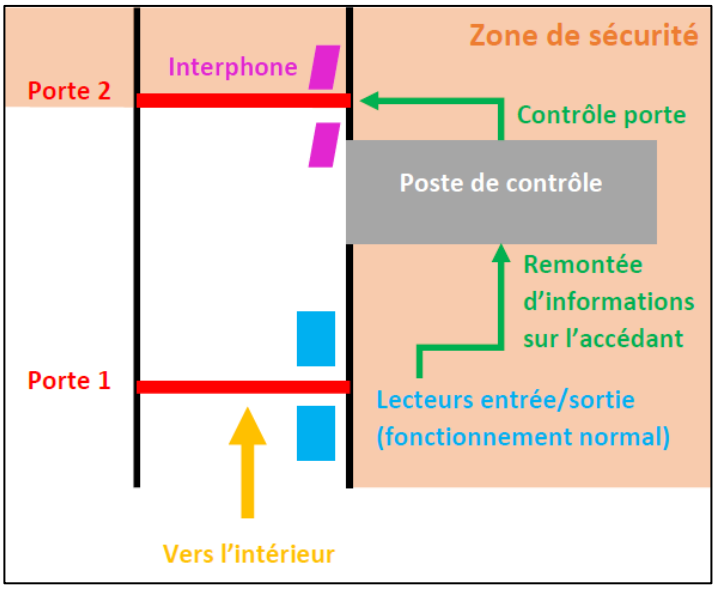


Figure 15 – Schéma d'un sas piéton à deux portes et deux zones de sécurité

Il est important de noter que les sas piétons à deux et trois portes avec deux zones de sécurité (Figure 15 et Figure 16) disposent d'interphones non seulement à l'intérieur du sas, mais également à l'extérieur de celui-ci dans la zone sécurisée. En effet, dès lors qu'une personne se trouve dans la zone sécurisée, il n'y a pas de risque à la faire passer par le sas pour rejoindre la même zone par une porte différente ou pour sortir complètement des zones sécurisées. Ainsi, les interphones servent d'interfaces de communication avec le poste de contrôle et sont en général reliés à des caméras.

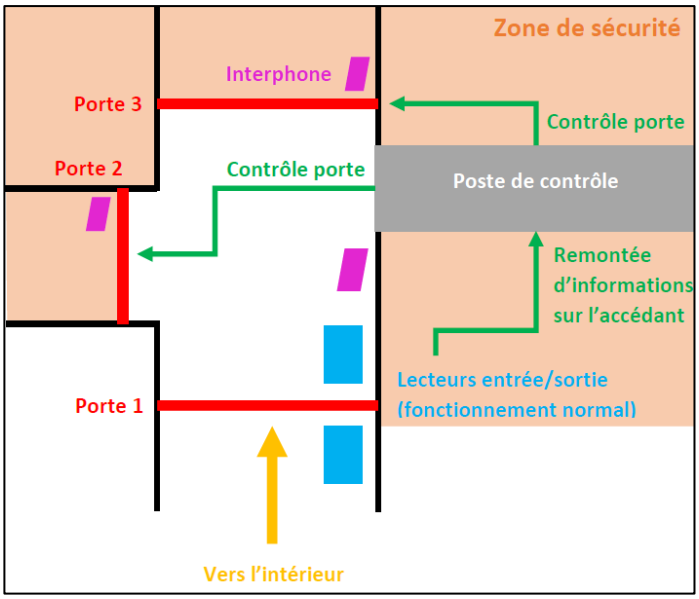


Figure 16 – Schéma d'un sas piéton à trois portes et deux zones de sécurité

Dans le cas d'un sas piéton à trois portes et trois zones de sécurité (Figure 17), le positionnement des lecteurs et des interphones est inversé. En effet, si une personne venant de la zone sécurisée A souhaite se rendre dans la zone sécurisée B, elle devra sortir de la zone A au moyen de son badge, rentrer dans le sas, puis entrer dans la zone B au moyen, encore une fois, de son badge.

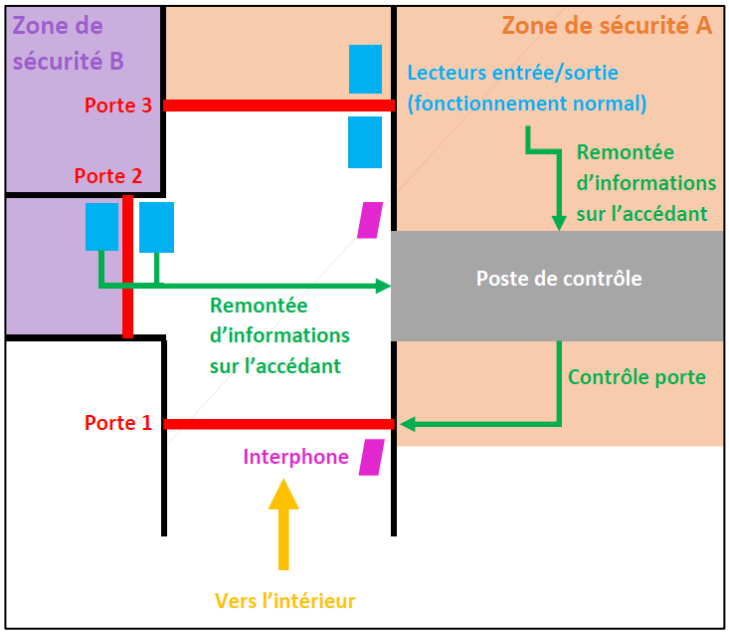


Figure 17 – Schéma d'un sas piéton à trois portes et trois zones de sécurité

Je me suis ensuite penché sur la prise en charge des fonctionnalités des sas dans la solution Evolynx.

Il est primordial que le système prenne en compte le changement de zone de l'accédant. En effet, si une personne est présente dans une zone elle ne peut pas rebadger pour rentrer dans la même zone, et ce, afin d'éviter que le badge ne soit envoyé à une tierce personne en dehors de la zone et qu'il serve à la faire rentrer. C'est ce que l'on appelle l'APB ou l'Anti PassBack, soit l'interdiction de rentrer deux fois dans la même zone si l'on n'en est pas sorti. Il existe aussi l'APB temporel afin d'éviter qu'une personne ne simule une sortie de zone et que son badge ne serve à faire rentrer une tierce personne dans la même zone dans un lapse de temps relativement court.

Il n'est cependant pas possible de réaliser ce changement de zone dans le système avec des lecteurs servant à la simple remontée d'informations sur une IHM. L'opérateur a donc besoin de manuellement transférer la personne présente dans le sas dans une zone différente.

Dans la solution, il est prévu une option permettant à l'opérateur, depuis son IHM qui affiche les informations des accédants (fonctionnalité ValidAccess d'Evolynx), de transférer une personne qui badgerait sur un lecteur du sas d'une zone à une autre et ainsi s'assurer que l'accédant se trouve bien dans la nouvelle zone aux yeux du système. Cette option n'est néanmoins pas définie à ce jour.

4.2.3 Borne visiteurs

Dans les exigences d'EDF, il est noté qu'il faut qu'une borne soit disponible à l'accueil pour gérer la gestion de la file d'attente et l'auto-enregistrement des personnes possédant déjà un BNU (Figure 18).

BORNE	Ticketing	Dans ou hors du système, une borne permet de distribuer des tickets dans le but de d'accèder au guichet d'accueil et prioriser la charge.

Figure 18 – Exigence mentionnant la nécessité d'un système de gestion de file d'attente

La solution proposée par Secure comprend deux autres logiciels : uHost et uDemand. Dès le début de la prise en main, je me suis attelé à comprendre le fonctionnement, l'implémentation et les contraintes de chacune des briques proposées par Secure.

N'arrivant pas à cerner l'utilité et le fonctionnement de ces deux parties, je me suis concentré sur Evolynx, brique la plus importante de la solution.

Après avoir effectué le gros du travail et des tests sur Evolynx, je suis revenu sur ce qui, d'après les documents fournis par Secure, permet de gérer des bornes à destination de visiteurs.

J'ai tout de suite pris l'initiative de noter les différentes questions qui me traversaient l'esprit afin de les poser lors d'une réunion avec les responsables de la solution chez Secure.

Au terme de cet échange, j'ai pu comprendre plusieurs choses :

- uHost est un système de borne hébergé sur uDemand. Il est donc possible de l'afficher sur un écran monté sur un piédestal à destination des visiteurs pour que ceux-ci puissent interagir avec le système.
- uDemand est une version allégée et bureautique d'Evolynx qui ne permet d'effectuer que certaines fonctions, notamment la gestion des visiteurs.

Une fois cela acquit, j'ai pu un peu plus creuser dans le fonctionnement et l'interconnexion des systèmes entre eux. J'ai remarqué que uDemand permettait de créer des visiteurs et des demandes de visites et qu'il était possible d'importer des visiteurs et des demandes de visites via un fichier CSV. Cependant, cela n'a pas été sans problèmes.

En effet, tantôt le système ne reconnaissait pas les champs renseignés dans le fichier CSV, tantôt le système ne trouvait pas de correspondance entre les informations à importer et celles déjà enregistrées.

Par exemple, il est demandé, pour l'importation d'une demande de visite, de renseigner la catégorie attribuée au visiteur. Celle-ci permet d'attribuer automatiquement des droits et d'activer ou désactiver des fonctionnalités dans le système qui dépendent des catégories. Ainsi, pour les tests de la solution, on retrouvera par exemple les catégories Visiteur, Prestataire et Permanent, mais il est possible d'en créer plus. La catégorie d'un visiteur doit être obligatoirement renseignée dans le fichier CSV.

Lorsque j'essayais d'importer mes données renseignées dans le fichier CSV, le système renvoyait le message d'erreur *PERSON_CAT_NOT_FOUND*. Ce message signifie bien que la catégorie de la personne que j'ai tenté d'importer depuis mon jeu de données n'est pas une catégorie enregistrée dans le système. uDemand ne la reconnaît donc pas et ne peut pas procéder à l'importation. J'ai longuement essayé de résoudre ce problème en modifiant les noms des catégories, l'ordre des champs de données aussi bien dans uDemand que dans le fichier CSV afin de m'assurer qu'ils soient en phase, mais rien.

Une autre erreur s'est ajoutée à la liste indiquant *VISIT_VISITOR_MANDATORY*, soit qu'un visiteur doit être obligatoirement renseigné dans la demande de visite, ce qui était déjà le cas.

N'arrivant pas à trouver la solution, j'ai encore une fois pris avantage d'une réunion avec les fournisseurs afin de leur expliquer mon point de blocage. Après m'avoir expliqué la subtilité dans l'ordre de placement des champs dans uDemand, j'ai pu correctement réorganiser les données dans le fichier CSV et dans la solution. Les données se sont alors importées dans problème !

Il est également possible d'importer des données, telles que : des badges, des demandes de visites, des personnes et des sociétés dans la solution Evolynx. Les données formulées dans uDemand peuvent également faire l'objet d'une exportation automatique vers Evolynx afin de lier les deux systèmes. Cependant, uDemand fonctionne exclusivement comme une source de données et n'est donc pas en capacité d'importer de manière automatique des informations comme j'ai pu le faire manuellement et c'est là que réside le problème majeur de uDemand et uHost.

En effet, dans les exigences, il est demandé que les informations soient importées dans le système depuis APS de manière automatique. Ainsi, il existe un roulement régulier permettant aux données d'être synchronisées, non seulement entre tous les sites EDF (puisque si un BNU est renseigné comme étant volé dans un site, il ne faut pas que le voleur du badge puisse rentrer dans un autre site), mais aussi avec APS.

Le fait que uDemand ne puisse pas importer automatiquement des données, ce que peut faire Evolynx de manière native, a été abordé lors de réunions avec Secure. Néanmoins, la solution proposée était de développer un autre script afin que uDemand puisse recevoir des données de manière automatique ce qui n'était pas souhaitable.

Afin de tenter de remplir les exigences de la borne, je me suis vu confier une nouvelle mission de recherche.

4.3 Deuxième mission : recherche de solutions du marché

L'objectif était alors pour moi de chercher sur le marché des solutions de bornes d'accueil des visiteurs avec certaines exigences séparées dans deux catégories :

- Les solutions d'accueil des visiteurs et de simple gestion de la file d'attente (similaire à ce qu'on peut retrouver dans les hôpitaux)
- Les solutions plus poussées avec lecteurs de cartes d'identité, imprimantes de badges, gestion de la file d'attente et interfaçage avec la solution de contrôle d'accès mise en place (ici Secure ou Genetec) afin d'utiliser les informations du système

J'ai d'abord cherché du côté de la simple gestion de la file d'attente.

Beaucoup d'entreprises proposent ce type de solution de manière plus ou moins poussée. Mon attention s'est alors portée sur la solution de l'entreprise Xifab (Figure 19) qui permet notamment :

- La gestion de la file d'attente et des priorités ;
- La lecture de badge ;
- La prise de photo avec une webcam ;
- L'affichage de la file d'attente sur un écran déporté.

Figure 19 – Logo et borne Xifab

L'aspect modulaire des bornes conçues permet aux clients de choisir les modules dont ils ont besoin en rajoutant par exemple une imprimante à ticket pour connaître son numéro dans la file d'attente voire un terminal de paiement.

Néanmoins, cette solution n'offrait pas d'interfaçage avec les solutions de contrôle d'accès, de lecteur de pièce d'identité ni même d'imprimante à badge ou d'encodeur.

Au fil de mes recherches, je me suis rapidement rendu compte que les bornes qui permettaient la gestion d'une file d'attente n'offraient pas d'option d'impression de badge, ni même de lecteur de carte d'identité pourtant essentiel dès lors qu'une personne possédant déjà un BNU souhaite vérifier ses accès (il n'est pas envisageable qu'une personne ayant trouvé un badge ne lui appartenant pas, puisse, grâce à ces bornes, connaître les permissions qui y sont associées et obtenir les informations de la personne réellement détentrice du badge).

Du côté des solutions offrant des solutions avec lecteurs de pièces d'identité, je me suis à nouveau heurté à un problème de taille : pas de mention d'interfaçage avec une solution de contrôle d'accès.

Je suis donc allé voir du côté des partenaires technologiques de Genetec. Là, j'y ai trouvé trois solutions de bornes d'accueil qui s'interfacent nativement avec le système de contrôle d'accès. Dont une qui est sortie du lot, vendue par l'entreprise Splan (Figure 20), cette solution permet de :

- Lire et encoder des badges ;
- Lire une pièce d'identité ;
- Prendre une photo et réaliser une comparaison avec la pièce d'identité.

Figure 20 – Logo et borne Splan

Cette solution se vend comme étant parfaitement intégrée à Genetec et se déployant On Premise, à l'inverse d'autres solutions qui n'étaient qu'exclusivement des SaaS (Software as a Service).

Le seul inconvénient de cette borne et des autres bornes pouvant lire des pièces d'identité et s'interfaçant avec des solutions de contrôle d'accès, est qu'elles ne gèrent pas la file d'attente. Elles fonctionnent de manière autonome pour ainsi dire, sans que l'intervention de l'accueil, afin de délivrer un badge ou vérifier des informations, ne soit nécessaire.

J'ai finalement réalisé une présentation PowerPoint à destination de l'équipe contenant toutes les informations essentielles sur mes recherches afin qu'il soit plus simple de lancer les discussions avec les fournisseurs et de faire des choix.

4.4 Documentation et exigences

Au fur et à mesure de mes tests et recherches, j'ai réalisé une documentation sur les points clés de la solution Evolynx qui contient des instructions pas-à-pas sur la réalisation de certaines opérations comme la création de demandes de visite, la création de badges (Figure 21), l'ajout d'équipements ou encore l'importation des données.

La documentation sert également de retour d'expérience, j'ai pu y écrire mes constatations, tout en gardant une approche neutre vis-à-vis de la solution afin de ne pas influencer mon raisonnement. Ainsi, j'ai pu par exemple expliquer aussi bien sous forme de court résumé concis que de manière détaillée, le fonctionnement de la borne proposée par Secure et les divergences avec nos besoins.

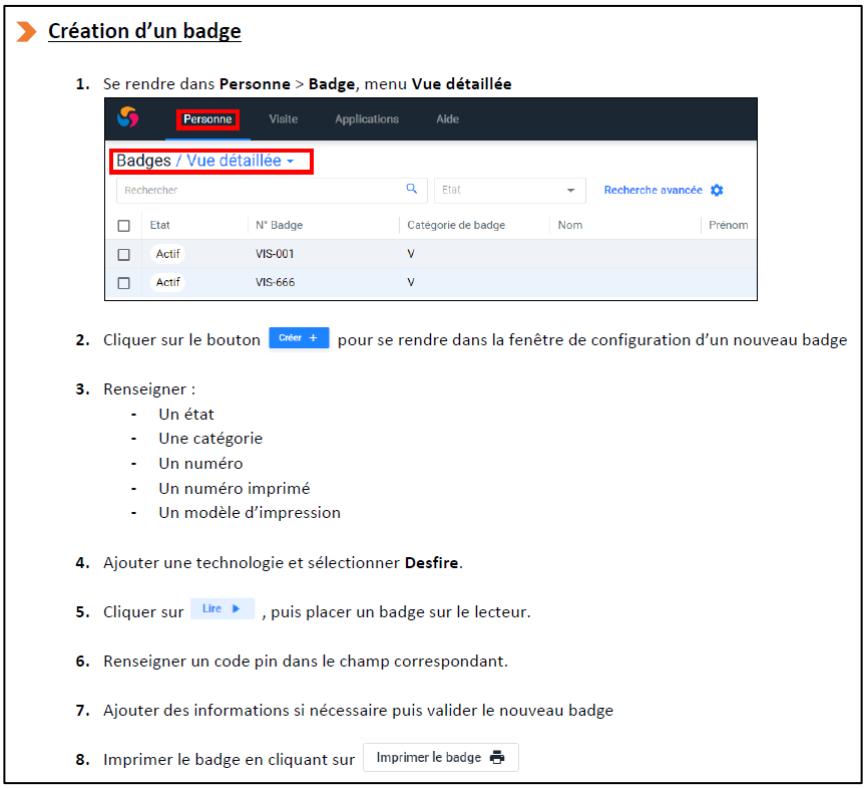


Figure 21 – Documentation pas-à-pas dur la création d'un badge

Au fil de mes tests, j'ai effectué le remplissage la matrice fonctionnelle en fonction de la réponse de la solution aux exigences en suivant un code couleur établi, et ce, afin de faire le parallèle entre les deux solutions (Figure 22).

Indicateur	Description	Aide		Note
	Fonctionne et respecte le processus	=	100%	3
	Fonctionne mais impose une adaptation du processus	>=	80%	3
	Fonctionne via des mécanismes offerts dans la solution mais détournés de l'utilisation standard. Problème de performance, d'optimisation, etc	>=	70%	2
	Fonctionne partiellement	>=	40%	1
	Ne fonctionne pas	<	40%	0
	Non déterminé			
	Non testable			

Figure 22 – Code couleur des réponses aux exigences

J'ai pu également réaliser un autre document reprenant chaque exigence de la matrice en ajoutant des recommandations basées sur mes tests et le retour d'expérience. Ainsi, j'ai été amené à proposer de nouvelles exigences afin de prendre en compte les spécificités de la solution et les différents tests menés.

Conclusion

Malgré les retards d'approvisionnement des briques de la solution (notamment l'hyperviseur afin d'utiliser la fonction de vidéosurveillance) ne me permettant pas de réaliser la totalité des tests, ce stage m'aura permis d'approfondir mes connaissances en termes de conduite d'un projet, qui plus est de grande envergure.

Même si je n'ai pas concrètement utilisé de compétence technique afin de réaliser les tâches qui m'étaient confiées, les capacités de raisonnement, de synthèse et d'adaptation que mes années d'études m'ont permis d'acquérir, m'ont été d'une grande aide, voire indispensables dans la réalisation de mes missions.

Les différentes missions qui m'ont été confiées au fil de ces dix semaines de stage, m'auront permis de me familiariser avec la réalisation de documents d'exigences, de comptes-rendus et de documentations, mais aussi d'animation de réunions aussi bien de mises au point qu'avec des fournisseurs, d'apporter mon retour et mes propositions.

J'ai pu, au travers de ce stage, du projet et des missions qui m'ont été confiées, découvrir le processus d'études. Cette découverte des rouages qui font la réalisation d'un projet conséquent (appropriation de la solution, tests et vérifications de la conformité du produit avec les attentes de l'entreprise, retours et propositions d'améliorations), m'a apporté de nouvelles perspectives d'avenir en élargissant mon champ de vision professionnel.

Remerciements

Je remercie Mme Delphine QUINTIN – Cheffe du groupe IIS de m'avoir accepté en tant que stagiaire au sein de son groupe, ainsi que tous les membres du CNEPE avec lesquels j'ai pu travailler, m'enrichir et qui m'ont accompagné dans mes travaux.

Je voudrais tout particulièrement remercier mon tuteur de stage M. Clément HERVE – Ingénieur au sein du groupe IIS, pour ses explications, ses compétences et connaissances qu'il m'a partagées, et pour sa présence et son encadrement.

Enfin, je remercie mon tuteur académique M. Ivan MADJAROV pour son encadrement et plus globalement toute l'équipe pédagogique de l'IUT Réseaux & Télécommunications pour leurs conseils, leurs enseignements et leur encadrement.

Glossaire

EDF : Electricité de France

DETU : Département Etudes

CIS : Contrôle Commande et Installations Electriques de Surveillance

DIPNN : Direction Ingénierie et Projets Nouveau Nucléaire

CNEPE : Centre National d'Equipement de Production d'Electricité

IIS : Informatique Industrielle Sécuritaire

CNPE : Centre Nucléaire de Production d'Electricité

Progiciel : Logiciel standard disponible sur le marché permettant plusieurs usages.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

IGI 1300 : Instruction Générale Interministérielle N°1300 sur la protection du secret de la défense nationale.

VMS : Video Management System. Système fédérateur de flux de vidéosurveillance.

Databook : Dossier contenant tous les éléments et documents relatifs aux projets qui auront été réalisés durant toutes les étapes de celui-ci.

OIV : Opérateur d'Importance Vitale

ZAC : Zone d'Accès Chantier

PAC : Poste d'Accès Chantier

POC : Proof Of Concept. Preuve concrète que les exigences avancées sont réalisables et fonctionnent

ZV : Zone Vitale

Hyperviseur : Logiciel permettant de fédérer plusieurs solutions (ici de sécurité) au sein d'une même interface et de les faire communiquer entre elles

IHM : Interface Homme-Machine

Showroom : Espace de présentation destiné

ITL : Intelligence de Traitement Local

UED : Unité d'Equipement Déporté

SAM : Secure Access Module. Carte servant à gérer la gestion des clés, le chiffrement et le déchiffrent des informations, notamment des cartes à puce, de manière sécurisée

Use Case : Cas d'Utilisation. Définition de la manière d'utiliser un système

BNU : Badge National Unique. Un seul badge propre à chaque personne et utilisable sur tous les sites EDF

APS : Accueil Protection de Site. Fichier permettant l'inscription d'informations en vue d'une demande d'accès ou de visite sur un site EDF.

CSV : Comma-Separated Values. Type de fichier de données sous forme de texte où les valeurs sont séparées par des virgules

On Premise : Est dit d'une solution qui peut être déployée de manière locale à l'échelle d'un site et ne pas se baser sur le cloud assurant ainsi la sécurité des informations confidentielles hébergées

SaaS : Software as a Service. Est dit d'une solution basée uniquement sur le cloud et ne pouvant être déployée localement de manière physique.

Bibliographie

Plaquette de présentation d'EDF

Plaquette de présentation du CNEPE

Site d'EDF [Consulté en Juin 2023], via https://edf.fr

Site intranet VEOL (Vivre EDF On Line)

ANSSI IGI 1300 [Consulté en Juin 2023], via https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/

Site de Secure [Consulté en Juin 2023], via https://secure-systems.fr

Plaquette d'information d'Evolynx (Secure) [Consultée en Avril 2023], via https://www.secure-systems.fr/wp-content/uploads/2023/01/Evolynx-NG-PL-FR-Plaquette-evolynx-NG-C.pdf

Note technique d'Evolynx pour l'ANSSI [Consultée en Juin 2023], via https://www.ssi.gouv.fr/uploads/2020/12/cible-cspn-2020_39.pdf

Site de Genetec [Consulté en Juin 2023], via https://genetec.com

Site de Splan [Consulté en Juin 2023], via https://www.splan.com

Site de Xifab [Consulté en Juin 2023], via https://www.xifab.com

Institut Universitaire de Technologie,
Aix-Marseille Université

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

Analyses et études au sein d'un progiciel de gestion de la sécurité de sites industriels

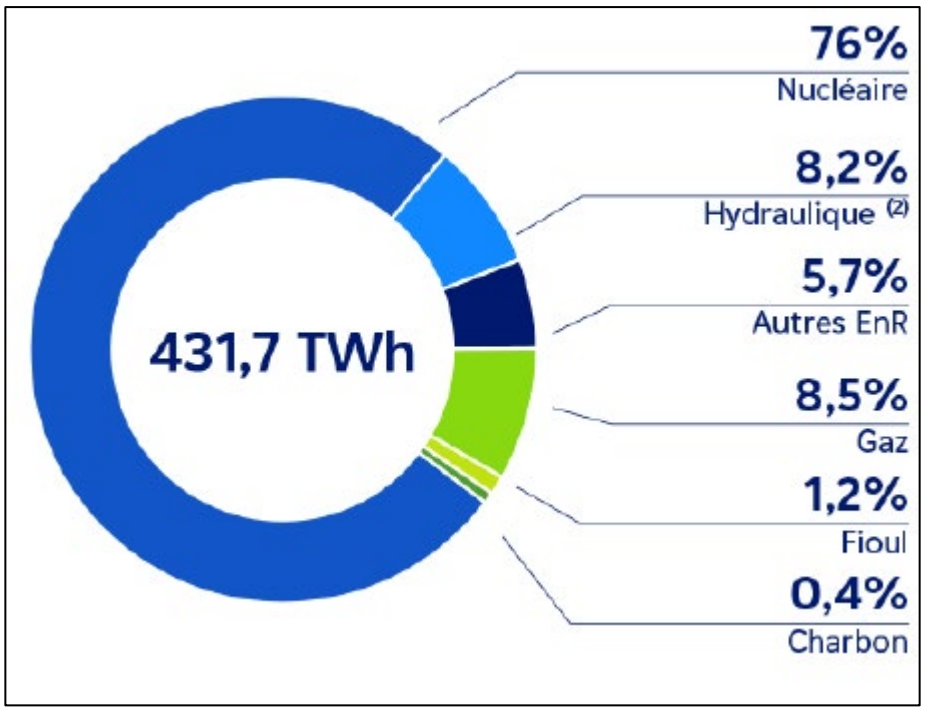
Nolan BEN YAHYA

EDF CNEPE

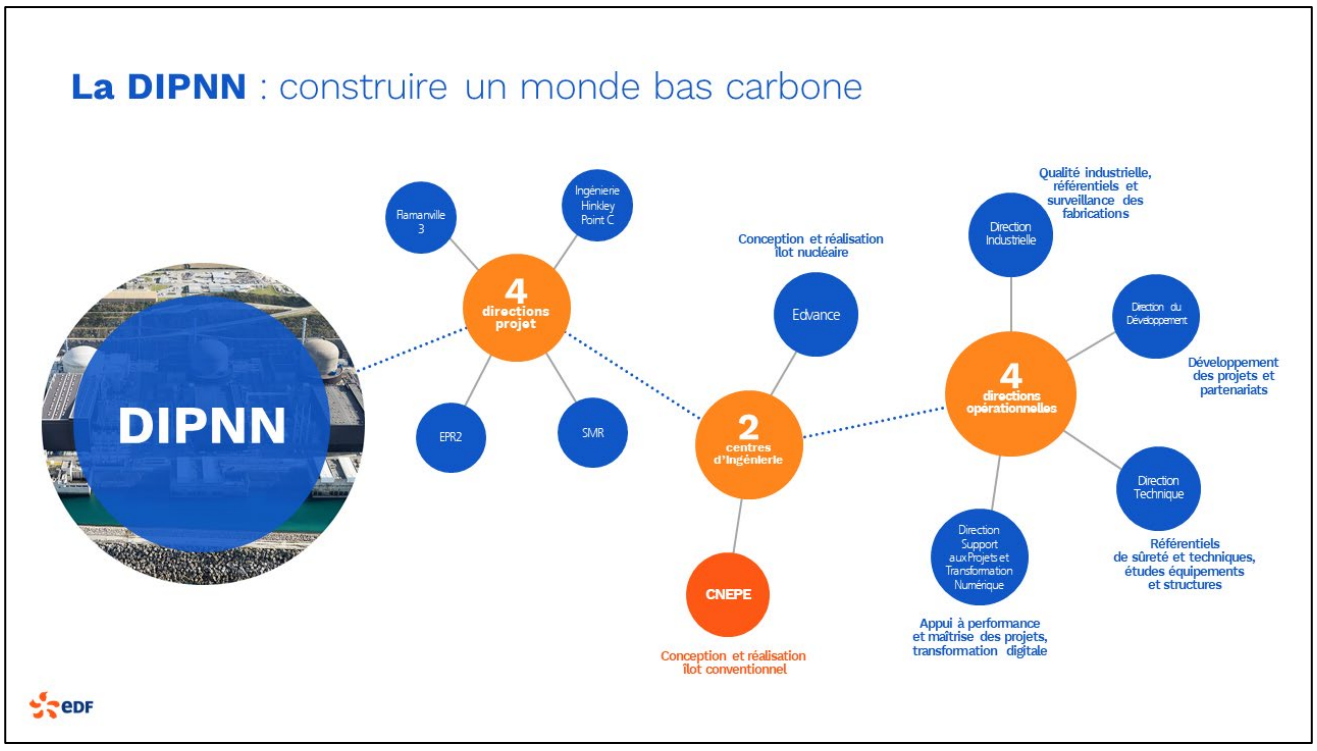
Responsable entreprise : Clément HERVE

Responsable académique : Ivan MADJAROV

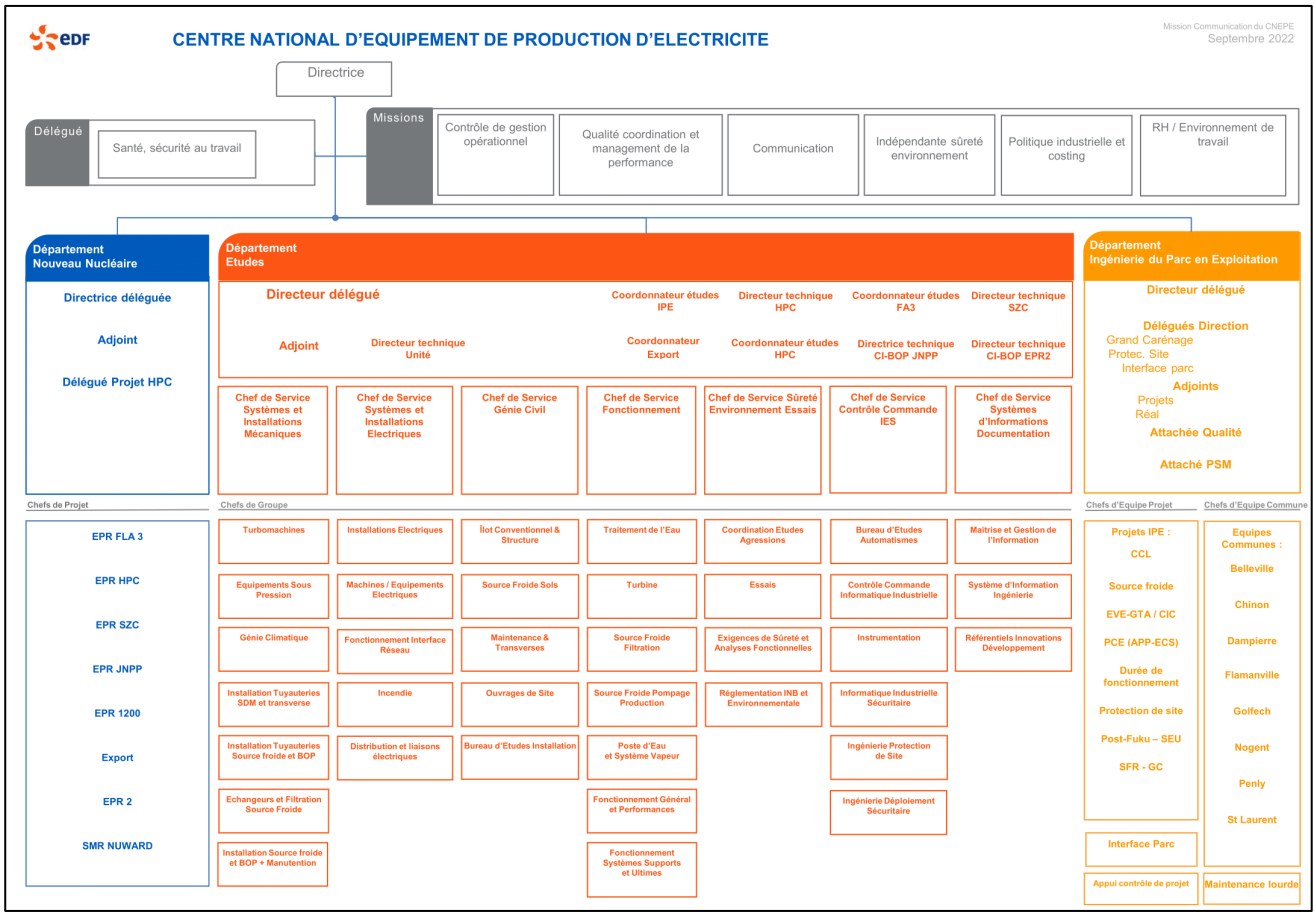
Annexes



Annexe 1 – Mix de production d'EDF par filière (en TWh, 2022)



Annexe 2 – Organigramme de la DIPNN



Annexe 3 – Organigramme du CNEPE

Annexe 4 – Un encodeur de badge Omnikey

Annexe 5 – Une imprimante à badges Zebra