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

Sensibilisation à la prise en compte de la cybersécurité à la conception dans le secteur nucléaire

Mathilde PAGE

Edvance

Responsable entreprise : Guillaume Gourlaouen

Responsable académique : Corinne Houssain

Table des matières

1 Introduction

En 2015, dans un contexte de tensions entre la Russie et l'Ukraine, l'attaque BlackEnergy a ciblé des centrales de production électrique ukrainiennes en période hivernale. Les cyberattaques sont de plus en plus nombreuses et les infrastructures critiques de production d'énergie sont des cibles privilégiées dans un contexte de montée des tensions internationales.

En 2017, la réglementation française a pris en compte le besoin impérieux de cybersécurité pour le secteur du nucléaire civil avec l'arrêté du 10 mars 2017 qui vient préciser les règles de sécurité relatives aux systèmes d'informations d'importance vitale.

Ce durcissement du cadre réglementaire en matière de cybersécurité concerne en particulier le projet Evolutionary Power Reactor (EPR2) piloté par Energie de France (EDF) qui est au cœur de la stratégie énergétique française avec le renouvellement du parc électronucléaire dans les années 2030.

Mon stage s'est déroulé au sein de l'équipe cybersécurité EPR2 du service conception et intégration contrôle commande d'Edvance située aux Jardins du Lou dans le septième arrondissement de Lyon. Cela m'a permis d'en apprendre davantage sur le domaine du nucléaire et le fonctionnement d'une entité d'ingénierie. J'ai dû notamment réaliser divers supports tels que des mémos ou des affiches de sensibilisation. J'ai eu aussi à accompagner des équipes dans l'analyse d'impact cyber de leur système. Afin de rendre compte des dix semaines et du contexte dans lequel s'est déroulé mon stage, le présent rapport s'articule autour des chapitres suivants :

En premier lieu, une brève présentation d'Edvance et de ses projets en France et à l'international. Par la suite, le contexte projet, technique et organisationnel de mon stage. Enfin, il sera question de la nature des missions qui m'ont été confiées, de mes réalisations et des différents savoirs que j'ai pu acquérir. Ainsi, je terminerai par une brève conclusion.

2 Présentation de l'entreprise

2.1 Historique

Edvance a été créée le 30 mai 2017, elle est détenue à 80% par EDF et à 20% par Framatome qui est le concepteur historique des chaudières de réacteurs nucléaires et un fournisseur incontournable de services de maintenance des réacteurs. Framatome est également une filiale à 80,5% du groupe EDF (les 19,5% restants étant détenus par Mitsubishi Heavy Industries, MHI).
Le siège social d'Edvance est actuellement implanté dans le 8^{e} arrondissement de Paris.
Edvance est une firme française du groupe EDF implantée en France et à l'internationale. En effet, elle possède six sites aux quatre coins de la France (en région parisienne, à Lyon, à Flamanville et à Penly), mais elle possède aussi des sites en Allemagne à Erlangen et en Grande-Bretagne à Bristol.
Les effectifs d'Edvance sont de l'ordre de quatre mille collaborateurs. Ces collaborateurs recouvrent différents statuts : EDF (mis à disposition), Framatome (mis à disposition) et les statutaires Edvance. De ce fait, la culture de l'entreprise est très diversifiée selon l'organisme d'origine.

2.2 Activité

L'activité principale d'Edvance est de prendre en charge les projets de conception et de réalisation d'îlots nucléaires et de contrôle-commande des réacteurs nucléaires en construction, en France et à l'international. L'entreprise est notamment impliquée dans 6 projets :

- Flamanville 3 (FA3) étant le premier réacteur EPR en France (tout d'abord nommé « European Pressurized Reactor » puis « Evolutionary Pressurized Reactor »). Ce réacteur étant une version modernisée des réacteurs déjà présents sur le parc nucléaire actuel en France rajoutant des mesures post-Fukushima, une durée de vie plus longue (conception sur une base d'un fonctionnement de 60 ans), plus de redondance et pour finir plus de performance passant d'une production maximale de 1450 mégawatts électriques (MWe) à 1670 MWe ;
- L'EPR2 sur lequel j'ai travaillé dans le cadre de mon stage et dont la cible est le renouvellement du parc électronucléaire français dans les années 2030 quand les réacteurs du parc historiques seront progressivement arrêtés ;
- Nuward petit réacteur modulaire ou SMR pour « small modular reacteur » étant une centrale produisant 340MWe (avec deux unités de 170 MWe). A l'échelle internationale, la cible des SMR peut être de s'imposer comme un nouveau standard, avec des délais de construction réduits permettant le remplacement de centrales à charbon produisant entre 300MWe et 400 MWe.
- Dans le projet de construction de 2 réacteurs EPR à Hinkley Point C (HPC) dans le sud-ouest de la Grande-Bretagne et de deux autres à Sizewell C dans le sud-est ;
- L'EPR1200 étant un réacteur produisant 1200 MWe à Dukovany en République Tchèque ;
- Jaitapur nuclear power plant (JNPP) qui est un projet de 6 réacteurs EPR en Inde.

Edvance travaille au service de directions projets. Dans le contexte français la direction projet représente elle-même l'exploitant du parc nucléaire.

Vis-à-vis de la cybersécurité, les systèmes d'information sont répartis en quatre domaines distincts : le domaine industriel, le domaine protection de site, l'informatique de gestion et le domaine des Télécommunications d'exploitation.
L'équipe cybersécurité dans laquelle j'ai pu réaliser mon stage travaille essentiellement sur les systèmes d'information du domaine industriel parmi lesquels se trouvent le contrôle commande du réacteur ainsi que des contrôles commandes de différents systèmes dédiés à des activités d'exploitation (manutention, traitement d'effluents etc.).

2.3 Organigramme du service dans lequel s'est déroulé mon stage

Mon stage s'est déroulé au sein de la branche Electricité et Contrôle Commande (EIC) du projet EPR2.
Le schéma ci-dessous montre la répartition du pilotage des activités électricité d'une part et contrôle-commande d'autre part au sein de la branche. Le pilotage de chaque scope est assuré par un Senior Project Manager (SPM) appuyé par un architecte.

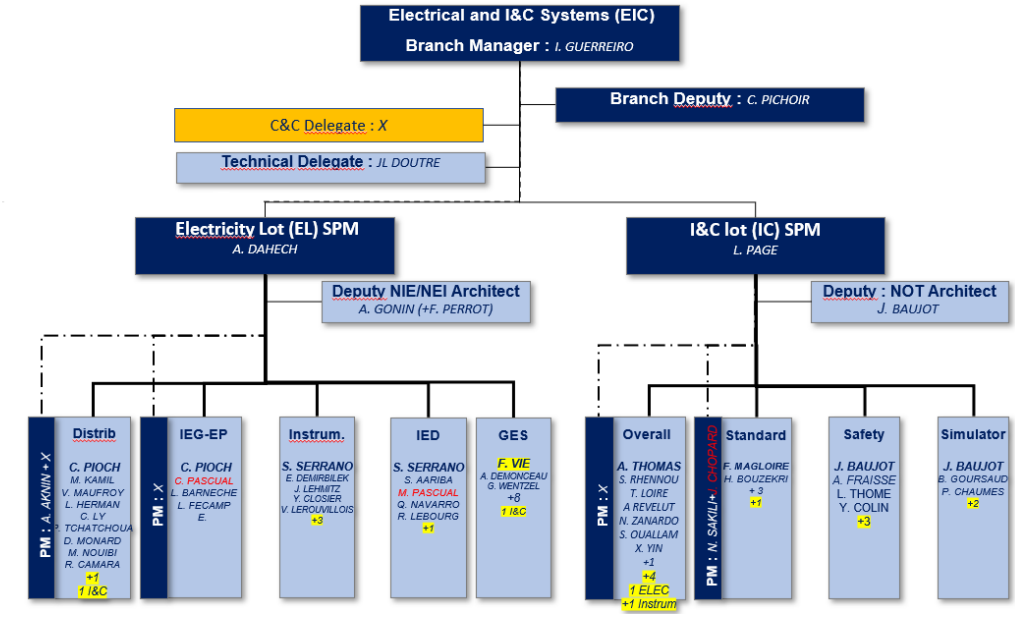

Figure 1 : Organigramme de la branche EIC

3 Présentation du cadre technique général du sujet

3.1 Contexte

L'arrivée en fin de vie du parc nucléaire actuel en France dans les années 2030 voire 2040 pose une problématique de sécurité d'approvisionnement électrique à terme. La stratégie énergétique française prévoit le renouvellement de la capacité de production nucléaire grâce au programme EPR2. L'objectif de ce projet, est l'optimisation par rapport à son prédécesseur qu'est l'EPR de FA3, tout en conservant ses atouts tels que sa puissance de 1670 MWe, bien supérieure à celle des centrales déjà en place sur le parc nucléaire français produisant entre 900 MWe et 1450 MWe. De plus, le projet prévoit aussi l'intégration de mesures post-Fukushima dès la conception ainsi qu'un récupérateur de corium fondu de 170 m² permettant de collecter et refroidir les matériaux fondus dans le cas où la fusion du cœur du réacteur serait suivie d'une percée de la cuve par le corium. Les rejets environnementaux seront également réduits de 20 % par rapport aux réacteurs actuellement en exploitation sur le parc nucléaire français. La première version de ce réacteur sera construite en France à Penly en Seine-Maritime sur un site existant où deux réacteurs de 1300 MWe sont actuellement exploités.

Avant cela, il faut noter que le projet suit différentes phases de l'ingénierie système basée sur le modèle du cycle en V (Figure 2). Tout d'abord on commence par définir les grands besoins à satisfaire et établir les spécifications pour pouvoir y répondre, on peut comparer cette phase à l'écriture d'un cahier des charges. C'est notamment dans cette partie qu'on réalise une conception conceptuelle en 2 dimensions et en 3 dimensions qu'il faut ensuite valider avec le génie civil.

À la suite de cela, il y a la phase d'approfondissement de cette conception avec la construction de l'architecture. Cette phase permet d'assurer le dimensionnement des principaux systèmes et composants majeurs ainsi que des bâtiments pour les accueillir. Puis, on réalise une conception plus détaillée. En effet, l'étape précédente permettait de réfléchir aux premières solutions et le dimensionnement des pièces. Durant cette phase, on réalise l'ensemble des études permettant d'avoir les plans nécessaires à la fabrication des matériels et à la réalisation de l'ensemble des travaux, cela comprend notamment l'étude de l'installations des chemins de câbles, calculs de la tuyauterie, l'affectation des départs aux tableaux électriques, etc.

Lorsque tout est validé avec le génie civil et les ingénieurs systèmes, on rentre dans l'appel d'offre. Une discussion avec de potentiels fournisseurs va commencer afin de trouver l'entreprise la plus à Lorsque mon stage a débuté, les différentes équipes étaient à cheval entre la phase d'architecture et le démarrage de la phase de conception détaillée qui fait suite aux appels d'offre et la signature des contrats même de réaliser la prestation demandée. (Figure 2).

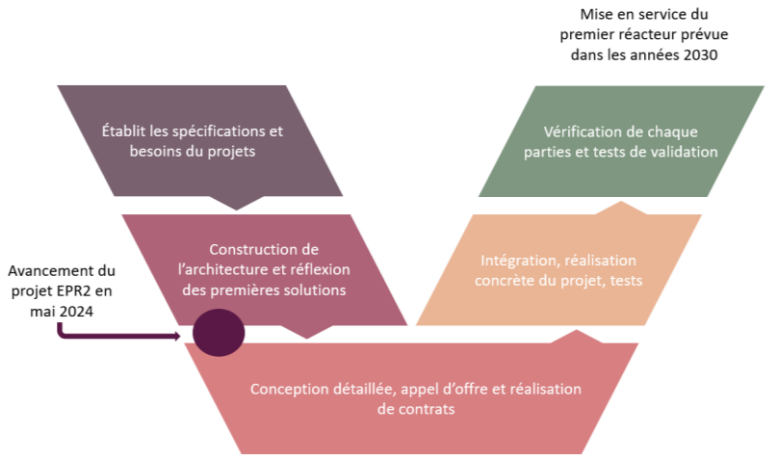

Figure 2 : Cycle en V du projet

Pour le projet EPR2, le référentiel prévoit que la cybersécurité soit prise en compte dès la conception des systèmes. Cela signifie que, dans la mesure où des systèmes prévoient d'assurer des fonctions grâce à des équipements numériques, les exigences de cybersécurité EPR2 doivent systématiquement faire l'objet d'une analyse et d'une implémentation dans l'architecture des systèmes.
L'équipe cybersécurité du projet doit assurer la bonne application du référentiel et l'accompagnement des responsables systèmes dans la prise en compte de la cybersécurité à la conception. Pour y parvenir, une communication systématique est nécessaire et celle-ci doit s'appuyer sur des supports de communication adaptés et répondant aux différents points clefs à connaître par les acteurs.

3.2 Comment fonctionne une centrale nucléaire ?

Afin de travailler sur le projet d'un nouveau réacteur nucléaire et d'en étudier ses systèmes, il est d'abord important de bien saisir les bases de ce que c'est et comment cela fonctionne. De ce fait, chaque arrivée se marque par une initiation au fonctionnement d'une centrale nucléaire ainsi qu'une présentation d'un plan architectural de la centrale dans son ensemble.

La création d'électricité grâce à une centrale nucléaire est rendue possible grâce à l'utilisation de plusieurs circuits d'eau distincts et fermés, chacun jouant un rôle spécifique dans la conversion de l'énergie.

Tout d'abord, le cœur du réacteur est constitué d'assemblages de crayons combustibles (Figure 3). Les crayons sont des tubes métalliques fermés de très faible épaisseur contenant des pastilles composées de combustible (dioxyde d'uranium). Ces pastilles sont maintenues entre elles à l'aide d'un ressort. Cet assemblage s'appelle l'assemblage combustible (AC).

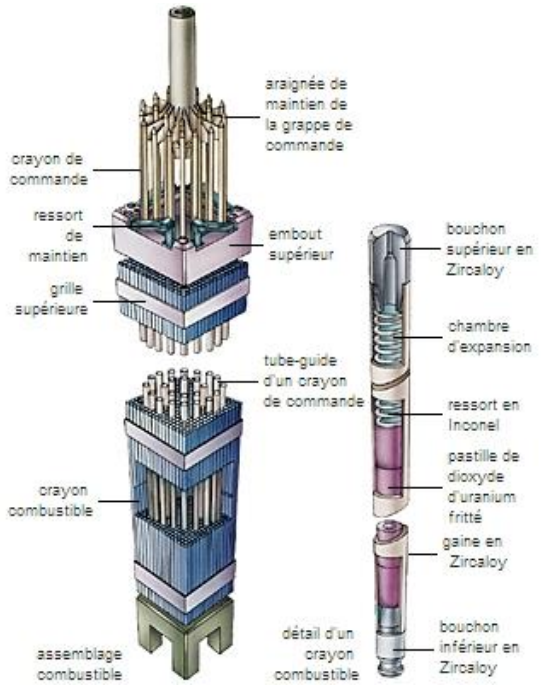

Figure 3: Assemblage combustible (source : Larousse)

La fission des atomes d'uranium dans les crayons combustibles libère une grande quantité d'énergie. Cette chaleur dégagée dans le combustible fait augmenter la température de l'eau qui vient circuler de bas en haut du cœur au contact de la gaine des crayons combustibles jusqu'à atteindre une température de l'ordre de 320°C en sortie de cœur. L'eau est maintenue sous pression (environ 155 bar) grâce à un pressuriseur qui va permettre d'empêcher l'eau du circuit primaire de bouillir et par extension de s'évaporer.

Les grappes de commande (nommées « crayons de commande » dans la Figure 3) sont absorbantes en neutrons et permettent de contrôler la réaction ainsi que de maintenir la puissance du réacteur au niveau désiré. De plus, la concentration en Bore du circuit primaire joue également sur la réactivité du cœur. En effet, le Bore est un ralentisseur ou absorbeur de neutrons lents. De ce fait, il est mélangé à l'eau du circuit primaire permettant de contrôler les réactions. Dans les cas les plus graves, les crayons de commande peuvent s'enfoncer complètement au sein du cœur du réacteur ce qui a pour effet d'arrêter quasi-instantanément le réacteur et donc de limiter le risque. Ce circuit fermé est nommé le circuit primaire (Figure 4).

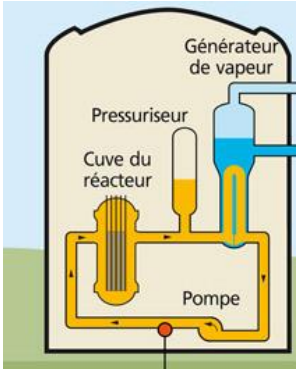

Figure 4 : Circuit primaire (source EDF)

Le générateur de vapeur constitue un échangeur thermique entre le circuit primaire et le circuit secondaire (Figure 5). Dans ce générateur de vapeur, l'eau « chaude » passant dans des tuyaux du circuit primaire vient réchauffer l'eau « froide » du circuit secondaire. La quasi-totalité de l'eau va alors se transformer en vapeur permettant d'entraîner des turbines. Ces turbines sont couplées à des générateurs qui vont alors convertir l'énergie mécanique en énergie électrique (courant électrique alternatif). Par la suite, un transformateur va venir élever la tension électrique de sorte qu'elle soit adaptée au réseau de transport.

La vapeur d'eau utilisée pour faire tourner les turbines est ensuite refroidie grâce à un condenseur afin de redevenir à l'état liquide et donc d'être réutilisée dans le processus. Dans ce condenseur circule de l'eau froide souvent prélevée dans une source naturelle tel qu'un fleuve, la mer ou venant d'un aéroréfrigérant transférant la chaleur à l'air ambiant. Ce circuit permettant de refroidir la vapeur produite dans le circuit secondaire s'appelle le circuit de refroidissement.

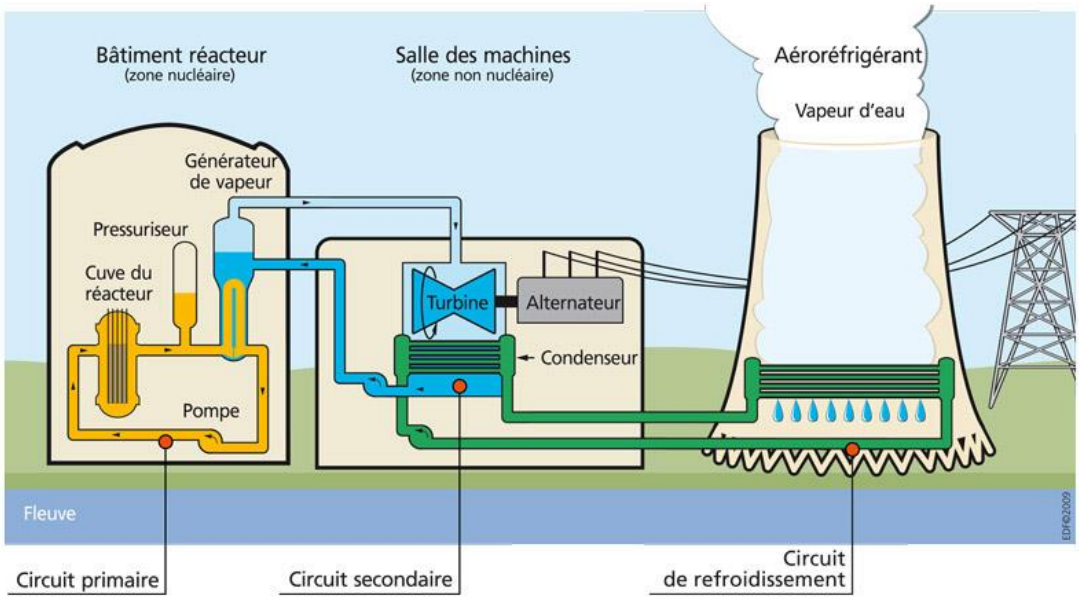

Figure 5 : Fonctionnement d'une centrale avec aéroréfrigérant (source : EDF)

3.3 Objectif du stage

Ma première mission était de réaliser divers supports de sensibilisation se basant sur différentes composantes de référentiel cybersécurité du domaine industriel : le référentiel cybersécurité EPR2 et des principes de sécurité de l'entreprise. Pour cela j'ai eu à me familiariser dans un premier temps avec les différentes normes et lois s'appliquant aux systèmes d'information d'importance vitale ainsi que les différentes documentations traitant de la cybersécurité chez Edvance. Par la suite j'ai eu à étudier plus en profondeur certaines de ces documentations afin de les synthétiser dans plusieurs maquettes. Ces supports sont alors transmis pour validation à différents acteurs de référence afin de choisir la plus pertinente et d'apporter des modifications en fonction des besoins spécifiques.

J'ai eu à réaliser par la suite une seconde mission qui consistait à accompagner les équipes de manutention pour établir ensemble le Degré de Sécurité (DS) de deux systèmes. J'ai notamment eu à comprendre le fonctionnement de systèmes ainsi qu'à analyser ce qui le compose afin d'identifier les risques liés à la perte de confidentialité, d'intégrité ou de disponibilité selon 3 catégories que sont la sûreté, la performance et la sécurité de site.

4 Présentation du travail réalisé

4.1 Partie I : Sensibilisation des équipes

4.1.1 En quoi consiste la sensibilisation dans ce contexte

La sensibilisation est un processus crucial dans la diffusion de connaissances et la mobilisation collective. Elle consiste à éveiller la conscience et l'attention des individus à l'égard d'une problématique, d'une cause ou ici d'une procédure obligatoire. Cela implique de diffuser des informations sur divers supports tel que des affiches, des présentations ou encore des plateformes de cours en ligne afin d'encourager la réflexion et l'action. En suscitant une prise de conscience et en encourageant l'engagement, la sensibilisation cherche à provoquer un changement positif dans les attitudes et les comportements.

Comme indiqué au paragraphe 0 et illustré en Figure 2, à mon arrivée au sein de l'entreprise, les différents contrats étaient à des niveaux d'avancement variables : entre phase de spécification et phases d'appels d'offres. En l'espace d'un mois, j'ai pu constater les difficultés de différents responsables de conception à prendre en compte la cybersécurité dans la démarche d'ingénierie. Il était donc important d'aider les différents collaborateurs à mieux assimiler certains points clés de la démarche cybersécurité tels que les exigences à appliquer au contrat, la démarche à suivre avec les étapes incontournables et leur jalonnement, ainsi que la base des principes fondamentaux de la sécurité informatique dans le nucléaire imbriquant différents concepts dans une architecture.

Dans ce contexte il était fondamental que chacun des responsables systèmes connaisse les exigences de cybersécurité et soit en mesure d'en discuter avec les potentiels fournisseurs.

4.1.2 Réalisation d'un support

La création d'un support quel qu'il soit suit différentes étapes. Tout d'abord, il y a le début du projet qu'on peut aussi nommer l'initialisation. Durant cette étape, je commence par prendre connaissance de la documentation associée. Les informations brutes sont alors triées par catégorie au sein d'une fiche Excel, puis traduites en français si nécessaire (la langue du projet EPR2 étant l'anglais). Lorsque tout est classé et organisé, je réalise entre 2 et 3 croquis afin de couvrir plusieurs possibilités et de laisser le choix parmi les différentes propositions.

Ensuite, vient la phase de réalisation du support. Je réalise alors les différentes maquettes basées sur les croquis que j'ai pu faire lors de l'étape précédente. Cette maquette sera alors présentée à différents acteurs de référence tels que le responsable de la sécurité des systèmes d'information du domaine industriel (RSSII) ou alors le service cybersécurité couvrant l'ensemble des projets. Ce moment d'échange permet d'améliorer les supports afin de correspondre au mieux aux besoins des différentes équipes. De cette manière, certains supports pourront être utilisés sur une communauté plus large de collaborateurs couvrant différents projets en plus de l'EPR2.

Après avoir peaufiné les derniers détails, le support final va alors être validé d'un commun accord entre tous les services traitant de la cybersécurité. Afin d'être par la suite présenter aux correspondants cybersécurité des différents métiers au travers d'un comité. Chaque support va alors avoir son propre canal de publication que ça soit au sein de la newsletter hebdomadaire ou mensuelle de l'entreprise, d'être affichée dans les bureaux, d'être présentée en plénière ou alors d'être distribué au sein des différents services.

4.1.3 Support sur les exigences applicables aux produits

La réalisation d'un support suivant toujours le même fil conducteur (comme vu au paragraphe 4.1.2), je vous propose de vous détailler uniquement la réalisation de mon premier support soit celui sur les exigences applicables aux produits.

Les exigences à appliquer dans le contrat en termes de cybersécurité se distinguent en deux catégories :

- Tout d'abord, on retrouve les exigences applicables vis-à-vis des produits comportant la sécurité des réseaux, le contrôle d'accès physique aux équipements, la remontée de journaux, la cybersurveillance des équipements et réseaux ou encore la reprise d'activité en cas d'évènement lié à la cybersécurité (tels que des pertes de disponibilité ou d'intégrité).

- Ainsi que les exigences applicables sur les activités permettant de garantir que l'organisation prévoit les mesures nécessaires pour un développement sécurisé. Parmi ces exigences : le cycle de vie, l'identification et le traitement des risques, l'accès physique et logique au matériel, la défense contre les malveillances numériques, le maintien en condition de sécurité, etc. Ces exigences sont applicables indépendamment de la sensibilité du produit. Elles sont également qualifiées d'exigences « transverses ».

Ma première mission a été d'illustrer en un support au format A4 les exigences à la conception des systèmes d'informations industriels applicables aux produits. En effet, il s'agit des exigences qui impactent directement les activités de conception.

J'ai commencé par lire le référentiel applicable au domaine industriel EPR2. La documentation commence par rappeler les grands principes de la démarche cybersécurité EPR2 tels que le classement en degré de sécurité (que j'expliquerai par la suite), l'existence d'un socle d'exigences sur les activités, les différentes normes, documentations et lois sur lesquelles le document se repose. Puis, on retrouve 74 exigences en anglais classées dans 7 catégories : services de sécurité réseau, administration réseau, contrôle d'accès physique, collecte de journaux, surveillance des équipements, surveillance des réseaux et pour finir la capacité de l'équipement à se remettre d'un évènement tel qu'une attaque. Pour chacune des exigences, il est précisé le contexte selon lequel l'exigence est applicable, la référence, l'auteur et les normes ou réglementations sur lesquelles elle se repose.

Lorsque j'eus fini de les lire, je les ai traduites puis triées à nouveau sur la base de 6 nouvelles catégories qui me semblaient pertinentes dans la compréhension : échange de données ; sécurité physique ; authentification ; journaux et supervision ; administration et sauvegarde. Ces catégories ont été retravaillées pour prendre en compte des catégorisations mieux adaptées à des échanges avec des autorités. Ce travail étant fini, j'ai pu commencer à réaliser différents croquis (Figure 5, 6).

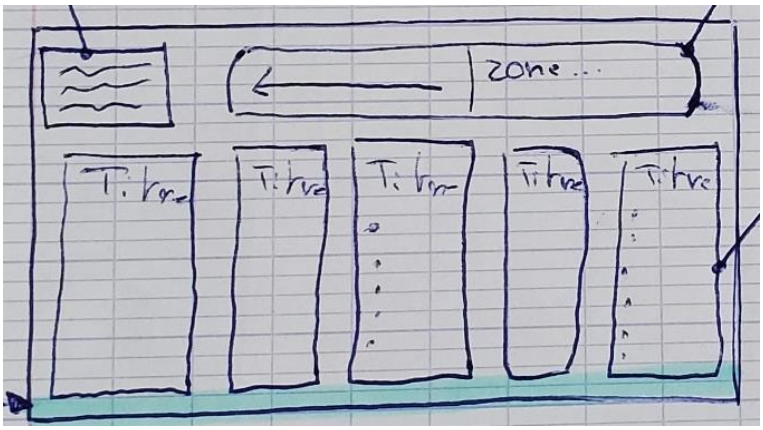

Figure 6: Croquis validé pour le support

Les différents croquis réalisés, ils passent une première validation afin de déterminer la représentation la plus pertinente et compréhensible. Puis le croquis ayant été validé (Figure 5), je commence à réaliser une première version en incluant les règles triées dans chacune des catégories. Cette première version (Figure 7) est assez dense en information. En effet, pour être la plus précise possible, j'avais inscrit toutes les exigences traduites par catégories sans faire de synthèse.

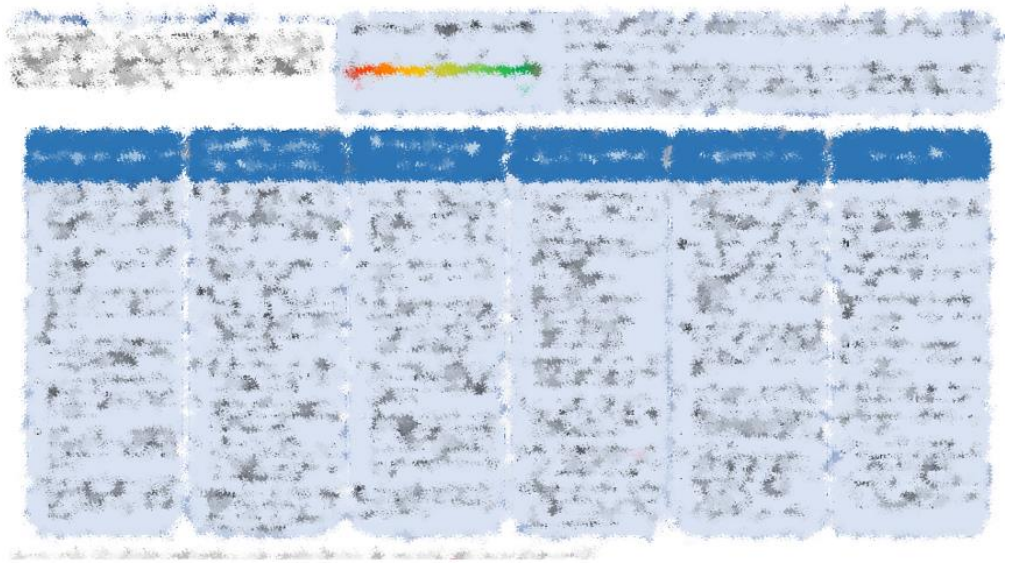

Figure 7: Première version du support sur les exigences

Après avoir réalisé cette première maquette, j'ai eu la chance d'avoir une discussion avec un alternant Edvance travaillant également sur la sensibilisation de collaborateurs dans le cadre du projet de HPC. Il m'a alors montré son travail et m'a fait son retour d'expérience. Suite à cet échange, j'ai pu tirer divers enseignements tels que l'importance d'être très synthétique et explicite ce qui manquait à ma première version du support. En effet, avant de réaliser un support, il est important de se poser plusieurs questions fondamentales telles que :

- Qui est la cible ?
- Quel message veut-on transmettre ?
- Le périmètre : qu'est-ce qui est pertinent et qu'est-ce qui ne l'est pas ?

En effet, le but de la sensibilisation ici et de prendre conscience de ce qu'il faut appliquer dans ses appels d'offres de sorte à faciliter le travail de recherche ainsi que d'éviter le traitement d'une anomalie (en cas d'oubli de rajout des exigences cyber) pour la personne ciblée.

Aussi, il est important de réaliser des supports colorés afin d'attirer l'œil et de donner l'envie de lire le support. Pour finir, il m'a expliqué à quel point être humble et demander divers retours était important pour peaufiner et améliorer les supports. Bien que le sujet principal fût les exigences, pour plusieurs personnes à qui j'ai montré mon support, la première chose vers laquelle se dirigeait leur regard était la flèche présentant les différents DS. J'ai donc modifié le support en prenant compte de ses conseils ainsi que des différentes remarques qui ont pu survenir lors des moments d'échanges sur le support.
La version améliorée de ce support (Figure 8) a passé la première phase de validation auprès de mon tuteur.

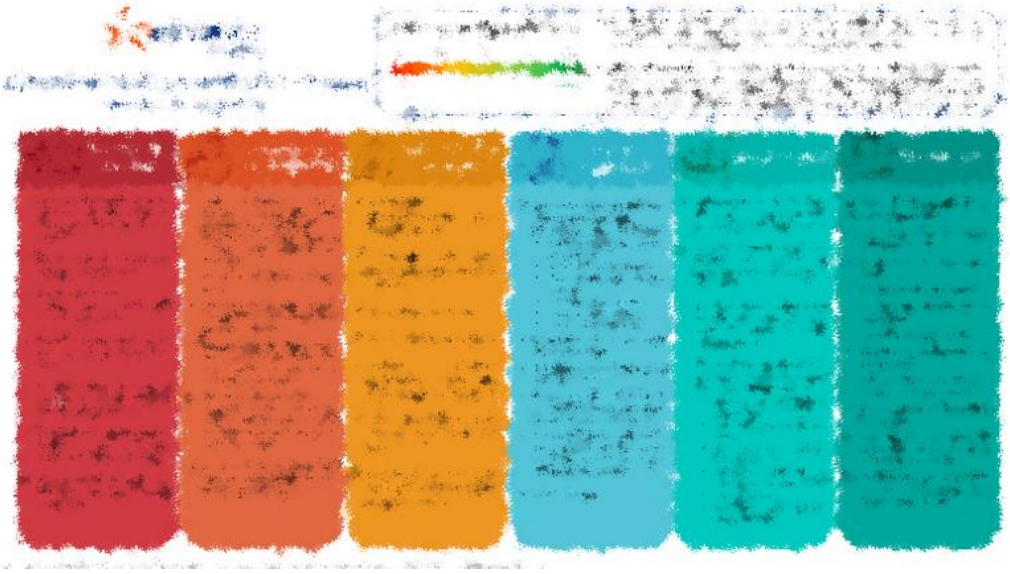

Figure 8: Version améliorée du support sur les exigences

Il a alors été présenté au sein d'une réunion hebdomadaire où se rencontrent tous les acteurs cyber travaillant sur le projet EPR2 afin d'être amélioré et corrigé. De nombreuses améliorations furent proposées, notamment la proposition d'afficher en rouge les choses à ne pas faire ainsi qu'éviter de mettre les colonnes de la même couleur que la flèche de classement en DS pour éviter les confusions qui pourraient rattacher une colonne à un DS en particulier. À la suite de quelques réunions et améliorations, il fut validé par l'équipe cybersécurité du projet EPR2.

La deuxième phase de validation ayant été passée, le support va passer une troisième validation auprès de toute l'équipe cybersécurité couvrant les divers projets pour valider la cohérence et confronter les différents points de vue. Le support est alors modifié une ultime fois en prenant compte de toutes les remarques et commentaires.

Enfin, le support final validé par les différentes équipes (Figure 9 et 10) est présenté aux correspondants cybersécurité des différents métiers en comité cybersécurité EPR2 le mercredi 12 juin 2024.

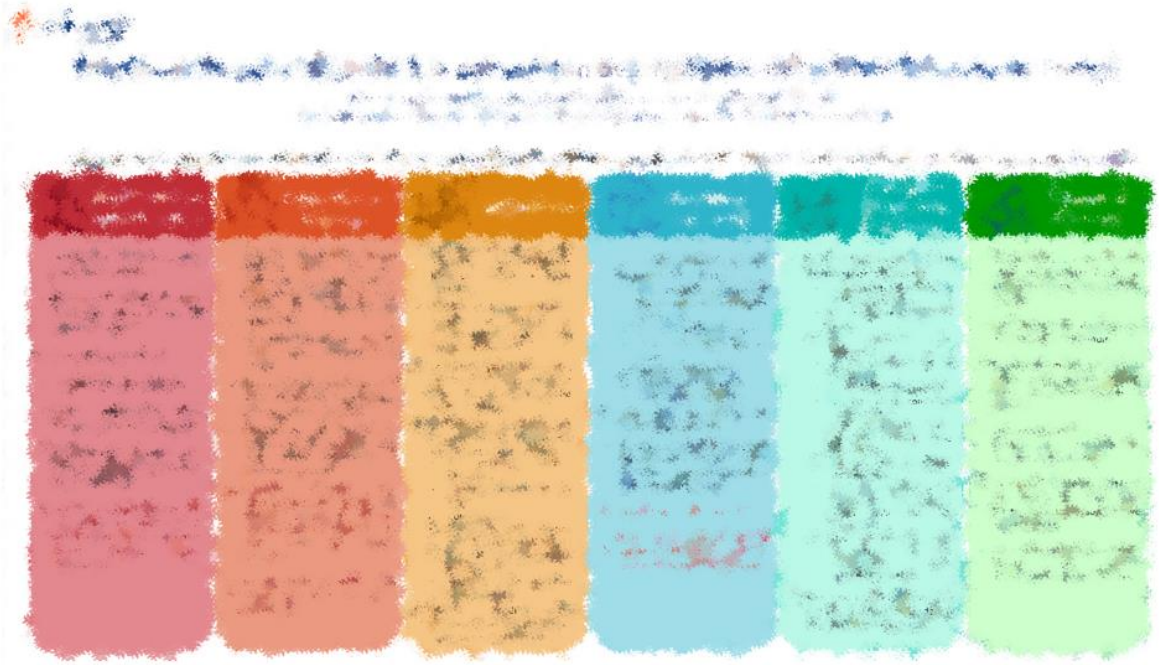

Figure 9:Recto de l'affiche finale des exigences applicables aux produits

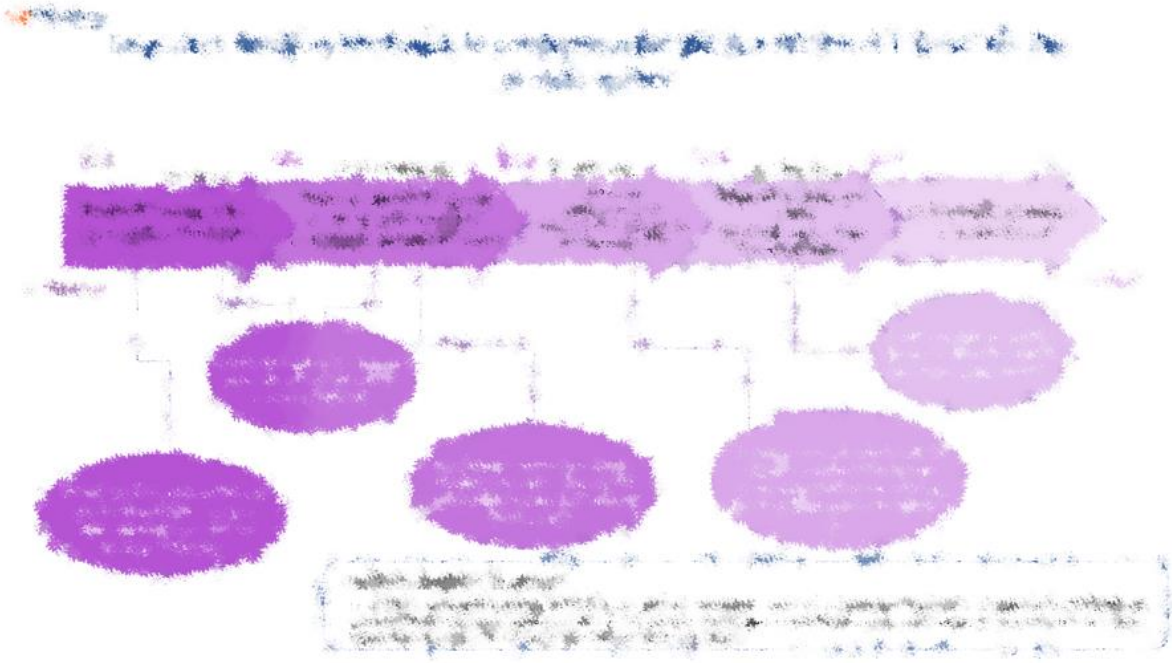

Figure 10: Verso de l'affiche finale des exigences applicables aux produits

Une fois par mois, se déroule une réunion où siègent tous les collaborateurs Edvance présents dans le bureau d'étude local travaillant dans le domaine industriel. Cet évènement est notamment l'occasion d'aborder différents sujets importants à l'organisation et est aussi un moyen de sensibiliser oralement les différents métiers. Ce support sera alors destiné à être présenter lors d'une de ces plénières afin, tout d'abord, de présenter ce qu'est un degré de sécurité avec le verso de l'affiche (Figure 10) mais aussi présenter l'existence et le fonctionnement du support afin qu'il soit utilisé en cas de besoin (Figure 9).

4.1.4 Support sur les principes fondamentaux de sécurité informatique du nucléaire

Une fois le support sur les exigences applicables aux produits finalisé, je me suis attachée à la production d'un support permettant de rendre de compte des principes fondamentaux de cybersécurité vis-à-vis de l'architecture. La problématique est ici l'intégration d'un ensemble de systèmes ayant des sensibilités distinctes.

Le référentiel et donc le support s'applique non pas uniquement au projet EPR2 mais à tout le parc nucléaire qu'il soit en exploitation ou en cours de conception au travers d'autres projets. En effet, le parc utilise des systèmes numériques de plus en plus évolués ce qui implique la nécessité d'une approche évaluant le risque de malveillance informatique. Il s'agit donc de garantir la sûreté au travers de la protection des installations ainsi que du combustible et d'assurer la disponibilité des équipements favorables à la production. Le support ici sert à rappeler graphiquement les exigences fondamentales qui seront à appliquer tout au long du cycle de vie des différentes installations.

On y retrouve de nombreux aspects de la cybersécurité tels que la prévention et la protection en profondeur d'une attaque extérieure ainsi que la possibilité de menace interne (bonhomme rouge sur la Figure 11). Le principal enjeu de ce support était d'illustrer de manière claire les différents principes. En effet, les exigences ont dû être triées par pertinence et degré d'importance, de ce fait, elles n'ont pas pu être toutes illustrées afin de ne pas surcharger le schéma.

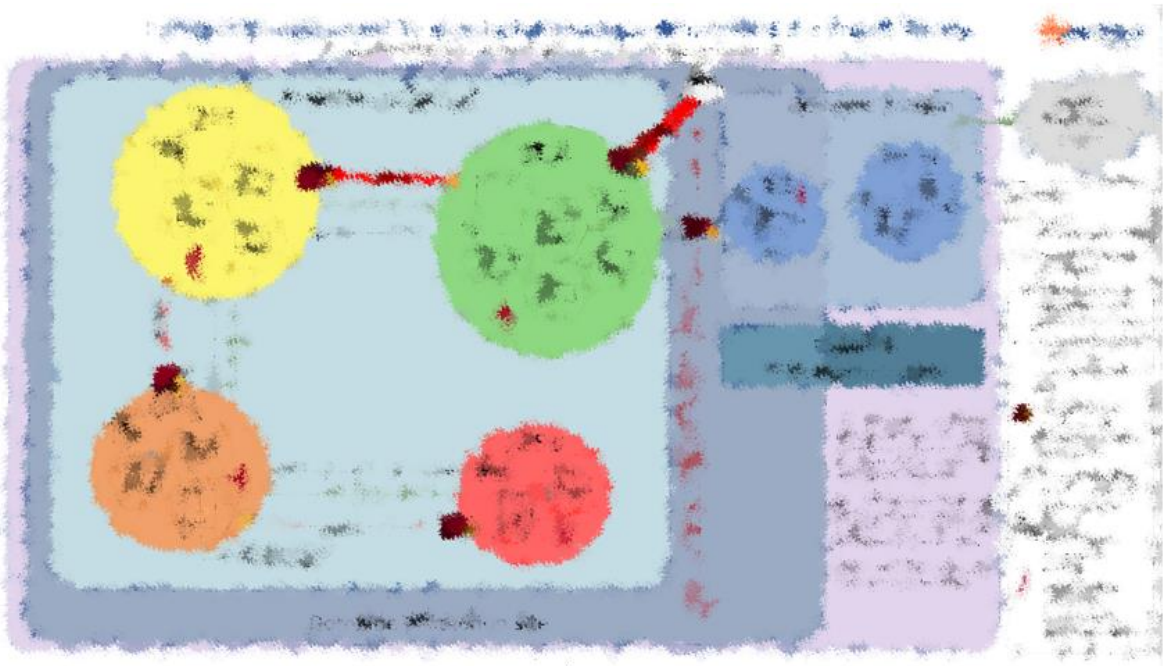

Figure 11 : Affiche sur les principes fondamentaux de sécurité informatique

Cette affiche (Figure 11) vise à être incorporée dans une des newsletters de l'entreprise transmise au personnel. Il en existe deux types : les mensuelles et les hebdomadaires. De plus, elle pourra aussi être présentée en plénières tout comme le support sur les exigences applicables aux produits.

4.1.5 Support sur la démarche cybersécurité industrielle EPR2

De plus en plus de composants numériques sont programmés dans les équipements. Il en va de même pour les systèmes qui étaient jusqu'à présent considérés comme analogiques (comme les grues, les générateurs, etc.) possédant pour la plupart une partie de numérique. Le code présent dans cette partie numérique peut être volé ou modifié malicieusement. De ce fait, il est nécessaire d'intégrer la cybersécurité dès la conception d'un système afin de prévenir ces risques.

L'objectif principal de ce support est d'être distribué au sein des différentes équipes de concepteurs systèmes afin qu'ils comprennent au mieux la démarche cybersécurité et les étapes à suivre. De ce fait, ils n'auront qu'à regarder l'affiche afin de savoir où ils en sont dans la démarche, l'étape suivante à réaliser ou alors pour vérifier qu'ils n'ont pas oublié une étape cruciale dans le développement de leur système. Pour réaliser ce support, je me suis basée sur une maquette déjà réalisée (Figure 12) mais qui était très complète en termes d'information et par conséquent très dense. Ma hiérarchie, étant globalement satisfaite de mon travail, m'a alors demandé de retravailler cette affiche afin de la rendre plus attractive.

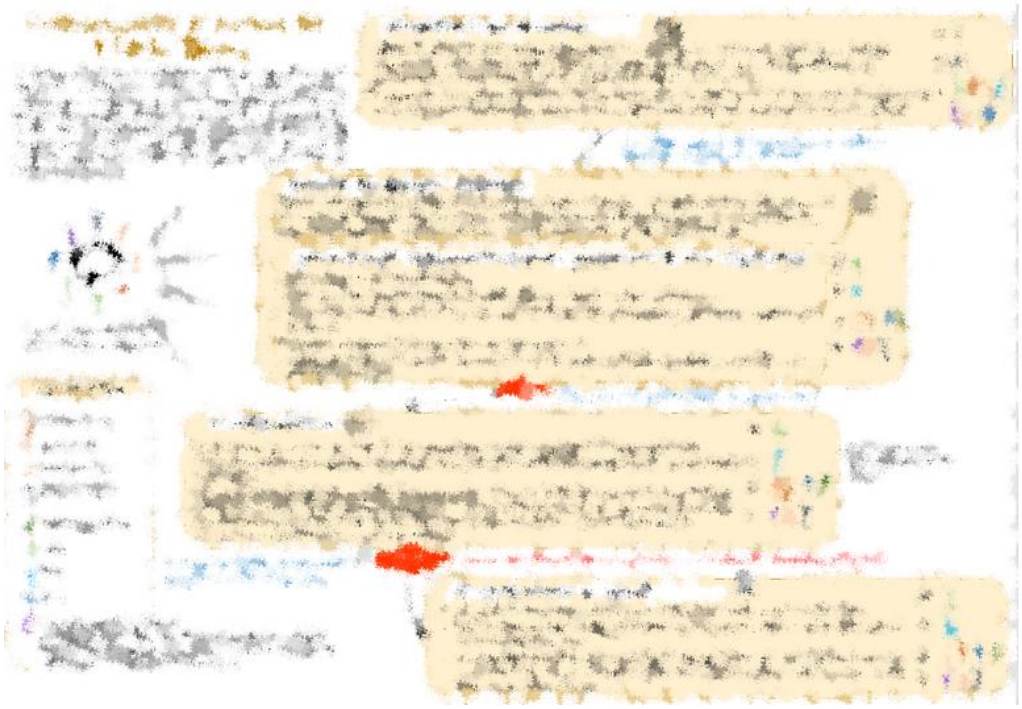

Figure 12 : Première maquette de la démarche cybersécurité industrielle EPR2

De ce fait, j'ai commencé à réfléchir à un moyen simple et ludique d'aborder un processus et l'idée du jeu de l'oie m'est tout de suite paru intéressante. Sa forme enfantine et simple permet de capter la curiosité et d'être facile à lire et à comprendre tout en gardant une quantité d'informations similaire. En effet, seules les grandes étapes sont illustrées et les informations supplémentaires nécessaires pour une étape sont inscrits sous la forme de cartes à piocher de sorte à être disponible en cas de nécessité sans altérer la compréhension du processus.

Cela a aussi permis de mettre plus en lumière un point crucial : passer par chacune des étapes. En effet, de nombreux éléments de la nouvelle affiche (Figure 13) le rappelle. Tout d'abord, on remarque qu'il y a un dé vide et un dé de 1 point permettant (malgré n'importe quel lancé de dé) de n'avancer que d'une case. Vient s'ajouter à cela le système de points où une case vaut un point couplé à la phrase « pour gagner passez par chacun des cases et récoltez 10 points ». De plus, cela permet aussi de se positionner vis-à-vis de sa propre avancée grâce à l'image du pion.

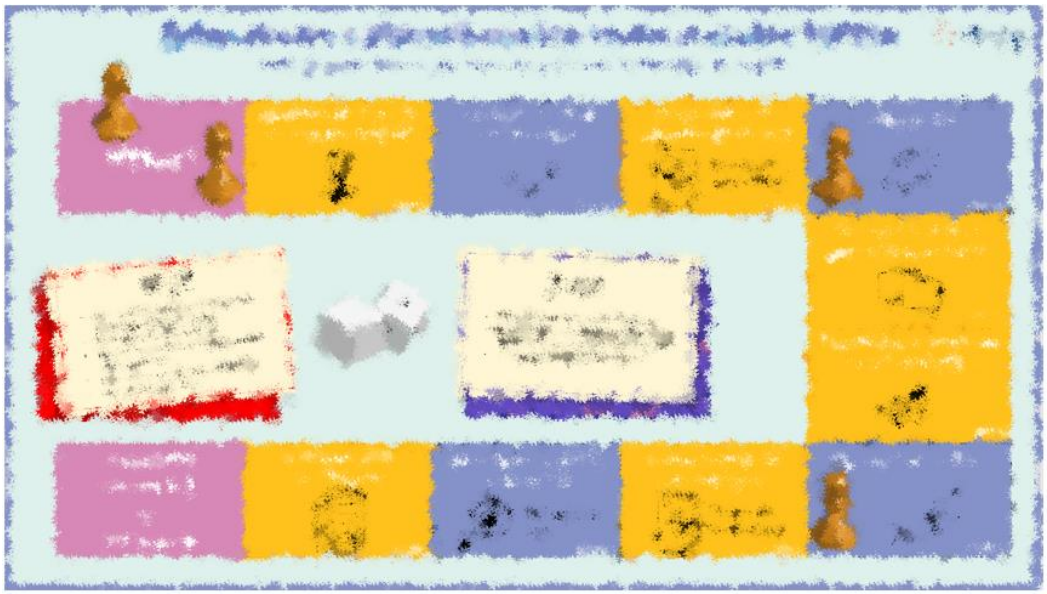

Figure 13 : Support validé sur la démarche cybersécurité industrielle EPR2

4.1.6 Support bonus

Ces deux affiches sont assez différentes des trois présentées précédemment. En effet, ces supports ne se basent pas sur un référentiel de l'entreprise mais sur un besoin de sensibiliser de manière plus large le personnel face aux risques liés à la cybersécurité. Tout s'articule autour d'un message fort « L'atterrissage d'un avion c'est comme la cybersécurité, ce n'est pas une option ! ».

Au travers de ces deux affiches, on illustre le parallèle entre un vol d'avion et un projet. En effet, au commencement, un avion a le choix entre décoller et rester sur la piste de l'aéroport, de la même sorte qu'un projet peut débuter ou rester en phase conceptuelle. Cependant, lorsqu'il vole, il n'a pas d'autre choix que d'atterrir que ce soit par un atterrissage en douceur ou par un crash d'avion. La phase de réalisation du projet s'apparente donc à un vol d'avion où la cybersécurité est une obligation qui doit être appliquée et réfléchie tout au long du vol. Cela explique aussi les deux versions de l'affiche.

Tout d'abord, si la cybersécurité est négligée pendant le déroulement du projet, alors lorsque le réacteur sera mis en service, il peut encourir de gros risques illustrés par l'image du crash d'avion. De plus, ce propos est illustré en bas de l'affiche (Figure 14) par un cas réel où une négligence informatique a pu causer un réel crash d'avion. En effet, en 2008, un cheval de Troie avait infecté un ordinateur du centre de contrôle censé détecter les alertes de sécurité. De ce fait, l'équipage n'a pas pu être alerté des problèmes de l'avion et a tout de même décollé, puis s'est crashé une centaine de mètres plus loin.

Figure 14 : Affiche de sensibilisation échec de l'atterrissage

Cependant dans la deuxième éventualité selon laquelle la cybersécurité est bien prise en compte dès la conception jusqu'à la fin de la phase de déploiement du projet (Figure 15), le vol et donc le projet se termine de manière sécurisée. D'un côté, l'avion atterrit bien, garantissant la sécurité de ses passagers. De l'autre, le projet peut se terminer avec des systèmes sécurisés garantissant un risque moins important. Pour finir, l'atterrissage ici est réussi et cela est appuyé par la phrase : « Considérer la cybersécurité, c'est un gage de confiance ».

Figure 15 : Affiche de sensibilisation réussite de l'atterrissage

Le but ici sera d'afficher les deux versions dans tous les bureaux afin de permettre une prise de conscience collective de son propre impact sur la réalisation du projet ainsi que des deux finalités possibles.

4.2 Partie II : Accompagnement des équipes

4.2.1 Qu'est-ce qu'un degré de sécurité

En première instance, la conception de la cybersécurité d'EDF repose sur le cloisonnement des 4 domaines informatiques (gestion, télécommunication, protection site et industriel) totalement indépendants. Cependant, avec les besoins croissants d'échanges d'informations entre les différents domaines, la pertinence des séparations a progressivement été nuancée. Ainsi, une approche plus graduée en DS couvrant et interfaçant les systèmes numériques (ordinateurs, automates, équipements réseau, etc.) des quatre domaines a vu le jour.

Le concept de degré de sécurité correspond au concept de « niveau de sécurité » du guide NSS 17T de l'Agence internationale de l'énergie atomique (AIEA). Il ne s'agit donc pas d'une notion spécifique au nucléaire français.

Il existe cinq DS (DS1 étant le plus sensible et DS5 le moins sensible). Dans le domaine industriel, chaque DS correspond, dans les grandes lignes, aux définitions suivantes :

- DS1 : attribué aux systèmes les plus critiques pour la sûreté,
- DS2 : attribué aux systèmes participant à la conduite du procédé principal (depuis la production de chaleur jusqu'à l'évacuation de l'énergie électrique),
- DS3 : attribué aux systèmes ayant un impact à court terme (moins d'une semaine),
- DS4 : attribué aux systèmes ayant un impact à moyen terme (d'une semaine à un mois),
- DS5 : attribué aux systèmes ayant un impact à long terme (plus d'un mois) ou sans impact.

4.2.2 Pont auxiliaire

Après avoir servi dans le réacteur de la centrale, l'AC usagé est encore radioactif et dégage toujours de la chaleur. Lorsqu'il est retiré du réacteur, il est déplacé du bâtiment réacteur au bâtiment combustible à l'intérieur d'une piscine d'entreposage (Figure 16) où l'eau formera une barrière radiologique et où il sera constamment refroidi. Cependant, il ne restera pas indéfiniment dans cette piscine. En effet, lorsque leur puissance résiduelle diminue suffisamment, l'AC usé sera envoyé pour retraitement et stockage final. De plus, cette piscine peut aussi contenir le combustible neuf en attente de mise en place dans le réacteur.

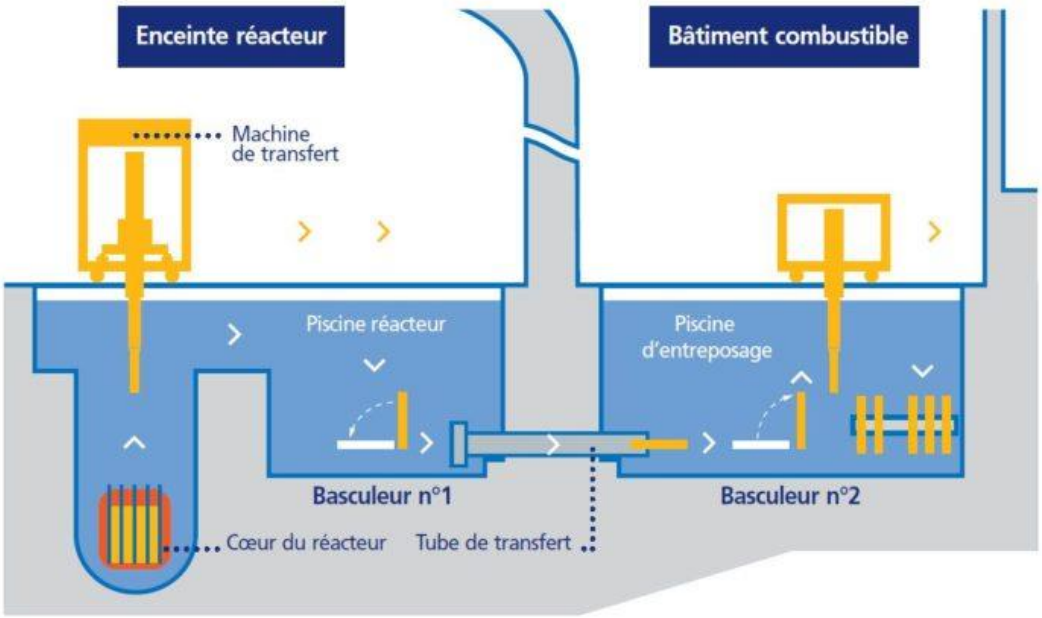

Figure 16 : Illustration de la manutention du combustible usagé (source : journal de l'Energie)

Le pont auxiliaire (PMC) est une machine de chargement qui sert à la manutention du combustible. Il est situé au-dessus du hall piscine dans le bâtiment combustible où se trouve la piscine de stockage. Le pont auxiliaire prend le relais en cas de défaillance du pont perche (illustré à la Figure 17 et pont présent au sein du bâtiment combustible dans la Figure 16). S'il est utilisé, il permet d'introduire et d'installer les équipements du local piscine lors de la phase de chantier ainsi que de les désinstaller et de les évacuer lors de la phase de démantèlement. Lors de l'exploitation de la centrale, ce pont roulant permet de faire la manutention des AC neuf dans le hall piscine afin de pouvoir être transmis dans la piscine réacteur et recharger la cuve. Il permet aussi de réaliser la manutention des combustibles usés évacué de la piscine réacteur ainsi que la manutention des déchets présents dans la piscine de désactivation (Figure 17) provisoire où se trouvent les AC irradiés ou destinés au rechargement d'un réacteur à l'arrêt. Pour finir, il permet aussi l'évacuation des AC usés.

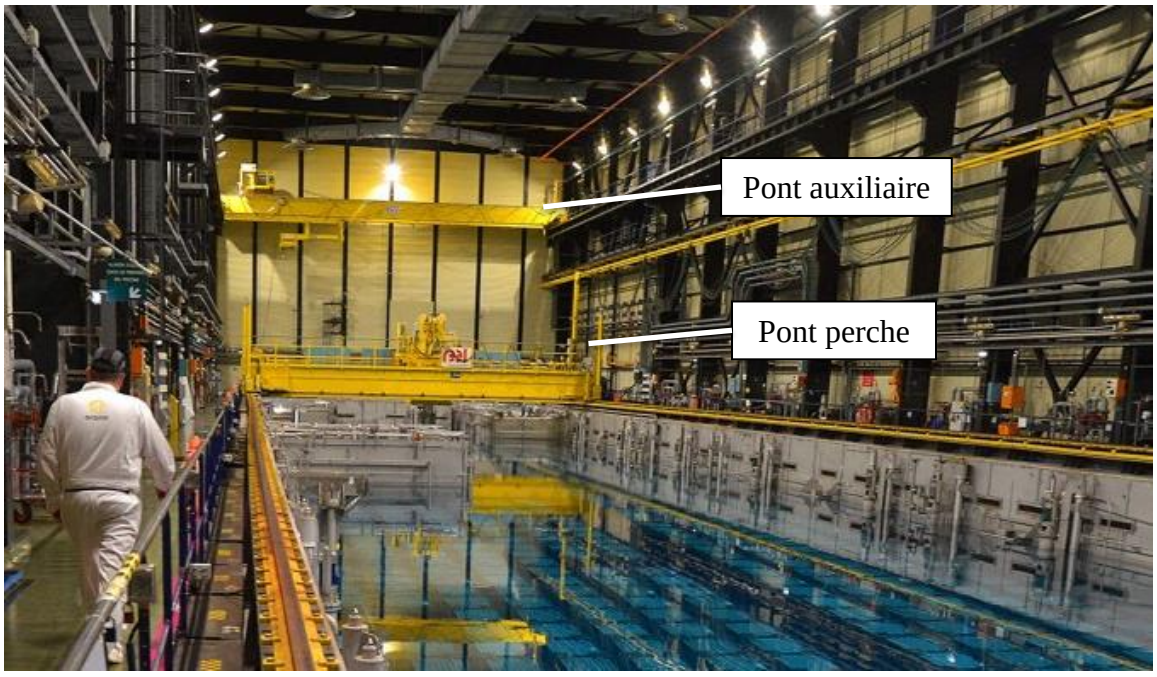

Figure 17 : Différents ponts présents dans la piscine d'entreposage (source : ouest-France)

4.2.3 Pont lourd

Le pont lourd (DMK) est, comme le PMC, un pont roulant servant à la manutention présent dans le bâtiment combustible (Figure 18). Cet appareil permet d'introduire les équipements nécessaires dans le bâtiment combustible et le bâtiment réacteur sur le plancher de service lorsque la centrale est en chantier puis de déconstruire et évacuer ces équipements lors du démantèlement de la centrale. En phase d'exploitation, le DMK permet la manutention de la machine de serrage et de desserrage des goujons du couvercle de la cuve réacteur. De plus, le pont permet aussi l'introduction des outils d'inspection combustibles jusqu'au plancher de service ainsi que l'introduction des charges et équipements nécessaires à l'exploitation du bâtiment combustible et celui du réacteur.

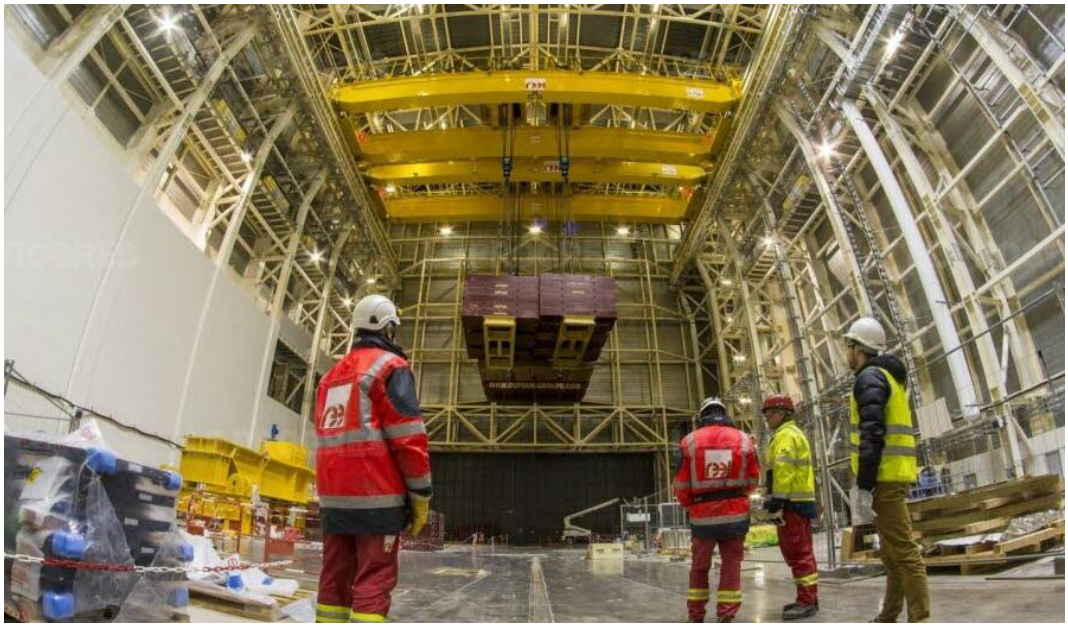
Figure 18: Pont lourd dans le bâtiment combustible (source : Le Progrès)

4.2.4 Fiche d'analyse d'impact

Le classement en DS est la première étape de la démarche cybersécurité industrielle (Figure 12) car il va permettre de définir des exigences propres aux systèmes à inscrire dans les spécifications techniques. Pour définir le DS d'un système, il faut remplir une fiche nommée Fiche support d'analyse d'Impact pour Classement en Degré de sécurité. Dans cette fiche, les ingénieurs systèmes qui conçoivent et définissent les équipements étudiés et les ingénieurs cybersécurité se rencontrent afin de déterminer ensemble le DS du système associé.

Tout d'abord, on commence par faire une description du système où l'on détaille toutes ses fonctions et ses sous fonctions numériques, son schéma d'architecture, son domaine associé et les réglementations applicables (lois, normes ou documentations de l'entreprise) ainsi que toutes ses interfaces avec d'autres systèmes ou réseaux. Par la suite, on analyse les conséquences possibles de la perte de disponibilité (interruption totale ou partielle de la fonction), de l'intégrité (modification ou perte d'une information nécessaire ou générée par la fonction) et de confidentialité (divulgation d'une information en rapport avec la fonction à des personnes non autorisées). Chaque critère est ensuite étudié vis-à-vis des enjeux en termes de sûreté (risque radiologique), de performance (perte de production, exploitation des systèmes) et de sécurité (atteinte à la sécurité physique du site). Chacun de critères est alors placé selon une échelle de niveau de conséquence en fonction de chacun des enjeux. La place la plus haute de ces critères dans l'échelle définit le DS du système.

Il est ensuite validé par le comité opérationnel de sécurité informatique du nucléaire et par le comité de sécurité informatique du nucléaire en présence des représentants de chacun des quatre grands domaines, des acteurs de références du nouveau nucléaire et de l'exploitant.

4.2.5 Réalisation de la fiche d'analyse d'impact de chacun des systèmes

Une fiche d'analyse d'impact suit un cycle très précis. Tout d'abord, une première version préliminaire est élaborée et rédigée par un ingénieur système, puis, elle est vérifiée et retravaillée en collaborations entre les différents ingénieurs systèmes et ingénieurs cybersécurité. Quand un accord est trouvé, le circuit de signature est lancé.

En ce qui concerne la fiche d'analyse d'impact des systèmes DMK et PMC, une première version avait déjà été réalisée. Cette version regroupait les analyses pour deux systèmes distincts ce qui en complexifiait la prise en main et la vérification. Mon travail était alors d'analyser les informations ainsi que vérifier que toutes les fonctions de chacun des ponts aient bien été analysées afin de déterminer au mieux le DS. Pour cela, l'ingénieur système nous a communiqué le schéma d'architecture d'un projet précédent (HPC) du pont auxiliaire. Cela s'explique par le fait que le schéma d'architecture du système n'avait pas encore été réalisé dans le cadre du projet EPR2 et le fait que le système ne comporte que des changements mineurs vis-à-vis du projet précédent.

Ce schéma comprenant près de 70 éléments me permettait d'identifier par moi-même les éléments numériques et leurs interfaces. J'ai donc commencé par classer tous les éléments dans un tableau Excel selon 5 catégories :

- La zone dans laquelle se trouve l'élément (zone géographique sur le pont),
- L'élément,
- La classe de l'élément (classement de sûreté),
- Si c'est numérique ou non
- La ou les interfaces avec d'autres éléments en identifiant les interfaces numériques qui peuvent être le moyen de propager une attaque

- Le classement de sûreté du ou des éléments interfacés avec les fonctions numériques étudiées

Mais je me heurte à trois principaux problèmes. Tout d'abord, ce schéma d'architecture ne représente que le pont auxiliaire et n'aborde pas le pont lourd (alors que celui-ci est également présent dans la fiche que je dois vérifier). Ensuite, la description des éléments sur le schéma est trop imprécise par rapport à mon besoin qui est d'identifier si l'élément est numérique ou non. En effet, il est juste écrit des éléments tel que des capteurs, des télécommandes, des encodeurs, un système de levage, etc. mais leur usage et la technologie derrière l'appareil ne sont pas expliqués. Prenons l'exemple d'un capteur, il peut être numérique comme analogique. De ce fait, je me suis renseignée grâce à divers outils de l'entreprise. C'est notamment grâce à l'un d'entre eux que j'ai pu me plonger dans la documentation d'où provenait le schéma d'architecture du PMC fournit précédemment. Cette documentation contenait en plus du schéma le descriptif précis de chacun des éléments ainsi que leur utilité. Cela m'a alors permis de reclasser les éléments et de mieux assimiler le fonctionnement du système.

Pour donner suite à cela, l'ingénieur en charge des deux systèmes m'a communiqué plusieurs informations m'aidant à pousser mon analyse. Tout d'abord, uniquement les fonctions classées 3 pouvaient contenir du numérique, réduisant donc grandement le périmètre de l'analyse. De plus, il m'a communiqué la liste des mesures du sûreté définies par les analyses de risque menée sur chacun des ponts. Ces mesures de sûreté servent à définir tous les éléments qui devront être étudiés puis ajoutés à l'architecture afin de garantir la sûreté physique du matériel. Parmi les mesures de sûreté on peut retrouver : la détection de la surcharge, la détection d'un mouvement opposé à celui demandé menant à l'arrêt du mouvement, l'interdiction de l'abaissement de la charge dans une zone non prévue à cet effet, la détection d'une survitesse du treuil, etc.

Afin de déterminer au mieux le DS de chacun des systèmes, il fallait alors réaliser une analyse d'impact (niveau de conséquence selon la perte d'intégrité, de confidentialité et de disponibilité) sur chacune de leurs mesures de sûreté. Cela permet tout d'abord d'établir le DS le plus sensible que peut atteindre le système, mais cela permet aussi de trouver les mesures sur lesquelles il faut éviter de mettre du numérique. À la suite de cet exercice, un classement préliminaire de degré de sécurité est établi. Mais avant de reprendre contact avec l'ingénieur système, il est essentiel d'estimer une liste couvrant le niveau de conséquences maximum possibles à prévoir pour chacun des systèmes. Pour cela je reprends chacune des mesures de sûreté ainsi que les éléments que j'ai identifiés comme étant du numérique et je réfléchis aux conséquences dans l'éventualité d'une perte des trois critères. Pour reprendre les exemples précédents :

- **Détection de la surcharge** : cela peut endommager voire casser le pont ainsi que mener à un heurt du combustible ou de l'équipement ;
- **Détection d'un mouvement opposé et interdiction de l'abaissement dans une zone non prévue à cet effet** : Déposer l'AC (PMC) ou l'équipement (DMK) dans une zone non prévue, mise en danger du personnel ;
- **Détection d'une survitesse du treuil** : Peut mener à un heurt du combustible sur une des parois du bâtiment.

Mais j'ai aussi réfléchi vis-à-vis du matériel :

- **Encodeur :** Mauvaise transmission de la vitesse ou de la position pouvant mener à un heurt du combustible ou de l'équipement ;
- **Variateur de vitesse** : Truquer la vitesse ou l'accélération du pont pouvant mener à un heurt du combustible ou de l'équipement.

Parmi toutes les conséquences trouvées, la plus redondante et la plus redoutée a permis de relever une question importante : 'Qu'advient-il en cas de heurt du combustible dans le hall piscine ?'. Un nouvel échange a alors été programmé avec l'équipe de concepteurs systèmes afin de finaliser la fiche avec les différentes remarques que j'ai pu trouver durant mon analyse.

Cet échange a permis de répondre aux différentes zones d'ombre que j'avais relevées, notamment le risque de heurt du combustible. Tout d'abord, il a été mis en lumière la redondance des éléments de type capteurs ou encodeurs couplés à une technologie vérifiant que les informations soient cohérentes et arrêtant le pont en cas de données contradictoires. De plus, l'opérateur possède un visuel constant sur le pont correspondant et a la capacité d'actionner un bouton d'arrêt d'urgence fonctionnant de manière analogique. Pour finir, le PMC se trouvant au-dessus de la piscine d'entreposage, en cas de heurt ou de chute du combustible, cela se déroulerait dans la piscine réduisant donc grandement la radioactivité qui n'est pas élevée dans le cas de combustible neuf. De plus, comme expliqué précédemment, l'eau constitue une barrière de protection radiologique.

Au terme de cette discussion, toutes mes remarques ont pu être abordées et traitées, ce qui nous a permis de confirmer ensemble avec quasi-certitude le résultat que j'avais obtenu. La dernière modification était alors de séparer la fiche en deux distinctes par système et inscrire sur chacune d'entre elles les précisions échangées en réunion.

Pour clôturer cette analyse d'impact, la fiche a été envoyée pour validation de sorte que les ingénieurs systèmes puissent intégrer les exigences en termes de cybersécurité applicables aux produits correspondant à leur DS au sein de leur appel d'offres.

5 Conclusion

Pour conclure, durant mon stage chez Edvance, j'ai eu l'occasion d'acquérir de nouvelles connaissances du domaine cybersécurité en continuité avec les connaissances théoriques acquises durant mes 2 années de bachelor universitaire de technologie (BUT). En effet, lors de mon stage, j'ai pu réaliser diverses missions telles que la sensibilisation des collaborateurs aux risques liés à la cybersécurité et à l'importance de la considérer dès le début de la conception ; ainsi que la réalisation d'analyses d'impact pour plusieurs systèmes.

A la fin de mon stage, mes différentes productions ont été présentées aux correspondants cybersécurité des différents métiers, enthousiastes à l'idée de la publication des supports (qui se fera après mon départ) au sein des équipes.

Cette expérience fut très enrichissante et instructive, ce qui m'a permis de découvrir le fonctionnement du travail au sein d'un bureau d'étude et m'a permis de découvrir une nouvelle facette du métier d'ingénieur cybersécurité que je souhaiterais réaliser à la suite de mes études. Ce stage m'a ainsi conforté dans mon envie de poursuite d'étude et dans mon projet professionnel.

6 Remerciements

Tout d’abord, je souhaiterais remercier mon tuteur de stage M. Guillaume GOURLAOUEN, pour sa bienveillance, son accompagnement et les connaissances qu’il a su partager avec moi. Il m’a beaucoup appris sur le domaine du nucléaire et les défis quotidiens qu’un ingénieur en cybersécurité doit relever. Enfin, je tiens à lui témoigner toute ma gratitude pour sa précieuse aide à la relecture et à la correction de mon rapport de stage.

Je profite également de cette occasion pour adresser un grand merci au corps enseignant du BUT réseau et Télécommunication qui m’ont fourni les outils nécessaires au bon déroulement de ce stage au travers de leurs enseignements. Je tiens tout particulièrement à remercier Mme. Corinne HOUSSAIN, professeure d’anglais technique ainsi que ma responsable académique, pour son soutien dans ma démarche de recherche de stage ainsi que pour son investissement durant ces 10 semaines en entreprise.

Je voudrais enfin exprimer ma reconnaissance envers les amis et collègues qui m’ont apporté leurs conseils, ainsi que leur soutien moral et intellectuel tout au long de mon stage.

7 Glossaire

EDF, Energie De France

CIC, conception et intégration contrôle commande

MWe, megawatt électrique

EPR, Excellence Pressurized Reactor

EPR2, Evolutionary Power Reactor

HPC, Hinkley Point C

AC, Assemblage combustible

Acteurs de référence, dans ce document cela représente les différentes équipes traitant de la cybersécurité (RSSII, ingénieurs cybersécurité, etc.)

RSSII, Responsable de la sécurité des systèmes informatiques du domaine industriel

DS, degré de sécurité

PMC, Pont auxiliaire

DMK, pont lourd

Classement de sûreté, Le classement de sûreté des équipements permet de leur affecter des exigences adaptées en termes de conception, de fabrication, de qualification, d'exploitation et de suivi en service, proportionnées à leur importance pour la sûreté. Les catégories que j'ai rencontrées sont : classe 1, classe 2, classe 3 et Non Classé. Le classement de sûreté des équipements est expliqué en détail dans un document disponible en ligne sur le site de l'IRSN Eléments de sûreté nucléaire - Les réacteurs à eau sous pression (irsn.fr).

BUT, Bachelor Universitaire de Technologie

8 Bibliographie

Lesénéchal, G. (29 janvier, 2015). *Le fonctionnement d'un réacteur nucléaire électrogène (CEA)* Disponible sur : https://www.cea.fr/comprendre/Pages/energies/nucleaire/essentiel-sur-fonctionnement-reacteur-nucleaire-electrogene.aspx

Huron, J-M. (08 février 2017). *Fonctionnement d'un réacteur nucléaire (IRSN).* Disponible sur : https://www.irsn.fr/savoir-comprendre/surete/fonctionnement-dun-reacteur-nucleaire

Croquelois, E. (03 mai 2023). *Réacteur EPR et EPR2 : quelles sont les différences ? (SFEN).* Disponible sur : https://www.sfen.org/vos-questions/lepr-et-lepr-2-quels-changements/

Houard, V. (29 mars 2024). *Newsletter n°9 EPR, EPR2 : quelles différences ? (Linkedin).* Disponible sur : https://fr.linkedin.com/pulse/newsletter-n9-epr-epr2-quelles-diff%C3%A9rences-la-cci-business-houard-nn5ze

9 Table des illustrations