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

STAGE CYBERSECURITE

Nicolas ROBERT

Arkema

Responsable entreprise : Philippe JEANSON

Responsable académique : Anouch HOVSEPIAN

2023

Table des matières

1 Introduction

Mon parcours d'étudiant en *BUT* Réseaux et Télécommunications* comporte un stage en entreprise que j'ai eu l'opportunité de réaliser au sein d'*Arkema*, à Saint-Auban (04), sur le poste d'ingénieur en informatique industrielle spécialisé dans la cybersécurité. J'ai intégré le service Informatique Industrielle et Automatisation (IIA*) du site, composé de cinq professionnels dédiés à la maintenance, au dépannage et à la sécurisation des systèmes industriels de l'usine.

Ma principale responsabilité était de mettre en place la directive sur la cybersécurité du site, en étroite collaboration avec le RSSC-L*. À cet effet, j'ai été chargé de diverses missions, parmi lesquelles :

- Effectuer l'audit annuel de cybersécurité pour évaluer et pour améliorer la posture globale de l'entreprise.
- Réaliser des audits des armoires de l'entreprise afin de détecter d'éventuelles vulnérabilités et de proposer des mesures correctives.
- Vérifier la conformité des pratiques en place avec les directives d'Arkema, en veillant à atteindre les niveaux de sécurité requis.
- Assurer la mise à jour régulière des modes opératoires, en évaluant leur pertinence et en encourageant leur adoption systématique.
- Déboguer et optimiser les applications PowerApps pour assurer leur bon fonctionnement.

Tout au long de cette expérience, j'ai pu mener à bien la plupart de ces missions. J'ai également été amené à accomplir diverses tâches supplémentaires, comme la réalisation de projets d'infrastructure, le dépannage de systèmes et l'accomplissement de tâches administratives liées à la cybersécurité des systèmes industriels. Les détails des missions les plus importantes seront précisés dans la suite de ce document.

2 Présentation de l’entreprise

2.1 L’entreprise *Arkema*

Arkema est un groupe chimique français créé le 1er octobre 2004, suite à la restructuration de la branche chimique de *Total*. Grâce à sa stratégie axée sur l'innovation, *Arkema* est rapidement devenu un leader mondial dans le domaine de la chimie de spécialité. L'entreprise s'est distinguée par des acquisitions ciblées, notamment celles de *Coatex* en 2007, une société spécialisée dans les additifs rhéologiques*, et de *Dow Chemical Company* en 2010, orientée vers la pratique des activités monomères*.

Aujourd'hui, *Arkema* est structurée en quatre principaux segments d'activité. Le premier, représentant 24% des ventes, est dédié aux solutions adhésives dans le secteur industriel et la construction. Pour 32,5% des ventes, le deuxième s’applique aux matériaux avancés utilisés dans diverses industries. Le troisième segment, représentant 29% des ventes, s’oriente vers les solutions de revêtements, telles que les modificateurs de rhéologie. Enfin, le dernier segment, à hauteur de 14,5% des ventes, s’intéresse aux solutions chimiques fluorées intermédiaires, comme les gaz de climatisation.

Les produits d'*Arkema* sont présents dans notre quotidien. Ils apparaissent dans de nombreuses fabrications. Par exemple, l'entreprise produit du PVC pour l'isolation thermique en collaboration avec sa filiale *Kem One*. Elle fournit également des fibres de filtration pour la fabrication d'eau potable, des traitements contre l'acné, de l'eau de Javel, ainsi que des plastiques plus durables, légers et recyclables pour l'industrie automobile.

Arkema emploie plus de 20 500 salariés dans le monde, répartis dans 55 pays, près de 7 300 en France, représentant 36% de l'effectif total du groupe. Environ 45% de la production d'*Arkema* est réalisée sur le territoire national. L'entreprise dispose de 24 sites de production et de 7 centres de recherche et développement (R&D), souvent associés à ses sites.
Arkema a réalisé un chiffre d'affaires de 11,5 milliards d'euros en 2022.

Le groupe *Arkema*, est un acteur mondial reconnu dans le domaine de la chimie de spécialité et des matériaux avancés. Il se divise en trois pôles majeurs. Le premier s’intéresse aux produits de performance, comprenant les adhésifs de spécialité (sous la marque *Bostik*), les polymères techniques et les additifs de performance. Le deuxième pôle développe la chimie industrielle, avec des activités dans la thiochimie (chimie du soufre), le peroxyde d'hydrogène et le plexiglas. Enfin, le troisième pôle concerne les produits vinyliques, tels que les acryliques, les résines de revêtement et les additifs.

2.2 L’entreprise de Saint Auban

Figure 1 : Site Arkema Saint-Auban

2.2.1 Histoire du site de Saint-Auban

Construite pendant la première guerre mondiale, en 1916, l'usine de Saint-Auban est l'un des plus anciens sites d'*Arkema*. Mais, presque centenaire, il existait avant la création de l'entreprise. À l'origine, il était destiné à répondre aux besoins de production du chlore utilisé à des fins de défense nationale, notamment le dichlore ou chlore en état gazeux. Cette localisation stratégique dans un endroit isolé recherchait également une protection contre les avions allemands de l'époque.

Au fil des années, le site industriel de Saint-Auban a diversifié sa production. Dans les années 1920 à 1950, il est devenu *La Compagnie des produits chimiques d'Alais et de la Camargue*, élargissant ses activités pour inclure la production d'ammoniac, d'aluminium, de trichloroéthane* (T111) et de chlorure de vinyle. L’infrastructure a connu différents changements de propriétaire, passant successivement sous la direction de *Péchiney, Saint-Gobain, Rhône-Poulenc*, *Atochem* et *Atofina*, avant d'être acquis par *Arkema*.

2.2.2 Activité principale du site de Saint Auban

Aujourd'hui, l'activité principale de l'usine de Saint-Auban est la production du T111, un produit chimique utilisé par le site de Pierre-Bénite.

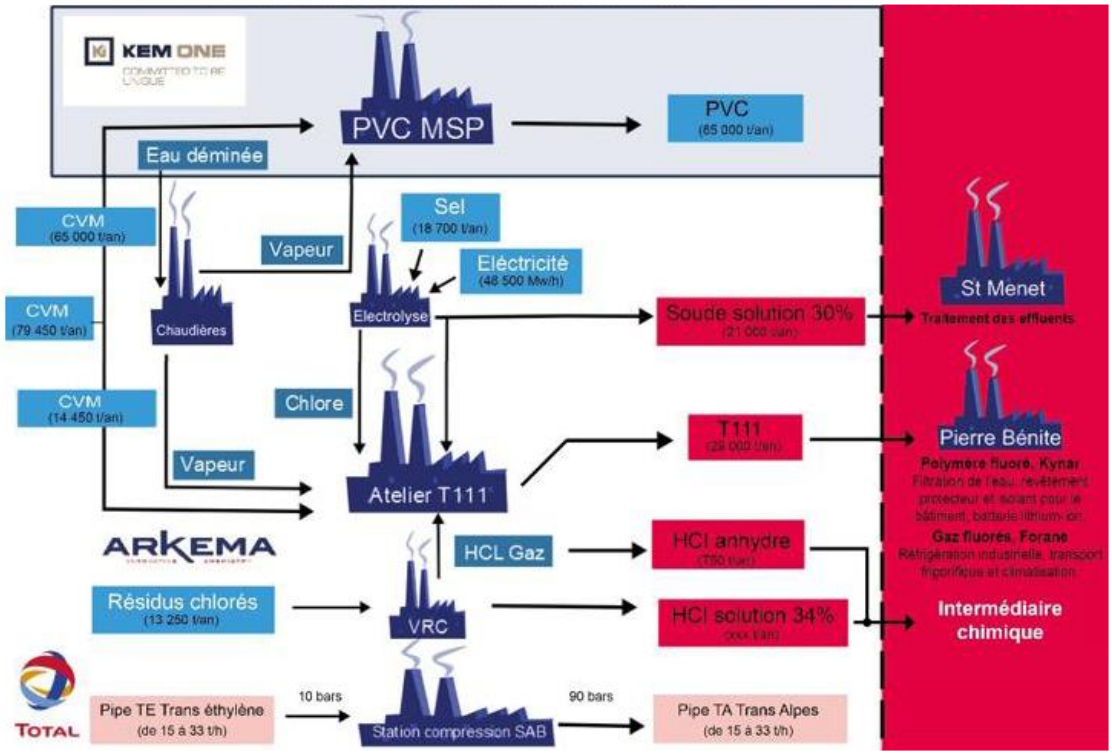

Figure 2 : Schéma de fabrication Saint-Auban

La production annuelle de T111 atteint le volume de 29 000 tonnes. En plus de cette activité, l'usine de Saint-Auban partage sa plateforme avec les entreprises *Kem One*, spécialisée dans la fabrication de *PVC*, et *Total*, qui canalise de l'éthylène depuis l'usine vers d'autres régions.

Le site de Saint-Auban compte 216 employés permanents, auxquels s'ajoutent 120 personnes travaillant pour des sociétés extérieures. Il est classé *Seveso 2 - Seuil Haut*, en raison de la nature des activités industrielles qui s'y déroulent. *Arkema*, soucieuse des enjeux environnementaux, a mis en place des structures pour le traitement des effluents de l'usine, ainsi qu'une ferme solaire qui génère jusqu'à 30% de la consommation électrique du site.

En résumé, le site de Saint-Auban est ancré dans l'histoire par sa construction pendant la première guerre mondiale. Au fil des décennies, il a évolué pour devenir un site majeur de production de T111, tout en étant partagé avec d'autres entreprises pour des activités complémentaires.

2.2.3 Service

Pendant mon stage, j'ai été affecté au *Service Technique Moyens Centraux* (ST MC*) où j'ai travaillé dans la cellule *Informatique Industrielle et Automatisme* (IIA). Cette cellule est dirigée par M. Philippe JEANSON. Elle forme, rappelons-le, une équipe de cinq personnes dont l'activité touche à la maintenance des systèmes de conduite centralisés et d'automatismes liés aux procédés de fabrication des différents ateliers de production présents sur les sites d'*Arkema*, *Kem One* et *Total*.
Le service IIA traite :

- l'intervention, le suivi et le dépannage des systèmes de conduite centralisés et d'automatisme
- l'évolution du parc matériel IIA et la gestion du magasin
- l'étude de systèmes de conduite centralisée
- l'étude et la réalisation des travaux neufs
- la formation des utilisateurs aux systèmes de conduite centralisés et d'automatismes
- la veille technologique pour rester à la pointe des avancées dans le domaine
- la réalisation d'analyses fonctionnelles détaillées
- la sécurité des systèmes en mettant en place des mesures de cybersécurité

Ces responsabilités englobent un large éventail de tâches et de compétences, permettant ainsi de garantir le bon fonctionnement des systèmes de conduite centralisés et d'automatismes essentiels aux procédés de fabrication des ateliers de production des entreprises partenaires.

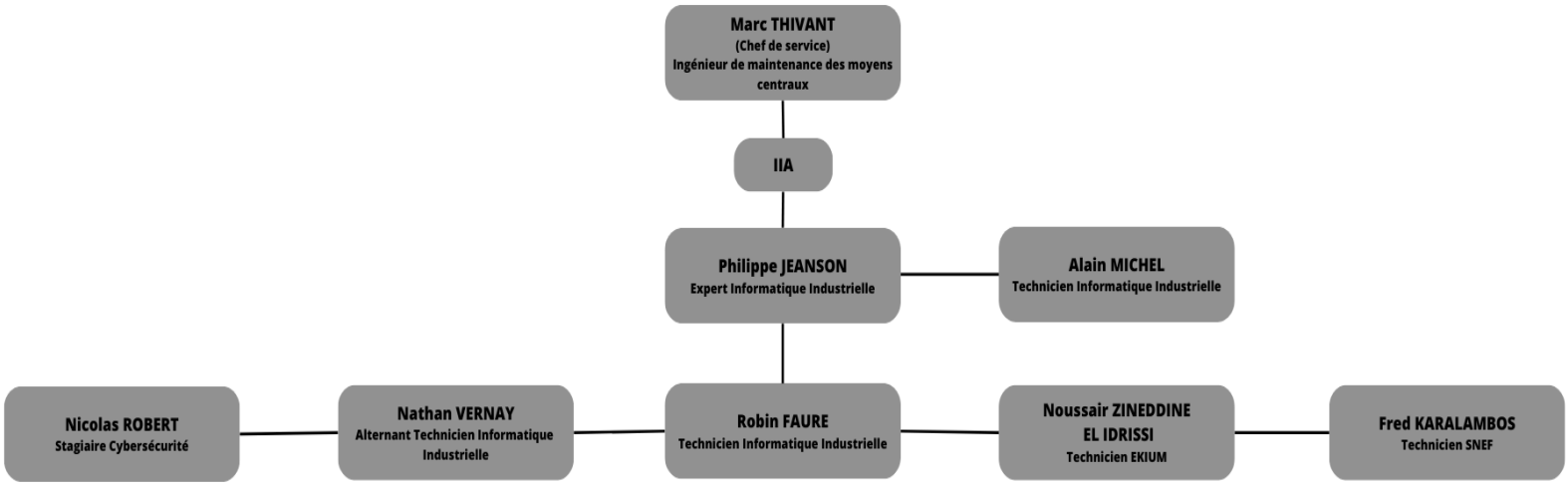

Figure 3 : Organigramme de la cellule IIA

3 Application Annuaire

3.1 Outils utilisés

Mon stage m'a permis de me familiariser avec des outils puissants tels que *SharePoin*t et *PowerApps*. Voici un aperçu de leur champ d'application :

SharePoint est une plateforme de collaboration et de gestion des contenus d'entreprise développée par *Microsoft*. Dans cet espace centralisé, les membres d'une organisation peuvent stocker, organiser et partager des documents, des informations et des ressources. *SharePoint* permet également la création de sites web internes afin de faciliter la collaboration et la gestion de projets. Durant mon stage, j'ai utilisé *SharePoint* comme base de données pour améliorer une application *PowerApps*. Des listes *SharePoint* m'ont permis de stocker les données nécessaires à l'application.

PowerApps est une plateforme de développement d'applications proposée par *Microsoft*. Elle permet aux utilisateurs de concevoir et de créer des applications professionnelles personnalisées. *PowerApps* offre une interface conviviale et intuitive associée à une compatibilité avec les appareils mobiles. On peut ainsi créer des applications utilisables sur des smartphones, des tablettes et des ordinateurs. Au cours de mon stage, j'ai utilisé PowerApps pour améliorer une application existante. J'ai pu fabriquer une interface utilisateur attrayante et fonctionnelle à partir de différents contrôles tels que des formulaires, des boutons et des galeries.

L'un des principaux avantages de *PowerApps* réside dans sa capacité à se connecter à différentes sources de données, y compris *SharePoint*. J'ai intégré *SharePoint* en tant que source de données dans *PowerApps*, ce qui m'a permis d'utiliser la liste *SharePoint* comme base de données pour notre application. Ainsi, j'ai pu afficher, saisir et modifier les données de la liste *SharePoint* directement depuis l'application *PowerApps*. L'expérience de l'utilisateur est facilitée par la possibilité d'interagir en toute transparence avec les données stockées dans *SharePoint*.

3.2 But de l'application

L'application annuaire *PowerApps* répertorie les informations sur le personnel de l'entreprise *Arkema*, ainsi que sur celui des entreprises extérieures. Ces informations incluent le nom de la société, le nom du service, le numéro interne, le numéro externe, le bâtiment, le numéro de bureau, la fonction, l'adresse

électronique et le numéro *TAMAT* (liste d'appel du robot d'alerte). Plusieurs types de recherche sont disponibles, par nom, par numéro ou par mot-clé en utilisant la barre de recherche. De plus, il est possible d'accéder à un annuaire par nom, qui organise les noms par ordre alphabétique, à un annuaire externe qui classe les sociétés extérieures par ordre alphabétique, ou encore à un annuaire par société et service proposé.

3.3 Les problèmes de l'application

Sur cette application, plusieurs améliorations m'ont été demandées. Tout d'abord, il était nécessaire d'ajouter un bouton "Ajouter" (+) pour permettre l'adjonction directe de personnes ou de sociétés externes depuis l'application, sans passer par la liste *SharePoint*. Cette fonctionnalité facilite le processus en rendant l'ajout plus intuitif et plus pratique pour les utilisateurs.

Une autre difficulté apparaissait lorsqu'un utilisateur modifiait un numéro interne ou externe : la modification ne prenait pas effet immédiatement. Pour corriger cela, un bouton "Réinitialiser" était requis, afin de supprimer complètement le numéro de la base de données avant de le réécrire. Cependant, dans le but d'améliorer l'expérience utilisateur, mon objectif était de supprimer ces boutons "Réinitialiser" et de permettre que les modifications s'appliquent automatiquement dès que l'utilisateur modifie le numéro.

La suppression du zéro au début de chaque numéro ajouté à la base de données était aussi un désagrément. Une solution a été trouvée par l'adjonction d'un zéro statique dans l'application *PowerApps*. La conservation du zéro initial du numéro est dès lors assurée. Cela permet d'éviter toute confusion ou perte de données lors de l'ajout de numéros.

Enfin, il était nécessaire d'améliorer la réactivité de l'application. Une meilleure adaptation à l'écran était attendue, en particulier lors de son utilisation sur une tablette. Des problèmes de superposition de texte et de mauvais alignement devaient être résolus afin d'offrir une expérience visuelle fluide et agréable pour les utilisateurs. Cette optimisation de l'affichage facilite l'utilisation de l'application, quel que soit le dispositif utilisé.

3.4 Solutions et résultat

J'ai donc bien intégré le bouton "+" qui me permet d'ajouter des personnes dans l'annuaire directement depuis l'application. Quand on clique dessus, il ouvre sur le formulaire. Vous pouvez le voir ci-dessous.

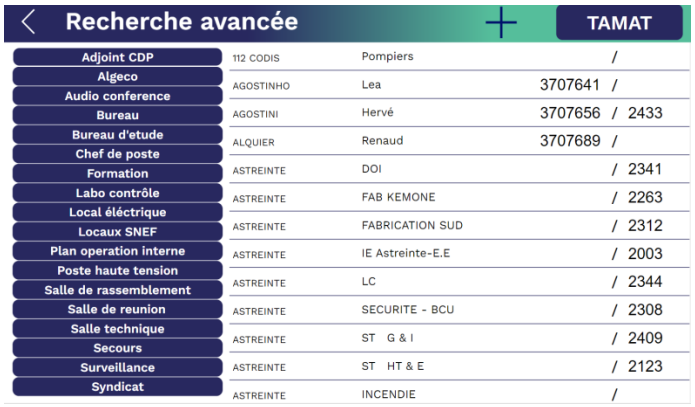

Figure 4 : Application *PowerApps* section Recherche avancée

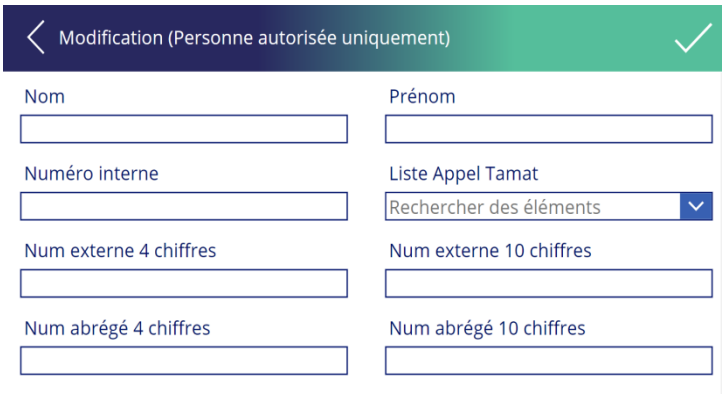

Figure 5 : Formulaire application *PowerApps*

En ce qui concerne le problème de modification et du zéro sur les numéros de téléphone, j'ai opté pour la solution la plus simple, qui consiste à changer le type de données dans la liste *SharePoint* de "nombre" à "texte". Cela m'a permis de supprimer le zéro statique et les boutons de réinitialisation. Désormais, les modifications s'appliquent automatiquement dès que l'utilisateur modifie le numéro.

En ce qui concerne le responsive*, le problème résidait dans la superposition des conteneurs, par exemple lorsque le conteneur du nom se superposait à celui du prénom. J'ai donc modifié toutes les pages de *PowerApps* pour éviter cette superposition des conteneurs.

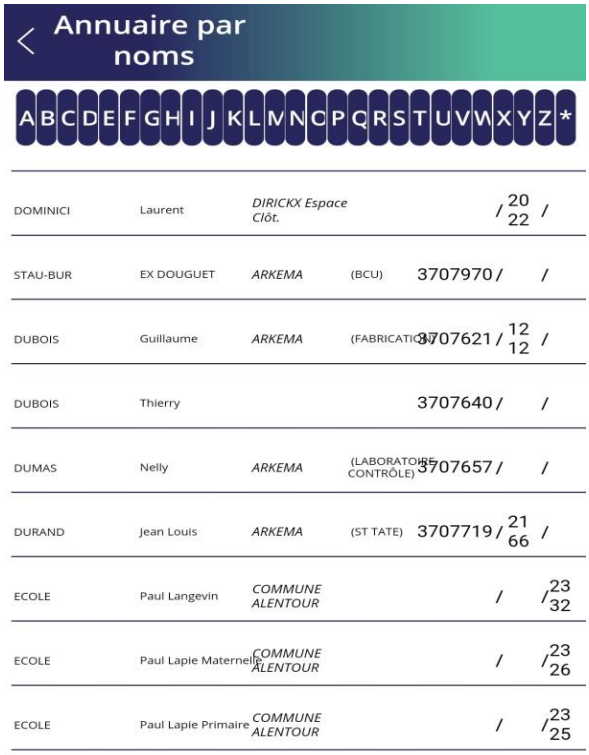

Figure 6 : Application sur tablette (Avant)

Figure 7 : Application sur tablette (Après)

Grâce à ces améliorations, on peut maintenant ajouter des personnes directement depuis l'application en utilisant le bouton "+". Les modifications des numéros de téléphone s'appliquent automatiquement

sans avoir besoin de réinitialiser les données, et les conteneurs ne se superposent plus. Le système gagne ainsi en convivialité.

3.5 Conclusion

C'était ma première mission et je suis satisfait de l'accomplissement de mes tâches en ce qui concerne les demandes spécifiques pour l'application. Bien que j'aie rencontré quelques difficultés en raison de mon manque d'expérience avec les outils *PowerApps*, j'ai pu surmonter ces obstacles avec succès.

4 Audit Cybersécurité

4.1 La directive de Arkema

4.1.1 Présentation générale de la directive

Arkema, en tant que grand groupe international, a élaboré une directive confidentielle établissant formellement les exigences spécifiques de l'entreprise en matière de cybersécurité pour les systèmes de conduite et les réseaux industriels. Cette directive vise à garantir la disponibilité, l'intégrité des unités de production et la protection de la propriété intellectuelle dans toutes les entités d'*Arkema*, quel que soit le pays.

Pour assurer la sécurité des réseaux industriels en constante évolution et de plus en plus connectés, *Arkema* a adopté une politique mondiale visant à renforcer la sécurité de ses systèmes informatiques. Un protocole strict a été établi. Il précise les exigences d'*Arkema* dans le domaine de la cybersécurité en se fondant sur l'approche A.I.C (Disponibilité, Intégrité et Confidentialité) Il s'agit de garantir l'accès, la préservation des informations échangées et stockées, le secret.

Cette directive s'appuie sur plusieurs documents de référence, tels que la norme internationale IEC 62443 pour la sécurité des réseaux de communications industriels, la norme ISO 27005 pour la gestion des risques, le NIST 800-82 (guide pour la sécurité des systèmes de conduite industriels) et des directives règlementaires de l'ANSSI, ainsi que le guide des bonnes pratiques.

Les usines d'*Arkema* sont classées en trois niveaux (C1, C2, C3) en fonction de leur importance en termes de production et de leur avantage compétitif. Les usines de classe 3 ont les exigences les plus élevées, notamment en raison de leur compétitivité, des contraintes réglementaires et des risques HSE. Les usines de classe 2 sont celles classées SEVESO (en Europe) ou COI (aux États-Unis) ou équivalent. Les usines de classe 1 sont les autres usines d'Arkema.

La directive regroupe les exigences selon cinq critères principaux :

1. exigences organisationnelles
2. exigences de conception
3. exigences opérationnelles
4. exigences de protection
5. gestion des incidents

En suivant ces critères, *Arkema* sécurise ses réseaux industriels, la protection des données et la réaction adéquate en cas d'incidents. La classification des usines permet d'adapter les exigences de cybersécurité en fonction de la criticité de la production, afin de limiter les contraintes au strict nécessaire pour chaque site.

4.1.2 Exigences organisationnelles

Ce critère vise à mettre en place la base administrative de la gestion de la cybersécurité dans l'usine. Il définit deux postes importants : le Responsable de la Sûreté des Systèmes de Conduite Régional (RSSC-R*) et le Responsable de la Sûreté des Systèmes de Conduite Local (RSSC-L). Le RSSC-R est chargé de superviser la sûreté du SII et des réseaux associés, tandis que le RSSC-L est responsable de l'application des règles de la directive au sein de l'entité et sert de relais d'information avec le RSSC-R.

Le RSSC-L doit gérer différentes listes, notamment celles des utilisateurs autorisés à accéder au SII, qu'ils soient des employés d'*Arkema*, des fournisseurs ou des sous-traitants. Il tient aussi à jour une liste des composants critiques des systèmes de conduite, en incluant les matériels obsolètes, les matériels sans mécanisme de protection, les dispositifs de protection et les matériels interconnectés à l'usine.

La directive exige également la mise en place de mesures de sensibilisation à la cybersécurité pour tous les utilisateurs ayant accès au SII. Un programme de formation approprié apporte aux personnels les connaissances nécessaires pour faire face aux menaces cybernétiques.

En plus du contrôle de leur permis de travail, les intervenants extérieurs doivent se conformer à une charte de cybersécurité spécifique. Avant d'utiliser leurs équipements sur le système, leurs matériels sont soumis à un contrôle préalable.
Il est nécessaire d'établir un inventaire détaillé des logiciels de maintenance et des systèmes utilisés. Des sauvegardes redondantes effectuées régulièrement et testées permettent de reconstruire le système en cas de problème.

La directive établit également des règles strictes concernant les accès à distance, généralement limités pour les intervenants extérieurs. Seules les équipes d'*Arkema* sont autorisées à apporter des modifications à distance.

Enfin, le critère exige des mises à jour régulières et prévoit la mise en place de mesures de compensation en cas d'impossibilité de mettre à jour un composant.

4.1.3 Exigences de conception

Il s'agit ici de définir les exigences sur la conception des réseaux et des interconnexions SII/SIE, en intégrant la cybersécurité dès la phase de conception pour réduire les risques le plus tôt possible dans la procédure de mise en place des systèmes. L'isolement du réseau est un critère important qui intègre la séparation totale du réseau industriel et de l'entreprise (bureautique). Si une interconnexion est nécessaire, elle doit être implémentée* avec des équipements de sécurité adaptés, sous la forme de firewalls ou de diodes. Une séparation facile est aussi exigée. Les connexions de l'extérieur au réseau transitent par un tunnel.

Cette section traite aussi des exigences concernant le contrôle d'accès aux données, en mettant en place une gestion d'accès nominative. Un système d'authentification est indispensable, avec un suivi des personnes inscrites, des mots de passe et des droits affectés en tant que points principaux. Les équipements réseaux industriels sont impérativement installés dans des endroits sécurisés qui assurent physiquement et logiquement la meilleure protection. L'installation de logiciels tiers non approuvés par *Arkema*, est naturellement soumise à des restrictions et à des contrôles. Il en va de même pour l'utilisation de dispositifs amovibles ou de tout autre dispositif capable d'introduire un risque dans le système. Enfin, cette partie aborde les accès physiques aux bâtiments et locaux techniques, ainsi que l'accès aux équipements et aux câbles du réseau.

4.1.4 Exigences opérationnelles

Ce critère vise à remédier aux risques de cybersécurité introduits par les opérations sur le système, en intégrant la cybersécurité dans le cycle de vie d'un système industriel. Des analyses de risques permettent d'identifier les vulnérabilités qu'il faut ensuite traiter. La sécurité des opérations de maintenance, de mise à jour, de modification de programme, de décommissionnement*, de reconfiguration ou d'installation d'équipements est soumise à un système d'audits.

Des architectures et cartographies détaillées sont stockées dans un endroit sûr. Les documents sensibles, tels que les architectures IP du site, sont l'objet d'une protection particulière. Des exigences sont également formulées concernant l'intégration de la cybersécurité dans les contrats et les spécifications, la gestion des modifications et des évolutions des programmes, les audits et tests de cybersécurité, l'analyse des risques, la gestion de l'obsolescence et le démantèlement des composants obsolètes du système.

La connaissance du système industriel, avec des règles sur la cartographie, la gestion de la documentation, les comptes et l'authentification sont un autre secteur important qui inclut l'administration du réseau, la gestion des comptes, l'authentification sécurisée, la sûreté des protocoles et la gestion des secrets tels que les badges, les clés et les mots de passe.

En résumé, ce critère implique l'existence d'outils permettant d'opérer sur le système de manière sécurisée, en réalisant une étude de cybersécurité avant de commencer l'exploitation. Il met en évidence la nécessité d'intégrer la cybersécurité dans le cycle de vie du système industriel, ainsi que sur la gestion sécurisée des opérations et la connaissance approfondie du système.

4.1.5 Exigences de protection

Ces exigences portent sur la protection des équipements, la gestion des outils de protection et de prévention, en intégrant des attentes spécifiques en matière de gestion des antivirus et de durcissement de la configuration. Les équipements sont forcément dotés d'antivirus à jour, avec une procédure claire de suivi, de gestion des alertes et d'analyse des événements. Les stations critiques nécessitent une protection plus élevée, ce qui suppose qu'elles soient isolées. L'accès aux systèmes pour les dispositifs amovibles est, quant à lui, contrôlé via une station de décontamination approuvée par *Arkema*.

Tous les événements systèmes et les flux d'informations entrants et sortants du système doivent être sécurisés et enregistrés dans des journaux, stockés de manière à garantir leur intégrité. Dans le cadre du durcissement de la configuration, il est important de désactiver les comptes par défaut non souhaités, les ports physiques inutilisés, les périphériques amovibles et les services web non souhaités.

Une subdivision des systèmes industriels est également requise, avec l'élaboration d'une cartographie et des subdivisions physiques entre les zones fonctionnelles du système. D'autres règles sont établies pour la gestion des vulnérabilités, celle des médias amovibles et mobiles, la sécurité des postes de développement et d'administration, la sûreté des consoles de programmation qui ne sauraient être connectées à *Internet*. La surveillance du SII est également abordée, avec l'historisation des événements et la détection d'un état anormal du réseau.

En résumé, ces exigences visent à assurer la protection des équipements en mettant en place des outils de prévention et de protection, tout en intégrant des mesures spécifiques telles que la gestion des antivirus, le durcissement de la configuration, la subdivision des systèmes, la gestion des vulnérabilités et la surveillance du SII.

4.1.6 Réaction en cas d'incidents

Cet ensemble de règles compose un cadre de réponses aux incidents, en se préparant à affronter des événements exceptionnels pour lesquels toutes les mesures précédentes ont échoué. Des procédures consignées et testées permettent de réagir en cas d'attaque, en manipulant tous les éléments relatifs à l'incident sur un équipement isolé du système industriel afin d'éviter une propagation éventuelle. Des procédures particulières, incluant des modalités de fonctionnement en mode dégradé, mettent la production à l'abri d'une paralysie consécutive à une éventuelle attaque.

Des consignes de reprise du fonctionnement normal dans les meilleurs délais s'appliquent à la phase de post-attaque. Cette séquence comprend également des règles sur le traçage des incidents, l'endiguement d'une attaque grâce à un plan de crise, le plan de reprise d'activité, le mode dégradé et la gestion de crise.

4.2 Audit des locaux informatiques

4.2.1 Contexte

Une de mes principales missions pendant la durée de mon stage a consisté à réaliser un audit des armoires réseau de l'usine, tout en tenant compte des exigences opérationnelles de la directive de sécurité. Ces armoires contiennent divers équipements : des tiroirs à fibres optiques, des switches et des PC, qui permettent la communication entre les différentes parties de l'usine. L'audit que j'ai effectué comprend plusieurs aspects, notamment l'inventaire des appareils présents dans chaque armoire, la mise à jour de la cartographie du réseau et, éventuellement, la modification des noms des fibres. Il est essentiel de mener cet audit pour maintenir la sécurité de l'infrastructure réseau de l'usine, conformément aux directives d'*Arkema*. Pour m'aider dans cette tâche, j'ai disposé d'outils comme un plan d'infrastructure détaillé et une application d'audit spécifique.

4.2.2 Plan d'architecture fibre

L'usine possède un vaste réseau de fibre optique qu'il faut préserver. Il est donc nécessaire de maintenir à jour le plan existant qui détaille le contenu de chaque salle informatique. Cependant, des erreurs sont possibles en raison des modifications apportées à l'architecture réseau ou parfois d'oublis humains. Les salles qui contiennent des armoires abritant du matériel réseau sont vérifiées. Ci-dessous, une comparaison entre une armoire réelle et sa représentation sur le plan :

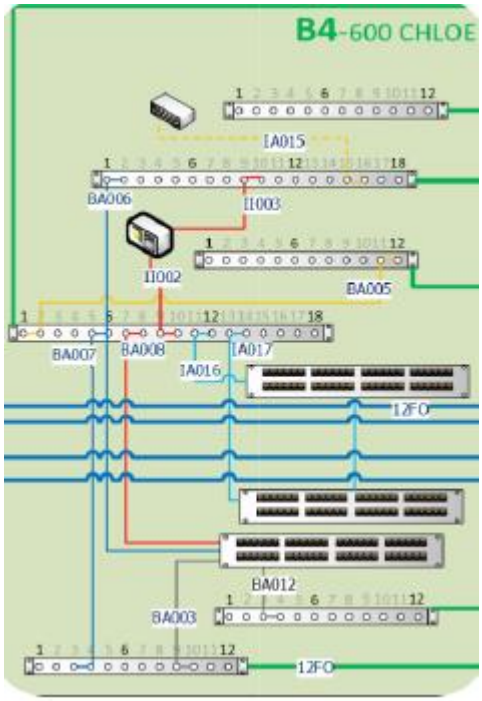

Figure 8: Armoire sur le plan

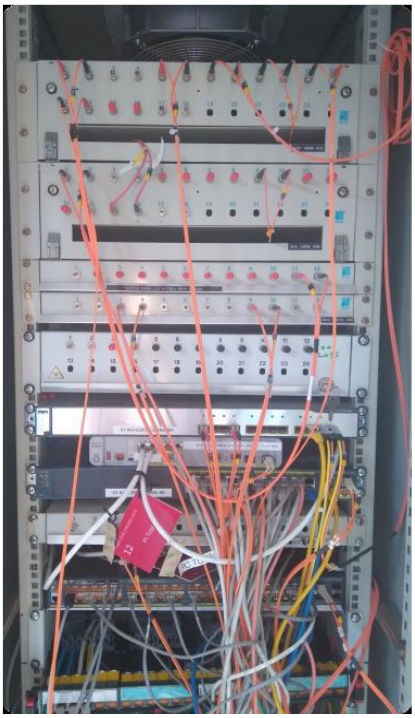

Figure 9 : Armoire Réelle

On constate que chaque équipement réseau dispose d'une représentation correspondante. Les connexions en fibre à l'intérieur de l'armoire sont étiquetées avec un identifiant unique afin de prévenir toute confusion. Les connexions en fibre à l'extérieur (vers d'autres salles) sont étiquetées en fonction de leur diamètre, ce qui permet d'obtenir une indication sur la vitesse de la connexion.

4.2.3 Application d'audit cybersécurité : son fonctionnement et son champ d'application

Afin de faciliter le travail de l'auditeur et de garder une trace des résultats d'audits, le service IIA a mis en place une application PowerApps qui permet d'effectuer des audits sur le terrain à l'aide d'une tablette.

L'application définit donc les critères de sécurité suivants :

- **Nom de l'armoire**
- Vérifier si le nom de l'armoire est présent sur celle-ci. Cela est indispensable pour éviter toute erreur lorsque plusieurs armoires sont présentes dans la même pièce.
- **Type de local**
- Vérifier le type de local dans lequel se trouve l'armoire, qu'il s'agisse d'un bureau, d'un couloir, d'une salle technique ou d'une salle de contrôle.
- Local fermé.

- Vérifier si le local est fermé et si son accès est contrôlé.

- **Armoire verrouillée**

- Vérifier si l'armoire est verrouillée afin d'empêcher un accès non autorisé et de s'assurer que les personnes ferment correctement les armoires.

- **Nombre de switches**

- Indiquer le nombre de switches présents dans le local ou dans l'armoire si plusieurs armoires sont présentes dans le local.

- **Nombre de PC**

- Indiquer le nombre de PC présents dans l'armoire.

- **RJ45 bloqués**

- Vérifier que tous les ports RJ45 sont bloqués à l'aide de bloqueurs pour éviter les connexions non autorisées. Si les ports ne sont pas bloqués, ils doivent être bloqués immédiatement. Le point est ensuite validé.

- **USB bloqués**

- Vérifier que les ports USB sont bloqués pour les mêmes raisons. Si les ports ne sont pas bloqués, ils doivent être bloqués immédiatement, de la même manière que les ports RJ45. Puis, le point est validé.

- **Repères sur les fibres optiques**

- S’assurer que les repères correspondent à ceux indiqués sur la cartographie. Si ce n'est pas le cas, il faut vérifier si le problème provient du repérage ou du plan en suivant les fibres sur d'autres baies optiques.

- **Observations**

- Des observations particulières appellent un signalement, comme notamment la répartition de l'armoire dans plusieurs endroits de la pièce, l'absence de bloqueurs ou la nécessité de vérifier des repères...

- **Photos**

- L'auditeur doit également prendre une photo de l'armoire afin de disposer d'informations sans avoir à quitter le bureau.

- **Nom et date**

- Il est également nécessaire d'indiquer le nom de l'auditeur pour assurer une traçabilité adéquate. La date est renseignée automatiquement.

Figure 8 : Page d'audit armoire (1)

Figure 9 : Page d'audit armoire (2)

Je me suis déplacé partout dans l'usine pour effectuer les audits en utilisant les deux outils décrits précédemment. Certaines armoires qui n'avaient pas été visitées depuis un certain temps présentaient des erreurs de représentation sur le plan. D'autres avaient des problèmes d'étiquetage au niveau des fibres optiques ou manquaient de bloqueurs RJ45 ou USB.

En général, la mission n'était pas compliquée. Cependant, certaines armoires étaient difficilement accessibles. Quelquefois, elles nécessitaient l'utilisation d'équipements de sécurité spéciaux ou la présence d'encadrants pour m'accompagner.

4.2.4 Amélioration de l'application d'audit cybersécurité

On m'a également demandé d'améliorer l'application d'audit susceptible de faciliter la sélection des armoires à auditer.

J'ai donc ajouté des filtres à l'application, tels que "Armoire non conforme", repère pour les armoires ne respectant pas la directive d'*Arkema*. La mention "Par date, s'applique aux armoires en fonction de leur dernière date d'audit, et "Criticité", signale les armoires par ordre décroissant de leur niveau de criticité.

Figure 10 : Page filtre application audit

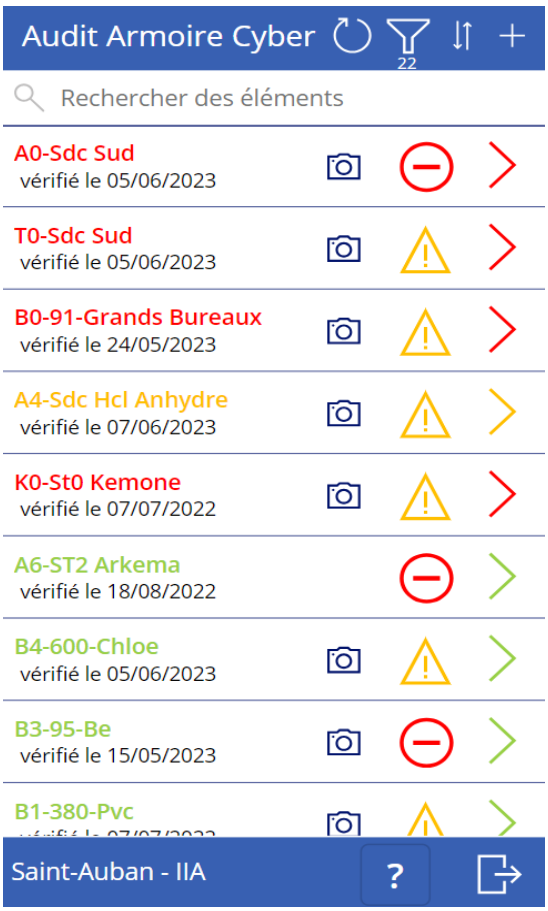

Figure 11 : Page liste des armoires non conformes

De plus, il m'a été demandé de rajouter des icônes pour une meilleure visualisation de l'état de conformité des armoires. Une icône avec un panneau rouge a été apposée pour alerter sur une armoire non conforme. Une icône d'attention orange a été retenue pour indiquer une légère non-conformité. J'ai également coloré le texte des armoires en fonction de leur criticité, soit rouge, soit jaune, soit verte.

Voici comment j'ai déterminé si l'icône du panneau rouge ou l'icône d'attention devait apparaître en fonction de l'audit réalisé :

L'icône du panneau rouge s'affiche lorsque le local n'est pas fermé ou lorsque l'armoire n'est pas verrouillée, ou encore en cas de problème avec la cartographie.

```
If(
    Or(
        And(
            ThisItem.'Local Fermé' = false;
            ThisItem.'Armoire verrouillée' = false
        );
        ThisItem.'Repère cartographie'=false
    );
    true
)
```

Figure 12 : Programme affichant le panneau rouge

L'icône d'attention s'affiche lorsque les conditions de l'icône rouge sont remplies et qu'il n'y a pas de bloqueur RJ45 ou USB, pas de système de vidéosurveillance, et que l'armoire a une criticité rouge. De plus, si l'armoire n'a pas de nom ou s'il manque des repères de fibre optique, l'icône d'attention est également retenue.

```
If(
    And(
        And(
            Or(
                ThisItem.'Local Fermé' = true;
                ThisItem.'Armoire verrouillée' = true
            );
            ThisItem.'Repère cartographie' = true
        );
        Or(
            And(
                ThisItem.'Nb De Switch' > 0;
                ThisItem.'RJ45 bloqué' = false
            );
            And(
                ThisItem.'Nombre PC' > 0;
                ThisItem.'USB bloqué' = false
            );
            And(
                ThisItem.'Criticité de l''armoire'.Value = "Rouge";
                Or(
                    ThisItem.'Matériel Vidéosurveillance' = false;
                    ThisItem.'Matériel Vidéosurveillance' = Blank()
                )
            );
            ThisItem.'Nom sur l''armoire' = false;
            ThisItem.'Repère FO' = false
        )
    );
```

Figure 13 : Programme affichant le panneau attention

J'ai également intégré une icône photo quand une photo de l'armoire a été prise lors de l'audit. De plus, l'affichage rouge des problèmes de non-conformité attire l'attention.

Enfin, j'ai mis en place un bouton Pop-up pour aider l'auditeur à nommer les repères de fibre.

Figure 14 : Affichage du Pop-up pour le repérage de fibre optique

Ces améliorations permettent à l'auditeur de mieux identifier les armoires à vérifier. Elles facilitent la gestion des audits en offrant une meilleure visualisation des informations pertinentes.

5 Conclusion

Je suis très heureux d'avoir eu l'opportunité d'effectuer mon stage chez *Arkema*, une entreprise de classe mondiale. Durant cette période, j'ai pu mettre en pratique les compétences acquises tout au long de ma formation et découvrir le monde du travail et de l'industrie. J'ai pu approcher le fonctionnement d'une grande entreprise et participer modestement à ses activités.

Les tâches que j'ai effectuées étaient variées, allant de l'utilisation d'outils tels que PowerApps ou SharePoint, avec lesquels je n'avais jamais travaillé auparavant, à des aspects liés à la cybersécurité. J'ai pu prendre conscience des exigences d'*Arkema* dans le domaine de la cybersécurité, que ce soit en ce qui concerne les procédures opérationnelles mises en place, par exemple pour la reprise d'activité en cas d'attaque, ou encore la cartographie complète du réseau du site.

Ce stage m'a apporté énormément tant sur le plan humain que technique. Je conserve un excellent souvenir des quelques semaines passées au sein de la cellule IIA.

Cette expérience est précieuse dans l'apprentissage de ma vie professionnelle et dans ma vie personnelle.

6 Remerciements

Je tiens à remercier sincèrement Madame Margaux GALETTI du service des ressources humaines pour la confiance qu'elle m'a accordée lors de mon recrutement.

Je remercie chaleureusement mon tuteur de stage, Philippe JEANSON, pour le temps précieux qu'il m'a accordé tout au long de mon stage. Sa grande expertise et sa disponibilité ont grandement contribué à la réussite de mes missions.

Je souhaite également exprimer ma gratitude envers toute l'équipe de la cellule IIA avec laquelle j'ai eu le privilège de travailler au quotidien. Leur bienveillance et leur expérience m'ont permis d'approfondir mes connaissances techniques et de mieux appréhender le fonctionnement de l'entreprise.

Je remercie toutes les personnes que j'ai pu croiser à *Arkema* pour la qualité de leur accueil.

Je souhaite exprimer ma reconnaissance envers ma tutrice académique, Anouch HOVSEPIAN. Son suivi attentif et avisé tout au long de mon stage m'a beaucoup apporté.
Je remercie également l'Université d'Aix-Marseille qui m'a offert l'opportunité d'effectuer ce stage et de mettre en pratique mes connaissances acquises au cours de ma formation.

7 Glossaire

BUT, Bachelor Universitaire de Technologie

IIA, Informatique Industrielle et Automatisation

ST MC, Service Technique Moyens Centraux

RSSC-L, Responsable de la Sûreté des Systèmes de Conduite Local

RSSC-R, Responsable de la Sûreté des Systèmes de Conduite Régional

Rhéologie : La rhéologie se concentre sur la manière dont les matériaux se déforment et s'écoulent en réponse à des forces appliquées, ce qui permet de mieux comprendre et de modéliser leur comportement mécanique et leurs propriétés de flux.

Responsive : Le terme "responsive" est principalement utilisé dans le contexte du design et du développement web. Il fait référence à la capacité d'un site web ou d'une application à s'adapter et à répondre de manière dynamique à différents appareils et tailles d'écran, offrant ainsi une expérience utilisateur optimale quel que soit le dispositif utilisé (ordinateur de bureau, tablette, smartphone, etc.)

Implémenter : "Implémenter" signifie mettre en œuvre, réaliser ou exécuter quelque chose. Lorsqu'on implémente quelque chose, on prend les mesures nécessaires pour concrétiser une idée, un plan ou une solution spécifique.

Décommissionnement : signifie arrêter, retirer ou désactiver quelque chose qui n'est plus nécessaire. Cela implique de mettre hors service, de retirer physiquement ou de désactiver de manière appropriée ce qui est concerné, tout en prenant en compte la gestion des déchets et la remise en état si nécessaire.

Monomère : Une activité monomère fait référence à une molécule chimique qui est capable de s'assembler avec d'autres molécules identiques pour former un polymère. Les monomères sont les unités de base des polymères et leur répétition permet la formation de chaînes plus longues.

8 Bibliographie

- https://www.arkema.com/global/fr/ (Site officiel de Arkema)

- https://www.arkema.com/france/fr/locations/production-centers/saint-auban/ (Site de Saint-Auban)