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 EN CYBERSECURITE

Finaritra ANDRIAMAHAKAJY

ARKEMA France

Responsable entreprise : Georges SIMONCINI

Responsable académique : Anouch HOVSEPIAN

2023

Table des matières

1 Introduction

La Cybersécurité devient primordiale dans notre ère. En effet, nous ne sommes pas à l'abris des dangers, surtout en informatique. C'est pourquoi Arkema met en place plusieurs solutions tels que des formations, des modules en ligne ou encore des appareils pour sensibiliser les employés.

J'ai réalisé un stage en Cybersécurité à l'usine d'Arkema Saint-Menet, à Marseille, afin de finaliser ma deuxième année de BUT, Bachelor Universitaire de Technologie, en Réseaux et Télécommunications, parcours Cybersécurité que je suis au sein de l'IUT, Institut Universitaire de Technologie à Marseille Luminy.

Le but de mon stage était d'exploiter les connaissances que j'ai acquis lors de ma formation en réseaux, en informatique, et en Cybersécurité. De plus cela m'a permis d'approfondir et d'améliorer mes compétences techniques et comportementales mais aussi d'en obtenir de nouvelles. Enfin mon stage consistait à m'intégrer le plus possible dans le monde du travail, plus particulièrement dans l'univers de l'industrie.

J'ai intégré le service de l'Informatique Industrielle où j'ai pu m'initier dans ce domaine. L'informatique Industrielle, c'est de l'informatique intégrée dans des équipements. Aujourd'hui l'automatisation occupe une part importante dans l'industrie, elle est essentielle pour une meilleure production en sécurité.
L'équipe est composée de 4 personnes : le responsable en Informatique Industrielle et 3 techniciens dont un renfort d'une entreprise extérieure (figure 1). Un stagiaire en automatisme est arrivé en cours de route, ce qui nous a permis d'échanger et de partager nos acquis.

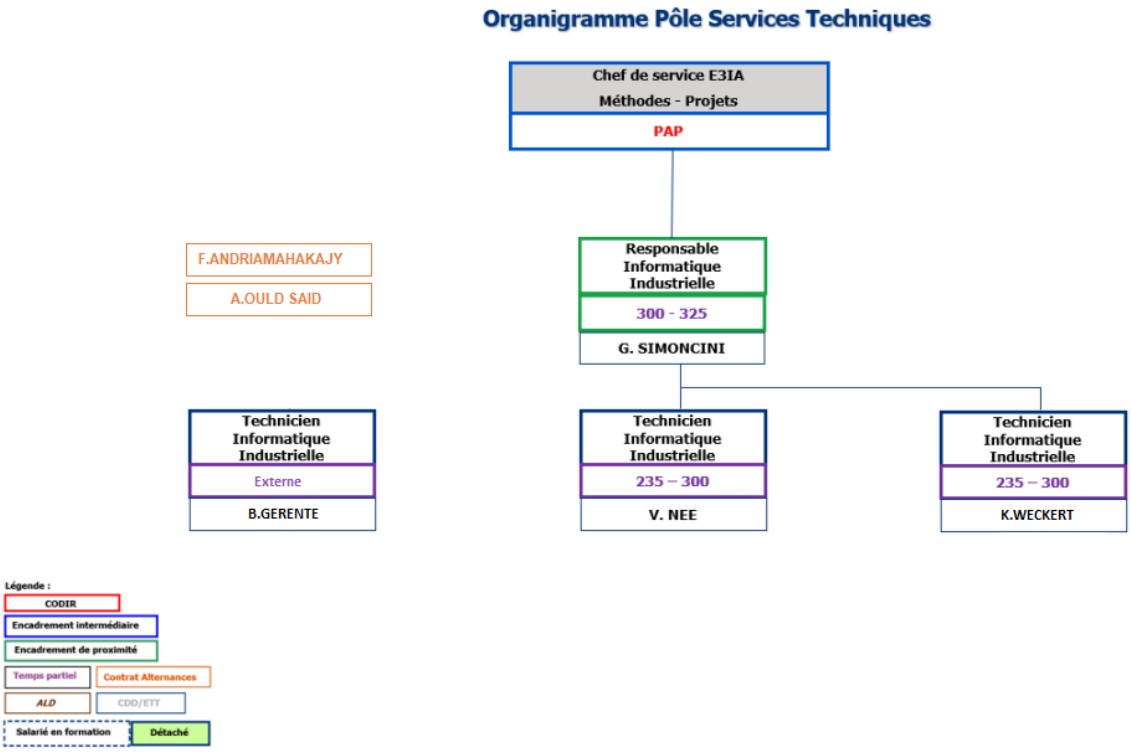


Figure 1 : Organigramme du Service Informatique Industrielle

Dans un premier temps, vous verrons une présentation du groupe Arkema à l'échelle internationale, nationale et locale. Ensuite, nous nous intéresserons à mes

différents projets de stage au sein de cette entreprise, ayant pour thème la cybersécurité, et l'informatique industrielle.

2 Présentation de l'entreprise

2.1 Groupe Arkema

2.1.1 À l'Internationale

Arkema est un groupe chimique français, particularisé dans la chimie de spécialité et des matériaux de performance. Il souhaite devenir un acteur à 100% des Matériaux de Spécialités d'ici 2024. Le groupe est organisé autour de quatre parties innovantes ceux qui représentent 80% du chiffre d'affaires du Groupe : les Adhésifs, les Matériaux Avancés, les Coating Solutions et les Intermédiaires. L'entreprise offre des solutions technologiques de pointe pour répondre aux enjeux des nouvelles énergies, de l'accès à l'eau, du recyclage, de l'urbanisation, ou encore de la mobilité.

En 2022, Arkema compte 21 100 collaborateurs dans 55 pays, donc dans 148 sites industriels au total dans le monde. Son chiffre d'affaires est de 11,5 milliards d'euros, soit 21,3% de plus qu'en 2021. Son siège social est situé à Colombes, dans les Hauts-de-Seine en France.

2.1.2 En France

Arkema essaie de préserver une forte implantation en France et conduit plusieurs chantiers de modernisation et de développement sur différents sites. En France, elle dispose de 7 centres de recherche et développement et 26 sites de production. Près de la moitié des investissements d'Arkema concernent la France. De plus environ 45% de la production du Groupe est réalisée sur le territoire français.

2.2 Arkema Marseille

2.2.1 Un site de production

Créée en 1955, l'usine Arkema Marseille s'occupe de la production d'un monomère, l'acide amino-11-undécanoïque ou "amino-11", à partir d'une matière première : l'huile de Ricin ; afin d'obtenir du plastique d'origine 100% végétale et renouvelable.

Ce produit est mondialement connu sous le nom de Rilsan®. C'est un plastique technique à hautes performances dont la production se caractérise par un minime besoin en énergie et de plus faibles émissions de CO^2. Il est performant en termes de résistance mécanique mais aussi de température, de corrosion et de légèreté. Il est utilisé dans des secteurs variés tels que l'automobile, l'aviation, les équipements sportifs, les textiles techniques mais aussi dans les industries cosmétique, les industries médicales et pharmaceutiques, ou encore pour la parfumerie.

Figure 2 : Plan de l'usine

Le site d'Arkema Marseille (figure 2) possède 5 unités :

- L'unité 10, nommé le PARC, qui regroupe tous les co-produits
- L'unité 20, appelée C11, qui est dédiée aux premières étapes de la transformation de l'huile
- L'unité 30 est la bromuration
- L'unité 40 ou 45 est l'amination
- L'unité 900 et 950, dit aussi la CENTRALE, qui gère la distribution en électricité, en gaz, en eau et en air et où l'on produit de la vapeur.

Le procédé de fabrication de l'amino-11 (figure 3) est unique au monde. Tout d'abord, l'huile de ricin va subir des transformations chimiques en passant par le C11 et se transformer en un acide gras composé de 11 atomes de carbone, l'acide undécylénique. Celui-ci est envoyé à l'unité 30, soit la bromuration, pour réagir avec l'acide bromhydrique et devenir l'acide bromo-undécanoïque, surnommé à l'usine le bromo. Par la suite, le bromo est déplacé vers l'amination, là où il se mélangera à de l'ammoniac afin de se transformer en acide undécanoïque. La réaction de ces derniers sera lente. Enfin, l'amination est l'endroit où le produit est purifié avant d'être placé dans de grands sacs à expédier.

L'usine peut produire 21000 tonnes par an d'amino-11, qui sont expédiées dans les usines de Serquigny en Normandie, Shangshu en Chine et Birsboro aux Etats-Unis, pour être polymériser, c'est-à-dire que la poudre d'amino-11 subira une réaction chimique pour se transformer en de billes de plastique.

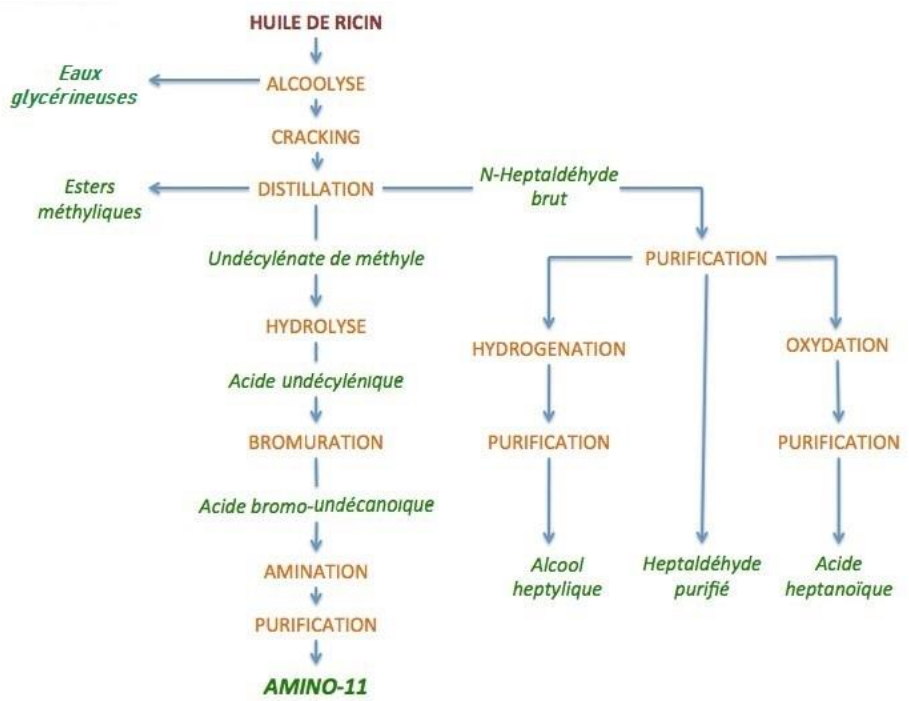


Figure 3 : Schéma de fabrication de l'amino-11

La production de l'amino-11 engendre la formation d'autres composés comme la glycérine pure, les esters méthyliques, l'alcool heptylique qu'on appelle aussi éthanol, l'heptaldéhyde purifié ou encore l'acide heptanoïque. Ces co-produits sont stockés dans le PARC puis sont vendus car tout ce qui est produit est réutilisable.

Arkema priorise la sécurité à la production, En effet, l'usine se trouve dans la ville de Marseille, donc à côté des habitants. De plus, elle utilise et stocke des produits dangereux en grande quantité et en grande concentration : il s'agit du chlore, du brome et de l'ammoniac, ce sont des produits dangereux pour les êtres humains et pour l'environnement. Par conséquent le site marseillais est classé site SEVESO seuil haut. Cette directive permet de prévenir aux employés mais aussi aux riverains du danger de l'usine.

Figure 4 : Panneau ATEX

Sur le terrain, il y a des zones « ATEX », Atmosphère Explosive, par conséquent, nous avons un EPI, équipement de protection individuel, qui est obligatoire lorsqu'on monte sur le terrain : un bleu de travail, un casque, des lunettes de protection, des protections auditives, des chaussures de sécurité et un masque de fuite si un incident se produit. Certains ont des gants car ils manipulent.

2.2.2 Le Grand Arrêt

Le Grand Arrêt est un moment important pour l'usine : d'où son nom, le Grand Arrêt est l'arrêt complet obligatoire règlementaire et nécessaire pour la fiabilité de l'usine. Il se passe tous les 6 ans afin de remettre à niveau le site de production et d'effectuer de grands travaux de maintenance : la migration des équipements, les changements des raccords ou des tuyaux, ainsi que la sécurité. Par exemple, cette année une chaudière de 50 tonnes a été complètement changée, ce qui a nécessité la mobilisation de plusieurs employés. Le Grand Arrêt se prépare pendant plusieurs mois pour une durée de 2mois environ. Celui de 2023 s'est tenu de mi-mars à mi-mai.

Il représente un investissement d'environ 27M€ pour des projets d'amélioration de l'efficacité énergétique du site, des travaux sur les postes électriques et sur les systèmes de contrôles avancées, ainsi que des travaux de perfectionnement de nos équipements et également des opérations de nettoyages et de contrôles des appareils, et 10M€ de plus pour les projets connexes.

Le Grand Arrêt implique la coopération de tous les services d'Arkema mais aussi la collaboration entre Arkema et plusieurs entreprises extérieures sur le site. En effet, il y a environ 600 employés dont environ 300 viennent de l'extérieur.
Le précédent arrêt s'est déroulé en 2017.

3 Mon projet de stage

3.1 Cybersécurité

Le site d'Arkema Marseille est un site sensible OIV. Il nécessite d'une protection de haut niveau au quotidien. En effet, beaucoup de données sont confidentielles ce qui fait de lui une véritable cible pour les attaquants. C'est la raison pour laquelle la Cybersécurité est indispensable pour un site comme Arkema.

La Cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les réseaux et les données contre les attaques malveillantes. Toutes les personnes doivent être au courant des différents dangers qu'ils courent notamment en informatique. Pendant mon stage, j'ai effectué différentes missions concernant ces parties de la cybersécurité.

3.1.1 Le SNCC

La première partie de mon stage se passait pendant le Grand Arrêt. J'ai contribué à la mise à jour des architectures réseaux de l'usine (figures 5 et 12). En effet, grâce au Grand Arrêt, on a pu changer et déplacer les appareils des armoires de ABB et Emerson, c'est-à-dire les serveurs et les switchs. J'ai donc fait les relevés pour actualiser les adresses IP des différents postes, des serveurs, des réseaux et des switchs, vérifié l'emplacements des équipements et j'ai pu échanger avec les ingénieurs de ABB. Les armoires de ABB se trouvent à la bromuration et à l'amination tandis que celles d'Emerson sont à la Centrale et au C11. Les armoires d'Emerson sont reliées par une fibre qui est leur seul point de reliure pour sauvegarder toutes les données des serveurs dans un serveur qui sert de backup, situé à la Centrale.

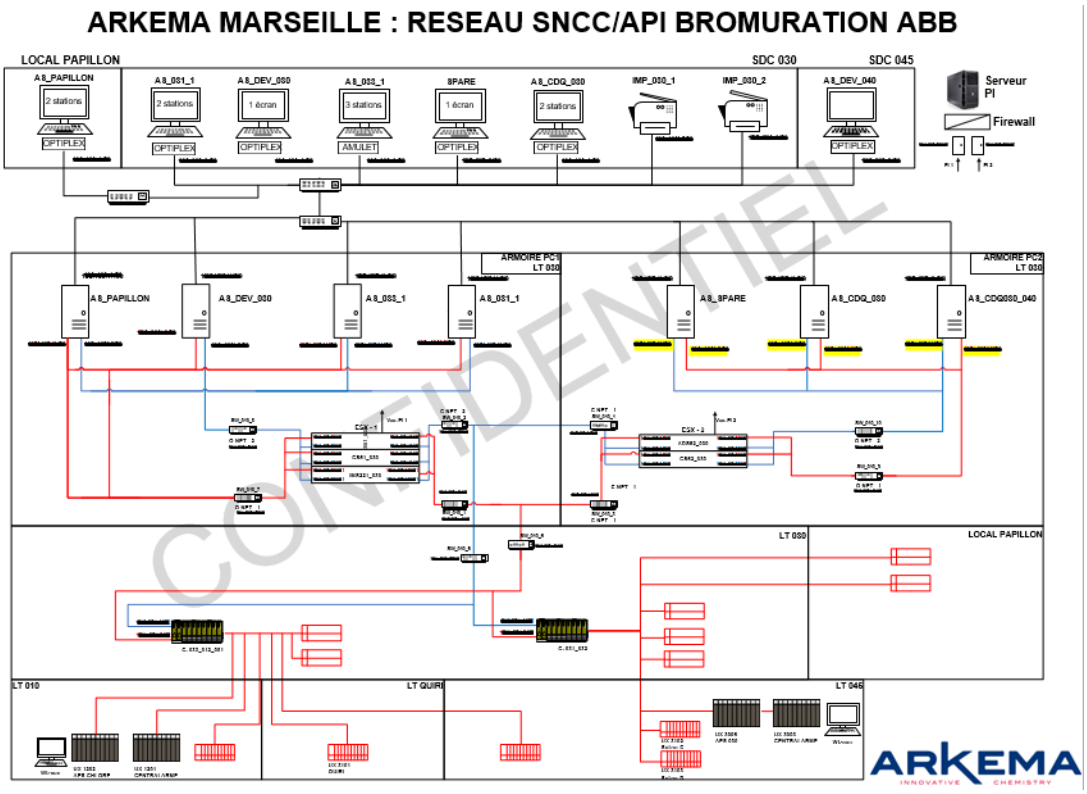


Figure 5 : Architecture du réseau informatique de ABB

Au sein du SNCC, Sytème Numérique de Contrôle Commande, il existe 2 types de réseaux :

- **Operating Network**, c'est le réseau du côté des opérateurs : les serveurs sont reliés aux postes opérateurs. Les opérateurs pourront faire différentes manipulations : marche/arrêt des séquences, les régulations, les alarmes, les courbes de tendances. Grâce aux synoptiques (figure 6), ils conduisent les installations.

- **Controlling Network**, le réseau des contrôleurs : les serveurs sont doublement reliés aux contrôleurs (voir 3.2.1) afin d'avoir une redondance du réseau, cela veut dire que si nous avons un réseau dysfonctionnel, le deuxième réseau prendra le relais.

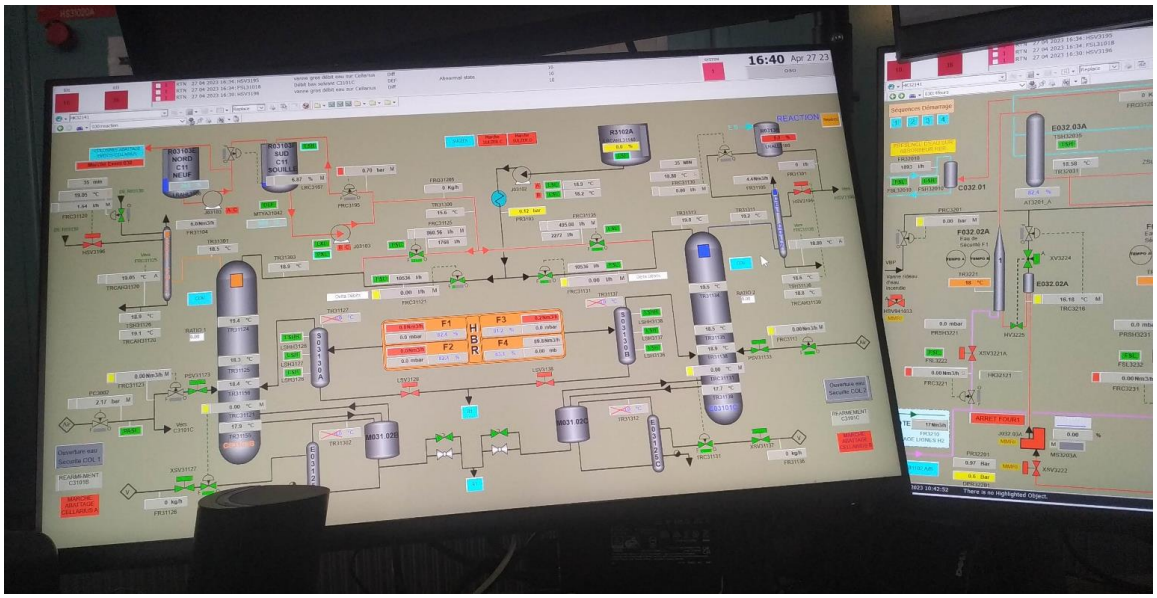


Figure 6 : Synoptique des colonnes de la bromuration

Quand j'allais sur le terrain, j'étais plus souvent du côté de la bromuration et de l'amination, donc j'ai pu voir les armoires de ABB et observer plusieurs synoptiques de la bromuration.

Lors de notre cursus à l'IUT, nous avons vu qu'il existe différents protocoles réseau, et l'un d'eux était fort semblable au réseau SNCC : il s'agit du STP, Spanning-Tree Protocol, qu'utilise les appareils Cisco. Il est important d'avoir une redondance de réseau pour ne pas avoir qu'un seul point de défaillance ; mais elle peut causer des boucles réseaux. Le STP permet d'avoir cette redondance sans boucles en désactivant certains liens de réseaux et en ayant qu'un seul chemin. Si un des switches ou qu'une liaison est défectueux/-se, l'autre réseau remplace le premier.

Ensuite j'ai créé une procédure pour l'utilisation du logiciel HiView (figure 7), et plus particulièrement comment bloquer les ports des switchs Hirschmann. Cela permettrait aux utilisateurs et aux nouveaux arrivants de les guider. Il est important de bloquer les ports pour que les personnes malveillantes ne puissent pas se connecter au réseau.

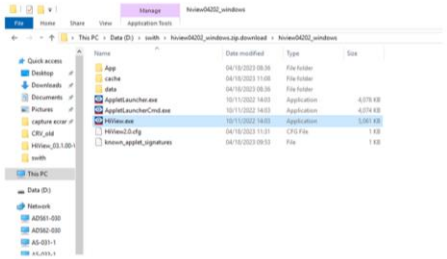
TUTO BLOCAGE DES PORTS SWITCHS

Grâce à ce document, nous allons apprendre à bloquer les ports des switchs.

1. D'abord, **se connecter sur la station en administrateur**. A partir de la "connexion de bureau à distance", Choisir la machine virtuelle cs51-030 (si vous êtes à l'unité 30) ou cs51-040 (l'unité 40).

2. Sur la machine virtuelle, aller sur l'arborescence et suivre le chemin suivant afin d'accéder au logiciel "HiView" :

D:\switch\hiview04202_windows.zip.download\ hiview04202_windows

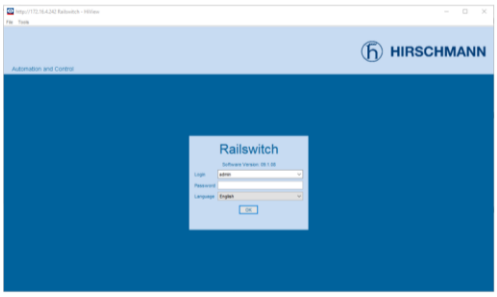


3. On peut voir tous les équipements sur la page d'accueil. Cliquer sur le switch dont vous voulez bloquer les ports pour accéder à son interface graphique (GUI).

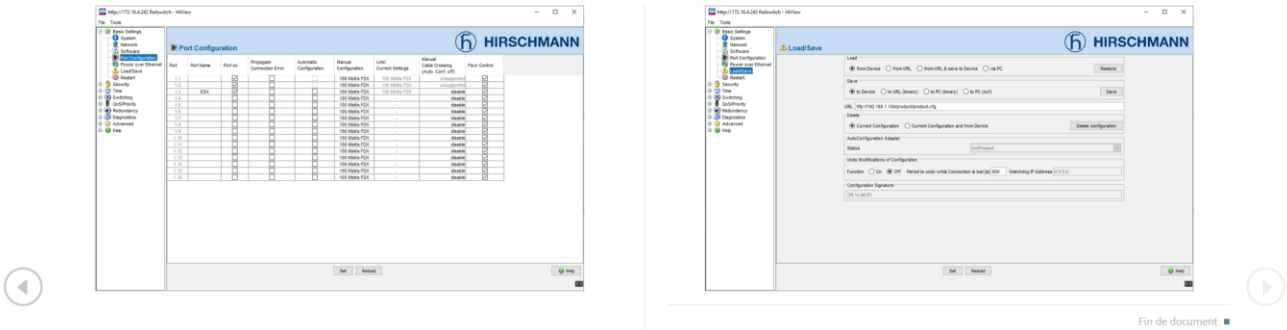
4. On atterrira sur une page de connexion. **Connectez-vous en mode administrateur.**

Login: admin

Password: private



5. Maintenant **bloquons les ports**. Pour cela, aller sur l'onglet "Port Configuration" et décocher les ports cochés dans la colonne Port on. Ne pas oubliez de cliquer sur le bouton "Set".



6. Enfin, **sauvegarder les modifications sur l'équipement et sur le portable**. Aller sur l'onglet "Load/Save" et sélectionner "Save to Device". Ne pas oublier de cliquer sur le bouton "Save" puis sur le bouton "Set". Faire de même pour l'ordinateur : "Save to PC (binary)".

Fin de document

Figure 7 : Procédure du bloquage des ports des switchs

À l'institut universitaire, on a pu voir comment sécuriser les ports de nos switchs Cisco. Grâce à ces lignes de commande (figure 8), il est possible d'autoriser les adresses MAC, c'est-à-dire les personnes qui peuvent accéder au réseau. Si une règle "port-security" n'est pas respecté alors le mode de Violation que nous avons défini s'active. Il y a 3 modes de violation :

- Le mode **protect** permet au port d'arrêter de transférer le trafic des adresses non autorisées sans envoyer de message de log.
- Le mode **restrict** va arrêter de transférer le trafic des adresses non autorisées et va transmettre un message de log.
- Le mode **shutdown** va fermer le port et envoyer un message de log.

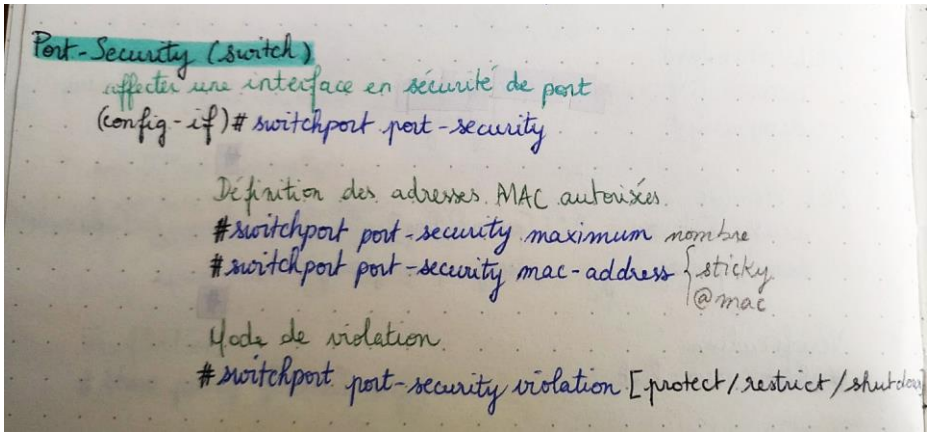


Figure 8 : Commandes Cisco pour sécuriser les ports

Le logiciel de Hirschmann possède une interface graphique, de ce fait je n'ai pas utilisé les commandes.

Par la suite, on m'a demandé de modifier le site web de HiView pour avoir toutes les informations concernant chacun des équipements. Malheureusement, j'ai constaté qu'il n'était pas possible de modifier directement le site web du logiciel. Il fallait donc trouver une solution pour avoir toutes les données. De mon côté, j'ai contacté le gérant du logiciel mais sa réponse ne m'a pas plus éclairé.

Enfin, j'ai eu pour mission de gérer les comptes SNCC. Chaque utilisateur a son propre compte et nous avons la possibilité de savoir qui est allé ou a modifié

son compte en dernier. Ma partie consistait à mener la suppression des comptes SNCC lorsqu'un utilisateur quitte son poste. Effectivement, nous n'étions pas directement avertis des départs. Pour en être informé et d'être sûr des personnes sortantes, il y a une fiche de sortie qui permet à tous les services d'exécuter chaque action pour le départ de l'employé.
Je suis allée au bureau administratif pour qu'il puisse ajouter à ce fichier, la suppression des comptes SNCC comme action principale. Après c'est la GED, Gestion Electronique des Documents, qui approuve la modification du document. Aujourd'hui cette procédure peut être appliqué convenablement.

3.1.2 Les équipements

Des équipements de sécurité sont mis à disposition pour éviter toute attaque. En matière de cybersécurité, le Groupe a mis en place une politique de renforcement de la protection des réseaux informatiques d'entreprise et d'informatique industrielle au niveau mondial. Afin de déployer cette politique sécurité, le programme de sensibilisation « i-Safe » lancé en 2018 est basé sur les bonnes pratiques.

Figure 9 : Bloqueur i-Safe

Lors de notre arrivée, Arkema nous donne un outil de la mobilité i-Safe qui nous permet d'utiliser nos appareils en sécurité. Il s'agit d'un bloqueur (figure 8) qui empêche les échanges de données. J'ai eu l'occasion de me servir de ce bloqueur lors d'un trajet en train : N'ayant plus de batterie, j'ai dû charger mon téléphone dans le train. Par conséquent je me suis servi du bloqueur pour que les données de mon téléphone ne soient pas envoyées ou que celles-ci ne reçoivent rien de compromettant. J'ai pu voyager en toute sécurité et sereinement.

Il y a aussi une borne de décontamination ou un blanchisseur KUB Cleaner (figure 10), qui permet de "contrôler" les clés USB et disques amovibles pour offrir une protection optimale et complète contre les cybermenaces USB. Il va analyser si le support de stockage amovible est infecté. Dans le cas où le support est corrompu, le KUB propose un nettoyage. Par la suite, le disque reçoit une certification KUB. Tous les supports doivent passer par là avant d'être utilisé sur un appareil de l'entreprise.

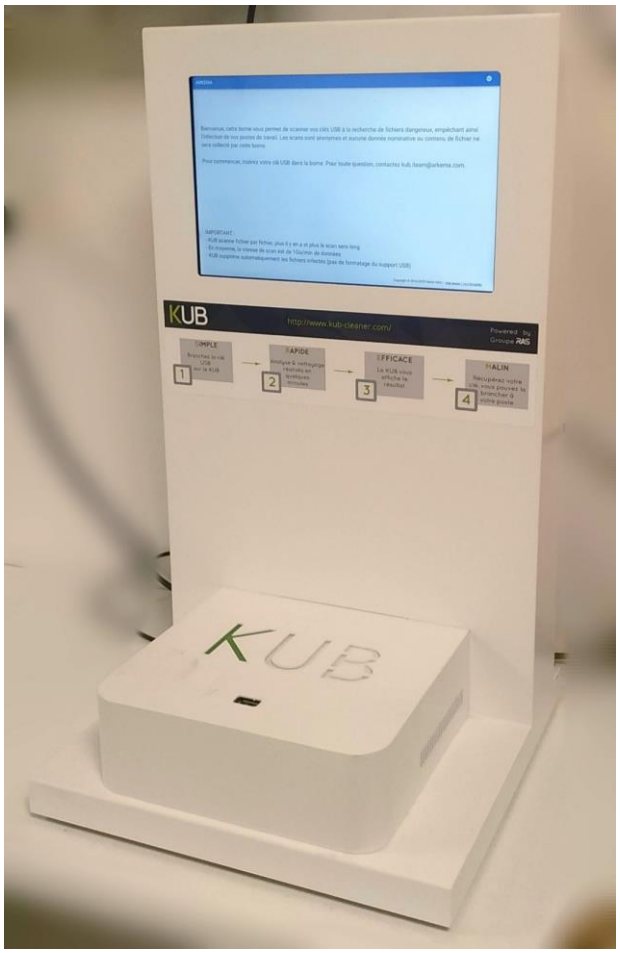


Figure 10 : Blanchisseur KUB Cleaner

J'ai pu tester le blanchisseur avec mes clés USB personnelles. L'une d'elles étaient contaminées et grâce à elle, on a pu voir qu'un des anti-virus était périmé. Par conséquent j'ai contacté les responsables des équipements KUB pour qu'ils fassent une mise à jour. En plus d'avoir fait cette mise à jour, ils m'ont informé qu'ils avaient détecté une clé infectée (la mienne). En effet, ils ont accès aux informations du KUB, qui ne garde pas les données de la clé mais connait chaque clé qui y passe.
Ma clé est désormais nettoyée mais il fallait que je cherche la source de l'infection.

J'ai réalisé la reconfiguration réseau du KUB pour le connecter à un nouveau proxy. Celle-ci se fait en 3 étapes grâce aux fichiers déjà mis en place par les gérants du KUB. D'abord on désassocie le blanchisseur du serveur. Ensuite on configure le réseau et pour terminer on associe le KUB au nouveau serveur. Chaque fichier appartient à une étape. Dans une clé vierge, on va déposer le premier fichier. La clé est ensuite insérée dans le blanchisseur et on appuie sur le nom du fichier qui s'affiche sur le KUB. Une fois celui-ci redémarré, on supprime me fichier et fait les mêmes opérations pour les 2 autres fichiers. Il faut s'assurer que toutes les étapes ont bien été réalisé, surtout la deuxième car c'est la plus importante.

3.1.3 KeePass

L'une de mes missions consistait à trouver une solution pour gérer les mots de passe des équipements du service de façon sécurisée, mais que tous les membres du service y aient accès. Pour cela j'ai été mise en relation avec plusieurs services Arkema qui ne se trouve pas forcément à l'usine. Premièrement j'ai contacté le service WORKSTATION ou bureautique. D'après eux, le fait de partager

tous les mots de passe n'est pas très sécurisé donc on m'a proposé de faire un fichier Excel partagé. Malheureusement cette solution ne me semblait pas du tout confidentiel. Par conséquent j'ai contacté la personne qui m'a répondu pour le KUB. Enfaite il s'agit d'un "Expert leader cybersécurité industrielle". Sa réponse correspondait bien plus aux attentes du service. Il est possible de stocker les fichiers confidentiels grâce à KeePass, un logiciel que le service Informatique Industrielle utilise déjà pour gérer ses mots de passe.

Cette procédure m'a fait penser à un des travaux pratiques que nous avons faits au sein de notre Institut, celui de la cryptographie. Nous avons Vincent, le propriétaire d'un fichier, qui souhaite l'envoyer à Sylvie. Le fichier a besoin d'une authentification pour des questions de sécurité. En effet Vincent a crypté son fichier à l'aide de sa clé privée. La destinatrice doit posséder la clé publique de Vincent pour pouvoir décrypter le fichier. De ce fait le document pourra être lu par Sylvie en sécurité.

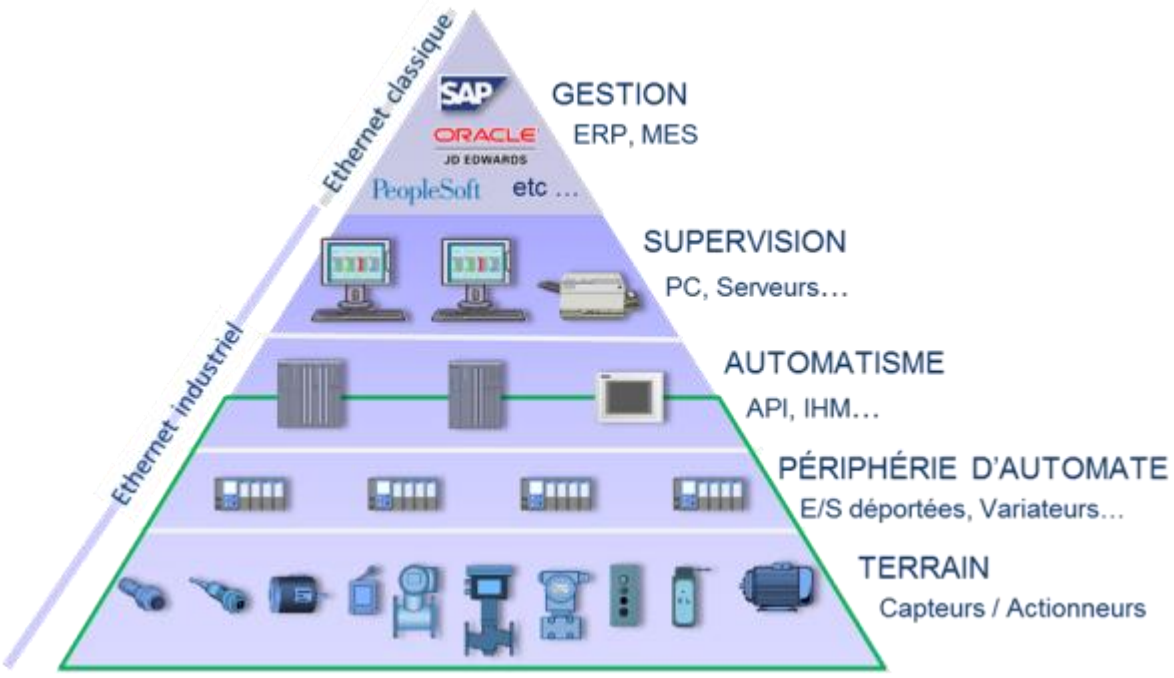
C'est la même procédure avec KeePass : chaque membre a accès à ses propres fichiers et mots de passe et peut se partager des fichiers grâce à une clé partagée. Le propriétaire partage la clé à tout le service. Si l'un d'eux quitte ce service, alors le propriétaire récupèrera la clé avant que celui-ci parte.

3.2 Informatique Industrielle

L'informatique industrielle comporte plusieurs équipements. Il y a :

- Les capteurs et les actionneurs qui sont sur le terrain
- Les automates programmables qui vont exécuter nos programmes de manière répétés,
- Les systèmes de supervision : j'ai programmé dans un contrôleur qui se trouve à l'intérieur du SNCC,
- Les gestionnaires qui servent à stocker nos données.

Tous ce matériel peut traiter en temps réel les informations issues d'un grand nombre de capteurs et assurer la commande de multiples actionneurs.



J'ai eu des projets qui concerne l'Informatique Industrielle ce qui m'a permis de mieux comprendre le fonctionnement des équipements dans l'usine et la fabrique même. J'ai utilisé différents langages de programmation comme les schémas logiques, les organigrammes, le ladder ou les textes structurés (ST).
J'ai eu plusieurs exercices de ce type pour comprendre comment fonctionne les différents blocs mais aussi pour avoir un esprit de logique. Malheureusement je n'ai pas une le temps de tous les faire.

3.2.1 Les automates et les contrôleurs

Un automate (figure 11) est un appareil qui va exécuter un programme en boucle de façon autonome. Il comporte une carte d'alimentation pour l'alimenter, un processeur où nous allons intégrer notre programme, et des racks de cartes auxquels on connecte les entrées : les capteurs ou les interrupteurs ; et les sorties qu'on appelle aussi les actionneurs : une pompe, un moteur, les vannes TOR (Tout Ou Rien) ou ANA (Analogique) 4-20mA. Les cartes peuvent s'étendre. Un contrôle est composé de la même façon qu'un automate.

Figure 11 : Un automate Schneider TSX 7

Il existe plusieurs types d'automates et de contrôleurs dans l'usine.

Nous avons le contrôleur "normal" qui va s'assurer de la disponibilité des cartes. Par exemple, une carte tombe en panne, par conséquent l'automate va en utiliser une autre.
Ensuite Il y a le contrôleur SIS qui va garantir la bonne exécution de son fonctionnement jusqu'à l'entrée-sortie grâce aux autotests. Celui-ci est capable d'exécuter une solution de repli sur défaillance interne. Il est utilisé pour la gestion des sécurités.

Il existe aussi des API, Automate Programmable Industriel et des APS, Automate Programmable Sécurité qui ont, respectivement, exactement le même rôle que les contrôleurs normaux et les contrôleurs SIS.

Ce qui diffère les contrôleurs des automates c'est que les contrôleurs sont dans un SNCC alors que les automates ne sont pas reconnus par le système. Par

conséquent ils ont besoins d'un Modbus, c'est un protocole destiné à permettre une communication simple, fiable et rapide entre les dispositifs d'automatisation et le SNCC.

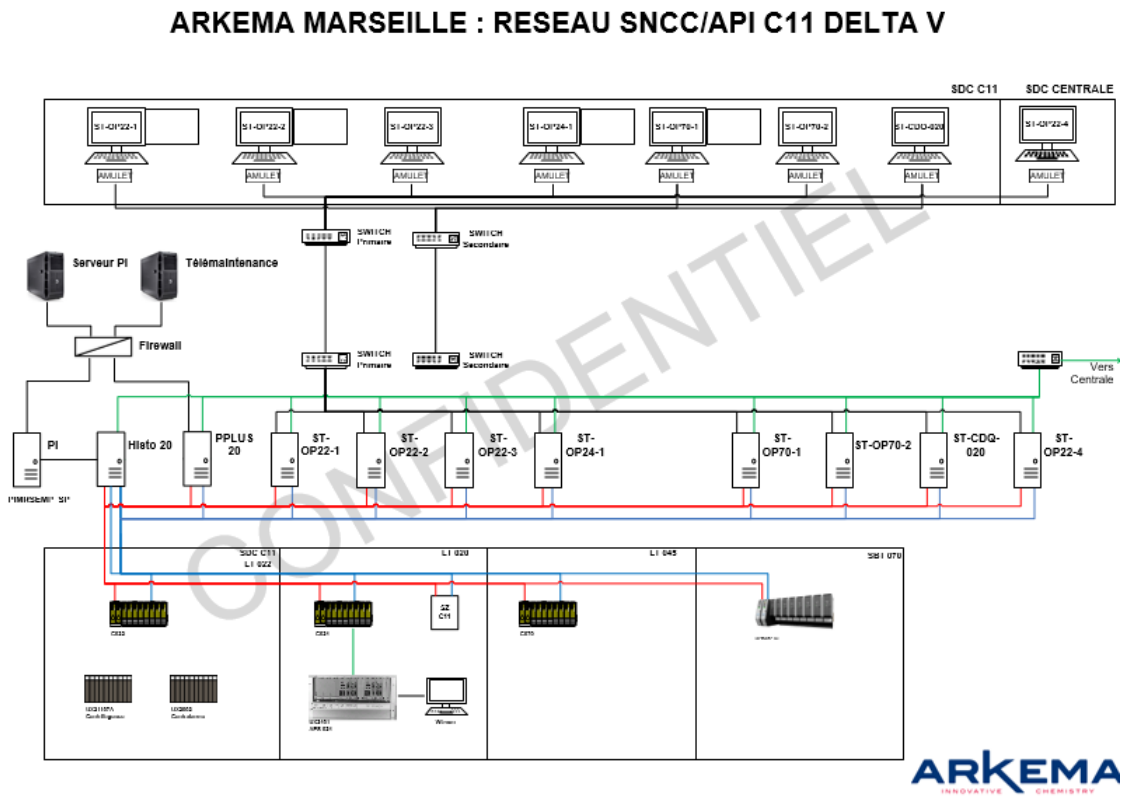


Figure 12 : Architecture du réseau informatique de Emerson

3.2.2 Programmation

À la suite de l'installation d'une nouvelle pompe lors du Grand Arrêt, j'ai eu pour projet de programmer le fonctionnement d'une pompe par rapport à son asservissement, le débit. L'arrêt de la pompe est asservi à un débitmètre, il détecte le passage du fluide. Si le débit est au-dessus du seuil minimum la pompe peut fonctionner. La pompe est entrainée par un moteur électrique.

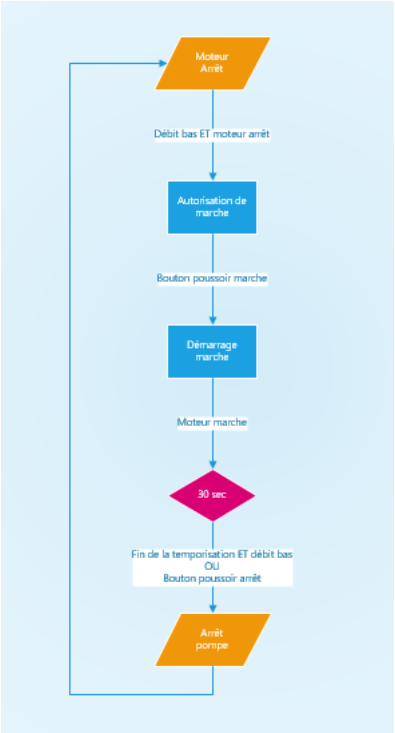


Figure 13 : Diagramme de contexte

J'ai programmé pour un contrôleur « normal » grâce un système SNCC du fournisseur Emerson : le Delta V. Avant de coder sur le delta V, j'ai fait un diagramme pour mieux visualiser le projet. Ensuite j'ai transcrit le diagramme en langage Ladder. Ça m'a permis de voir les différents langages de programmation qu'on utilise dans le service.

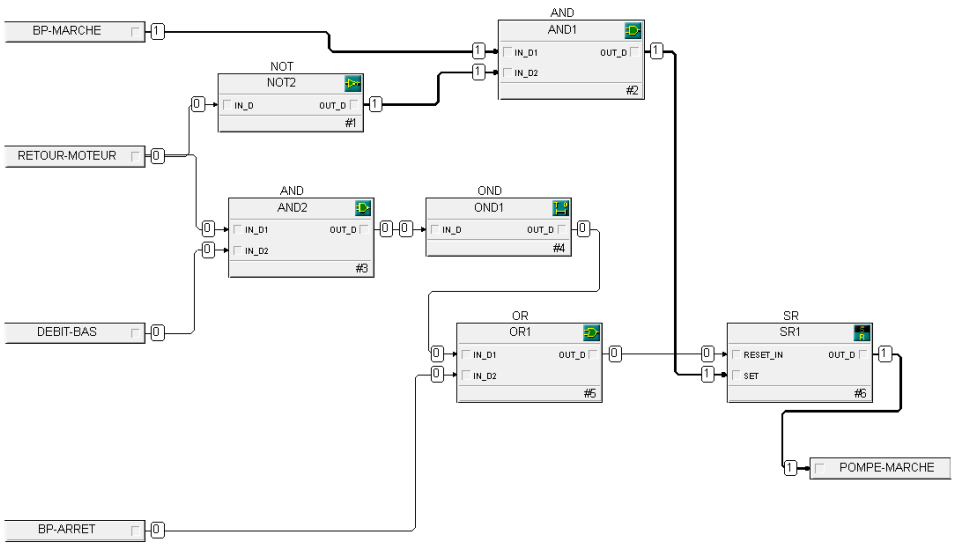


Figure 14 : Programmation par bloc de l'asservissement d'une pompe

D'abord on appuie sur le bouton « Marche ». Notre le moteur démarre, notre sortie est à 1. Or le débit est bas, l'entrée du capteur de débit est à 0. Nous devons mettre en place un by-pass de démarrage pour maintenir la pompe en marche. On utilise une temporisation. À la fin de cette temporisation si notre débit est toujours bas alors la pompe s'arrêtera sinon le moteur reste en marche. La pompe peut aussi s'arrêter si le bouton « Arrêt » est appuyé.

Le bloc OND1 (figure 14) est une temporisation on-delay, cela signifie que le bloc va comptait le temps que nous avons défini avant de s'actionner. On dit que la

temporisation déclenche un retard au démarrage. Effectivement, lorsque j'ai programmé, j'ai découvert qu'il y avait différentes temporisations : la temporisation on-delay et off-delay.

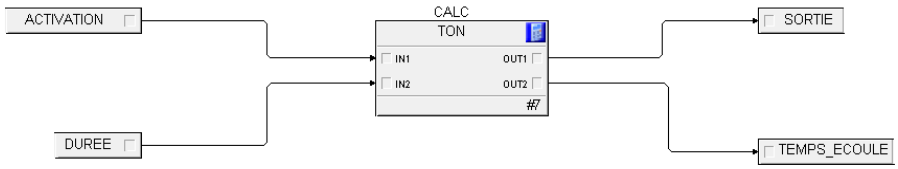


Figure 15 : Programmation par bloc de la temporisation

Expression:

```
1  IF 'IN1' = TRUE THEN
2      IF 'OUT1' = FALSE THEN
3          'OUT2' := 'OUT2' + 1;
4      END_IF;
5
6      IF 'OUT2' >= 'IN2' THEN
7          'OUT1' := TRUE;
8      END_IF;
9  ELSE
10     'OUT1' := FALSE;
11     'OUT2' := 0;
12 END_IF;
13
```

Figure 16 : Programme en ST de la temporisation On-delay

J'ai donc codé les deux pour mieux faire la différence. Le code (figure 16) représente une temporisation on-delay. On appuie sur le bouton et parallèlement, le temps sera compté. Dès que le temps aura la même valeur que le temps défini, la sortie sera activée. Il est possible que le temps ne s'écoule pas jusqu'à la fin car le bouton d'activation a été désactivé avant. Par conséquent, le bouton de sortie ne s'allumera pas et le compte se réinitialise.

Expression:

```
1  IF 'IN1' = TRUE THEN
2      'OUT1' := TRUE;
3      'OUT2' := 0;
4  ELSE
5      IF 'OUT1' = TRUE THEN
6          'OUT2' := 'OUT2' + 1;
7          IF 'OUT2' >= 'IN2' THEN
8              'OUT1' := FALSE;
9              'OUT2' := 0;
10         END_IF;
11     END_IF;
12 END_IF;
```

Figure 17 : Programme en ST de la temporisation Off-delay

La temporisation off-delay a le même fonctionnement mais inversé, c'est-à-dire qu'on appuie sur le bouton d'activation, la sortie s'activera et lorsque le bouton d'activation est désactivé, le temps s'écoule. À la fin de l'écoulement de celle-ci la sortie se désactivera. Si le temps ne s'écoule pas jusqu'à la fin car le bouton d'activation a été activé alors le bouton de sortie s'allumera et le compte se réinitialise. La temporisation déclenche un retard à l'arrêt.

Enfin, on procède aux tests du programme. Pour vérifier que notre programme de la temporisation fonctionne, nous suivons les instructions de la fiche de test que j'ai créé (figure 18).

	A	B	C	D	E
1	FICHE DE TEST				
2	temporisation on delay				
3			CONFORME	NON COFORME	
4	définition de la durée de la tempo		X		
5	activation de l'entrée		X		écoulement de la tempo
6	arrêt temps écoulé		X		activation sortie
7	désactivation entrée		X		désactivation sortie + reset tempo
8					
9	cas où l'entrée est décativée avant la fin de la tempo				
10	activation de l'entrée				écoulement de la tempo
11	désactivation de l'entrée				tempo arrêtée, sortie pas activé + reset tempo
12					
13					

Figure 18 : Fiche de test de la temporisation On-delay

Dans l'usine Les tests fonctionnels sont réalisés de la même façon. Ils sont divisés en **FAT**, Factory Acceptance Test, ce sont les tests que nous faisons dans notre espace de travail avant d'être implanter dans l'équipement ; et **SAT**, Site Acceptance Test, les tests réalisés pour s'assurer que les entrées et les actionneurs répondent correctement. Ils sont réalisés sur le site.
Il existe aussi les tests sécurités auxquelles j'ai pu assister, effectués par les opérateurs internes et externes de l'usine. Ce sont les tests qui assurent les sécurités de l'usine.

3.2.3 Mise en pratique

J'ai eu l'occasion de manipuler en atelier divers appareils utilisés sur le site pour le déroulement de l'usine. Après avoir programmé la pompe, les instrumentistes avec qui j'étais durant une partie de mon stage nous ont emmené, l'autre stagiaire et moi, dans leur atelier où ils testent les équipements. Nous avons réalisé le même circuit que mon programme mais au lieu de capter l'asservissement du débit, nous avons capté la pression.

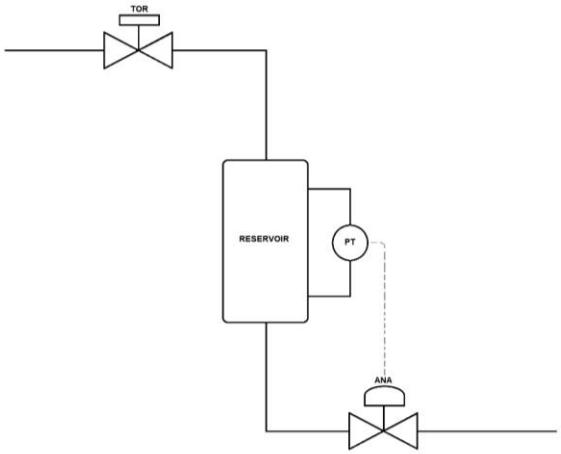


Figure 19 : Schéma du générateur de pression

Le générateur de pression émet de l'air en fonction du nombre de bar que nous voulons. L'air passe par 2 vannes : l'électrovanne représenté par une vanne TOR, Tout ou Rien ; et une vanne pneumatique symbolisé par une vanne ANA pour analogique. La différence entre ces 2 vannes est que la vanne TOR va se fermer u s'ouvrir en fonction du programme, et la vanne ANA va réguler.
Dans notre montage, l'électrovanne est connectée au relais, l'équivalent du contrôleur sur le terrain mais avec seulement 2 entrées et 2 sorties, qui va s'ouvrir au bout d'une certaine pression définit dans le relais, et la vanne pneumatique va réguler la pression.

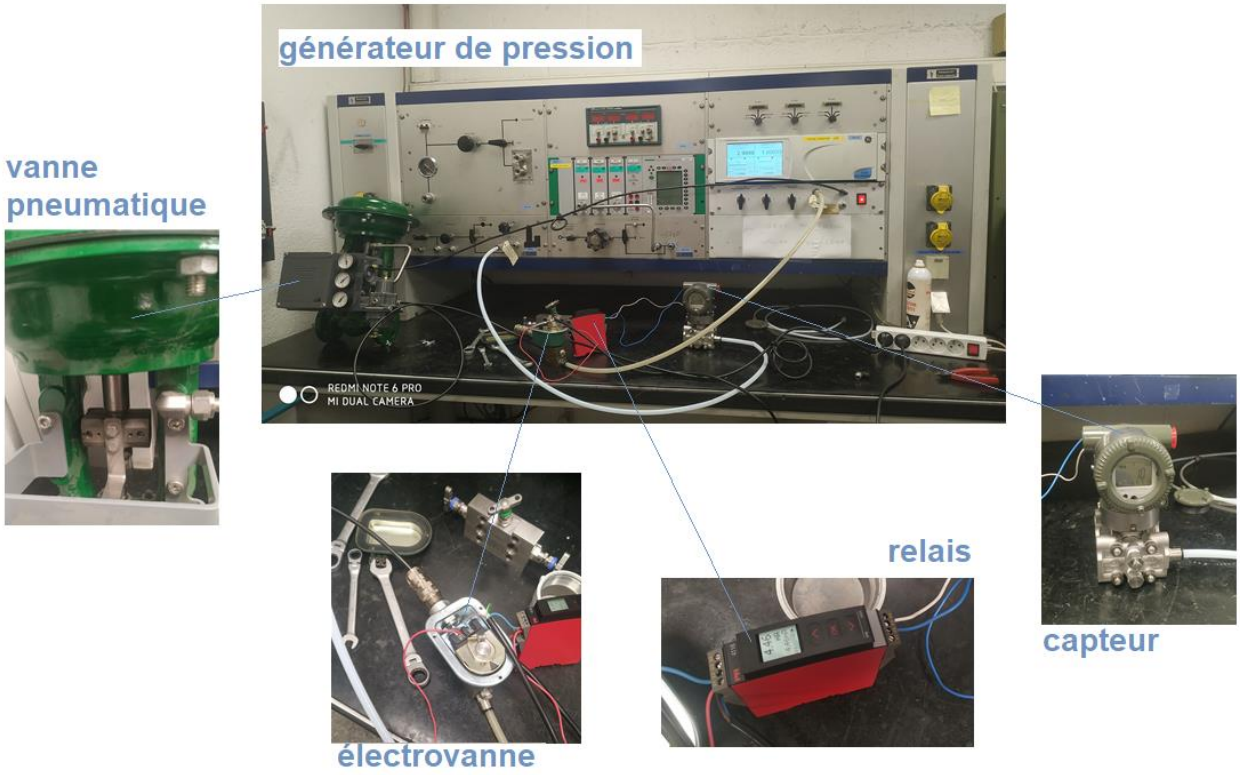


Figure 20 : Montage du générateur de pression

4 Conclusion

Pour conclure, ma participation a permis à l'usine de continuer d'avancer. J'ai contribué au fonctionnement de l'usine grâce à mes diverses missions tels que les mises à jour de l'architecture réseau effectué lors du Grand Arrêt et le procédé sur HiView qui servira aux techniciens et aux nouveaux arrivants.

Outre cela, ce stage m'a beaucoup apporté. Tout d'abord, au niveau de mes savoir-faire, j'ai une meilleure gestion de mon travail, mais aussi une meilleure organisation entre ma vie personnelle et professionnelle. De plus, j'ai développé mon autonomie : j'allais de moi-même vers les différents services pour me renseigner ou avoir de l'aide. Cela m'a permis aussi d'être plus communicative et de me sociabiliser avec toutes les personnes que je croise régulièrement.

Lors de ce stage, j'ai pu approfondir mes compétences en cybersécurité. En effet, c'est beaucoup de recherches et de documentations mais c'est aussi prévenir les personnes qui nous entourent des potentiels dangers qu'ils pourraient rencontrer. J'ai eu l'occasion d'obtenir des savoir-faire en automatisme et d'utiliser des langages de programmation que je ne connaissais pas comme le ladder ou le ST.

Le stage m'a permis d'avoir une meilleure visualisation du monde du travail, et plus particulièrement du monde industriel. En effet, au travail, il faut être sérieux mais il faut aussi s'y plaire. J'ai pu observer des personnes motivées et qui voulaient faire avancer l'entreprise mais aussi qui rigolaient, se partageaient des anecdotes, ce qui crée un bien-être au travail.

Enfin, j'ai pu avoir un éclaircissement sur mon projet avenir. Je souhaite plus m'orienter vers la cybersécurité. C'est un milieu qui devient important qui assure la protection de tous au sein de l'informatique, et qui m'a spécialement plu.

5 Remerciements

J’adresse mes plus sincères remerciements mon tuteur de stage, Georges SIMONCINI, Responsable Informatique Industrielle et RSSC-L Cybersécurité, Responsable Sécurité des Systèmes de Contrôle-Local, pour ses explications claires et précises et qui n’a pas hésité à me réexpliquer si nécessaire ceux qui m’ont permis d’approfondir mes connaissances.

Je remercie Bastien GERENTE, technicien en Informatique Industrielle, qui m’a aidé à comprendre les différentes notions en automatisme ce qui m’a permis d’avoir de nouvelles compétences.

Je souhaite remercier les Instrumentistes Alex IDER et Guillaume JEHAN, ingénieur et technicien, qui m’ont aidé à me mettre en confiance dans l’entreprise et d’avoir contribué dans mon stage.

Enfin, un grand MERCI à toute l’équipe et celles que j’ai rencontré en dehors du service de m’avoir intégré, pour leur bienveillance ainsi que pour leur disponibilité.

Je n’oublie pas de remercier ma tutrice académique, Anouch HOVSEPIAN qui s’est rendue disponible pour répondre à toutes mes questions et pour son soutien.

6 Glossaire

DeltaV, c'est le réseau qui permet d'accéder aux machines virtuelles pour commander les divers équipements chez EMERSON. ABB utilise le réseau 800xA

L'**instrumentiste industriel** définit les conditions d'intervention. Il met des capteurs sur les équipements mécaniques et automatiques permettant d'enregistrer des informations utiles et nécessaires pour la maintenance du circuit de production.

KUB, devient TYREX

Le **log** (diminutif de **logging**) est le « journal de bord » d'un système qui nous permet de stocker les évènements qui sont horodatés et ordonnés en fonction du temps. Il sera consulté en cas de besoin, par exemple pour essayer d'identifier l'origine d'une panne ou l'auteur d'une intrusion.

Monomère : composé constitué de molécules simples, et capable de former des polymères

OIV, Opérateur d'Importance Vitale.

En cybersécurité, les OIV sont des organisateurs qui permettent de minimiser les risques d'attaques sur les équipements et réseaux (infrastructures) importants et nécessaire pour le bon fonctionnement de l'entreprise. Ils doivent mettre en place des mesures de prévention, détection et réaction en cas d'évènements inhabituels en sécurité informatique. Si l'évènement s'avère être grave, les OIV préviennent le plus vite possible les personnes qui peuvent gérer le problème.
Les OIV doivent être évaluer pour tester leurs dispositifs de sécurité.

Le **service WORKSTATION**, c'est le service qui s'occupe de répondre à toutes nos questions concernant l'espace de travail Microsoft 365

SEVESO, existe depuis un accident technologique à Seveso (ville italienne) en 1978 : c'était un nuage de produits toxiques qui circulait hors de l'usine et qui contaminait les alentours.

La première directive SEVESO a été mise en place en 1982, elle permet d'identifier et de prévenir des risques d'accident. On sait que si un site est SEVESO, alors il

stocke ou produit des substances dangereuses pour l'homme et l'environnement. Arkema stocke et produit du brome, du chlore et de l'ammoniac ; des produits dangereux. Par conséquent, Arkema est classé SEVESO seuil haut, c'est à dire qu'elle a pour obligation de mettre à disposition du public, les informations des dangers et des effets pour la santé humaine et l'environnement.

En 2012, une mise à jour de SEVESO a été faite pour mieux anticiper les risques, on appelle cette nouvelle directive SEVESO3.

SNCC, Système Numérique de Contrôle Commande

En cybersécurité, les OIV sont des organisateurs qui permettent de minimiser les risques d'attaques sur les équipements et réseaux (infrastructures) importants et nécessaire pour le bon fonctionnement de l'entreprise. Ils doivent mettre en place des mesures de prévention, détection et réaction en cas d'évènements inhabituels en sécurité informatique. Si l'évènement s'avère être grave, les OIV préviennent le plus vite possible les personnes qui peuvent gérer le problème.

Les OIV doivent être évaluer pour tester leurs dispositifs de sécurité.

7 Sitographie

https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/#:~:text=La%20cybers%C3%A9curit%C3%A9%20des%20OIV%20s,rattach%C3%A9%20%C3%A0%20un%20minist%C3%A8re%20coordonnateur.

https://www.orangecyberdefense.com/fr/insights/blog/reglementation-de-la-cyber/oiv-et-pdis-tout-ce-quil-faut-savoir#:~:text=publi%C3%A9es%20en%202016.-,Quelles%20sont%20les%20obligations%20des%20OIV%20%3F,s%C3%A9curit%C3%A9%2C%20la%20protection%20des%20syst%C3%A8mes.

https://www.gironde.gouv.fr/Actions-de-l-Etat/Seveso#:~:text=Les%20%C3%A9tablissements%20class%C3%A9s%20Seveso%20seuil,sant%C3%A9%20humaine%20et%20l'environnement.

https://www.ecologie.gouv.fr/risques-technologiques-directive-seveso-et-loi-risques

https://marseille.ic.corp.local/

https://www.arkema.com/global/fr/arkema-group/profile/#

https://community.cisco.com/t5/networking-knowledge-base/how-to-configure-port-security-on-cisco-catalyst-switches-that/ta-p/3132907#toc-hId--1446074684