وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

Année : 2017

Faculté: Sciences de l'Ingéniorat
Département: Electronique

MEMOIRE
Présenté en vue de l'obtention du diplôme de : MASTER

Intitulé

GESTION D'UNE CENTRALE ÉLECTRIQUE À TRAVERS UN RÉSEAU INFORMATIQUE INDUSTRIEL SOUS-SYSTÈMES DCS, PLC, SCADA

Domaine : Sciences et Technologie
Filière : Automatique
Spécialité : Automatique Industrielle

Par :
HICHEM GHERBI

DEVANT Le JURY

Président	**: Mourad Lafifi**	**MCA**	**Université Badji Moktar Annaba**
Directeur de mémoire	**: Rabah Lakel**	**Professeur**	**Université Badji Moktar Annaba**
Examinateur	**: Faycel Larbaoui**	**MCA**	**Université Badji Moktar Annaba**

DEDICCES

C'est avec une grande émotion,

Je dédie ce modeste travail de fin d'étude

A ma chère mère

Pour son soutien inconditionnel

Ses sacrifices, sa tendresse,

Son amour infini

A la mémoire de mon père

A mes chères sœurs

A mon cher frère

A toute Ma famille

A mes chères amies

Ainsi qu'à tous les camarades de ma section

Et tous mes professeurs

A tous qui m'aiment

Remerciements

Mon grand remerciement, et gratitude va de plus profond de mon cœur au Dieu .

J'exprime mon sincère remerciement à toutes les personnes qui ont aidés de prés et de loin Pour réaliser ce travail.

Ces remerciements sont adressés chaleureusement à mon encadreur PR.LAKEL pour avoir bien voulu me diriger pour la réalisation de ce projet. Je tiens à exprimer tout ma gratitude aux membres du jury Mr.Lafifi et Mr.Larbaoui

Nous tenons à remercier aussi l'ensemble des enseignants et responsables de la filière automatismes qui ont contribues à amener à bien ma formation par leur aides et leurs conseils.

Grand Merci à tous

HICHEM GHERBI

Liste des abréviations

ADSL	Asymmetric Digital Subscriber Line
AMDEC	Analyse des modes de défaillance de leurs effets et criticités
API	Automate programmable industriel (PLC en anglais)
CPU	Central Processing Unit
DoS	Denial of Service (déni de service)
DRP	Disaster Recovery Plan
EIA	Electrical Industry Association
ERP	Enterprise Resource Planning
FMEA	Failure Mode and Effects Analysis
FAT	Factory Acceptance Test
GSM	Global System for Mobile
GTB	Gestion technique de bâtiment
GTC	Gestion technique centralisée
HAZOP	HAZard & OPerability method
ICS	Industrial Control System
IHM	Interface homme-machine
MES	Manufacturing Executive System
OLE	Object Linked & Embedded
OPC	OLE for Process Control
P&ID	Process & Instrumentation Diagram
PID	Proportionnel Intégral Dérivé
PLC	Programmable Logic Controller
PCA	Plan de continuité d'activité
PRA	Plan de reprise d'activité
PSSI	Politique de sécurité des systèmes d'information
RTC	Réseau téléphonique commuté
RTU	Remote Terminal (unité aussi distant télémétrie)
PID	Proportionnel-intégral - dérivé
SAT	Site Acceptance test
SCADA	Supervisory Control And Data Acquisition
SdF	Sûreté de fonctionnement (= FMDS)
SIL	Safety Integrity Level
SNCC	Système Numérique de Contrôle Commande
SOAP	Service Object Access Protocol
SPC	Statistical Process Control
VFD	Variable Frequency Drive
DCS	Distributed control system
FBD	Function Bloc Diagram
SQL	Langage d'interrogation structuré

Liste des tableaux

Chapitre 02

Liste des figures

Chapitre 01

Chapitre 02

Chapitre 03

RESUME

Ce travail a pour but de connaitre, dans la branche de production de l'électricité à base des turbines à gaz qui ont été installées au niveau des centrales électriques et ont été gérés par les exploitants de la société. Cette société fait la production de l'électricité par l'utilisation des (turbines à gaz, turbines à vapeur) et aussi des énergies renouvelables (solaire, vents…).

Ce travail a été réalisé au niveau d'une centrale électrique cette dernière est un ensemble de différents systèmes combinés de façon intelligente entre eux afin d'assurer la production de l'électricité. Autant qu'automaticien, ce travail c'est concentré sur l'étude d'un système de supervision et de contrôle et acquisition de données « SCADA » basé sur un serveur et des PCs clients, en simulant ce système et en réalisant une application réelle d'une boucle de mesure de température à afficher sur un HMI au niveau du laboratoire universitaire.

Le serveur collecte toutes les informations des transmetteurs installées à l'extérieur de la salle de contrôle commande, les informations entrantes et sortantes doivent être passé à travers des automates programmables industriels, qui jouent le rôle d'une partie d'un système de contrôle distribué (DCS).

Où on a abordé les parties suivantes : La première est la description de la station en expliquant le principe de fonctionnement de la centrale électrique. La deuxième est une étude détaillée sur le système de contrôle industriel, le système SCADA, le système DCS et les automates programmables industriels. Ainsi, on a détaillé le coté hardware (matériel) et le coté software (logiciel) de ces derniers. Sans oublier la partie de sécurité parce que des nombreux réseaux des systèmes de contrôle industriel sont vulnérables aux menaces basées sur Internet.

ABSTRACT

The purpose of this work is to discover, in the industry of the production of electricity from gas turbines installed at the level of the factory and managed by the operators of the Plant. This company manufactures electricity using (gas turbines, steam turbines) and renewable energies (solar, wind ...).

This work was carried out at a plant, the latter being a set of different systems intelligently combined to ensure the production of electricity. As an automation, this work focuses on the study of a "SCADA" monitoring and control system based on a server and client computers, simulating this system and realizing a real application. A temperature measurement loop to be displayed-on a HMI At the level of the university laboratory.

The server collects all information from the transmitters installed outside the control room; the incoming and outgoing information must be passed through PLCs, which are part of a distributed control system (DCS).

Where we dealt with the following parts: the first is the description of the station explaining the operating principle of the plant. The second is a detailed study of the industrial control system, the SCADA system, the DCS system and the industrial programmable logic controllers. Thus, we have detailed the hardware side and the software side of the latter. Not to mention the security part because many networks of industrial control systems are vulnerable to Internet-based threats.

ملخص

الغرض من هذا العمل هو اكتشاف صناعة إنتاج الكهرباء من توربينات الغاز المثبتة على مستوى المصنع وتدار من قبل مشغلي الشركة. تقوم هذه الشركة بتصنيع الكهرباء باستخدام (توربينات الغاز والتوربينات البخارية) والطاقات المتجددة: الطاقة الشمسية والرياح

تم تنفيذ هذا العمل بأخذ مصنع إنتاج الكهرباء كمثال تطبيقي، وهذا الأخير هو مجموعة من أنظمة مختلفة مجتمعة بذكاء لضمان إنتاج الكهرباء. ويركز هذا العمل على دراسة نظام مراقبة "سكادا" والسيطرة على أساس أجهزة الكمبيوتر الخادم والسرفير، ومحاكاة هذا النظام وإنجاز تطبيق حقيقي لقياس درجة الحرارة ليتم استظهارها على شاشة العرض على مستوى المختبر الجامعي.

ويقوم الخادم بتجميع كل المعلومات من أجهزة الإرسال المثبتة خارج غرفة التحكم؛ يجب أن يتم تمرير المعلومات الواردة والصادرة من خلال أجهزة التحكم المنطقية، والتي هي جزء من نظام التحكم الموزعة.

حيث تعاملنا مع الأجزاء التالية: الأول هو وصف المحطة شرح مبدأ التشغيل للمصنع. والثاني هو دراسة مفصلة لنظام التحكم الصناعي، ونظام سكادا، ونظام دي سي أس وأجهزة التحكم المنطقية القابلة للبرمجة الصناعية. وهكذا، لدينا تفصيل الجانب الأجهزة والجانب البرمجيات من هذا الأخير. ناهيك عن الجزء الأمني لأن العديد من شبكات أنظمة التحكم الصناعي معرضة للتهديدات القائمة على الإنترنت.

SOMMAIRE

INTRODUCTION GENERALE :

La problématique traitée dans ce mémoire concerne la gestion des données techniques d'un système industriel complexe, à travers la communication entre un PLC et le système SCADA.

Le système industriel est une centrale électrique à base des turbines à gaz, le PLC est un SIEMENS SIMATIC S7-400 et la plateforme logicielle utilisée comme système SCADA est le logiciel MOVICON.

L'information technique à gérer est la température de l'air comprimé d'air au niveau de l'unité de traitement d'air avant son distribution au diffèrent systèmes tels que les turbines à gaz et les autres auxiliaires.

La gestion de cette information technique consiste à réaliser l'acquisition en temps réel, gérer les alarmes associe à des dépassements des seuils Max et Min et établir l'historique à des fins d'utiliser pour l'analyse et le diagnostic des défauts.

L'acquisition de l'information est réalisée à travers un PLC, instrumentation déportée, elle transmise via des réseaux informatiques industriels à un PC serveur sur lequel est hébergé MOVICON (logiciel SCADA), et sera transmise à son tour vers les PCs Clients.

CHAPITRE 01 : Description de la centrale thermique de production d'électricité

1.1. Introduction :

La pression économique sur le marché de l'électricité a poussé la grille de puissance afin d'exploiter plus près des limites du système et ses composants. La technologie des mesures synchronisées fournit un moyen idéal pour surveiller et contrôler les systèmes de puissance, en particulier dans des conditions de stress. Il faut mettre en œuvre l'estimation de l'État rapidement et de manière fiable, évaluer les marges et les risques de stabilité et prendre des mesures de contrôle préventif et de réparation. Toutefois, pour les exigeants ça revient à demander : la communication, le stockage, et le traitement des données. Ceci peut être réalisé par

la localisation optimale des défauts d'une part, et l'intégration des données dans un système SCADA d'autre part [1].

1.2. Description générale de la centrale électrique :

Une centrale électrique est un site industriel destiné à la production d'électricité. Les centrales électriques alimentent en électricité, au moyen du réseau électrique, les consommateurs, particuliers ou industriels éloignés de la centrale. La production d'électricité y est assurée par la conversion en énergie électrique d'une énergie primaire qui peut être soit mécanique (force du vent, force de l'eau des rivières, des marées...), soit chimique (réactions d'oxydoréduction avec des combustibles, fossiles ou non tels que la biomasse), soit nucléaire, soit solaire...

Ces énergies primaires peuvent être renouvelables (biomasse) ou quasiment inépuisables (énergie solaire) ou au contraire peuvent constituer des ressources dont la disponibilité est limitée dans le temps (combustibles fossiles) [2].

1.3. Système SCADA et la centrale électrique :

Aujourd'hui, la surveillance des systèmes de production est plus complexe à réaliser, non seulement en raison du nombre de variables, toujours plus nombreux à suivre mais aussi en raison de nombreuses interrelations existant entre eux, très difficile d'interpréter le processus peut être hautement automatisé.

Le défi des années futures est basé sur la conception des systèmes de soutien qui permettent une part active aux opérateurs de surveillance en fournissant des outils et des informations leur permettant de comprendre le fonctionnement des équipements de production [14].

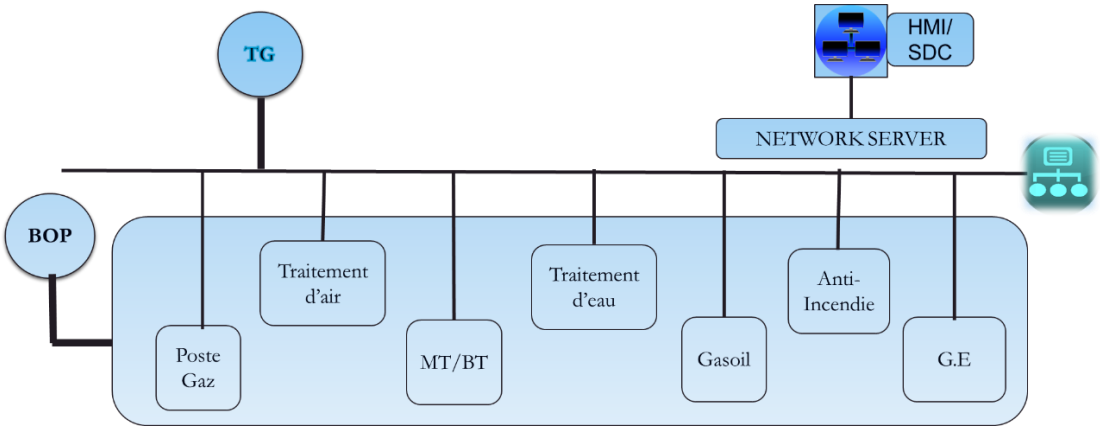

Figure 1.2 : **exemple centrale électrique à base de turbine à gaz**

TG : Turbine à Gaz.
BOP : Balance of plant (équilibre du chantier).
HMI/SDC : Interface Homme Machine/ Salle de commande.
MT/BT : Moyenne tension / Basse tension.
G.E : Groupe électrogène.

1.4. Air comprimé dans l'industrie :

L'air comprimé est de plus en plus utilisé par l'industrie ou les services grâce à sa souplesse de mise en œuvre ; les impératifs économiques incitent les utilisateurs à mieux anticiper les coûts de production afin de maîtriser les dépenses en énergie et en maintenance.

L'apparition sur le marché de nouveaux matériels, de compression et de traitement, les contraintes imposées par les normes de qualité et le respect de l'environnement amènent les décideurs à considérer l'air comprimé comme une énergie à part entière et à en confier sa production à des spécialistes capables de gérer l'ensemble de ces paramètres.

Au fur et à mesure que les utilisations de l'air comprimé se développent, les industriels installent dans leurs usines ou sur leurs chantiers des centrales d'air comprimé et des réseaux de distribution [15] .

1.4.1. Température de l'air comprimé :

La température de l'air comprimé l'un des paramètres qui caractérise l'énergie disponible et stockée par ce fluide.

Si l'air comprimé est utilisé pour une application de conduite, il ne doit pas être refroidi. Au contraire, il est possible de lui apporter de l'énergie en réchauffant soit à l'entrée, soit, ce qui est préférable, pendant la détente .Cet apport de chaleur accroît en effet l'énergie interne du fluide et donc la part de travail qu'il peut fournir. Dans la majorité des cas, l'air comprimé doit être utilisé à température ambiante. La compression de l'air se faisant avec élévation de température, il faut refroidir le compresseur et l'air à la sortie [15].

1.5. Description du système de supervision :

Le système de supervision interconnecte l'opérateur à l'installation, pour un fonctionnement efficace de l'installation. Il permet de visualiser en temps réel les variables les plus importantes du panneau de contrôle, les alarmes qui sont archivées dans un serveur redondant qui se trouve dans la salle de contrôle.

Grace à la supervision, l'opérateur peut interagir avec les systèmes les plus importants. Voir l'évolution des variables, voir les alarmes analyser les paramètres à travers les archives historiques. L'opérateur aura des rapports disponibles, afin de contrôler les variables plus importantes pour la conduite de l'installation.

Les commandes qui peuvent être données par la supervision sont limitées aux points de départ / arrêt, de réinitialisation et de consigne, qui ne peuvent être augmentés car les fabricants des différents systèmes limitent les opérations à distance pour des raisons de sécurité. Ces fonctions n'ont aucun type de supervision de la part de la supervision. Les systèmes de contrôle de chaque système sont indépendants de la supervision et ont préséance sur les commandes issues de la supervision.

1.6. Conclusion :

Les systèmes de contrôle des infrastructures critiques pour générer, transmettre, distribuer, stocker et utiliser de l'énergie ainsi que les processus de fabrication ne sont plus isolés. La formation aux systèmes de contrôle industriel en réseau est due à plusieurs facteurs. L'intégration d'actifs géographiquement distribués grâce à un contrôle centralisé améliore l'agilité pour répondre aux changements dans l'offre et la demande, réduit le coût des opérations et permet l'efficacité des procédés impossible à atteindre dans le passé.

CHAPITRE 02 : Description du Système de contrôle industriel (SCADA, DCS, PLC, SECURITE)

2.1. Introduction :

Le Système de contrôle industriel (ICS) est un terme général qui englobe plusieurs types de systèmes de contrôle, y compris la surveillance des systèmes de contrôle et acquisition de données (SCADA), les systèmes de contrôle distribué (DCS) et autres configurations de système de contrôle plus petits tels que les contrôleurs logiques programmable (PLC). ICS est généralement utilisés dans les industries telles que l'électrique, l'eau, pétrolière et gazière, chimique, transport, industrie pharmaceutique, pâtes et papiers, nourriture et boisson et de la fabrication discrète (p. ex., automobiles, aérospatiales et durables marchandises.).

Ces systèmes de contrôle sont essentiels à l'exploitation des infrastructures critiques, qui sont souvent hautement interconnectés et interdépendants. D'autres exemples incluent, le contrôle du trafic aérien et la manutention des matériaux (p. ex., Service Postal courrier traitement.) Cette section fournit une vue d'ensemble des systèmes SCADA, DCS et PLC, y compris les composants et les architectures typiques. Généralement, plusieurs diagrammes sont présentés pour décrire les composantes trouvés sur chaque système pour faciliter la compréhension de ces systèmes et les connexions réseaux.

2.2. Description générale du système SCADA :

2.2.1. Notion et concept de base de système SCADA :

Par SCADA, généralement, on entend des systèmes centralisés qui surveillent et contrôlent des sites entiers, ou des systèmes complexes réparties sur de vastes étendues. La plupart des actions de contrôle sont effectuées automatiquement par Remote Terminal Units (RTU) ou par automates programmables (API).

Les fonctions de contrôle hôte se limitent habituellement à la substitution de base ou la surveillance au niveau d'intervention. Par exemple, un PLC peut contrôler

l'écoulement de l'eau de refroidissement par la partie d'un processus industriel, mais le système SCADA peut-être permet aux opérateurs de modifier les points de réglage pour le débit et permettre de fixer les conditions d'alarme, tels que la perte de débit et de température élevée, pour être affichés et enregistrés.

Le contrôle de rétroaction de la boucle passe par RTU ou l'automate, tandis que le système SCADA surveille les performances globales de la boucle.

L'acquisition des données commence au niveau du RTU ou PLCs et comprend des relevés de compteurs et de rapports de situation des équipements qui sont communiquées au SCADA.

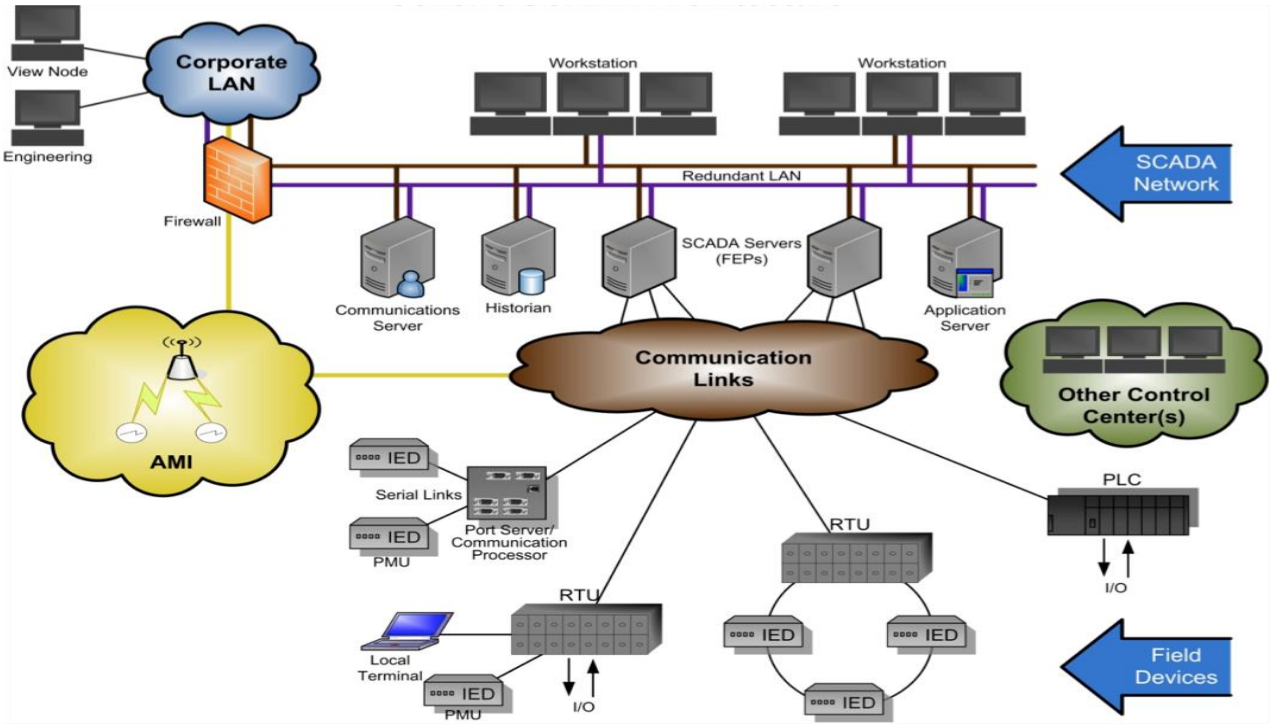

Figure 2 .1 : Système SCADA

Les données sont alors compilées d'une façon qu'un opérateur de contrôle, à l'aide de l'HMI, peut prendre des décisions surveillance pour ajuster ou outre passer au contrôle normale de RTU (PLC) .Les données peuvent également alimentées un PC qui gère l'historique (appelé PC historien) .

Les systèmes SCADA implémentent généralement une base de données distribuée, communément appelé une *base de données de tag*, qui contient des éléments de données appelés *balises* ou *points*. Un point représente une entrée unique ou une valeur de sortie surveillée ou contrôlée par le système.

Les points peuvent être « Hardware » ou « Software ». Un point dur représente une réelle entrée ou la sortie au sein du système, tout point flottant correspond à des opérations logiques ou mathématiques appliquées à d'autres points.

Les points sont normalement stockés en tant que timestamp (horodatage) de valeur paires : une valeur et une date (soit enregistrée ou calculée). Une série de paires valeur-timestamp donne l'histoire de ce point. Il est également fréquent pour stocker des métadonnées supplémentaires avec des balises, tels que le chemin d'accès à un dispositif de terrain ou registre PLC, conception temps commentaires et informations alarme.

2.2.2. Composants du SCADA :

Un système SCADA comprend habituellement les sous-systèmes suivants :

- L'**Interface Homme-Machine** ou HMI est un appareil qui présente des données de processus à un opérateur humain, et par ce biais, l'opérateur humain surveille et contrôle le processus.
- Un **système de surveillance** (**informatique**), collecte de données (acquéreur) sur le processus et l'envoi des commandes (contrôle) au processus.

- **Unités terminales distantes** (RTU) raccordement de capteurs dans le processus, capteur de conversion des signaux de données numériques et envoi les données numériques vers le système de surveillance.
- **Automate programmable** (API) utilisés comme appareils de terrain parce qu'ils sont plus économiques, polyvalent, souple et configurable que les RTU spéciales.
- **Infrastructure de Communication** fait la liaison entre le système de surveillance des Unités terminales distantes.(RTU)

2.2.3. Interface Homme-Machine :

L'Interface Homme-Machine ou HMI est l'appareil qui présente des données de processus à un opérateur humain et à travers lequel l'opérateur contrôle le processus.

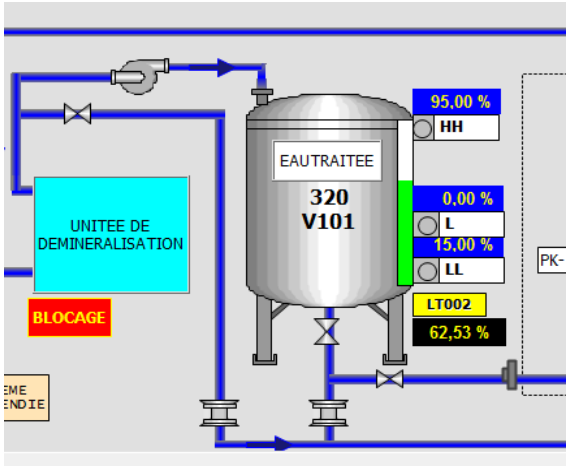

Figure 2.2.3 : Animations de base SCADA typiques

L'IHM est généralement lié à du système SCADA bases de données et logiciels, pour fournir une tendance, données de diagnostic et des informations de gestion tels que les procédures de maintenance planifiée, informations logistiques, détaillée des schémas pour un capteur particulier ou machine et les guides de dépannage de système expert.

L'IHM est un logiciel et un matériel permettant aux opérateurs humains de surveiller l'état d'un processus sous contrôle, de modifier les paramètres de contrôle pour modifier l'objectif de contrôle et de remplacer manuellement les opérations de

contrôle automatique en cas d'urgence. L'HMI permet également à un ingénieur de contrôle ou à un opérateur de configurer des points de consigne ou des algorithmes de contrôle et des paramètres dans le contrôleur. L'IHM affiche également des informations sur l'état des processus, des informations historiques, des rapports et d'autres informations auprès des opérateurs, des administrateurs, des gestionnaires, des partenaires commerciaux et d'autres utilisateurs autorisés. L'emplacement, la plate-forme et l'interface peuvent varier considérablement. Par exemple, une IHM pourrait être une plate-forme dédiée dans le centre de contrôle, un ordinateur portable sur un réseau local sans fil ou un navigateur sur n'importe quel système connecté à Internet.

2.2.4. Les domaines d'application du système SCADA :

Plusieurs domaines d'utilisation du système SCADA peuvent être distingués :

- ✓ Le pilotage de grandes installations industrielles automatisées :

- métallurgie (laminoir à froid et à chaud) production pétrolière (distillation),
- production et stockage agroalimentaire (lait, céréales...)
- production manufacturière (automobile, biens de consommation...)

- ✓ Le pilotage d'installations réparties :

- alimentation en eau potable,
- traitement des eaux usées.
- gestion des flux hydrauliques (canaux, rivières, barrages...).
- gestion de tunnels (ventilation, sécurité).

- ✓ La gestion technique de bâtiments et gestion technique centralisée (GTC):

- gestion des moyens de chauffage et d'éclairage (économies d'énergie).
- gestion des alarmes incendies.
- contrôle d'accès, gestion des alarmes intrusion.

2.2.5. Les méthodes de communication :

Les différentes méthodes de communications sont :
- Connexion directe
- Porte-lignes électriques
- Micro-onde
- Radio (large spectre)
- Fibre optique

2.2.6. Méthodes et infrastructures de communication :

Les Systèmes SCADA ont traditionnellement utilisé, pour leurs besoins de communications, des liaisons radio, des liaisons filaires et des liaisons par modem (internet).

Les protocoles SCADA sont conçus pour être très compact et beaucoup sont conçus pour envoyer des informations à la station maître uniquement lorsque celle-ci interroge le RTU.

Les Protocoles SCADA traditionnels typiques incluent Modbus RTU, RP-570 et Profibus . Ces protocoles de communication SCADA sont spécifiques à chaque fournisseur. Beaucoup de ces protocoles contiennent maintenant des extensions sur TCP/IP.

Pour résumer le système de contrôle et commande permet de :

- ✓ fournir un statut de réseau.
- ✓ Permettre la commande à distance.
- ✓ Optimiser les performances du système.
- ✓ Réaliser les Opérations d'urgence.
- ✓ Répartir les équipages de réparation et coordination avec d'autres Services publics.

2.3. Stratégie de contrôle :

2.3.1. Centrale de contrôle :

La centrale de contrôle ou la salle de contrôle-commande est conçu pour :

- Contrôler l'acquisition des données

- Équilibrer la production et la demande (envoi)
- Surveiller les flux et observer les limites du système
- Coordonner les activités de maintenance et les fonctions de réponse d'urgence.

2.3.2. Localisation et les principales propriétés :

La stratégie de contrôle nous oblige de choisir les endroits les plus importants pour transmettre les informations aux opérateurs au niveau de la salle de contrôle par exemple sur une centrale électrique on doit prendre en considération le :

- Contrôle de rétroaction (par exemple, régulateurs, régulateurs de tension)
- Protection (p. Ex., Relais de protection, disjoncteurs).

Les principales propriétés du système SCADA sont :

- La sécurité.
- Protection contre tout endommagement des équipements.
- Donne la confiance qui agit sur la fiabilité du système d'une façon générale.
- Travailler plus vite et plus efficacement et d'une manière plus économique. La pression est toujours – pour augmenter la productivité, l'efficacité, l'agilité, la qualité et la profitabilité tout en minimisant les coûts.

2.4. Vue d'ensemble des SCADA, DCS et PLC :

Les Systèmes SCADA est distribué à grande échelle des systèmes permettant de contrôler les actifs géographiquement dispersés, souvent dispersés sur des milliers de kilomètres carrés, où le contrôle et acquisition de données centralisées sont essentiels au fonctionnement du système. Ils sont utilisés dans les réseaux de distribution tels que la distribution de l'eau et les systèmes de collecte des eaux usées, huile et gazoducs, grilles d'alimentation électrique et systèmes de transport ferroviaire. Un *Centre de contrôle SCADA* réalise centralisé de suivi et de contrôle pour le terrain par des réseaux de communications longue distance, y

compris la surveillance des alarmes et de traitement des données. Basé sur les informations reçues des stations éloignées, des commandes de surveillance automatisés ou pilotée par l'opérateur peuvent être poussés pour dispositifs de commande de console distante, qui sont souvent appelés *dispositifs de champ*. Appareils de terrain contrôlent les opérations locales comme les vannes à fermeture et d'ouverture et de disjoncteurs, recueillir des données de systèmes de détection et surveillance de l'environnement local pour les conditions d'alarme.

DCSs sont utilisés pour contrôler les procédés industriels comme nourriture de génération, les raffineries de pétrole et gaz, d'eau et traitement des eaux usées et chimique, énergie électrique et la production automobile. DCSs sont intégrés comme une architecture de contrôle contenant un niveau de responsabilité de contrôle supervise plusieurs, intégrés des sous-systèmes qui sont chargés de contrôler les détails d'un processus localisé. Contrôle des produits et processus sont habituellement réalisé en déployant la cabine avancée boucles produit clé et/ou des conditions de processus sont automatiquement demeure autour d'un point de consigne souhaité ou en alimentation arrière. Pour réaliser le produit souhaité et/ou processus tolérance autour d'un point spécifié, des automates programmables (PLC) travaillent sur le terrain et proportionnel, intégral, et/ou paramètres différentiels sur l'automate sont réglés pour fournir la tolérance souhaitée ainsi que bouscule le taux d'autocorrection au cours du processus. DCSs sont largement utilisées dans les industries axées sur les processus.

PLCs sont des dispositifs à semi-conducteurs informatisés qui contrôlent les processus et les équipements industriels. Tandis que les automates sont composants de système de contrôle utilisé tout au long de systèmes SCADA et DCS, ils sont souvent les principaux composants en plus petites configurations de système de contrôle utilisées pour fournir un contrôle réglementaire des processus discrets tels que des chaînes de montage automobiles et suie centrale contrôle du

ventilateur. Automates programmables sont largement utilisées dans presque tous les processus industriels.

Les industries axées sur les processus de fabrication utilisent généralement deux procédés principaux :

- ✓ P**rocédés Continue de fabrication.** Ces processus fonctionne continuellement, souvent avec des transitions de faire différentes qualités d'un produit. Processus de fabrication continu type incluent le combustible ou la vapeur débit dans une centrale électrique, dans une raffinerie de pétrole et la distillation dans une usine chimique.
- ✓ **Processus de fabrication du lot.** Ces processus ont des étapes de traitement distinct, menées sur une quantité de matière. Il y a un départ distinct et une étape de la fin d'un traitement par lots avec la possibilité d'opérations bref état stationnaire au cours des étapes intermédiaires.

Les industries de la fabrication discrète sur généralement procéder à une série d'étapes sur un seul appareil pour créer le produit final. Assemblage de composant électroniques et mécaniques et de pièces d'usinage sont des exemples typiques de ce type d'industrie.

Tant sur les processus discrets industries et utilisent les mêmes types de systèmes de contrôle, des capteurs et réseaux. Certaines installations sont un hybride de discrète et axée sur les processus de fabrication.

Tandis que les systèmes de contrôle utilisés dans la distribution et les industries manufacturières sont très similaires en fonctionnement, ils diffèrent à certains égards. Une des principales différences est que DCS ou sous-systèmes contrôlé par PLC sont généralement situés dans une usine plus confiné ou de la région axée sur les manufactures, par rapport aux sites de champ SCADA géographiquement dispersés. DCS et PLC communications sont habituellement effectuées à l'aide de technologies de réseau local (LAN) qui sont généralement plus

fiable et à haute vitesse par rapport aux systèmes de communications longue distance utilisé par les systèmes SCADA. En fait, les systèmes SCADA sont spécialement conçus pour gérer les défis de communication longue distance tels que des retards et des pertes de données posés par les divers moyens de communication utilisés. Systèmes DCS et PLC utilisent généralement des niveaux plus de commande de boucle bloquée que les systèmes SCADA parce que le contrôle des procédés industriels est généralement plus compliqué que le réseau de contrôle des processus de distribution. Ces différences peuvent être considérés subtiles pour la portée du présent document, qui met l'accent sur l'intégration de la sécurité informatique (IT) dans ces systèmes. Durant le reste de ce document, les systèmes SCADA, DCSs et systèmes PLC seront être dénommés *ICSs* sauf s'il est fait expressément référence à l'un (par exemple, dispositif de champ utilisé dans un système SCADA).

2.4.1 Opération ICS :

Le fonctionnement de base de l'ICS est illustré à la Figure_2.4.1,les éléments clés sont les suivants :

- ✓ **Contrôleur de boucle :** Une boucle de régulation est constitué de capteurs de mesure, contrôleur matériel tels que les automates, les actionneurs tels que des vannes de régulation, disjoncteurs, interrupteurs et moteurs et la communication des variables. Variables contrôlées sont transmises au contrôleur des capteurs. Le contrôleur interprète les signaux et génère des variables manipulées correspondantes, basés sur des points de consigne, dont elle transmet aux actionneurs. Processus varie de résultat de perturbations dans les nouveaux signaux de capteurs, déterminant l'état du processus, encore une fois être transmises au contrôleur.
- ✓ Interface Homme-Machine (HMI) : Ingénieurs et opérateurs utilisent HMI pour configurer des points de consigne, algorithmes, de contrôle et ajuster et

établir les paramètres du contrôleur. L'IHM affiche également les informations d'état de processus et de données historiques.

- ✓ **Diagnostic à distance et les utilitaires de Maintenance.** Diagnostics et les utilitaires de maintenance sont utilisés pour prévenir, identifier et récupérer des échecs.

Un ICS typique contient une prolifération des boucles de régulation, IHM et diagnostic à distance et les outils de maintenance construits en utilisant une gamme de protocoles de réseau sur les architectures de réseau en couches. Parfois, ces boucles de contrôle sont imbriqués et/ou en cascade – auquel cas le point de consigne pour une seule boucle est basé sur la variable de processus déterminée par une autre boucle. Supervision niveau boucles et boucles de niveau inférieur fonctionnent en permanence pendant la durée d'un processus avec cycle de temps allant de l'ordre des millisecondes à minutes.

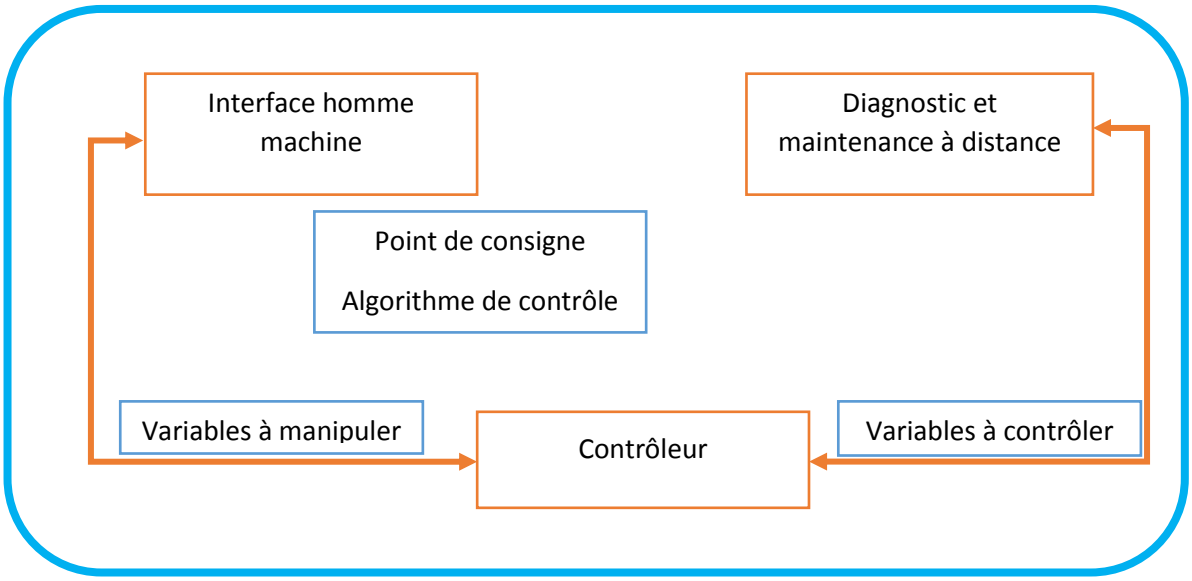

Figure_2.4.1. Opération d'ICS

2.5 Composants clés de l'ICS :

2.5.1 Composants de contrôle :

Les composants principaux de contrôle de l'ICS sont [1]:

- **Contrôler serveur.** Le serveur de contrôle héberge le logiciel de contrôle-commande DCS ou PLC qui est conçu pour communiquer avec des

dispositifs de contrôle de niveau inférieur. Le serveur de contrôle accède à des modules de commande subordonné sur un réseau ICS.

- **Serveur SCADA ou Master Terminal Unit (MTU).** Le serveur SCADA est le dispositif qui agit comme le maître dans un système SCADA. Unités terminales distantes et appareils PLC (comme décrit ci-dessous) située au domaine distant sites agissent habituellement comme des esclaves.
- **Unité terminale distante (RTU).** Le RTU, appelé également une unité de distance de télémétrie, est d'acquisition de données spéciaux et régulateur de vitesse conçu pour soutenir des stations à distance SCADA. RTU est des appareils de terrain souvent équipés d'interfaces radio sans fil pour soutenir des situations éloignées où les communications filaires sont indisponibles. Parfois les automates sont implémentées comme des appareils de terrain pour servir de RTU ; dans ce cas, l'automate est souvent dénommé une RTU.
- **Contrôleur logique programmable (PLC).** Le PLC est un petit ordinateur industriel initialement conçu pour remplir les fonctions de logique exécutées par le matériel électrique (relais, interrupteurs à tambour et minuterie/compteurs mécaniques). Automates programmables ont évolué vers des contrôleurs ayant la capacité de contrôler les processus complexes, et ils sont utilisés essentiellement dans les systèmes SCADA et de DCSs. Autres contrôleurs utilisés sur le terrain sont des contrôleurs de processus et RTU ; ils contiennent le même contrôle que les automates mais sont conçus pour des applications de contrôle spécifique. Dans des environnements de SCADA, automates programmables sont souvent utilisés comme appareils de terrain parce qu'ils sont plus économiques, polyvalent, souple et configurable que RTU spéciales.
- **Des appareils électroniques intelligents (IED).** Un IED est un capteurs/actionneurs « intelligents » contenant l'intelligence requise pour

acquérir des données, communiquer avec d'autres appareils et effectuer le contrôle et le traitement local. Un IED pourrait combiner un capteur d'entrée analogique, sortie analogique, les capacités de contrôle de bas niveau, un système de communication et mémoire de programme dans un seul appareil.

- **Interface Homme-Machine (HMI).** L'IHM est logiciel et le matériel qui permet à des opérateurs humains à suivre l'état d'un processus sous contrôle, modifier les paramètres de contrôle pour modifier l'objectif de contrôle et remplacer manuellement les opérations de contrôle automatique en cas d'urgence. L'IHM permet également un Automaticien ou pour configurer des points de consigne ou les algorithmes de commande et les paramètres du contrôleur. L'IHM affiche également les informations d'état de processus, des informations historiques, rapports et autres informations aux opérateurs, administrateurs, dirigeants, partenaires commerciaux et autres utilisateurs autorisés. L'emplacement, la plate-forme et interface peuvent varier énormément. Par exemple, une HMI pourrait être une plate-forme dédiée au centre de contrôle, un ordinateur portable sur un réseau local sans fil, ou un navigateur sur n'importe quel système connecté à Internet.
- **Historique des données.** L'historique de données est une base de données centralisée pour consigner toutes les informations de processus au sein de l'ICS. Les informations stockées dans cette base de données sont accessibles pour les besoins d'analyses, de maîtrise statistique des processus et de planification au niveau de l'entreprise.
- **Serveur d'entrée/sortie (e/s).** IO le serveur est un composant de contrôle responsable de la collecte, la mise en mémoire tampon et donnant accès à traiter l'information de sous-composants de contrôle tels que les automates et RTU. Un serveur d'e/s peut résider sur le serveur de contrôle ou sur une

plate-forme d'ordinateur distinct. Serveurs d'e/s sont également utilisés pour interfacer avec des composants de contrôle tiers, comme une IHM et un serveur de contrôle.

2.5.2 Composants du réseau [1]:

Il y a des caractéristiques de réseau différent pour chaque couche dans une hiérarchie de système de contrôle. Les topologies de réseau à travers différentes implémentations d'ICS varient avec les systèmes modernes en utilisant l'Internet et les stratégies d'intégration des entreprises. Les Réseaux de contrôle ont été fusionnés avec les réseaux d'entreprise à fin de permettre aux ingénieurs de surveiller et contrôler les systèmes en dehors du réseau de système de contrôle. La connexion peut également permettre aux décideurs de niveau entreprise d'avoir accès aux données de processus. Voici une liste des principales composantes d'un réseau ICS, quelles que soient les topologies de réseau utilisé :

- **Réseau Fieldbus :** Le bus de terrain est un réseau qui relie des capteurs et autres dispositifs à un automate programmable ou un autre contrôleur.
  L'utilisation des technologies de fieldbus élimine le besoin pour le câblage de point à point entre le contrôleur et chaque périphérique.
  Des capteurs communiquent avec le contrôleur de bus de terrain à l'aide d'un protocole spécifique. Chaque capteur a unique identifiant.
- **Control Network :** Le réseau de contrôle connecte à son niveau les modules de commande du niveau inférieur.
- **Communications routeurs : U**n routeur est un dispositif de communication qui transfère des messages entre deux réseaux. L'utilisation courante pour les routeurs inclut la connexion à un LAN avec le serveur MTU d'une part et les RTU d'autre part.
- **Pare-feu.** Le firewall protège les périphériques sur un réseau de surveillance et de contrôle des paquets de communication en utilisant des

stratégies de filtrage prédéfinies. Le Pare-feu est également utile dans la gestion des stratégies de ségrégation du réseau ICS.

- **Modems.** Le modem est un dispositif servant à convertir des données numériques série d'un signal approprié pour la transmission sur une ligne téléphonique pour permettre aux périphériques de communiquer. Modems sont souvent utilisés dans des systèmes SCADA pour permettre des communications longue distance série entre MTU et dispositifs de champ lointain. Ils sont également utilisés dans les systèmes SCADA, DCSs et automates d'accès distant pour des fonctions opérationnelles telles que la commande ou en modifiant des paramètres et des fins de diagnostic.
- **Points d'accès à distance.** Les Points accès à distance sont des périphériques différents, des zones et des lieux d'un réseau de contrôle pour configurer à distance les systèmes de contrôle et accès aux données de processus. Citons à l'aide d'un assistant numérique (PDA) pour accéder aux données via un réseau local via un point d'accès Wi-Fi et utilisant une connexion ordinateur portable et modem pour accéder à distance à un système d'ICS.

2.6. Systèmes SCADA :

Les systèmes SCADA sont utilisés dans les systèmes complexes industriels où l'acquisition de données à partir des RTU est aussi importante que le contrôle lui-même [6] [7]. Ces systèmes sont utilisés dans les réseaux de distribution tels que les systèmes de collecte des eaux usées et de distribution eau, oléoducs et gazoducs, les systèmes de transmission et de distribution de service public d'électricité et rail et d'autres systèmes de transport en commun. Les systèmes SCADA intègrent des systèmes d'acquisition de données avec les systèmes de transmission de données et logiciel HMI pour fournir un contrôle centralisé et système de contrôle pour nombreux processus entrées et sorties. Les systèmes SCADA sont conçus pour recueillir des informations en temps réel, et de les

transférer vers l'ordinateur central à des fins d'affichage sous forme graphique ou textuelle, permettant ainsi à l'opérateur de surveiller ou de contrôler le système complet.

Les systèmes SCADA sont constitués de matériels et logiciels. Le matériel typique comprend : un MTU (serveur) placé au centre de contrôle, un système de communication (p. ex., radio, ligne téléphonique, câble ou satellite) et un ou plusieurs RTU répartis sur différents sites géographiquement. Le RTU peut être un PLC, qui contrôle ou surveille les capteurs actionneurs [1]. Le MTU stocke et traite les informations de RTU entrées et sorties, tandis que le RTU ou PLC contrôle le processus local. Le matériel de communication permet le transfert des informations et des données dans les deux sens entre le MTU et RTU / automates. Le logiciel est programmé pour indiquer au système quoi et quand surveiller, quelles gammes de paramètre sont acceptables et quelle réponse à lancer quand les paramètres vont des valeurs acceptables à l'extérieur. La figure 2.6.1 montre les composants et la configuration générale d'un système SCADA. Le centre de contrôle héberge un serveur de contrôle (MTU) et les routeurs de communications. Les autres composants du centre de contrôle comprennent la HMI, ingénieries de stations de travail et l'historien de données, qui sont tous reliés par un réseau local. Le centre de contrôle recueille le journal des informations recueillies par les sites de champ appelé DATALOGGER et affiche des informations au niveau de l'IHM et peut générer des actions basées sur des événements détectés. Le centre de contrôle est également responsable de la gestion centralisée des alarmes, des analyses, des tendances et établit des rapports. Sur chaque site ,le contrôle local des actionneurs , des capteurs et des moniteurs, est effectuée . Les sites sont souvent équipés d'une capacité d'accès à distance pour permettre aux opérateurs de terrain d'effectuer le diagnostic à distance et les réparations à distance par connexion WAN. Les protocoles de communication standard et propriétaires en cours d'exécution au cours de la communication série sont utilisés pour transporter des informations entre les

sites Centre et champ de contrôle à l'aide de techniques de télémétrie tels que ligne téléphonique, câble, fibre et radiofréquence comme émission, micro-ondes et satellite.

2.7 Systèmes de contrôle distribué DCS :

Les systèmes DCSs sont utilisés pour contrôler les systèmes de production dans la même situation géographique pour les industries telles que les raffineries de pétrole et de gaz, traitement des eaux, centrales électriques, usines de produits chimiques et des installations de transformation pharmaceutique. Ces systèmes généralement contrôlent les processus ou les systèmes de commande de partie discrète. Un DCS utilise une boucle de contrôle centralisé à la médiation d'un groupe de contrôleurs localisées qui se partagent les tâches globales de mener à bien un processus de production [10].

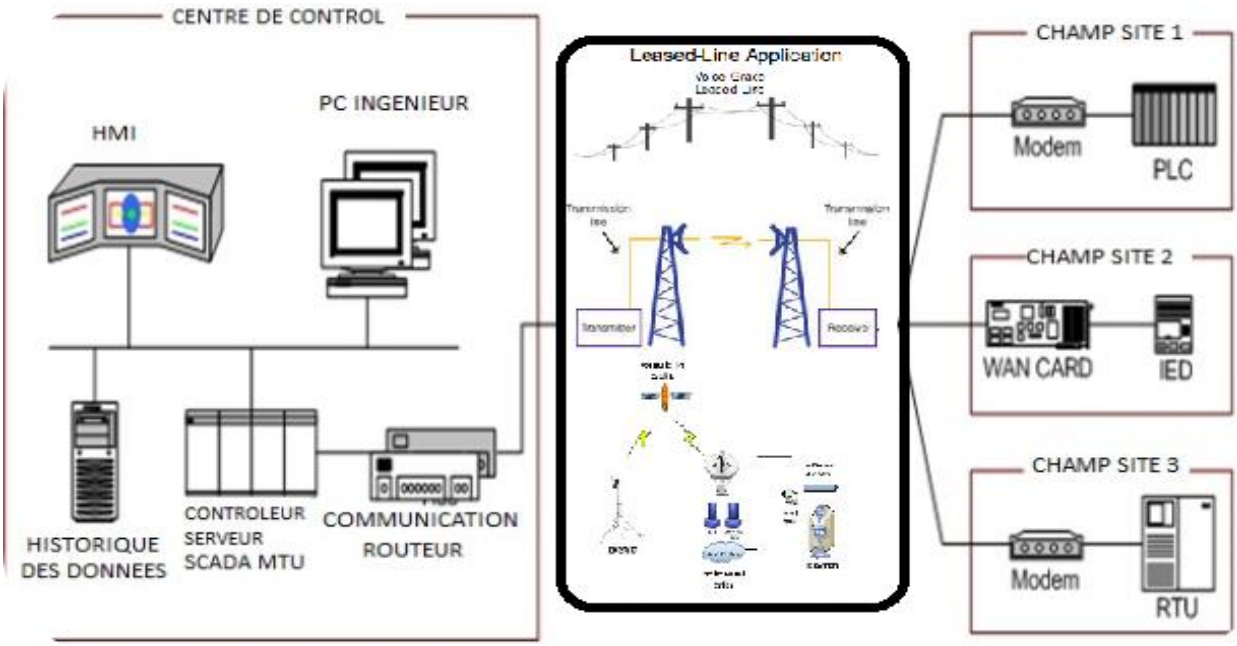

Figure 2.6.1. Présentation générale du système SCADA

De modularisation du système de production, un DCS réduit l'impact d'une défaillance sur l'ensemble du système. Dans la plupart des systèmes, les contrôleurs de domaine est interfacé avec le réseau d'entreprise pour fournir aux opérateurs commerciaux, une vue de la production.

Les dispositifs de commande de champ indiqués comprennent un PLC, un régulateur de processus, un contrôleur de boucle simple et un contrôleur de la machine. Le contrôleur de boucle simple interface les capteurs et les actionneurs à l'aide de câblage de point à point, alors que les autres appareils intègrent les réseaux de bus de terrain pour s'interfacer avec les processus de capteurs et d'actionneurs. Les réseaux de bus de terrain éliminent la nécessité pour le câblage de point à point entre un contrôleur et de champ de capteurs et d'actionneurs. En outre, un bus de terrain permet une plus grande fonctionnalité hors de contrôle, y compris le diagnostic de dispositif de champ et peut accomplir des algorithmes de contrôle dans le bus de terrain, évitant ainsi le routage de signaux vers l'automate pour toute opération de contrôle. Protocoles de communication industrielle standard conçus par secteurs d'activité tels que Modbus et Profibus sont souvent utilisés sur les réseaux de contrôle et bus de terrain.

Outre les circuits de contrôle de supervision et de terrain, des niveaux intermédiaires de contrôle peuvent également exister. Par exemple, dans le cas d'un DCS contrôlant une partie discrète, usine de fabrication, il y aurait un superviseur de niveau intermédiaire pour chaque cellule dans la plante. Ce superviseur engloberait une cellule de fabrication contenant un contrôleur de la machine qui traite une partie et un contrôleur de robot qui gère les matières premières et produits finis. Il pourrait y avoir plusieurs de ces cellules qui gèrent les contrôleurs sur le terrain sous la boucle principale de contrôle-commande des contrôleurs de domaine.

2.8 Contrôleurs logiques programmables PLC :

Automates programmables sont utilisés dans les systèmes SCADA et de contrôleurs de domaine comme les composants de commande d'un système hiérarchique dans l'ensemble pour assurer une gestion locale des processus grâce à la commande de rétroaction comme décrit dans les sections précédentes. Dans le cas de systèmes SCADA, ils fournissent la même fonctionnalité de RTU. Lorsqu'il est

utilisé dans DCSs, automates programmables sont implémentées comme des contrôleurs des au sein d'un système de contrôle-commande. Automates programmables sont également implémentées comme les principaux composants en plus petites configurations de système de contrôle. Sociétés anonymes ont une mémoire programmable par l'utilisateur pour le stockage des instructions pour l'application des fonctions spécifiques telles que les e/s contrôle, logique, calendrier, comptage, contrôle de trois mode proportionnel-intégral-dérivé (PID), communication, arithmétique et données et traitement des fichiers. Figure 2.8 montre le contrôle d'un procédé de fabrication effectué par un automate programmable via un réseau de bus de terrain.

L'automate est accessible via une interface de programmation située sur une station de travail technique, et les données sont stockées dans un PC de l'historique de données, tous connecté sur un réseau local.

Figure 2.8. Exemple de mise en œuvre de système contrôle PLC

2.9. La structure du protocole TCP / IP :

2.9.1 Introduction :

Les réseaux d'ordinateurs ont pris peu à peu une importance considérable dans la vie de tous les jours. La plupart des informations peuvent prendre un format électronique, ce qui permet de les échanger facilement avec d'autres utilisateurs. Afin de pouvoir échanger ces informations, il est nécessaire de connecter les

ordinateurs entre eux. Une fois reliés, il forme un réseau ou Lan (Local Area Network).

Si on relie plusieurs Lan entre eux, on obtient l'Internet un Wan (Wide Area Netwok).

L'Internet (INTERconnexion NETwork) est le plus grand Wan conçu par l'homme. Les particuliers ont accès à ce réseau par l'intermédiaire d'un FAI (Fournisseur d'Accès Internet).

Les réseaux utilisant la technologie TCP/IP est actuellement le plus utilisé pour plusieurs raisons : – Le protocole est libre ; – Interopérabilité.

2.9.2 Vue d'ensemble :

Parler de TCP/IP, c'est parler de différents concepts. On pourrait grossièrement traduire TCP/IP par :« Protocole de communication pour la transmission de données »».

TCP : Transmission Control Protocol.

IP : Internet Protocol.

Un protocole de communication est un ensemble de règles permettant à plusieurs ordinateurs de dialoguer entre eux. A la manière des humains, les ordinateurs doivent parler le même langage afin de se comprendre. Tcp/Ip recouvre toute une famille de protocoles :

– UDP : User Datagram Protocol

– FTP : File Transfert Protocol

– TELNET : Terminal Emulation Protocol

– HTTP : Hyper Text Transfert Protocol

TCP / IP fournit trois couches de services comme indiqué dans la T**able 2.9**.

Services d'application
Service de transport sécurisé
Service de livraison de paquets sans connexion

Table 2.9. Les trois couches de services Internet

Le protocole qui décrit cela s'appelle le protocole Internet abrégé en IP.

IP a trois fonctions importantes :

• Spécification du format du protocole.

• Routage du paquet via un certain chemin d'Internet.

• Spécification de la manière dont les paquets doivent être traités et comment gérer les erreurs, etc.

2.9.3 Vue d'ensemble des applications TCP/IP

2.9.3.1 Modèle client / serveur :

La plupart des applications TCP/IP fonctionnent sur le modèle client / serveur. Un serveur est une machine TCP/IP sur laquelle tourne un logiciel serveur qui a pour rôle principal d'attendre un message de la part d'un client. Il analyse la requête du client, formate sa réponse et la renvoie au client. L'exemple typique est le navigateur web, qui demande au serveur de lui envoyer une page. La demande se fait sous la forme d'une chaîne de caractères : « http://www.google.fr/index.html ». Le serveur (en l'occurrence la machine qui a pour nom « www » dans le domaine « google.fr ») renvoie le contenu de la page « index.html » (<html><body> ... </html></body>), et le logiciel client l'interprète et l'affiche en retour.

2.9.3.2 Telnet (Terminal Emulation Protocol) :

Telnet permet à un utilisateur de se connecter à distance sur un hôte. L'utilisateur travaille sur l'hôte distant comme s'il était directement connecté dessus. Les séquences de touche tapées sur l'ordinateur sont envoyées à l'hôte qui les interprète et renvoie les réponses à l'ordinateur appelant.

2.9.3.3 Ftp (File Transfert Protocol) :

Ftp permet de transférer des fichiers entre deux machines sur un réseau TCP/IP. Le client se connecte au serveur distant et établi une session interactive. Il peut alors visualiser les fichiers et les répertoires distants et lancer des commandes de transfert.

2.9.3.4 Smtp (Simple Mail Transfert Protocol) :

Smtp permet à un utilisateur d'envoyer un message à un destinataire connecté à un réseau TCP/IP. Le message est composé sous forme de texte, et l'utilisateur tape

l'adresse électronique du destinataire, l'objet du message et le texte lui-même. Smtp utilise TCP/IP pour envoyer ce message à un serveur de messagerie. Les serveurs de messagerie agissent comme des relais et délivrent leurs messages au destinataire.

2.9.3.5 Snmp (Simple Network Management Protocol) :

Snmp permet la gestion à distance de périphériques tels que les ponts, routeurs ou switches. Un agent snmp doit tourner sur ces périphériques. Une station Snmp envoie des requêtes pour lire ou modifier les paramètres d'un périphérique. Il utilise UDP et IP.

2.9.3.6 Dns (Domain Name System) :

Dns constitue un annuaire électronique permettant de nommer les différentes ressources d'un réseau. Dns associe les noms des périphériques à leur adresse IP. Par exemple l'hôte www.google.com porte l'adresse IP : 216.58.205.206. Les noms Dns jouent un rôle prépondérant dans tous les protocoles TCP/IP, car ils permettent de travailler avec des mots plutôt que des chiffres.

2.9.3.7 Http (Hyper Text Transfert Protocol):

Http est un protocole permettant d'envoyer des pages web à un ordinateur équipé d'un navigateur. Ce navigateur peut lire des documents textes, graphiques, audio ou vidéo.

2.9.4 Routage :

Le routage est la tâche consistant à trouver un chemin d'un émetteur à une destination souhaitée. Il se réduit essentiellement à trouver des routeurs entre des réseaux. Aussi longtemps qu'un message reste sur un réseau ou sous-réseau unique, tout problème de routage est résolu par une technologie qui est spécifique au réseau. Par exemple, Ethernet définit un moyen par lequel tout émetteur peut parler à toute destination spécifiée à l'intérieur de ce propre réseau. Le routage IP entre en jeu essentiellement quand les messages doivent aller d'un émetteur sur un tel réseau vers une destination située sur un autre réseau. Dans ce cas, le message doit traverser des routeurs connectant les réseaux. Si les réseaux ne sont pas adjacents, le message peut

traverser plusieurs réseaux intermédiaires, et les routeurs les connectant. Une fois que le message arrive sur un routeur situé sur le même réseau que la destination, la technologie propre de ce réseau est utilisée pour atteindre la destination.

2.10. Les Avantages du système SCADA :

De toute évidence, le coût initial d'un système SCADA doit être justifié. Quelques raisons typiques pour la mise en œuvre d'un système SCADA sont :

• Amélioration du fonctionnement de l'usine ou du processus entraînant des économies en raison d'optimisation du système.

• Augmentation de la productivité du personnel.

• Amélioration de la sécurité du système en raison d'une meilleure information et d'un meilleur contrôle.

• Protection de l'équipement de la centrale.

• Protection de l'environnement contre une panne du système.

• Amélioration des économies d'énergie grâce à l'optimisation de l'usine.

• Une réception améliorée et plus rapide des données afin que les clients puissent être facturés plus rapidement et avec précision.

• Réglementations gouvernementales pour la sécurité et la mesure du gaz (pour les redevances et taxes, etc.).

2.11. Sécurité du SCADA : Menaces, Vulnérabilités et conséquences :

Les vulnérabilités peuvent être d'origines multiples et l'objet de ce guide n'est pas de les répertorier.

Les besoins croissants de consolidation des données de l'entreprise, de leur accès en temps réel depuis n'importe quel point de la planète, la réduction des coûts de développement et de possession ainsi que les contraintes de planning ont précipité la convergence du domaine de l'informatique industrielle et de l'informatique de gestion.

Les réseaux Ethernet sont désormais employés dans les systèmes industriels jusque dans le domaine des bus de terrain. Ils offrent de nouvelles fonctionnalités comme la mutualisation des infrastructures réseau et la possibilité d'utiliser les couches IP (pour la télémaintenance par exemple).

Les outils de développement, de maintenance et télémaintenance sont aujourd'hui entièrement développés sur des briques génériques issues de l'informatique de gestion (plateforme .Net, Java par exemple). Le Smart Grid est basé sur ces capacités. La figure 2.12 montre un exemple de grille intelligente du système SCADA.

La standardisation des systèmes et les nouvelles fonctionnalités ont apporté aux systèmes industriels les vulnérabilités du monde de l'informatique de gestion. Les systèmes dits propriétaires, souvent pauvres en mécanismes de sécurité, ne sont pas pour autant à l'abri de vulnérabilités pouvant être exploitées par des attaquants motivés et organisés.

Alors que le monde de l'informatique de gestion parvient à corriger régulièrement les vulnérabilités, notamment par l'application de correctifs publiés par les constructeurs et les éditeurs de logiciels, le monde industriel, de par ses contraintes de disponibilité et de sûreté, ne peut pas adopter les mêmes protections. Cette différence de réactivité face aux vulnérabilités publiques est un des principaux risques des systèmes d'information industriels.

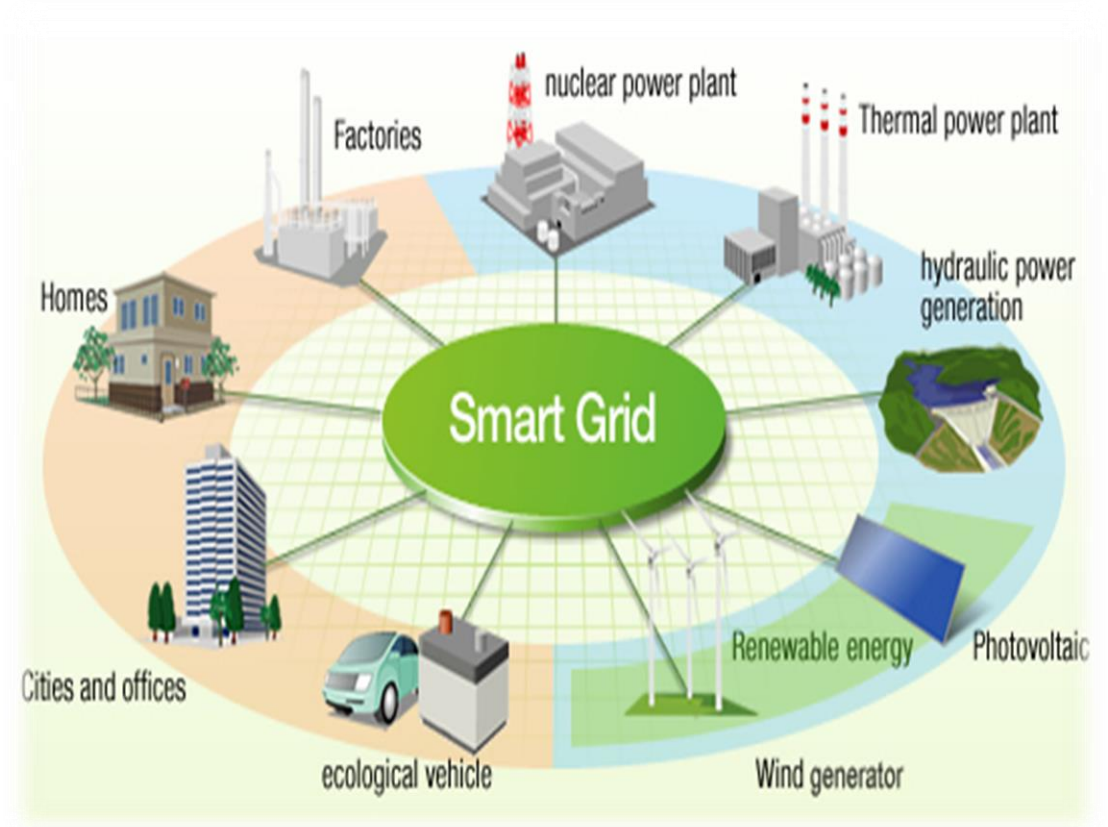

Figure 2.12 : SCADA grille intelligente

2.12. Menaces :

2.12.1. Menaces pour l'environnement :

Les équipements du système SCADA installés dans le système doit être protégé contre les effets de la poussière, la saleté, l'eau, agents corrosifs, autres fluides et contamination par emplacement approprié au sein de l'établissement ou en spécifiant des enclos appropriés pour l'environnement.

2.12.2. Menaces électroniques :

Les menaces électroniques aux systèmes SCADA comprennent des tensions transitoires, interférences de radiofréquence (RFI), armes de RF, la différence de potentiel au sol et impulsion électromagnétique (EMP). Ces menaces peuvent tous être largement atténués par une conception adéquate des systèmes.

2.12.3. Sécurité matérielle :

En général, l'équipement du système SCADA doit être placé à l'intérieur des zones sécurisées, ayant le même degré de sécurité jugé approprié pour les systèmes pris en charge. Toutefois, la nature électronique de ces systèmes offre des possibilités de compromis en provenance de l'intérieur et à l'extérieur de la zone sécurisée qui doit être abordée.

2.12.4. Les réseaux de communication et d'information :

Les connexions entre les systèmes SCADA et réseaux qui s'étendent entre établissements en un même endroit introduisent la menace d'attentats.

a. Ces attaques sont de plusieurs types :

1. Un accès non autorisé d'un utilisateur (piratage).
2. L'écoute ; enregistrement des données transmises.
3. Interception des données, modification, retransmission.
4. La rediffusion des données interceptées et enregistrées.
5. Un déni de Service ; inondation du réseau avec le trafic.

b. La meilleure défense contre ces menaces est d'éviter complètement les connexions de réseau avec d'autres réseaux intérieur ou extérieur à l'installation. S'ils doivent être utilisés, les techniques de cryptage de données doivent être appliquées à tout le trafic de réseau. Envisager également le moyen de renforcer la sécurité supplémentaire suivant :

1. physiquement déconnecter quand pas en service ; applicables aux connexions dial-up pour le service du vendeur.
2. utilisation fibre optique media qui ne peut pas être exploité ou intercepté sans perte de signal à la fin de la réception.
3. circulation unidirectionnelle ; est autorisée la transmission alarme et état seulement avec aucun contrôle.

2.13. Autres défis de vulnérabilité :

Dans nos jours les défis de vulnérabilité du système SCADA augmentent de plus en plus, on peut citer les défis comme suit :

- La gestion de la configuration n'est pas pratiquée au-delà des systèmes affectant directement les opérations physiques [16].
- L'interconnexion et les interdépendances ne sont pas largement comprises.
    - Les limites des systèmes et des autorités (en particulier les systèmes d'information) deviennent floues.
    - Le niveau de confiance accordé est souvent injustifié
    - Le partitionnement des systèmes logiques pour contrôler l'accès et limiter l'influence n'est pas largement utilisé.
    - Aucune validation explicite de la sécurité des fournisseurs
- Capacité de détection, de déclaration, de récupération et de médecine légale limitée

2.14. Conclusion :

L'avenir des systèmes SCADA est lié aux «services d'information de la société». La tendance générale dans les affaires est de déplacer toutes les données, y compris le système SCADA sur le format HTML.

Cela intégrera le système SCADA dans une base de données complète de l'entreprise. Les améliorations matérielles dans le passé ont été dissimulées par un meilleur logiciel. Cela continuera dans l'avenir. Les entreprises utiliseront www pour accéder aux données SCADA de n'importe où dans le monde. Cela permettra à toute personne de l'entreprise et même au-delà d'avoir accès à SCADA données dérivées.

CHAPITRE 3 : APPLICATION

3.1. Introduction :

D'après l'étude théorique de système SCADA que nous avons présenté au-dessus. Pour éclairer cette étude il faut un exemple ou bien une réalisation pratique illustrative qui explique l'architecture de ce système.

Notre travail consiste, dans une première phase, à réaliser une simulation comportant 3 PCs dont le premier comporte le simulateur d'un PLC siemens SIMATIC S7-300, le deuxième jouant le rôle de PC SERVEUR et hébergeant le logiciel SCADA MOVICON et le dernier PC jouant le rôle de client et hébergeant lui aussi un logiciel Movicon. Voir figure 3.1

Dans une deuxième phase une application pratique a été réalisée au niveau de laboratoire de l'automatique au niveau de département d'électronique de l'université de Badji Mokhtar Annaba.

L'objectif est de visualiser un paramètre ou bien une variable analogique à partir d'un transmetteur de température en basant sur un PC Server, un PC Client pour l'opérateur, les deux PCs doivent être équipés d'un logiciel SCADA, il faut un switch pour créer un réseau et un PLC Siemens « SIMATIC S300 » avec une communication de réseau Ethernet « CP343-1 »

La visualisation de la valeur de température mesurée sur le PC de l'opérateur signifie que la boucle de mesure fonctionne correctement.

3.2. Objectif :

L'objectif de cette application est de réaliser un petit système Scada qui nous permet de visualiser des valeurs analogiques, par exemple une température ou numérique à partir des transmetteurs installés à l'extérieur

3.3. Présentation du (hardware) :

Les figures 3.1 et 3.2 représentent les équipements utilisés dans la phase de simulation.

Les figures 3. 3 et 3.4 représentent les équipements de la réalisation pratique.

Figure 3.1 : PC Server, PC Client et PC (Simulateur PLC)

Figure 3.2 : **moyen de communication**

Figure 3.3 : PLC SIEMENS SIMATIC S300

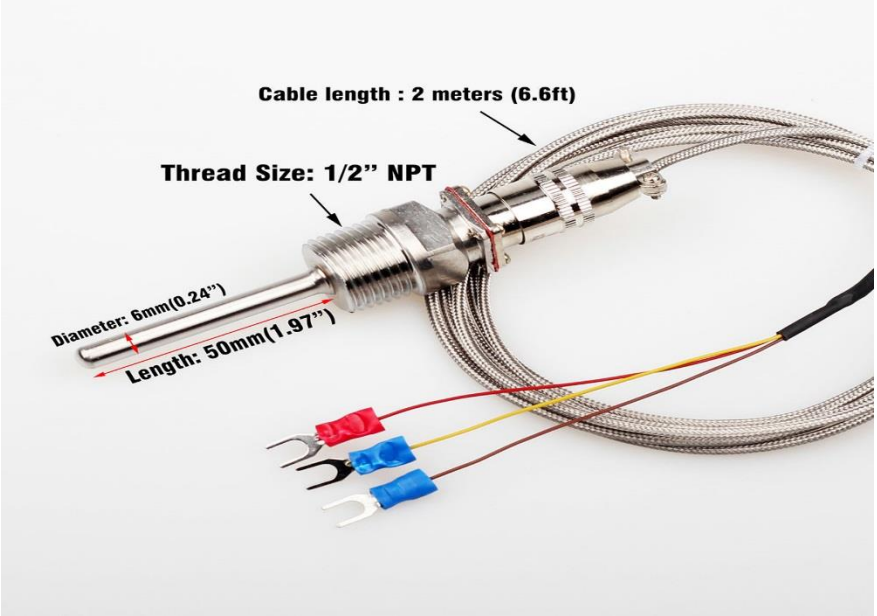

Figure 3.4 : SONDE DE TEMPERATURE PT 100

3.4. Caractéristiques techniques du CPU :

Les caractéristiques techniques de la CPU 314C-2 DP sont :

Une mémoire de travail 96 Ko; 0,1ms/kinst; DI24/DO16; AI5/AO2 intégrées; 4 sorties d'impulsion (2,5kHz); 4 voies pour comptage et mesure avec codeurs incrémentaux 24V (60kHz); fonction de positionnement intégrée; ports MPI+ DP

(Maître ou esclave DP); configuration multi-rangées jusqu'à 31 modules; échange de données direct possible (émetteur et récepteur); équidistance; routage; communication S7 (FB/FC chargeables); Firmware V2.6 [11]

3.5. Eléments de commande et d'affichage : CPU 314C-2DP :

3.5.1. Eléments de commande et de signalisation de la CPU 314C-DP :

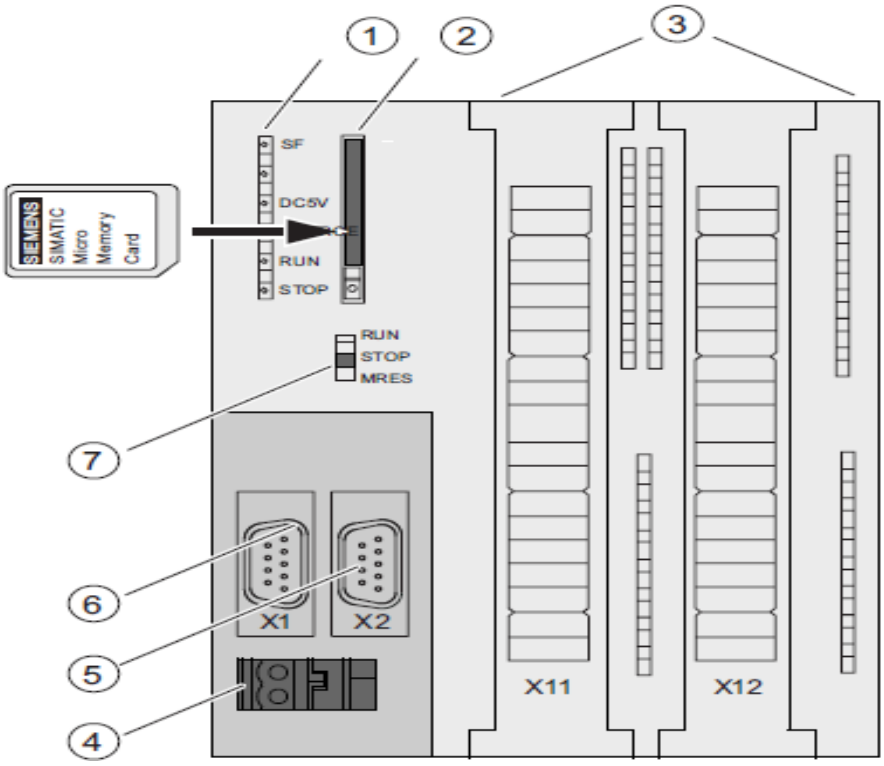

Figure 3.5.1 CPU 314C-2DP

La **figure 3.5.1** montre les éléments de commande et de signalisation de la CPU 314C-DP [11].

Chiffre	Désignation
①	Indicateurs d'état et d'erreur
②	Logement de la micro-carte mémoire SIMATIC avec éjecteur
③	Raccordements des entrées et sorties intégrées.
④	Raccordement de la tension d'alimentation
⑤	2ième interface X2 (PtP ou DP)
⑥	1ière interface X1 (MPI)
⑦	Commutateur de mode de fonctionnement

Le graphique **Figure 3.5.2** vous montre les entrées et sorties numériques et analogiques intégrées d'une CPU, les volets avant ouverts.

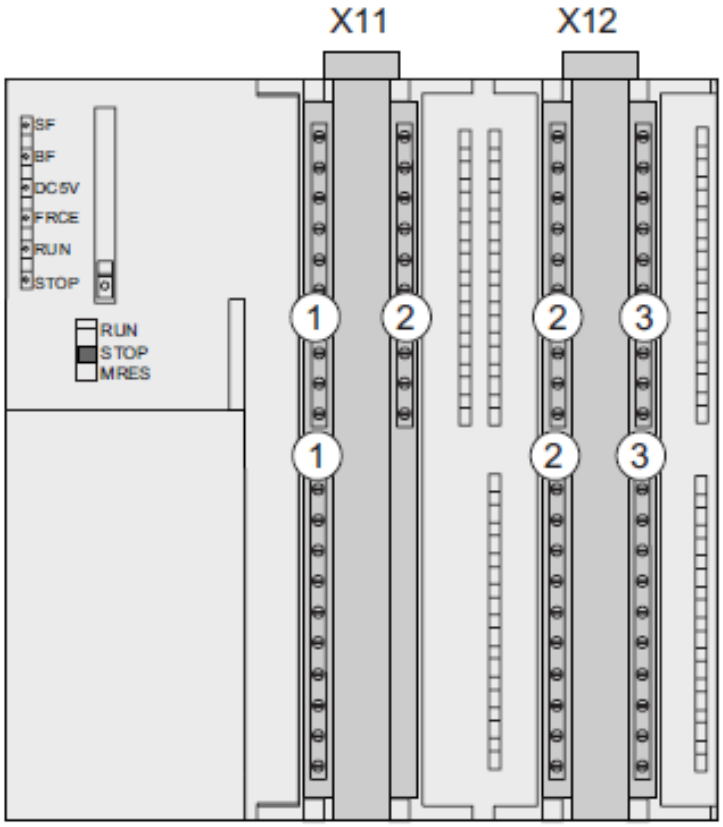

Figure 3.5.2 Les entrées et sorties numériques et analogues intégrées d'une CPU

Chiffre	Désignation
①	Entrées analogiques et sorties analogiques
②	Pour 8 entrées TOR
③	Pour 8 sorties TOR

Logement de la micro-carte mémoire SIMATIC

Une micro-carte mémoire SIMATIC est utilisée comme cartouche mémoire. Elle peut faire office de mémoire de chargement et de support de données amovible [11].

Remarque :
Ces CPU ne possédant pas de mémoire de chargement intégré, vous devez enficher une Micro Memory Card SIMATIC dans la CPU pour le fonctionnement.

3.5.2. Schéma de connexion de la périphérie TOR/analogique intégrée :

Les entrées/sorties intégrées des CPU 31xC peuvent être utilisées pour les fonctions technologiques et/ou en tant que périphérie standard.
Les figures Figure 3.5.5 présentent l'utilisation éventuelle des entrées/sorties intégrées sur le CPU [11].

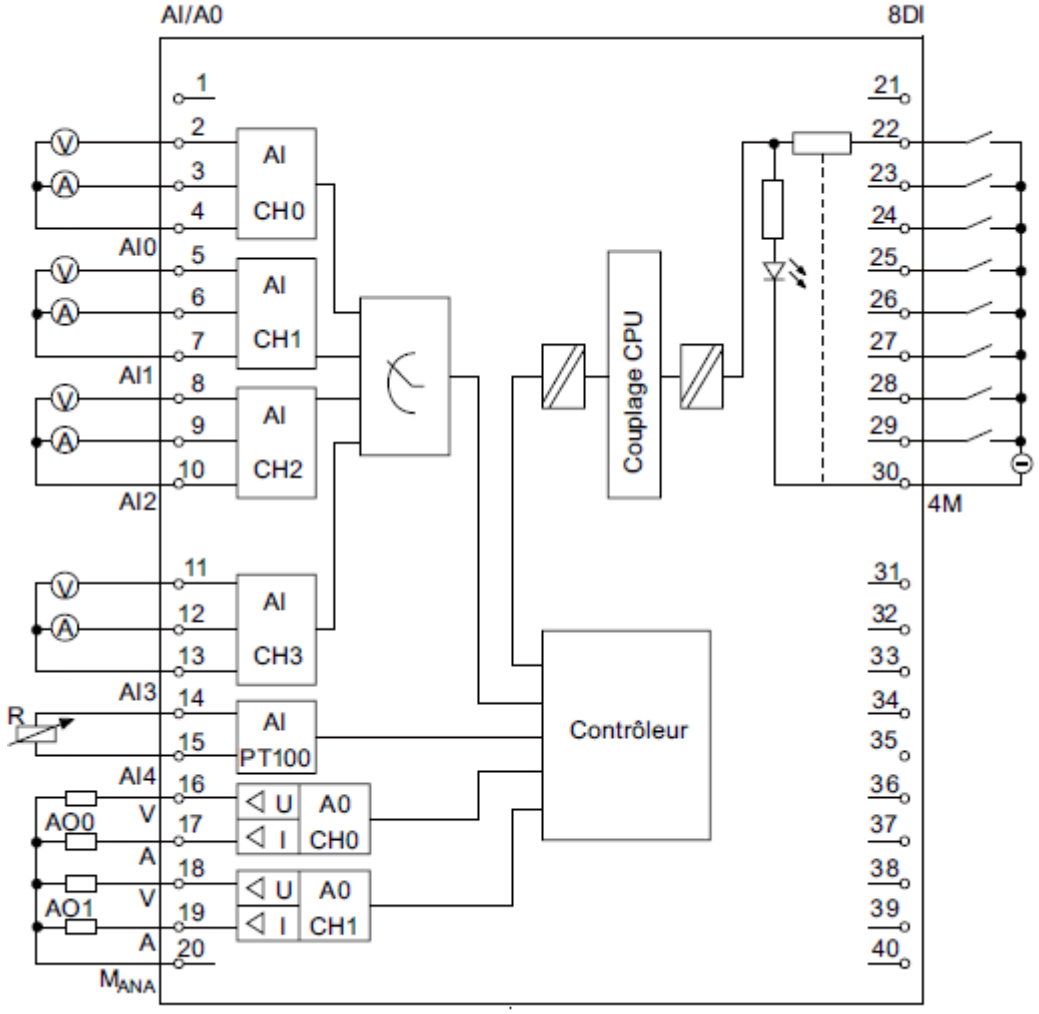

Figure 3.5.5 : Schéma de connexion de la périphérie TOR/analogique intégrée

3.5.3. Raccordement : exemple de montage 2 , 3 et 4 fils de résistances et RTD:

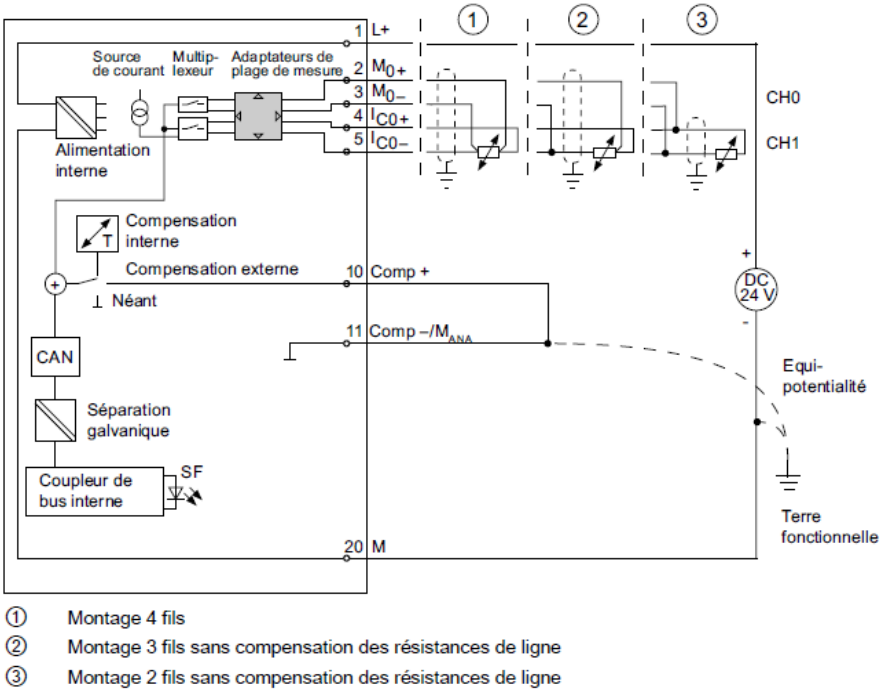

Figure 3.5.6 : Schéma de branchement des résistances

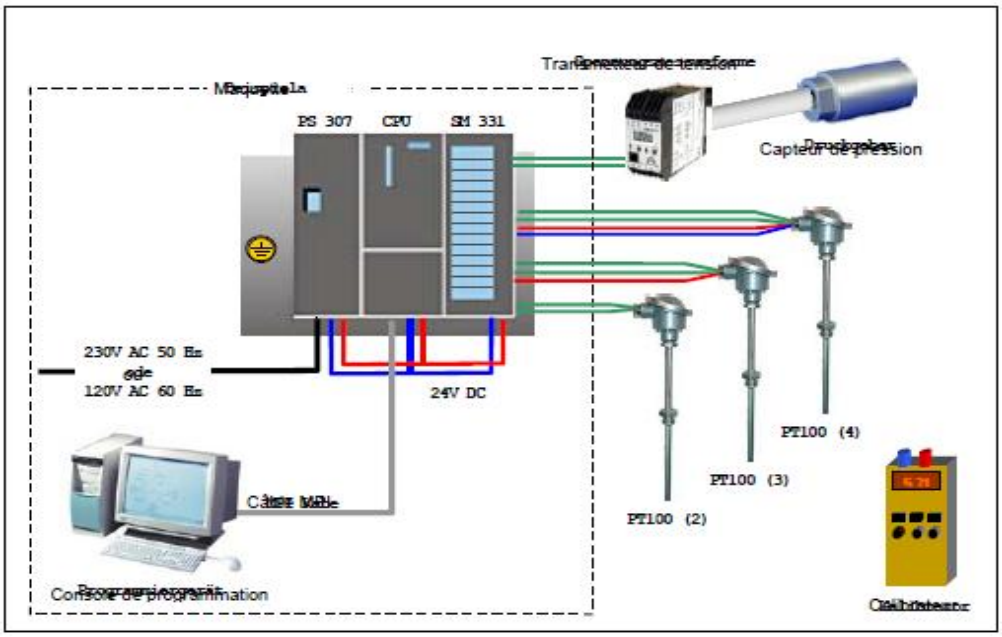

Figure 3.5.7 : Composants de la maquette commis l'exemple (RTD).

Les figures **3.5.6 et 3.5.7** montrent les différents cas de câblage concernant les sondes des sondes Pt100 de 2, 3 et 4 fils.

3.5.4. Configuration et paramétrage du module d'entrée analogique (SM331) :

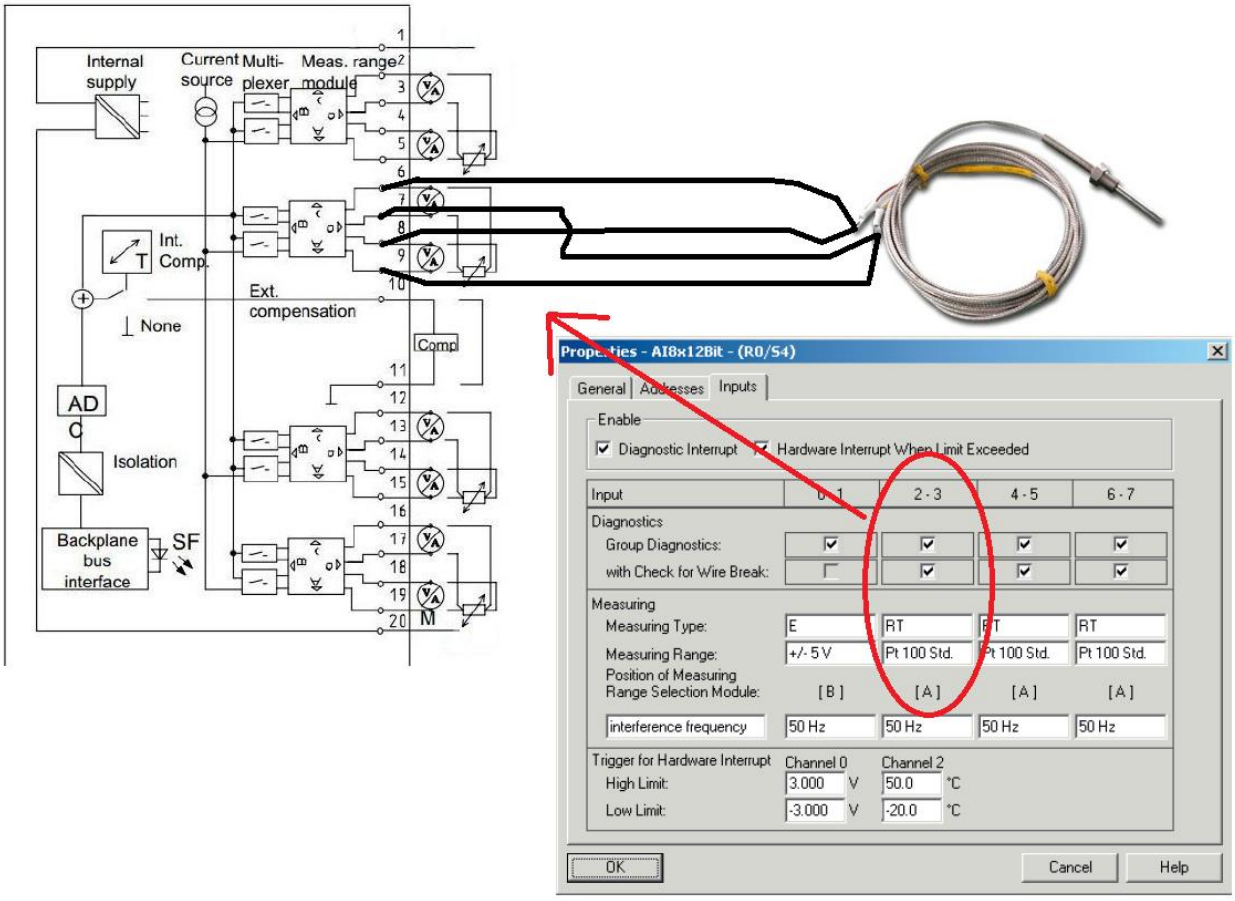

Figure 3.5.8 : Configuration du module de l'entrée analogique du PT100

La figure 3.5.8 montre la configuration du module de l'entrée analogique du Pt100, en utilisant le logiciel Step7 [12].

3.6. Présentation du logiciel SCADA :

Le logiciel utilisé est **Movicon ™ 11** qui représente la technologie puissante et flexible Scada / HMI, une plate-forme pour la supervision et le contrôle industriels. Movicon représente plus de 15 ans d'évolution technologique basée sur les concepts de simplicité, d'évolutivité, de puissance et d'ouverture. La technologie exclusive «XML-inside» de Progea fonctionne désormais parfaitement dans la version 11.4, entièrement compatible avec la version précédente, et renouvelle les concepts de supervision en fonction de la modularité et de l'ouverture, offrant la technologie Serveur et client OPC DA 2.4 et bientôt (Rel. 11.5), même la technologie OPC UA Server & Client.

En maintenant et en développant ses caractéristiques d'évolutivité, Movicon ™ 11 est proposé sur le marché en tant que plate-forme logicielle standard pour tous ceux qui opèrent dans l'automatisation industrielle, la télécommande et l'automatisation du bâtiment, en tant que logiciel Scada / HMI unique pour tout type de déploiement et de matériel, comme montrer sur la figure 3.6.

Movicon peut être déployé à la fois dans des panneaux tactiles et / ou des appareils mobiles basés sur WinCE, que ce soit un écran tactile PC avec Win7 / XP Embedded, des systèmes basés sur un PC avec Windows 8 ou Windows Server, dans une architecture client / serveur complexe et redondant, en se connectant à travers Avec n'importe quel type de PLC et bus de terrain industriel ou civil. Chaque application Movicon, que ce soit dans Windows ™ 8, Windows ™ 7, Windows ™ Embedded, Windows ™ CE, prend en charge la puissante technologie de réseau dans laquelle chaque périphérique peut devenir un client, un serveur ou un serveur Web indifféremment [13].

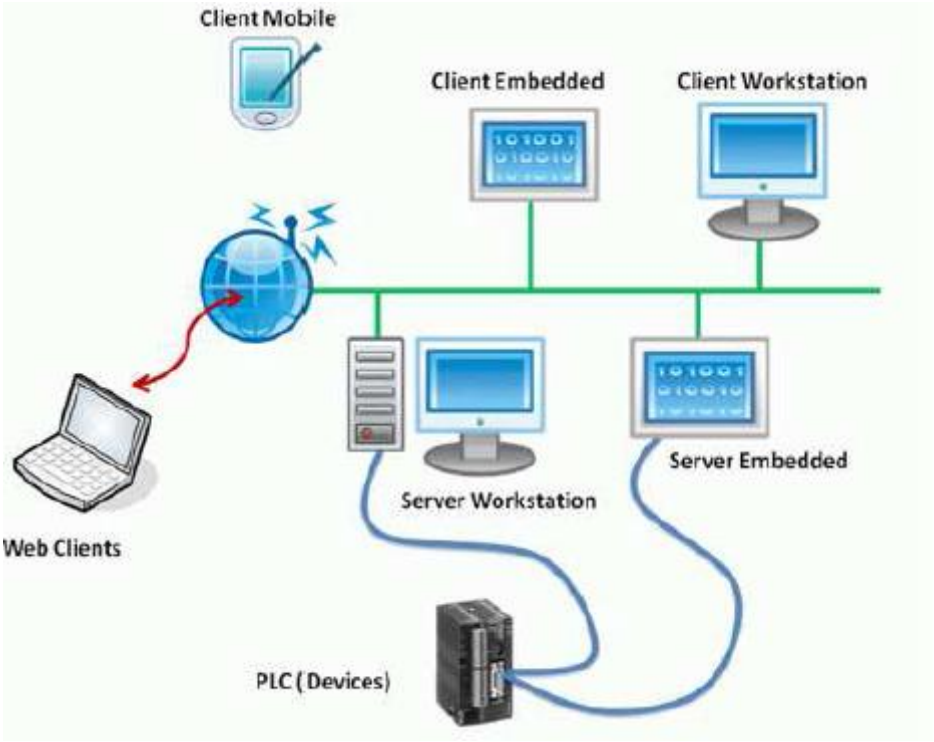

Figure 3.6 Configuration hardware du MOVICON

3.6.1. Comment créer et structurer le projet ?

En lançant Movicon sans options sur la ligne de commande, le logiciel démarre en mode Programmation (Développement). Généralement, le programme s'ouvre sur le dernier projet utilisé [13].

La zone de travail s'affichera vide à la première exécution.

La zone de travail utilise la technique moderne des fenêtres escamotables. Il suffit donc de pointer la souris sur l'onglet de la fenêtre intéressée pour la faire apparaître dans la zone de travail. Pour maintenir l'affichage des fenêtres de travail, utiliser les commandes correspondantes comme indiqué :

Remarque : pour afficher les fenêtres de travail, il suffit de les pointer avec la souris, et d'utiliser la commande de stationnement prévue à cet effet pour maintenir leur affichage.

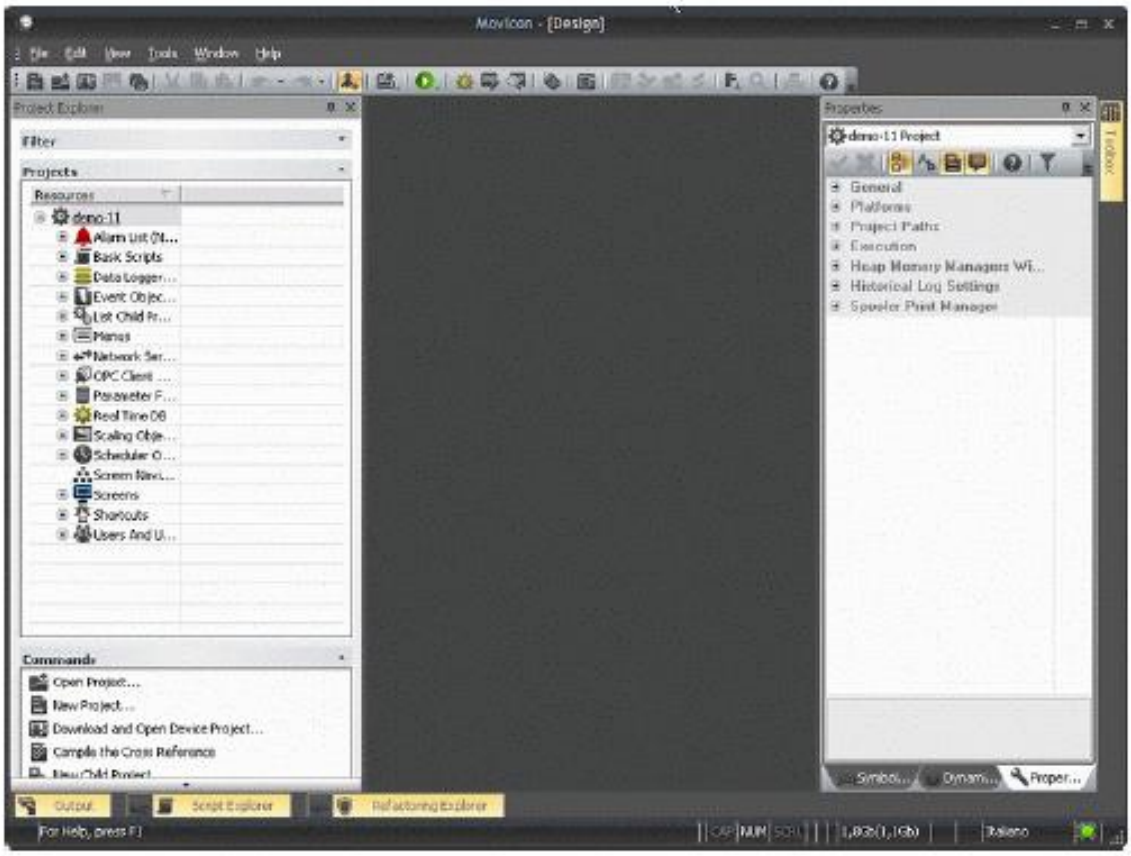

Figure 3.6.1 : Zone de travail Movicon avec les fenêtres maintenues.

3.6.2. Structure de projet :

Les projets de Movicon sont constitués d'un ensemble de fichiers en format XML. Chaque ressource du projet est sauvegardée sur un fichier XML dans le dossier du projet correspondant et dans le sous-dossier des ressources correspondantes.

Sauf indication contraire, les projets sont implicitement sauvegardés dans le dossier "Documents\Movicon Projects\".

Bien que « ouvrables » grâce à l'XML, les fichiers peuvent être codés et compressés par le biais de propriétés du projet.

La structure des fichiers respecte la structure des ressources disposées dans la fenêtre du projet de Movicon.

Examinons à présent en détail, la structure des fichiers du projet avec l'Explorateur Ressources de Windows [13].

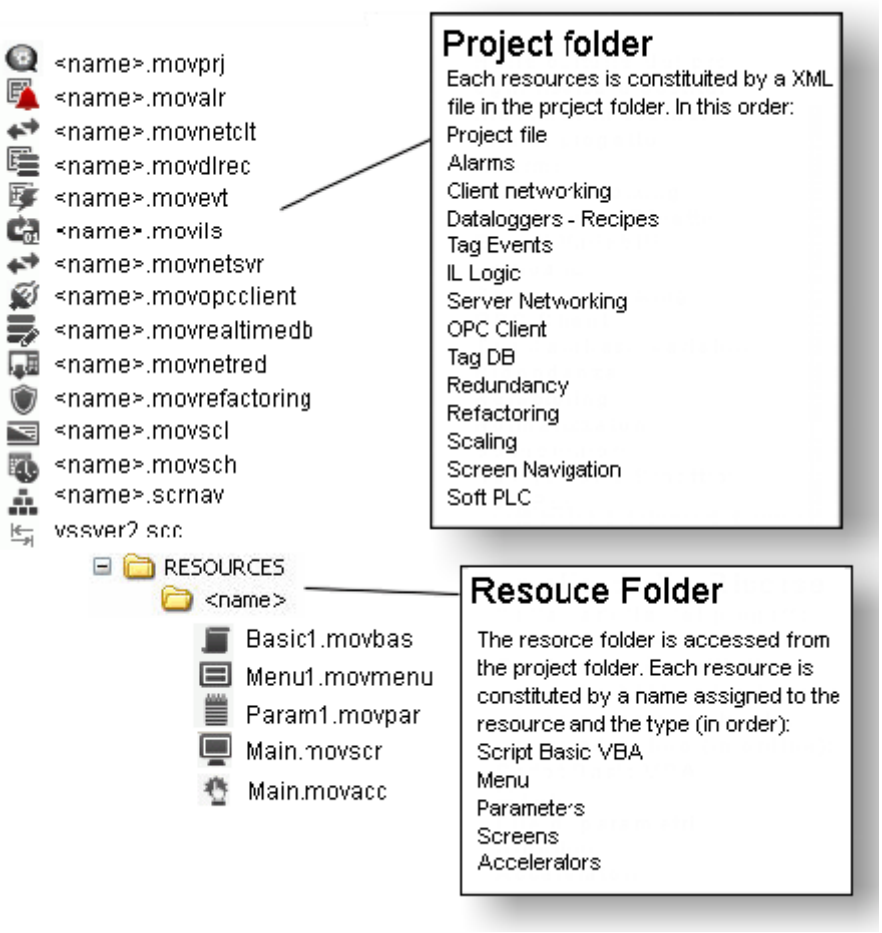

Figure 3.6.2 : Structure de projet :

3.6.3 Configuration du driver :

Prenons comme exemple le driver Siemens S7-TCP/IP. Les techniques sont identiques pour les autres drivers, sauf les particularités de chaque protocole.

1. Il faut d'abord effectuer la configuration des Caractéristiques générales du driver.

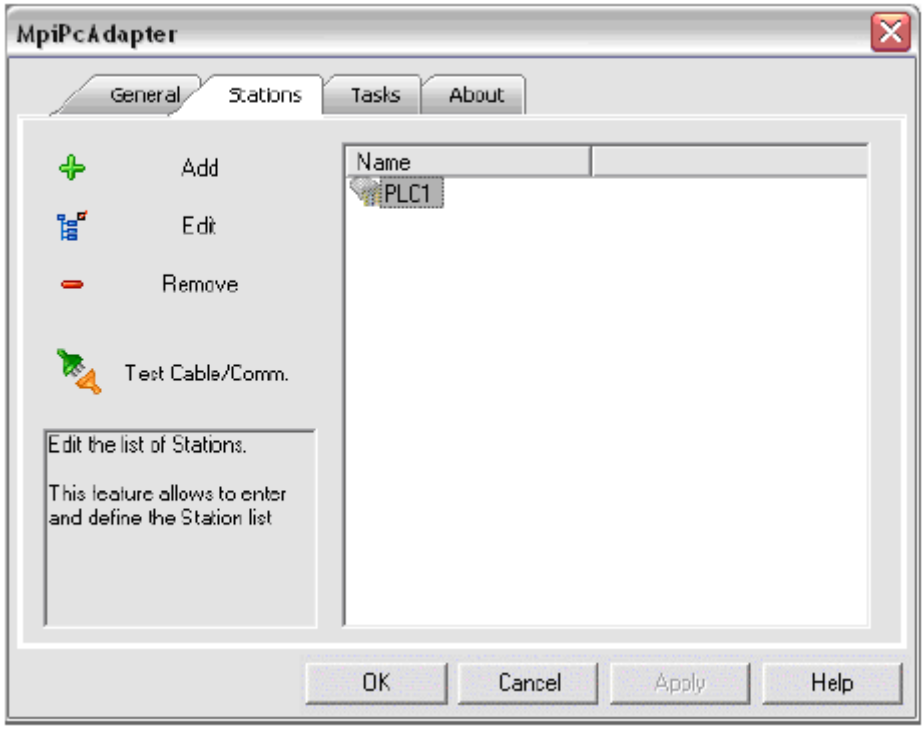

Figure 3.6.3 : Configuration du driver

A ce stade, le driver est inséré. Si le dispositif est connecté et prêt à communiquer, vous pouvez effectuer le test de la communication avec le bouton "Test Câble/Comm.". De cette façon, Movicon vérifiera le paramétrage de la communication avec le dispositif PLC, ainsi que le câblage. Si le test n'aboutit pas, éliminez la cause qui empêche la communication de se dérouler régulièrement.

3.7- La procédure de réalisation de la phase simulation :

Notre réseau constitue d'un PC simulateur hébergé d'un logiciel et un programme de contrôle des informations « Siemens STEP7 » joue le rôle d'un PLC. Plus un PC serveur et un PC client.

La figure 3.7 présente les deux configurions possibles (filaire et sans fil) de la topologie réseau, avec les adresses IP de chaque équipement.

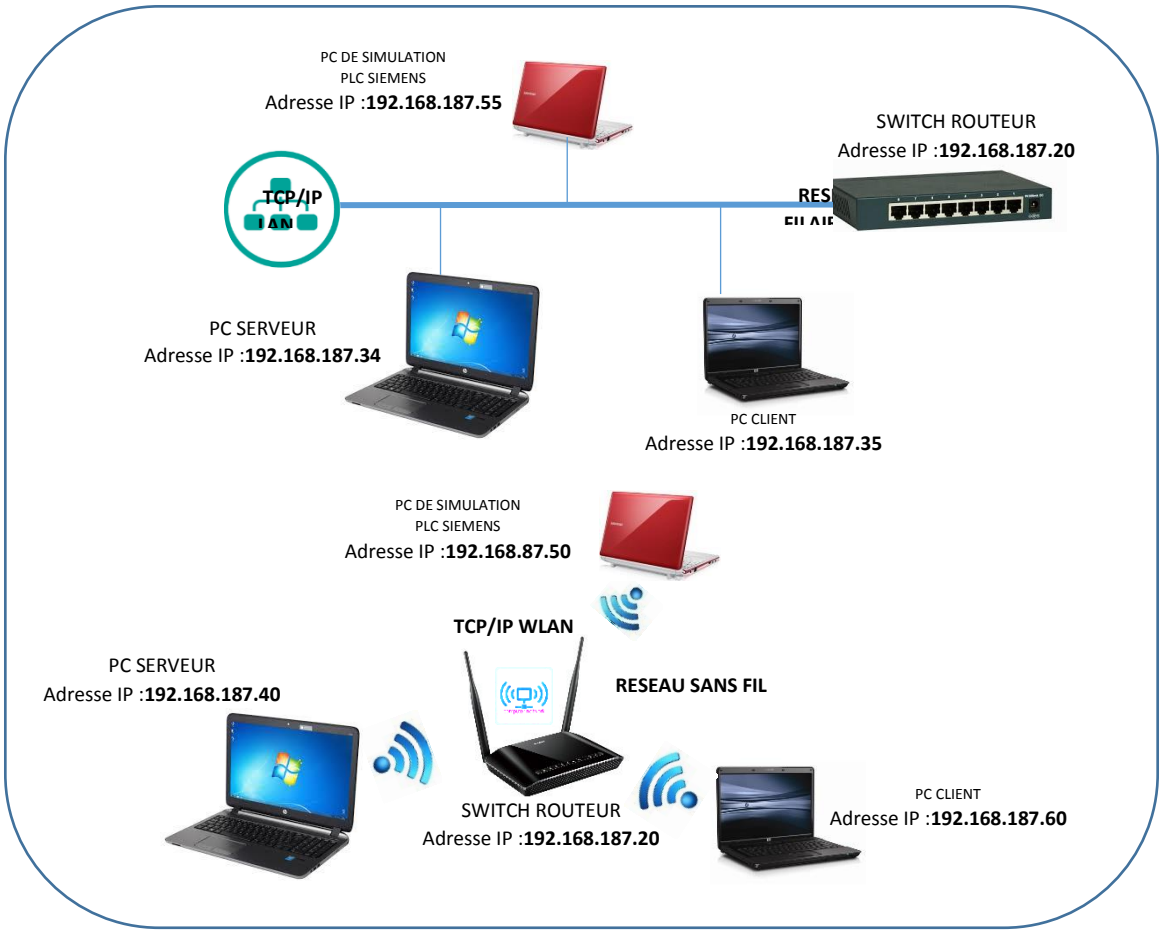

Figure 3.7 : Configuration réseau sans fil et filaire

Pour simuler le système d'acquisition, le contrôle et la supervision des données, nous avons pris comme exemple l'information de la température de l'air comprimé venue du champ à fin de visualiser sur une station d'opérateur, en appelant aussi PC Client, il faut suivre la procédure suivante :

1- Allumer les trois PCs (simulateur client et serveur).
2- Vérifier la configuration réseau qui assure la communication entre les trois PCs .
3- Lancer le logiciel STEP7 sur le PC Simulation et fait un appel de simulateur « PLC-SIM et mettre en mode RUN.
4- Lancer le logiciel Movicon et exécuter le programme de notre application sur le PC Serveur et le PC client.

5- Assurer la communication entre le logiciel Movicon (PC Serveur) et le simulateur PLC-SIM (PC de simulation) par l'installation du driver SIEMENS comme expliquer avant sur le § 3.6.3.

6- Modifier la valeur de température par le curseur qui varie la valeur de notre variable, de l'entrée analogique PEW256, comme montrer sur la figure 3.7.1.

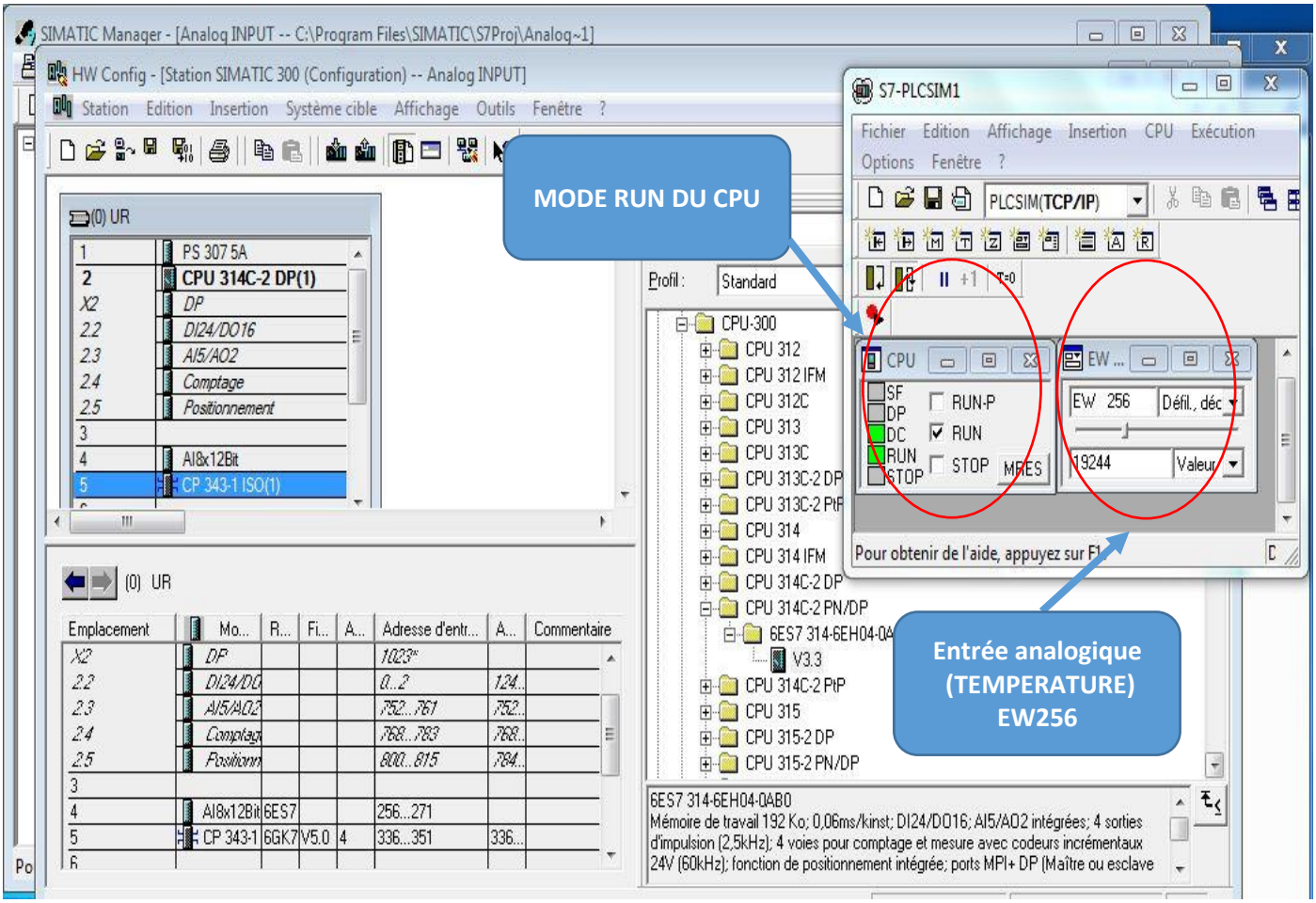

Figure 3.7.1 : PLC-SIM (PC de simulation)

7- Vérifier sur le PC client si la variation du variable analogique sur le PC de simulation agit sur la valeur de température visualisée sur la HMI devant l'opérateur, comme montrer sur la figure 3.7.2 .

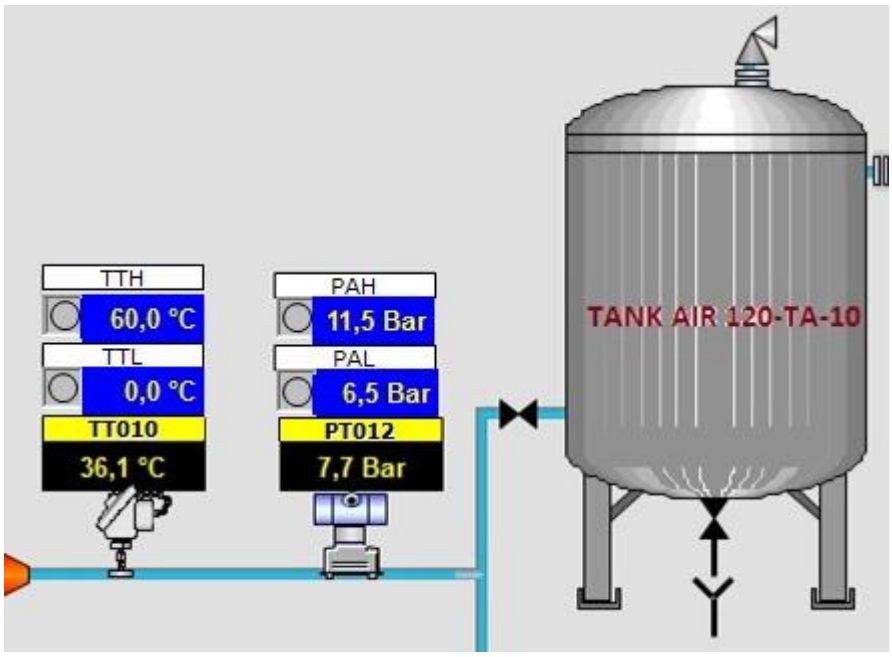

Figure 3.7.2 : Visualisation de température sur le PC client

8- Essayer maintenant de varier la valeur de la température en dépassant le seuil haut, cette fois-ci une alarme sera déclenchée et affichée sur le PC serveur, cette valeur sera enregistrée comme historique, à l'aide du logiciel de base de donnée SQL-Server ,la figure 3.7.3 montre l'apparition de l'alarme sur le PC-Serveur , nous pouvons aussi voir la même alarme sur le PC-Client.

9- Acquitter l'alarme et utiliser en même temps cette alarme pour faire l'analyse et le diagnostic des défauts.

DESCRIPTION	TEMPS ENCL.	ETAT	CONDITION
(AIR) EW256-120-TT-010 HAUTE TEMPERATURE	14/06/2017 ...	APP.	Oui

Figure 3.7.3 : Visualisation d'alarme sur PC-Serveur « Température élevée »

3.8- La procédure de réalisation de la phase pratique :

Notre application a été réalisée sur le laboratoire de l'université Comme vous voyez sur la figure 3.8.

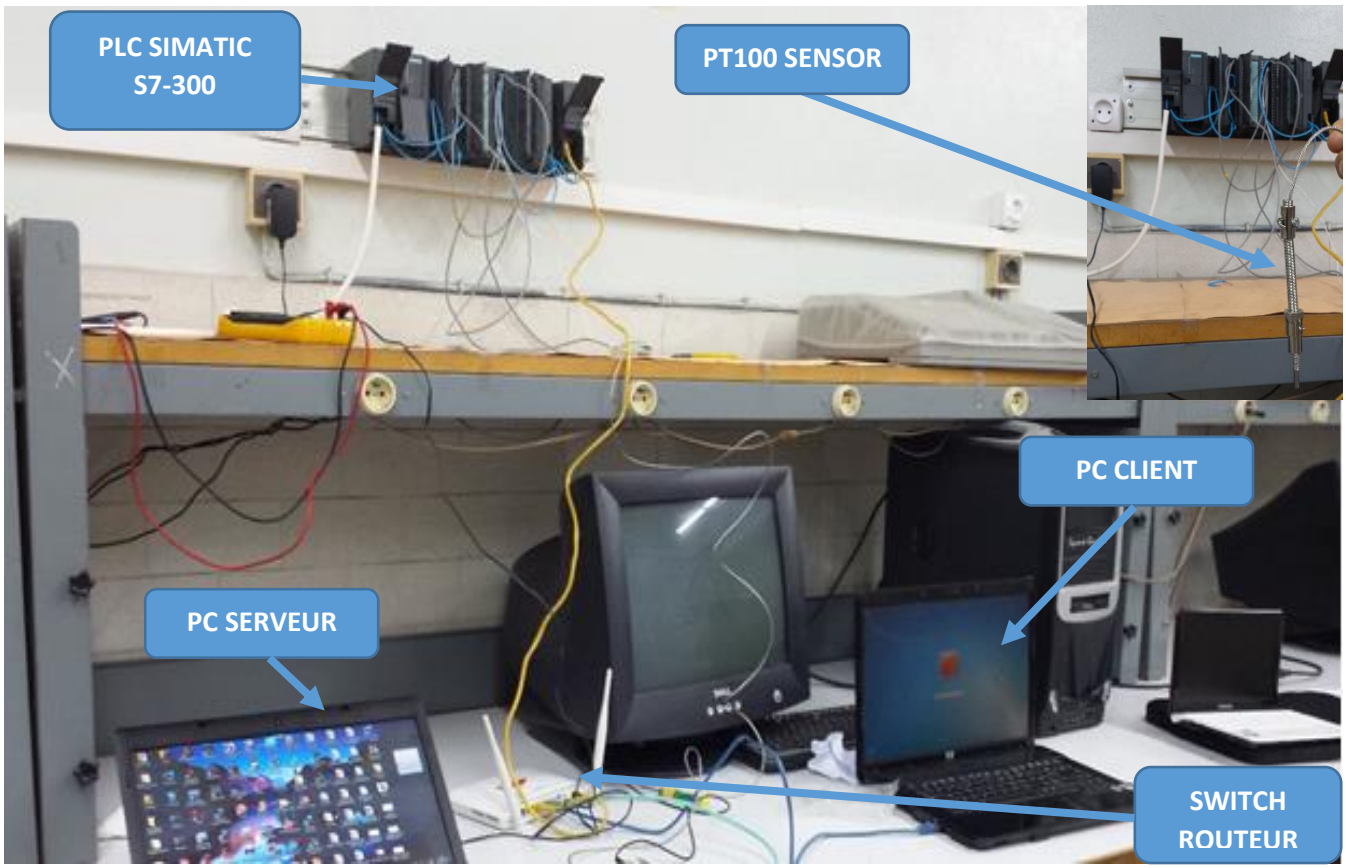

Figure 3.8 : La phase pratique de l'application

L'utilisation d'un automate programmable réel (PLC Siemens Simatic s7-300) fait la différence par rapport à la phase de simulation montrée ci-dessus.

3.9. Conclusion :

D'après l'étude présentée on peut conclure :

- L'application a été réalisée avec succès.
- La réalisation pratique de l'application était bénéfique sur le plan pédagogique et technique aussi, comme on peut tirer les connaissances acquises suivantes :
  - ✓ Le développement d'applications de supervision et de drivers de communication.
  - ✓ La réalisation d'application de supervision mono-postes, réseaux LAN et WLAN.

- ✓ Définition de la base de données des variables : Mise en œuvre des drivers de communication, définition des variables et de leurs caractéristiques (fréquence d'acquisition, adresse automate, historisation, mise à l'échelle…).
- ✓ Définition de la base de données des alarmes : définition des alarmes et de leurs caractéristiques (condition d'alarme, historisation et impression …).
- ✓ Développement des synoptiques, suivant l'analyse fonctionnelle.
- ✓ Définition des recettes de développement des taches d'automatismes avec les langages Structure, Ladder et Log.
- ✓ Développement des rapports et mise en place de procédures de génération automatique.
- ✓ Développement des Script permettant l'automatisation de certaines fonctions métiers.
- ✓ Développement de drivers de communication sur liaison Série , Ethernet via TCP/IP et OPC etc…

CONCLUSION GENERALE :

Ce travail nous a permis de mieux connaitre le domaine de l'industrie d'énergie et précisément la production de l'électricité en utilisant des turbines à gaz.

Ce travail s'est focalisé sur le système de contrôle industriel (PLC, DCS, SCADA),

La technologie SCADA fournit un niveau de sécurité très élevé, et augmente l'efficacité du système et optimise aussi bien le temps que les ressources. Ainsi « SCADA » est un logiciel conçu spécifiquement pour fonctionner sur des ordinateurs pour le suivi, la supervision et le contrôle des procédés industriels à distance. Ses avantages sont :

- Information en temps réel sur l'état des dispositifs.
- Contrôle à distance des stations, du diagnostic et de la maintenance.
- Fournit un contrôle intégré tous des ressources et des informations sur le système industriel.
- Capacité à exécuter des programmes sur différents dispositifs de surveillance de l'usine, en évitant la nécessité d'une surveillance humaine continue.
- Agissant directement sur le processus par un ordinateur.
- Affichage des signaux du système, tels que des évènements et des alarmes.
- l'Analyse des historiques et des données stockées.

Le développement scientifique a laissé sa trace sur les systèmes de production donnant naissance au Système Automatisé de Production, et SCADA s'avère être une réponse satisfaisante au paradoxe des paramètres coût-qualité

visés généralement par la gestion de production (Optimisation du coût, de la qualité et des délais).

Malgré les avantages, cités ci-dessus, du système SCADA, il reste néanmoins sujet à des faiblesses représentées par les points de vulnérabilité de pénétration au cœur du système. La nécessité de renforcer les protections contre toutes les formes menaces (piratage, virus, espionnage industriel,...)

Enfin, ce travail nous donnons une image claire et générale sur les systèmes de contrôle et de supervision et l'acquisition des données des grandes et petites usines, qui fonctionnent d'une manière continue et sans interruption à l'aide des ingénieurs et des techniciens, ces derniers sont familiarisés avec les différents systèmes proposés par les constructeurs spécialisés sur le marché.

Références Bibliographiques

[1] ***Guide to Supervisory and Data Acquisition -Scada and Industrial Control Systems Security-***2007 Recommendations of the National Institute of Standards and Technology
Keith Stouffer, Joe Falco, Karen Kent.

[2] ***Supervisory Control and Data Acquisition (SCADA) Introduction.*** Pacific Northwest National Laboratory Grainger Lecture Series for the University of Illinois at Urbana-Champaign September 15, 2005
Jeff Dagle, PE.

[3] ***Architecture For Secure Scada and Distributed Control System Networks.*** White Paper 2010
Juniper Networks, Inc.

[4] ***Modèles, méthodes et outils pour l'analyse, la conception et l'implantation des*** *Systèmes de contrôle et de commande industriels Systèmes de supervision industrielle Systèmes d'informations industrielles :* Université Henri Poincaré Nancy 1
Jean-François PETIN

[5] ***Protection multicouche pour les systèmes de contrôle industriel et les réseaux SCADA*** Livre blanc Check Point Software Technologies Ltd. Mars 2013

[6] ***Standards for Security Categorization of Federal Information and Information Systems,*** **February** 2004. FIPS PUB 199

[7] ***Minimum Security Requirements for Federal Information and Information System***, March 2006. FIPS PUB 200,

[8] ***Practical SCADA for Industry*** Linacre House, Jordan Hill, Oxford OX2 8DP
200 Wheeler Road, Burlington, MA 01803 First published 2003
David Bailey, Edwin Wright

[09] ***Guidelines on Active Content and Mobile Code***, October 2001. NIST SP 800-28

[10] ***Remote Data Acquisition System for Hydro Power Plants***- Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006

[11] SIMATIC ***S7-300 CPU 31xC et CPU 31x : Caractéristiques techniques*** Manuel 6ES7398-8FA10-8CA0 06/2008 A5E00105476-08

[12] ***Système d'automatisation S7-300 Caractéristiques des modules*** *02*/2013 A5E00105506-08 Chapitre 6.7 Module d'entrée analogique SM 331 ; AI 8 x 12 bits ; (6ES7331-7KF02-0AB0), p.385-413.

[13] ***Movicon 11 Supervision and control XML-based from Windows Vista to Windows CE*** Programmer Guide Version 11.3 Ed. Feb. 2012 Cod. DOCS 11 DEV-E Build 1101

[14] ***Application of Functional Analysis on a SCADA System of a Thermal Power Plant***- Advances in Electrical and Computer Engineering Volume 9, Number 2, 2009 p90-98

[15] ***Techniques de l'ingénieur : Air comprimé dans l'industrie*** Doc. BM 4 130 – 1
Bernard GOURMELEN Jean-François LEONE

[15] ***Transmitting electric power system dynamics in SCADA using polynomial fitting***- www.scichina.com

[16] ***Security & Vulnerability in Electric Power Systems***- NAPS 2003, 35th North American Power Symposium, University of Missouri-Rolla in Rolla, Missouri, October 20-21, 2003. pp. 559-566.