Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Conception et validation du Contrôle Commande Appui à la mise en œuvre et à la modélisation d'une architecture réseau d'une centrale nucléaire

VISITTHIDETH Lau Jacky

Responsable entreprise : Didier PAQUET

Responsable académique : Éric SOCCORSI

2019

Table des matières

I. Introduction

Dans le cadre de mon DUT Réseaux & Télécoms, j'ai effectué un stage de fin d'études dans le domaine du réseau, durant la période du 8 Avril au 14 Juin au sein de **EDF-DIPDE** (Electricité de France - Division de l'Ingénierie du Parc nucléaire, de la Déconstruction et l'Environnement) à Marseille.
Ce stage me donne la possibilité de me former au métier d'ingénieur réseau et système, et me semble parfaitement cohérent au vu de mon parcours scolaire et me permettrait d'exploiter au mieux mes connaissances en lien avec ma formation.

La mission d'appui à la mise en œuvre et à la modélisation d'une architecture réseaux dans le domaine industriel m'a paru particulièrement intéressante, sachant qu'elle s'applique dans le cadre d'un projet dans le contexte de rénovation des réseaux des centrales nucléaires.
Cela consiste-en :

- Modélisation des flux de données et des équipements sur l'outil MEGA
- Mise en place d'un port-mirroring et s'assurer d'un transfert FTPS (*File Transfer Protocol Secure*) en mode passif
- Relevé de fiche d'identité des postes d'administrations et des serveurs
- Configurations des switchs et des firewalls, et de la réinstallation des serveurs
- Test de performance d'un boitier de coupure : DENELIS (Diode réseau)
- Migration d'un serveur par la mise en place d'un NAT (*Network Address Translation*)
- Mise en place d'une plateforme CTT (*Compliance Test Tools*) d'OPC UA

Ainsi, cette mission pourra me permettre de valider mes connaissances en réseau, en cybersécurité et en administration système, cela me permettra de découvrir les architectures mises en place dans un contexte de cybersécurité.

Par conséquent, j'ai eu l'opportunité de faire mon stage au sein d'EDF, leader dans la production et la vente d'électricité en France.
Entre autres, EDF est en plein cœur des débats actuels, sur des sujets tels que sa renationalisation et le débat des énergies polluantes face aux énergies renouvelables. Par ailleurs, l'importance des centrales dans notre quotidien n'est plus à prouver (elle représente 75% de la production d'électricité en France), c'est pourquoi avec les récentes vagues de cyberattaque tels que NotPetya et Wannacry, et par le risque que pourrait engendrer les centrales nucléaires pour le pays, qu'il est nécessaire de sécuriser le réseau informatique de ces derniers. Dans notre rapport, nous répondrons donc à la **problématique de rénovation des réseaux des centrales nucléaires au sein d'un contexte de cybersécurité**.

Dans un premier temps, nous aurons une **présentation de l'entreprise et des différents services en lien avec lien avec la sécurité des réseaux des centrales EDF**. Enfin, nous étudierons **les différentes missions qui m'ont été confiés lors de mon stage**, afin de dresser un bilan de celui-ci.

II. Présentation de l'entreprise

A. Présentation de EDF

Electricité de France (EDF) est le premier producteur et fournisseur d'électricité en France et en Europe. Elle a été créée le 8 Avril 1946 à la suite du vote de la nationalisation de l'électricité et du gaz sur la proposition de Marcel Paul, ministre de la production industrielle.

Actuellement, EDF se compose de plusieurs directions et filiales (*cf. Annexe Organigramme EDF*) :

- **Transport RTE** : Gère le réseau public d'électricité très haute tension (THT, > 100 kV) ; différents postes permettent de distribuer les différents réseaux de moyenne et basse tension, qui vont vers le client final
- **Direction Ingénierie et Projet Nouveau Nucléaire** (DIPNN) : Gère les nouveaux projets liés au nucléaire, actuellement, le sujet principal concerne l'EPR (*Evolutionary Power Reactor*)
- **Direction du Parc Nucléaire et Thermique (DPNT)** : La filiale dans laquelle je suis, gère l'exploitation des centrales nucléaires du parc EDF (58 tranches sur 19 sites) et l'ingénierie associée (hors périmètre DIPNN), et l'exploitation de la thermique classique. Plusieurs unités constituent la DPNT (DPN pour l'exploitation, DIPDE pour l'ingénierie, …)
- **Pôles Energies Renouvelables** : Gère l'exploitation des centrales hydrauliques et l'ingénierie associée
- **Commerce** : Gère les contrats avec les clients importants d'EDF, en matière de distribution d'électricité
- **Distribution ENEDIS** : Gère le réseau public d'électricité de moyenne et basse tension, contrairement à RTE qui gère les très hautes et hautes tensions

Aujourd'hui, EDF est une multinationale, sous la direction de Jean-Bernard Lévy, et qui génère un chiffre d'affaire de 68 milliards d'euros.

EDF – Division de l'Ingénierie du Parc nucléaire, de la Déconstruction et de l'Environnement (DIPDE) est une entité appartenant à la **DPNT** et compte environ 1900 collaborateurs répartis sur Marseille, Lyon et 11 sites nucléaires. Elle a pour mission de concevoir et réaliser les modifications nécessaires aux centrales nucléaires afin de prolonger leur durée de vie ainsi que d'optimiser leur déconstruction.
Une partie des équipes est localisée au niveau national (Marseille et Lyon) pour les études et une autre partie est directement sur chaque site nucléaire (équipe commune), chargée de piloter le déploiement des modifications conçues au niveau national.

B. EDF-DIPDE, une culture de l'entreprise complexe

En France, la production d'électricité est principalement représentée par la production nucléaire (environ **75% de la production total**), le reste correspondant aux productions thermiques à flamme, marémotrice, solaire, etc…
Toute arrivée à **EDF-DIPDE** se marque par une initiation à la culture de l'entreprise, ici, le thème est le **nucléaire**, puisque le rôle principal de la division d'EDF est de gérer toutes les affaires en liens avec le nucléaire.

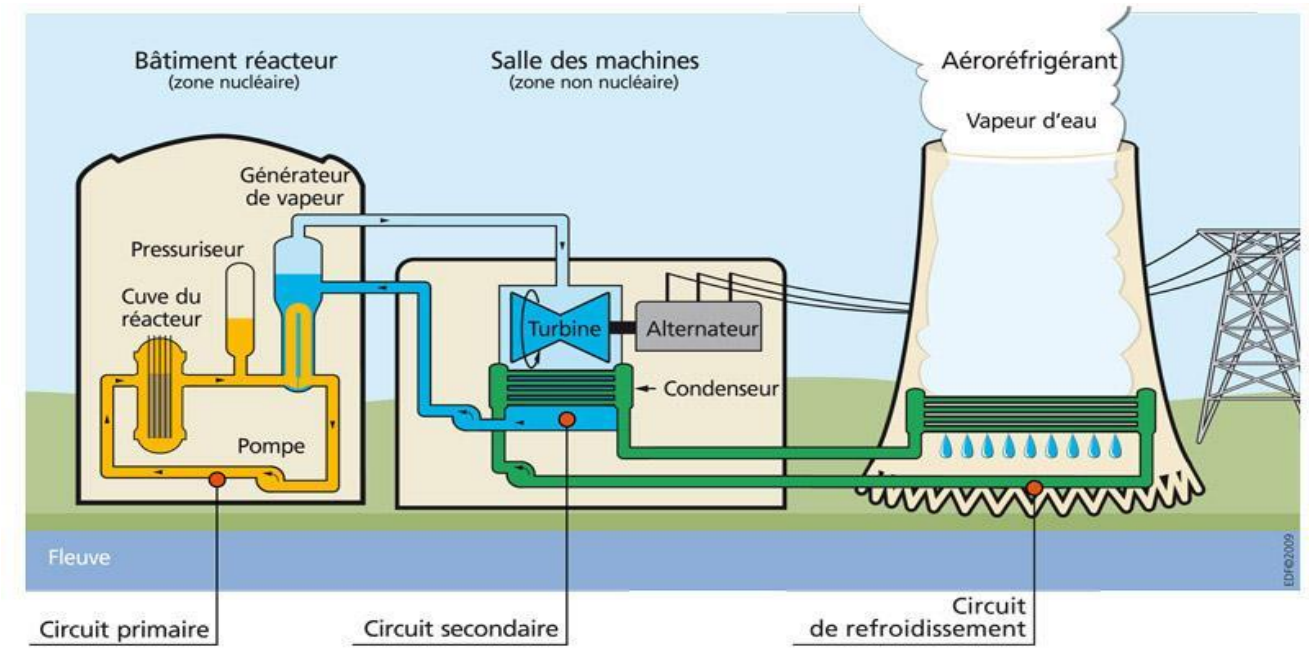


Figure Schéma du fonctionnement d'une centrale nucléaire

Voici un schéma "macro" représentant le fonctionnement d'une centrale nucléaire, globalement, la fission de l'uranium au cœur de la cuve du réacteur, génère de l'énergie thermique sous forme de chaleur. Puis, cette énergie thermique chauffe le système hydraulique, et l'eau chauffée se transforme sous forme de vapeur au sein du générateur de vapeur (énergie thermique). Enfin, l'énergie cinétique fait tourner les turbines, afin de créer de l'énergie mécanique, ensuite transformé en énergie électrique pas le biais de l'alternateur. (*cf. Annexe Process nucléaire*)

Le fonctionnement d'une centrale nucléaire est bien plus complexe que ce schéma, j'ai donc fait une formation e-learning d'une trentaine de chapitre pour comprendre les subtilités d'une centrale nucléaire.
On distingue 4 types de centrales selon leur production d'électricité en sortie, que l'on nomme palier (ceci est important pour la suite) :

- Palier 900 MW (production en sortie de 900 MW)
- Palier 1300 MW (production en sortie 1300 MW)
- **Palier N4 (production en sortie de 1450 MW et le palier sur lequel j'ai travaillé)**
- Palier EPR (production en sortie 1600 MW, celui de Taishan étant le seul en activité et celui de Flamanville, actuellement en cours de déploiement)

C. Le Contrôle-Commande nucléaire et l'Informatique Industriel

Le **Contrôle-Commande** correspond à l'ensemble des systèmes qui, dans une installation nucléaire, effectue les mesures, assurent les fonctions de régulation et les traitements réflexe, qui permet de faire fonctionner les différents composants du process nucléaire et les fonctions de protection.

En parallèle, on peut aussi parler d'**Informatique Industrielle**, interfacée avec le contrôle-commande, elle embarque divers systèmes industriels informatisés, tels que la supervision de données, divers modèles de calcul embarqués utile à la conduite, ou d'applications en lien avec la maintenance ou la réalisation d'essais périodiques. L'informatique industrielle est aussi chargée d'alimenter le réseau bureautique de l'entreprise EDF, avec les données du process nucléaire. Ces données sont ensuite utilisées par des acteurs nationaux divers et variés.
A noter que diverses chaînes de configuration existent, à la fois au niveau local et national, pour gérer la configuration des données et des systèmes industriels.

Distinction entre degré de sécurité et niveaux de contrôle-commande :
En appliquant le référentiel de cybersécurité, le contrôle-commande est classé selon des **degrés de sécurité**, allant de **DS1 à DS5** selon les fonctions dont les systèmes sont en charge, le degré de sécurité 1 étant le plus sensible.
Il existe aussi un référentiel de sûreté nucléaire qui associe un niveau de classement selon l'enjeu de la fonction de contrôle-commande considérée.

Il ne faut pas confondre degré de sécurité et niveau de contrôle commande, tel que la figure ci-dessous. Le niveau de contrôle-commande permet de regrouper l'architecture système du contrôle commande, on a :

- CC N0 : Appareils de terrains du process nucléaire (capteurs des pompes et vannes, ...)
- CC N1 : Automates (machines qui s'occupent de récupérer les différentes données provenant du processus nucléaire pour les transmettre aux réseaux)
- CC N2 : Visualisation à des fins de conduite (Interface (type écran) sur des automates)
- CC N3 : Informatique Industrielle : Réseau informatique dans lequel les données sont traitées puis transmises vers des destinataires internes/externes

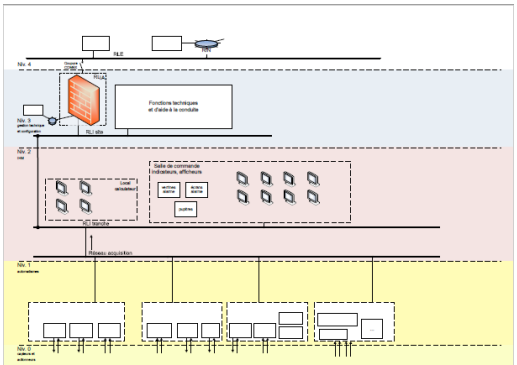


Figure Schéma Contrôle Commande

Exploitation-maintenance du contrôle-commande :

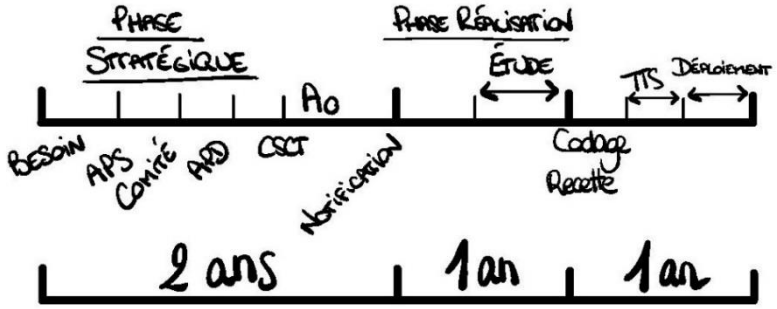
Les actions au sein d'EDF sont classées selon un référentiel normatif (AFNOR), cela correspond à différents niveaux de maintenance :

- Niveau 1 AFNOR : Actions simples ou de maintenance sur des éléments accessibles, souvent effectuées par des exploitants sur sites nucléaires
- Niveau 2 AFNOR : Opérations avec outillage standard et formation standard, qui demandent des instructions et procédures simples
- Niveau 3 AFNOR : Opérations complexes avec des outils et des compétences spécialisés
- Niveau 4 AFNOR : Modification majeure
- Niveaux 5 AFNOR : Travaux de rénovation majeur et de reconstruction

Les **niveaux 1 et 2** sont opérés par les exploitants sur les sites nucléaires, en cas de problème, ils peuvent faire appel à une liste de Titulaires (sous-traitant officiel d'EDF) par des contrats MCO (maintien en condition opérationnelle).

Les agents en charge du contrôle-commande au sein d'EDF-DIPDE et les Titulaires MCO, sont **en charge des niveaux 3 et 4 voire 5**, la plupart du temps en surveillance de leur sous-traitant qui exécute les opérations.

Fonctionnement du processus d'ingénierie :



Dans le processus d'ingénierie d'une affaire de rénovation « courte », on a pour commencer un besoin, qui va être l'élément déclencheur pour la phase d'étude :

- **Expression du besoin-métier** par la maîtrise d'ouvrage (DPN - exploitant des centrales)
- **APS** : Avant-Projet Sommaire, phase d'étude amont pour identifier diverses solutions techniques associées au besoin-métier, chacune avec son coût et le planning associés
- **Comité décisionnel** : Réunion où l'on valide la solution retenue et la stratégie associée
- **APD** : Après-Projet Détaillé, phase d'étude détaillée
- **La phase de rédaction du cahier des charges (CSCT)**, une étape cruciale, car c'est un contrat qui va relier EDF avec son ou ses sous-traitants, le moindre manque d'exigence dans ce cahier des charges peut risquer d'amener à un avenant et coûtera plus cher pour EDF
- **Une phase d'appel d'offres** peut être lancée (conformément à la réglementation) et une analyse des offres techniques et commerciales est menée par EDF
- Après **notification du sous-traitant** retenu, EDF démarre la **phase de réalisation**, avec les spécifications du titulaire et la gestion des interfaces avec d'autres affaires
- La phase d'étude du titulaire débouche sur une **phase de codage/recette** qui correspond à plusieurs tests, chez le titulaire ou sur une plateforme d'intégration à EDF-DIPDE.
- Vient ensuite l'étape de la **TTS** (Tranche-prototype), avec la mise en service sur site.
- Quand le retour d'expérience* (REX) de la TTS est correct, le **déploiement** sur toutes les centrales concernées peut démarrer.

Il faut savoir que la durée des affaires de rénovations peut être longue, une affaire de rénovation lorsqu'elle est **simple dure 1 à 4 ans**, qui est un chiffre assez optimiste, mais lorsqu'elle est **complexe, peut durer jusqu'à 15 ans** (déployer une modification sur 34 centrales 900MW est en effet, consommateur de temps, avec le processus décrit plus haut).

III. Les groupes liés à la Cybersécurité : C2I et C3D

*Pour ma part, je travaille au sein du groupe **Contrôle Commande Informatique Industrielle (C2I)**, et plus précisément dans le groupe **ADIC (Architecture, Donnée, Intégration, Cyber sécurité)**.*

C2I est le service de DIPDE **en charge des études en lien avec le contrôle-commande et l'informatique industrielle** (*cf. Annexe Organigramme DIPDE*).
Plusieurs groupes composent C2I, dont le groupe **ADIC**, **en charge de thèmes plus transverses**.
Un autre service, **C3D**, est **en charge de l'expertise sur le thème spécifique de la cybersécurité**, en coordination avec les activités de C2I.

Le contrôle commande est assez complexe, ainsi, il existe plusieurs sous-groupes au sein de C2I :

- **ADIC : Architecture, Données, Intégration et Cybersécurité**
- SCII : Systèmes de contrôle et d'informatique industrielle
- ARC : Automatismes de régulation centralisée
- PFC : Plateformes Communes
- SIMU : Simulateurs
- SPC : Systèmes de protection-cœur

A. Présentation du groupe C2I-ADIC

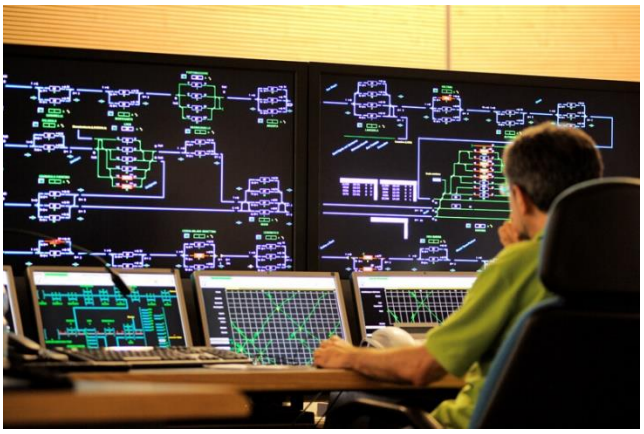


Figure Salle de commande sur le palier N4

Le groupe ADIC s'occupe principalement :

- De la **gestion des données de configuration du contrôle-commande et de l'informatique industrielle** (niveau 2) des centrales nucléaires.
- De **l'appui technique, sur les thèmes « architecture et cybersécurité »**, sur les différentes **modifications du contrôle-commande et de l'informatique industrielle**
- De la **gestion des plateformes nationales qui sont utilisées par EDF** pour interconnecter les différentes modifications qu'il est question de déployer sur un site nucléaire (activité d'intégration).

Il contribue aux évolutions d'architecture du Contrôle Commande et de l'Informatique Industrielle du parc en intégrant une vision technique et patrimoniale.
Les architectures réseaux des centrales nucléaires sont complexes (beaucoup de systèmes connectés avec des données diverses et variées qui circulent, architectures différentes selon les paliers, coexistence et/ou transition de composants d'ancienne génération vers des composants de nouvelle génération, distinctions entre contrôle-commande et informatique industrielle, …) et **nécessitent de nombreuses personnes ayant des connaissances variées**.

B. Présentation du service C3D

Le **Centre de Compétences en Cybersécurité (C3D)** est une **cellule indépendante et spécialisée dans la cybersécurité**, au sein d'EDF. En coordination avec C2I, C3D vérifie les modalités de **mise en œuvre de loi de programmation militaire (LPM)** sur les architectures du parc nucléaire, que nous étudierons plus tard dans le rapport. Il est en charge de la rédaction de référentiels et de guides de sécurisation, en charge d'apporter une expertise et un appui aux projets et contribue au processus de recherche de vulnérabilités sur les systèmes informatiques.
C3D peut aussi mettre à disposition de C2I des outils en lien direct avec la cybersécurité et la cybersurveillance, à déployer dans le cadre des affaires de rénovations de centrales nucléaires. Ils réalisent des audits de cybersécurité et laissent des avis sur les manières de sécuriser les réseaux des centrales.

C. Contexte de la loi de programmation militaire

Les réseaux des centrales EDF sont soumis à la **loi de programmation militaire (LPM),** c'est-à-dire, qu'elle a des exigences sur la cybersécurité des centrales.
La loi de programmation militaire (LPM) concerne les opérateurs d'importance vitale (OIV), qui sont des organisations identifiées par l'État comme ayant des activités indispensables ou dangereuses pour la population.

Depuis 1958, les textes de loi de programmation militaire, concernait uniquement la sécurité physique des points d'importances vitales (PIV). Par la suite, en 2013, un nouvel article, l'article 22 de la LPM, **met en valeur l'importance de la sécurité des systèmes d'informations d'importance vitale (SIIV)**.

Elle exige un respect des règles de sécurité spécifiques, un recours à du matériel et des prestataires qualifiés, une notification obligatoire des incidents de sécurité, des contrôles de sécurité réguliers commandités par l'ANSSI, et tout cela sous risque de sanction en cas de non-conformité aux obligations prévues.

L'ANSSI, étant l'Agence Nationale de la Sécurité des Systèmes d'Informations est une référence dans le domaine de la cybersécurité, c'est un service à compétence nationale, rattaché au Secrétaire Général de la Défense et de la Sécurité Nationale, chargée d'assister le Premier Ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. (*Source : ANSSI*)

IV. Présentation de mon lieu de travail

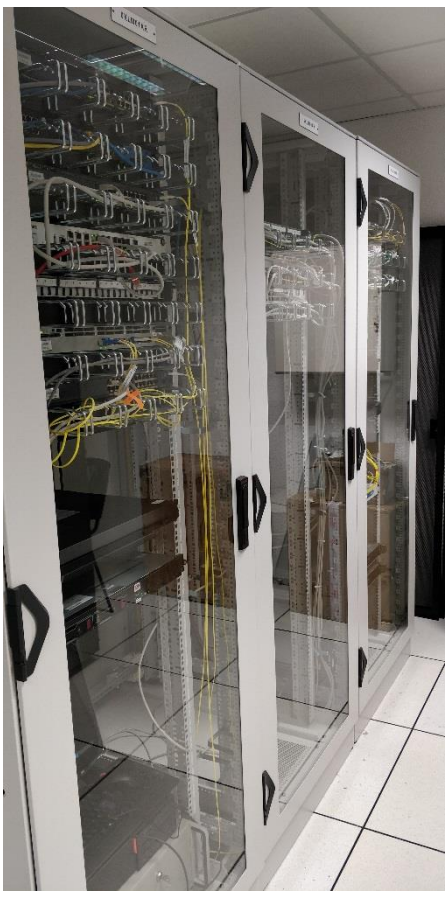
A. Bureau : Analyse documentaire, échange MEGA, préparation projets

Figure Bureau de travail

Les agents EDF travaillent une grande partie de leur temps, dans leurs bureaux, c'est ici, qu'ils traitent leurs affaires, contribuent à d'autres affaires et gèrent leurs Titulaires. Ils se doivent d'être à jour et avoir une connaissance avancée sur leurs projets, et cela, afin de tenir informer les autres affaires en cours pour qu'ils puissent prendre compte des dernières modifications.
Pour ma part, j'ai partagé mon bureau avec deux agents EDF :

- **Didier PAQUET**, mon tuteur de stage et **référent des architectures réseaux des centrales**
- **Jean-Luc**, en charge du **CNC (Centre de Crise National), de LGP2I (Outil de gestion du patrimoine et de l'informatique industrielle**) et d'une affaire concernant la rénovation du réseau sur le palier 900

B. Plateforme N4 (PF N4) : Simulation, test et expérimentation



La **Plateforme de Test du Palier N4**, souvent **appelé PF N4 Rénové**, est une plateforme de simulation « réduite » du réseau d'une centrale nucléaire N4. Elle permet aux agents EDF de **vérifier leurs configurations** et permet aussi aux Titulaires, de **venir tester et attester de la conformité de leur configuration**. Elle est **indispensable** et les agents ont bien **conscience de l'intérêt d'avoir une maquette de test au sein de leurs locaux**.

Figure Plateforme de Simulation N4

C. Réunion : MV, Formation, réunion sur certains points…

Figure Salle de Réunion

La salle de réunion est une salle de réunion classique utilisée au sein d'ADIC, elle permet d'assurer :

- Réunions de Management Visuel : Ce sont des réunions hebdomadaires durant lesquelles, on discute de divers sujets ou alertes sur nos affaires en cours
- Réunions/Débats : Ce sont des réunions occasionnelles durant lesquelles, nous sommes confrontés à des problématiques et chacun essaye d'apporter une solution, tandis que les autres donnent leur avis : avantages et inconvénients
- Formations : On peut assister à des formations sur des sujets techniques et en faciliter notre compréhension, pouvoir échanger et débattre, et donc répondre à nos questions. Personnellement, j'ai eu la chance d'assister à une formation sur OPC UA, un protocole de communication innovant, présenté par Michel Condemine, directeur de 4CE Industry et président de la fondation OPC UA en France

D. Protection physique des accès et confidentialité des infos :

« La première étape dans la cybersécurité est la protection de la sécurité physique »

Stormshield
Data Security
ENTERPRISE

Travailler dans la **cybersécurité** implique une **grande responsabilité et une grande vigilance**, la moindre erreur peut réduire en cendre des heures de travail.
Travailler dans la cybersécurité nécessite de signer une charte avec l'entreprise en question, concernant un **engagement de confidentialité nominatif**.
Chez EDF, **protéger les accès physiques** à certains endroits par des badges est primordial, cela empêche les intrus/personnes malhonnêtes d'avoir accès à des zones sensibles.
Ensuite, il est nécessaire de **sécuriser notre outil de travail principal, notre ordinateur portable**, on le sécurise physiquement en le cadenassant à notre bureau, et on le sécurise virtuellement en envoyant des mails chiffrés/signés, sécurisant nos données grâce à **Stormshield Data Security**, puis en verrouillant nos postes lorsque l'on quitte notre bureau.

V. Présentation des différents points de mon stage

Une de mes tâches a été de m'approprier des différentes spécificités de l'architecture réseau N4, principalement par de l'analyse documentaire.

A. Appropriation des spécificités de l'architecture réseau du N4

Comme expliqué précédemment, l'**Informatique Industrielle du Contrôle-Commande** est la branche du contrôle-commande en charge des systèmes informatiques.

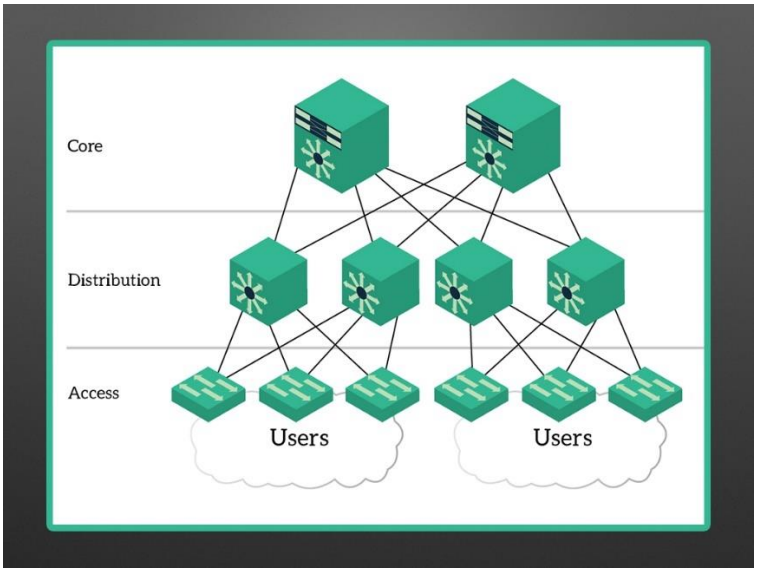


Figure Schéma Architecture hiérarchique

La partie informatique industrielle du palier N4 étant actuellement en cours de rénovation, elle comporte donc, de nombreuses affaires en lien avec le réseau et la cybersécurité. Elle s'inscrit dans une architecture réseau hiérarchique (vu en classe avec Mr NGUYEN) adapté pour l'informatique industrielle : Core, Distribution et Access (voir figure ci-dessus).
Les marques d'équipements réseau sur lesquels j'ai travaillé dont Cisco, Fortinet et Seclab.

Durant mon stage, **toutes les connaissances et compétences acquises en réseau ont été nécessaires**, j'ai alors été confronté aux **problématiques de cloisonnement d'architecture**, avec des sujets tels que les Vlan, protocole de routage, traduction d'adresse, filtrage de flux, diode réseau et firewall.
J'ai pu notamment participer à **une formation OPC UA**, un protocole de communication « complet » et novateur dans les domaines de l'informatique industrielle. Des entreprises telles que Schneider ou Siemens ont complètement basculé leurs systèmes sous OPC UA.

Ainsi, les différents modules qui m'ont été nécessaires lors de mon stage, ont été :

- Initiation aux réseaux d'entreprise
- Principe et architecture des réseaux
- Base des systèmes d'exploitation
- Administration des systèmes
- Réseaux locaux et équipements actifs
- Automatisation des tâches d'administration

B. Modélisation d'équipements et de flux sur MEGA

La modélisation MEGA correspond à la modélisation des différents flux de données et équipements liées aux réseaux cibles.

MEGA est un **outil de modélisation de donnée** mais aussi de processus et de flux. La modélisation de l'architecture-cible est **indispensable** car cela permet de croiser les différentes affaires en cours sur le N4 et correspond à **un référentiel unique sur lequel se baser**.
Pour pouvoir utiliser MEGA, on ajoute des informations (équipements, flux de données et applications) dans **des fichiers injecteurs en .csv** qui sont **ensuite importés sur MEGA, à l'aide d'un script VBA*** (Visual Basic for Applications, voir figure ci-dessous).
Ainsi, j'ai travaillé en collaboration avec une prestataire modélisatrice MEGA de chez SOPRA-STERIA, afin de lui **apporter mes connaissances sur l'architecture N4**, en lui transmettant les documents appropriés, en lui indiquant les spécificités au sein du N4 et en répondant à ses questions pour faciliter son travail de modélisation. Il existe trois types de modélisations :

- Equipement (équipements réseaux, postes d'administration, serveurs, …)
- Flux de données (protocoles, flux de données, logs, …)
- Applicatif (logiciel, application, sur lequel, je n'ai pas eu le temps de travailler)

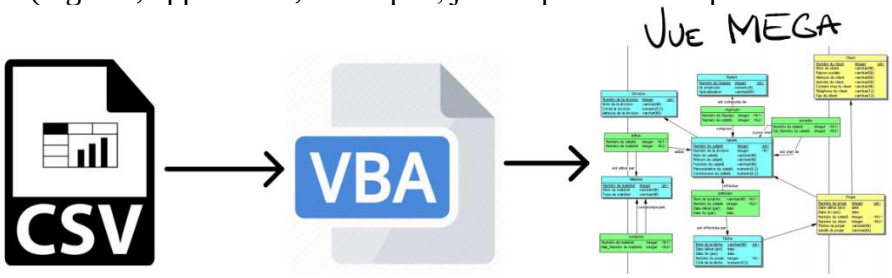


Figure Schéma Fonctionnement MEGA

Pour la modélisation des équipements du N4, nous avons listé :

- Équipements réseaux (switchs et firewalls)
- Machines physiques et virtuelles
- Armoires et locaux
- Repères fonctionnels des équipements et des machines
- Systèmes d'exploitation des équipements et des machines

Pour la modélisation des flux de données du N4, nous avons listé :

- Nom du flux et sa description
- Source et destination, et celui qui est à l'initiative de la communication
- Protocole utilisé sur les flux

La modélisation m'a permis de **m'imprégner des différentes caractéristiques de l'architecture N4**, au-delà de son aspect global et de **formaliser des hypothèses de modélisation**, lorsqu'il me manquait certaines informations. Enfin, grâce aux fichiers injecteurs, nous pouvons aussi modéliser des vues graphiques selon nos choix de modélisation (*cf. Annexe MEGA*).

Dans le cadre de mon stage, sachant que je n'aurais pas assez de temps pour finir la modélisation MEGA du réseau N4, j'ai donc effectué un **compte-rendu pour mon tuteur pour qu'il puisse récupérer mon travail lorsque je serais parti**.
Dans ce compte-rendu, appelé « Fiche de Formalisation », je note **les différentes hypothèses de modélisation que j'ai choisi de faire**, cela correspond à des situations où je n'ai **pas d'information officielle et où je fais un choix qui se rapprochera le plus du résultat cible**.

C. Transfert FTPS mode passif et configuration de Port-Mirroring sur une plateforme hors EDF-DIPDE

Une de mes tâches a été de configurer un port mirroring sur switch afin de m'assurer d'un transfert FTPS en mode passif.
Les tests se sont effectués sur une plateforme qui n'est pas située à Marseille, mais au sein de FRAMATOME à Grenoble.

Compte tenu de la configuration de la plateforme de test distante et des spécifications du protocole FTPS à tester, mes activités ont permis de mettre à jour la plateforme d'intégration de ce système industriel.

Notions générales sur le fonctionnement du protocole FTPS :

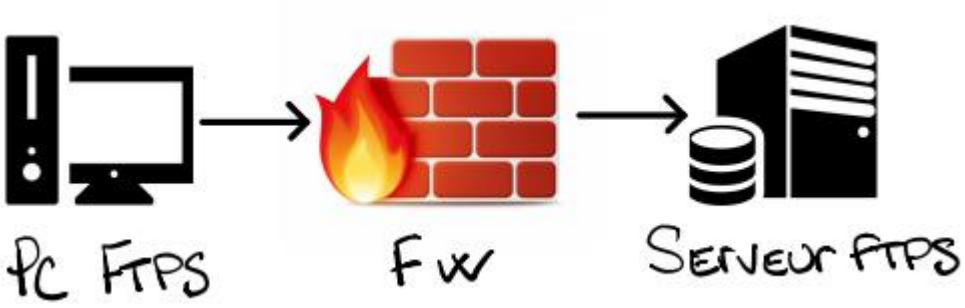


Figure Schéma Contexte Plateforme Framatome

FTPS ("File Transfer Protocol Secure") est un **protocole de transfert de fichier** (Client-Serveur), il se base sur TCP/IP et utilise les ports 20 (Data Channel) et 21 (Command Channel) en mode actif.
Plusieurs modes ou commandes sont possibles d'être configurées : **CCC, PROT C**/PROT P, actif/**passif** et explicite/implicite. Par défaut pour FTPS, les informations sont négociées dans le Command Channel et les données sont échangés dans le Data Channel, et sont chiffrées.

Il existe deux modes pour FTPS :

- Actif : Port d'écoute sur le port 21 et Port d'envoi sur le port 20 (Configuration "statique")
- **Passif (notre cas, figure ci-dessous)** : Port d'écoute du serveur sur le 21 et Port d'envoi sur un port supérieur à 1024 et choisi après un échange avec le client FTP/FTPS (Configuration "dynamique")

En mode passif, le client est **toujours à l'initiative de communication** (sur DATA et COMMAND), ce type de fonctionnement a une **meilleure compatibilité avec la présence de firewall** dans une architecture et présente un **réel avantage en termes de cyber sécurité**. (*cf. Annexe FTPS*)

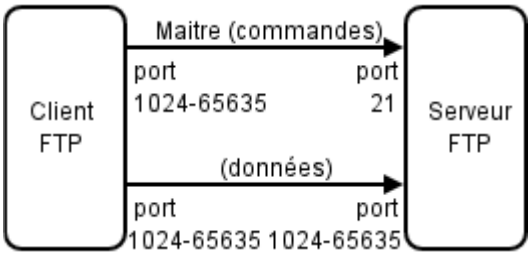


Figure Schéma FTP/FTPS mode passif

Un des intérêts de cette mission est de s'assurer de l'implémentation des commandes CCC et PROTC par le serveur FTPS :

- **CCC* (Clear Command Channel)** est une commande FTP/FTPS permettant **de mettre en clair la négociation de port, les échanges sur le Command Channel**, après l'authentification.
- **PROT C*** est une commande FTP indiquant que les échanges de données sur le Data Channel sont envoyés en clair, donc non-chiffrées dans le Data Channel

Présentation et explication de ma mission sur le transfert FTPS :

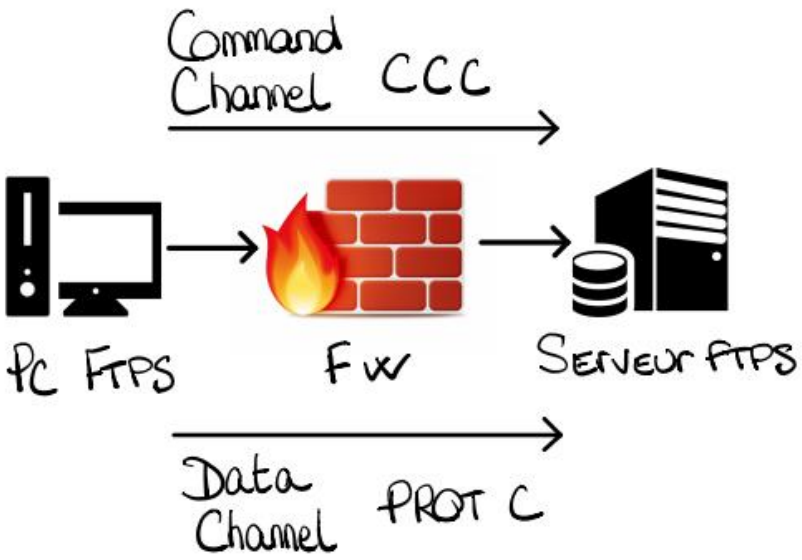


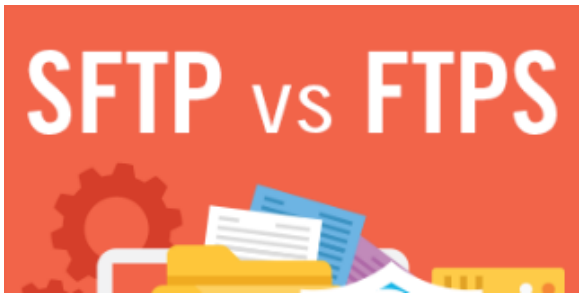
Figure Schéma PROT C et CCC

La plateforme FRAMATOME comporte quelques contraintes : les échanges FTPS/passif sont configurés et il existe un pare-feu entre le client FTPS et le serveur FTPS.
Historiquement l'implémentation de **PROT C est faite pour le couplage des plateformes hors EDF**, mais **CCC à une réelle utilité**, car elle permet au firewall de **voir la négociation de port dans le Command Channel et permet à ce pare-feu d'ouvrir dynamiquement les ports correspondant à la négociation de ports**.

Les objectifs de ce point sont :

- **S'assurer du fonctionnement des échanges FTPS**
- **Vérifier la présence des commandes CCC et PROT C**, à l'aide d'un port-mirroring sur un switch Cisco, entre le client et serveur FTP, comme appris durant ma formation réseau

J'ai eu la chance de **porter un appui aux exploitants de chez FRAMATOME** et à distance, pour qu'ils puissent faire des tests, afin de savoir si les échanges FTPS fonctionnaient et si les commandes PROT C et CCC ont bien été intégrés sur la plateforme située dans leurs locaux.



Enfin, j'ai pu me rendre compte de la **difficulté de coordonner des « actions simples » à distance avec des acteurs pas toujours avec un profil technique adapté**.
Ma mission s'est arrêtée à la configuration du port-mirroring sur le switch de leur plateforme, afin d'écouter les échanges FTPS et vérifier la présence de CCC et PROT C.

Un axe potentiel de stage aurait été de reproduire un **substitut de cette plateforme au sein d'EDF-DIPDE**, avec les mêmes configurations que la plateforme chez FRAMATOME, afin de donner un avis **sur le choix d'un FTPS avec PROT C et CCC, plutôt qu'un SFTP (Secure File Transfert Protocol, protocole de transfert de fichier sécurisé par SSH), plus sécurisé et plus simple à implémenter**.

D. Test de relevé de fiche d'identité

Une de mes tâches a été de tester des scripts permettant d'avoir des relevés les configurations de machines physique ou virtuelle, sous Linux, afin de créer des fiches d'identités au format JSON pour LGP2I et C3D.

Contexte des relevés de fiche d'identité :
L'intérêt de cette mission est de de pouvoir alimenter l'outil **LGP2I*** (Logiciel de Gestion du Patrimoine d'Informatique Industrielle) de fiche d'identité Linux et Windows et certains outils de **C3D**, qui utilise aussi ces fiches d'identité pour ses propres activités.

Une **fiche d'identité** est une fiche se présentant sous **format JSON ou Docx**, et renseignant des **informations sur les configurations des postes d'administration et serveurs**.

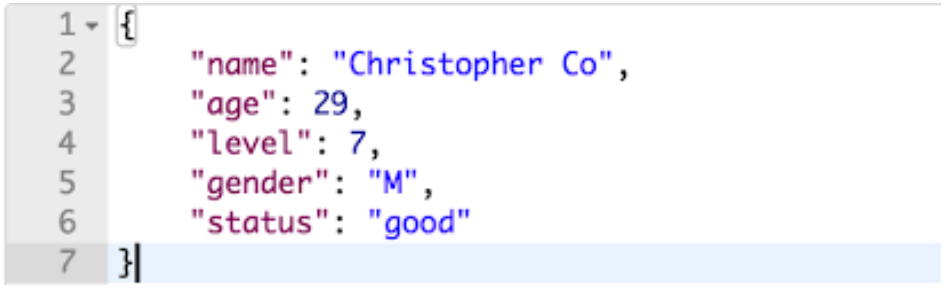
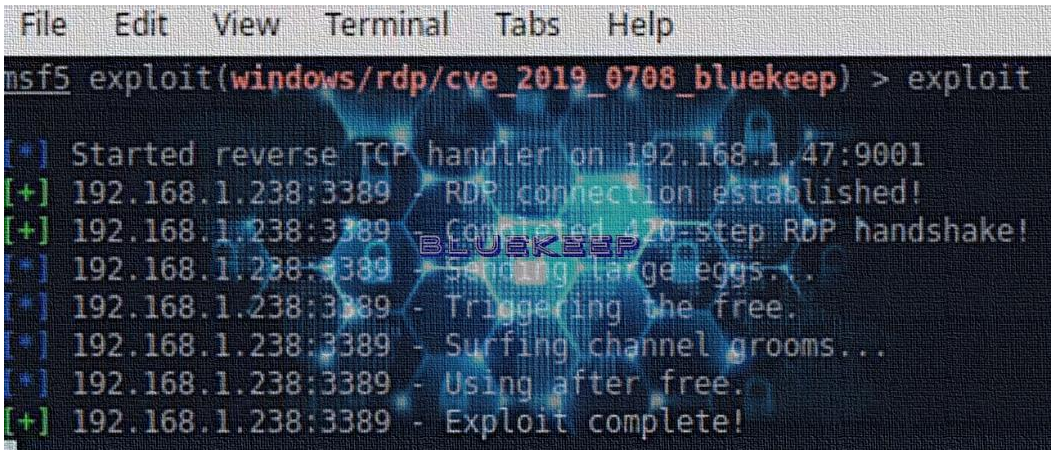


Figure Exemple format JSON

Le format **JSON** (*JavaScript Object Notation)* est un **nouveau format de donnée** (.pdf, .xml, .doc) à la mode, grâce à **sa structure qui permet de manipuler des objets JavaScript**, et **plus facilement utilisable** avec un langage de programmation tel que JavaScript.



Courant mois de Mai 2019, **« Bluekeep », une faille critique au sein des systèmes d'exploitation Windows** permettant l'intrusion de **ransomware**, assez semblable à « **WannaCry** », a été découverte.

Bluekeep exploite une **faille dans un protocole Windows, Remote Desktop Protocol (RDP)**, qui est un **protocole permettant de se connecter sur un ordinateur distant**, en utilisant Microsoft Terminal Service. Cette faille concernait les versions inférieures à Windows 7 et un patch de la part de Microsoft est très vite apparu pour corriger ce bug.
Ainsi, un **cas d'usage des fiches d'identité** est **de lister l'ensemble des systèmes d'exploitation et leurs versions**, afin de **rapidement détecter si cette faille crée de réels risques sur notre architecture réseau**.

Présentation des tests effectués pour la création de fiche d'identité :
A l'aide des scripts fournis par C3D, j'ai été en charge de **tester les scripts pour les postes et serveurs Linux sur la plateforme N4** (sachant que les scripts Windows n'étaient pas encore automatisés), et d'y **donner un avis critique quant aux résultats obtenus**.

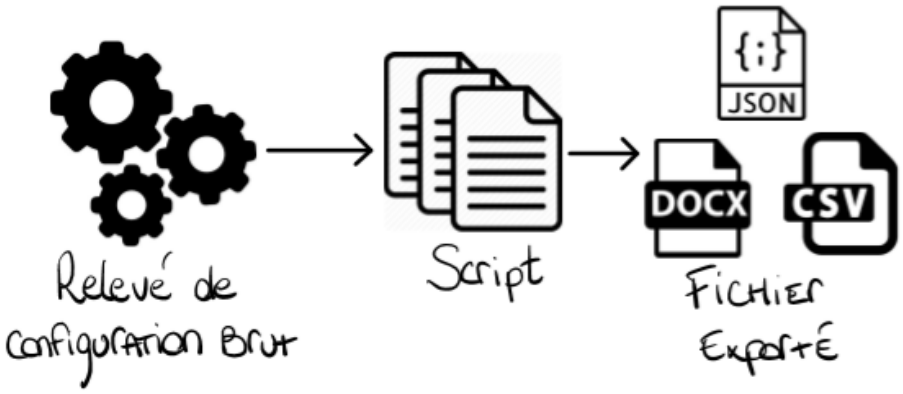


Figure Schéma Fonctionnement Fiche d'identité

Le fonctionnement de la création des fiches d'identité correspond à **un résultat brut des relevés de configuration, en entrée d'un script pour le convertir au format souhaité** (JSON, Docx, …).

Ainsi, après avoir lancé les scripts et récupéré les différentes fiches d'identités, j'ai pu me **rendre compte des différentes erreurs** qui nécessitaient des connaissances en administration système sur une distribution Linux autre que celles étudiées en classe, mais que j'ai tout de même réussies à trouver.
J'ai **relevé les différentes erreurs que j'ai détectées, trouvé une solution alternative, puis les ai partagés avec C3D**, afin qu'ils en discutent avec leur prestataire en charge de ces scripts.

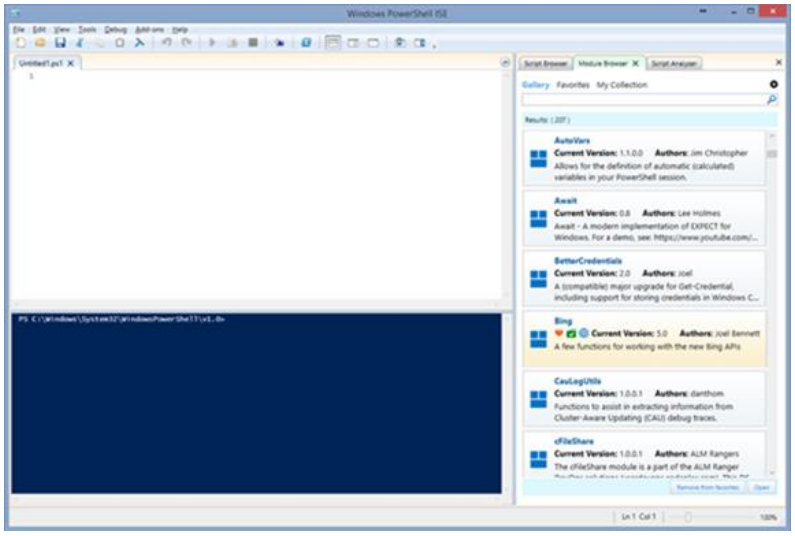


Figure Powershell ISE (Scripting Windows)

Un sujet potentiel de mon stage aurait été de créer un script automatisant les fiches pour la partie Windows. Un simple test d'un script en version de test, avec formalisation du résultat en plateforme, a été mené sur ce plan et j'ai effectué un retour concernant cette version test auprès de mon tuteur.

Je me suis rendu compte de la **difficulté d'inscrire ce type d'activités dans un cadre organisationnel pérenne** (les scripts doivent pouvoir être repris et maintenus dans le temps par un service EDF identifié).

Compte tenu que la **réalisation et le maintien pérenne de ces scripts, sont du domaine de responsabilité de C3D** et compte tenu de leur charge de travail et de leurs priorités au cours de mon stage, je n'ai pas pu finaliser cette action.

E. Configurations équipements et serveurs

Une de mes tâches a été de faire une analyse critique de notre configuration en plateforme, afin de donner un avis sur les installations sur les équipements réseaux (SW et FW) et les serveurs du réseau N4.

Présentation du contexte et du périmètre des configurations des équipements (réseaux, serveurs, …) :
Il faut savoir que **la rénovation des architectures réseau des CNPE** (*Centre Nucléaire de Production d'Électricité)* se fait à **l'aide de différents sous-traitants** tels qu'Atos, Sogeti High Tech, Sopra-Steria, Snef, Framatome et Assystem.
Pour la répartition des tâches, **EDF gère la partie de "gestion de projet"**, rédige des cahiers des charges, de la documentation, et gère les différents évènements liés à leur affaire telle que les phases de test de leur sous-traitant. D'autre part, **EDF a l'habitude de confier la partie "technique" à des sous-traitants**, qui eux, gèrent la mise en place des équipements et des configurations demandés par EDF et effectue l'analyse des besoins pour savoir s'ils peuvent être implémentés.

Retours et technologies sur lesquels j'ai travaillé :
Les **équipements réseaux et de la réinstallation des serveurs**, étant sous le **périmètre Atos**, ainsi, j'ai dû dans un premier temps, faire une **analyse des documents fournis par Atos et en donner un avis**.
Enfin, j'ai dû **vérifier en plateforme à l'aide des fichiers de configuration des switchs et firewall, de la cohérence de l'implémentation entre les documents et la plateforme physique**.
Après une vérification documentaire et matérielle des configurations des équipements fournis, suivie des tests en plateforme, j'ai trouvé que les configurations étaient complètes. Par ailleurs, je n'ai jamais rencontré de souci sur les équipements réseau lors de mon stage.

Dans un second temps, j'ai dû **tester la réinstallation des différents serveurs sous périmètre Atos qui sont des serveurs VMware ESXI et donner un avis critique de la difficulté de cette réinstallation pour un exploitant sur CNPE**, ne connaissant au mieux que quelques bases en l'administration système, et aussi, relever les différentes erreurs dans le document fourni par Atos.
Par ailleurs, j'ai pu manipuler **Puppet, un outil de gestion de de configuration de serveurs**, et aussi **Kibana, un plug-in d'Elasticsearch qui permet de faire de la visualisation de données**. Il faut savoir que **Puppet et Kibana sont des outils très en vogue** pour les métiers liés aux Devops et au Big Data.

Après des tests, je me suis rendu compte qu'il y avait des **soucis concernant une partie de gestion des certificats Web**, le **Titulaire Atos a corrigé ce problème à la suite de mes observations**.

F. Test de performance FTP sur le DENELIS (Diode réseau)

Une de mes tâches a été de faire un test de performance de transfert FTP, afin de donner un avis sur les un boitier de coupure Seclab, DENELIS, au regard des flux prévus dans l'architecture-cible.

Objectif général de mon activité :
Vérifier le comportement aux limites de la diode-réseau
Valider les performances temporelles de transfert de fichiers
Identifier en amont les difficultés qui se présenteront à EDF dans la nouvelle architecture du N4

1. Principe d'une diode réseau et le cas du DENELIS

Aujourd'hui, lorsque l'on cherche **un moyen de filtrer et maîtriser des flux entre 2 zones réseau**, la première chose à laquelle qui nous vient à l'esprit est le **firewall**. Cela nous permet gérer des flux dans un sens bidirectionnel, en revanche, lorsque l'on souhaite faire **circuler des flux dans un sens unique et être sûr de ne pas remonter le flux dans un autre sens**, l'unique équipement le permettant est la **diode réseau**.

DENELIS est un **boitier de coupure** développé par **SECLAB** (*cf. Annexe DENELIS*). Elle permet de **sécuriser des échanges de données bidirectionnels entre différentes zones de degré de sécurité**. Il permet une **rupture protocolaire hardware et un filtrage des données** afin d'assurer une isolation des systèmes à protéger. Il est certifié CSPN par l'ANSSI.

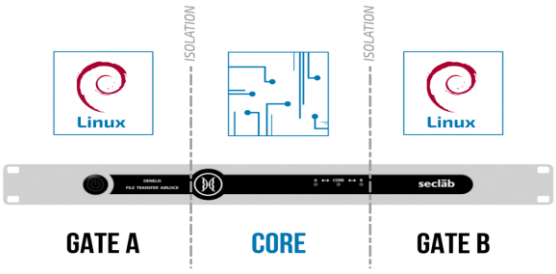


Figure Schéma DENELIS et diode réseau

2. Contexte et test effectué sur le DENELIS

Contexte et informations sur les tests à effectuer :
La problématique de cette mission est due à l'échange de deux flux au travers du DENELIS en transfert de fichiers (SFTP ou FTP).
Nous avons deux flux :

- Un **flux A**, statégique (exigence de performance temporelle) et transmis au « fil de l'eau » (données métier au fil de l'eau)
- Un **flux B**, de moyenne importance, transmis 1 fois/jour, de l'ordre du Go

Le DENELIS ne pouvant **gérer qu'un seul flux à la fois (monothread)**, **l'envoi du flux B risquerait de mettre en retard l'envoi du flux A**.
Après un échange avec Seclab, nous apprenons que le débit de transfert théorique est de 40Mbps, soit 5 Mo/s.

Calcul Temps de transfert Flux B via FTP = 1000 Mo / 5 Mo/s = 200 s =3 min 20 s

Après calcul, on voit que le retard créait par le flux B (1 Go, 1 fois/jour) par FTP via DENELIS serait de **3 min 20 s, ainsi cela créerait un trop grand retard pour le flux A, supérieur à 5 secondes**.

Durant les tests, j'ai cherché à m'assurer **de la cohérence entre les informations théoriques données par Seclab avec des tests expérimentaux sur plateforme N4 sur le DENELIS**.
Donc, j'ai **mis en place une plateforme de simulation afin de tester les transferts FTP via DENELIS**.

Fonctionnement du DENELIS :

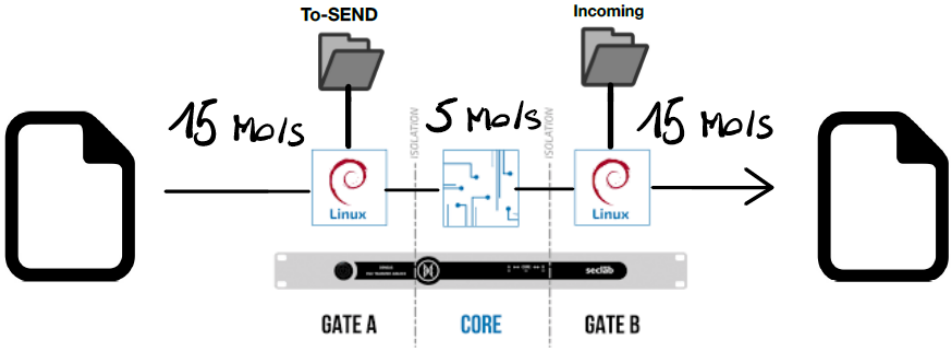


Figure Schéma Fonctionnement DENELIS et FTP

Il existe trois équipements principaux du DENELIS : **Guichet Bas (Gate A), Core et Guichet Haut (Gate B)**. Ces **guichets sont configurés comme des serveurs FTP et contiennent des répertoires dans lesquels nous pouvons y déposer nos fichiers, les plus importants : to-send, incoming et error**.

Voici le fonctionnement du DENELIS sur transfert FTP entre un Client A et un Client B via DENELIS :

- Le Client A **dépose son fichier dans le répertoire to-send du Guichet Bas** du DENELIS, à l'aide d'un client FTP (ici, Filezilla Client)
- Le DENELIS **vérifie la conformité du fichier**, par un mécanisme de vérification des signatures, le DENELIS envoie directement le fichier dans le répertoire error, en cas d'erreur
- Si le fichier est conforme, il est transmis **du Guichet Bas vers le répertoire incoming du Guichet Haut**
- Le Client B écoute sur le Guichet Haut du DENELIS et lorsque le fichier est arrivé sur le répertoire incoming, il ne lui reste plus qu'à récupérer le fichier

Test effectué sur le DENELIS :

Après **Simulation en plateforme N4**, mes tests confirment que :

- Les transferts FTP Passif peuvent être bien implémentés en plateforme
- **Débit de Transfert entre Guichet Bas/Haut = 5-6 Mo/s, comme donné par Seclab**
- Débit de Transfert entre Client et Serveur Guichet = 15 Mo/s (via Filezilla Client)

Par ailleurs, j'ai aussi pris la décision **d'implémenter du SSH sur le flux d'administration du Guichet Haut DENELIS**, ce qui n'était pas encore implémenté à ce jour et permet de faciliter les modifications de configuration sur ce guichet.

Plusieurs solutions sont envisageables pour régler le problème du retard du Flux A :

- Une demande à Seclab, de créer une version de leur **DENELIS supportant le multithread**, afin d'envoyer simultanément les Flux A et B
- **Achat par EDF d'un deuxième DENELIS** : Un DENELIS pour chaque flux
- **Modifier la fréquence d'envoi du Flux B**, afin d'avoir des envois de fichiers de taille inférieur :

Fréquence d'envoi pour 1 Go (Flux B)	Temps de transfert
1 fois/jour	200 s (3 min 20) /jour
1fois/heure	8.33 s/h
1 fois/30min	4.20 s/30 min

La solution que je recommande est celle de la modification de fréquence d'envoi car elle ne nécessite pas de modification matérielle et permet un envoi plus fréquent du flux B sans grandement impacter le flux A.

G. Migration d'un serveur

Une de mes tâches a été de faire un NAT d'un serveur, afin de l'intégrer à l'architecture rénovée sans avoir à faire de modification sur ce serveur.

Présentation du serveur KDT :

Le serveur KDT* étant un système ancien, il est préconisé de **ne pas modifier directement son adresse IP**, car certains de ses logiciels pourraient être impactés. Pour pouvoir remédier à cela et permettre la migration du serveur KDT au sein de la nouvelle architecture N4, **la solution proposée est de mettre en place un NAT (Network Adress Translation)**.

Présentation de la technologie Network Adress Translation (NAT) :

Un **NAT* (Network Adress Translation) est traduction d'adresse IP**, dans le cas, le plus courant, cela sert à correspondre des adresses d'un réseau privé vers des adresses d'un réseau publique (voir figure ci-dessous). Le NAT permet au réseau privé de communiquer avec le réseau public.

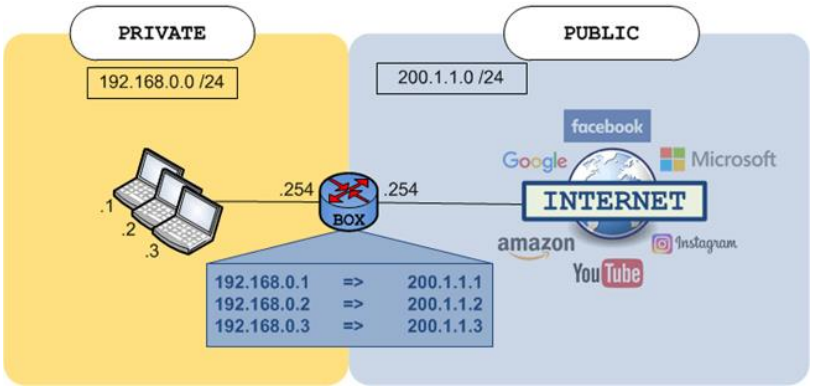
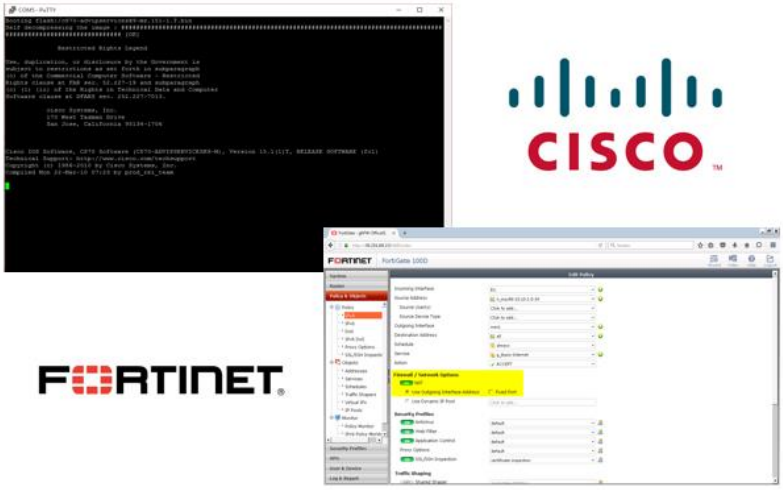


Figure Explication NAT

Présentation des tests effectués pour la migration du serveur KDT :

Dans le cadre de cette mission, j'ai pu **manipuler les équipements réseaux pour implémenter ce NAT**. Ainsi, j'ai pu mettre en avant mes connaissances et **mes compétences acquises durant ma formation sur l'environnement Cisco et découvrir l'environnement Fortinet, sur le firewall**.



Dans le cadre de ma mission, j'ai dû **vérifier de la mise en place des règles ICMP et FTP** pour les tests, et j'ai pu **implémenter le NAT sur le KDT** en faisant **correspondre son adresse IP Privée vers la bonne adresse IP du réseau de la plateforme N4**.

Enfin, j'ai **testé le fonctionnement du KDT sur le réseau,** grâce aux commandes « ping » et « tracert » et **vérifier la possibilité de faire du transfert FTP** à l'aide d'un serveur FTP (Filezilla Server) et le KDT, en tant que client FTP.

H. Mise en place d'une plateforme de certification OPC UA

Ce sujet n'a pas pu être déroulé car le temps disponible manquait, durant le stage.
Le palier N4 utilise ce type de technologie et mon activité aurait pu contribuer à mettre en œuvre une plateforme de test des profils OPC développés sur ce palier.
Les retards sur les développements ont également compliqué le déroulement de cette activité.

OPC UA est un **protocole de communication « complet et novateur »** dans le domaine industriel qui intègre transfert de fichiers, abonnements, modèle de donnée structuré, signature et chiffrement. Il permet en outre de faire de la **certification afin de tester son implémentation au sein de serveurs et clients** embarquant OPC UA, à l'aide d'un outil appelé **Compliance Test Tool* (CTT)** (*cf. Annexe OPC UA*). Il est multi-plateforme (Windows, Linux, …)

Par manque de temps, je n'ai pas eu le temps de mettre en place **les tests de CTT** sur les serveurs de la plateforme N4. J'ai tout de même fait **une formation sur OPC UA** et j'ai pensé qu'il aurait été intéressant de présenter cette technologie.

Pour pouvoir **comprendre la certification OPC UA**, il faut connaitre **une terminologie spécifique** :

- Test Case : Un test unitaire, il permet de tester une fonction du serveur/client OPC UA
- Conformance Unit : Somme de Test Case, il s'agit d'un ensemble de test unitaire
- Facet : Il s'agit d'un ensemble fonctionnel présent sur une application OPC UA
- Profil UA : Il s'agit d'un ensemble de « facet » qui peut être testé par un laboratoire de certification. Il existe plusieurs profils selon le niveau de certification que l'on souhaite

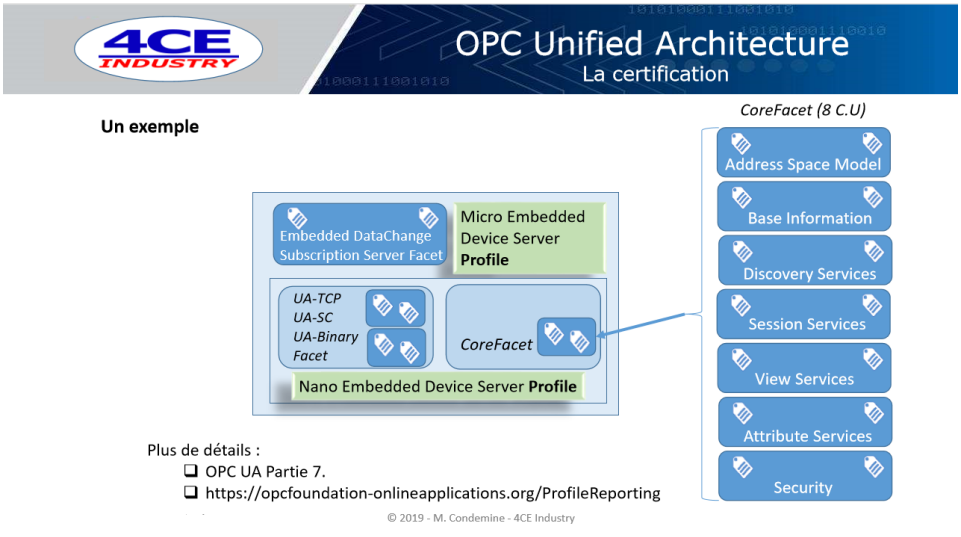


Figure Slide OPC UA

A l'aide d'une slide de la formation de Michel Condemine, directeur de 4CE Industry et président de la fondation OPC UA en France, on a **un exemple de certification avec les différents Test Case, Conformance Unit, Facet et Profile**. On voit une certification sur le profile **Nano Embedded Device Server Profile** avec les différents éléments qu'il contient, et **le CoreFacet, qui est le plus petit profil certifiable OPC UA**.

Un axe de mon stage aurait été de mettre en place une plateforme Client/Serveur, afin de **vérifier la conformité des implémentations OPC UA sur les clients et serveurs de la plateforme N4**.

VI. Conclusion et Bilan

Ce stage a été très instructif pour moi, il m'a permis de mettre en œuvre, mes connaissances et mes compétences acquises lors de mes deux années de formation, dans des cas et projets concrets.
Il m'a permis de découvrir le monde du travail, avec ses avantages comme ses inconvénients, de m'inscrire au sein d'un groupe, et d'en apprendre plus sur les acteurs et les enjeux liés au nucléaire.

Ce stage m'a permis de comprendre que travailler en ingénierie, et principalement au sein de l'informatique industrielle, comportait des contraintes telles que la coordination voire la dépendance avec d'autres acteurs, les contraintes liées à la représentativité de l'architecture de la plateforme, l'existence d'un grand nombre d'acteurs, une large délégation par EDF des thèmes techniques vers la sous-traitance, …
Dans ces conditions, un nouvel arrivant ne peut pas arriver, décider de repartir à zéro et de tout reprendre, car cela nécessite un coût et certaines décisions peuvent se révéler très impactantes, un retour en arrière n'est pas toujours aisé, en cas de problème.

J'ai pu remarquer au cours de mon stage que le métier d'ingénieur ADIC demande beaucoup d'adaptation, il faut savoir être polyvalent sur de multiples domaines et prendre en main de nouvelles technologies pour être à jour. Dans cette idée et sur certains projets majeurs d'ADIC, j'ai pu observer les conséquences de l'évolution du périmètre et du contexte de certaines affaires.

La complexité de l'organisation en entreprise EDF est aussi un thème qui a suscité mon étonnement : multiplicité des groupes des services et des unités, circuits décisionnels complexes et délai lié aux processus administratifs.
Au sein du groupe ADIC, il est très important de formaliser les discussions et les échanges en interne ou concernant des affaires, cela permet de tracer et partager les décisions prises et éviter des sujets hors contexte ou bien, d'éviter des erreurs de compréhension. Formaliser est pourtant complexe, sur des points techniques et car cela nécessite des connaissances de base en informatique. Sans cela, le risque d'erreur dans le compte-rendu peut se révéler élevé. Cela m'a fait prendre conscience de mes axes d'améliorations sur la formalisation et m'a permis de m'améliorer.

Par ailleurs, j'ai remarqué l'importance d'un profil « technique » au sein d'EDF, les agents EDF étant majoritairement des chargés d'affaires, ils sont donc très orientés « gestion de projet ».
Dans l'informatique industrielle, un profil technique est un gros avantage, et permet de mieux vérifier l'exactitude ou les erreurs d'un sujet lors de tests expérimentaux ou sur un document.

Personnellement, j'ai trouvé que la coordination et la compréhension réciproque pouvait être compliqué entre les différents acteurs d'une affaire, à cause de connaissances techniques disparates et influer énormément sur la gestion du risque sur une affaire en informatique industrielle.
La cybersécurité, enjeu moderne de l'informatique, reste encore une découverte pour certains acteurs, et je trouve que certains sujets techniques tels qu'OPC UA ou la PKI (Public Key Infrastructure) auraient mérité, plus d'investissement, de connaissance, et de réflexion.

Je remercie ADIC de m'avoir pris en tant que stagiaire réseau, car cela m'a permis de prendre conscience, de mes points forts (mon profil technique acquis grâce à ma formation) et de certains de mes défauts, concernant la formalisation que j'essaierai d'améliorer au fur et à mesure. Le réseau, l'administration système et le scripting sont des sujets qui m'ont passionné et enrichi, c'est pour cela, que j'aimerais orienter mon choix de parcours dans l'informatique, après cette agréable expérience au sein d'EDF.
Ainsi, mon expérience personnelle et professionnelle acquise au sein d'ADIC sera un plus pour mon futur et m'accompagnera au fil des années.

VII. Remerciements

Dans cette lettre de remerciements, je tiens à remercier toutes les personnes ayant contribué à l'avancée de mon stage et fait en sorte qu'elle soit une excellente expérience.

Pour mes premiers pas dans le monde de l'entreprise, j'ai pu évoluer au sein d'une entreprise réputée, EDF-DIPDE et plus précisément au sein de C2I-ADIC, qui gère énormément de thème transverse en lien avec l'Architecture, la Donnée, l'Intégration et la Cybersécurité, en parfaite cohérence avec ma formation de DUT Réseaux et Télécommunications.

Tout d'abord, je souhaiterais remercier Philippe COL pour m'avoir aidé dans ma démarche de recherche de stage au sein d'EDF, et Franck SIAS, qui a pris le soin d'analyser ma candidature et de m'intégrer au sein de son groupe et un poste dans lesquels, je me suis pleinement épanoui et en totale adéquation avec ma formation.

Je tiens à apporter un grand remerciement à Didier PAQUET, mon tuteur de stage et référent architecte réseau, il a su me donner un excellent accompagnement et suivi au cours de ce stage. Il a effectué un énorme travail en amont, afin de me trouver des missions et sujets toujours passionnants et m'a apporté une aide précieuse à la rédaction de mon rapport de stage. Par ailleurs, il m'a donné de remarquables conseils professionnels et personnels qui me suivront tout au long de ma carrière. En résumé, encore un grand merci à Didier, pour son accueil, le temps passé ensemble et son écoute envers moi, en espérant pouvoir le rencontrer à l'avenir dans le monde professionnel.

Par ailleurs, je tiens à remercier Maxime, chargé d'affaires, qui m'a été d'un grand soutien lors de ce stage, il m'a été d'une grande aide (apport des documents liés à mes missions, suivi du stage, …).
Par ailleurs, Maxime a toujours pris de son temps pour me venir en aide lorsque j'avais des soucis techniques en plateforme et a toujours apporté des réponses à mes questions. Ses connaissances liées aux affaires du N4 et ses compétences techniques sont ses points forts, et c'est pour cela, qu'il représente une personne indispensable au sein d'ADIC.

De plus, je tiens à remercier Jean-Luc, chargé d'affaires, avec qui j'ai partagé mon bureau et m'a permis d'avoir des renseignements concernant les sujets qu'il traitait tels que CNC et LGP2I.
En outre, il m'a donné de précieux conseils sur le monde professionnel et m'a permis de prendre contact avec SNEF pour mes recherches d'alternances. Jean-Luc et Didier au sein de leur bureau, ont su apporter une ambiance toujours joyeuse même lors de moments difficiles, je leur souhaite le meilleur pour leurs projets futurs.

En outre, je tiens à remercier toutes les personnes du groupe ADIC, m'ayant si bien accueilli, je leur souhaite à tous une très bonne continuation dans leurs projets, et du courage dans les moments difficiles qu'ils auront à faire face.
Par conséquent, je souhaiterais remercier les enseignants de ma formation qui m'ont permis d'avoir les connaissances actuelles et m'ont toujours soutenu durant mes deux années de DUT.

VIII. Sitographie

Intranet VEOL [Vivre EDF OnLine]

Intranet Modélisation MEGA

EDF, 2019 [Consulté en Avril 2019], via https://www.edf.fr/groupe-edf/espaces-dedies/l-energie-de-a-a-z/tout-sur-l-energie/produire-de-l-electricite/le-fonctionnement-d-une-centrale-nucleaire

ASN Lexique, 2019 [Consulté en Avril 2019], via https://www.asn.fr/Lexique

Wikipédia Contrôle-Commande, 2018 [Consulté en Avril 2019], via https://fr.wikipedia.org/wiki/Système_numérique_de_contrôle-commande

ANSSI, 2019 [Consulté en Mai/Juin 2019], via https://www.ssi.gouv.fr/

Symposium sur la sécurité des technologies de l'information et des communications, 2019 [Consulté en Mai 2019], via https://www.sstic.org/2019/news/

Seclab Security, 2019 [Consulté en Mai/Juin 2019], via https://www.seclab-security.com/

Fortinet, 2019 [Consutlé en Mai 2019], via https://www.fortinet.com/

IT-CONNECT.FR, 2014 [Consulté en Juin 2019], via https://www.it-connect.fr/quelle-est-la-difference-entre-ftps-et-sftp/

OPC Foundation, 2019 [Consulté en Mai/Juin 2019], via https://opcfoundation.org/

VMware, 2019 [Consulté en Juin 2019], via https://www.vmware.com/fr.html

Kibana, 2019 [Consulté en Juin 2019], via https://www.elastic.co/fr/products/kibana

Puppet, 2019 [Consulté en Juin 2019], via https://www.elastic.co/fr/products/kibana

Zabbix, 2019 [Consulté en Juin 2019], via https://www.zabbix.com/

Culture Informatique, 2019 [Consulté en Juin 2019], via https://www.culture-informatique.net/cest-quoi-le-nat-cest-quoi-le-pat/

Le Monde Informatique : La vulnérabilité BlueKeep Windows 7/XP dangereuse selon la NSA, 2019 [Consulté en Mai 2019], via https://www.lemondeinformatique.fr/actualites/lire-la-vulnerabilite-bluekeep-windows-7-xp-dangereuse-selon-la-nsa-75543.html

IX. Glossaire

ADIC, Groupe de C2I, Architecture Donnée, Intégration et Cybersécurité

Automate : Un automate est un dispositif reproduisant en autonomie une séquence d'actions prédéterminées sans l'intervention humaine, le système fait toujours la même chose, ou s'adapte à des conditions environnementales perçues par ses capteurs

C2I, Contrôle Commande de l'Informatique Industrielle

C3D, Centre de compétences en cybersécurité

CCC, Clear Command Channel

CTT, Compliance Test Tools (OPC UA)

DUT, Diplôme Universitaire de Technologie

EDF-DIPDE, Electricité de France - Division de l'Ingénierie du Parc nucléaire, de la Déconstruction et l'Environnement

EPR, Evolutionary Power Reactor

FTP, File Transfer Protocol – **FTPS**, File Transfer Protocol Secure – **SFTP**, Secure File Transfer Protocol

JSON, JavaScript Object Notation, format de fichier de donnée JavaScript

KDT, Serveur et calculateur du réseau N4

MV, Management Visuel : C'est une terminologie anglo-saxonne regroupant plusieurs concepts de Lean management centrés sur la perception visuelle

Plateforme N4 (PF N4), Plateforme de Simulation Réseau des centrale nucléaires du palier N4

LGP2I, Logiciel de Gestion du Patrimoine d'Informatique Industrielle

NAT, Network Adress Translation

OPC UA, Protocole de communication

PROT C, chiffrement FTP/FTPS en clair

RDP, Remote Desktop Protocol

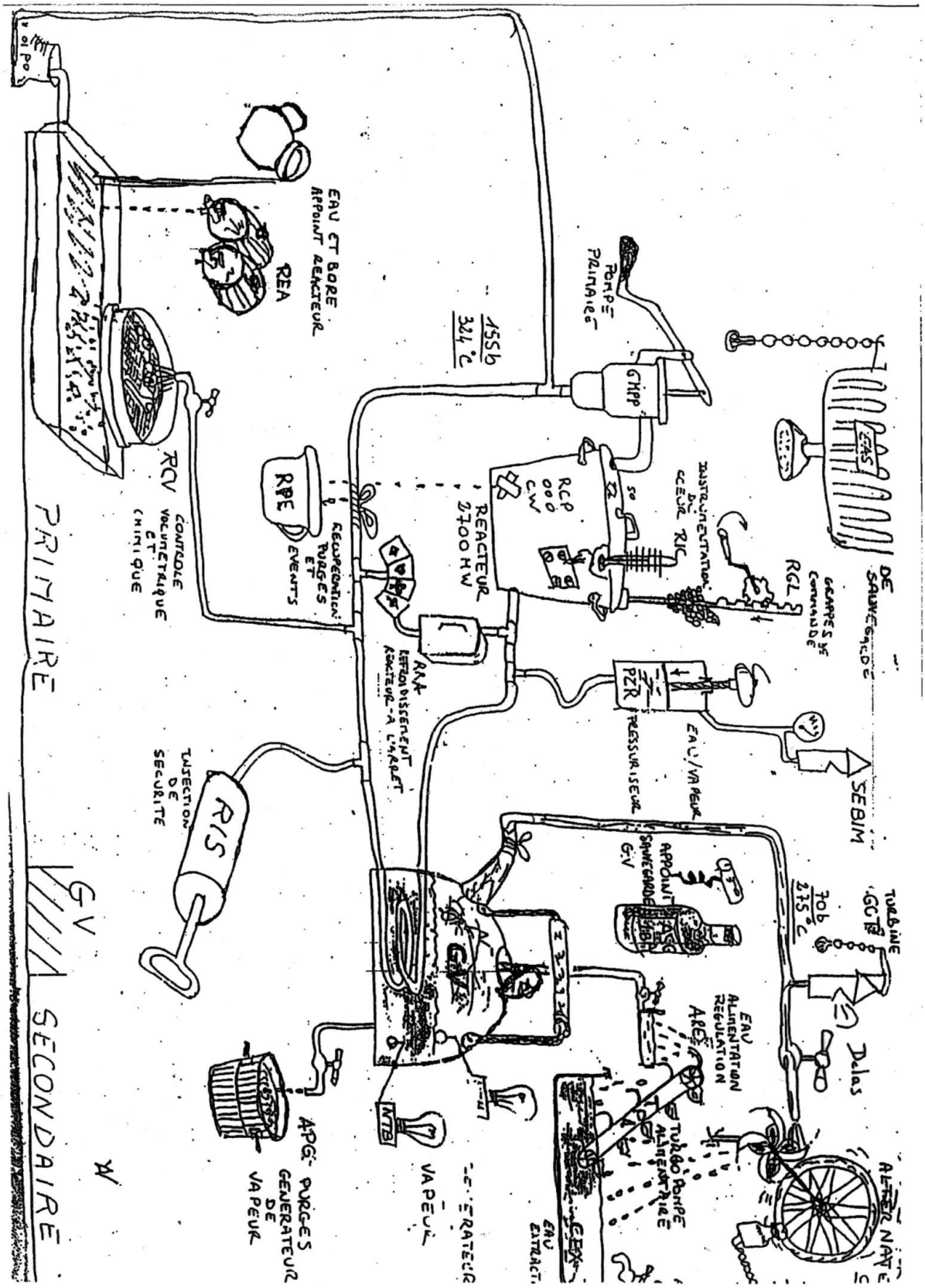
REX, Retour d'expérience

VBA, Visual Basic for Applications

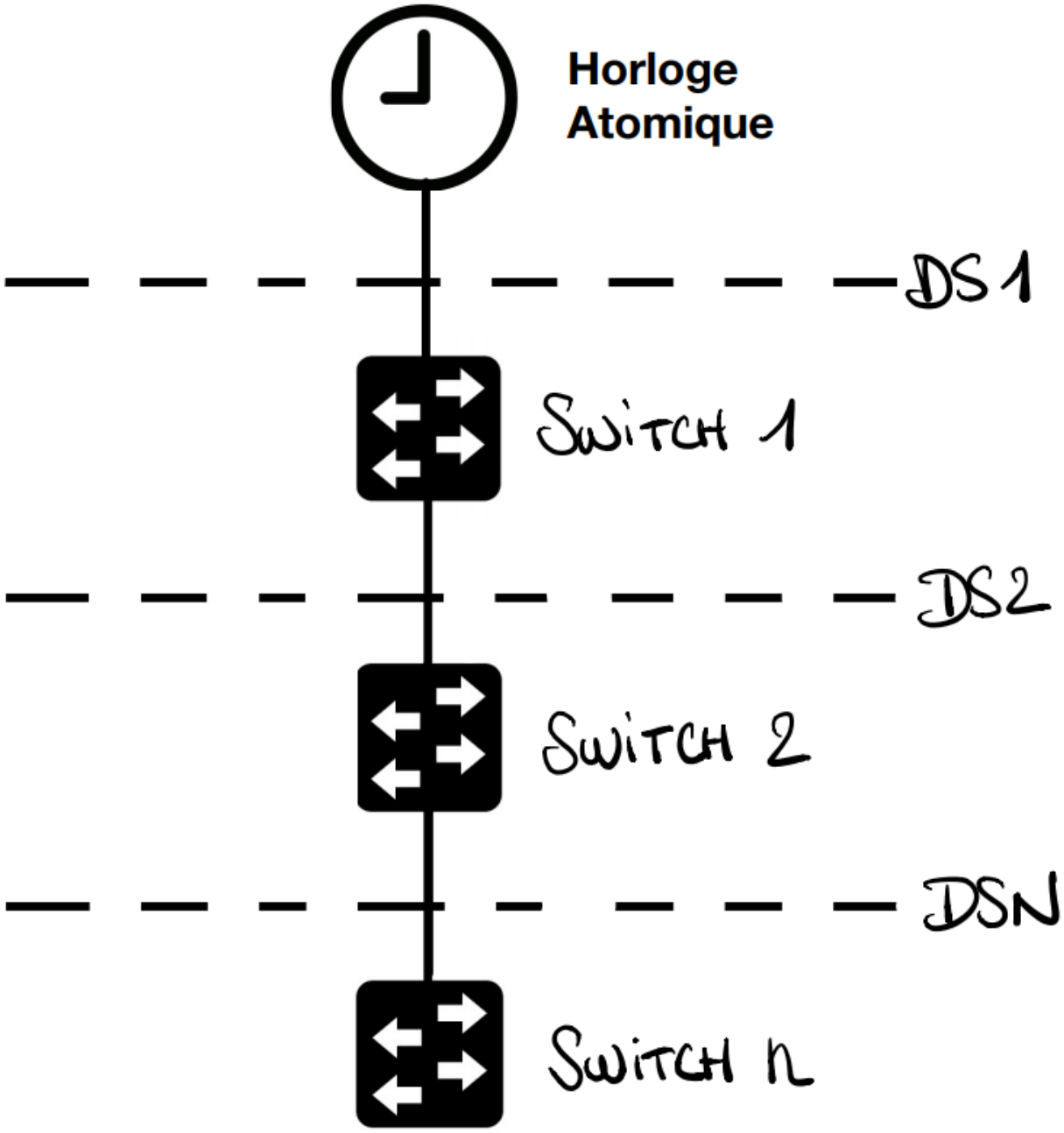
PARTIE ANNEXES

X. Annexes

A. Fiche Annexe Process Nucléaire



B. Fiche Annexe MEGA

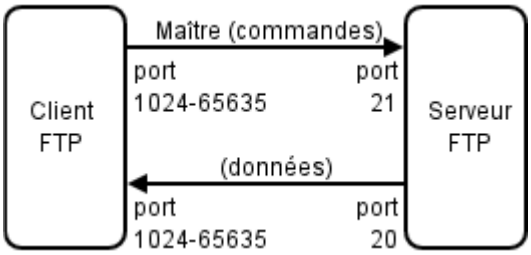


C. Fiche annexe FTPS Actif/Passif

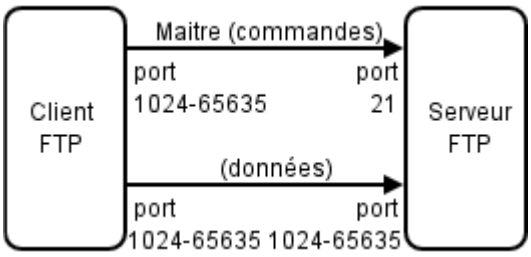
FTPS (“File Transfer Protocol Secure”) est un protocole de transfert de fichier (Client-Serveur), il se base sur TCP/IP et utilise les ports 20 (Data Channel) et 21 (Command Channel) en mode actif.

Il existe deux modes pour FTPS :

- **Le mode actif :** Le client FTP/FTPS initie l’échange depuis un port supérieur à 1024, en destination du serveur FTP/FTPS, qui lui est en écoute sur le port 21. Durant cette l’échange sur le Command Channel, le client indique son port sur lequel il souhaite recevoir des données (> 1024) et le port du serveur depuis lequel vont être envoyé les données sur le Data Channel (en mode actif, le port 20). Enfin, les données sont échangées (initiative par le serveur sur le Data Channel) sur le Data Channel.



- **Le mode passif** : On reste sur le même principe que le mode actif. On a toujours l’échange sur le Command Channel, depuis un port client supérieur à 1024 vers le port d’écoute par défaut du serveur, le port 21. Durant cette échange (Command Channel), le client donne le port sur lequel il souhaite recevoir des données (>1024), enfin, la différence se fait sur le port serveur sur lequel les échanges vont se faire. En mode actif, le port était alloué statiquement, le port 20 par défaut, et en mode passif, le port est alloué dynamiquement, sur un port supérieur à 1024. Ainsi, à la fin de l’échange dans le Command Channel, le serveur FTP/FTPS envoie au client FTP/FTPS, le port utilisé pour l’échange, afin que le client initie la communication sur ce port.



La dernière partie du FTP/FTPS mode passif présente son atout majeur, car il évite que le serveur FTP/FTPS initie l’échange, et créerait des risques de sécurité. En revanche, son implémentation reste complexe dans le cas où un FW, se trouverait entre le client et le serveur, car il nécessite d’ajouter une règle afin d’autoriser le transfert FTP/FTPS sur ce port dynamique (cette règle nécessite d’implémenter CCC sur FTPS pour ouvrir le port de façon dynamique).

L’avantage du FTPS mode passif est dû grâce à la négociation de port et au fait, que le client est toujours à l’initiative de communication.

D. Fiche annexe DENELIS

Seclab est une société française orientée cybersécurité, elle est née de la collaboration de trois experts de la cybersécurité :

- Xavier Facélina, entrepreneur spécialiste de la protection des systèmes et des réseaux
- Benoît Badrignans, docteur en microélectronique appliquée à la cybersécurité
- Pascal Sitbon, ingénieur en cybersécurité chez EDF R&D

En 2007, Pascal constate un besoin en cyber protection pour l'échange de donnée chez EDF R&D et que les solutions logicielles existantes sont insuffisantes. EDF R&D conçoit une solution, dépose un brevet et faitappel à NETHEOS (Société de cybersécurité) où travaille Xavier et Benoit, pour tester la première implémentation de leur brevet.

Ainsi, de 2007 à 2009, NETHEOS réalise pour le compte d'EDF R&D un produit qui bénéficie en 2010 d'une première certification par l'ANSSI.
Souhaitant poursuivre leur collaboration, Xavier, Benoît et Pascal fondent la société Seclab en 2011. Ils développent leur technologie DENELIS, entièrement maîtrisée et fabriquée en France par Seclab.

Leurs principaux produits sont le DENELIS (boitier de coupure réseau), le SCOOP (boitier de coupure USB) et le POCKET PASS.

DENELIS

SCOOP

POCKET PASS

E. Fiche annexe OPC UA

1. Présentation de OPC UA

OPC UA *(OPC Unified Architecture)*, développé par *OPC Foundation*, est un protocole de communication intermachine (M2M), il est particulièrement utilisé pour de l'automatisation industrielle. L'intérêt principal de cette technologie est l'interopérabilité des systèmes. OPC Foundation veille aux tests et à la certification des produits OPC. (Voir cf. Annexe OPC UA)

Le choix d'OPC UA est basé sur différents critères :

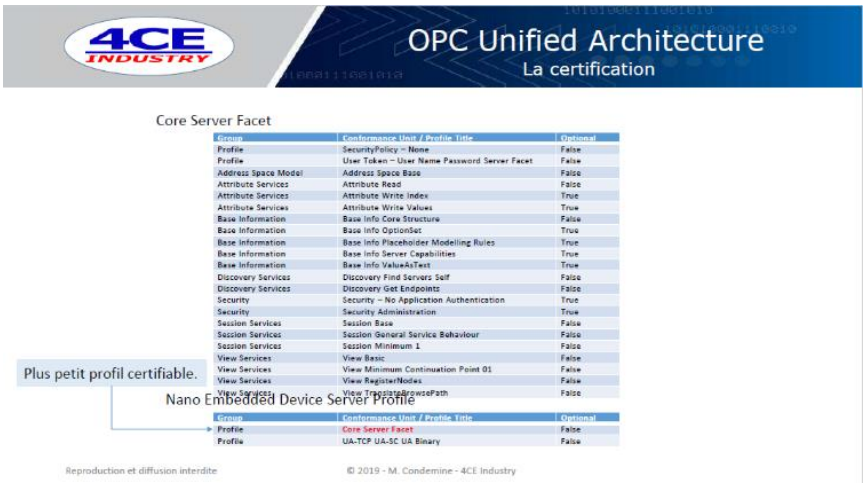
- Standard du marché / interopérabilité : Modèle standard Client/Serveur, un protocole basé sur le modèle OSI, avec une norme IEC 62541
- Donnée structurée : Modèle de données structuré (valeur, type, champs, …)
- Pérenne : Norme IEC,
- Multiplateforme (Windows et Linux) :
- Flux au Fil de l'eau (abonnement, lecture, écriture, …) : Les systèmes s'abonnent à des variables, et obtiennent des infos en temps réels
- Sécurisable : Signature et chiffrement, security policy, authentication settings, user token, …

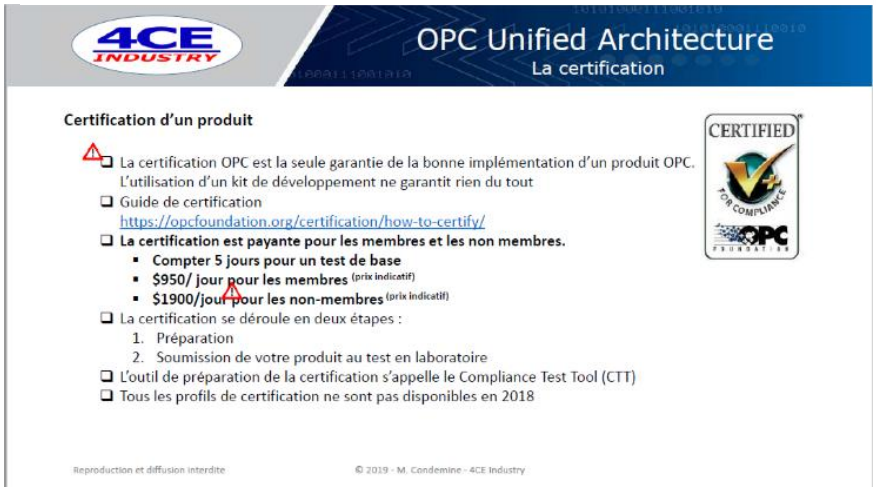
Pour résumer, OPC UA est une technologie complète, assez semblable à un protocole de communication. Il permet de faire de la redondance, des abonnements sur des variables pour des données temps réel, de la sécurité, des certifications, et bien d'autre possibilités.

2. Présentation des facettes et de la certification OPC UA

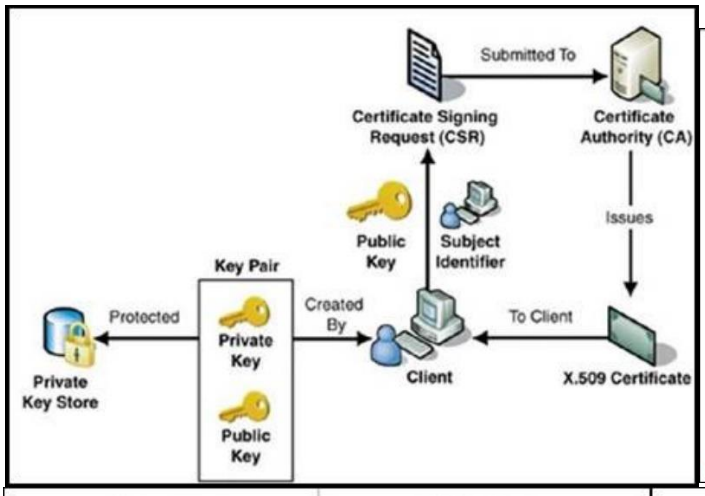
Le programme de certification de la fondation OPC exige que les produits basés sur OPC passent un niveau de test élevé pour garantir la conformité, l'interopérabilité, la robustesse et l'efficacité des ressources.
L'outil de préparation de la certification s'appelle le Compliance Test Tool (CTT).

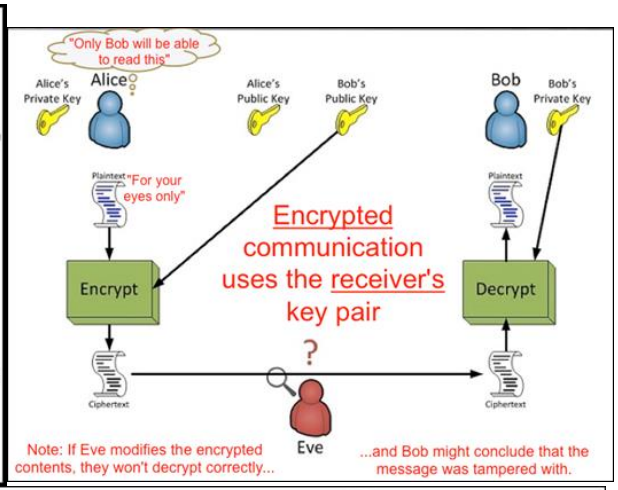
3. *Quelque slide de ma formation OPC UA*

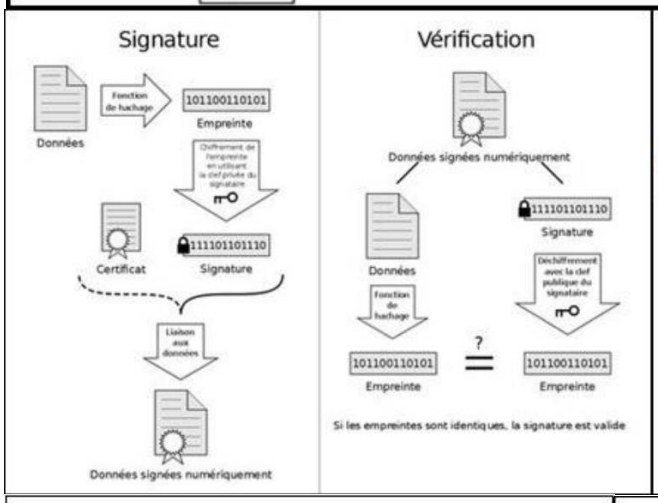


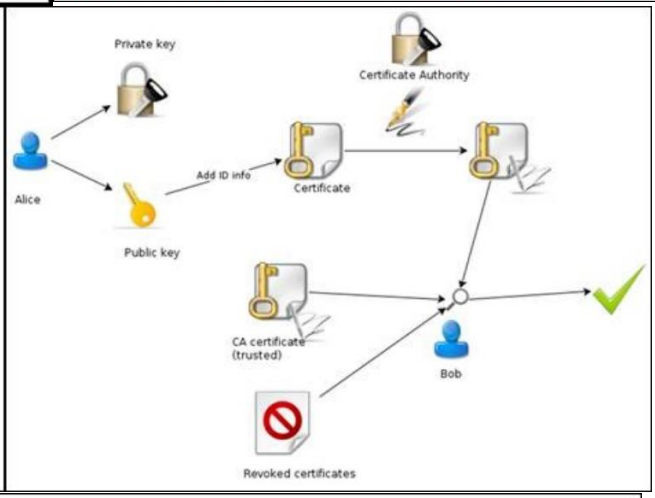


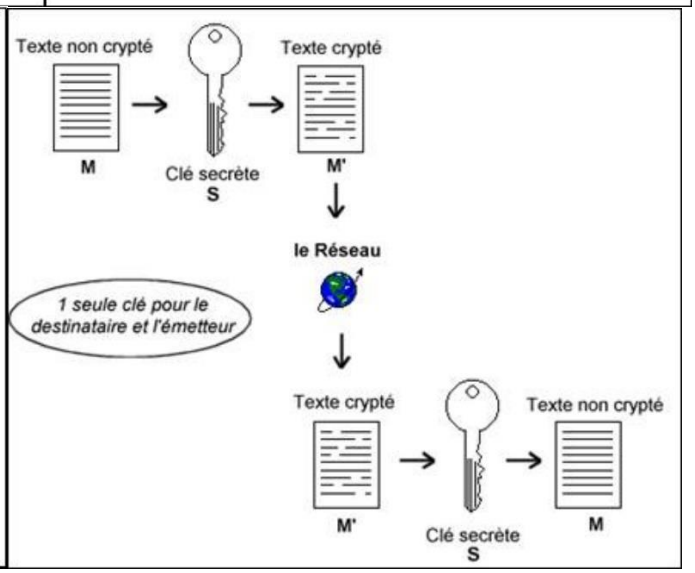
F. Annexe cryptographie (schémas pour la culture générale)





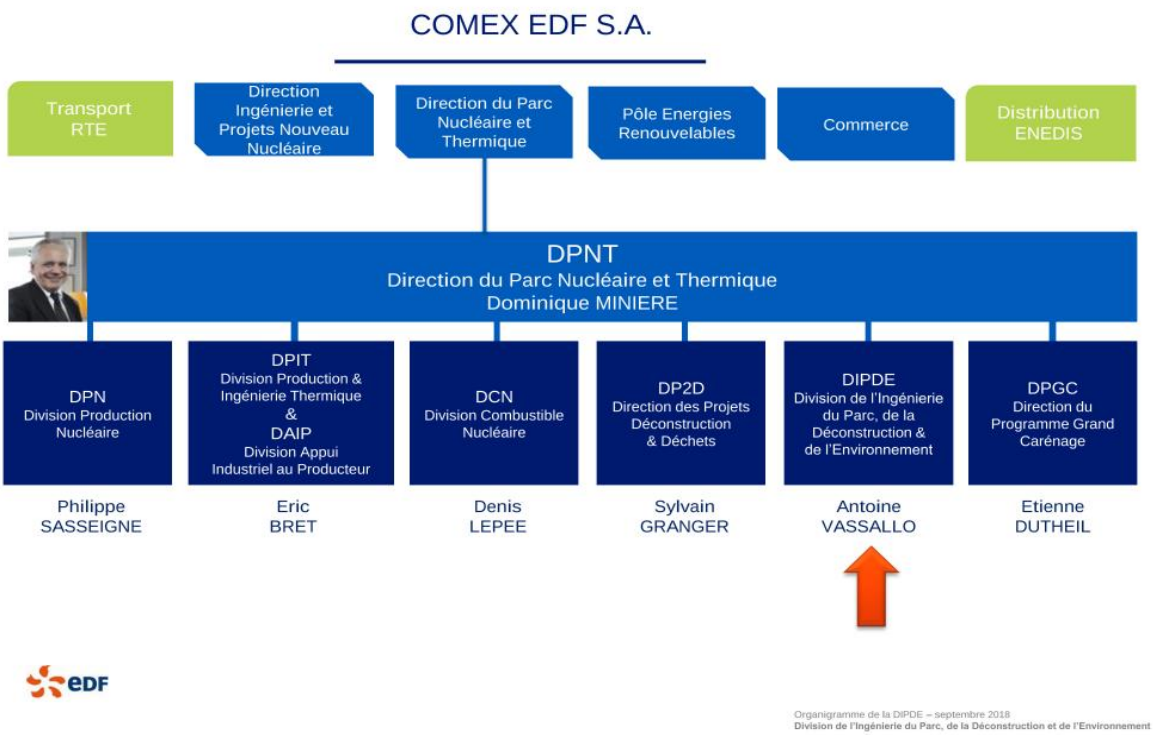






G. Partie annexes photos

1. Fiche Annexe Organigramme COMEX EDF



2. Fiche Annexe Organigramme DIPDE