REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE A.MIRA-BEJAIA
FACULTE DE TECHNOLOGIE
DEPARTEMENT GENIE ELECTRIQUE

MEMOIRE

EN VUE DE L'OBTENTION DU DIPLOME DE MASTER

Domaine : Sciences et Technologies
Filière : Télécommunications
Spécialité : Système des Télécommunications

Présenté par
HASSANI FARES
TENICHE TINHINANE

Thème

Etude d'un système de supervision SCADA de l'ouvrage ROB1 SP3 M'sila terminal arrivée Bejaia (SONATRACH)

Soutenu le 10 juillet 2019

Devant le Jury

Président	**M. Aliche.A**	**UNIVERSITE DE BEJAIA**
Examinateur	**Mlle. Achour. L**	**UNIVERSITE DE BEJAIA**
Encadreurs	**M.MADDI. K**	**SONATRACH**

Année Universitaire : 2018/2019

Remerciements

***T**out travail de recherche n'est jamais totalement l'œuvre d'une seule personne, à cet effet, nous tenons à exprimer notre sincère reconnaissance et nos vifs remerciements à nos parents et tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.*

Nous remercions Dieu tout puissant de nous avoir accordé santé et courage pour pouvoir accomplir ce travail.

Et sur ce je tiens à remercié :

Mr M.TOUNSI, qui a cru en nous et a su nous guider et nous faire progresser tout au long de ce travail de recherche, nous ne pouvons que louer ses qualités humaines.

Toutes les personnes de l'entreprise SONATRACH qui a accepté de répondre à nos questions avec gentillesse et particulièrement Mr K.MADDI qui nous a beaucoup aide à la réalisation de ce travail.

Sans oublier notre collègue Mr I.MAOUCHE pour son aide précieuse.

Nos remerciements vont également aux membres du jury pour avoir accepté d'évaluer notre travail.

Merci.

Dédicace

__J__e dédie ce mémoire

__A__ mes chers parents. Qui mon encouragé à aller de l'avant et qui mon procurer touts les moyens pour réussir.

__P__our leurs patiences, leurs amours, leurs soutiens et leurs Encouragements.

__A__ mes frères. Je leur souhaite tout le succès... tout le bonheur.

__A__ tout ma famille.

__A__ ma binôme tinhinane.

__A__ mes amis et mes camarades.

__S__ans oublier tous les professeurs que ce soit du

Primaire, du moyen, du secondaire ou de l'enseignement supérieur.

Fares

Dédicace

Je dédie ce mémoire

A ma mère et mon oncle *Qui mon encouragé à aller de l'avant et qui mon procurer touts les moyens pour réussir,*

A *mon chère père qui était présent a chaque instant dans mon cœur qui ma offert une vision son cette dernière je ne serais pas arrivée la aujourd'hui*

P*our leurs patiences, leurs amours, leurs soutiens et leurs Encouragements.*

A *mes frères. Je leur souhaite tout le succès... tout le bonheur.*

A *tout ma famille.*

A mon fiancé mazigh.

A *mon binôme fares.*

A *mes amis (amel, djida et nydia) et mes camarades.*

S*ans oublier tous les professeurs que ce soit du*

Primaire, du moyen, du secondaire ou de l'enseignement supérieur.

Tinhinane

Liste des abréviations

ADR	Add-drop Multiplexer
CRC	Contrôle de redondance cyclique
DCS	Distributed control system
FMX	Brasseur multiplexeur
HEH	Haoud-El-Hamra
HP	Haut pression
HF	High frequency
HMI	L'interface Homme Machine
IP	Internet Protocol
LAN	Local Area Network
MAN	Métropolitain Area Network
MTU	Master Terminal Unit
OSI	Open Systems Interconnection
PLC	Programmable Logic Controller
PI	Proportionnelle intégrale
PID	Proportionnelle intégrale dérivés
P	Pression
RTU	Remonte Terminal Unit
RTI	Région Transport Ain-Amenas.
RTH	Région Transport Haoud El Hamra
RTO	Région Transport Ouest Arzew
SCADA	Supervisory control and data acquisition
SCR	Système contrôle en réseau
SED	Systèmes a événement discret
TRC	Région de transport centre bejaia
TMB	Terminal marin bejaia
TCP	Transmission Control Protocol
T	Température
VHF	Verry high frequency
VE	Virtual Environment
VM	Virtual Machines
WAN	Wide Area Network

SOMMAIRE

INTRODUCTION GENERALE

Introduction générale

La supervision est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. Elle concerne l'acquisition de données et des paramètres de commande des processus généralement confiés à des automates programmables.

Les systèmes de supervision permettent d'obtenir des vues synthétiques des équipements ou ensembles d'équipements afin de visualiser leurs états physiques ou fonctionnels et offrent la possibilité de déporter et de centraliser la vision et le pilotage des organes physiques (capteurs, actionneurs) parfois très éloignés.

Les systèmes SCADA (supervisory control and data acquisition) sont utilisés depuis les années 1970 et ont été adoptés à une époque où la conception du système industriel était axée sur la fonctionnalité et la fiabilité. On peut les considérer comme un système de télégestion a grande échelle reparti au niveau des mesures et des commandes des processus industriels. Ils incluent le matériel, les contrôleurs, l'interface utilisateur, le réseau de communication, la base de données et le logiciel de signalisation des entrées-sorties. Il fait essentiellement partie de la branche des technologies de l'instrumentation. Le champ d'application SCADA se reporte habituellement sur un système central de contrôle par des moniteurs et des commandes sur un emplacement complet ou un système étendu sur une longue distance.

Les domaines d'application des systèmes SCADA sont nombreux. Nous citrons entre autre le pilotage de grands installation industrielles automatisées (production et stockage agroalimentaire, production pétrolière…) ou la supervision de grands réseaux de distribution (réseau électrique, transport d'hydrocarbures, distribution Hydraulique…). Notre thème de travail et justement la supervision de l'ouvrage ROB1 M'Sila-terminal Bejaia de la société nationale SONATRACH faisant partie de l'oléoduc OB1 HAOUD EL HAMRA –BEJAIA.

Notre mémoire est organisé en quatre chapitres répartis comme suit :

Dans le premier chapitre nous présenterons brièvement les activités de la direction régionale générale de Bejaia lieu de notre stage de projet de fin d'étude.

Dans le deuxième chapitre nous présenterons les systèmes de contrôle en réseau, leurs évolutions et leurs nécessités.

Dans le troisième chapitre, nous décrirons les systèmes de supervision et de contrôle SCADA, leurs atouts, leurs architectures et leurs spécificités.

Le quatrième chapitre est consacré à une simulation d'un système SCADA dédié à la supervision de l'ouvrage ROB1 M'SILA- terminale de Bejaia a base du logiciel Tia portal V12.

Nous terminerons notre travail de mémoire par une conclusion générale suivie des références bibliographiques utilisées.

Le quatrième chapitre est consacré à une simulation d'un système SCADA en utilisant le logiciel Tia portal V12.

Nous terminons notre travail de mémoire par une conclusion générale suivie des références bibliographiques utilisées.

CHAPITRE I : Présentation de l’entreprise

I.1 Introduction [1][2]

Après l'indépendance, l'Algérie a très tôt compris que l'accès à l'énergie est une voie essentielle menant au développement économique, social et politique. C'est dans cette perspective qu'au lendemain de son indépendance, l'Algérie a créé, le 31.12.1963, la «Société nationale» de transport et de commercialisation des hydrocarbures» qui a pris comme dénomination sociale SONATRACH.

SONATRACH joue pleinement son rôle de locomotive de l'économie nationale. Elle a pour mission de valoriser les importantes réserves en hydrocarbures de l'Algérie. Cet acteur majeur de l'industrie pétrolière, surnommé la major africaine, tire sa force de sa capacité à être un groupe entièrement intégré sur toute la chaine de valeur des hydrocarbures.

SONATRACH répondait au souci d'une mobilisation des ressources de la rente pétrolière, perçue très tôt comme un élément moteur dans le développement de l'Algérie. Au fil des années, elle est devenue un puissant élément d'intégration nationale et d'envergure internationale; c'est la clé de la stabilité économique et sociale. Adoptant une stratégie d'internationalisation et de partenariat, elle opère, en effort propre ou en partenariat avec des compagnies pétrolières étrangères, en Afrique (Mali, Niger, Libye, Égypte), en Europe (Espagne, Italie, Portugal, Grande-Bretagne), en Amérique Latine (Pérou) et aux USA.

Ses gisements pétroliers en Algérie, sont parmi les plus importants du monde: Hassi Messaoud, HassiR'Mel, HassiBerkine, Ourhoud,Tin FouyéTabankort, RhourdeNouss, In Salah et In Amenas.

Ses activités à l'international connaissent un développement intense qui se caractérise par une diversification aussi bien sur le plan géographique que sur le plan des activités. Ainsi, les activités que le groupe SONATRACH développe sur le plan international sont les suivantes :

. Transport par canalisation

. Commercialisation des produits pétroliers

. Transport maritime

I.2 L'activité de Transport par canalisation (TRC) [2]

A sa création, le 31 décembre 1963, SONATRACH s'est fixée pour missions le transport et la commercialisation des hydrocarbures extraits des gisements du Sahara par les premières compagnies étrangères opérant à l'époque en Algérie. Le premier projet lancé et réalisé par SONATRACH était l'oléoduc OZ1 reliant Haoud-El-Hamra à Arzew, en 1966.

L'activité Transport par Canalisation est regroupée en divisions :

- Division Exploitation.

- Division Maintenance.

Elle est assurée par cinq régions de transport à savoir (voir la figure I.1) :

- Région Transport Ain-Amenas RTI.
- Région Transport Haoud El Hamra RTH.
- Région Transport Centre Bejaia RTC.
- Région Transport Ouest Arzew RTO.
- Région de transport Est SKIKDA RTE.

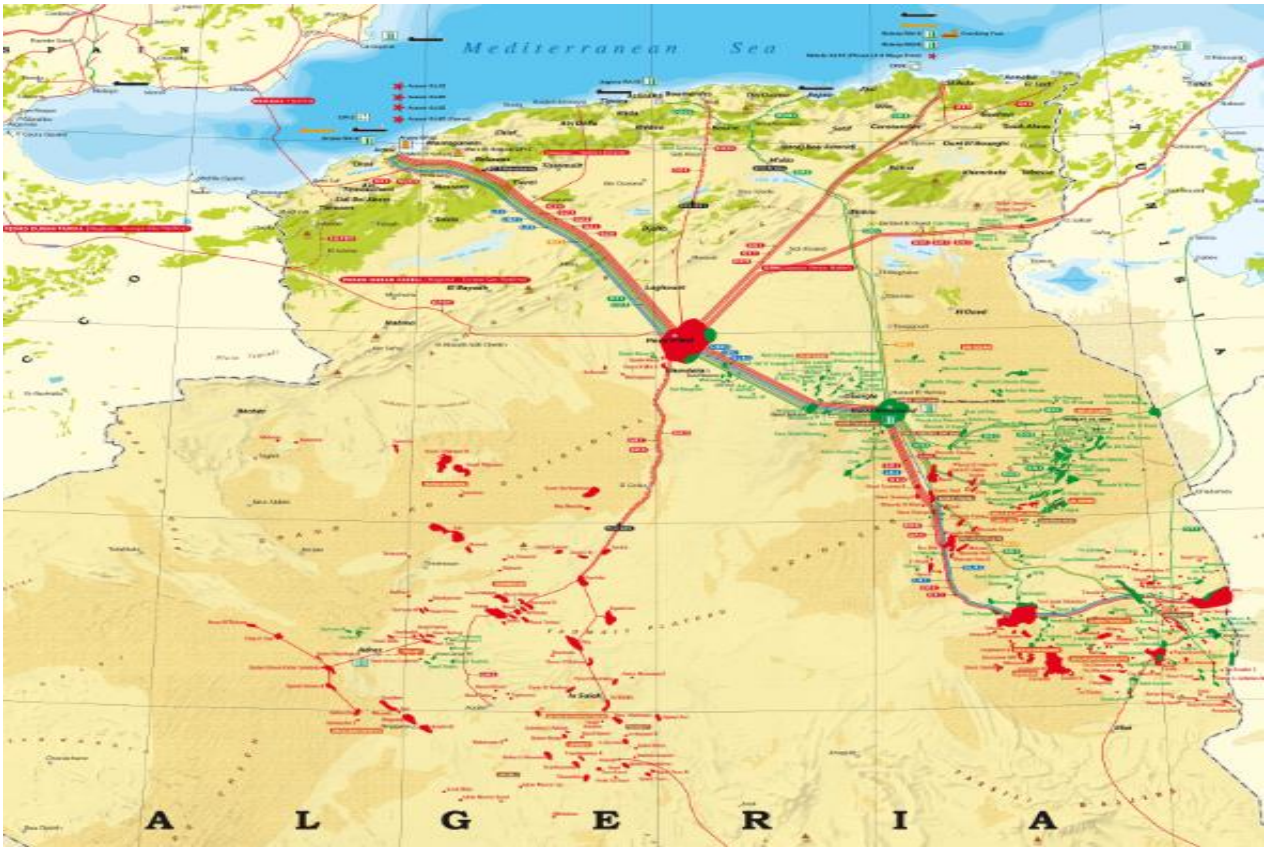


Figure I.1: *Réseau de transport par canalisations de sonatrach.*

I.3 Le réseau transport centre de SONATRACH (RTC) [2]

La Région Transport Centre Bejaïa (RTC) ou direction régionale de Bejaia (DRGB) est une des cinq directions régionales de Sonatrach qui assure le transport du pétrole brut et condensât à partir du terminal départ Haoud El Hamra jusqu'au terminal arrivée marin de Bejaïa (voir la figure I.2). Afin de l'exporter vers l'étranger, ainsi que l'approvisionnement en gaz de la région centre à partir du terminal Hassi-R'mel jusqu'au terminal Arrivée Isser.

I.3.1 Ouvrage exploités [2]

La RTC se charge de l'exploitation et la maintenance des Ouvrages suivants :

I.3.1.1 Oléoduc OB1

L'oléoduc OB1 est le premier ouvrage de transport par canalisation réalisé par la société pétrolière de gérance (SOPEG) en Algérie en 1957 par la compagnie française des pétroles CFP et société nationale de recherche et d'exploitation des pétroles en Algérie (SNREPAL), mis en service en 1959 pour relier Haoud-El-Hamra au terminal marin de Bejaia

L'oléoduc OB1 de diamètre 24 pouces a une longueur totale de 660.72Km ; reparti en deux tronçons :

- Un tronçon reliant le terminal HEH au col de selatna qui est le point le plus culminant de la ligne (1033m d'altitude) de diamètre 24 pouce et de longueur 533.17Km
- Un second tronçon reliant le col de selatna au terminal marin dont le diamètre est de 22 pouce sur une longueur de 125.551 Km où l'écoulement est gravitaire; le diamètre est réduit de 24 à 22 pouce pour qu'il y'ait une pression finale suffisante pour acheminer le pétrole brut vers les packs de stockage du terminal marin (TMB)

L'OB1 est équipé de postes de sectionnement (vanne à opercule)

A chaque crête du pipe, il y a des évents pour évacuer l'air crée en cas de faible pression, et des clapets non-retour qui permettent au fluide de s'écouler dans une seule direction.

Les stations de pompage qui sont chargées de faire circuler les fluides sous haute pression (HP) à des vitesses de l'ordre de 1 à 3m/s (3.6 à 10km /h) ; le débit étant en

fonction de la ligne. Elles sont équipées de pompes montées en série ou en parallèle, destinées à fournir la pression nécessaire pour vaincre les pertes de charge.

Les stations qui existent dans l'oléoduc OB1 sont :

- Station de pompage de Haoud-El-Hamra(HEH) SP1.
- Station de pompage de DJAMAA SP1 BIS.
- Station de pompage de Biskra SP2.
- Station de pompage de M'SILA SP3.

I.3.1.2 L'Oléoduc DOGA 16

C'est l'oléoduc alimentant la raffinerie d'Alger à partir de la station de pompage de Beni-Mansour.

I.3.1.3 Gazoduc GGA 42

C'est l'oléoduc alimentant en gaz la région centre.

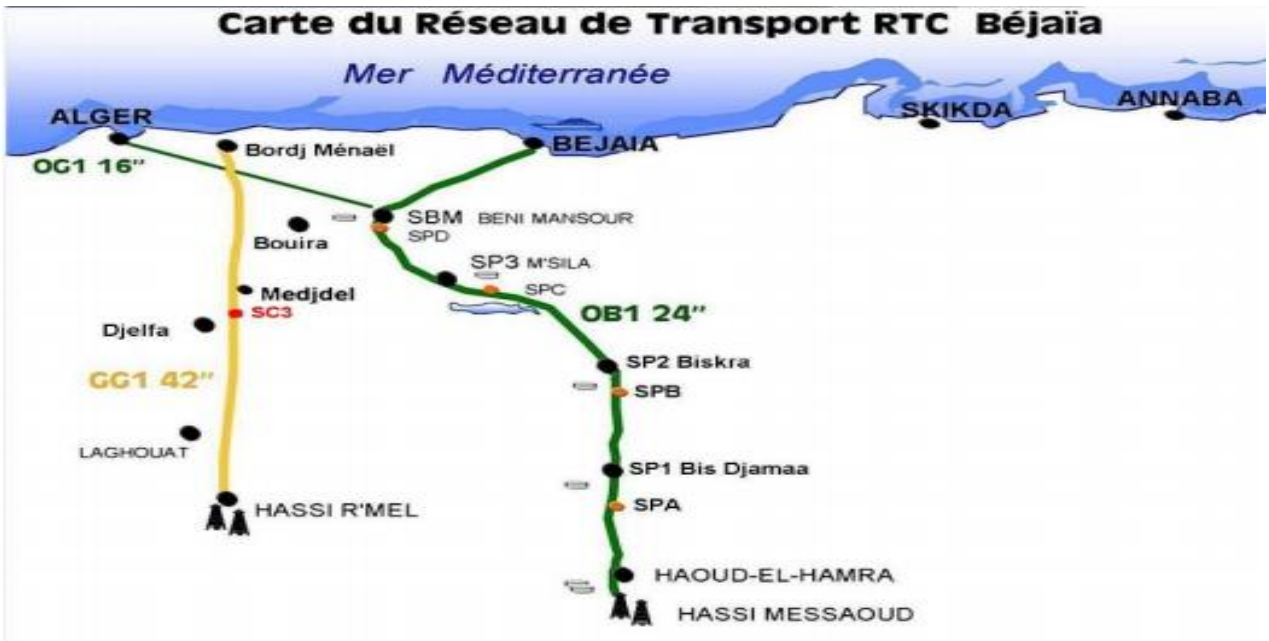


Figure I.2: *Réseau de transport RTC Bejaia.*

I.4 La direction régionale de Bejaia (DRGB) [3]

La direction régionale de Bejaia (D.R.G.B) est l'une des sept directions opérationnelles composant l'activité transport par canalisation de SONATRACH avec les régions d'Arzew ,Skikda ,Houed El Hamra (H.E.H), Elle est chargée du transport, du

stockage et de la livraison des hydrocarbures (pétrole , condensat et gaz naturel), Elle est en charge d'un port pétrolier , d'un gazoduc (GGA) et deux Oléoducs (OB1 et OGA) décrits précédemment.

I.4.1 Organisation de la DRGB

Elle est organisée selon l'organigramme de la figure suivante :

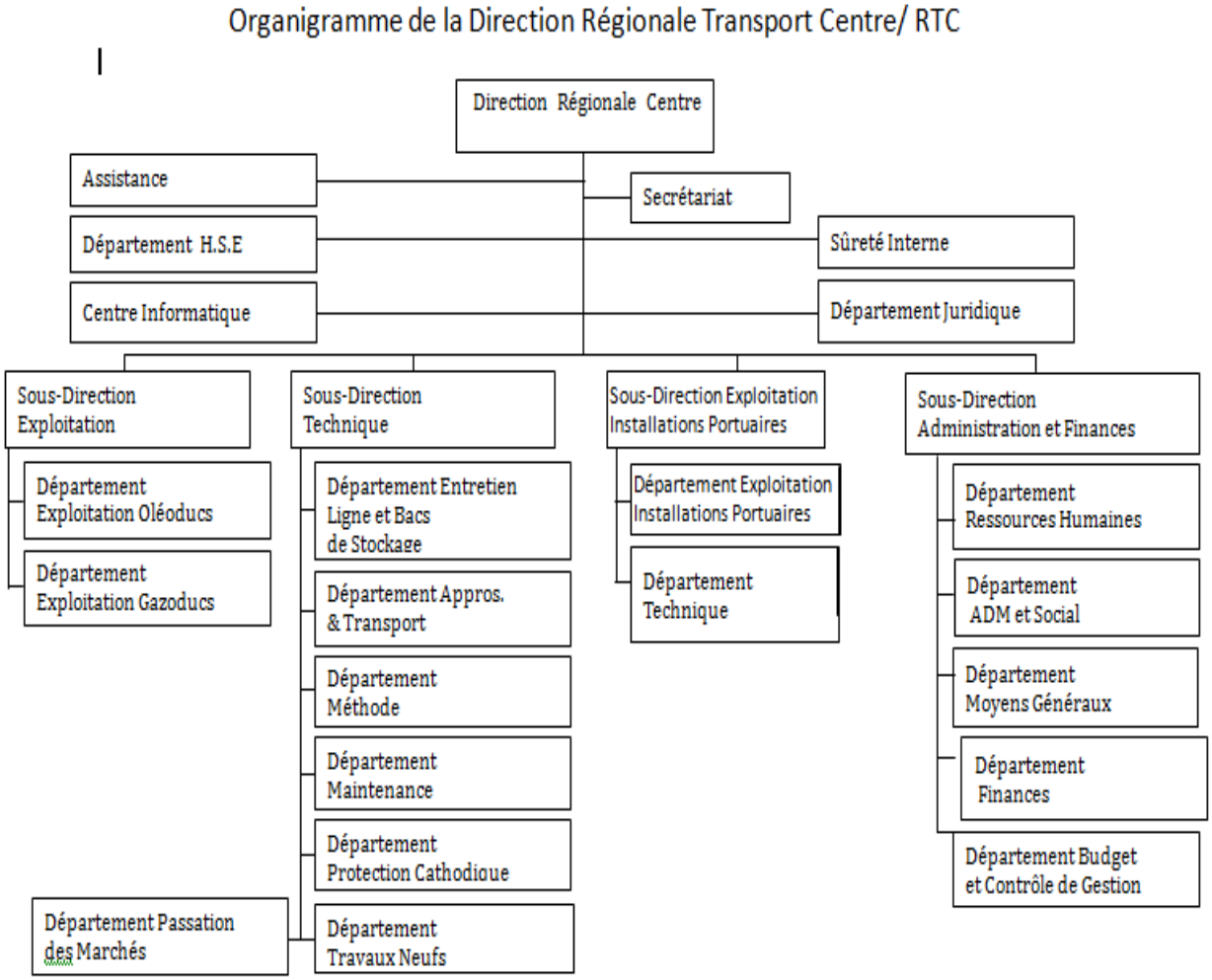


Figure I.3 : *Organigramme de la Direction Régionale Transport Centre/ RTC.*

I.4.2 Le port pétrolier [2]

Il assure le stockage et la livraison des hydrocarbures qui arrivant par l'oléoduc OB1. Il est constitué de deux terminaux.

I.4.2.1 Le terminal nord

D'une surface globale de 3 600 510 m^2, il est composé de :(voir la figure I.4)

- 12 bacs à toit flottant, d'une capacité de 35 000 m^3.

- Un bac de purge à toit fixe de 29 000 m^3 , pour récupérer les purges des collecteurs et de manifold et recevoir le produit à l'entrée de la ligne lors d'une surpression.
- Le manifold permet d'envoyer le liquide arrivant par la ligne vers un réservoir choisi, de vidanger un bac ou plusieurs vers le poste de chargement et transvaser le brut d'un bac à un autre.
- groupe électropompe (GEP) composé de 7 unités.

I.4.2.2 Le terminal sud

Occupant une superficie de 123 925 m^3, il est composé de : (voir la figure I.4)

- Quatre bacs de stockage à toit flottant, d'une capacité de 50 000 m^3 , d'un volume utile de stockage de 41 000 m^3 pour chacun, d'une hauteur de 14,65 m.
- Le manifold sud assure les mêmes manœuvres que celui du nord.
- Une pomperie de trois unités de différents débits.

Figure I.4: *Terminal arrivé Bejaia.*

I.4.3 Le département maintenance [2]

Ce département très important au sein de la DRGB, Il englobe des services d'entretien de la ligne de transport des hydrocarbures, il s'ajuste au premier plan par rapport à

l'importance de ces activités. Ce département administre la gestion des services assurés par des branches opérationnelles telles que les directions fonctionnelles qui élaborent et veillent à l'application d'une politique et d'une stratégie de groupe. Elles fournissent l'expertise et l'appui nécessaires aux activités. Il est divisé en cinq services, sa structure est représentée dans la figure suivante :

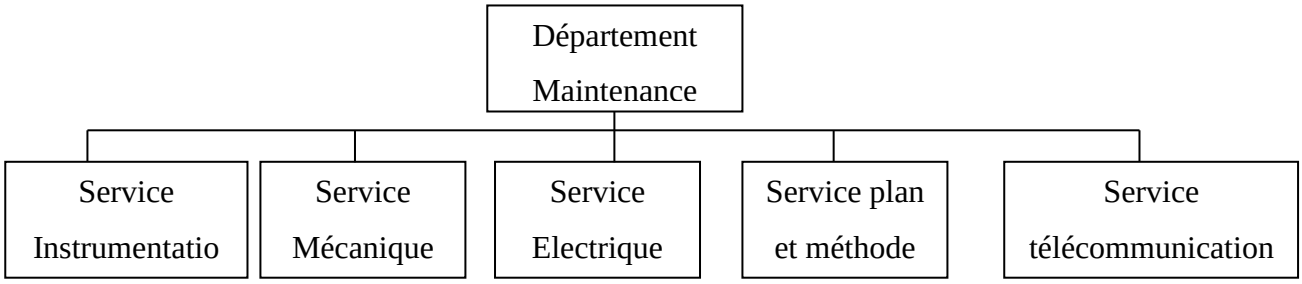


Figure I.5: *Département maintenance.*

Ci-après, nous décrivons son service télécoms :

I.4.4 Le service Télécoms [1][2]

Le service télécoms est indispensable dans l'entreprise SONATRACH, son rôle principal est d'assurer le bon fonctionnement des structures de la TRC ainsi que ses activités, il est chargé aussi d'une liaison permanente entre ses différents sièges, et entre les stations afin d'assurer le transport fiable des hydrocarbures pour accomplir ses missions avec succès, le service est doté de :

I.4.4.1 Réseau radio [1][2]

Il se compose de :

- **Un réseau HF** : C'est un réseau de secours opérant dans la bande (3-30 MHz), la portée est de plusieurs milliers kilomètres.
- **Un réseau radiocommunication VHF :** Assurant les différentes liaisons à l'intérieur de la région, un système simplex permettant de réaliser les liaisons point à point entre les différentes stations (mobiles, portables, fixe).
- **Un réseau radiocommunication UHF :** Il assure les liaisons entre les différentes stations (mobiles, portables, fixes)

I.4.4.2 Système commutation [1][2]

Comme mentionné précédemment la TRC est divisée en deux secteurs (nord, sud) et comme la téléphonie est la partie la plus importante, elle est composée d'un autocommutateur ou PABX (Private Automatic Branch exchange), d'un répartiteur, de sous répartiteur, des points de concentration (PC) et des appareils téléphoniques (postes IP, postes analogiques, DECT. La figure suivante représente l'architecture hiérarchisée en téléphonie.

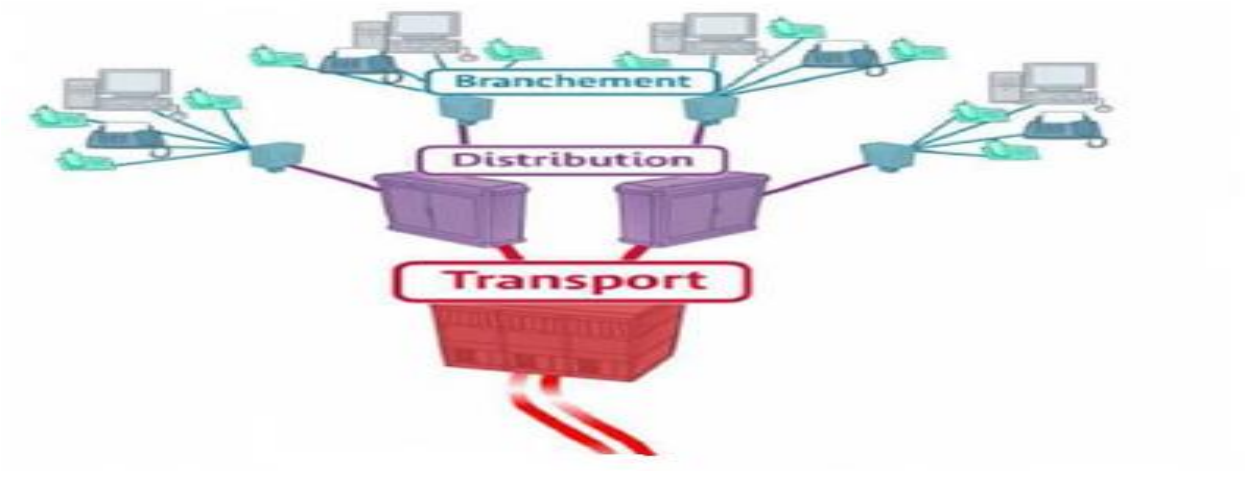


Figure I.6 : *Architecture d'un réseau tel fixe.*

I.4.4.3 Système SCADA [1][2]

C'est un système de télé-supervision, de télétransmission et télémesure, il traduit les informations transmises par la pipe sous formes de données (température, débit,...) qui sont acheminées vers le terminal arrivée ou elles sont traduites par un automate. Toutes les communications sont gérées à partir de la salle auto-com, qui contient des armoires avec des châssis faites spécialement pour installer tous les organes qui permettent de bien gérer les communications : le processeur, carte réseau interne, carte CPU, carte de signalisation(MMT), panneau de brassage (fibre optique)…etc.

I.4.4.4 La tour de contrôle [1][2]

La salle de contrôle ou salle de commende sert à contrôler et à surveiller les actions générées autour d'une entité quelconque, Elle est dotée de deux tableaux synoptiques, l'un

utilisé pour les systèmes de commande de la bouée et l'autre pour visualiser toutes les opérations de remplissage et de vidange des bacs au port pétrolier des deux terminaux.

Les opérations de contrôle sont :

- Contrôle la pression et le débit de la ligne.
- Contrôle du remplissage et la vidange des bacs avec affichage automatique.
- Commandes des vannes et des pompes.
- Contrôle de pression dans la conduite de chargement.
- Contrôle de chargement pétrolier (pétrole brute) au navire.

I.4.5 Présentation des équipements de transmission [4][5]

Le développement des applications sur internet et l'exposition du trafic qui en résulte exigent des transmissions et des équipements de réseaux de plus en plus performants. Sagem développe des solutions de transmissions et d'accès basés sur les technologies les plus performantes, la figure suivante représente l'équipement de transmission SAGEM utilisé par le service télécom.

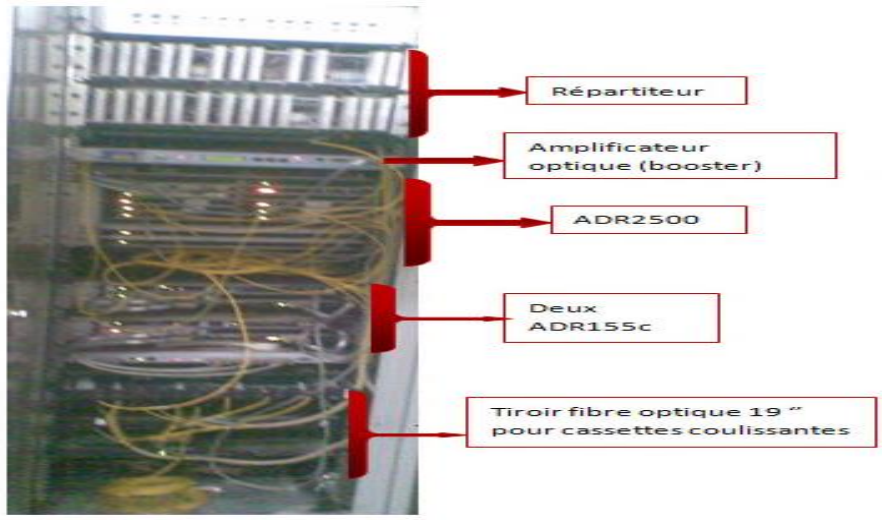


Figure I.7: *L'équipement de transmission SAGEM.*

- **L'ADR 2500c [4]**

L'ADR 2500c (add-drop Multiplexer 2500 Mbit/s Compact) est un multiplexeur add-drop optique STM-16 qui permet de construire des liaisons point à point STM16 (liaisons optique de la (DRGB), des anneaux STM16 ou des réseaux maillés. Réalisant ainsi le

transport de liaisons STM-1, STM4, STM16, pour ce dernier, il autorise des sections de régénération jusqu'à 60Km pour 1.33nm et 100Km pour 1.55nm ; s'il est associé à un amplificateur optique il peut atteindre 150Km.

- **L'ADR 155C [5]**

C'est un multiplexeur Add-drop optique STM1, il permet de construire des liaisons :

-Point à point.

-Des anneaux STM1.

-Réseaux maillés.

Avec protection des conduits (SNC) et des lignes (MSP), l'ADR155 réalise le transport de liaisons (2Mb/s, 34Mb/s, 45Mb/s, Ethernet et STM1).

- **FMX P4.3B**

Brasseur multiplexeur de circuits à 64kb/s et n × 64kb/s, il offre une grande variété d'interfaces normalisées et permet de raccorder de nombreux terminaux au réseau public ou privé, et s'adapte facilement au changement de configuration réseau.

I.5 L'objectif de notre travail

Notre travail consiste à l'étude et la proposition d'une architecture d'un système de supervision SCADA de l'ouvrage ROB1 SP3 M'Sila-terminale arrivée Bejaia de SONATRECH.

La supervision vise l'acquisition de données de mesures et la sécurité du transport des fluides hydrocarbures tout le long de l'ouvrage suscité.

I.6 Conclusion

Dans ce chapitre, nous avons situé et décrit les missions de la direction régionale centre de SONATRACH (DRG Bejaia).

Nous avons aussi présenté les activités de son département de maintenance et plus précisément son service télécoms.

CHAPITRE II : Les Systèmes de contrôle en réseau

II.1 Introduction [6]

Le système de contrôle repose sur des mesures qui permettent d'évaluer les progrès réalisés afin de les comparer aux standards prédéterminés. L'analyse des écarts par rapport aux prévisions indique s'il y a lieu d'effectuer des corrections au niveau des opérations de base. C'est un processus nécessaire pour assurer le bon fonctionnement de l'organisation.

Un système contrôle en réseau (SCR) (ou networked control Systems dans la littérature anglophone) correspond simplement à un système de contrôle/commande distribué via un réseau pouvant être partagé avec d'autres applications non impliquées dans la commande du système. Le contrôle peut être discret ou analogique, manuellement ou automatiquement, périodique ou continu.

II.2 Notion de contrôle de systèmes [6]

II.2.1 Boucles de régulation

une boucle de régulation est un dispositif constitué d'un ou de plusieurs capteurs mesurant une grandeur physique à contrôler, fournissant ainsi les données nécessaires au système de commande d'une machine ou d'un processus dont l'état est susceptible de modifier cette grandeur L'action correctrice s'effectue après que les effets des grandeurs perturbatrices aient produit un écart entre la mesure et la consigne. Cet écart peut être également provoqué par un changement de consigne. Dans les deux cas, le rôle de la boucle fermée est d'annuler l'écart. Tout ce si ce résume par la figure qui suit :

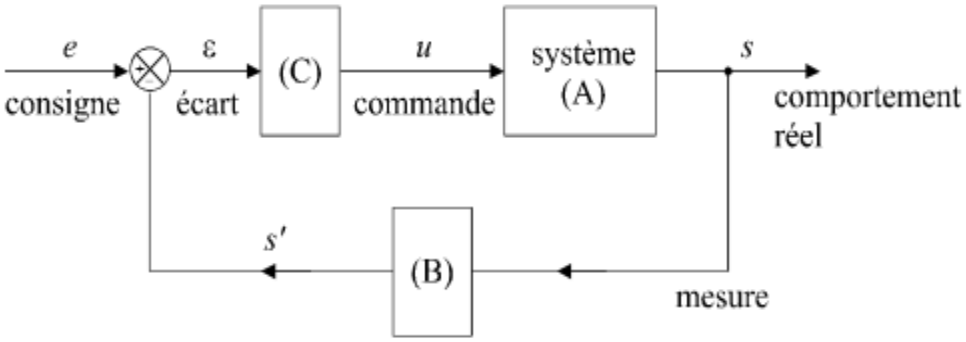


Figure II.1: *Schéma général d'une boucle de régulation*

II.2.2 Le contrôle discret [6]

Le contrôle discret peut fonctionner qu'avec les systèmes dans lesquels chaque élément ne peut être que dans certains états définis. Un exemple de contrôle discret est de démarrer un ventilateur lorsque la température dépasse une valeur prédéterminée et l'arrêt du ventilateur lorsque la température tombe au-dessous d'une valeur prédéfinie. La température (variable de processus) est soit dans l'intervalle acceptable, soit non. Le relais de commande du ventilateur (actionneur) est allumé ou éteint. Ce type de contrôle est mis en œuvre avec des diagrammes et des circuits logiques. En contrôle discret, même si certains paramètres sont enfaite une gamme continue de valeurs, la seule information utilisée par le système de commande est de savoir si leur valeur est supérieure, inférieure ou égale à une certaine valeur désirée. Un schéma de principe d'un système de contrôle discret simple est illustre dans la Figure suivant :

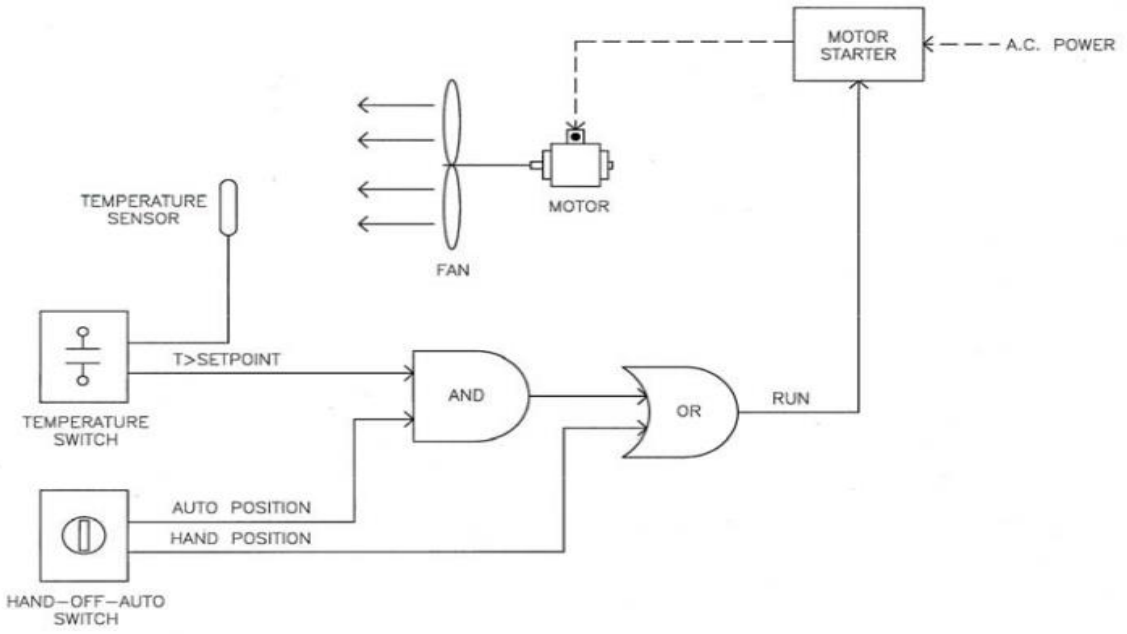


Figure II.2: *Diagramme d'un &système de contrôle discret.*

II.2.3 Contrôle analogique [6]

Le contrôle analogique fonctionne avec les systèmes analogiques à variables continues. Il consiste en la mesure la variable de processus et la comparer à la valeur désirée. Et d'agir selon leur écart par les actionneurs (consigne). Ce processus peut être aussi simple que le conducteur d'un véhicule comparant la vitesse de son véhicule (paramètre) à la limite de vitesse (consigne) et le réglage de la position de la pédale d'accélérateur (action de contrôle) pour accélérer ou ralentir le véhicule en conséquence.

Dans la plupart des systèmes qui nous intéressent, ce type d'action de contrôle est effectué automatiquement par des processeurs électroniques, qui reçoivent des signaux depuis les capteurs, les traitent et envient des signaux aux actionneurs tels que les pompes, les vannes, les moteurs, ou d'autres dispositifs pour effectuer l'action contrôle. La figure suivant représente un schéma synoptique d'un système de base de commande analogique.

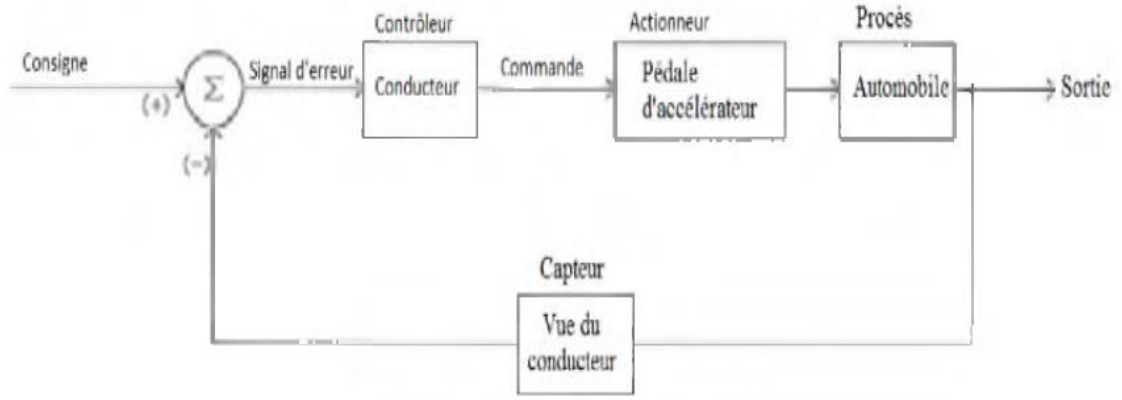


Figure II.3: *Schéma fonctionnel du système de contrôle analogique.*

II.2.4 Classe de contrôleurs analogiques

Contrôleurs analogiques peuvent être classés par la relation entre leur signal d'erreur d'entrée et l'action de contrôle qu'ils produisent

II.2.4.1 Le contrôleur Proportionnel (P) [8]

Dans le cas d'un contrôle proportionnel, l'erreur est virtuellement amplifiée d'un certain gain constant qu'il conviendra de déterminer en fonction du système

$$\text{Consigne}(t) = Kp\ \varepsilon(t)$$

Ce qui en Laplace donne :

$$Consign(p) = Kp\ \varepsilon(p)$$

Kp : effet de l'erreur

$\varepsilon(t)$: écart type

Ils produisent une sortie qui est directement proportionnelle au signal d'erreur, telle que le signal d'erreur doit toujours être différent de zéro pour produire une action de commande .Par conséquent, le contrôle proportionnel seul ne peut pas retourner le processus à la consigne suite à une perturbation extérieure.

II.2.4.2 Le contrôleur proportionnel intégral (PI)

Au contrôle proportionnel, nous pouvons ajouter l'intégration de l'erreur. Dans ce cas nous obtenons une régulation PI (proportionnelle et intégral), Ils produisent une action de

commande qui est proportionnelle au signal d'erreur et proportionnel à l'intégrale du signal d'erreur. L'action intégrale répète l'effet de l'action proportionnelle, jusqu'à ce que l'écart entre la mesure et la consigne soit nul. Le contrôle PI peut amener à un dépassement de la consigne, ce qui n'est pas toujours très souhaitable.

II.2.4.3 Les contrôleurs proportionnelle intégrale dérivés (PID)

Le PID (proportionnel intégral dérivé) est le contrôleur standard le plus utilisé dans l'industrie. Il permet une régulation optimale en associant les avantages de chaque action : la composante P réagit à l'apparition d'un écart de réglage, la composante D s'oppose aux variations de la grandeur réglée et stabilise la boucle de régulation ; et la composante I élimine l'erreur statique.

II.3 Les systèmes de contrôle industriels [6] [9]

Le contrôle peut être réalisé en utilisant soit des contrôleurs individuels autonomes, appelés contrôleurs à boucle unique, ou en combinant plusieurs boucles de régulation dans un contrôleur plus grand, Les contrôleurs à boucle unique ne sont généralement pas utilisés dans les systèmes complexes comme les systèmes SCADA ou DCS.... qui sont caractérisé par la capacité de contrôle à la fois discret et analogique, les interfaces homme-machine avancées (IHM), et la capacité de communiquer en réseau.

II.3.1 Les contrôleurs distribuées

Il existe plusieurs systèmes de contrôleurs distribuées pour les quelles, nous citrons :

II.3.1.1 Les systèmes SCADA

Ce sont des systèmes hautement distribués utilisés pour contrôler des actifs géographiquement dispersés, souvent dispersés sur des milliers de kilomètres carrés, où l'acquisition et le contrôle centralisés des données sont essentiels, au fonctionnement du système.

Ils sont utilisés dans les systèmes de distribution tels que la distribution d'eau les systèmes de collecte, les oléoducs et les gazoducs, les réseaux électriques et les systèmes de transport ferroviaire.

Le centre de contrôle SCADA effectue une surveillance et un contrôle centralisés sur les sites, y compris la surveillance des alarmes et le traitement des données d'état. Basé sur l'information reçue de stations distantes, les commandes de supervision automatisées ou gérées par l'opérateur peuvent être poussées vers des dispositifs de commande de station

distante, souvent appelés appareils de terrain. Les appareils de terrain contrôlent local opérations locales telles que l'ouverture et la fermeture de vannes, de disjoncteurs, la collecte de données à partir de systèmes de capteurs, et surveillance de l'environnement local pour les conditions d'alarme.

II.3.1.2 Les DCS (Distributed Control System)

Les systèmes de contrôle distribués sont utilisés pour contrôler des processus industriels tels que la production d'énergie électrique, les raffineries de pétrole et de gaz, le traitement de l'eau, et les productions, chimique, alimentaire et automobile. Les DCS sont intégrés en tant qu'architecture de contrôle contenant un niveau de contrôle supervisant plusieurs sous-systèmes intégrés chargés de contrôler les détails d'un processus localisé.

II.3.2 Les Automates programmable industriel (API ou PLC) [6] [10]

Un automate programmable industriel (API) (ou PLC programmable logic controller) constitue un composant fondamental d'un système de contrôle industrielle est destiné à réagir et à communiquer en temps réel avec son environnement. Un tel contrôleur est à base de microprocesseurs d'usage universel qui fournissent la logique de commande, synchronisation, avec des possibilités de communications en réseau

Les API sont recommandées pour les raisons suivantes :

- Ils ont été développés pour des plateformes industrielles vu leur fiabilité, et la et leur tolérances élevées pour la chaleur, la vibration, et l'interférence électromagnétique.
- leur extension est facilitée par la disponibilité de pièces de services de programmation et de support technique
- ils fournissent le traitement à grande vitesse ce qui est important dans divers applications temps réel
- ils soutiennent des configurations de secours immédiat pour des applications élevées de fiabilité.

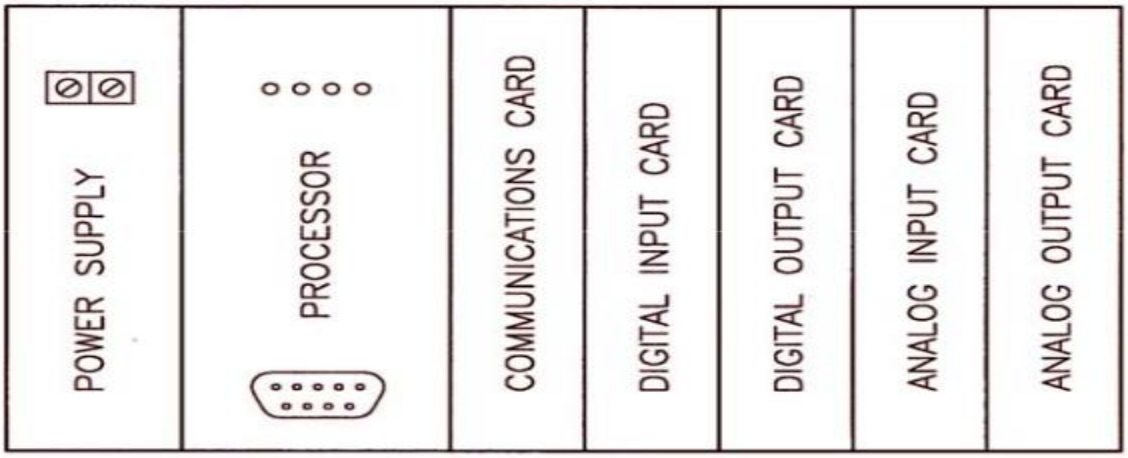


***Figure II.4**: Schéma général D'un API.*

II.3.3 API 1164

Il s'agit d'une norme volontaire de l'industrie spécifique au contrôle de surveillance et à l'acquisition de données (SCADA) pour le secteur des oléoducs. La norme fournit les meilleures pratiques de sécurité pour guider les exploitants de pipelines de liquides dans l'évaluation des risques, la conception de systèmes, ainsi que dans l'établissement et la révision des politiques de la société.

L'API 1164 traite du contrôle d'accès, de la sécurité des communications, de la classification de la distribution des informations, des problèmes physiques, (y compris des plans de continuité et de reprise d'activité), des systèmes d'exploitation, de la conception de réseaux, de l'échange de données entre les clients et les clients tiers, des systèmes de gestion et de la configuration d'accès, Cette norme et beaucoup utilisé en industrie notamment a Sonatrach

II.4 Systèmes de commande en réseau [11] [12]

Les Systèmes de Commande en Réseau notés NCS (Network Control Systems) sont des systèmes automatiques (ou automatisés) dans lesquels les actionneurs, les capteurs et les organes de contrôle / commande, communiquent (émission et réception de données) à travers un réseau .ce dernier permet aux équipements du système d'échanger les données informations en respectant des protocoles de communication bien prédéfinis, améliore la modularité, et rend l'architecture plus flexible. Et échangent des, Par ailleurs, l'insertion du réseau dans la boucle de contrôle introduit des effets tels que les délais, les pertes de paquets et la prise en compte de la charge du réseau

II.5 Evolution des systèmes de commande en réseau [11]

L'évolution d'un système de commende en réseau est illustrée par la figure suivant :

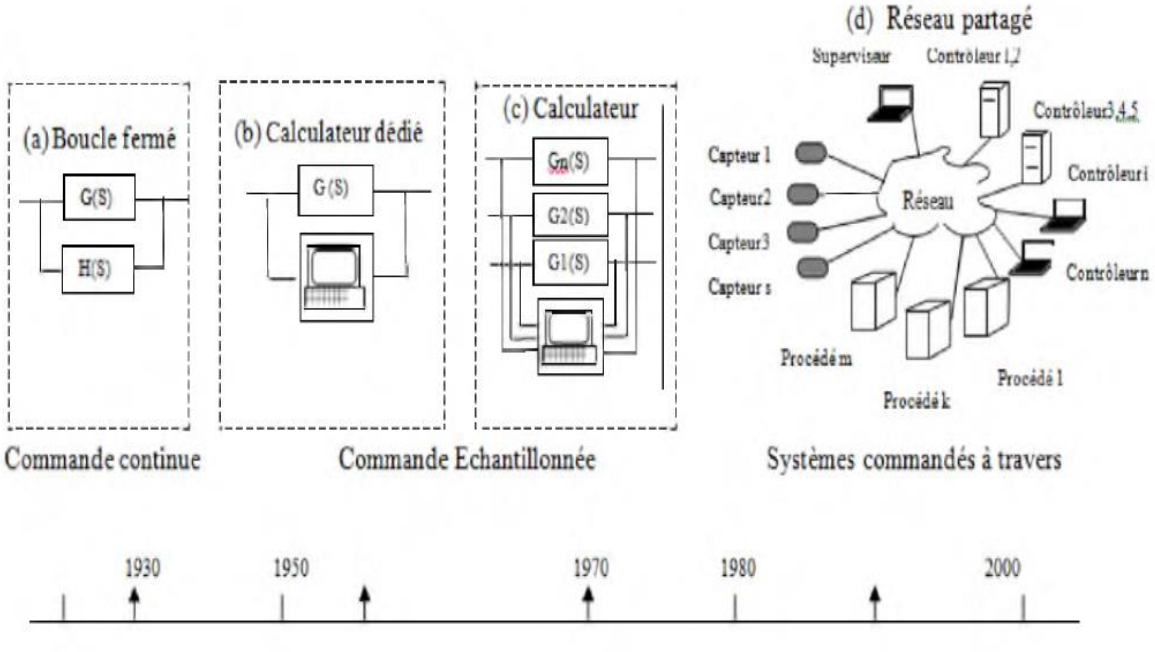


Figure II.5: *Chronologie de l'évolution des systèmes de commande.*

(a) : la notion de retour « feedback ».

(b) : la boucle fermée à travers un calculateur dédié.

(c): plusieurs systèmes de commande à travers un calculateur partagé.

(d): systèmes commandés en réseau (NCS).

La commande classique (analogique) a commencé dans l'année 1930 avec des boucles de régulation simples (a), et Par la suite (1950), avec l'évolution de l'électronique numérique, la commande est orienté vers les systèmes échantillonnés à base des calculateur numériques.

L'apparition des systèmes de commande en réseau et venue avec l'extension d'unité industrielle sur de vastes étendues à partir des années 1980

II.5.1 Architecture d'un système de contrôle en réseau [12]

Les systèmes de commande en réseau sont des systèmes automatiques répartis où les capteurs, contrôleurs, actionneurs et autres composants sont distribués autour d'un réseau de communication. Comme illustré par la figure suivant:

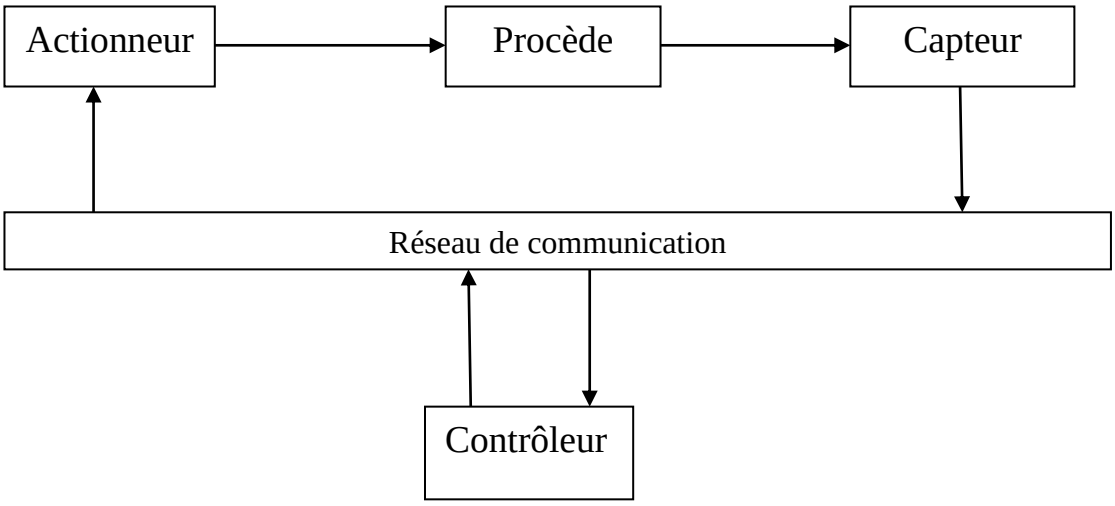


Figure II.6: *Architecture d'un système contrôlé en réseau***.**

II.5.2 Définition d'un réseau [14] [15] [16]

Un réseau de communication est l'ensemble de matériels et de logiciels permettant à des équipements de communiquer entre eux, ayant pour objectif le partage des ressources mise en communication

Les réseaux de communication sont de nos jours très présent dans le domaine de la commande temps-réel permettent par exemple d'augmenter la flexibilité des systèmes, d'utiliser des capteurs sans fils, de télé-opérer des applications distantes, de faire communiquer des systèmes autonomes, de déporter les contrôleurs pour économiser du temps de calcul et donc de l'énergie...

On distingue différents types de réseaux classés selon leur taille, leur vitesse de transfert des données, ainsi que leur étendue, (figure II.7) :

- **Un réseau local (Local Area Network):** 10 à 100 Mbit/s. Sur une étendue limitée (bâtiment d'entreprise).
- **Un réseau métropolitain (Métropolitain Area Network)** : sur une étendue d'une centaine de kilomètres, (réseau campus).
- **Un réseau étendu (Wide Area Network)** : de quelques kbit/s à quelques Mbit/s assurent généralement le transport d'information sur de grande distance (un pays).

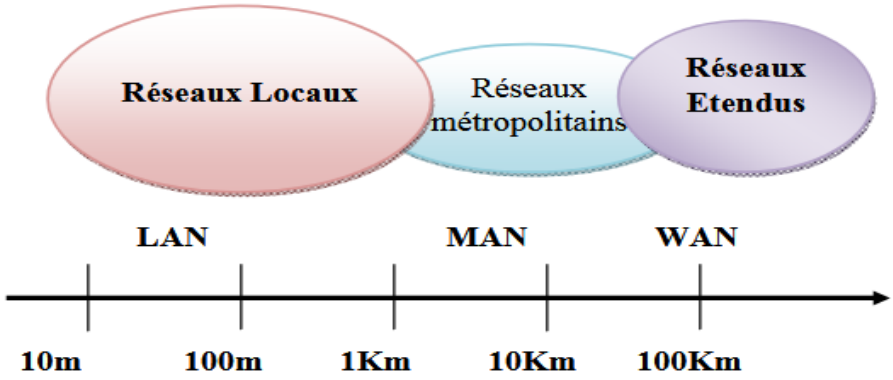


Figure II.7: *Classification des réseaux selon la taille.*

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la topologie physique, qui décrit comment les machines sont raccordées au réseau, de la topologie logique qui renseigne sur le mode d'échange des messages dans le réseau, illustré dans la figure II.8

- Les topologies point à point ou multipoint
- Le réseau en bus
- La topologie étoile
- Dans la topologie en anneau

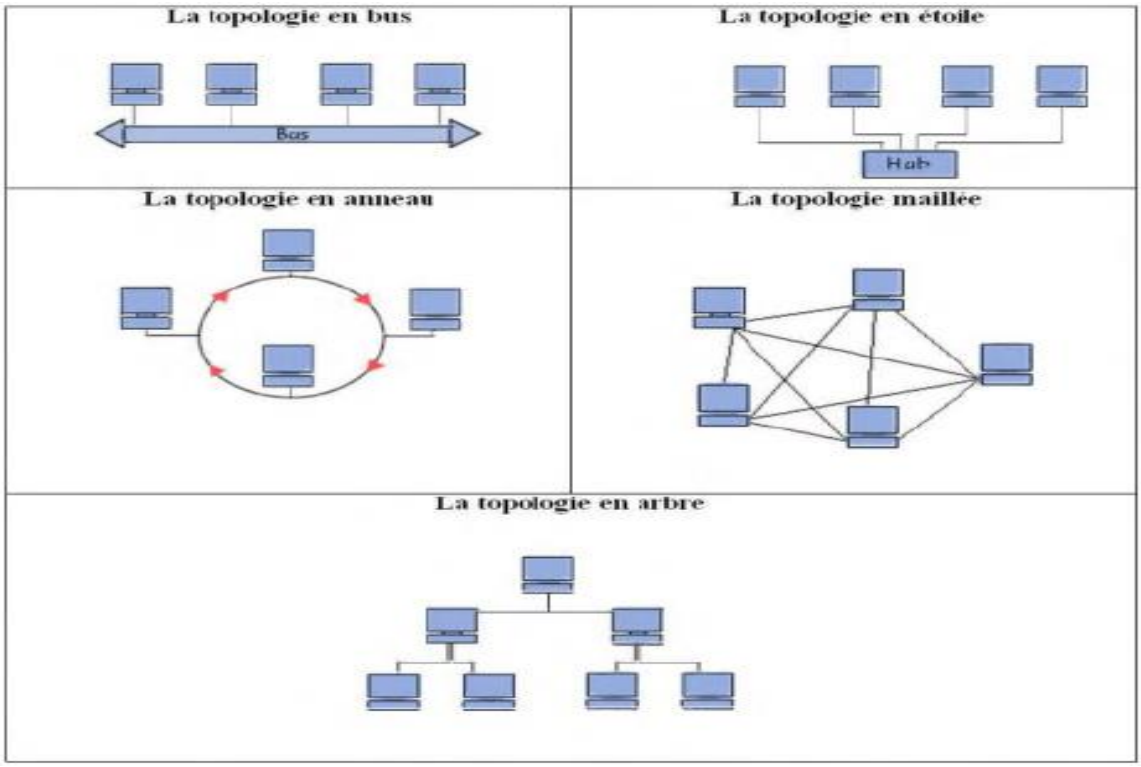


Figure II.8 *: les différentes topologies du reseau.*

II.5.3 Les réseaux de communication industriels

Dans une entreprise, il peut arriver fréquemment que l'automate, les actionneurs et les capteurs ne soient pas situés au même endroit mais à des distances importantes les uns des autres. L'utilisation d'un réseau industriel permet donc de faire communiquer plusieurs automates, chacun relié à une partie des capteurs/actionneurs, Les réseaux de communication industriels sont devenus incontournables dans la conception de systèmes automatisés. Ce la s'explique par la performance de ces réseaux, tant au niveau de l'échange de données critiques qu'au niveau de la distribution de signaux de commande.

II.5.4 Architecture d'un ensemble industriel [18]

Généralement un réseau de communication industriel est représenté en plusieurs niveaux comme illustré par la figure qui suit :

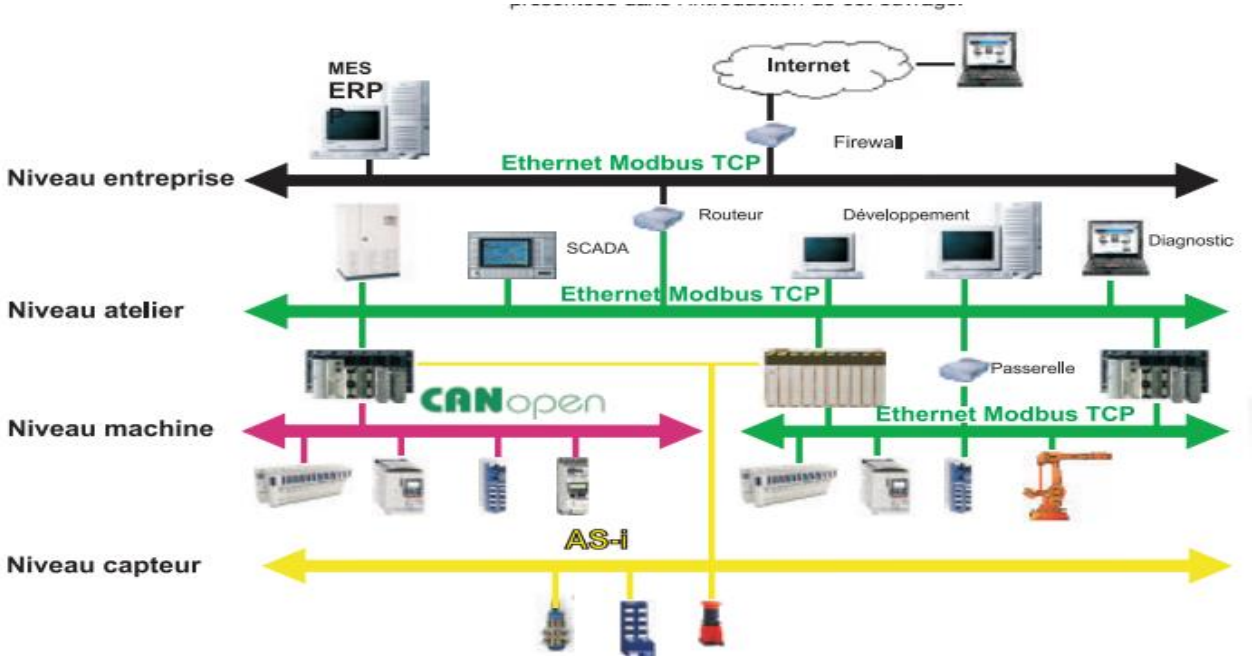


Figure II.8: *Niveau d'un réseau communication industriel.*

II.5.4.1 Ethernet Modbus TCP

La généralisation d'Ethernet dans les entreprises et sur Internet en a fait un standard de communication incontournable. Son usage généralisé a permis de réduire les coûts de connexion, d'augmenter les performances, la fiabilité et les fonctionnalités. Sa rapidité ne limite pas les applications, son architecture permet facilement les évolutions. Les produits et les logiciels demeurent compatibles, ce qui assure la pérennité des systèmes. Le

protocole “Modbus”, standard de fait dans l’industrie, fournit une couche applications simples et peu onéreuse à mettre en œuvre.

II.5.4.2 Can Open (Controller area network)

C’est la version industrielle du bus CAN. Créé pour l’automobile. Ce réseau a prouvé sa souplesse et sa fiabilité depuis plus de 10 ans dans de multiples applications telles que les équipements médicaux, les trains, les ascenseurs, ainsi que dans de multiples machines et installations.

II.5.4.3 As-Interface

Les machines modernes ont une grande quantité d’actionneurs et de capteurs et souvent des contraintes de sécurité. AS-Interface est le réseau niveau capteur conforme aux exigences des automatismes industriels. Il présente l’avantage d’offrir une connectique rapide et un seul

II.6 Conclusion

Dans ce chapitre, nous avons essayé de situer les inconvénients des systèmes de commande classique tout en introduisant les systèmes de commande en réseau et leur avantage telle que La communication à travers un réseau permet aussi une multitude d’échanges d’information entre composants de plus en plus intelligents et géographiquement dispersés. Et elle permet d’envoyer et recevoir les informations au lieu d’un câble pour chaque composant comme c’est le cas en commande classique, Vu leur généralisation dans les applications industrielles importantes.

CHAPITRE III : Les systèmes de supervision et de contrôle SCADA

III.1 Introduction

Les systèmes de Télégestion sont utilisés souvent pour piloter et superviser en temps réel et à distance des procédés de production embarqués sur des plates-formes Géographiquement très éloignées d'un site central, mais c'est surtout un précieux outil d'aide à la prise de décisions concernant le procédé de fabrication, et sur les choix stratégiques de l'entreprise.

La collecte des mesures et données physiques de production permet d'améliorer les rendements d'exploitation, de réduire les temps d'arrêt, d'effectuer des interventions de maintenance à distance, de renforcer la sécurité des accès, et de se prévenir des perturbations réseaux susceptibles d'entrainer des coupures ou la paralysie des principaux systèmes de transport dans le cadre d'une éventuelle attaque (informatique ou autre). La supervision à distance facilite aussi l'acquisition et le traitement des données requises par les réglementations et les normes en vigueur.

Dans ce chapitre, nous allons justement décrire le système de supervision expliciter toutes ces fonctionnalités.

III.2 Eléments de supervision des procédés industriels [24]

La supervision est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. La supervision concerne l'acquisition de données (mesures, alarmes, retour d'état de fonctionnement) et des paramètres de commande des processus généralement confiés à des automates programmables et a pour objectif d'assurer la gestion réactive et sure des modes de fonctionnement d'un processus. Ces modes ou situations sont définis à partir de l'analyse des données, de la connaissance du système et du savoir-faire des opérateurs.

Toute description du procédé, qui apporte une connaissance à priori sur ses caractéristiques et ses fonctionnalités, constitue un modèle du procédé. Ceci permet de comparer l'évolution du procédé réel au travers du suivi des mesures à la description théorique offerte par le modèle.

Le résultat de cette comparaison détecte le bon ou mauvais fonctionnement du procédé. Nous pouvons considérer le modèle comme la façon de valider le fonctionnement Correct du procédé et de déterminer les déviations par rapport aux conditions attendues d'opération. Les modèles peuvent être de différentes natures selon les informations disponibles sur le processus : il existe des modèles de type analytique (équations

Différentielles, équations aux différences, relations entre variables, etc.), ainsi que des modèles qualitatifs (équations qualitatives, modèles a base d'ensembles flous, règles, description du comportement, etc.), qui représentent le fonctionnement statique ou dynamique, normal ou anormal du procédé.

Pour la mise en place d'un système de supervision, deux fonctions doivent être prises en compte : la surveillance et la reconfiguration. Comme illustré par la figure III.2.

La surveillance du procédé traite les données disponibles en ligne, afin d'obtenir son état de fonctionnement. Dans ce dernier nous retrouvons les fonctions de détection de défaillances et de diagnostic.

III.2.1 La surveillance

La surveillance des procédés industriels consiste à générer des alarmes à partir des informations délivrées par des capteurs. Elle recueille les signaux en provenance du procédé et de la commande et reconstitue l'état réel du système commande. Des seuils sont définis sur des variables clés par des experts du procédé selon des critères de sécurité concernant le personnel, l'installation et son environnement. Cette génération d'alarmes apporte une aide aux OHS (operateurs humains de supervision) dans leur tache de surveillance afin qu'ils puissent analyser la situation et prendre une décision adaptée (procédure d'arrêt d'urgence, mode dégrade, action corrective).

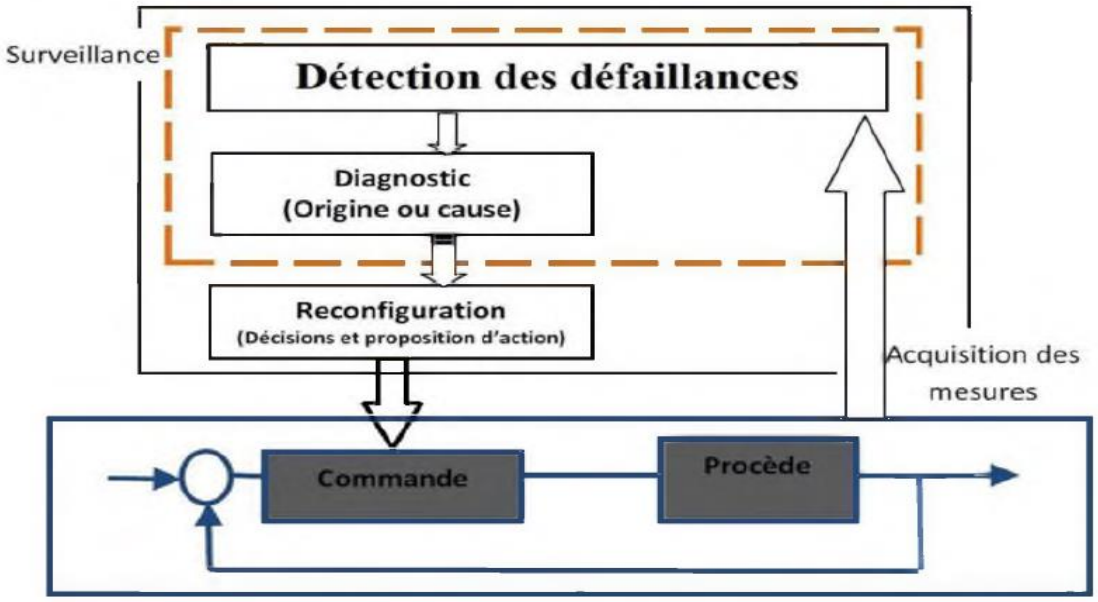


Figure III.1: *Schéma générale de la supervision.*

III.2.2 La détection

Elle consiste en l'identification des changements ou déviations des mesures du procédé par rapport au fonctionnement normal, ce qui se traduit par la génération des symptômes.

III.2.3 Le diagnostic

Elle consiste à déterminer quelles sont l'origine et/ou la/(les) cause(s) qui ont pu engendrer le symptôme détecte. A ce stade, le système doit avoir la capacité de décider quand le procédé se trouve dans une situation de fonctionnement normal, et quand une action corrective doit être appliquée.

III.2.4 La reconfiguration

L'action corrective correspond à l'étape de reconfiguration de la Commande de façon à ramener le procédé dans un mode de fonctionnement normal.

Cependant, on peut trouver d'autres approches pour la mise en place d'un système de supervision. En effet, pour la communauté de systèmes a événements discrets (SED), la supervision a pour but : de nous alerte et des problèmes, et si possible les anticiper. On commence par effectuer des tests, puis analyser les résultats sous forme de graphiques ou autres, et en fonction de certains critères, déclencher des actions (redémarrage de services, alerte de l'administrateur sur le comportement d'un processus etc.), mettre en place des actions face à des évènements. La supervision peut se résumer à la formule :

Informations + Traitement = Supervision

La supervisons à lieu dans une structure hiérarchique (au moins avec 2 niveaux), et recouvre l'aspect du fonctionnement normal et anormal :

• en fonctionnement normal, le rôle de la supervision est de prendre, en temps réel, les décisions correspondantes aux degrés de liberté exigés par la flexibilité décisionnelle;

• en présence de défaillances, la supervision aide à prendre toutes les décisions nécessaires pour le retour vers un fonctionnement normal.

III.3 Description d'un système SCADA

III.3.1 Définition du SCADA [19] [20]

SCADA est un acronyme qui signifie le contrôle et la supervision par acquisition de Données (en anglais : Supervisory Control and Data Acquisition), il effectue une surveillance et un contrôle centralisé pour les sites sur le terrain via des réseaux de

communication longue distance, y compris la surveillance des alarmes et le traitement des données d'état. Le Système SCADA collecte des données de divers appareils d'une quelconque installation, puis transmet ces données à un ordinateur central, pour contrôler et superviser l'installation. Comme illustré par la figure suivante

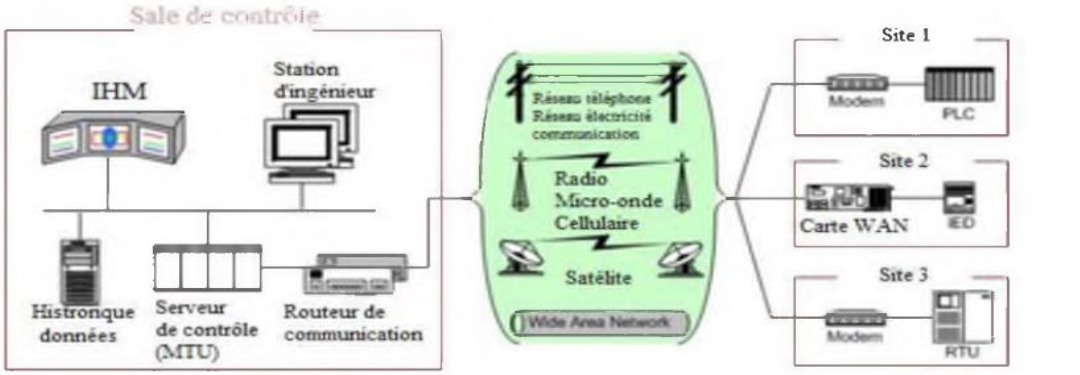


Figure III.2: ***Schéma général d'un système SCADA.***

III.3.2 Eléments du système SCADA [21] [22] [23]

Principalement un système SCADA, comme illustré par la figure III.3, se compose de :

- **Le site central** : qui est la station de contrôle pour l'ensemble du système, fournissant normalement à l'utilisateur l'interface pour l'affichage des informations et le contrôle des sites éloignés ;
- **RTU (Remote Terminal Unit) :** ce sont des terminaux délocalisés (isolés) servant à collecter les informations à partir de l'instrumentation de terrain et à les transmettre au terminal maitre MTU, à travers le système de communication.
- **MTU (Master Terminal Unit) :** il recueille les données provenant des RTU, les rend accessibles aux opérateurs via l'interface HMI et transmet les commandes nécessaires des opérateurs vers l'instrumentation de terrain.
- **Système de communication :** moyen de communication entre le MTU et les différents RTU, la communication peut être par le biais d'internet, de réseaux sans fil ou câblés, ou du réseau téléphonique public…etc.

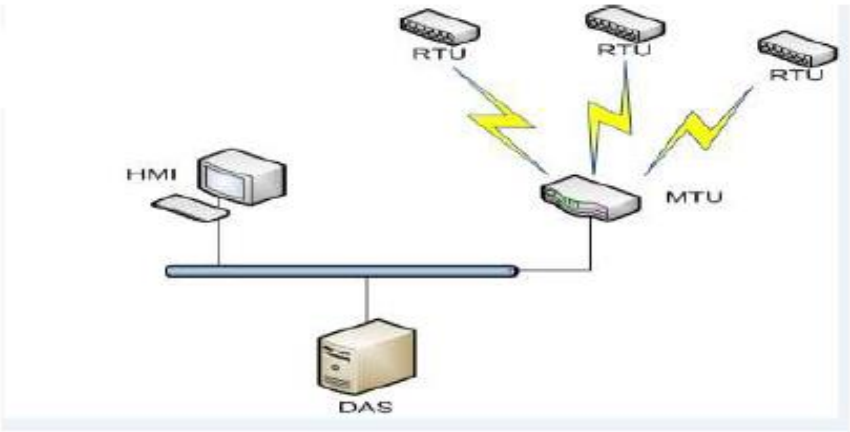


Figure III.3: *Eléments d'un système SCADA.*

III.3.2.1 RTU/PLC [21] [22] [23]

C'est une entité d'acquisition de données et de commande généralement à base de microprocesseur (actuellement on utilise des automates programmables), elle sert à contrôler et superviser localement l'instrumentation d'un site éloigné et transférer les données requises vers la salle de contrôle principal où parfois à d'autres RTU. Il recueille également des informations provenant de l'appareil maitre et met en œuvre des processus qui sont dirigés par le maitre. Les RTUs sont équipées de voies d'entrée pour les capteurs ou les compteurs, canaux de sortie pour le contrôle, l'indication ou les alarmes et un port de communication, la figure suivante représente un schéma typique d'une RTU.

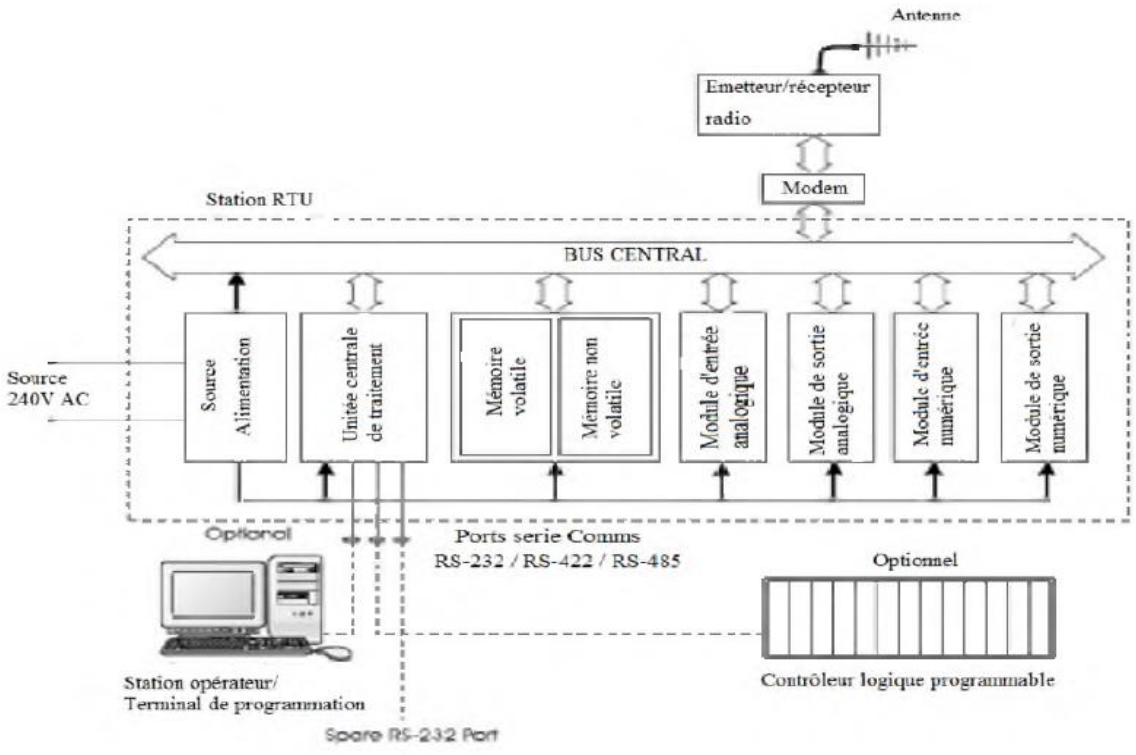


Figure III.4: Schéma général d'un RTU.

III.3.2.2 MTU [21] [22] [23]

Unité maitre peut être décrite comme une station ayant plusieurs postes opérateur (liés ensemble avec un réseau local) connectés a un système de communication. Elle recueille les données de l'instrumentation du terrain périodiquement à partir des stations RTU et permet la commande a distance par le biais des postes opérateurs, en général elle sert à configurer et à programmer les RTU, diagnostiquer la communication et les stations RTU. La figure ci-dessous montre un schéma général d'une MTU.

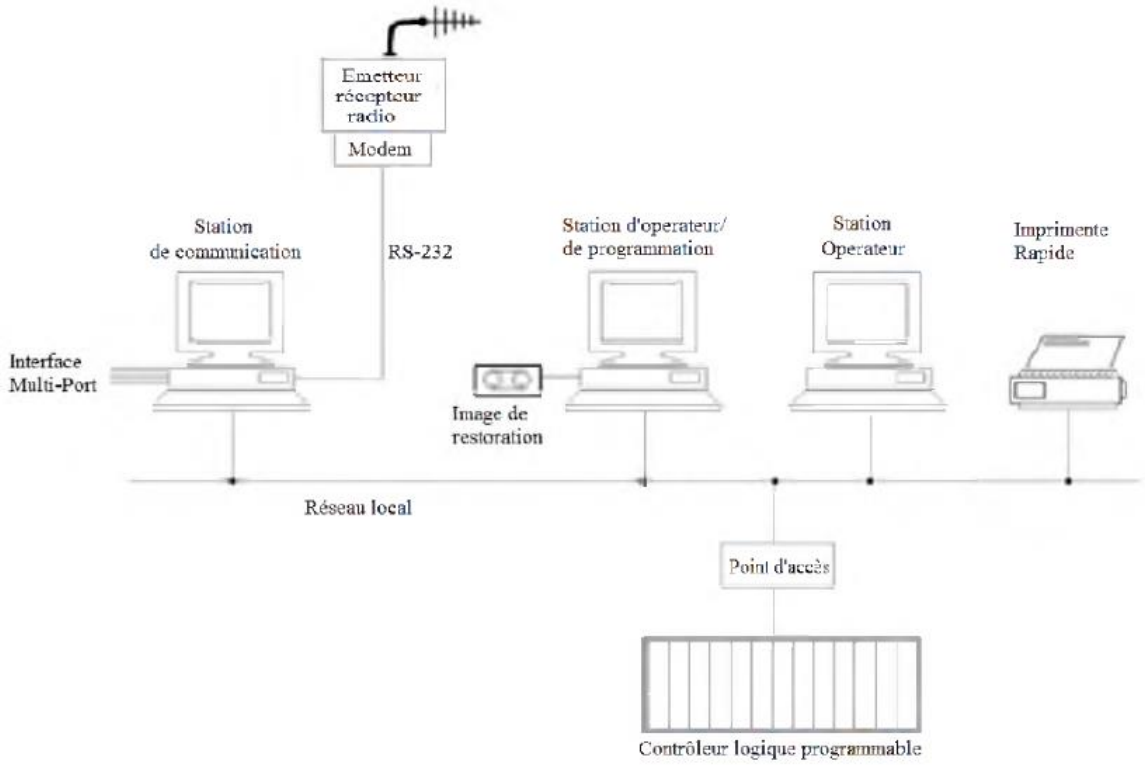


Figure III.5: *Schéma général d'un MTU.*

III.3.2.3 Communication [25] [26]

Il existe plusieurs architectures de communication pour un système SCADA. La plus simple est la communication point à point ou la communication est établie entre deux nœuds du réseau (l'un maitre et l'autre esclave), la deuxième architecture est la communication multipoint qui consiste en un maitre et plusieurs esclaves, une topologie des différents modes de communication est présentée sur la figure suivant :

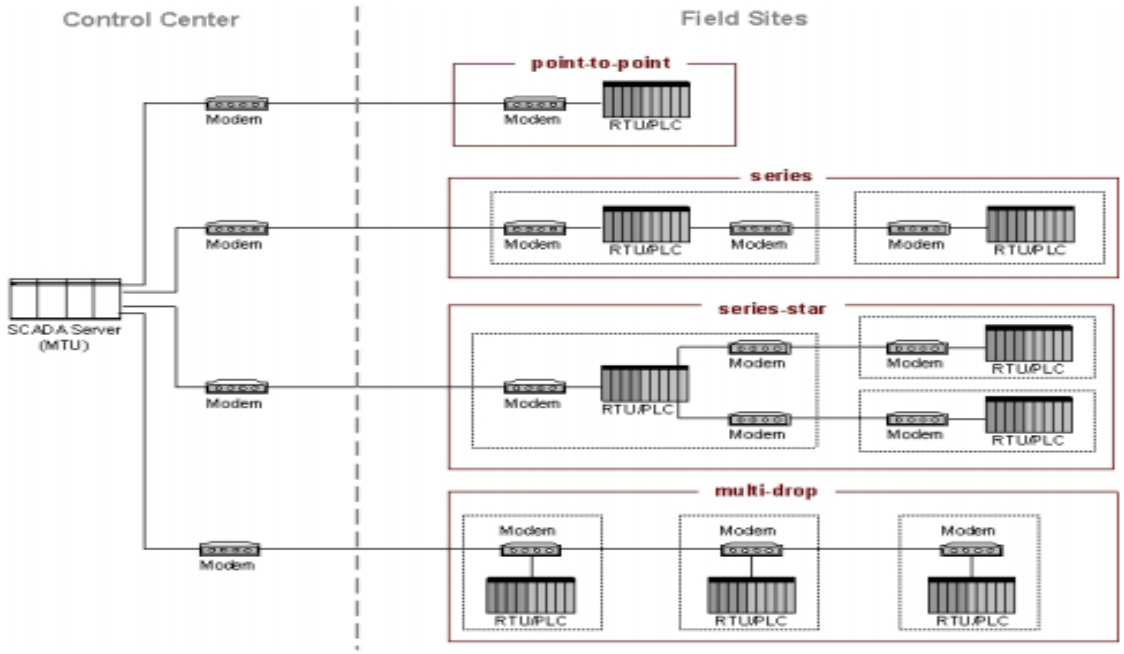


Figure III.6 : *Topologie de différents modes de communication SCADA.*

Il existe deux approches selon lesquelles on peut classifier la communication, la première qui se base sur l'approche d'interrogation et la deuxième est l'approche paire à pair (peer to peer) **[25] [27]**

- **Approche interrogation (Maitre-esclave)**

Cette approche peut être utilisée pour des systèmes de communication configurés en mode point à point ou multipoint. Le maitre contrôle totalement le système de communication puisqu'il gère périodiquement les demandes de transfert des données des différents esclaves, ces derniers ne peuvent pas prendre l'initiative mais répondent seulement aux demandes du maitre.

- **Approche pair à pair (peer to peer) :**

Cette approche est appliquée pour la communication entre RTU et un autre RTU, elle repose sur l'aptitude de chaque nœud du réseau de communiquer avec un autre nœud directement, seulement il doit avoir un contrôle d'accès et un contrôleur des éventuels collisions avant d'entamer la communication.

III.3.3 Protocoles employés dans un environnement SCADA [25]

Suite à la nécessité d'envoyer et de recevoir des données jugées critiques généralement pour de longues distances et en temps réel dans un environnement SCADA on fait appel aux protocoles de communications, cette optique a donné naissance à plusieurs protocoles dont on va développer les plus utilisés :

III.3.3.1 Le protocole Modbus [26]

Modbus : est une marque déposée par Modicon comme protocole de communication pour des réseaux d'automates programmables.

C'est un protocole de transmission de données régissant le dialogue entre une station "Maitre" et des stations "Esclaves" comme illustré par la figure III.7. L'échange Maitre-Esclave s'effectue par l'envoi de trames MODBUS dont le format de base est le suivant :

Champ Adresse	Champ Fonction	Champ Données	Contrôle de Redondance Cyclique

- ✓ Le champ adresse correspond à l'adresse de la station Esclave destinatrice de la requête.
- ✓ Le champ fonction détermine le type de commande (lecture mot, écriture mot, etc.)
- ✓ Le champ de données contient l'ensemble des paramètres et informations liés à la requête.
- ✓ Le contrôle de redondance cyclique (CRC) permet à la station destinatrice de vérifier l'intégrité de chaque trame.

A chaque réception d'une trame, la station adressée envoie une trame de réponse, dont le format est identique à celui de la trame émise par la station Maitre avec selon le type de commande, un champ de données plus ou moins important.

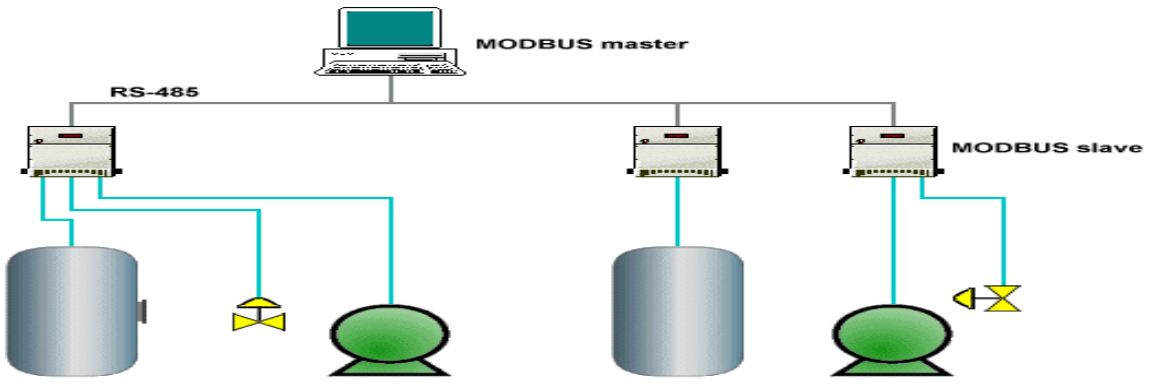


Figure III.7: *Communication par le Protocole Modbus.*

III.3.3.2 Le protocole DNP3 [26]

DNP3 est construit sur le profil EPA (Enhanced Performance Architecture) qui est une version simplifiée du modèle OSI (Open System Interconnexion) à 3 couches (physique, liaison, application).

Ce protocole de communication multipoint permet d'échanger des informations entre un système de conduite (superviseur ou RTU) et un ou plusieurs équipements électroniques intelligents (IED : Intelligent Electronic Device)

Le système de conduite constitue l'équipement maître, les IED sont les équipements esclaves, chaque équipement est identifié par une adresse unique, de 0 à 65519, l'émission des trames en diffusion est possible. Comme le montre la figureIII.8.

Pour permettre la transmission de messages de taille importante (2 kilooctets ou plus), des fonctions de segmentation et de réassemblage de données ont été ajoutées dans DNP3. L'ensemble de ces fonctions constitue une pseudo-couche Transport.

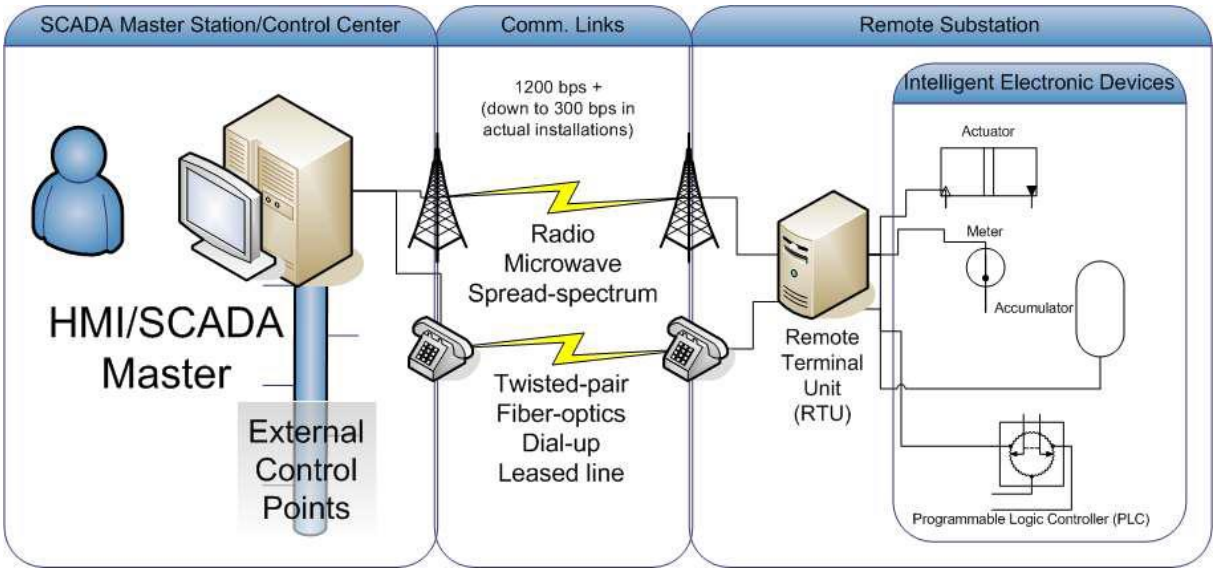


Figure III.8: *Communication par le Protocole DNP3*

III.3.3.3 Le protocole PROFIBUS [26] [27]

PROFIBUS répond à des normes internationales, son architecture repose sur 3 couches inspirées du modèle en 7 couches de l'OSI :(la figure III.9)

- ✓ **la couche 1,** physique, décrit les caractéristiques physiques de la transmission.
- ✓ **La couche 2,** liaison de données, spécifie les règles d'accès au bus.

- ✓ **la couche 7,** application, définit les mécanismes communs utiles aux applications réparties et la signification des informations échangées

C'est un protocole pour réseau de terrain ouvert, non propriétaire, répondant aux besoins d'un large éventail d'applications dans les domaines du manufacturier et du procès, Il se décline en trois protocoles de transmission, appelés profils de communication, aux fonctions bien ciblées DP, PA et FMS, selon l'application, il peut emprunter trois supports de transmission ou supports physiques (RS 485, CEI 1158-2 ou fibre optique).

- **Le Profibus-DP** (Decentralised Peripheral ou périphérique décentralisée) est utilisé pour commander d'actionneurs, vérifier l'état des capteurs par, commander un autre automate programmable.

  On reconnaît un réseau Profibus-DP à la couleur de son câble (violet).Dans ce câble il y a 2fils : un vert et un rouge, nommé "A" et "B".
- **Le Profibus-FMS** (Fieldbus Message Spécification) il est utilisé pour la communication non déterministe
- **Le Profibus-PA :** (Process Automation) c'est pour le contrôle des équipements de mesure par l'intermédiaire d'un système de contrôle de procédé. Cette variante du profibus est utilisée dans les zones dangereuses et explosives. Les courants dans ces câbles sont limités pour raison de sécurité, ainsi le nombre d'équipements sur une ligne profibus PA, est limité. La vitesse de transmission est de 31,25 kbit/s. Cependant, le profibus PA utilise le même protocole que le DP, les deux réseaux pouvant être liés à l'aide d'un coupleur. Le profibus DP est plus rapide que le PA.

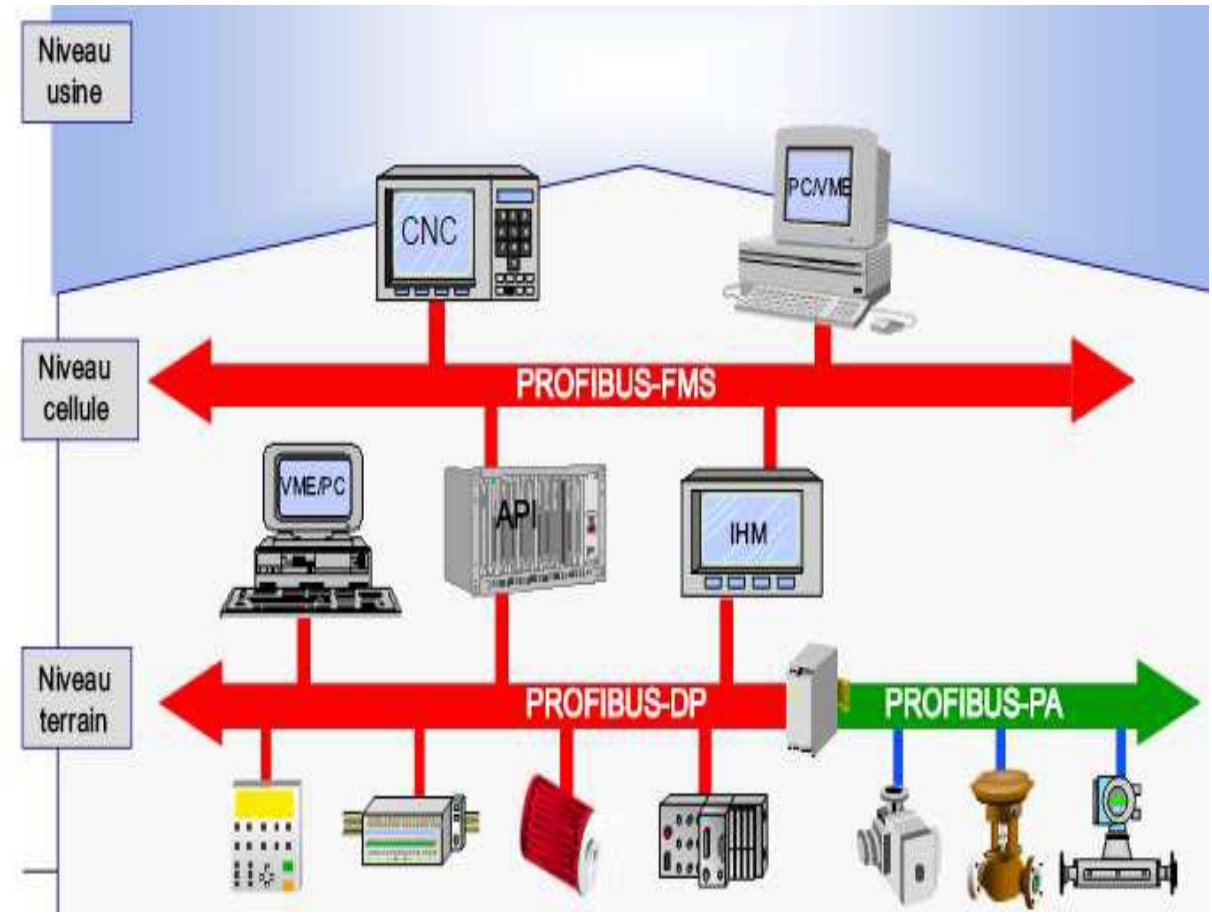


Figure III.9: *Communication par le Protocole Profibus.*

III.3.4 L'interface Homme Machine (HMI) de SCADA [9]

Interface Homme-Machine (IHM ou HMI) est un logiciel et un matériel qui permettent aux opérateurs de surveiller l'état d'un processus sous contrôle, de modifier les paramètres de contrôle soit, l'objectif de contrôle, et d'annuler éventuellement les opérations de contrôle automatique en cas d'urgence. Il permet également à l'opérateur de contrôle de configurer des points de réglage ou des algorithmes et paramètres de contrôle dans l'automate. L'HMI affiche également des informations sur l'état du processus, des informations historiques, des rapports et d'autres informations destinées aux opérateurs, administrateurs, responsables, partenaires commerciaux et autres utilisateurs autorisés. L'emplacement, la plate-forme et l'interface peuvent varier considérablement. Par exemple, une IHM peut être une plate-forme dédiée dans le centre de contrôle, un ordinateur portable sur un réseau local sans fil ou un navigateur sur tout système connecté à Internet.

Le logiciel HMI de SCADA fournit a la fois des vues graphiques de l'état des terminaux distants et leurs historiques d'alarmes, Il permet aussi de visualiser l'ensemble des données du procédé , d'intervenir à distance sur les machines et de générer des rapports

d'exploitation et de contrôle de données en archivant la synthèse dans ses bases d'historiques. (Voir la figure III.10)

Les fonctions principales d'un logiciel SCADA sont les actions suivantes :

- La visualisation des données d'exploitation à travers la totalité des installations
- L'acquisition, le stockage et l'extraction des données d'exploitation importantes avec les commentaires saisis par l'opérateur
- La visualisation des tendances en temps réel à partir de données temps réel ou depuis les bases d'archivage
- L'amélioration de la disponibilité des installations et la fourniture des informations fiables…etc.

En plus l'interface graphique doit faciliter aux operateurs toute les taches citées. HMI du SCADA est très important pour le bon déroulement de la procédure d'aide a la décision, il est le seul point d'interaction entre l'operateur et les algorithmes d'aide a la décision, ainsi, il aide l'operateur dans sa tache d'interprétation et de prise de décision, en lui offrant une très bonne visibilité sur l'état et l'évolution de l'installation, avec l'affichage en différentes couleurs des résidus, des alarmes et des proposition sur l'action à entreprendre.

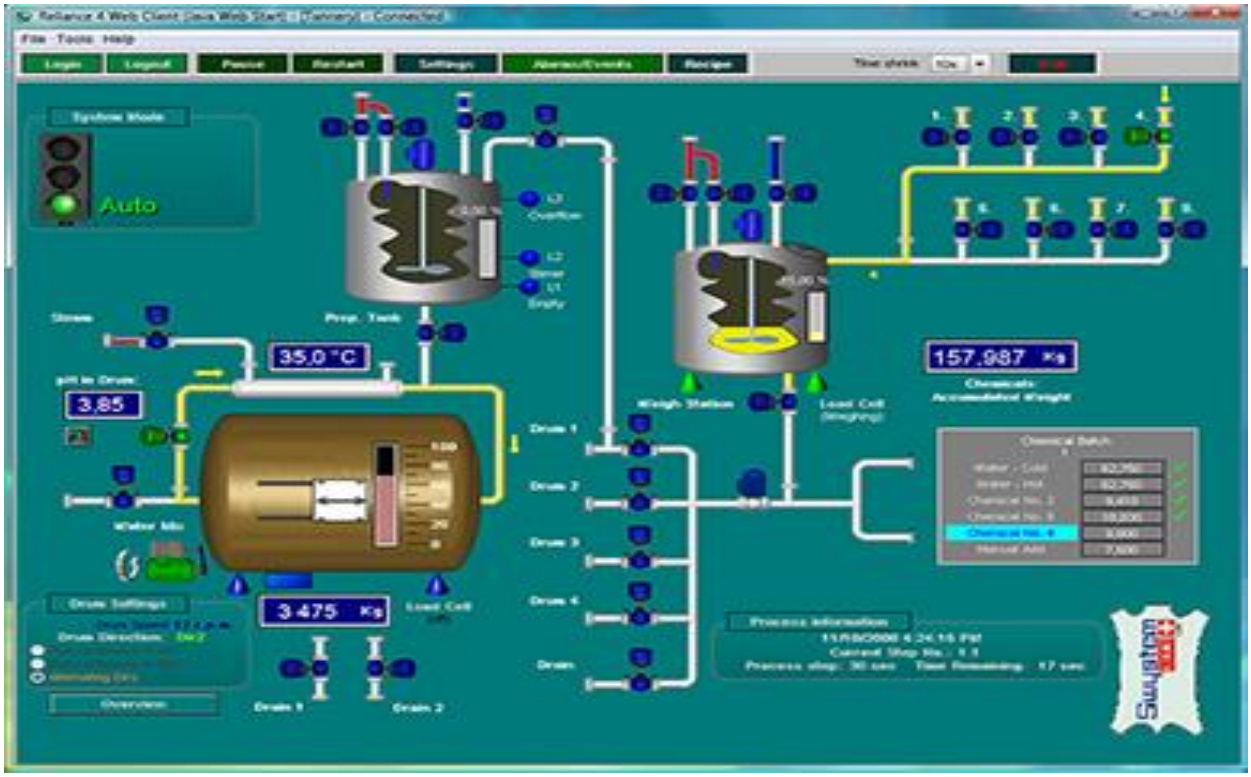


Figure III.10: *Exemple de logiciel SCADA.*

III.3.5 La sécurité d'un système SCADA [28]

SCADA utilise les mêmes techniques de sécurité que dans les réseaux OSI ou TCP/IP, seulement les réseaux SCADA doivent prendre en considération les contraintes additionnelles suivantes :

- L'emploi d'un antivirus est déconseillé car il affecte le temps de réponse ;
- Le système doit être tolérant aux pannes (notion de redondance) ;
- La perte des données ou les interruptions sont intolérables car elles peuvent engendrer des dégâts matériels et humains.
- Temps de réponse avec un retard presque nul.

Pour commencer nous allons introduire les attaques et les menaces qui ciblent un système SCADA puis nous verrons les mesures à prendre.

III.3.5.1 Vulnérabilités et attaques [28]

Au début, les systèmes SCADA n'étaient pas conçus avec des dispositifs de sécurité car ils travaillaient dans des environnements clos, ce qui n'est pas le cas de nos jours et particulièrement avec le développement de l'Internet. Un système SCADA est aussi sous la menace d'attaques conventionnelles du monde informatique. Les risques majeurs sont alors :

- Un retard d'exécution suite à l'implémentation de la sécurité ;
- Un emploi de matériels et logiciels standards qui présentent des vulnérabilités connues.

III.3.5.2 Les menaces [28]

Les menaces des systèmes SCADA peuvent être le résultat de phénomènes naturels, d'actes malicieux commis par des individus, des accidents, des procédures abusives, ou des défaillances techniques. Quelques exemples de menaces sont énumérés ici:

- Les virus ;
- Les chevaux de Troie ;
- L'erreur humaine ;
- Les accidents ;
- Toute interruption des services publics ;
- Le bruit sur les lignes électriques ;
- L'interdépendance avec d'autres réseaux.

III.3.5.3 Chemins d'attaques [29]

Pour qu'une menace soit réalisée, elle doit avoir un moyen d'accéder au système SCADA, puisqu'il est lié à l'Internet, ou aux réseaux d'entreprise, certains chemins typiques d'attaque SCADA sont cités ici :

- Ports informatiques ouverts, tels que des ports UDP ou TCP qui ne sont pas protégés ou laissé ouvert inutilement ;
- Authentification faible dans les protocoles et les composantes du SCADA ;
- Connexion Internet ;
- Connexions à d'autres réseaux qui contiennent des vulnérabilités ;
- Connexions sans fil non sécurisées ;
- Attaques de fragmentation IP.

III.3.5.4 Cibles préférées [29]

Généralement si un attaquant arrive à pénétrer un système SCADA, son but sera l'accès au contrôle du système afin de faire des modifications nuisibles. Quelques actions possibles lors d'une telle attaque sont les suivantes :

- Neutralisation de la communication entre MTU et les différents RTU ;
- Contrôle du MTU ;
- Arrêt des unités ;
- Modification des programmes des RTU ;
- Obtention du mot de passe.

III.3.5.5 Cyber-sécurité des systèmes SCADA [28]

Pour assurée la cyber-sécurité des systèmes SCADA nous devant passer par un processus de 21 étapes résumées en figure III.11 :

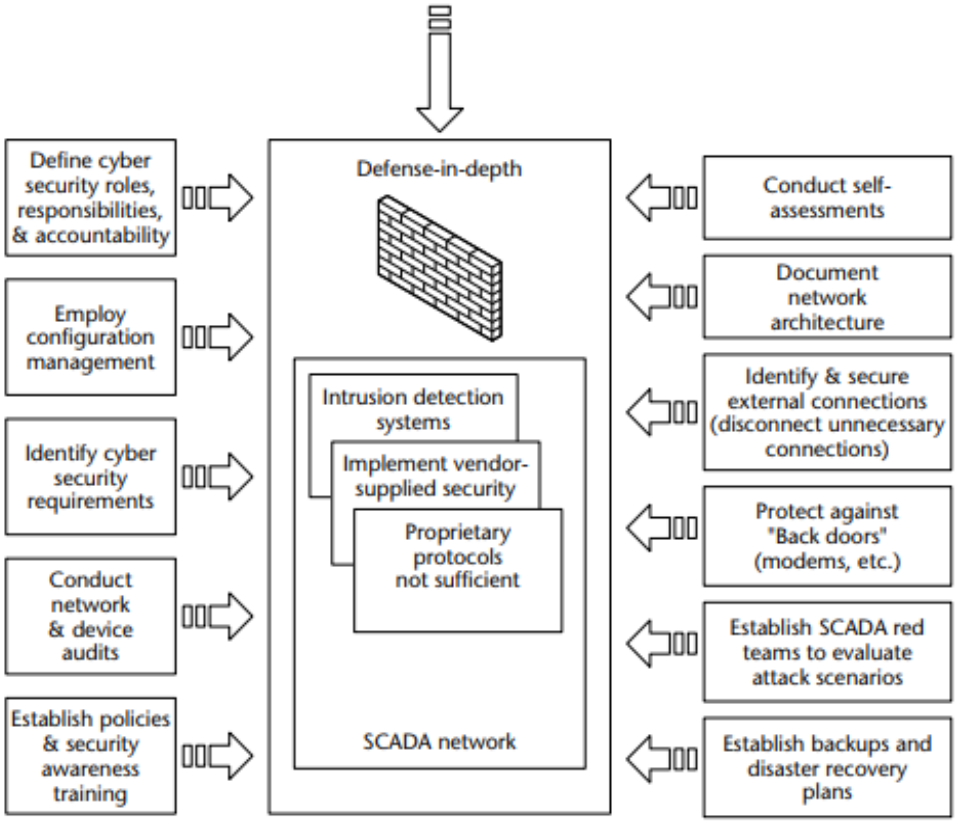


Figure III.11: *Résumé graphique des 21 étapes du cyber sécurité SCADA.*

III.3.5.6 Firewall (Les pare-feu) [30]

Les pare-feu de réseau sont des dispositifs ou des systèmes qui contrôlent le flux de trafic réseau entre les réseaux. Grace à différentes postures de sécurité. Un pare-feu est un équipement de réseau, la plupart du temps de type routeur, placé à l'entrée du réseau afin d'empêcher l'entrée ou la sortie de paquets non autorisés par l'entreprise. Comme illustré par la figure suivante :

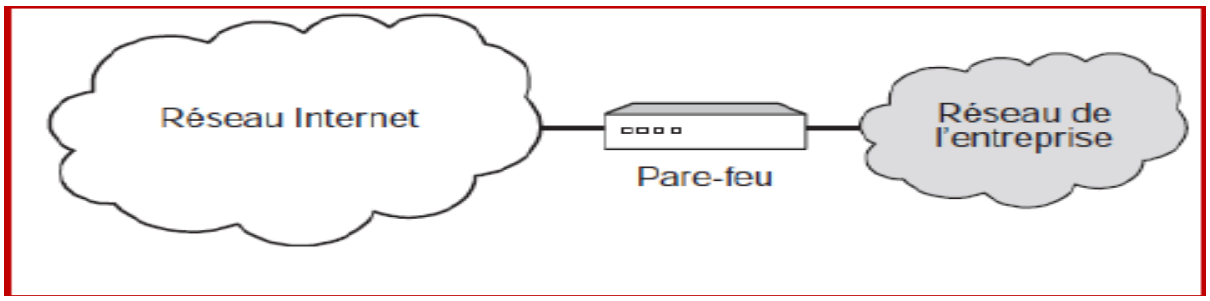


Figure III.12: *Situation d'un pare-feu dans l'entreprise.*

Pour reconnaître les paquets à accepter et à refuser, il est possible de travailler de deux façons :

- Interdire tous les paquets sauf ceux d'une liste prédéterminée ;
- Accepter tous les paquets sauf ceux d'une liste prédéterminée.

En règle générale, un pare-feu utilise la première solution en interdisant tous les paquets, sauf ceux qu'il est possible d'authentifier par rapport à une liste de paquets que l'on souhaite laisser entrer. Cela comporte toutefois un inconvénient lorsqu'un client de l'entreprise se connecte sur un serveur à l'extérieur, la sortie par le pare-feu est acceptée puisque authentifiée. La réponse est généralement refusée, puisque le port sur lequel elle se présente n'a aucune raison d'accepter ce message s'il est bloqué par mesure de sécurité.

Pour que la réponse soit acceptée, il faudrait que le serveur puisse s'authentifier et que le pare-feu lui permette d'accéder au port concerné. L'autre option est évidemment beaucoup plus dangereuse puisque tous les ports sont ouverts sauf ceux qui ont été bloqués. Une attaque ne se trouve pas bloquée tant qu'elle n'utilise pas les accès interdits. Avant d'aller plus loin, considérons les moyens d'accepter ou de refuser des flots de paquets. Les filtres permettent de reconnaître un certain nombre de caractéristiques des paquets, comme l'adresse IP d'émission, l'adresse IP de réception, parfois les adresses de niveau trame, le numéro de port et plus généralement tous les éléments disponibles dans l'en-tête du paquet IP. Pour ce qui concerne la reconnaissance de l'application, les filtres sont essentiellement réalisés sur les numéros de port utilisés par les applications.

Les numéros de port correspondent à des applications. Les pare-feu peuvent être de deux types, proxy et applicatif. Dans le premier cas, le pare-feu a pour objectif de couper la communication entre un client et un serveur ou entre un client et un autre client. Ce type de pare-feu ne permet pas à un attaquant d'accéder directement à la machine cible, ce qui donne une forte protection supplémentaire. Dans le second cas, le pare-feu détecte les flots applicatifs et les interrompt ou non suivant les éléments filtrés. Dans tous les cas, il faut utiliser des filtres plus ou moins puissants.

III.3.6 Les Alarmes [31]

Chaque opérateur utilisant un système SCADA doit disposer d'un plan écrit de gestion des alarmes pour permettre au contrôleur de réagir efficacement aux alarmes. Le plan de l'exploitant doit inclure les dispositions suivantes:

- examiner les opérations d'alarme liées à la sécurité du SCADA à l'aide d'un processus garantissant la précision des alarmes et la sécurité des opérations en cours.

- Identifiez au moins une fois par mois civil les points relatifs à la sécurité qui ont été retirés du contrôle de l'hôte SCADA, dont les alarmes ont été bloquées, qui ont généré de fausses alarmes ou qui ont des valeurs forcées ou manuelles dépassant celles requises pour les périodes associées. activités de maintenance ou d'exploitation.
- Vérifiez les valeurs de consigne et les descriptions d'alarme correctes liées à la sécurité au moins une fois par année civile.
- Examiner le plan de gestion des alarmes requis par ce paragraphe au moins une fois par année civile.
- Surveiller le contenu et le volume de l'activité générale dirigée vers et exigée de chaque contrôleur au moins une fois par année civile, afin de garantir aux contrôleurs le temps nécessaire pour analyser et réagir aux alarmes entrantes.

III.3.7 Architecture des systèmes SCADA [19] [20]

SCADA entoure un transfert de données entre le serveur MTU, et une ou plusieurs unités terminales distantes RTUs et entre le serveur et les terminaux des opérateurs, la figure ci-dessous représente un schéma de l'architecture d'un réseau SCADA qui utilisant des routeurs pour joindre le poste de pilotage par Internet.

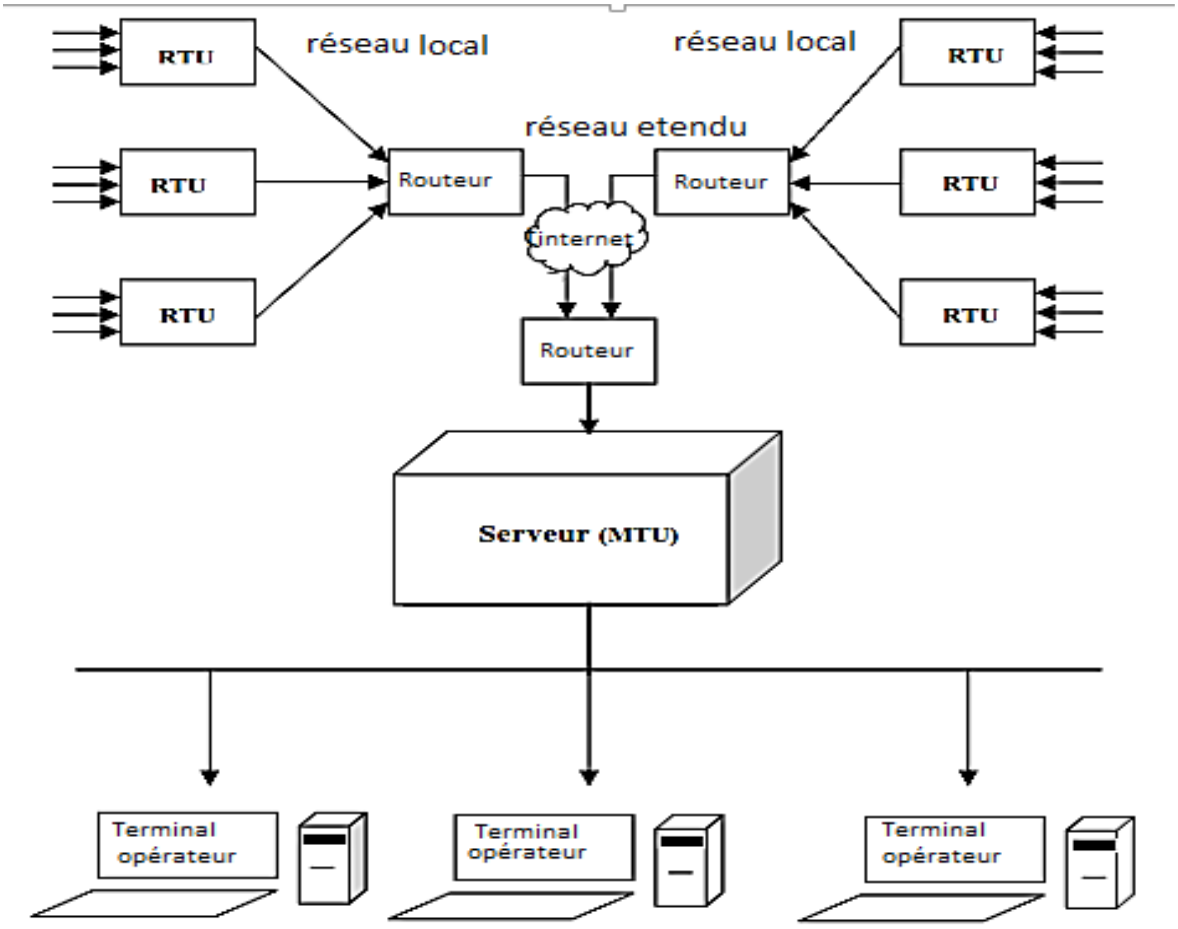


Figure III.13: Architecture de la supervision dans un environnement SCADA.

Nous allons prendre un exemple d'un système de sécurité Pipeline SCADA qui offrent une solution unique pour la détection d'activités sur et sous terre, Ce système détecte différents risques ainsi que des fuites et alerte immédiatement et efficacement les forces de sécurité ou les équipes de maintenance. Il détecte et localise de manière passive les intrusions en surface et sous la surface en temps réel

Représenter dans la figure III.14 :

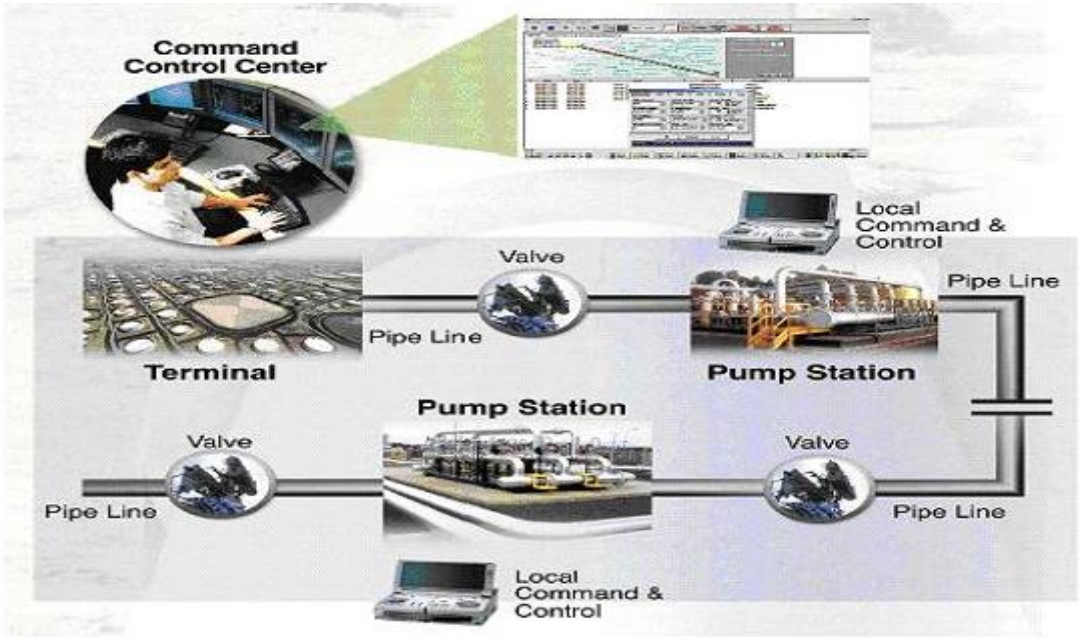


Figure III.14: *Les systèmes de sécurité Pipeline SCADA.*

III.4 Conclusion

Dans ce chapitre, nous avons présenté le système SCADA car c'est un outil qui permet de réaliser une supervision à distance, c'est-à-dire que l'installation à superviser pourrait se trouver à des milliers de kilomètres du poste de pilotage. Ce type de supervision est très utile pour les industries à hauts risques, telles que les industries chimiques et nucléaires car il évite des pertes humaines en cas d'accident survient et réduit énormément le nombre de visites au site.

CHAPITRE IV : simulation d'un système SCADA avec Tia portal V12

IV.1 Introduction

Ce présent chapitre est réservé à notre application dédiée à la supervision de l'ouvrage ROB1 SP3 M'Sila-Terminale arrivé Bejaia de SONATRACH.

Après une brève présentation logicielle (Tia Portal, WinCC), nous décrirons l'architecture SCADA de l'ouvrage sus - cité retenu par la société SONATRACH. En suit, nous expliquerons étape par étape la création, configuration et les tests de notre projet de supervision.

IV.2 Présentation du logiciel Tia portal [32]

Pour la création et la configuration de notre projet sous SCADA nous utilisant le logicielle STEP 7 Professional ou TIA Portal (Totally Integrated Automation Portal). Logiciel de programmation et de configuration sous environnement SIMATIC SCADA de Siemens dans. Il est formé d'un ensemble d'applications avec lesquelles nous pouvons aisément réaliser des taches partielles comme :

- la configuration et le paramétrage du matériel ;
- la création et le test de programmes utilisateur ;
- la configuration de réseaux et de liaisons ;
- la simulation en ligne du fonctionnement de la partie opérative.

S'ajoute une large gamme de logiciels optionnels, dont entre autres ceux des langages de programmation S7 GRAPH, SCL. Le gestionnaire de projets « SIMATIC Manager », sert d'interface graphique à toutes ces applications. C'est lui qui organise la mise en commun dans un projet de toutes ces données et de tous les paramètres requis pour réaliser une tâche d'automatisation. Les données y sont structurées thématiquement et représentées sous forme d'objets.

Avec TIA , Siemens concrétise sa vision d'un environnement unique pour le développement de solutions d'automatisation dans tous les secteurs.

IV.2.1 Fenêtre principale (Vue du portal)

Cette fenêtre affiche la liste des actions pouvant être réalisées pour la tâche d'automatisation retenue.

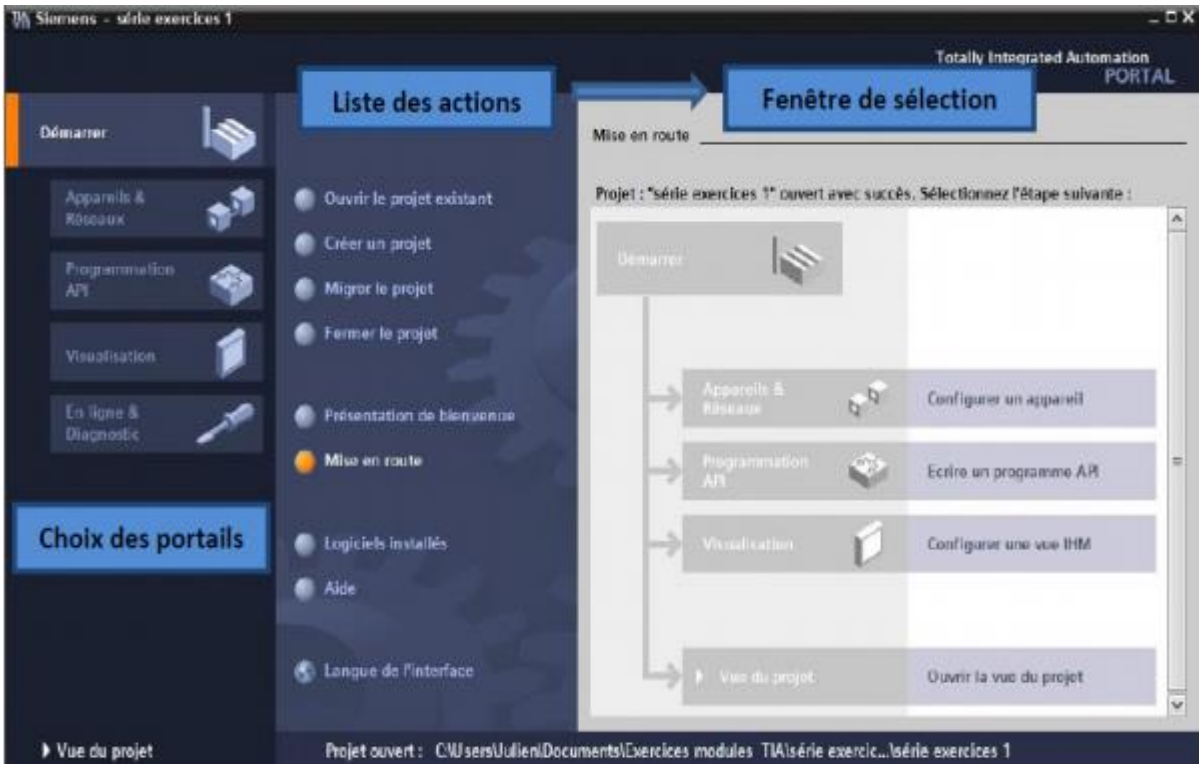


Figure IV.1: *Vue du portal.*

IV.2.2 Vue du projet

L'élément « Projet » contient l'ensemble des éléments et des données nécessaires pour mettre en œuvre la solution d'automatisation souhaitée.la figure ci dessue représente plusieurs fenêtre :

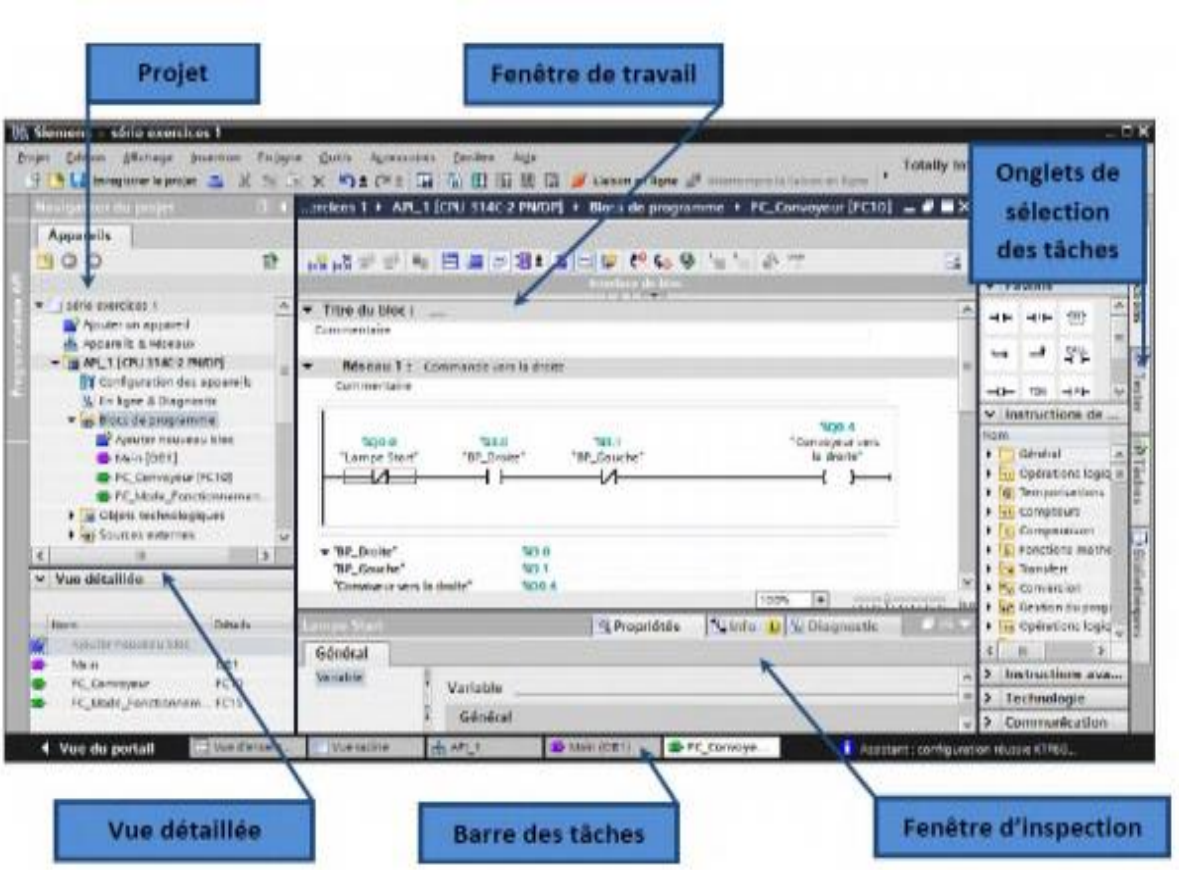


Figure IV.2: *exemple de « vu du projet ».*

- **La fenêtre de travail** qui permet de visualiser les objets sélectionnés dans le projet pour être traités. Il peut s'agir des composants matériels, des blocs de programme, des tables des variables, des HMI,…
- **La fenêtre d'inspection** Qui permet de visualiser des informations complémentaires sur un objet sélectionné ou sur les actions en cours d'exécution (propriété du matériel sélectionné, messages d'erreurs lors de la compilation des blocs de programme,…).
- **Les onglets de sélection de tâches**

Ce sont des contenus qui varient en fonction de l'objet sélectionné (configuration matérielle, bibliothèques des composants, bloc de programmes, instructions de programmation). Cet environnement de travail contient énormément de données. Il est possible de masquer ou réduire certaines de ces fenêtres lorsque l'on ne les utilise pas. Il est également possible de redimensionner, réorganiser, désancrer les différentes fenêtres.

IV.2.3 Win CC sur TIA portal [32]

C'est un logiciel d'ingénierie pour la configuration de pupitres SIMATIC, de PC industriels SIMATIC et de PC standard par le logiciel de visualisation. Le SIMATIC Win CC dans le TIA Portal fait partie d'un nouveau concept d'ingénierie intégré qui offre un environnement d'ingénierie homogène pour la programmation et la configuration de solutions de commande, de visualisation et d'entraînement. C'est le logiciel pour toutes les applications IHM allant de solutions de commande simples avec des Basic Panels aux applications SCADA pour systèmes multipostes basés sur PC.

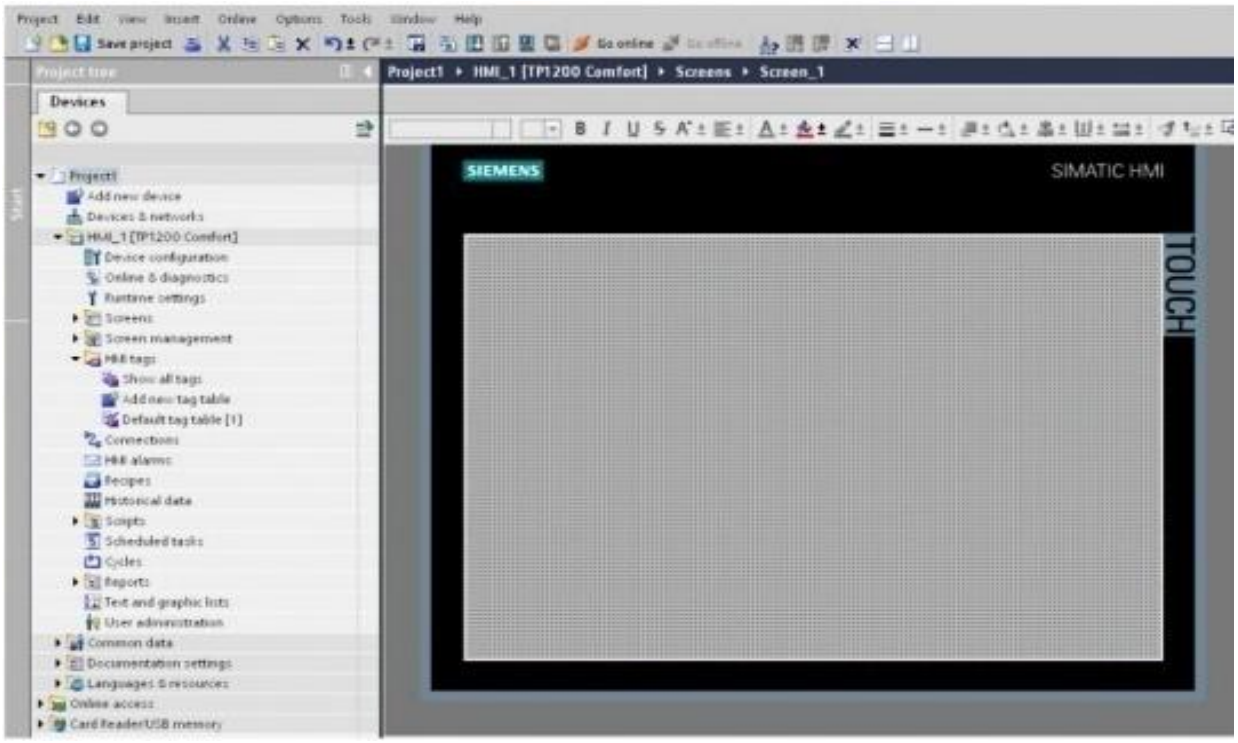


Figure IV.3: *Vue du Win CC dans TIA portal*.

IV.3 Architecture SCADA pour l'ouvrage ROB1 de SONATRACH [2]

L'oléoduc OB1 est l'ouvrage de transport par canalisation de Haoud-El-Hamra jusqu'au terminal marin de Bejaia ,tel toutes les station de pompage contrôlant ce pipe a son architecture propre qui comporte un réseau LAN, des postes HMI ,des postes interne , des RTU ; la transmission de données numériques à haut débit principalement sur fibre optique se fais par des lieux SDH(Synchronous Digital Hierarchy). Nous présentons ci-après l'architecture globale SCADA pour la supervision de ce pipe.

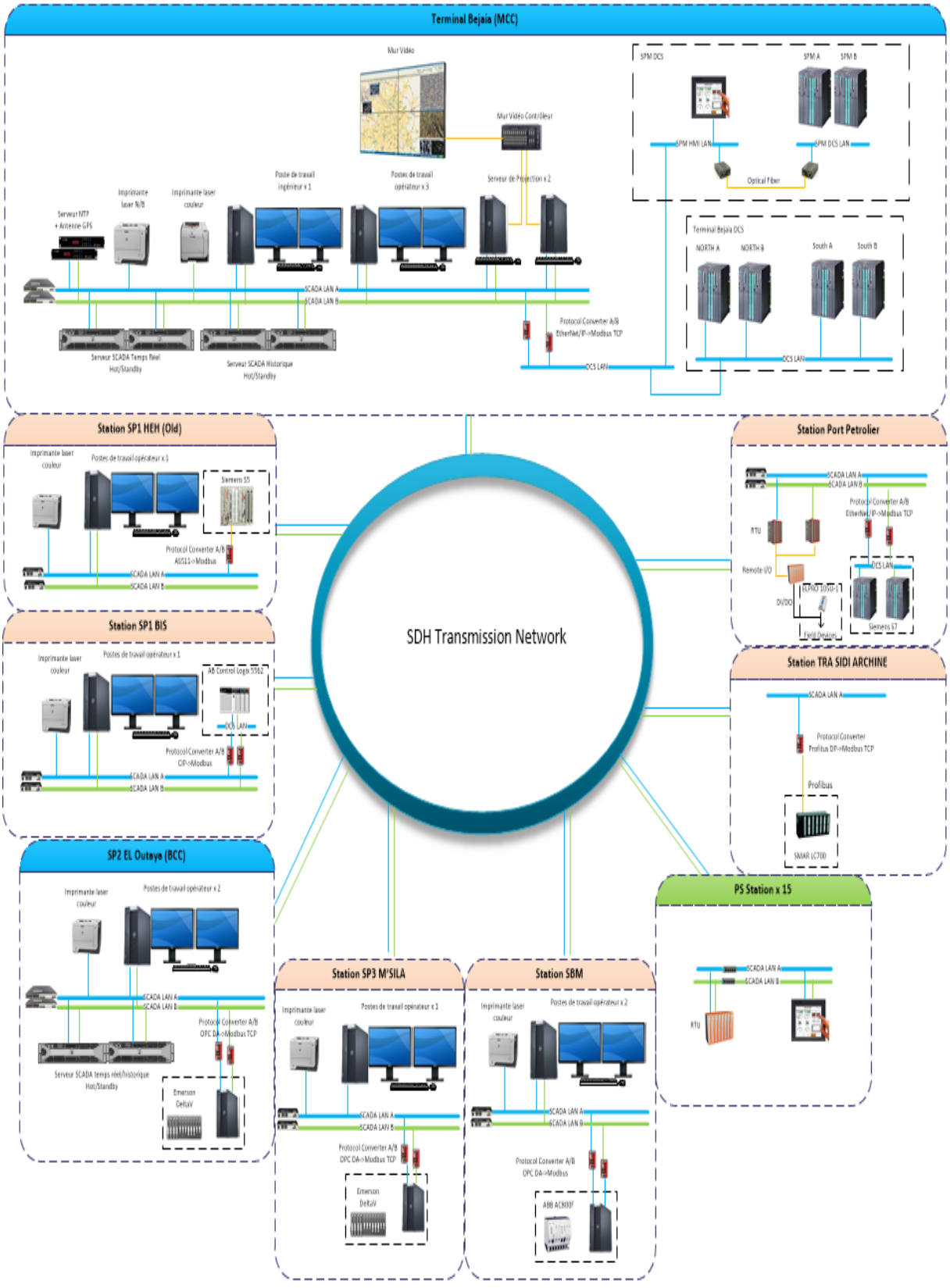
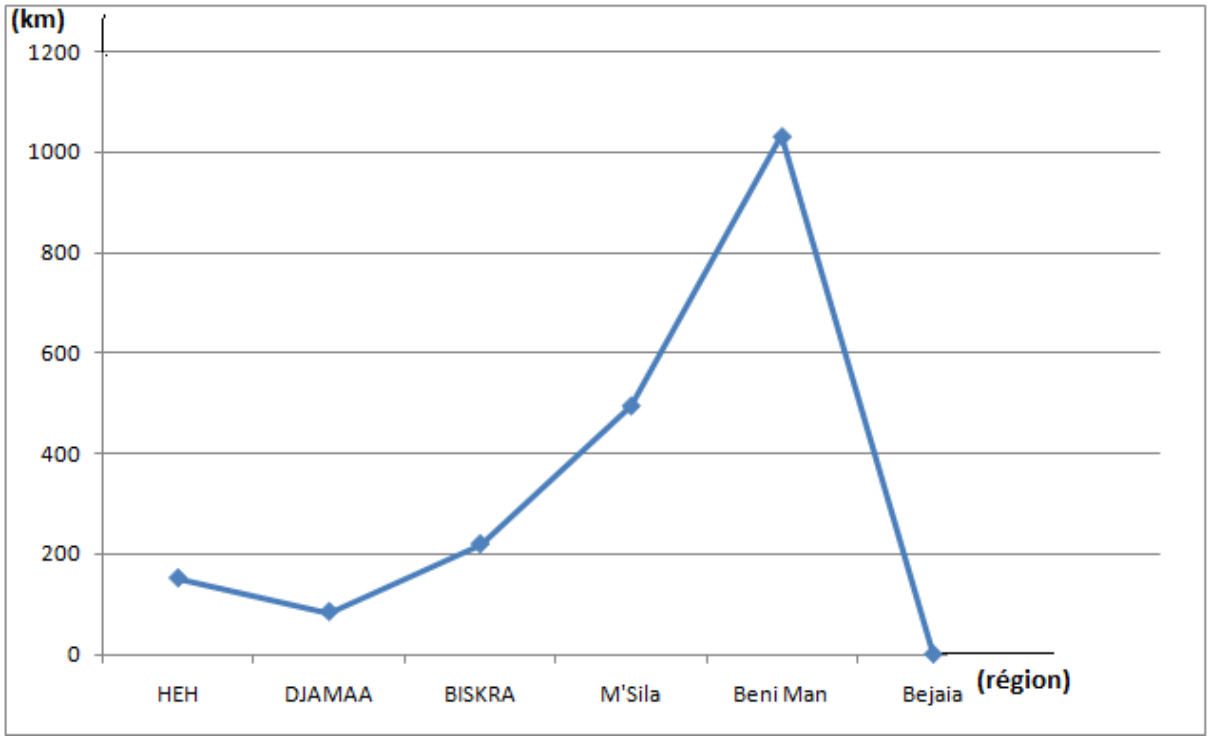


Figure IV.4: *Architecture d'un environnement SCADA de l'ouvrage ROB1.*

IV.4 Supervision de l'ouvrage ROB1-SP3 M'Sila-SP3-Bejaia

Notre projet consiste à visualiser les paramètres d'exploitation de la ligne (débit et pression) du pipe de l'OB1 de M'Sila ou terminal arrivée Bejaia, car ce dernier il suit un chemin qui est caractérisé par des altitudes déférentes, qui sont montrés dans la courbe suivant :



Le chemin de L'OB1 à trévère les stations de pompage

IV.4.1 Création

Dans cette suite, nous allons d'écrire et tester notre proposition de supervision d'un partie du pipe OB1 allant de la station de pompage SP3-M'Sila j'jusqu'au terminale arrivée à Bejaia. Cette simulation est décrite par étapes :

- Création du projet
- Sécurisation des accès au réseau du projet
- La configuration du PLC
- Les tests

Pour commencer nous avons ouvert le logiciel puis nous sommes aller dans la liste des action a fin de crée notre projet, ensuit nous rentrés dans la fenêtre de sélection , c'est la qu'on a ajouté les appareils nécessaires (PLC et IHM) et on les a lié pour crée un réseau, et ce

dernier permettant le transport des données du PLC vers IHM dans le but de les visualiser comme le montre la figure suivant :

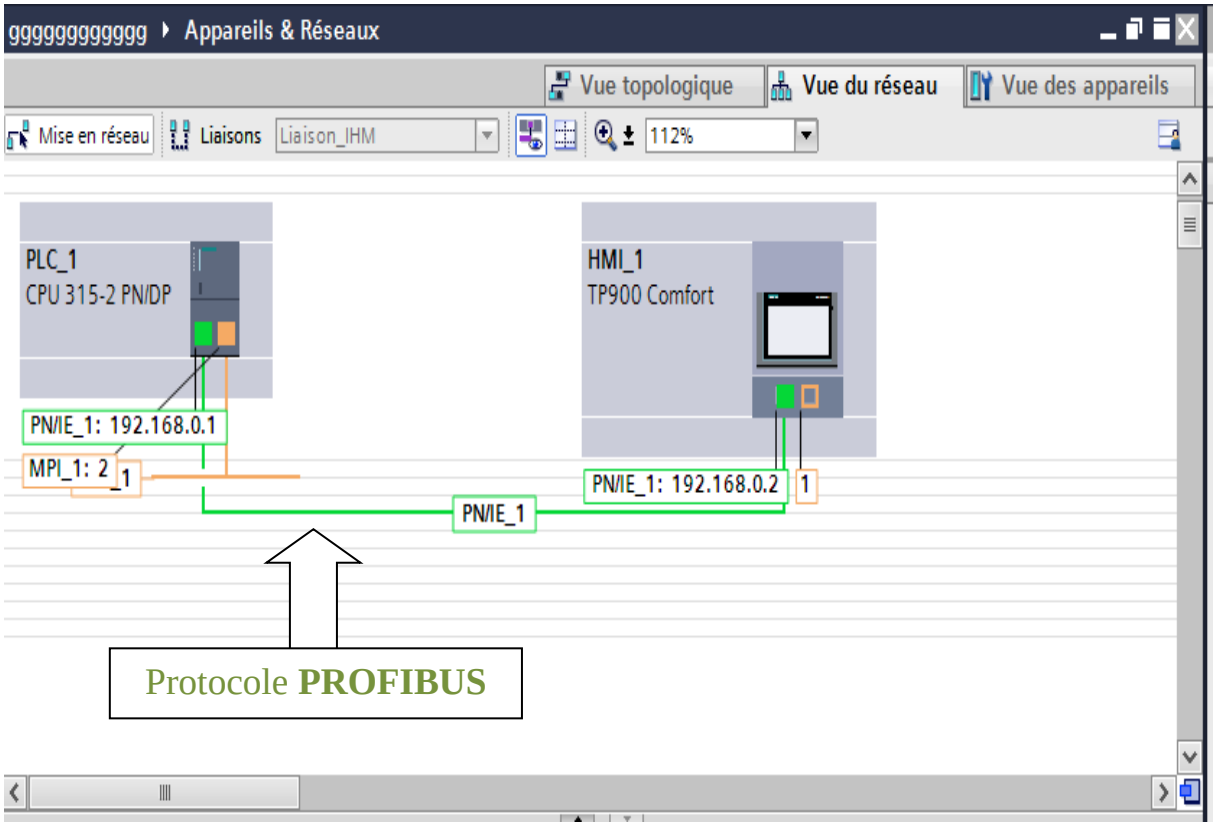
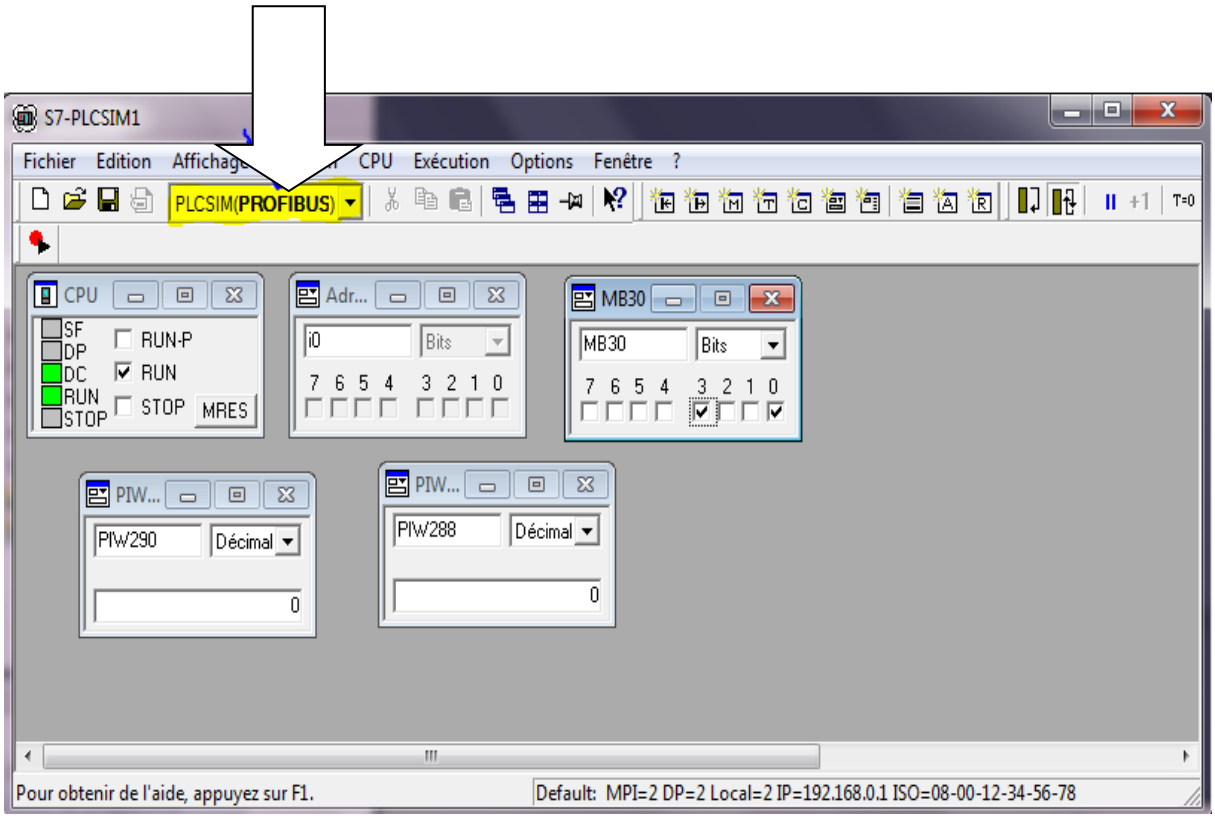


Figure IV.5 : *Appareils et réseaux.*

Suite à la nécessité d'envoyer et de recevoir des données jugées critiques généralement pour de longues distances et en temps réel dans un environnement SCADA, on fait appel aux protocoles de communications et dans notre environnement SCADA on à utilisé le protocole **PROFIBUS** comme le montre l'image suivant :



IV.4.2 La Sécurisation du réseau

La sécurisation du réseau de communication de notre projet SCADA est faite par une identification des équipements du réseau par adressage IP.

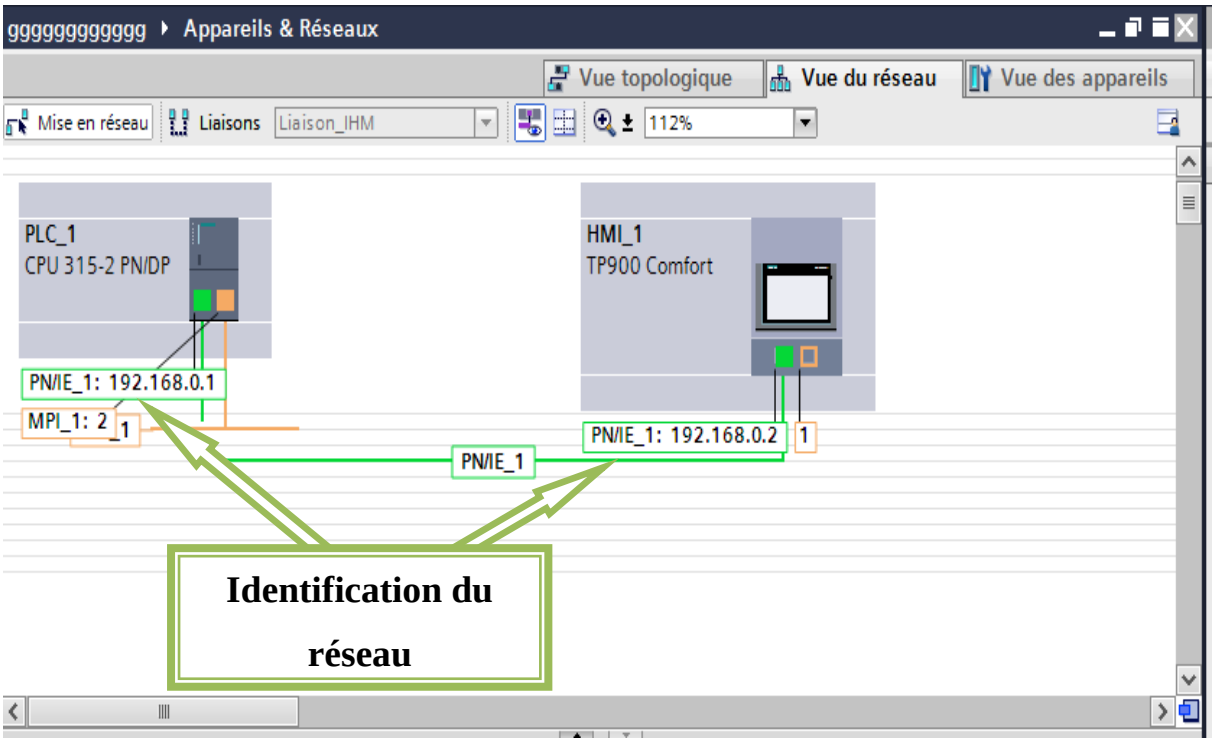


Figure IV.6: *Sécurité de notre réseau SCADA*

IV.4.3 Configuration du PLC

Dans ce qui suit nous allons décrire brièvement et montré les déférentes étapes de configuration pour le PLC de notre système.

IV.4.3.1 Création des entités et des alarmes

Dans cette partie nous avons crée six (6) pacs de stockage chacun est répartie en 2 parties : une partie gaz et une partie pétrole pour chacune des stations de pompage (M'Sila, Beni Mansour, Bejaia), doté d'une vanne et d'une alarme pour chacune des parties gaz et pétrole

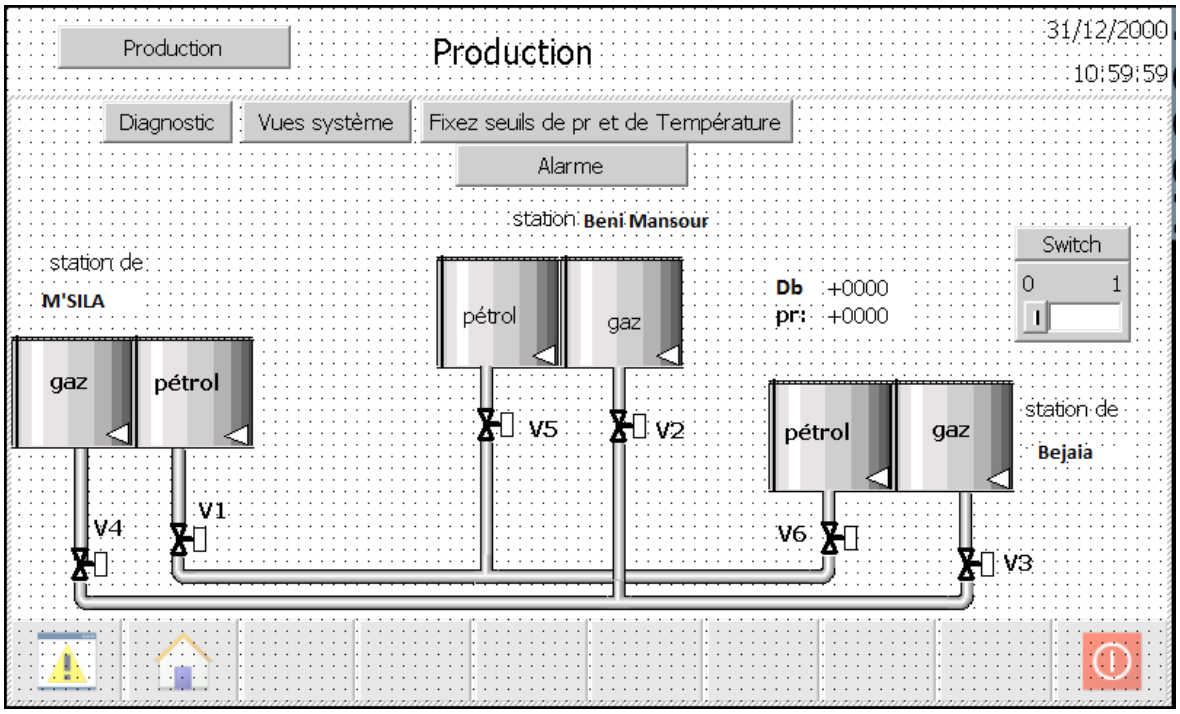


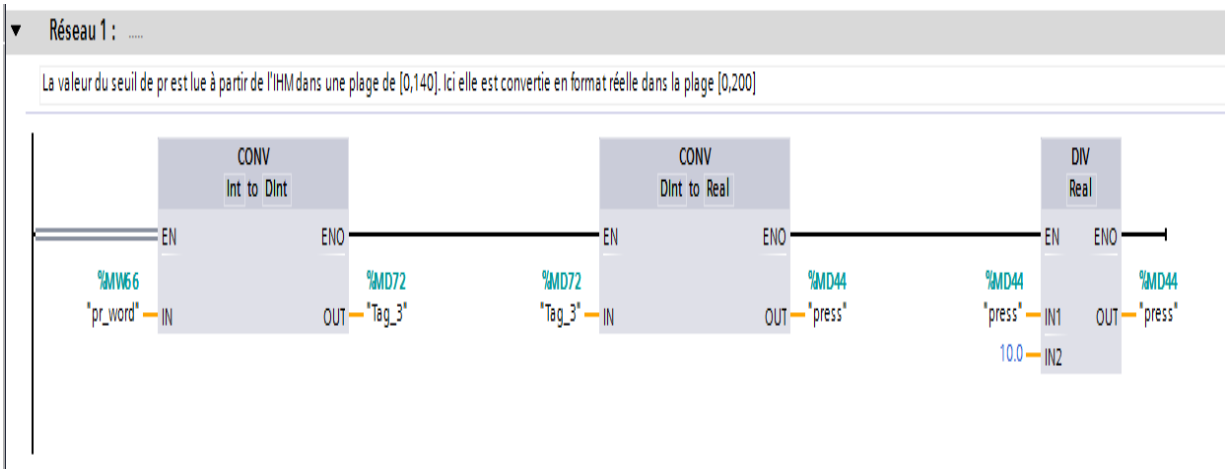
Figure IV.7: *création des entités du projet.*

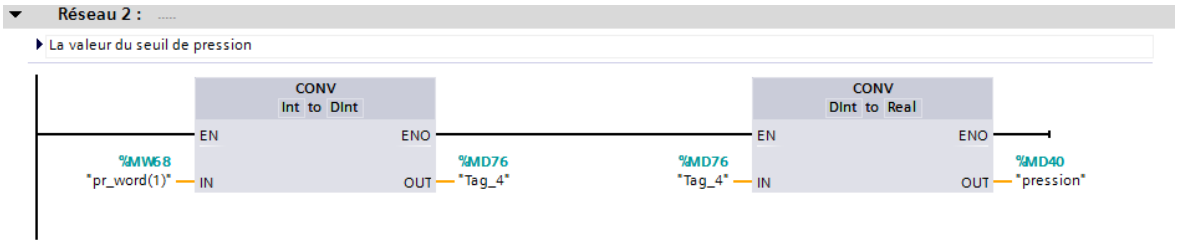
IV.4.3.2 La programmation Step7

Dans cette partie, nous allons crée des programmes Step7 :

- **Bloc OB1:**

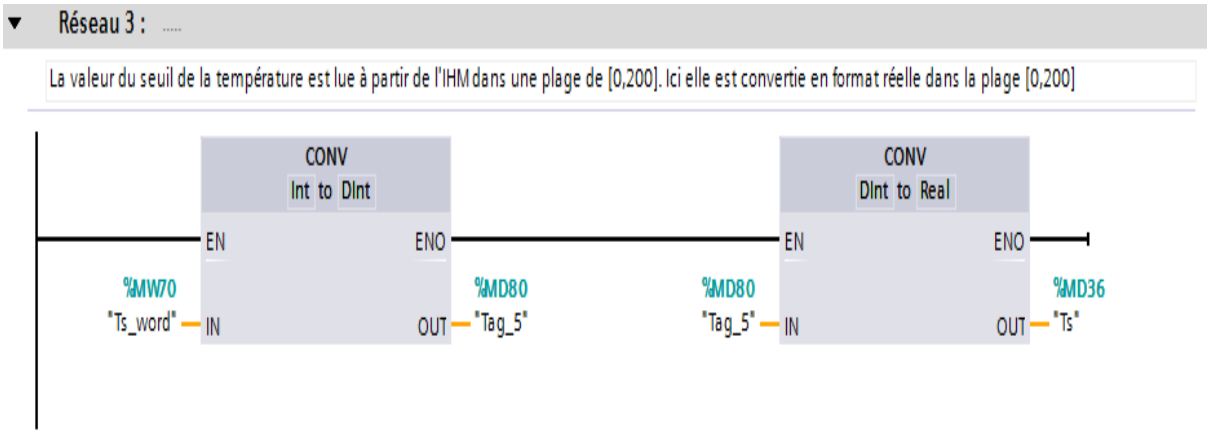
Un OB est appelé cycliquement par le système d'exploitation et constitue donc l'interface entre le programme utilisateur et le système d'exploitation. L'OB contient des instructions d'appels de blocs indiquant à l'unité de commande de l'automate l'ordre dans lequel il doit traiter les blocs.





La programmation manuelle de la valeur du seuil de la pression sur l'IHM et la conversion

de la valeur de cette dernière d'un entier vers un nombre réel (Ps).



La programmation manuelle de la valeur du seuil de la température sur l'IHM et la conversion de la valeur de cette dernière d'un entier vers un nombre réel (Ts).

➢ Grafcet

(Graphe Fonctionnel de Commande Étape / Transition) .C'est un outil graphique de description des comportements d'un système logique. Il est très utilisé pour la programmation des automates programmables industriels (API). Il est composé d'étapes, de transitions et de liaisons.

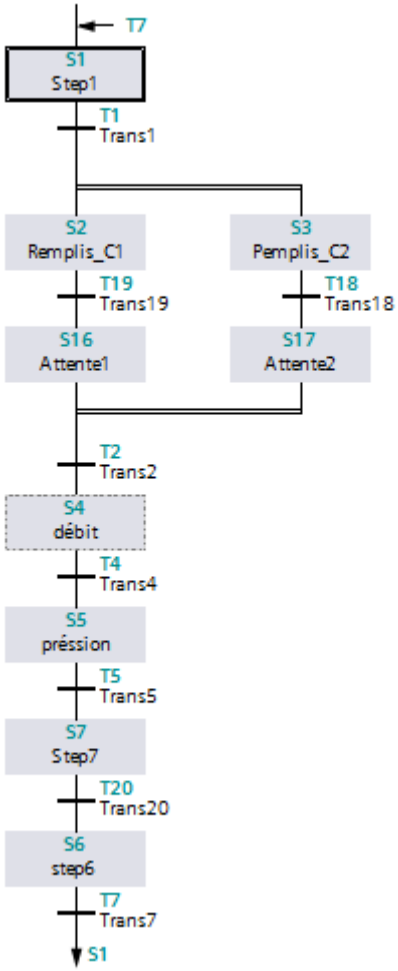
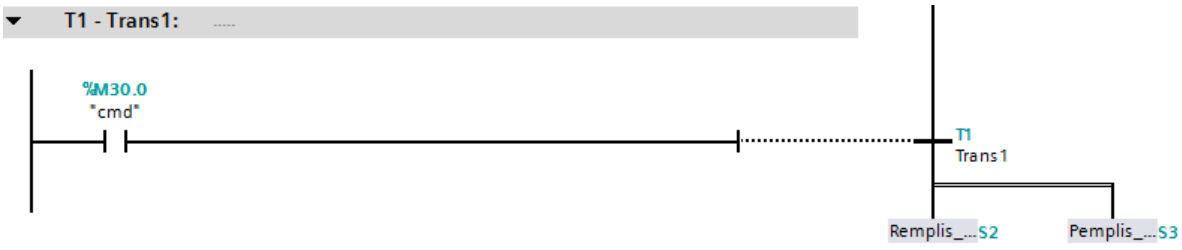
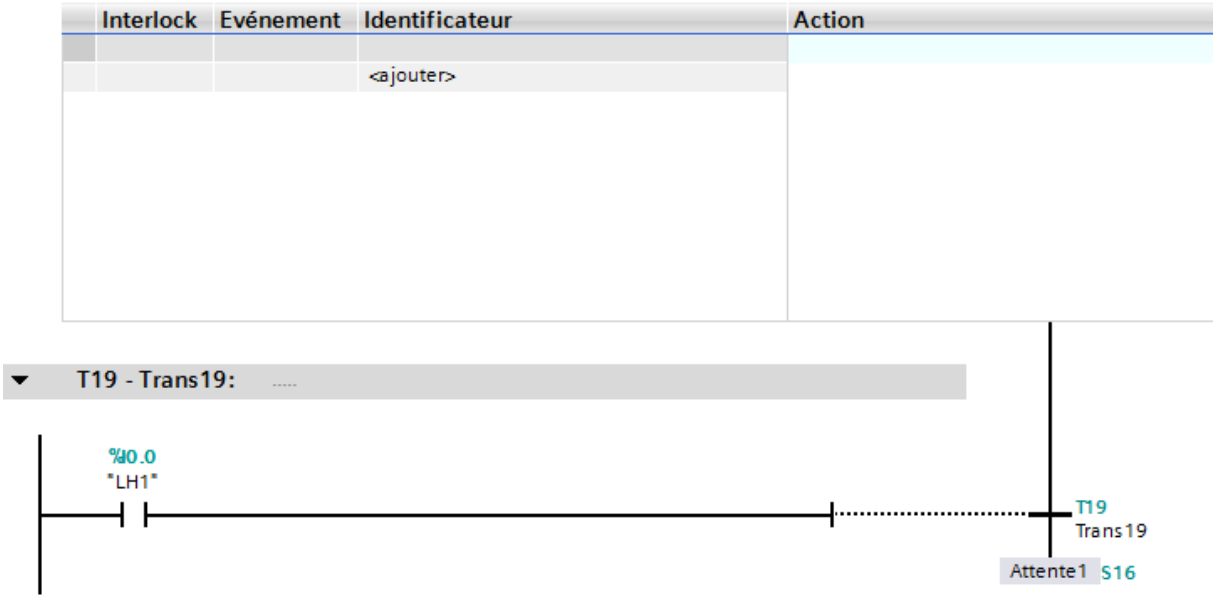


Figure IV.8: *Grafcet.*

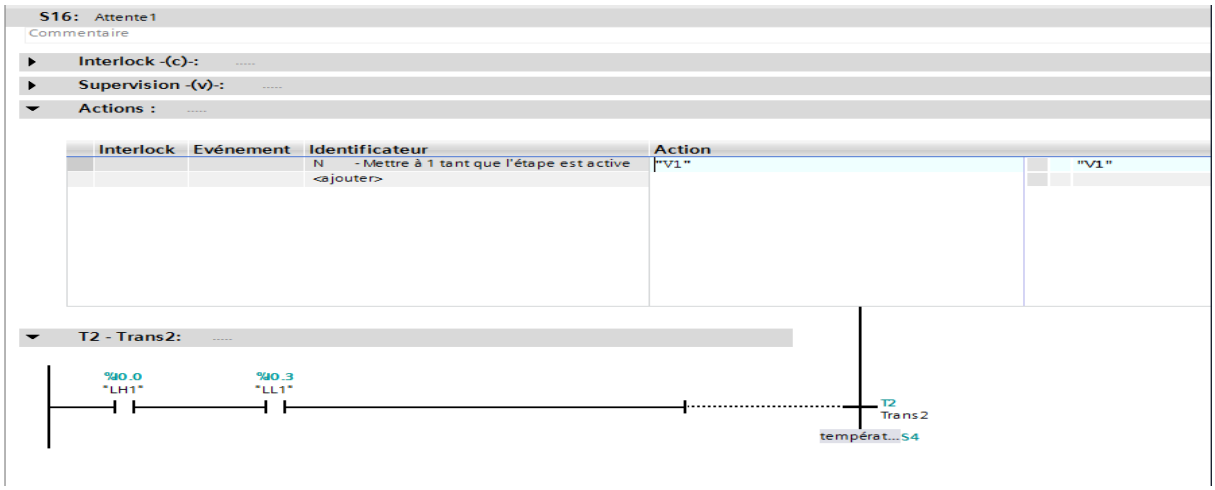
➢ Programmation des blocs :



Programme : nous avons inséré une commande de démarrage de Switch

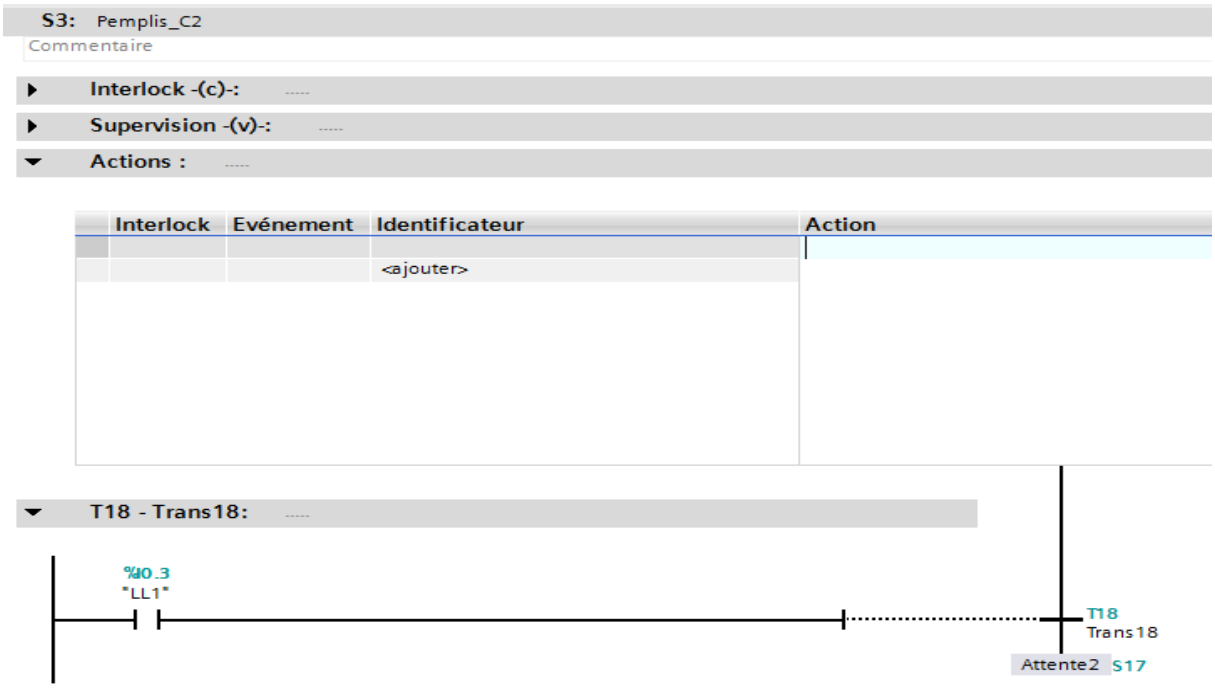


Programme : Nous avons programmé l'alarme LH1 pour détecter le pompage du pétrole.

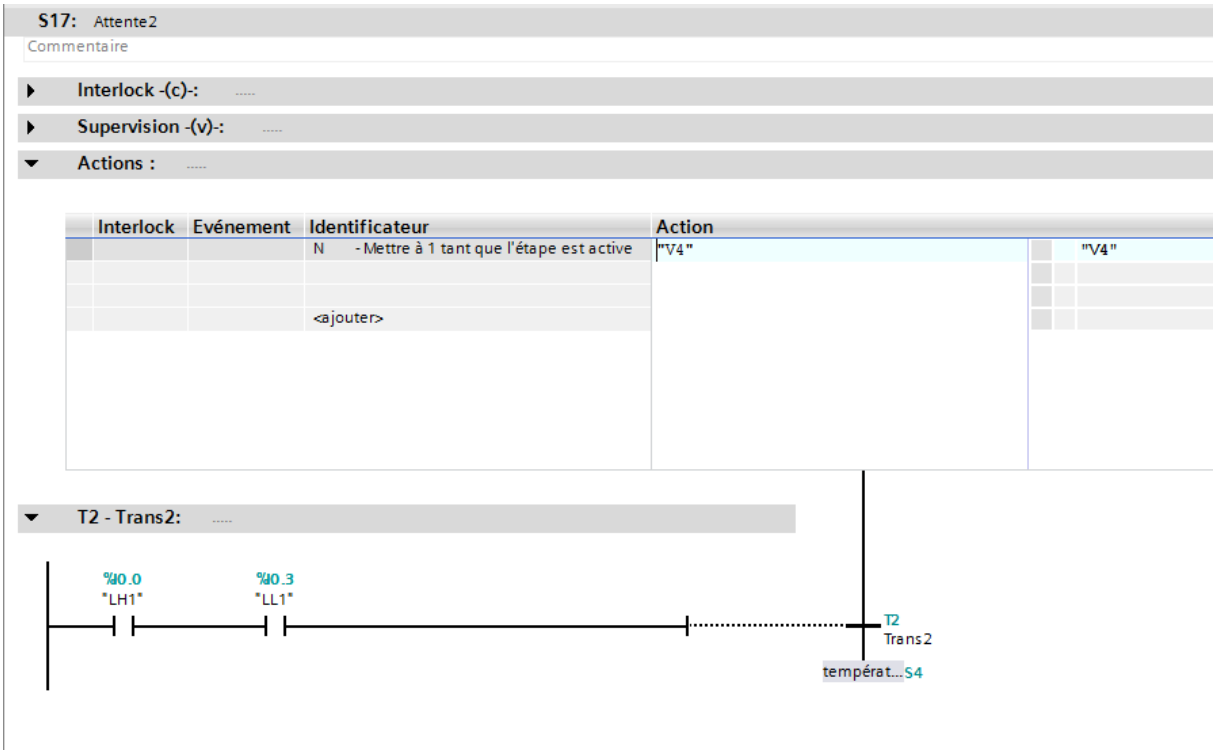


Programme : Nous avons inséré une condition si LH1et LL1 sont détecter la vanne V1 s'ouvre

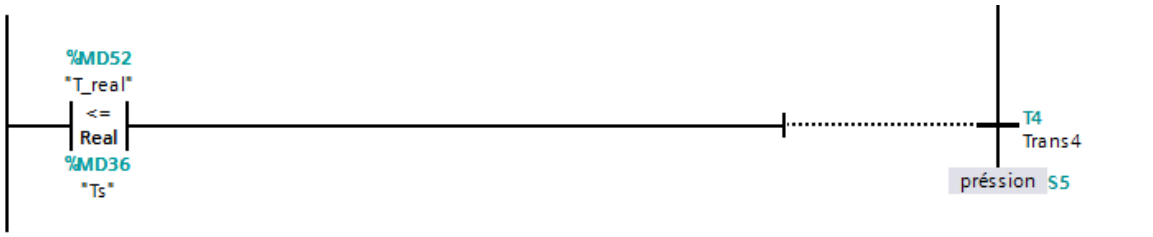
.



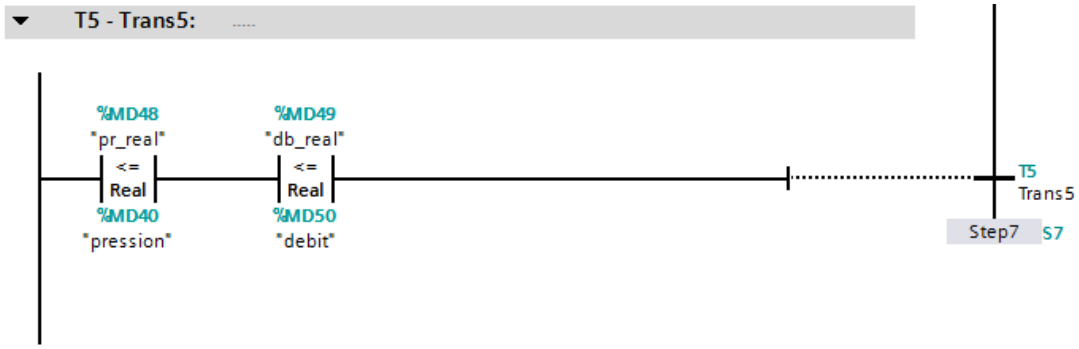
Programme : Nous avons programmé l'alarme LL1 pour détecter le pompage du gaz.



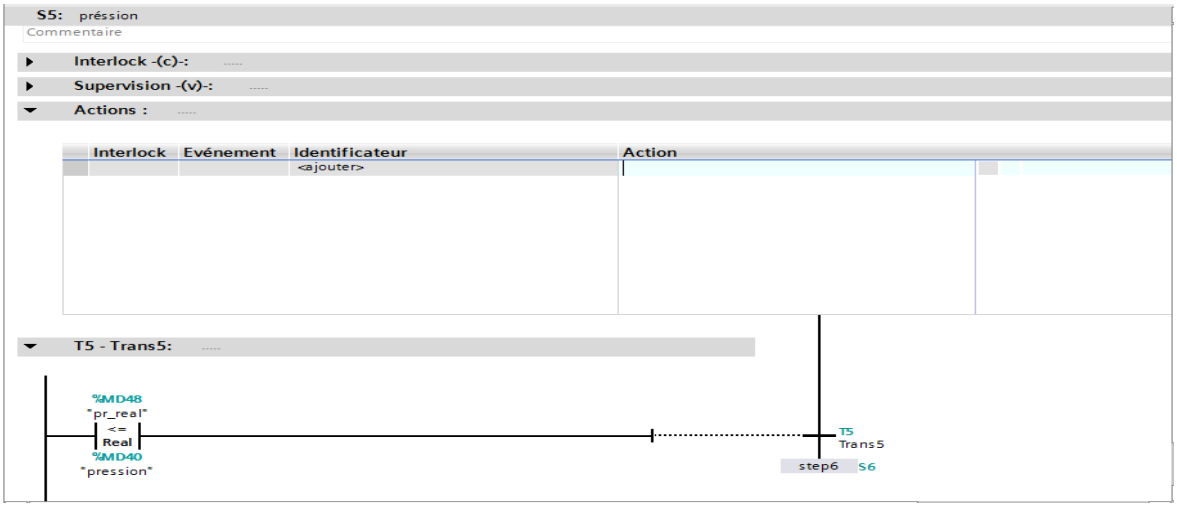
- **Programme :** nous avons inséré une condition si LH1 etLL1 sont détectés la vanne V4 s'ouvre**.**

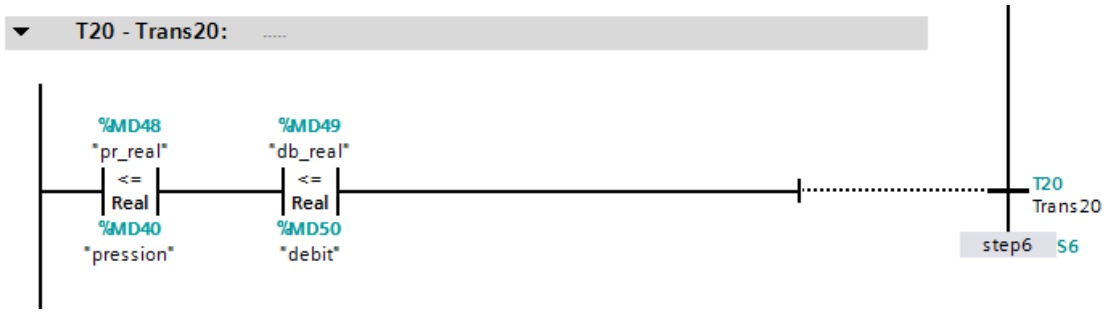


Programme : nous avons inséré la condition du débit (Ts>=T_real) si la condition est satisfaite on aura l'activation de V1 et V4.

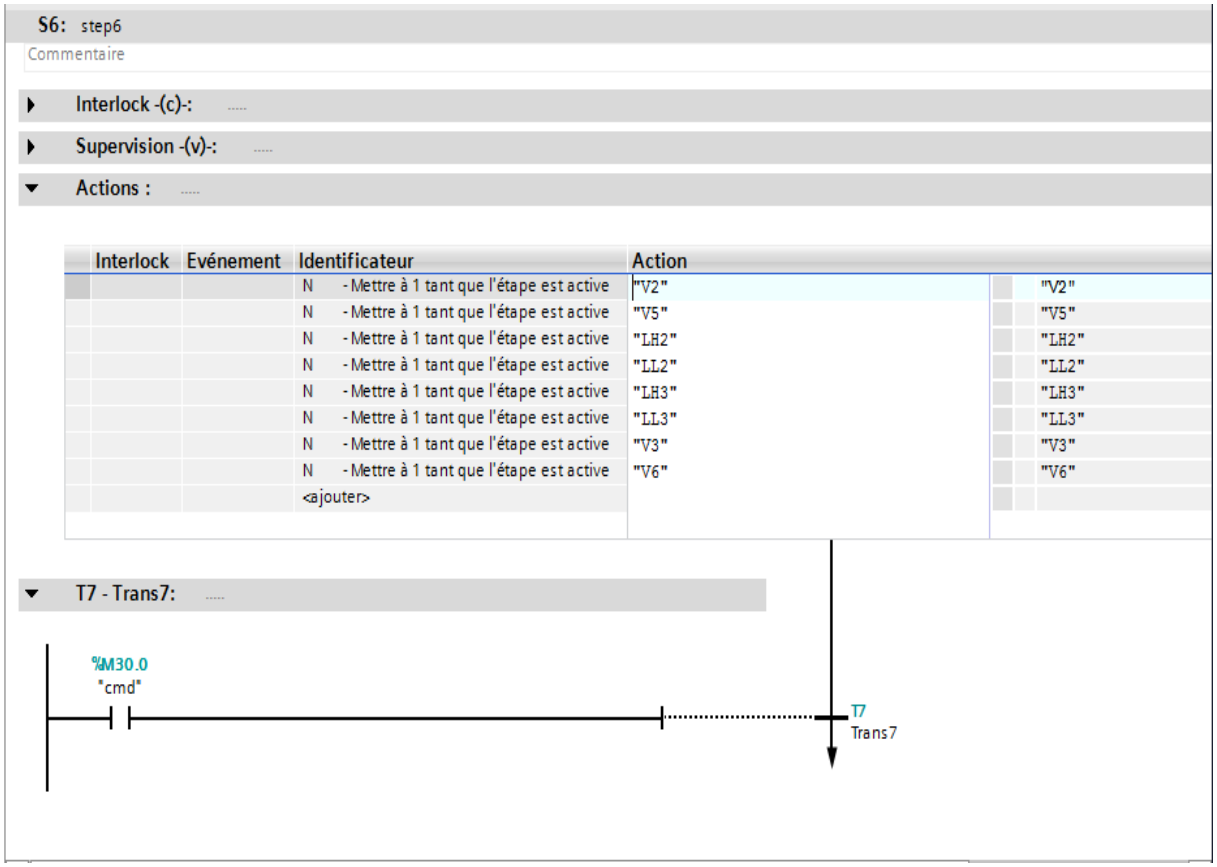


Programme : nous avons inséré insertion la condition de la pression et du débit (Ps>=Pr_real) et (Dbi>=Db-real) si la condition est satisfaite on aura l'activation de V1 et V4**.**





.



- **Programme :** nous avons implémenté une instruction afin de régénèré le système et cela on active V2, V5, V3, V6 et LH1, LL2, LH3, LL3**.**

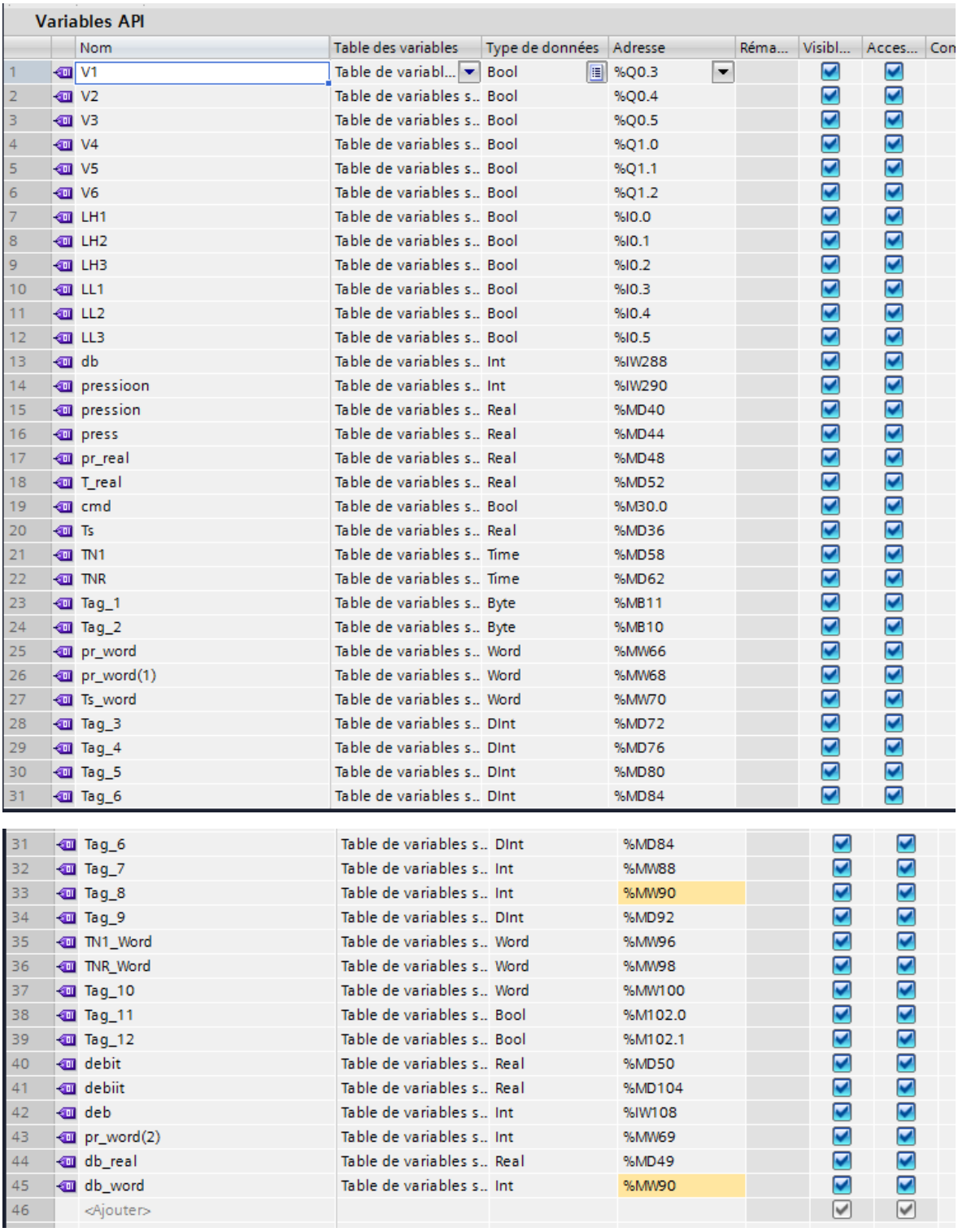
IV.4.3.3 La table de variable api

Nous avons programme dans le GRAFCET l'emplacement des deux premières alarmes (LH1 et LL2) :

LH1: i (0 ; 0).

LL2 : i (0 ; 3).

Le reste des variables seront placé d'une façon automatique comme le représente la figure suivante :



Variables API

	Nom	Table des variables	Type de données	Adresse	Réma...	Visibl...	Acces...	Con
1	V1	Table de variabl...	Bool	%Q0.3		☑	☑	
2	V2	Table de variables s..	Bool	%Q0.4		☑	☑	
3	V3	Table de variables s..	Bool	%Q0.5		☑	☑	
4	V4	Table de variables s..	Bool	%Q1.0		☑	☑	
5	V5	Table de variables s..	Bool	%Q1.1		☑	☑	
6	V6	Table de variables s..	Bool	%Q1.2		☑	☑	
7	LH1	Table de variables s..	Bool	%I0.0		☑	☑	
8	LH2	Table de variables s..	Bool	%I0.1		☑	☑	
9	LH3	Table de variables s..	Bool	%I0.2		☑	☑	
10	LL1	Table de variables s..	Bool	%I0.3		☑	☑	
11	LL2	Table de variables s..	Bool	%I0.4		☑	☑	
12	LL3	Table de variables s..	Bool	%I0.5		☑	☑	
13	db	Table de variables s..	Int	%IW288		☑	☑	
14	pressioon	Table de variables s..	Int	%IW290		☑	☑	
15	pression	Table de variables s..	Real	%MD40		☑	☑	
16	press	Table de variables s..	Real	%MD44		☑	☑	
17	pr_real	Table de variables s..	Real	%MD48		☑	☑	
18	T_real	Table de variables s..	Real	%MD52		☑	☑	
19	cmd	Table de variables s..	Bool	%M30.0		☑	☑	
20	Ts	Table de variables s..	Real	%MD36		☑	☑	
21	TN1	Table de variables s..	Time	%MD58		☑	☑	
22	TNR	Table de variables s..	Time	%MD62		☑	☑	
23	Tag_1	Table de variables s..	Byte	%MB11		☑	☑	
24	Tag_2	Table de variables s..	Byte	%MB10		☑	☑	
25	pr_word	Table de variables s..	Word	%MW66		☑	☑	
26	pr_word(1)	Table de variables s..	Word	%MW68		☑	☑	
27	Ts_word	Table de variables s..	Word	%MW70		☑	☑	
28	Tag_3	Table de variables s..	DInt	%MD72		☑	☑	
29	Tag_4	Table de variables s..	DInt	%MD76		☑	☑	
30	Tag_5	Table de variables s..	DInt	%MD80		☑	☑	
31	Tag_6	Table de variables s..	DInt	%MD84		☑	☑	
31	Tag_6	Table de variables s..	DInt	%MD84		☑	☑	
32	Tag_7	Table de variables s..	Int	%MW88		☑	☑	
33	Tag_8	Table de variables s..	Int	%MW90		☑	☑	
34	Tag_9	Table de variables s..	DInt	%MD92		☑	☑	
35	TN1_Word	Table de variables s..	Word	%MW96		☑	☑	
36	TNR_Word	Table de variables s..	Word	%MW98		☑	☑	
37	Tag_10	Table de variables s..	Word	%MW100		☑	☑	
38	Tag_11	Table de variables s..	Bool	%M102.0		☑	☑	
39	Tag_12	Table de variables s..	Bool	%M102.1		☑	☑	
40	debit	Table de variables s..	Real	%MD50		☑	☑	
41	debiit	Table de variables s..	Real	%MD104		☑	☑	
42	deb	Table de variables s..	Int	%IW108		☑	☑	
43	pr_word(2)	Table de variables s..	Int	%MW69		☑	☑	
44	db_real	Table de variables s..	Real	%MD49		☑	☑	
45	db_word	Table de variables s..	Int	%MW90		☑	☑	
46	<Ajouter>					☑	☑	

Figure IV.9: *présentation de la table des variables API.*

IV.4.4 Les tests

Une foi la programmation de tous les blocs terminée, nous allons visualiser tous les équipements de la station, les alarmes qui sont en marche et celles qui sont à l'arrêt, les vannes qui sont ouvertes et celles qui sont fermées telle que :

- Alarme en vert ⇨ ouvrir la vanne.
- Alarme en blanc ⇨ fermé la vanne.

Dans ce qui suit nous avons fixé la température a 25°C , le débit seuil et la pression seuil comme suit :

P seuil = 61 Bar.

Db seuil=1800 m^3 /h

T = 25°C.

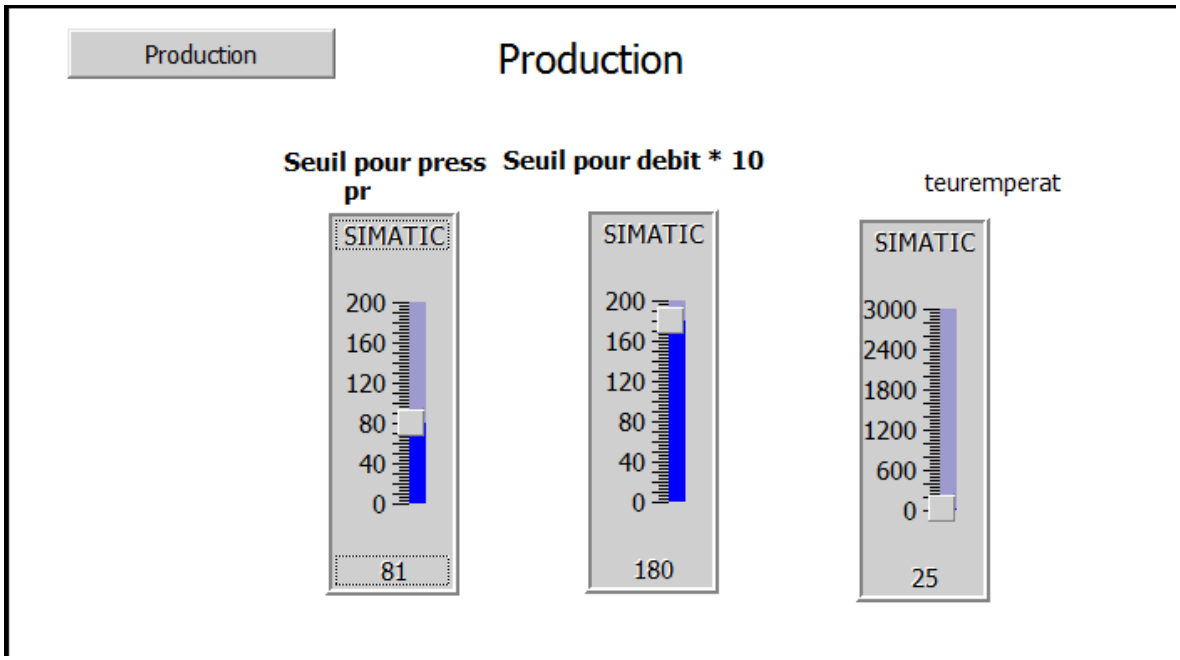


Figure IV.10 : *vue du seuil.*

Puis on va réaliser plusieurs testes et cela en variant le débit et la pressions :

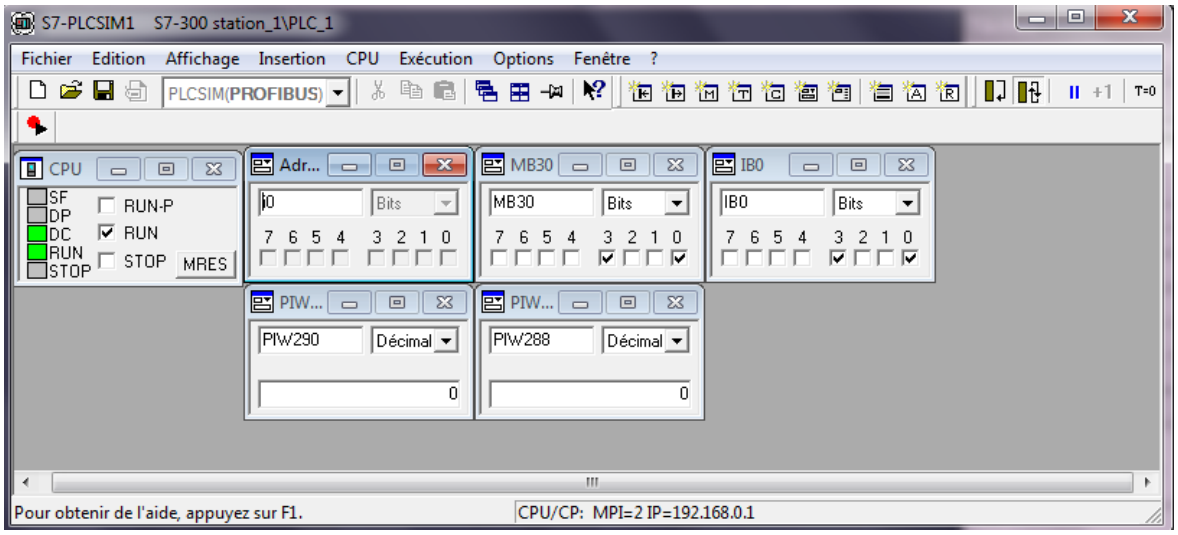
Et cela en introduisant la valeur de la pression et du débit qu'on désire simuler à l'aide de S7-PLCSIM telle que :

P= (27648*Pi)/200

Db= (27648*Dbi)/200

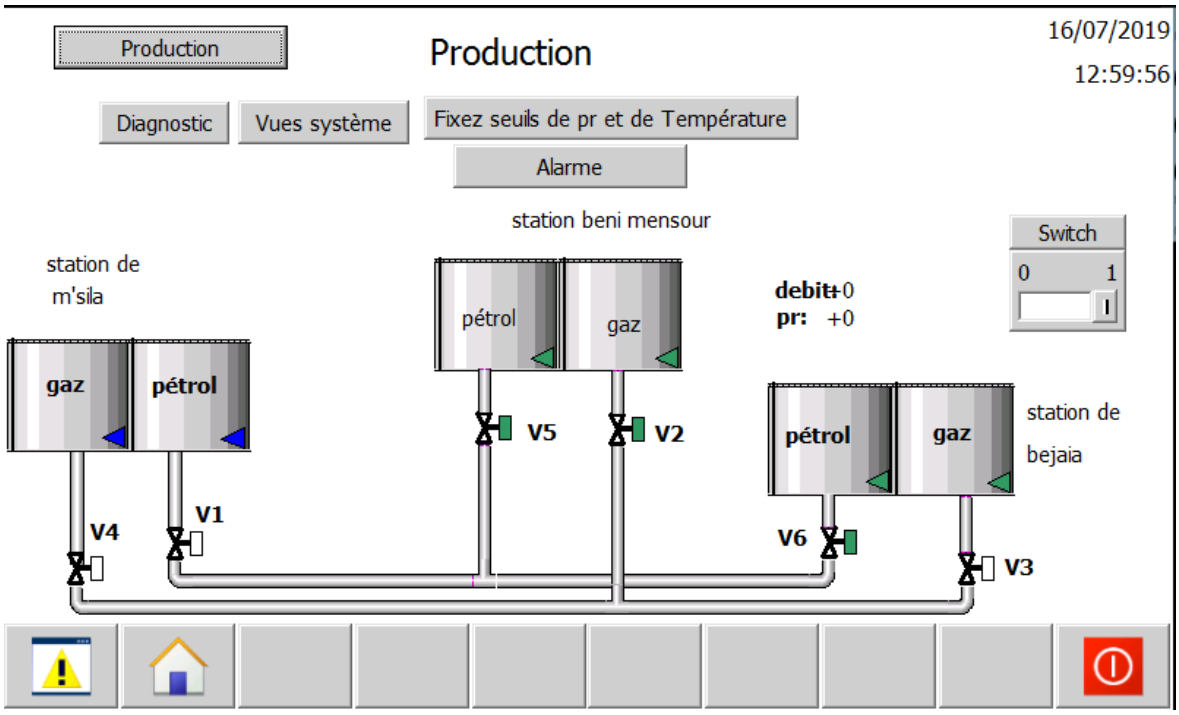
Tq: Ti et Pi c'est la valeur que nous voulons simuler

- **Db=0 m^3 /h , P=0bar :**



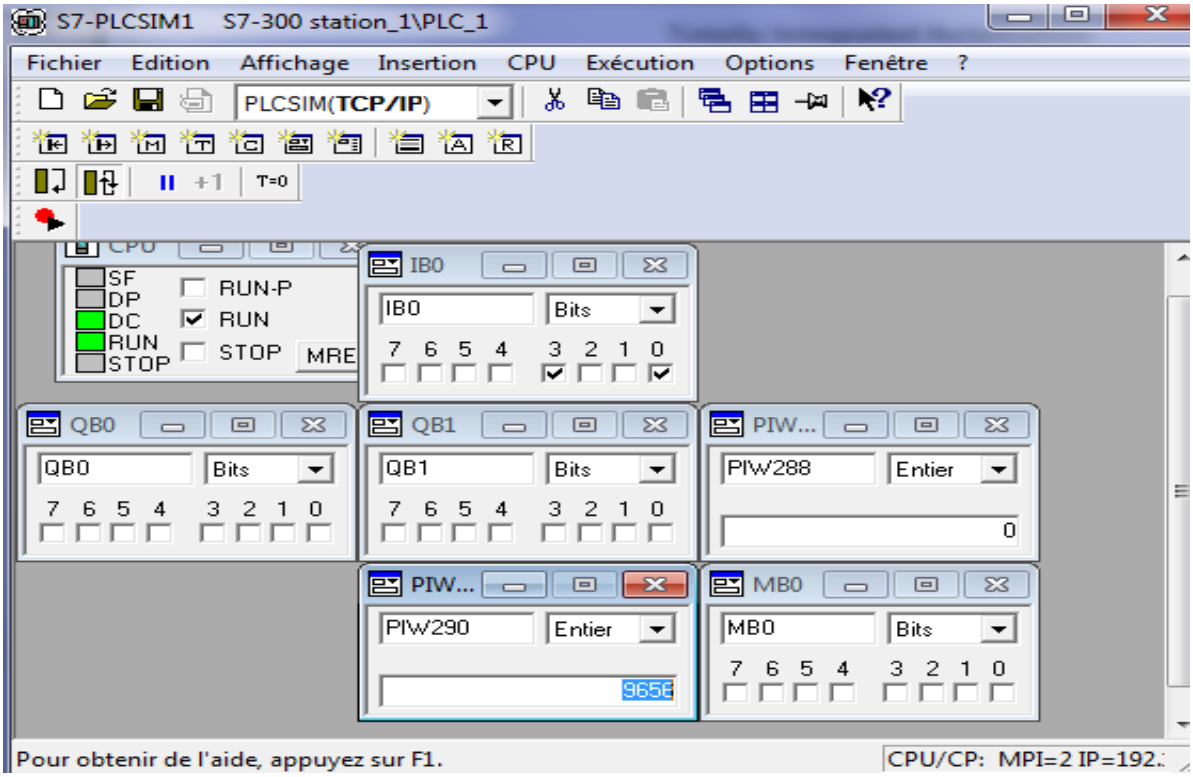
- **Après l'activation du Switch**

Nous avons activé le Switch pour lancer le fonctionnement du système

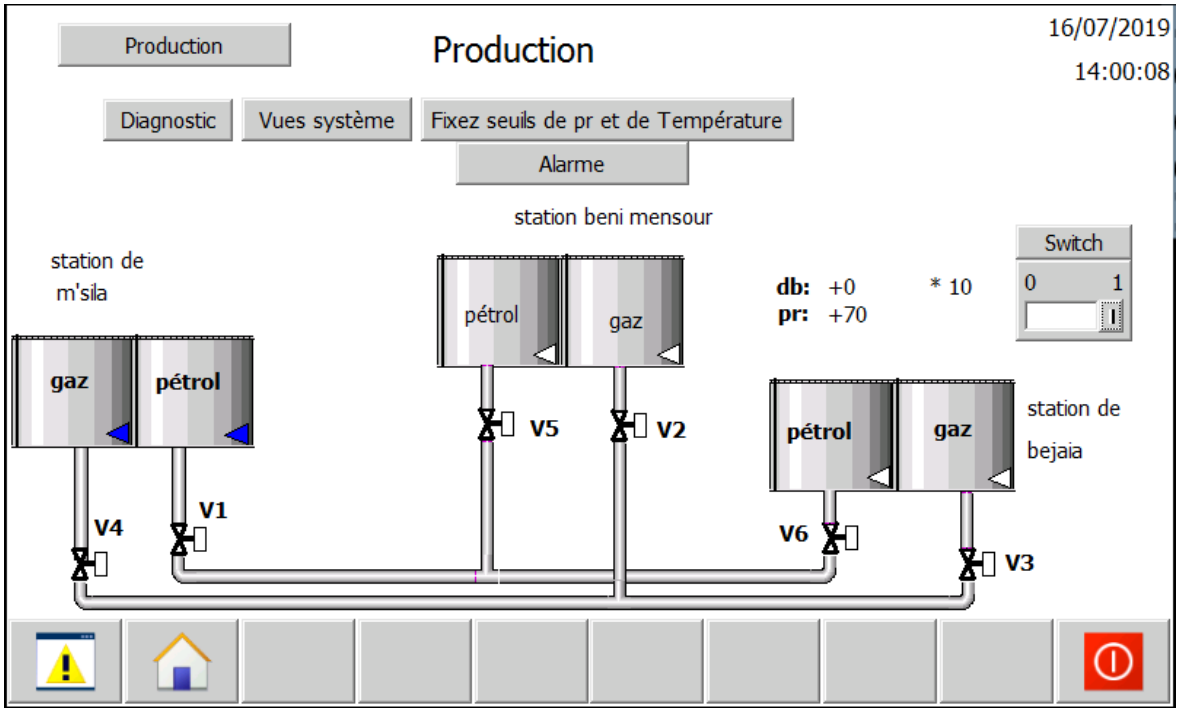


Commentaire : les deux paramètres sont inferieurs au seuil alors la détection d'alarme est en vert le systèmes marche normalement.

- **Db=0 m^3 /h, P=70bar :**

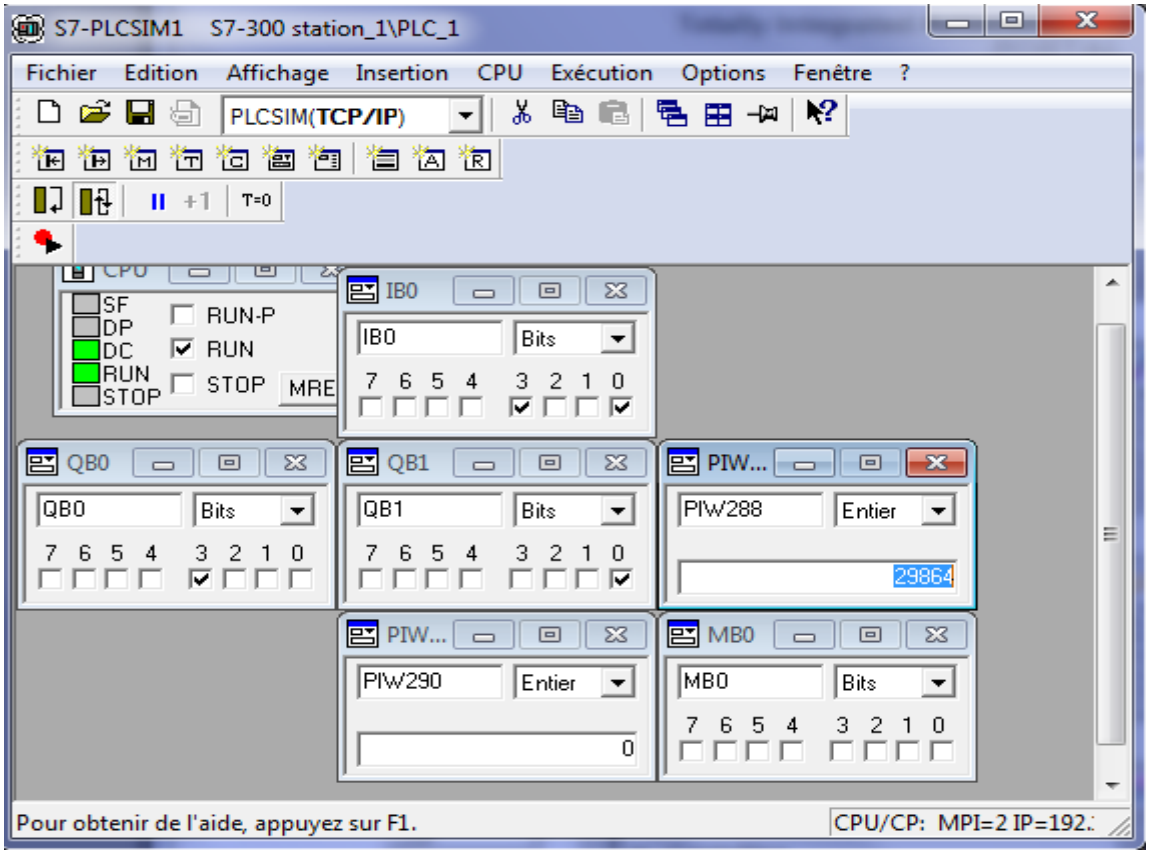


- **Après l'activation du Switch**

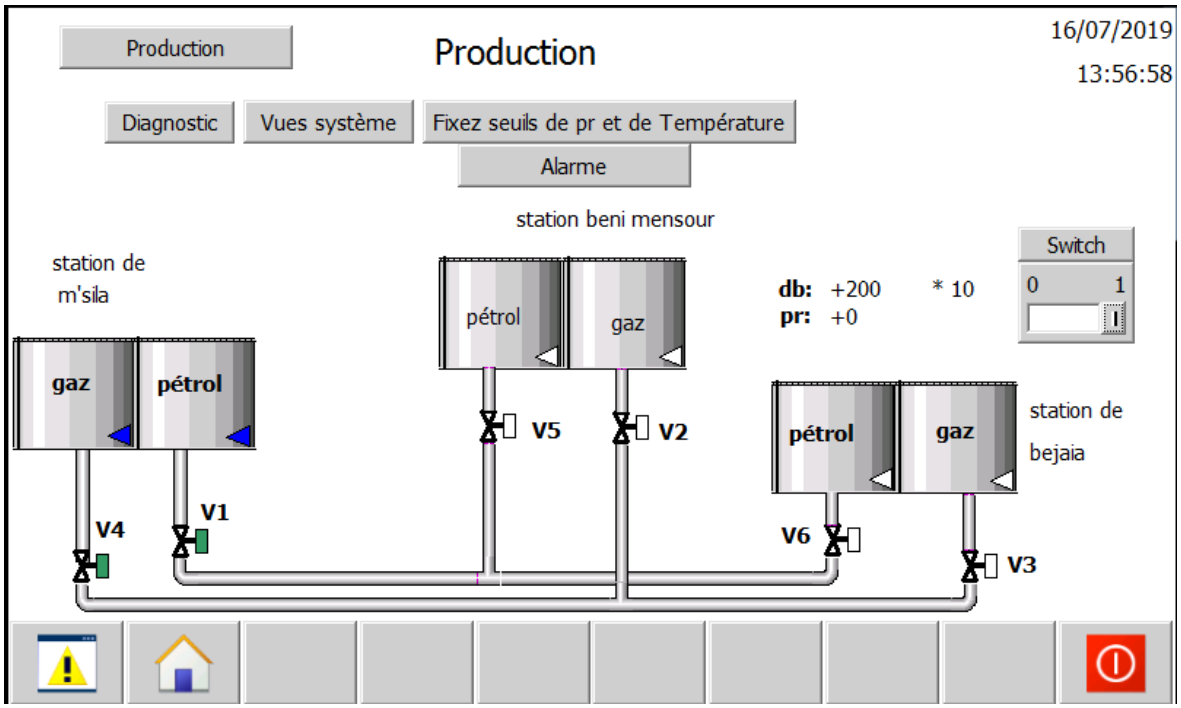


Commentaire : une fois l'un des deux paramètres (la pression) dépasse le seuil fixé, y'as une détection d'alarme (blanc) les vannes se ferment automatiquement.

- **Db=2000 m^3 /h, P=0bar**

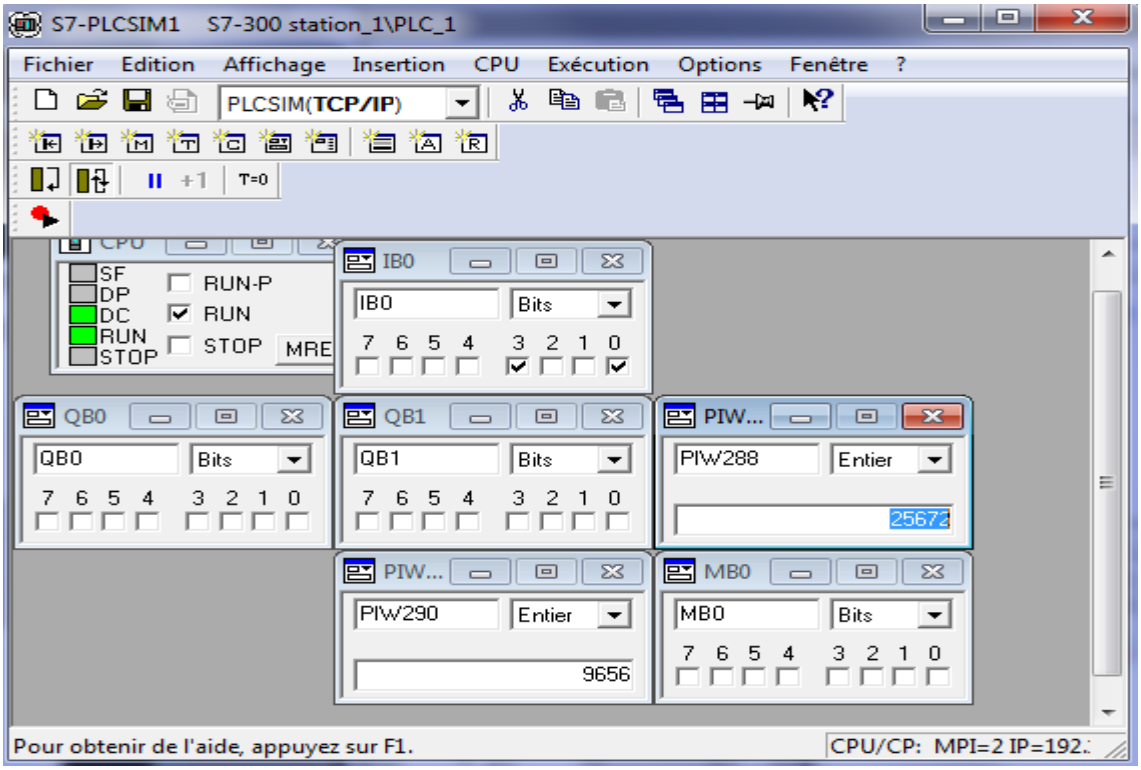


- **Après l'activation du Switch**

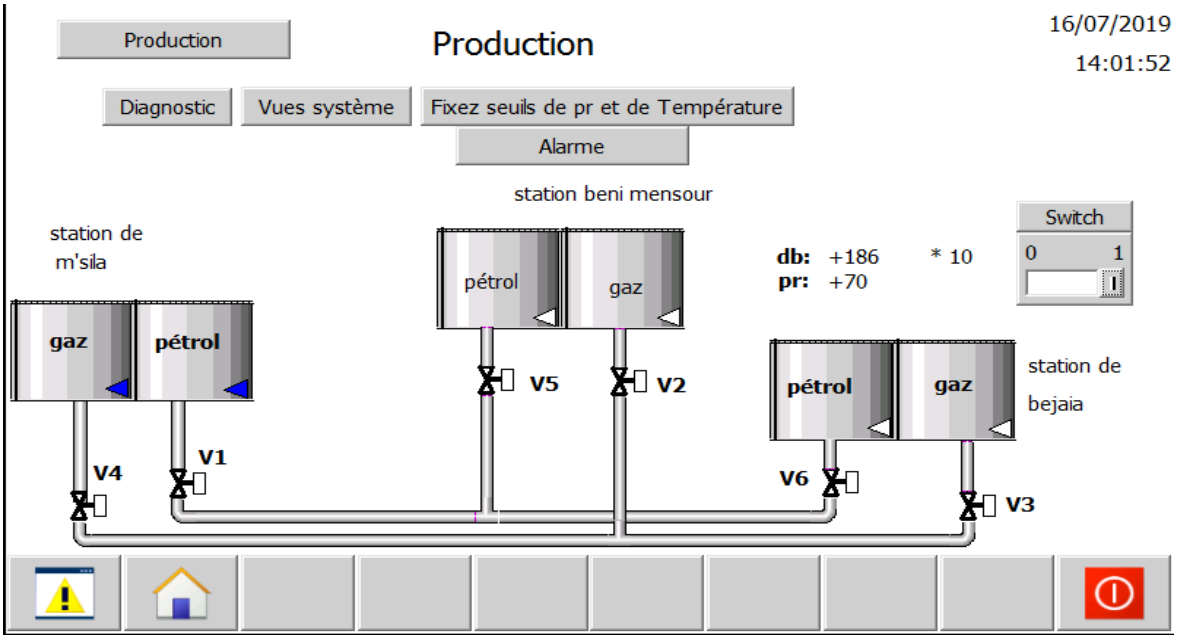


Commentaire : une fois l'un des deux paramètres dépasse le seuil fixé (le débit), y'as une détection d'alarme (blanc) les vannes se ferme automatiquement.

- **Db=1860 m^3 /h, P=74bar :**



- **Après l'activation du Switch**



Commentaire : Le système ne fonctionne pas normalement puisque les deux paramètres son supérieure au seuil qu'on à fixer.

IV.5 Conclusion

Dans ce chapitre nous avons élaboré le Grafcet de commande qui nous a permis de concevoir les programmes Step7 pour l'automatisation de notre projet.

Nous avons aussi réalisé un système de supervision pour les éléments des stations en utilisant un réseau de transmission doté du protocole PROFIBUS qu'on a sécurisé contre les intrusions, dans le but d'acquérir des données (la variation de la pression et de la température) afin de veiller à la sécurité du système à l'aide des alarmes, des vannes. Et cela à été fait en se basant sur le fonctionnement qui a était expliqué et vu en entreprise.

Conclusion générale

Conclusion générale

Les outils de supervision ou SCADA s'adressent à tous les industriels ayant des nécessités de pilotage et de visualisation de leurs équipements, ces outils «temps réel » ont pour principaux but Le contrôle et visualisation des performances désirées du système a chaque instant, et s'il y a une perte de performance une alarme se déclenchera d'une manière automatique pour prévenir l'opérateur.

Au cours de ce travail, nous avons étudié en premier lieux les différents types de contrôle en réseau ainsi que leur manière d'agir dans un environnement SCADA en suite Nous avons décrit de manière générale son les systèmes de supervision et de contrôle en présentant les différents protocoles de communication de cette environnement, son architecture et La sécurité qui représente le point le plus pertinent de ce système

Dans cette étude nous avons simulé un système de supervision et de contrôle SCADA d'un pipe transportant du pétrole et du gaz naturel a l'aide d'un réseau de communication en utilisant le protocole PROFIBUS avec le logiciel de simulation TIA PORTAL qui à pour but l'acquisition de donnée et la sécurité du système.

Ce modeste travail nous a permis d'élargir nos connaissances ou sujet des protocoles de télécommunication utilisé dans les industries ainsi que dans le domaine de l'automatisation et sur les différent type de contrôleur plus précisément le système SCADA.

Webographie

[1] http://www.sonatrach.com. Consulté le 30 mars 2019

[10] http://ar.21-bal.com/pravo/6532/index consulter le 30mars 2019

[18] http://sitelyceejdarc.org/autodoc/cours consulté le 06 avril 2019

Bibliographie

[2] Document interne de la RTC. Manuel d'exploitation de l'installation d'exportation de pétrole brut et de condensât a Bejaia. Numéro du document 1459-20-AM-1603-OM-0075.

[3] Ferradj Ghania, Mayou Moustapha .Etude De la sécurité d'un moteur diesel (ALCO V16).Electronique .université de Bejaia, 2005/2006

[4] Guide d'installation et d'utilisation, «ADR2500c », SAGEM, Mars 2004

[5] Guide d'installation et d'utilisation, «ADR155c», SAGEM

[6] Department of the Army, TM 5-601, Supervisory Control and Data Acquisition (SCADA) Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 21 January 2006

[7] Guide technique d'accréditation pour la caractérisation et la vérification des enceintes thermostatiques et climatiques, fours et bains thermostatés.mai 2009

[8] William Botton. Les Automates Programmables Industriels. DUNOD. Paris. 2010.

[9] Keith Stouffer, Joe Falco, Karen Kent. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security.US A .2006

[11] NGUYEN Xuan Hung." Réseaux de Communication et Applications de Contrôle-Commande», Thèse de doctorat, Institut National des Sciences Appliquées de Toulouse (INSA Toulouse), decembre2000

[12] Amine Mechraoui. Pronostic de défaillances d'un robot mobile commandé à travers un réseau sans fil Faults prognosis of a networked mobile robot. univ-valenciennes 13 May 2014.

[13] J. Baillieul ET P.J. Antsaklis. "Control and Communication Challenges in Networked Real-Time Systems". Proceedings of the IEEE, vol. 95, no. 1, January 2007.

[14] Jean-Pierre Richard. Systèmes commandés en réseau. Conférence EC Lille – Intelligence Ambiante 18 février 2011

[15] Guy Pujolle «Les Réseaux » Eyrolles 5° édition année 2006

[16] Andrew Tanenbaum « Réseaux » Pearson Education ,4 édition 2003

[17] Jean-Pierre Arnaud, Réseau et Telecom, Dunod, Paris, 2003, ISBN 2 10 00 79867

[19] Inhale Boualem «contribution à l'étude de supervision industrielle automatique dans un 107environnement SCADA » mémoire magistère université M'HAMED BOUGARA de BOUMERDES 2009

[20]Supervisory Control and Data Acquisition (SCADA) Systems», National Communications System, Technical Information Buletin 04-1 October 2004.

[21] David Bailey, Edwin Wright, «Practical SCADA for Industry», Edition Newnes 2003

[22] Ronald L. Krutz «Securing SCADA Systems», Edition Wiley Publishing, Inc 2006.

[23] John Park, Steve Mackay «Practical Data Acquisition for Instrumentation and Control Systems», Edition Newnes 2003

[24] Mémoire master, Etude d'un système de supervision et de contrôle, SCADA de la région de transport est RTE, Skikda année 2014

[25] Gordon Clarke, Deon Reynders, Edwin Wright «Practical Modern SCADA Protocols», Edition Newnes 2004

[26] John Park, Steve Mackay, Edwin Wright «Practical Data Communications for Instrumentation and Control», Edition Newnes 2003

[27] John Park, Steve Mackay, Edwin wright, Deon Reynders «Practical Industrial Data Networks», Edition Newnes 200

[28] Ronald L. Krutz «Securing SCADA Systems», Edition Wiley Publishing, Inc 2006

[29] Yongge Wang, Bei-Tseng Chu «SCADA: Securing SCADA Infrastructure

[30] Chuck Easttom «Computer security fundamentals», Pearson 2012.

[31] OASyS DNA and Control Room Management 15, 2014.

[32] Siemens, « S7-1200_System_Manual», Numéro de référence du document : A5E02486682-AG 03/2014.