République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de La Recherche Scientifique

Université 20 Aout 1955 Skikda

Faculté De Technologie

Département De Génie Electrique

Mémoire présenté en vue de l'obtention du diplôme de

MAGISTER EN AUTOMATIQUE

Option : Diagnostic Et Surveillance Des Systèmes

Elaboré par : CHEIKH MAROUANE

Thème : TELEGESTION DANS L'INDUSTRIE DE L'EAU PAR LES TECHNOLOGIES DU WEB

Devant le jury composé de :

Dr. M. Rouainia	MCA	Présidente	Université de SKIKDA
Pr. N. Doghmane	Prof	Rapporteur	Université d'ANNABA
Dr. A. Lachouri	MCA	Examinateur	Université de SKIKDA
Dr. K. Khelil	MCA	Examinateur	Université de SOUK AHRAS

Année 2013

DEDICACE

Je dédie ce mémoire : A mon petit trésor ma fille Alaa

A ma mère et mon pére qui m'ont éclairé mon chemin et m'ont encouragé toute au long de mes études

A ma femme qui m'a beaucoup aidé à la réalisation de ce mémoire

A mes frères : Houssam, Lamine et Moataz

A ma grande famille et mes amis.

REMERCIMENT

Je tiens tout d'abord à remercier Monsieur Noureddine Doghmane, Professeur à l'Université d'Annaba, qui a assuré l'encadrement de mon travail où Il a été une source de motivation et d'encouragement.

J'adresse également mes sincères remerciements :

A Mounira Rouania, Docteur à l'Université de Skikda, pour avoir accepté d'être présidente du jury de cette thèse.

A Messieurs : Abederrazek Lachouri, Docteur à l'Université de Skikda, Khaled Khelil, Docteur à l'Université de Souk Ahras, pour l'honneur qu'Ils m'ont fait en acceptant de participer à ce jury.

Marouane

Résumé

ملخص

التحكم عن بعد في مجال استغلال المياه يكاد يكون تلقائيا إن لم نقل إجباريا ودلك نظرا للتباعد الجغرافي للمنشات المائية كمحطات الضخ و السدود... الخ

إن التحكم عن بعد يجعل المسافات لا معنى لها و دلك لعدم وجود الحاجة للتنقل إلى المنشات بحيث كل العمليات اللازمة للاستغلال يمكن القيام بها عن بعد.

من خلال هدا العمل التجريبي قمنا بتجسيد نظام(SCADA) يتواصل عن طريق شبكة الانترنيت أي أن هده الأخيرة تستعمل بين النهائي الرئيسي و النهائي الثانوي عوضا عن شبكة تواصل خاصة تستعمل لهدا الغرض .

إن اختيار شبكة الانترنيت يخفض و بصفة ملحوظة كلفة هدا النظام. إلا انه يؤثر سلبيا على أمان المعلومات و سرعة نقلها و بالتالي على زمن الرد. اد انه من الواضح أن زمن الرد يرتفع و يقل حفظ المعلومات

إن فكرة تسيير الأنظمة الصناعية بواسطة تكنولوجيا الواب حديثة العهد و يبقى المجال مفتوح من اجل تطوير هده التقنية أكثر فأكثر .

Résumé

La télégestion dans l'industrie de l'eau est une solution idéale voire impérative pour l'exploitation du fait de la dispersion géographique des ouvrages de l'eau. Par télégestion la notion de distance est absurde car le besoin de se déplacer sur les lieux des équipements pour des fins d'exploitation ou de maintenance ne figure pas

Au cours de ce travail expérimental, nous avons réalisé un SCADA qui a comme particularité l'emploi du réseau Internet au lieu des réseaux dédiés classiques, c'est-à-dire que la communication entre le terminal principal et les terminaux déportés est établie via le réseau Internet.

Le choix du réseau Internet réduit nettement le cout d'une application très lointaine mais en contre partie il affecte la fiabilité du système, deux aspects importants à étudier la sécurité et le temps de réponse.

Il est évident que le temps de réponse augmente, cela est dû au trafic du réseau Internet et à la structure même de ce dernier. De même pour la sécurité qui reste loin d'être invulnérable.

L'idée de gérer les systèmes industriels par les technologies de Web est récente, notre travail va tenter de proposer une certaine contribution au développement de ce domaine.

Summary

Remote management in the water industry is an ideal solution even imperative for the operation because of the geographical dispersion of the water equipment. For remote management the concept of distance is absurd because there is no need to move on site for operating equipments or maintenance.

During this experimental work, we achieve a particular SCADA that has a special characteristic that it use the Internet instead of traditional dedicated networks, that is to say that communication between the main terminal and the remote terminals is via the Internet. The choice of the Internet dramatically reduces the cost of an application however it affects the reliability of the system, two important aspects to study the response time and network security.

It is obvious that the response time increases, it is the traffic of the Internet and the structure itself of the latter to the liver, also security remains far from to be invulnerable. The idea of managing industrial systems through Web technologies is new; our work will contribute to the development of this area while recognizing that much remains to be done.

Liste Des Abréviations

Liste des Abréviations

LAN:	Local Area Network
MAN:	Métropolitain Area Network
WAN :	Wide Area Network
OSI:	Open System Interconnection
TCP:	Protocole de Contrôle de Transmissions
IP:	Internet Protocole
TPDU:	Transport Protocol Data Unit
SPDU:	Session Protocol Data Unit
PPDU:	Présentation Protocol Data Unit
APDU:	Application Protocol Data Unit
ROM:	Read-Only Memory
UDP :	User Datagram Protocol
IPX :	Internetwork Packet Exchange
NFS :	Need for Speed
IBM :	International Business Machines
EBCDIC :	Extended Binary Coded Decimal Interchange Code
ASCII :	American Standard Code for Information Interchange
TLI :	Transport Logistics International
ICMP :	Internet Control Message Protocol
IGMP:	Internet Group Management Protocol
FTP :	File Transfer Protocol
Modbus:	Modicon Communication Bus
Profibus:	Process Field Bus

HTTP:	Hypertext Transfer Protocol Secure
TTL:	Transistor-Transistor Logic
MTU:	Maximum Transmission Unit
PSH:	Push
RST:	Reset
SYN:	Synchronize
IHM:	Interface Homme –Machine
ICS:	Interacting Cognitive Subsystems
ACT:	Adaptive Control of Thought
COSIMO	COgnitive SImulation Model
ICO:	Interactive Cooperative Objects
AFNOR:	Association française de normalization
MVC:	Modèle-Vue-Contrôleur
SCADA:	Supervisory control and data acquisition
RTU:	Remote Termina Unit
DNS:	Domain Naming System
LDAP:	Lightweight Directory Access Protocol
DHCP:	Dynamic Host Configuration protocol
FTP:	File Transfert Protocol
WinCC:	Windows Control Center
SQL:	Structured Query Language
MAD:	Methode Analytique de Description
DNP:	Distributed Network Protocol
GSM:	Global system for mobile communications
GPRS:	General packet radio service

WIFI: Wireless Fidelity

WIMAX: Worldwide Interoperability for Microwave Access

PDA: Personal Digital AssistantAcknowledgement

ASP: Active Server Pages

CGI: Common Gateway Interface

POP: Post Office Protocol

Liste Des Tableaux

Liste des Tableaux

Liste Des Figures

Liste des figures

Table Des Matières

Table des matières

Chapitre III Les Systèmes De Supervision, Commande et Acquisition Des Données (SCADA)

Chapitre IV / La Sécurité

Introduction Générale

Introduction Générale

L'eau est le principal constituant des êtres vivants et l'élément indispensable à toute forme de vie. Sans eau, aucun organisme, qu'il soit végétal ou animal, simple ou complexe, petit ou gros, ne peut vivre.

L'eau est très abondante sur notre planète. Elle est même probablement l'une des ressources les plus abondantes de la Terre et l'évolution de la vie humaine n'a pas exclus l'évolution d'exploitation et utilisation de cette ressource, d'abord le stockage de l'eau et puis les forages, les stations de pompage en arrivant aux stations d'épuration et dessalement de l'eau…etc.

L'essor technologique a fortement contribué et à la souplesse d'utilisation de l'eau et à la simplicité de gérer les ouvrage d'exploitation de l'eau, et comme il est évident de remarquer la répartition géographique de ces ouvrages (barrages, station de pompages, station d'épuration…) la télégestion s'impose systématiquement pour faire face à ce problème.

La télégestion désigne un ensemble de solutions technologiques permettant de piloter à distance des installations autonomes géographiquement dispersées.
De quoi, par exemple et de façon basique, permettre à l'exploitant d'un ouvrage d'être alerté en cas de problème technique. C'est toutefois loin d'être le seul atout de ces systèmes, puisqu'ils savent également enregistrer le fonctionnement des équipements surveillés (pompes, vannes, etc.).

Dans l'industrie de l'eau, la télégestion naît, dans les années soixante-dix, pour optimiser le couple station de pompage-réservoir d'eau potable. La télétransmission d'alors ne sert qu'à déclencher ou stopper le pompage, par radio ou via une liaison filaire. Dans les années quatre-vingt arrive la téléalarme, autorisant le poste local à prévenir l'exploitant du réseau d'un dysfonctionnement éventuel. L'étape suivante voit la mise en œuvre d'un dispositif permettant de connaître l'état de santé du réseau lui-même, à travers celui de ses équipements, ainsi que leur évolution dans le temps.

Cette fonctionnalité est rendue possible par l'enregistrement en local des états des capteurs de l'installation. Complémentairement, des calculs de bilans assistent l'exploitant dans l'analyse du fonctionnement.

Toutes ces données deviennent consultables par le biais d'un poste central ou par un simple Minitel : soit une technologie conçue pour le grand public mais utilisée à des fins industrielles. Cette approche s'est largement pérennisée depuis, puisqu'en complément des modems RTC (Réseau téléphonique commuté), ont été adoptées des solutions comme le GSM (Global System for Mobile Communications) Data, l'ADSL (Asymmetric Digital Subscriber Line) et aujourd'hui le GPRS (General Packet Radio Service). Ainsi, de « serveurs Minitel », les équipements de télégestion sont devenus « serveur Web », c'est-à-dire utilisés grâce aux technologies Internet.

Dans ce travail, où on va développer une étude sur la télégestion dans l'industrie de l'eau par les technologies de Web nous allons focaliser sur l'aspect sécurité qui prédomine du fait qu'on va utiliser un réseau publique cible de toute nature d'attaque.

Ce mémoire est organisé en cinq chapitres répartis comme suit :

Le 1ier chapitre comportera une introduction aux réseaux, l'étude de transfert de l'information dans le réseau Internet tout en détaillant le mécanisme et les protocoles utilisés. On y présentera les définitions de base, les principes généraux, ainsi que les plus importantes notions nécessaires à la bonne assimilation de la technologie Web.

Le 2ième chapitre, qui concerne l'interface homme-machine, où on a étudié les méthodes de conception des IHM en tenant compte de l'analyse et la modélisation des taches humaines et les spécifications de la conception d'un système interactif.

Le 3ième chapitre, est consacré aux systèmes SCADA dont notre travail fait partie de cette famille où on va détailler l'architecture de ces systèmes y compris la communication entre le terminal principal et les autres terminaux déportés, sans oublier de donner une description d'un environnent SCADA.

Le 4ième chapitre, présentera une étude en matière de sécurité qui occupe une place primordiale dans ce travail, où on va faire une étude théorique sur les risques et attaques visant le réseau Internet et l'environnement SCADA avec les moyens de sécurité envisagés afin de remédier à ces dangers.

Le 5ième chapitre, est l'objectif de notre travail. Il représente l’étude expérimentale tout en développant l’impact de la réalisation adoptée sur la sécurité et la fiabilité de la télégestion.

CHAPITRE (I)

PRINCIPES GENERAUX SUR Les RESEAUX

I-1/ Introduction

Avant d'entamer l'objet du thème il est essentiel voire indispensable de consacrer un chapitre sur les notions de base des réseaux qui constituent la matière première du travail à réaliser tout en se limitant sur les généralités et loin d'une étude exhaustive.

I-2/ Définition d'un réseau :

Un réseau est l'ensemble de matériels et de logiciels permettant à des équipements de communiquer entre eux, ayant pour objectif le partage des ressources matérielles et logicielles [1], [2].

I-3/ Classification des réseaux :

On peut classifier les réseaux selon plusieurs critères parmi lesquels on cite :

I-3-1/ Selon la taille :

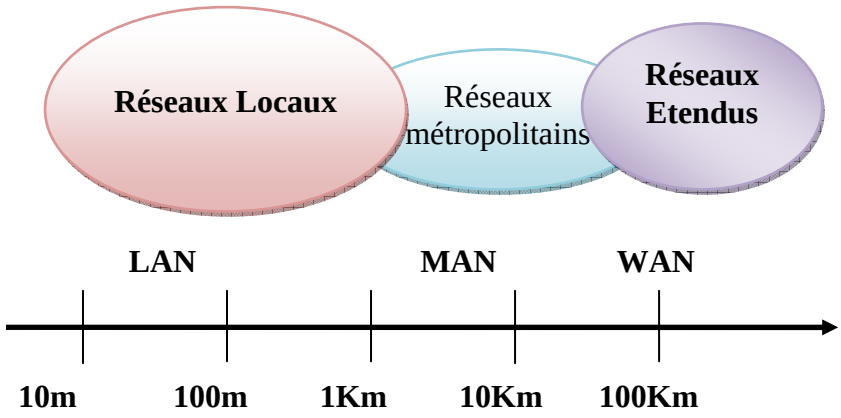


Figure I-1 : Classification des réseaux selon la taille [3]

- **Un réseau local (Local Area Network)** : peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut être développé sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Un réseau métropolitain (Métropolitain Area Network) :** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un réseau étendu (Wide Area Network)** : permet de communiquer à l'échelle d'un pays, ou de la planète entière. Les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunication.

I-3-2/ Selon la structure :

I-3-2-1/ Mode diffusion :

Son mode de fonctionnement consiste à partager un seul support de transmission, chaque message envoyé par un équipement sur le réseau est reçu par tous les autres. C'est l'adresse spécifique placée dans le message qui permettra à chaque équipement de déterminer si le message lui est adressé ou non, à tout moment un seul équipement a le droit d'envoyer un message sur le support. Il faut donc qu'il écoute au préalable si la voie est libre; si ce n'est pas le cas il attend selon un protocole spécifique à chaque architecture.

Les réseaux locaux adoptent pour la plupart le mode diffusion sur une architecture en bus ou en anneau. Dans une telle configuration la rupture du support provoque l'arrêt du réseau, par contre la panne d'un des éléments ne provoque pas (en général) la panne globale du réseau [1], [2].

I-3-2-2/ Mode point à point :

Dans ce mode le support physique relie une paire d'équipements seulement, quand deux éléments non directement connectés entre eux veulent communiquer ils le font par l'intermédiaire des autres nœuds du réseau.

Dans le cas de l'étoile le site central reçoit et envoie tous les messages, le fonctionnement est simple, mais la panne du nœud central paralyse tout le réseau. Dans une boucle simple, chaque nœud recevant un message de son voisin en amont le réexpédie à son voisin en aval, pour que les messages ne tournent pas indéfiniment le nœud émetteur retire le message lorsqu'il lui revient. Si l'un des éléments du réseau tombe en panne, alors tout s'arrête [1], [2].

I-3-3/ Selon le mode de fonctionnement :

I-3-3-1/ Mode de fonctionnement avec connexion :

Dans le mode avec connexion, toute communication entre deux équipements suit le processus suivant:

- L'émetteur demande l'établissement d'une connexion par l'envoi d'un bloc de données spécial
- Si le récepteur (ou le gestionnaire de service) refuse cette connexion la communication n'aura pas lieu

- Si la connexion est acceptée, elle est établie par mise en place d'un circuit virtuel dans le réseau reliant l'émetteur au récepteur.

Les données sont ensuite transférées d'un point à l'autre et la connexion est libérée c'est le fonctionnement bien connu du réseau téléphonique classique.

Les avantages du mode avec connexion sont la sécurisation du transport par identification claire de l'émetteur et du récepteur. La possibilité d'établir à l'avance des paramètres de qualité de service qui seront respectés lors de l'échange des données.

Les défauts sont la lourdeur de la mise en place de la connexion qui peut se révéler beaucoup trop onéreuse si l'on ne veut échanger que quelques octets ainsi que la difficulté à établir des communications multipoint [2], [4].

I-3-3-2/ Mode de fonctionnement sans connexion :

Dans le mode sans connexion les blocs de données, appelés datagrammes, sont émis sans vérifier à l'avance si l'équipement à atteindre ainsi que les nœuds intermédiaires éventuels, sont bien actifs. C'est alors aux équipements gérant le réseau d'acheminer le message étape par étape et en assurant éventuellement sa temporisation jusqu'à ce que le destinataire soit actif, ce service est celui du courrier postal classique et suit les principes généraux suivants [2], [4]:

- Le client poste une lettre dans une boîte aux lettres
- Chaque lettre porte le nom et l'adresse du destinataire
- Chaque client a une adresse propre et une boîte aux lettres
- Le contenu de l'information reste inconnu du prestataire de service
- Les supports du transport sont inconnus de l'utilisateur du service

I-4/ Les réseaux OSI et TCP/IP :

I-4-1/ Le Modèle OSI (Open System Interconnection)

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés ; et on s'est rendu compte qu'il serait impossible d'interconnecter ces différents réseaux si une norme internationale n'était pas adoptée. Cette norme établie par l'International Standard Organization (ISO) est la norme Open System Interconnection (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches. Chacune de ces couches correspondant à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 sont dites basses et les couches 5, 6 et 7 sont dites hautes. Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au-dessus d'elle en lui épargnant les détails d'implémentation nécessaires. Chaque couche du rang n d'une machine gère la communication avec la couche respective d'une autre machine en suivant un protocole propre du rang qui est un ensemble de règles de communication pour le service de niveau n comme le montre la figure I-2. [5], [6].

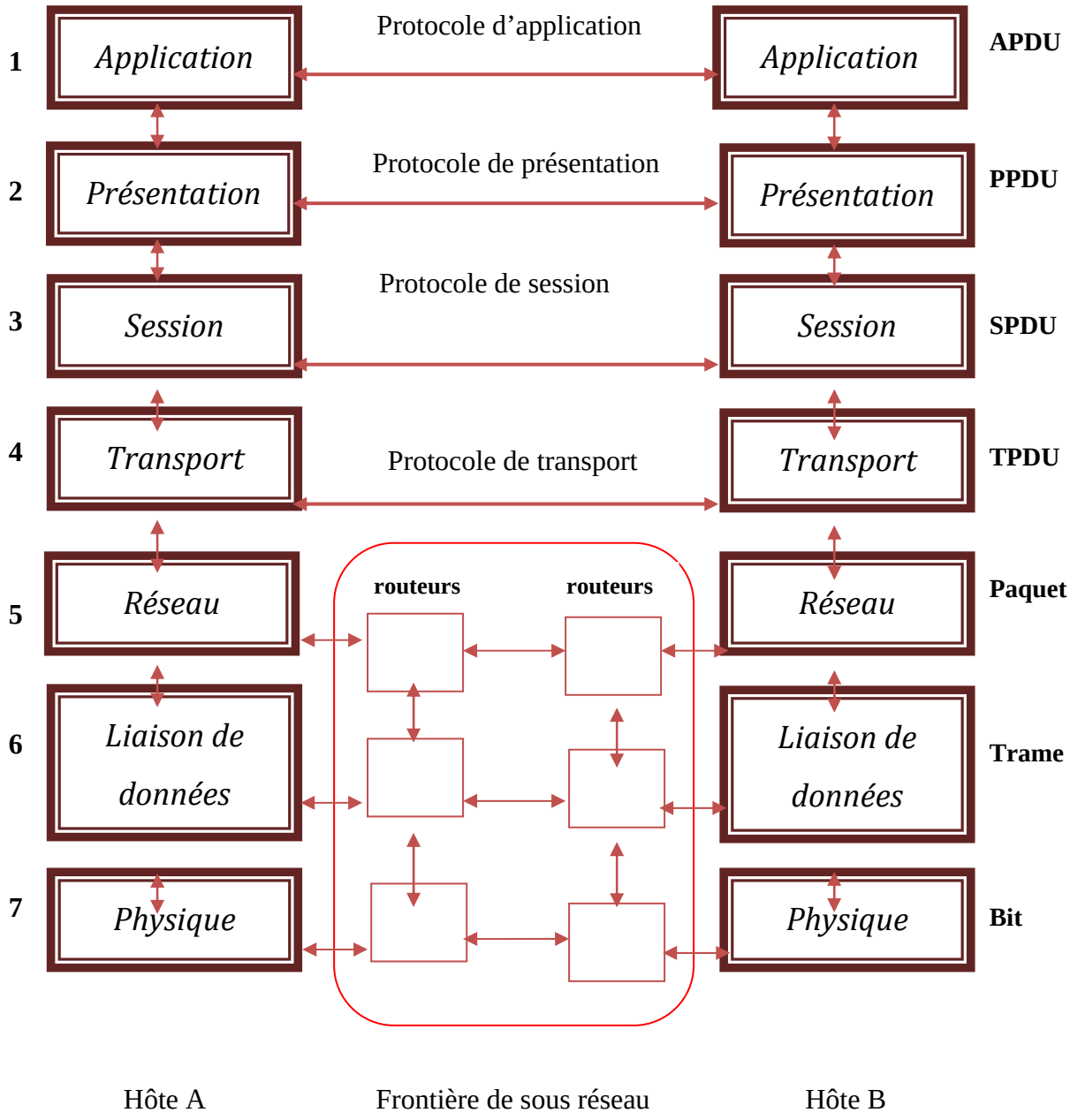


Figure I-2 : les Couches du modèle OSI [7]

I-4-2/ Les Couches du modèle OSI

❖ La Couche 1 : La couche Physique

Cette couche définit les propriétés physiques du support de données. Par exemple, dans le cas de câbles en cuivre, les méthodes de transmission sont différentes que celles utilisées sur une liaison par fibre optique. Selon la qualité du support, les vitesses de transmission sont naturellement très variables. La couche physique est représentée par le matériel de la carte réseau. [1], [2].

❖ La Couche 2 : La couche Liaison

La couche liaison assure la fiabilité de la transmission des données par la couche 1. Sur le support réseau, elle réalise cette fonction par l'établissement de sommes de contrôle (checksum), par la synchronisation de la transmission des données et par différents procédés d'identification et de correction d'erreurs. L'adressage des ordinateurs est réalisé dans cette couche par les adresses définies d'une manière fixe sur les cartes réseau.

Dans le cas des cartes Ethernet, cette adresse est appelée adresse Ethernet ou adresse matérielle, cette couche est matérialisée et exécutée par un logiciel résidant en ROM sur la carte réseau. [1], [2].

❖ La Couche 3 : La couche Réseau

La couche réseau prend en charge l'optimisation des chemins de transmission entre les ordinateurs distants. Les paquets de données sont transmis grâce à l'établissement d'une connexion logique entre les ordinateurs, qui peut comprendre plusieurs nœuds. L'adressage des ordinateurs est réalisé dans cette couche par des adresses logiques (par exemple des adresses IP) qui doivent être configurées sur chacun des ordinateurs. Parmi les protocoles chargés de la gestion de cette couche le protocole Internet Protocol (IP) de la famille TCP/IP. [5], [6].

❖ La Couche 4 : La couche Transport

La couche transport prend en charge le pilotage du transport des données entre l'expéditeur et le destinataire. Cette fonction est réalisée par les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) de la famille des protocoles TCP/IP, ou par SPX (Sequenced Packet Exchange) de la famille Novell IPX/SPX.
TCP établit ainsi un protocole orienté connexion pour assurer la transmission des données, ce type de communication permet de garantir la sécurité de la transmission par une confirmation

de la réception des données par le destinataire. Le protocole attend ainsi un accusé de réception de chaque paquet de données avant de transmettre le paquet suivant.

Si l'accusé de réception n'est pas reçu au bout d'un certain temps, le paquet concerné est retransmis au destinataire, le contrôle du contenu des données est assuré par une somme de contrôle (checksum).

Le protocole UDP permet de réaliser la fonction de cette couche par un protocole sans connexion. Dans ce cas, le destinataire ne transmet pas d'accusé de réception. L'expéditeur ne peut donc pas savoir si tous les paquets de données ont été correctement reçus par le destinataire. En outre, les checksum sont utilisés de manière moins intensive. S'il est nécessaire de réaliser un traitement des erreurs, celui-ci doit être pris en compte par une couche supérieure du modèle OSI. Cependant, le protocole UDP permet de réaliser un transfert de données plus rapide, en éliminant la nécessité de l'accusé de réception. Ses performances plus importantes justifient sa large utilisation dans le domaine Unix pour le service Network File System (NFS). [5], [6].

- **La Couche 5 : La couche Session**

Cette couche gère l'échange des données sur la connexion établie par les couches une à quatre. En particulier, c'est cette couche qui détermine lequel des ordinateurs connectés doit émettre les données et lequel doit les recevoir.

Le procédé Transport Independent Remote Procedure, qui permet des appels de procédures sur des ordinateurs distants, indépendamment du protocole de transport, est l'un des protocoles de cette couche, de nombreux procédés de connexion utilisent également un protocole de cette couche. [5], [6].

- **La Couche 6 : La couche Présentation**

C'est dans cette couche où est réalisée l'adaptation de la représentation des données en fonction de l'architecture des ordinateurs. Par exemple, l'échange de données entre un ordinateur central IBM. Qui utilise le codage de caractères EBCDIC, et un PC qui utilise le codage ASCII impose que les données soient d'abord converties au format réseau avant la transmission vers le destinataire. Celui-ci doit alors convertir les données reçues dans le format réseau pour les présenter dans Le format qu'il peut utiliser. [5], [6].

- **La Couche 7 : La couche Application**

La couche application est l'interface entre l'application et le réseau. Cette interface est désignée par le terme Transport Layer Interface (TLI). C'est ainsi que le modèle permet d'assurer l'indépendance de l'application vis-à-vis des accès réseau, exécutés par les couches inférieures. Certains programmes typiques utilisent cette couche, par exemple ftp, http. Des

services système comme NFS (Network File System) ou NIS (Network- Information Service) exploitent également cette interface.

Le modèle OSI ne préconise aucun logiciel ni matériel spécifique. Il ne s'agit pas non plus d'une norme obligatoire pour les réseaux. Il ne sert que de support et de base terminologique permettant la description et le développement des nouveaux protocoles. [5], [6].

I-4-3/ Le Fonctionnement du réseau de modèle OSI :

Les paquets de données constituent les éléments de base de la communication réseau, le destinataire des paquets de données les rassemble pour les replacer dans l'ordre initial, permettant ainsi de reconstituer les données de départ.

Lors du découpage des données en paquets, le logiciel réseau de l'ordinateur émetteur ajoute à chaque paquet des informations de contrôle spécifiques, ces informations sont indispensables pour permettre au destinataire de reconstituer les données émises, après leur découpage et leur transmission, les informations de contrôle contiennent également des zones de checksum qui permettent de vérifier l'absence d'erreurs lors de la transmission.

Ces informations de contrôle doivent également être transmises au destinataire, en même temps que les données proprement dites, c'est ainsi qu'une sorte d'en-tête de protocole s'ajoute aux données, et réduit les débits de transmission théoriquement possibles sur une connexion réseau. Ainsi chaque couche doit remplir une tâche spécifique, les informations nécessaires sont ajoutées sous forme d'un en-tête.

Lors de l'émission d'un paquet, chaque couche ajoute au paquet de données issu de la couche inférieure l'en-tête correspondant. Ces en-têtes sont exploités par les couches correspondantes de l'ordinateur destinataire, qui élimine ces informations du paquet de données pour le transmettre à la couche suivante.

Le programme de l'ordinateur cible ne reçoit donc que les données utiles. Les différents en-têtes contiennent ainsi toutes les informations nécessaires pour le transport, le guidage et la transcription des données sur le réseau. C'est ainsi que le transport des données sur le réseau est rendu totalement transparent pour l'application. [5], [6].

I-5/ Le réseau Internet et les protocoles TCP/IP.

Les réseaux TCP/IP représentent un cas particulier des réseaux OSI qui sont structurés en quatre couches de protocoles comme suit :

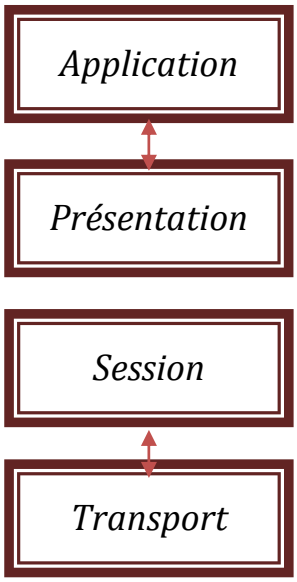


Figure I-3 : Les Couches de TCP/IP [7]

1. La couche d'ACCES RESEAU est l'interface avec le réseau et est constituée d'un pilote du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.
2. La couche INTERNET ou couche RESEAU gère la circulation des paquets à travers le réseau en assurant leur routage, elle comprend à titre indicatif les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol).
3. La couche TRANSPORT assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire, elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreurs et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas d'UDP (User Datagram Protocol). Pour UDP, il n'est pas garanti qu'un paquet (appelé dans ce cas datagramme) arrive à bon port, c'est à la couche application de s'en assurer.
4. La couche APPLICATION est celle des programmes utilisateurs comme Telnet (connexion à un ordinateur distant), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP….. etc.

Lorsqu'une application envoie des données à l'aide de TCP/IP les données traversent de haut en bas de chaque couche jusqu'à aboutir au support physique où elles sont alors émises sous forme de suite de bits. [7], [8].

I-5-1/ Encapsulation

L'encapsulation est le mécanisme qui permet à chaque couche de rajouter aux données ses informations propres. En pratique, lorsque les données parcourent les couches dans le sens descendant, chacune lui rajoute un en-tête contenant ces informations comme l'indique la figure I-4.

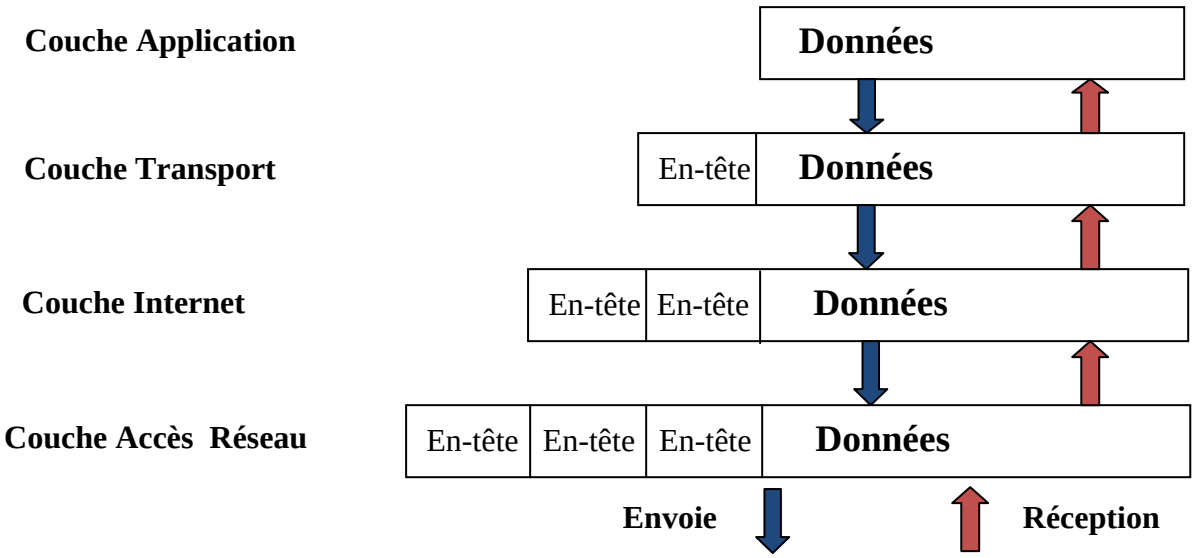


Figure I-4 : L'encapsulation des données [8]

Dans le sens inverse, chaque couche retire son en-tête, analyse les informations et transmet le reste à qui de droit dans la couche supérieure (en fonction de l'analyse effectuée). [7], [8].

I-6/ Le protocole IP :

Le protocole IP (Internet Protocol) est au cœur du fonctionnement de l'internet, il assure sans connexion un service non fiable de délivrance de datagrammes IP, le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination.

Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre, on parle de remise au mieux (best effort delivery) et ni l'émetteur ni le récepteur ne sont informés directement par IP des problèmes rencontrés. Le mode de transmission est non connecté car

IP traite chaque datagramme indépendamment de ceux qui le précèdent et le suivent. Ainsi en théorie, au moins, deux datagrammes IP issus de la même machine et ayant la même destination peuvent ne pas suivre obligatoirement le même chemin.

Le rôle du protocole IP est centré autour des trois fonctionnalités suivantes [7], [8]:

- définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet
- définir le routage dans Internet
- définir la gestion de la remise non fiable des datagrammes

I-6-1/ La structure d'un datagramme :

La structure d'un datagramme contient les champs suivants : [9], [10]

32 bits

Version (4 bits)	**Longueur d'entête (4 bits)**	**Type de service (8 bits)**	**Longueur Total (16 bits)**	
Identification (16 bits)			**Drapeau (3 bits)**	**Décalage fragment (13 bits)**
Durée de vie (8bits)		**Protocole (8bits)**	**Somme de contrôle en tête (16 bits)**	
Adresse IP Source (32 bits)				
Adresse IP Destination (32 bits)				
Données				

Tableau I-1 : Structure d'un datagramme IP [1]

1. **Version code :** sur 4 bits est le numéro de version du protocole IP utilisé (la version courante est la quatrième, d'où son nom d'IPv4), tout logiciel IP doit d'abord vérifier que le numéro de version du datagramme qu'il reçoit est en accord avec lui-même, si ce n'est pas le cas le datagramme est tout simplement rejeté, ceci permet de tester des nouveaux protocoles sans interférer avec la bonne marche du réseau.

2. **Longueur d'entête** : représente sur 4 bits la longueur, en nombre de mots de 32 bits, de l'en-tête du datagramme, ce champ est nécessaire car un en-tête peut avoir une taille supérieure à 20 octets (taille de l'en-tête classique) à cause des options que l'on peut y ajouter. [1], [2].
3. **Type de service (TOS) :**
   Qualifie le service de transmission demandé, il est utilisé pour optimiser l'algorithme de routage :
   - Priorités entre les différents types de flux de données.
   - Critères de choix lors du routage entre des chemins alternatifs.
4. **Longueur totale :** Contient la taille totale en octets du datagramme, et comme ce champ est de 2 octets on en déduit que la taille complète d'un datagramme ne peut dépasser 65535 octets, utilisée avec la longueur de l'en-tête elle permet de déterminer où commencent exactement les données transportées.
5. **Identification** : Sur 16 bits ce champ représente le numéro d'identification d'un paquet ou fragment, les fragments appartenant à un même paquet ont le même identificateur.
6. **Durée de vie (TTL) :** Indique le nombre maximal de routeurs que peut traverser le datagramme, elle est initialisée à N (souvent 32 ou 64) par la station émettrice et décrémenté de 1 par chaque routeur qui le reçoit et le réexpédie. Lorsqu'un routeur reçoit un datagramme dont la durée de vie est nulle, il le détruit et envoie à l'expéditeur un message ICMP, donc il est impossible qu'un datagramme tourne indéfiniment dans le réseau.
7. **Protocole :** Permet de coder quel protocole de plus haut niveau utilisé pour créer ce datagramme, les valeurs codées sur 8 bits sont 1 pour ICMP, 2 pour IGMP, 6 pour TCP et 17 pour UDP. La station destinatrice qui reçoit un datagramme IP pourra diriger les données qu'il contient vers le protocole adéquat.
8. **Total de contrôle d'entête :** Est calculé à partir de l'en-tête du datagramme pour en assurer l'intégrité. L'intégrité des données transportées est assurée directement par les protocoles ICMP, IGMP, TCP et UDP qui les émettent, pour calculer cette somme de contrôle, on commence par la mettre à zéro, puis en considérant la totalité de l'en-tête comme une suite d'entiers de 16 bits, on fait la somme de ces entiers en complément à 1.

   On complémente à 1 cette somme et cela donne le total de contrôle que l'on insère dans le champ prévu. À la réception du datagramme, il suffit d'additionner tous les

nombres de l'en-tête et si l'on obtient un nombre avec tous ses bits à 1, c'est que la transmission s'est passée sans problème.

9. **Adresse IP destination et source :** Sur 32 bits les adresses de la machine émettrice et destinataire finale du datagramme.
10. **Options :** Est une liste de longueur variable, mais toujours complétée par des bits de bourrage pour atteindre une taille multiple de 32 bits pour être en conformité avec la convention qui définit le champ longueur de l'en-tête. Ces options sont très peu utilisées car peu de machines sont aptes à les gérer, parmi elles on trouve des options de sécurité et de gestion, d'enregistrement de routes ……etc.
11. **Données :** les données du segment dont la taille maximale est 65 536 octets.

I-6-2/ La fragmentation des datagrammes IP :

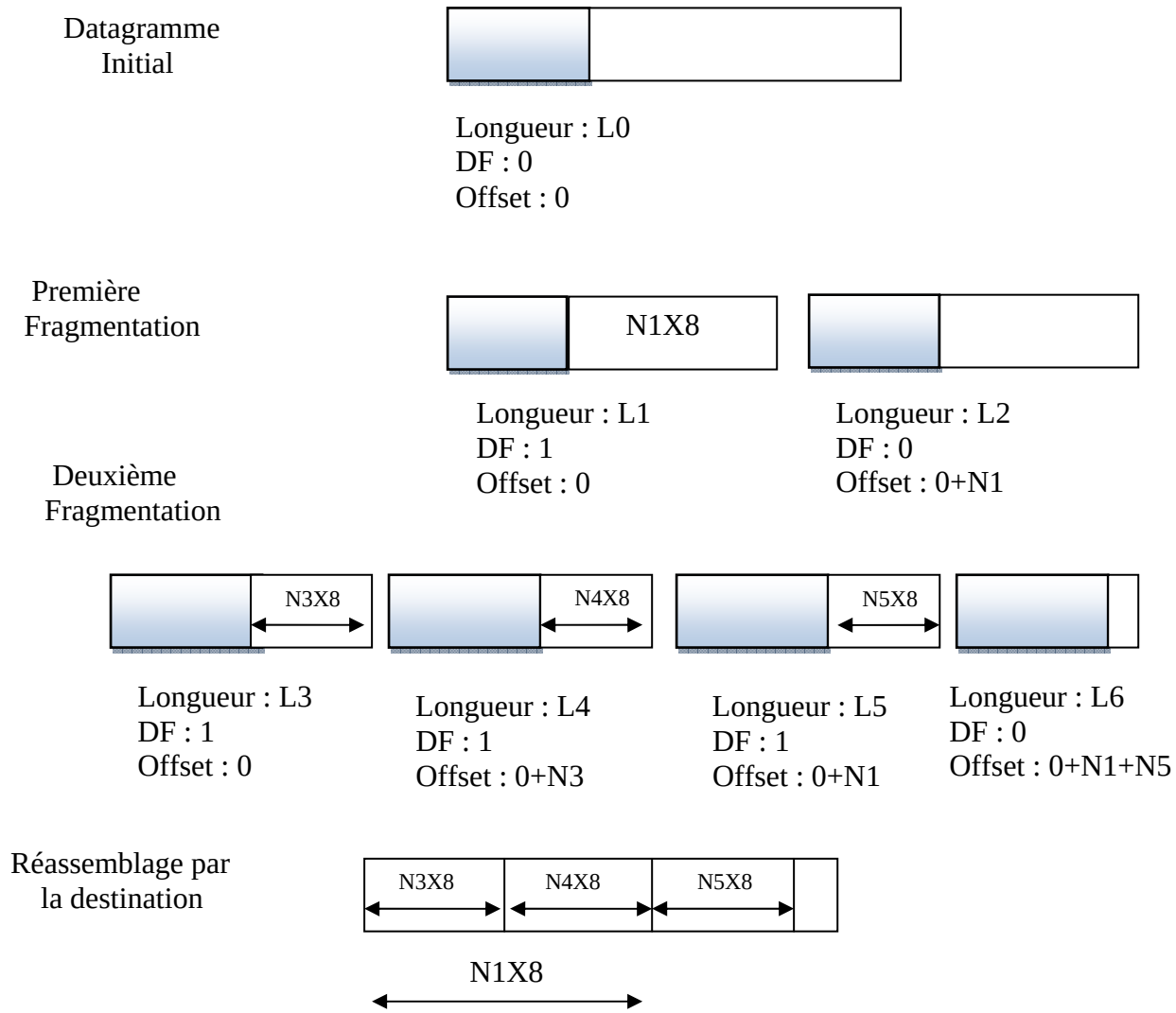


Figure I-5 : Mécanisme de fragmentation d'un datagramme IP[10]

En fait, il existe d'autres limites à la taille d'un datagramme que celle fixée par la valeur maximale de 65535 octets. Notamment pour optimiser le débit il est préférable qu'un datagramme IP soit encapsulé dans une seule trame de niveau 2 (Ethernet par exemple), mais comme un datagramme IP peut transiter à travers Internet sur un ensemble de réseaux aux technologies différentes il est impossible de définir, a priori, une taille maximale des datagrammes IP qui permet de les encapsuler dans une seule trame quel que soit le réseau (1500 octets pour Ethernet et 4470 pour FDDI par exemple). [9]

On appelle la taille maximale d'une trame d'un réseau le MTU (Maximum Transfert Unit) et elle va servir à fragmenter les datagrammes trop grands pour le réseau qu'ils traversent. Mais si le MTU d'un réseau traversé est suffisamment grand pour accepter un datagramme, évidemment il sera encapsulé tel qu'il est dans la trame du réseau concerné. [10]

Le processus de fragmentation-réassemblage est rendu possible grâce aux différents champs suivants :

- **Déplacement de fragment :** Ce champ précise la localisation du début du fragment dans le datagramme initial. Les fragments sont des datagrammes dont l'en-tête est quasiment identique à celle du datagramme original. Par exemple le champ identification est un entier qui identifie de manière unique chaque datagramme émis et qui est recopié dans le champ identification de chacun des fragments si ce datagramme est fragmenté. Par contre le champ longueur total est recalculé pour chaque fragment.
- **Drapeaux :** Comprend trois bits dont deux qui contrôlent la fragmentation, s'il est positionné à 1 le premier bit indique que l'on ne doit pas fragmenter le datagramme et si un routeur doit fragmenter un tel datagramme alors il le rejette et envoie un message d'erreur à l'expéditeur. Un autre bit appelé fragments à suivre est mis systématiquement à 1 pour tous les fragments qui composent un datagramme sauf le dernier. Ainsi, quand le destinataire reçoit le fragment dont le bit fragment à suivre est à 0 il est apte à déterminer s'il a reçu tous les fragments du datagramme initial grâce notamment aux champs offset et longueur totale de ce dernier fragment. Si un fragment doit être à nouveau fragmenté lorsqu'il arrive sur un réseau avec un MTU encore plus petit, ceci est fait comme décrit précédemment sauf que le calcul du champ déplacement de fragment est fait en tenant compte du déplacement inscrit dans le fragment à traiter.

I-6-3/ L'adressage IP :

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits, plus précisément, chaque interface dispose d'une adresse IP particulière. En effet un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau, une adresse IP est toujours représentée dans une notation décimale constituée de 4 nombres (1 par octet) compris chacun entre 0 et 255 et séparés par un point.

Plus précisément, une adresse IP est constituée d'une paire (identificateur de réseau, identificateur de machine) et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet comme le montre la figure I-6. [9], [10].

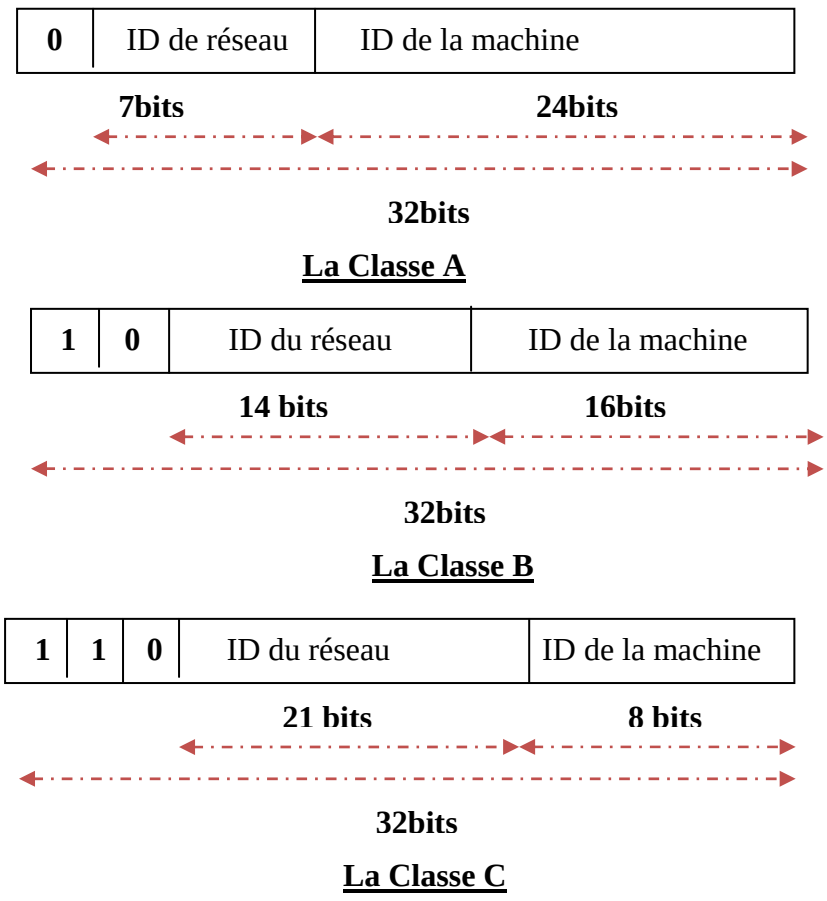


Figure I-6 : Les Classes d'adresse IP [10]

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe. [1], [2].

Classe	Adresse		
A	**0.0.0.0**	**à**	**127.255.255.255**
B	**128.0.0.0**	**à**	**191.255.255.255**
C	**192.0.0.0**	**à**	**223.255.255.255**
D	**224.0.0.0**	**à**	**239.255.255.255**
E	**240.0.0.0**	**à**	**247.255.255.255**

Tableau I-2 : Les adresses possibles pour les classes d'adresse IP [2]

I-6-3-1/ Classe A :

Les adresses de la classe A sont formées d'un octet pour l'adresse réseau et de trois octets pour l'adresse de l'ordinateur. Les adresses de la classe A ne peuvent donc retenir que des valeurs comprises entre 0 et 127 et ne peuvent adresser que 126 réseaux.

I-6-3-2 / Classe B :

Ce type d'adresse est composé de deux octets pour l'adresse du réseau et de deux octets pour l'adresse de l'ordinateur. Dans ce cas, le premier octet ne peut contenir que des valeurs comprises entre 128 et 191, ce type d'adresse ne peut donc définir que 16382 réseaux comportant chacun 65534 ordinateurs.

I-6-3-3/ Classe C :

Une adresse de la classe C est constituée de trois octets pour l'adressage de réseau. Le premier octet peut comporter des valeurs comprises entre 192 et 223, il est donc possible d'adresser 2097150 réseaux de 254 ordinateurs chacun.

I-6-3-4/ Classe D :

Cette classe d'adresses contient les adresses appelées Multicast, elles permettent d'adresser simultanément des groupes d'ordinateurs. Un ordinateur peut ainsi posséder à la fois une adresse fixe et une adresse Multicast.

Il ne peut cependant que recevoir des données par cette adresse, ce qui permet de configurer plusieurs ordinateurs sur la même adresse Multicast. Lorsqu'un paquet de données est transmis à ce type d'adresse, c'est l'ensemble du groupe d'ordinateurs qui est concerné. Le premier octet ne peut donc contenir que des adresses comprises entre 224 et 239.

I-6-3-5/ Classe E :

Il s'agit ici d'un domaine réservé pour des adressages futurs, qui ne doit pas être utilisé sur Internet. Dans ce type d'adresse, les valeurs du premier octet sont comprises entre 240 et 255.

I-6-4/ Le masque de sous réseau

Le masque de sous-réseau indique quelle partie de l'adresse Internet est utilisée pour adresser le réseau, et laquelle est réservée à l'adressage d'un ordinateur particulier à l'intérieur du réseau logique. [9], [10].

Le masque de sous-réseau n'a en principe aucune influence sur les paquets des données transmis par un ordinateur sur le réseau, il influence par contre le fonctionnement du logiciel local de réseau, en lui indiquant comment l'adresse Internet doit être interprétée. Il existe un masque de sous-réseau par défaut pour chaque type de classe d'adresses, qui indique comment l'adresse doit être interprétée dans le cas normal.

Le tableau ci-après présente les valeurs correspondantes :

Classe d'adresse	Adresse exemple	Adresse réseau	Masque de sous réseau
A	23.66.1.200	23.0.0.0	255.0.0.0
B	141.90.3.70	141.90.0.0	255.255.0.0
C	201.3.2.15	201.3.2.0	255.255.255.0

Tableau I-3 : Exemple d'un masque de sous réseau[10]

Le masque de sous-réseau indique au logiciel du réseau local le nombre d'octets de l'adresse Internet qui constituent l'adresse réseau. Le logiciel interprète alors tous les bits désignés par la valeur 1 dans le masque comme faisant partie de l'adresse réseau. Dans le cas d'une adresse de classe B, le logiciel réseau interprète cette instruction de la manière suivante: "Interpréter tous les bits du premier octet et tous les bits du second octet comme partie réseau de l'adresse Internet".

Pour configurer le logiciel réseau d'un ordinateur, quel qu'en soit le système d'exploitation, il est extrêmement important que le masque de sous-réseau soit défini en conformité avec la classe d'adresses. Dans certains cas particuliers, il peut être judicieux, pour

assurer la transmission des paquets de données à travers différents ordinateurs intermédiaires, de définir un masque de sous-réseau différent de la valeur par défaut.

1-6-5/ Le Routage IP

Le routage détermine le chemin que vont suivre les données de l'expéditeur au destinateur en passant par les nœuds du réseau, ceci se fait en fonction de la destination finale du paquet et selon une table de routage qui indique pour chaque destination finale quelles sont les voies de sortie possible.

Pour l'exemple de la figure suivante on pourrait avoir la table de routage suivante :

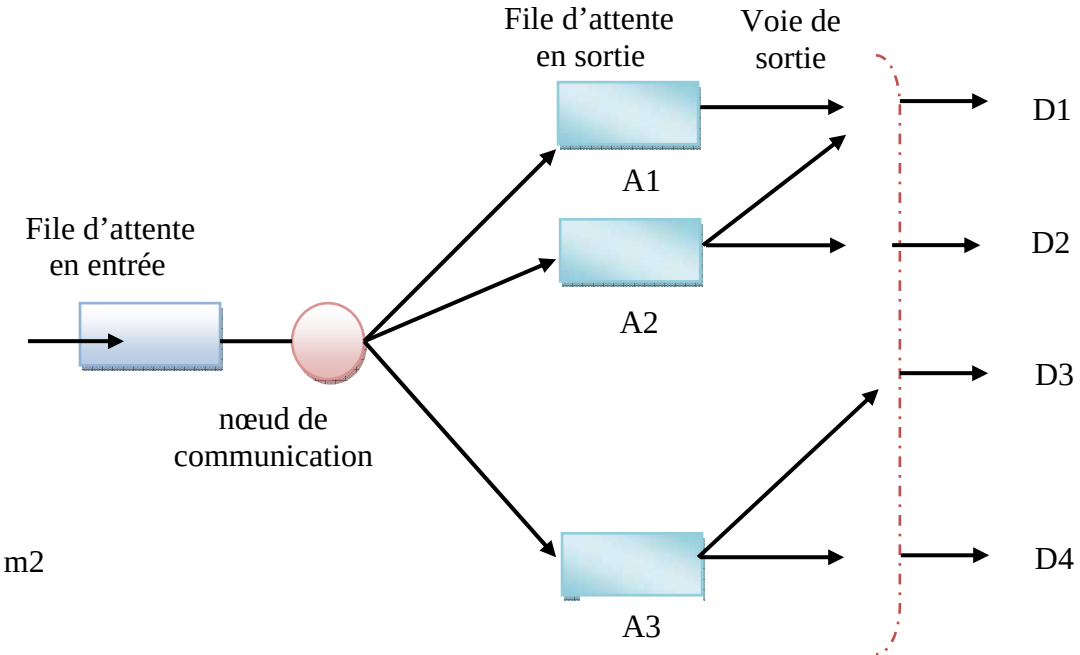


Figure I-7 : Exemple de routage [10]

Destination finale	Voie de sortie
D1	A1, A2
D2	A2
D3	A2, A3
D4	A3

Tableau I-4: la table de routage de l'exemple illustré dans la figure I-7 [10]

D'une manière générale le routage est un ensemble de processus algorithmiques devant prendre des décisions dispersés dans le temps et dans l'espace. Les algorithmes de routage peuvent être regroupés en deux classes principales:

1-6-5-1/ Routage non-adaptatif :

Ils ne fondent pas leurs décisions de routage sur des mesures ou des estimations du trafic de la topologie en temps réel. Le chemin emprunté pour toute communication est toujours le même. Les informations d'acheminement dans la table sont fixes, il peut exister un chemin de secours établi par des tables de secours, les tables de routage ne sont modifiées que pour optimiser les acheminements en fonction de l'évolution du réseau. [10]

1-6-5-2/ Routage adaptatif :

Ils modifient leurs décisions de routage pour traduire les variations de topologie et de trafic réel. Le chemin emprunté pour une communication est fonction de l'état du réseau, la table de routage des commutateurs est mise à jour régulièrement. [10]

Les algorithmes adaptatifs sont divisés en 3 groupes :

1-6-5-2-1/ Centralisés :

Les algorithmes globaux utilisent des informations collectées dans l'ensemble du sous-réseau pour prendre les meilleures décisions; le changement des tables de routage des nœuds est décidé par un centre de contrôle qui a une vue globale de l'état du réseau.

1-6-5-2-2/ Isolés :

Les algorithmes locaux s'exécutent séparément sur chaque IMP et n'utilisent que les informations qui y sont disponibles.

1-6-5-2-3/ Distribués :

Les algorithmes utilisent un mélange d'informations locales et globales; les tables de routage sont élaborées au niveau des nœuds, les différents algorithmes sont répartis sur chaque nœud du réseau et l'ensemble peut fonctionner de manière centralisée ou répartie. Parmi ces algorithmes on cite RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), OSPF (Open Shortest Path First)…..etc

I-7/ Le protocole TCP

TCP est un protocole qui procure un service de flux d'octets orienté connexion. Le terme orienté connexion signifie que les applications dialoguant à travers TCP sont

considérées l'une comme un serveur, l'autre comme un client, et qu'elles doivent établir une connexion avant de pouvoir dialoguer (comme dans le cas de l'utilisation du téléphone).

Les ordinateurs vérifient donc préalablement que le transfert est autorisé, que les deux machines sont prêtes en s'échangeant des messages spécifiques. Une fois que tous les détails ont été précisés, les applications sont informées qu'une connexion a été établie et qu'elles peuvent commencer leurs échanges d'informations.

Il y a donc exactement deux extrémités communiquant l'une avec l'autre sur une connexion TCP, cette connexion est bidirectionnelle simultanée (full duplex*)* et composée de deux flots de données indépendants et de sens contraire. Il est cependant possible d'inclure dans l'en-tête de segments TCP d'une communication de A vers B des informations relatives à la communication de B vers A.

Cette technique de superposition permet de réduire le trafic sur le réseau. Si elles sont trop volumineuses, les données à transmettre pour une application sont fractionnées en fragments dont la taille est jugée optimale par TCP. [1], [2], [6]

A l'inverse, TCP peut regrouper des données d'une application pour ne former qu'un seul datagramme de taille convenable de manière à ne pas charger inutilement le réseau. Cette unité d'information émise est appelée segment. Certaines applications demandent que les données soient émises immédiatement, même si le tampon n'est pas plein, pour cela, elles utilisent le principe du push pour forcer le transfert. Les données sont alors émises avec un bit marquant cela pour que la couche TCP réceptrice du segment remette immédiatement les données à l'application concernée. [1], [2], [6]

La fiabilité fournie par TCP consiste à remettre des datagrammes, sans perte, ni duplication, alors même qu'il utilise IP qui lui est un protocole de remise non fiable. Ceci est réalisé à l'aide de la technique générale de l'accusé de réception, chaque segment est émis avec un numéro qui va servir au récepteur pour envoyer un accusé de réception.

Ainsi l'émetteur sait si l'information qu'il voulait transmettre est bien parvenue à destination. De plus, à chaque envoi de segment, l'émetteur arme une temporisation qui lui sert de délai d'attente de l'accusé de réception correspondant à ce segment. Lorsque la temporisation expire sans qu'il n'ait reçu d'acquittement ACK, l'émetteur considère que le segment s'est perdu et il le réexpédie. Mais il se peut que la temporisation expire alors que le segment a été transmis sans problème, par exemple suite à un engorgement de réseau ou à une perte de l'accusé de réception correspondant.

Dans ce cas l'émetteur réémet un segment alors que c'est inutile, mais le récepteur garde trace des numéros de segments reçus. Donc il est apte à faire la distinction et peut

éliminer les doublons, le segment TCP sert aux trois fonctionnalités de TCP : établir une connexion, transférer des données et libérer une connexion. [1], [2], [6]

I-7-1/ Le Segment TCP

L'en-tête, sans option, d'un segment TCP a une taille totale de 20 octets et se compose des champs suivants : [1], [6]

<table>
<tr><td colspan="5">Port Source</td><td colspan="4">Port Destination</td></tr>
<tr><td colspan="9">Numéro de Séquence TCP</td></tr>
<tr><td colspan="9">Numéro d’acquiescement</td></tr>
<tr><td>Offset</td><td>Reserve</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Fenêtre</td></tr>
<tr><td colspan="6">Somme de contrôle</td><td colspan="3">Pointeur d’urgence</td></tr>
<tr><td colspan="6">Option</td><td colspan="3">Bourrage</td></tr>
<tr><td colspan="9">Données TCP</td></tr>
</table>

Tableau I-5 : La Structure d’entête TCP [1]

- **Le port source et le port destination** : Identifient les applications émettrices et réceptrices, en les associant avec les numéros IP source et destination du datagramme IP qui transporte un segment TCP on identifie de manière unique chaque connexion.
- **Le numéro de séquence :** Donne la position du segment dans le flux de données envoyées par l'émetteur; c'est-à-dire la place dans ce flux du premier octet de données transmis dans ce segment.
- **Le numéro d'accusé de réception :** Contient en fait le numéro de séquence suivant que le récepteur s'attend à recevoir; c'est-à-dire le numéro de séquence du dernier octet reçu avec succès plus 1. TCP n'acquitte pas un à un chaque segment qu'il reçoit, mais acquitte l'ensemble du flot de données jusqu'à l'octet *k*-1 en envoyant un acquittement de valeur *k*, par exemple dans une transmission de 3 segments de A vers B, si les

octets de 1 à 1024 sont reçus correctement, alors B envoie un ACK avec la valeur 1025. Puis, si le segment suivant contenant les octets de 1025 à 2048 se perd et que B reçoit d'abord correctement le segment des octets de 2049 à 3072, B n'enverra pas d'accusé de réception positif pour ce troisième segment. Ce n'est que lorsque B recevra le deuxième segment, qu'il pourra envoyer un ACK avec la valeur 3073, que A interprétera comme l'acquittement des deux derniers segments qu'il a envoyés. On appelle cela un acquittement cumulatif.

- **La longueur d'en-tête** : Contient sur 4 bits la taille de l'en-tête, y compris les options présentes, codée en multiple de 4 octets. Ainsi un en-tête peut avoir une taille variant de 20 octets (aucune option) à 60 octets (maximum d'options).
- **Le champ réservé** : Comporte 6 bits qui permettent de spécifier le rôle et le contenu du segment TCP pour pouvoir interpréter correctement certains champs de l'en-tête. La signification de chaque bit, quand il est fixé à 1 est la suivante:
  - **URG** : le pointeur de données urgentes est valide.
  - **ACK :** le champ d'accusé de réception est valide.
  - **PSH** : l'émetteur souhaite que les données de ce fragment soient délivrées le plus tôt possible au destinataire.
  - **RST :** réinitialiser la connexion.
  - **SYN :** synchroniser les numéros de séquence pour initialiser une connexion.
  - **FIN :** l'émetteur a atteint la fin de son flot de données.
- **La taille de fenêtre** : Est un champ de 16 bits qui sert au contrôle de flux selon la méthode de la fenêtre glissante. Il indique le nombre d'octets que le récepteur est prêt à accepter, l'émetteur augmente ou diminue son flux de données en fonction de la valeur de cette fenêtre qu'il reçoit.
- **Le checksum** : Est un total de contrôle sur 16 bits utilisé pour vérifier la validité de l'en-tête et des données transmises. Il est obligatoirement calculé par l'émetteur et vérifié par le récepteur.
- **Le pointeur d'urgence** : Est un offset positif qui, ajouté au numéro de séquence du segment, indique le numéro du dernier octet de donnée urgente.Il faut également que le bit URG soit positionné à 1 pour indiquer des données urgentes que le récepteur TCP doit passer le plus rapidement possible à l'application associée à la connexion.

- **L'option** : La plus couramment utilisée est celle de la taille maximale du segment TCP qu'une extrémité de la connexion souhaite recevoir. Lors de l'établissement de la connexion il est possible d'optimiser le transfert de deux manières. Sur un réseau à haut débit, il s'agit de remplir au mieux les paquets. Par exemple en fixant une taille qui soit telle que le datagramme IP ait la taille du MTU du réseau. Sinon, sur un réseau à petit MTU, il faut éviter d'envoyer des grands datagrammes IP qui seront fragmentés, car la fragmentation augmente la probabilité de pertes de messages.

I-7--2/ Le fonctionnement du TCP

Le fonctionnement du TCP est comme suit : l'extrémité demandant l'ouverture de la connexion est le client. Il émet un segment initial (où le bit SYN est fixé à 1) spécifiant le numéro de port du serveur avec lequel il veut se connecter. Il expédie également un numéro de séquence initial N.

Cette phase est appelée ouverture active et consomme un numéro de séquence, le serveur répond en envoyant un segment dont les bits ACK et SYN sont fixés à 1. Dans un même segment il acquitte le premier segment reçu avec une valeur de ACK=N+1 et il indique un numéro de séquence initial. Cette phase est appelée ouverture passive, le client TCP doit évidemment acquitter ce deuxième segment en renvoyant un segment avec ACK=P+1.

La terminaison d'une connexion peut être demandée par n'importe quelle extrémité et se compose de deux demi-fermetures puisque des flots de données peuvent s'écouler simultanément dans les deux sens, l'extrémité qui demande la fermeture émet un segment où le bit FIN est fixé à 1 et où le numéro de séquence vaut N'. Le récepteur du segment l'acquitte en retournant un ACK=N'+1 et informe l'application de la demi-fermeture de la connexion.

À partir de là, les données ne peuvent plus transiter que dans un sens (de l'extrémité ayant accepté la fermeture vers l'extrémité l'ayant demandée), et dans l'autre seuls des accusés de réception sont transmis. Quand l'autre extrémité veut fermer sa demi-connexion, elle agit de même que précédemment ce qui entraîne la terminaison complète de la connexion.

En fait, TCP gère ce type d'échange avec la procédure d'acquittement retardé qui consiste à envoyer l'acquittement en l'incluant dans un segment qui transporte également des données. [2], [6]

I-8/ Réseaux serveur client:

Les réseaux client/serveur sont les protocoles utilisés au niveau de la couche application. Le logiciel client est responsable de l'interface avec l'utilisateur, l'utilisateur entre des données à l'écran qui sont transformées en une requête par le logiciel client. Cette requête est écrite dans un langage spécifique comme par exemple le protocole HTTP pour le Web, et elle est envoyée par le logiciel client au logiciel serveur. [1]

Le logiciel serveur récupère les requêtes des logiciels clients qui s'adressent à lui, il exécute la requête et renvoie le résultat au logiciel client demandeur. Le logiciel client reçoit le résultat et modifie l'affichage en conséquence du côté utilisateur. En général le logiciel serveur est généralement installé sur un ordinateur puissant et dédié à ce service car il est destiné à traiter toutes les requêtes des utilisateurs souhaitant utiliser le service. [1]

I-9/ Conclusion :

Ce chapitre clarifie le parcours de l'information sur le réseau Internet, commençant par la couche physique en arrivant à la couche application, en expliquant étape par étape tous les détails du processus. Le protocole TCP/IP est le sujet le plus important de cette étude car il joue un rôle fondamental dans le réseau Internet et permet d'assurer des connexions sans perte de bout-en-bout (livraison en séquence, retransmission des paquets perdus, exploitation efficace de la connexion).

CHAPITRE (II)

INTERFACE HOMME-MACHINE (HMI)

II-1/ Introduction:

L'évolution de l'industrie a fait naître des besoins plus intenses en matière d'exploitation des installations industrielles, en passant par des schémas synoptiques vers des pupitres de contrôle et commande ,et puis vers des écrans tactiles ayant un seul objectif celui de faciliter au maximum la supervision et l'exploitation des équipements industriels.

Dans notre étude on va s'intéresser aux interfaces Homme -Machine dédiées à la supervision des systèmes industriels.

II-2/ Définition :

On définit une interface homme machine comme un ensemble des dispositifs matériels et logiciels permettant à un utilisateur d'interagir avec un système interactif où on représente une installation industrielle par des graphiques réparties sur plusieurs pages. Chaque page appelle une autre jusqu'à la couverture de toute l'installation ainsi on peut démarrer une pompe, visualiser le niveau d'un bac, ouvrir une vanne …..Etc. en cliquant tout simplement sur la sourie d'un PC ou en touchant sur une surface dans un écran tactile. [11], [12].

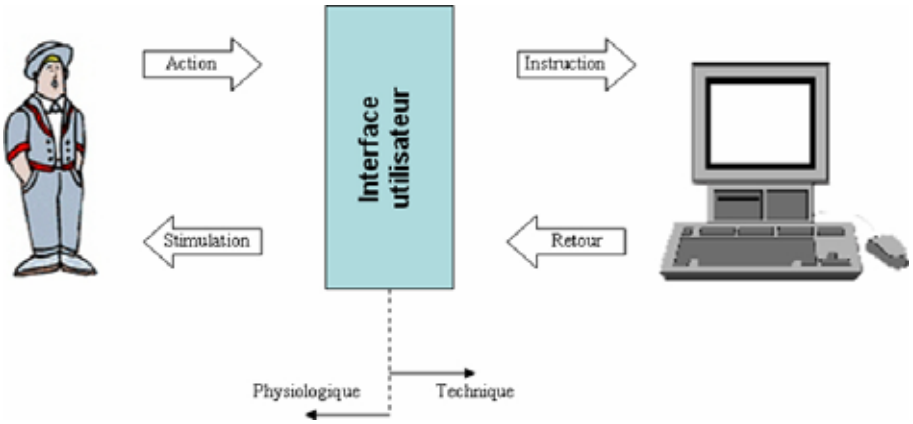


Figure II-1 : interface homme-machine [13]

II-3/ Conception des HMI:

Les enjeux élevés impliqués dans la plupart des projets d'informatisation et d'automatisation, visant la conception de systèmes industriels homme-machine de plus en plus complexes, rendent nécessaire la prise en compte des facteurs humains dans sa démarche globale.

À ce sujet, actuellement, de l'ensemble des sciences techniques et humaines émergent des outils, des techniques, des méthodes et des modèles susceptibles de contribuer au développement de systèmes homme-machine. Principalement la conception des HMI s'articule sur [14], [15]:

1. l'analyse et la modélisation du système technique
2. l'analyse et la modélisation des tâches humaines et des intervenants impliqués dans le système homme-machine
3. la spécification de l'imagerie
4. les environnements graphiques de réalisation de l'imagerie
5. l'évaluation du système homme-machine.

II-3-1/ <u>L'analyse et la modélisation du système technique</u> :

L'analyse et la modélisation du système sous l'angle technique constituent une phase essentielle dans une démarche de conception et/ou d'évaluation de système homme-machine. Cette phase peut s'appuyer sur des méthodes d'analyse éprouvées dont certaines sont couramment utilisées en automatique et en sûreté de fonctionnement. On distingue deux types de méthodes [11], [15], [16] :

1. les méthodes d'analyse du système en fonctionnement normal.
2. les méthodes d'analyse du système en fonctionnement dégradé.

II-3-1-1/ <u>Les méthodes d'analyse du système en fonctionnement normal</u> :

Les méthodes d'analyse en fonctionnement normal ont généralement pour objet de décrire et de comprendre le système technique. Il existe plusieurs méthodes pour la modélisation du système telles que : les Diagrammes-Blocs, les Graphes de Fluence, les Arbres Fonctionnels, SADT,…..etc. [12], [13], [17]

II-3-1-1-1/ <u>La méthode SADT</u> :

SADT « Structured Analysis and Design Technic », est un outil graphique associé à une méthode d'analyse descendante modulaire et hiérarchisée qui a comme but la représentation du modèle d'un système réel. Le modèle de son représentation peut prendre deux formes :

Actigramme : Décrit les activités ou les fonctions du système.

Datagramme : Représente les données existantes dans le système.

La méthode SADT modélise le système selon deux aspects : les composants du système et les activités humaines, matérielles et logicielles. Ainsi, SADT tire parti des avantages du graphique pour décrire le procédé en plusieurs niveaux et en montrer les relations. [16].

II-3-1-2/ Les méthodes d'analyse du système en fonctionnement dégradé

Les méthodes d'analyse du système en fonctionnement dégradé ont deux objectifs communs :

1. Recenser les modes de fonctionnement dégradé du système, par l'identification des différentes configurations susceptibles d'affecter sa mission, son intégrité, sa performance et son environnement : ces configurations prennent souvent la forme d'une liste de défaillances, associées à leurs combinaisons, leurs causes et leurs conséquences.
2. Eliminer ou au moins tenter de réduire la fréquence d'apparition de ces défaillances, ainsi que l'ampleur de leurs conséquences.

Plusieurs méthodes ont été développées pour analyser les systèmes en fonctionnement dégradé parmi lesquelles on citera : la méthode AMDE.

II-3-1-2-1/ La méthode AMDE

La méthode AMDE (Analyse des Modes de Défaillances et de leur**s** Effets) est une méthode inductive à partir d'un recensement des défaillances susceptibles d'affecter un système, elle permet d'évaluer les effets de chaque mode de défaillance des composants du système sur les différentes fonctions de celui-ci, et d'identifier les modes de défaillance ayant des conséquences sur la disponibilité, la production, la fiabilité, la maintenabilité ou la sécurité du système.

Il est ainsi mis en évidence pour chaque mode de défaillance, les causes, les effets, les moyens de compensation existants, on peut distinguer quatre étapes lors de la réalisation d'un AMDE. La première étape consiste en la définition du système, de ses fonctions et de ses composants : chacun des états de fonctionnement (en fonctionnement, en attente, en test, en maintenance...) est recensé, ainsi que les différentes fonctions, les limites du système et de ses composants, etc.

La seconde étape vise l'établissement des modes de défaillances des composants et de leurs causes : celui-ci s'effectue à partir de chacun des états de fonctionnement du système recensés préalablement, les causes peuvent être internes ou externes au système.

La troisième étape a pour objet l'étude des effets des modes de défaillances des composants : il est nécessaire d'étudier et d'évaluer de manière systématique les effets de chaque mode sur les fonctions du système et de ses composants. Les résultats de ce travail

sont centralisés dans un tableau à colonnes, il en existe plusieurs variantes, utilisées dans les différents domaines industriels.

Enfin, la quatrième étape exploite les travaux précédents pour mener à des conclusions et des recommandations : par exemple, à partir des données recensées dans le tableau, on peut s'assurer que toutes les défaillances possibles ont été considérées lors de la conception [15].

II-3-2/ Analyse et modélisation des taches humaines et des intervenants humains

L'analyse et la modélisation des tâches humaines d'une part, et des différents intervenants humains impliqués dans le système homme-machine d'autre part, sont étroitement liées, les limites et ressources cognitives et physiques des intervenants humains contribuant directement à leur efficacité et à leur fiabilité vis-à-vis des tâches à accomplir.

Dans un tel cadre pluridisciplinaire, l'analyse peut s'effectuer à l'aide de techniques variées :

1. Analyse de documents
2. Questionnaires
3. Observations et analyses de protocoles sur site de situations de travail
4. Entretiens avec les différents intervenants du processus de développement.

II-3-2-1/ Analyse et modélisation des taches humaines

L'importance accordée à l'analyse et la modélisation des tâches humaines est grandissante, cette analyse est réalisée par plusieurs méthodes.

II-3-2-1-1 / Méthode de modélisation basée sur l'utilisation conjointe de SADT et des réseaux de Petri

Cette méthode repose sur une décomposition hiérarchique descendante de plus en plus précise, à l'aide d'Actigrammes SADT, il est possible de décrire l'enchaînement des tâches, les données en entrée, en sortie, celles contrôlant la tâche, ainsi que les mécanismes ou supports d'activité exprimant les moyens utilisés pour exprimer la tâche.

À l'aide de SADT, il n'est pas possible de représenter la composante dynamique des tâches. C'est pourquoi l'utilisation des réseaux de Petri s'avère indispensable et complémentaire de SADT. La description sous la forme de réseau de Petri intervient lorsque le niveau de description sous la forme de SADT est suffisamment fin pour faire apparaître une tâche exécutable par l'opérateur humain. Un exemple de description à l'aide d'un réseau de Petri d'une tâche terminale de supervision d'un réseau ferroviaire est illustré en figure II-2.

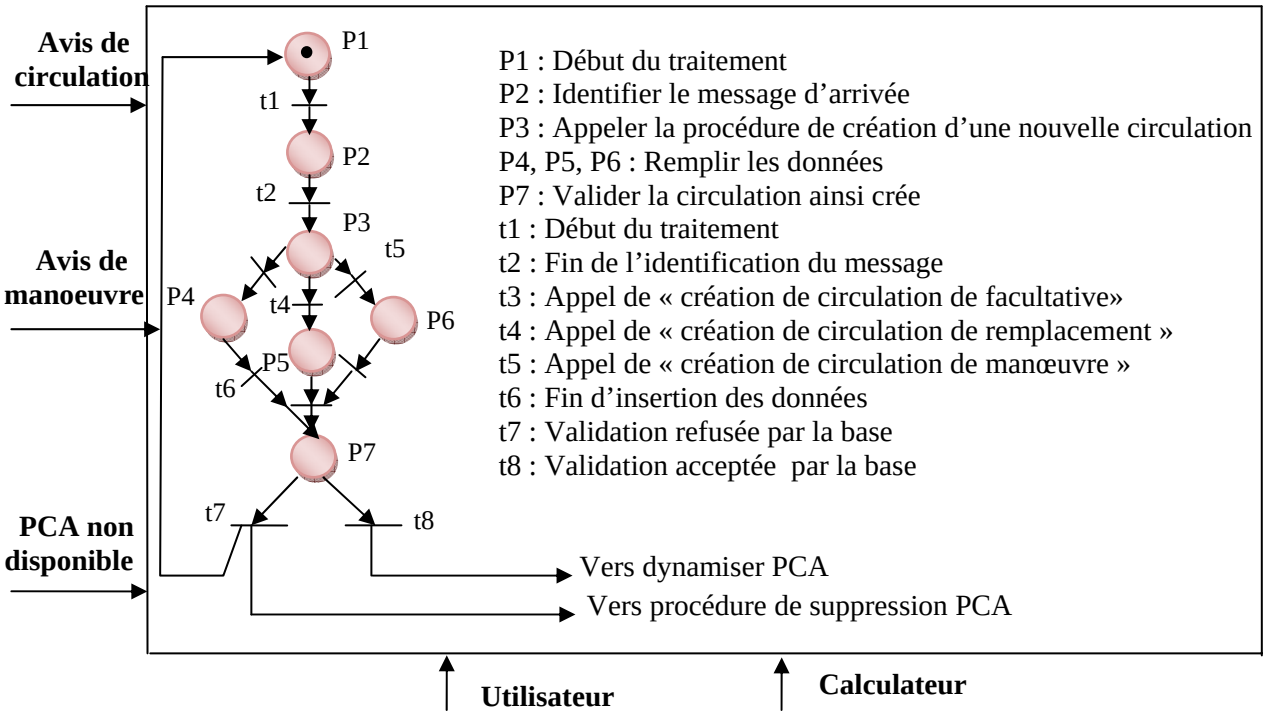


Figure II-2 : Exemples de modélisation par réseaux de PETRI [16]

II-3-2-1-2/ Méthode de modélisation des tâches humaines basée sur MAD

MAD (Méthode Analytique de Description) vise la description de tâches humaines dans un but de meilleure prise en compte de l'ergonomie dans la conception d'interfaces homme-machine. Les principaux concepts introduits dans le formalisme MAD sont ceux de tâche, d'action et de structure.

Le concept de tâche est représenté par un objet générique appelé objet-tâche et composé d'un état initial, d'un état final, d'un but, des préconditions et des postconditions, l'objet-tâche est la racine de deux sous-classes, la classe « tâche élémentaire» et la classe « tâche-composée », la « tâche élémentaire» est une tâche indécomposable, dont le niveau opérationnel est caractérisé par un objet-méthode de type simple, c'est-à-dire une action.

La tâche composée est une tâche dont le niveau opérationnel est défini par une structure décrivant le corps de la tâche. Le concept de structure est représenté par un objet générique caractérisé par un constructeur décrivant l'agencement des différentes tâches impliquées et les arguments du constructeur, plusieurs constructeurs ont été définis, tels que : SEQ : tâche séquentielle, PAR : tâches parallèles, ALT : tâches alternatives, BOUCLE : tâches itératives et FAC : tâches facultatives [17].

La figure **II-3** donne le principe de description d'une tâche humaine dans le domaine du contrôle aérien, sur la partie gauche apparaît la décomposition sous forme d'arbre de la tâche « Gérer la position », alors que sur la partie droite apparaît sa description.

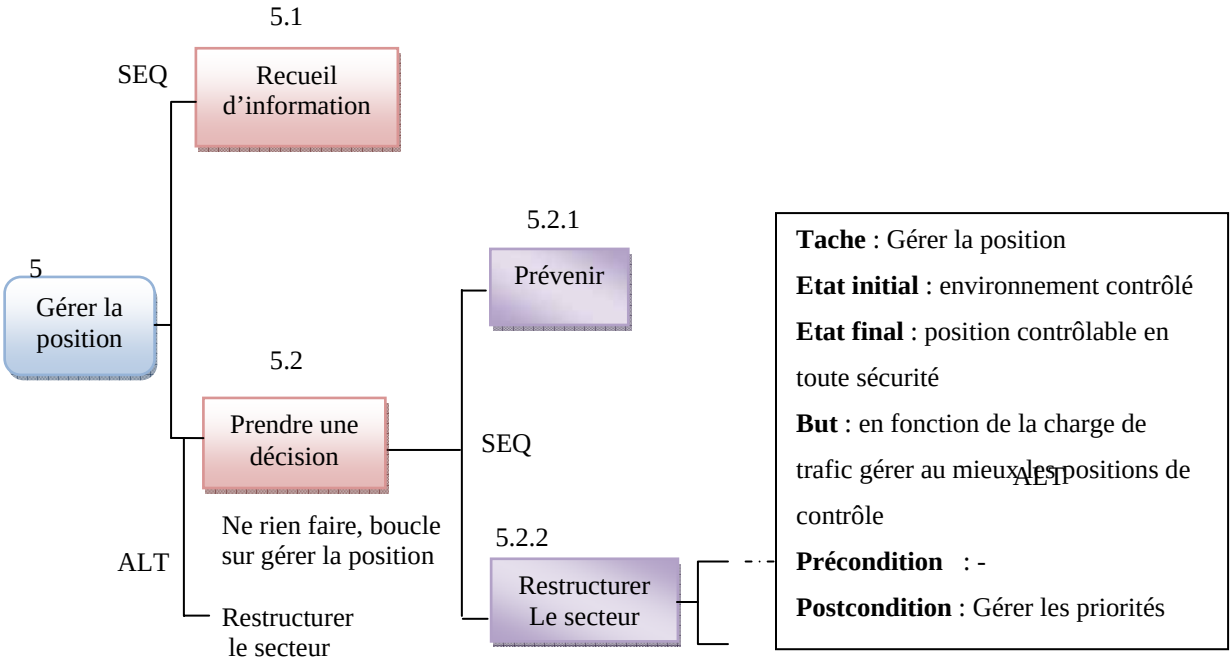


Figure II-3 : modélisation des tâches humaines basée sur MAD [17]

II-3-2-2/ Analyse et modélisation cognitive des opérateurs humains :

Afin d'assister efficacement les opérateurs humains et améliorer ainsi l'efficacité et la fiabilité du système homme-machine. Il s'agit d'analyser puis de modéliser leurs caractéristiques, leur manière de travailler, de raisonner et d'agir. Ce travail est réservé aux spécialistes des facteurs humains, et doit déboucher sur une banque de données qui sera considérée lors de la spécification et de l'évaluation des moyens interactifs mis à la disposition des opérateurs en salle de contrôle. En considérant que les fonctions du système d'assistance doivent être adaptées aux processus de raisonnement mis en œuvre par les opérateurs. L'identification de ces processus est nécessaire, celle-ci peut s'appuyer sur des tentatives de modélisation, recensées dans la littérature depuis plus de vingt ans, certaines d'entre elles sont successivement résumées ci-dessous [18].

II-3-2-2-1/ Tentative de modélisation de la mémoire humaine :

Selon une première approche, on considère que la mémoire humaine est composée de trois systèmes de stockage de l'information: le registre de l'information sensorielle, la mémoire à court terme et la mémoire à long terme. Selon le modèle, l'utilisateur d'un logiciel

est représenté par un système de traitement d'informations régi par des règles, et qui comprend un ensemble de mémoires et de processeurs interconnectés.

Chaque mémoire est caractérisée particulièrement par trois paramètres : sa capacité, sa persistance (ou durée de vie) et le type d'information mémorisée. Les informations stockées sont exploitées et mises à jour par des processeurs extérieurs, chaque tâche peut être décomposée en opérations élémentaire. Ces opérations sont ensuite mises en relation avec les besoins potentiels humains en matière de mémorisation, ce qui conduit à identifier des besoins en assistance.

II-3-2-2-2/ Tentative de modélisation des activités humaines :

Les deux approches de modélisation des activités humaines les plus couramment considérées actuellement sont certainement celles proposées par RASMUSSEN et NORMAN, représentatives de deux écoles de pensée, l'une européenne, et l'autre américaine.

Malgré leurs limites, elles ont permis à de nombreux développeurs de systèmes interactifs de prendre conscience d'un ensemble de notions, issues de la psychologie, relatives aux interactions homme-machine.

II-3-2-2-2-1/ Echelle de décision :

RASMUSSEN a proposé un cadre, appelé « échelle de décision », illustrant la démarche générale de résolution de problème suivie par un opérateur humain. « L'échelle de décision » de RASMUSSEN comprend plusieurs étages séquentiels de traitement d'informations. La détection d'événement anormal met l'utilisateur en état d'alerte, suite à l'apparition d'une alarme ou par l'observation de l'évolution anormale d'une ou plusieurs variables ; l'évaluation de la situation consiste pour l'opérateur à observer l'ensemble des informations utiles de façon à identifier l'état du système ; compte tenu de l'état précédemment identifié et des objectifs assignés à l'utilisateur. Celui-ci définit une stratégie générale de correction, qu'il décompose ensuite en tâches, puis en procédures d'actions ; le dernier étage concerne l'exécution des actions [18].

II-3-2-2-2-2/ Théorie de l'action de NORMAN :

La théorie avancée par NORMAN, quant à elle, introduit la notion de modèle conceptuel et explique les différentes étapes cognitives nécessaires à la réalisation d'une tâche exécutée à l'aide d'un système informatique. Le modèle conceptuel correspond à une représentation mentale en termes de variables dites psychologiques : à chaque concept, unité de connaissance ou sujet d'intérêt correspondra une variable psychologique.

La théorie de l'action comporte sept étapes [14] :

1. L'établissement d'un but : un but est une représentation mentale de l'état du système que l'opérateur souhaite atteindre, et ceci en agissant sur des dispositifs de commande.
2. La formulation d'une intention : celle-ci correspond à la décision d'agir afin d'atteindre un but préétabli.
3. L'adoption par l'opérateur d'un plan d'action : elle correspond à la représentation psychologique de l'ensemble des actions et de leur ordonnancement que l'utilisateur doit exécuter au moyen des dispositifs physiques, et ceci dans le but d'atteindre son objectif.
4. L'exécution du plan d'action : le plan est mis en application en agissant sur le système. Celui-ci est donc modifié.
5. La perception du nouvel état du système : l'opérateur constate un ensemble de changements survenus sur le système.
6. L'interprétation de la modification des variables physiques en termes psychologiques : elle aboutit à une représentation mentale du nouvel état du système.
7. La comparaison entre l'état du système avec le but préétabli et les intentions formulées : elle peut conduire à la poursuite du plan ou à sa modification.

II-3-3/ Spécification de l'imagerie de supervision :

La spécification de l'imagerie utilisée par les opérateurs en salle de contrôle est réalisée à partir de la modélisation des tâches humaines et des différents utilisateurs. Il s'agit de recenser rigoureusement les besoins, ergonomiques et techniques, puis de définir le nombre d'écrans à utiliser, l'architecture de l'interface homme-machine, l'enchaînement des vues, les modes de présentation des informations, les modes d'activation des différents outils d'aide, les modalités de dialogue homme-machine, etc.

Plusieurs facteurs sont à l'origine de la spécification de l'imagerie de supervision que nous allons aborder sommairement [19]:

II-3-3-1/ Spécifications issues du génie logiciel :

Ces techniques sont basées sur les langages formels qui permettent de spécifier la syntaxe du dialogue homme-machine, sous la forme de séquences d'actions autorisées pour les utilisateurs de l'imagerie telles que les automates d'état fini et les réseaux de Pétri.

II-3-3-2/ Spécifications issues de recommandations ergonomiques et de guides de style :

La spécification de l'imagerie peut être améliorée par l'utilisation de deux types de documents en rapport avec l'ergonomie des logiciels :

1. Les manuels ergonomiques.
2. Les guides de style.

II-3-3-3/ Spécifications provenant de normes :

Depuis les années 1970, des organismes de normalisation se sont penchés sur la normalisation des symboles graphiques et de leurs codes d'utilisation pour les affichages des composants représentant des installations industrielles telles que la norme internationale ISO 3511, la norme britannique BS 1646, et la norme allemandes DIN 19 227.

II-3-4/ Les environnements graphiques de réalisation de l'imagerie :

Le marché informatique actuel offre un éventail varié d'environnements graphiques facilitant la réalisation et la modification d'interface homme-machine en réduisant l'écriture de code et en permettant la réutilisabilité des programmes.

II-3-4-1/ Utilisation de boites à outils :

La première catégorie est basée sur l'utilisation de boîtes à outils, et s'adresse à des programmeurs. Elles facilitent l'écriture de programmes de dialogue à partir des différents dispositifs d'entrées/sorties d'information (écran, souris, clavier, etc.).

Les boîtes à outils exigent un apprentissage souvent long pour le programmeur qui doit de surcroît complètement concevoir les enchaînements entre vues. Cependant, elles ont l'avantage d'intégrer des critères ergonomiques de base, en particulier de standardisation de la présentation de l'information (menus prédéfinis, format et manipulation de fenêtres, présentation d'icônes par exemple).

Elles sont également caractérisées par la portabilité des logiciels interactifs résultants et l'extensibilité des fonctions qu'elles intègrent. Toutefois, le manque de souplesse qu'implique leur utilisation ne facilite pas le prototypage.

II-3-4-2/ Utilisation d'éditeurs d'interfaces :

Nous nous intéressons ici uniquement aux éditeurs d'interfaces permettant de spécifier interactivement l'interface, ceux-ci peuvent s'adresser à des développeurs non-informaticiens, et consistent en des outils graphiques interactifs facilitant le prototypage.

Un énorme avantage que possèdent de plus en plus d'éditeurs d'interfaces actuels est d'être facilement exploitables par des spécialistes de l'ergonomie du logiciel et de produire des interfaces immédiatement évaluables. Cependant, ils sont parfois limités par les modes de représentation disponibles (même remarque que pour certaines boîtes à outils). Même si le développeur a accès avec certains éditeurs à des modes de représentation classiques en supervision tels des barre-graphes, des courbes, des symboles, etc. Il peut éprouver les pires difficultés à parvenir à une représentation d'information moins conventionnelle.

Afin de pallier ce problème, certains environnements offrent la possibilité de programmer de nouveaux modes de représentation. La plupart des éditeurs graphiques du marché ne sont pas prévus au départ pour la supervision de systèmes complexes, ils s'intègrent donc dans des environnements logiciels plus ou moins adaptés aux contraintes temporelles sévères liées à certaines applications. Dans ce cas, il peut être nécessaire de remettre en cause l'utilisation d'un éditeur et de s'orienter sur une boîte à outils, plus « proche de la machine », ou sur un progiciel spécialisé [19].

II-3-4-3/ Utilisation de progiciels spécialisés :

Les progiciels graphiques spécialisés dans la supervision temps réel de systèmes industriels complexes sont généralement interfaçables directement avec plusieurs automates et calculateurs du marché.

Ces progiciels consistent en des squelettes d'applications interactifs et configurables, et regroupent le code réalisant les fonctions usuelles de l'interface homme-machine sous la forme d'un logiciel réutilisable selon les besoins.

La démarche consiste alors à configurer l'outil par rapport à l'application. Pour ce faire, on dispose d'outils de déclaration des caractéristiques de l'installation, de création de synoptiques, mais aussi de configuration de modules d'assistance : affichage d'alarmes, de conseils d'action, de valeurs prédites, etc.

Ainsi, au contraire des deux autres catégories d'outils citées, la plupart des progiciels graphiques spécialisés intègrent des fonctionnalités de base d'assistance à l'utilisateur lors de la réalisation de ses tâches.

II-3-5/ L'évaluation du système homme-machine :

Le système homme-machine est vérifié, s'il correspond aux spécifications issues de la définition des besoins. Il est validé, s'il correspond aux besoins en respectant les contraintes

du domaine d'application (sécurité, production, ergonomie…) ; sinon ses insuffisances par rapport à des critères identifiés a priori sont mises en évidence et doivent être corrigées.

Une évaluation rigoureuse nécessite de suivre une démarche avec des méthodes et des techniques. Lorsque le système à évaluer existe, des méthodes d'analyse de données comportementales recueillies au moyen d'observations ou de mesures, sur le terrain ou en laboratoire, sont préconisées, ces méthodes consistent généralement à réaliser des tests d'utilisabilité avec des opérateurs habituels ou des sujets sélectionnés pour l'expérience.

Ce type d'évaluation s'effectue a posteriori sur des imageries déjà utilisées ou prototypées et aboutit à l'émission de jugements relatifs à leur utilisation, cette approche d'évaluation est la plus répandue pour l'instant. De nombreuses méthodes et modèles issus de l'ingénierie et des sciences cognitives sont appliquées pour évaluer les systèmes homme-machine qu'on peut classer selon deux approches :

II-3-5-1/ <u>Approche empirique</u> :

Selon l'approche empirique, l'évaluation du système homme-machine est effectuée à partir du recueil et de l'analyse de données provenant de phases d'utilisation par des opérateurs représentatifs, et ceci dans un environnement d'évaluation le plus proche possible de celui d'utilisation, deux approches peuvent être distinguées :

II-3-5-1-1 / <u>Tests de conception, prototypage</u> :

Ce type d'évaluation peut être mis en œuvre a priori lorsqu'il n'existe pas encore d'expérience d'utilisation du système, des tests sont alors réalisés tout au long du processus de conception. Il est souvent utile de commencer par des tests relatifs à la sélection d'alternatives de conception lorsqu'il n'existe pas de critère de choix évident entre plusieurs possibilités (concernant par exemple le choix des symboles graphiques. La codification des variables du procédé, la structure des messages d'alarme, etc.), et le recueil des données empiriques doit alors permettre de hiérarchiser les solutions envisagées au départ, cette méthode est la plupart du temps conduite en amont du prototypage [16].

II-3-5-1-2/ <u>Évaluation par diagnostic d'usage</u> :

Cette évaluation est effectuée le plus souvent a posteriori lorsqu'il existe une expérience d'utilisation du système dans sa globalité. Pas mal de techniques, permettent de diagnostiquer des fonctions ou des modes de représentation défaillants, inutiles, difficiles à exploiter.

La méthode des incidents critiques consiste à recueillir systématiquement les dysfonctionnements du système homme-machine à partir d'entretiens avec les utilisateurs et d'observations effectuées sur leur poste de travail. Chaque incident est décrit sous la forme de court récit, les récits font l'objet d'une classification regroupant des incidents issus d'un même problème. Les problèmes sont ensuite regroupés en classes plus générales, elles peuvent être ensuite utilisées pour définir les premières fonctionnalités d'un nouveau système.

La méthode de questionnaire d'utilisation permet à l'évaluateur de recueillir des informations subjectives sous une forme sûre et structurée, propice à l'analyse, elle a l'avantage de permettre à l'opérateur de travailler à tête reposée. Même si ceci est susceptible d'introduire un biais dans ses réponses, puisqu'il n'est pas toujours en mesure de se souvenir des difficultés rencontrées lors des différentes situations de travail.

La méthode d'analyse des mouvements oculaire est un autre moyen qui sert à l'évaluation car dans la supervision. Il est fait énormément appel à la perception visuelle des informations, dans ces conditions. La direction absolue du regard devient un élément utilisable en parallèle avec d'autres moyens pour analyser l'activité d'un utilisateur devant un écran ou un ensemble de supports d'informations. Il est possible, à partir de l'étude de son activité oculomotrice, d'étudier la manière dont il recherche et localise les informations utiles en fonction des différentes situations, de mettre en évidence des stratégies utilisées et d'identifier des lacunes liées aux outils lors de certaines situations de crise [16].

II-3-5-2/ Approche analytique de l'évaluation [17]:

L'approche analytique vise à contrôler la qualité de l'interface selon un modèle défini a priori ; ce modèle peut être soit informel, soit formel.

II-3-5-2-1/ Evaluation par modèle informel :

Le premier type d'évaluation consiste à faire intervenir un spécialiste en communication homme-machine pour juger de la qualité du système homme-machine et proposer des améliorations. Cette méthode est sans doute celle qui donne les meilleurs résultats.

Le deuxième type d'évaluation repose sur des grilles d'évaluation qui ont pour objectif d'assister l'évaluateur en recensant des paramètres caractérisant l'ergonomie d'une imagerie. Pour chacun de ces paramètres, l'imagerie peut être notée systématiquement selon une échelle comportant plusieurs points, elle est utilisable par des concepteurs, des spécialistes des facteurs humains et des utilisateurs finaux du système.

II-3-5-2-2/ Evaluation par modèle formel :

Dans l'approche analytique on distinguera alors les modèles prédictifs et les modèles de qualité de l'interface, plusieurs modèles formels dits prédictifs sont progressivement mis au point. Partant de l'hypothèse que certaines performances de l'opérateur peuvent être prédites, et donc considérées lors de la conception de l'interface. Ces méthodes d'analyse et de modélisation des tâches humaines permettaient implicitement d'intégrer un état d'esprit d'évaluation a priori dans la démarche de conception telle que la méthode de modélisation MAD [17].

II-4/ Architecture logicielle d'interface homme-machine :

Quoique cette partie soit réservée aux informaticiens, il s'avère nécessaire d'introduire quelques notions élémentaires sur la conception de logiciels dédiés aux HMI. En effet la mise en œuvre d'un système interactif et en particulier de la partie correspondant à l'interface homme-machine est une tâche difficile, longue et coûteuse.

Cette affirmation refuse de disparaître en dépit des progrès techniques et des efforts de recherche dans le domaine de l'interaction homme-machine. Les raisons à cela sont multiples : tout d'abord l'attitude de l'utilisateur change, l'utilisateur soumis aux "ordres de la machine", succède aujourd'hui un utilisateur plus demandeur qui veut voir en l'ordinateur un outil utile et disponible de partout et à tout instant. De plus l'innovation technologique accélère l'allure, elle se manifeste par le progrès des performances et de la miniaturisation mais aussi par des techniques interactives toujours plus robustes.

II-4-1/ Modèles d'architecture pour les systèmes interactifs :

Bien que les modèles d'architecture diffèrent, ils répondent tous au même principe celui de la distinction entre les services d'une application et les fonctions chargées d'assurer l'interaction avec l'utilisateur. L'application appelée aussi Noyau Fonctionnel, regroupe les concepts du domaine et les opérations qui leur sont applicables quant à l'interface il a la charge de présenter à l'utilisateur concepts et fonctions et de lui permettre de les manipuler selon un enchaînement défini par le modèle de tâches.

Deux classes de modèles d'architecture à distinguer : les modèles qui fournissent des structures fonctionnelles canoniques, et les modèles multi-agent qui visent une décomposition fonctionnelle plus fine [20].

II 4-1-1/Structures fonctionnelles canoniques :

II 4-1-1-1/ Modèle de Seeheim :

Comme nous venons de le voir le noyau fonctionnel modélise le domaine à l'aide d'objets sémantiques liés par des relations, et l'interface ou présentation est un ensemble organisé d'objets interactifs qui définissent la partie perceptible et manipulable du système interactif, le modèle de Seeheim repose sur l'indépendance entre le noyau fonctionnel et l'interface sans qu'il y ait impact sur l'échange d'information entre ces derniers, cette fonctionnalité est assuré par un troisième module qui est le contrôleur de dialogue comme le montre la figure suivante :

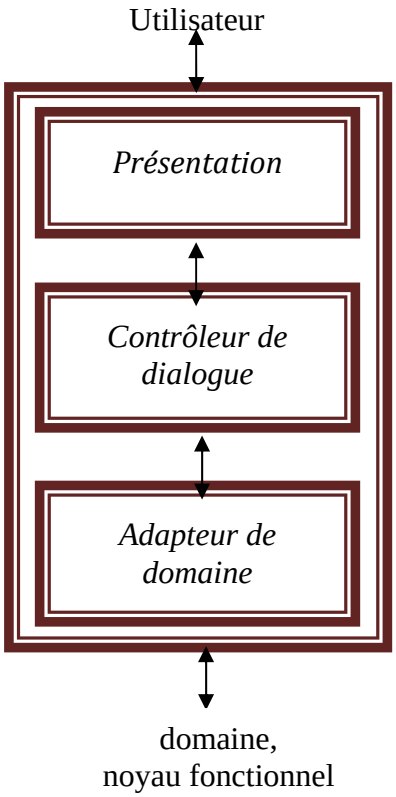


Figure II-4 : Le Modèle de Seeheim [20]

II 4-1-1-2/ Modèle Arch :

Le modèle Arch s'appuie sur les composants conceptuels du modèle Seeheim, on y retrouve les notions du noyau fonctionnel et du contrôleur de dialogue. Les pieds de l'arche constituent les composants imposés par la réalité : le noyau fonctionnel réalise les concepts du domaine ; le composant d'interaction physique, en contact direct avec l'utilisateur, est mis en œuvre au moyen des objets d'interaction d'une boîte à outils.

En clé de voûte, le contrôleur de dialogue gère l'enchaînement des tâches ainsi que les liens entre les objets regroupés dans les deux composants voisins : l'adaptateur de noyau fonctionnel et le composant d'interaction logique.

L'adaptateur de noyau fonctionnel sert, pour l'essentiel, à ajuster les différences de modélisation des objets conceptuels entre le noyau fonctionnel et le contrôleur de dialogue. Le composant d'interaction logique joue un rôle similaire : il permet au contrôleur de dialogue de s'affranchir du fonctionnement de la boîte à outils du niveau interaction physique. Le composant d'interaction logique peut se voir comme une boîte à outils virtuelle qui implémente des objets d'interaction logique concrétisés par une boîte à outil comme l'illustre la figure suivante [21]:

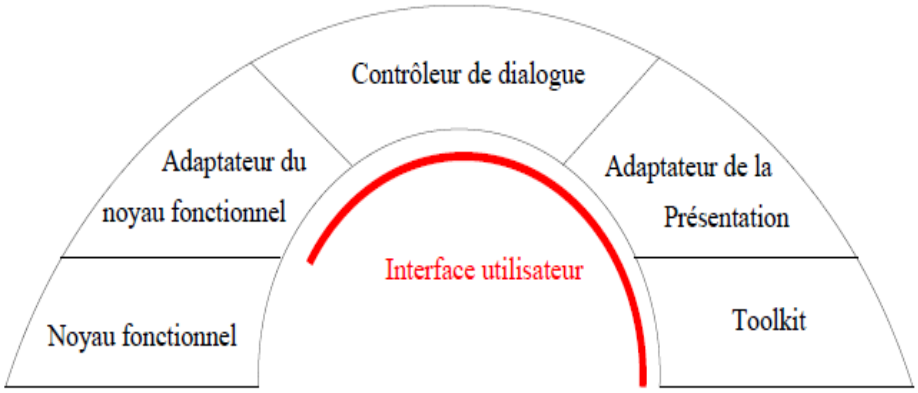


Figure II-5 : Le Modèle Arch[21]

II- 4-1-2/ Modèles multi-agent :

Les modèles multi-agent, comme PAC ou MVC, structurent un système interactif en un ensemble d'agents spécialisés réactifs. Ces modèles se caractérisent par une organisation fortement modulaire, des traitements exécutés en parallèle et une communication par événements.

Le modèle multi-agent structure un système interactif en un ensemble d'agents spécialisés qui produisent et réagissent à des événements. Un agent est un système de traitement de l'information : il possède des récepteurs et des émetteurs pour acquérir et produire des événements ; il dispose d'une mémoire pour mémoriser un état, il comprend un processeur spécialisé dans le traitement d'une ou plusieurs classes d'événements. Le résultat d'un traitement se traduit généralement par un changement d'état de l'agent et par l'émission de nouveaux événements.

Le modèle multi-agent se caractérise par une organisation fortement modulaire, des traitements exécutés en parallèle et une communication par événements. Ce modèle abstrait est à rapprocher des modèles à objets pour lesquels il existe des outils de réalisation.

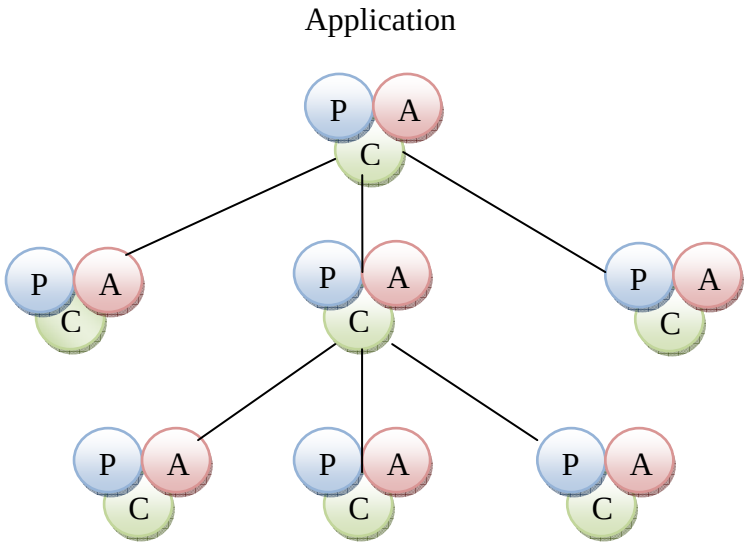
L'agent définit la granularité de la modularité, il est donc possible de modifier localement un comportement sans mettre en cause le fonctionnement de l'ensemble, comme il définit l'unité d'exécution. Donc il est possible d'exécuter des agents sur des processeurs distincts, cette propriété est essentielle à la réalisation de systèmes répartis.

L'agent définit une unité d'état, cet état peut contenir les informations nécessaires à la reprise d'une activité locale et l'agent modélise alors un fil d'activité interruptible. Un ensemble cohérent d'agents coopérants réalise avec l'utilisateur (ou avec un groupe d'utilisateurs), un dialogue à plusieurs fils d'activité. [20]

II- 4-1-2-1/ <u>Modèle PAC</u> :

PAC structure récursivement un système sous forme d'une hiérarchie d'agents, la hiérarchie permet d'exprimer des relations entre agents et reflète un continuum de niveaux d'abstraction depuis l'application jusqu'aux éléments fins de l'interaction. Un agent PAC définit une compétence à un niveau d'abstraction donné, c'est un acteur à trois facettes.

- La Présentation définit le comportement perceptible de l'agent.
- Abstraction représente son expertise.
- Contrôle qui a un double rôle : il sert de lien entre les facettes Présentation et Abstraction de l'agent et il gère des relations avec d'autres agents PAC de la hiérarchie comme le représente la figure suivante [20].



<u>Figure II-6 : Le modèles multi-agent PAC [20]</u>

II- 4-1-2-2/ Modèle MVC :

Le modèle multi-agent MVC structure aussi un agent en trois composantes, à l'origine réalisables le Modèle pour représenter un comportement interne, la Vue pour présenter l'état du Modèle, et le Contrôle pour interpréter les actions de l'utilisateur sur la Vue.

Le modèle MVC n'impose pas de contrainte sur la structuration globale d'un système interactif en agents MVC, et distingue, au sein d'un agent, le traitement des entrées (assuré par un Contrôleur) et les opérations de sortie (la Vue), la figure suivante représente le modèle MVC.

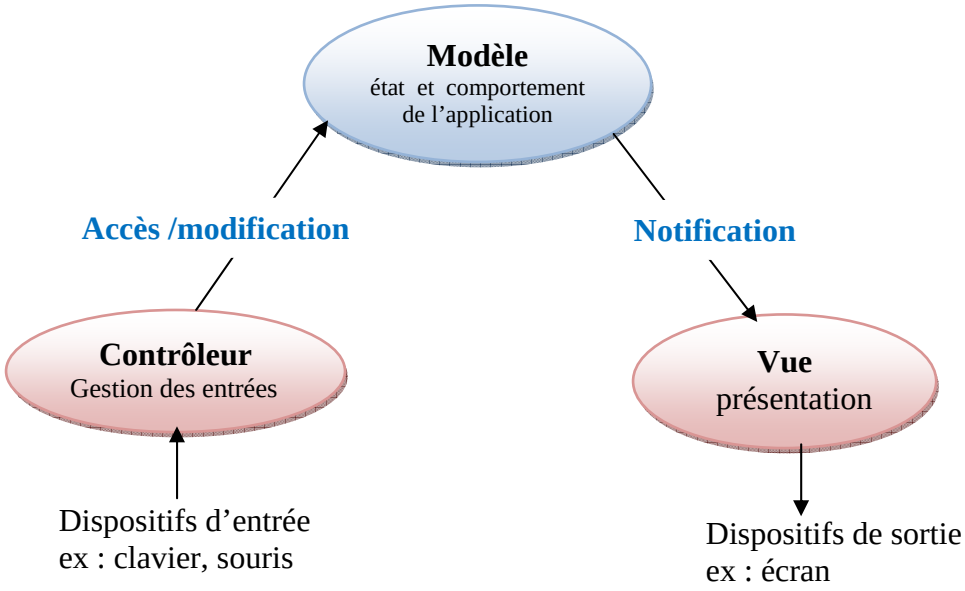


Figure II-7 : Le modèle multi-agent MVC [21]

D'autres modèles selon d'autre approches de classification existent toutefois nous allons nous limiter aux deux modèles présentés sans faire une étude approfondie qui sort du cadre de ce travail [21].

II-5/ <u>Conclusion</u> :

Dans ce chapitre on s'est intéressé à l'ingénierie des HMI en jetant la lumière sur l'architecture de logiciel des interfaces homme-machine, le sujet qu'on vient d'aborder très sommairement est très riche et diversifié en méthodes, modèles, techniques, connaissances, critères et architectures.

Il est de plus en constante évolution, liée en partie aux progrès réalisés dans les Sciences et Technologies de l 'Information, la communication et notamment l'automatisation des procédés de contrôle où l'HMI est indispensable.

CHAPITRE (III)

Supervisory Control And Data Acquisition SCADA

III-1/ Introduction

Industriels de la production ou du transport de pétrole ou de gaz naturel, il vous faut sans cesse accroître la production, répondre à des délais de livraison toujours plus serrés, réduire les coûts d'exploitation et de maintenance, tout en respectant les impositions environnementales et les politiques de sécurité.

Dans le domaine de la gestion de l'eau potable ou des eaux usées, vous devez veiller aux normes sanitaires de santé publique, protéger l'environnement et faire fonctionner les installations au meilleur coût, tout en assurant un service de distribution ou de collecte ininterrompue.

Les réglementations se multiplient, la demande croît continuellement, la sensibilisation en matière de sécurité s'intensifie, aussi la plupart des entreprises industrielles envisagent d'équiper leurs installations d'un système de supervision, de contrôle/commande et d'acquisition de données (SCADA), ou de moderniser l'existant.

Le SCADA est un système qui permet de piloter et de superviser en temps réel et à distance des procédés de production embarqués sur des plates-formes souvent géographiquement très éloignées d'un site central, mais c'est aussi un précieux outil d'aide à la prise de décisions concernant le procédé de fabrication, et sur les choix stratégiques de conduite.

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'entraîner des coupures ou la paralysie des principaux systèmes de transport dans le cadre d'une éventuelle attaque informatique ou terroriste.

III-2/ Définition du SCADA :

SCADA est un acronyme qui signifie le contrôle et la supervision par acquisition de données (en anglais : Supervisory Control and Data Acquisition) permettant la centralisation des données, la présentation souvent semi-graphique sur des postes de « pilotage ». Le système SCADA collecte des données de divers appareils d'une quelconque installation, puis transmit ces données à un ordinateur central, que ce soit proche ou éloigné, qui alors contrôle et supervise l'installation. Ce dernier est subordonné par d'autres postes d'opérateurs, l'allure générale d'un système SCADA est montrée sur la figure ci-dessous : [22], [23]

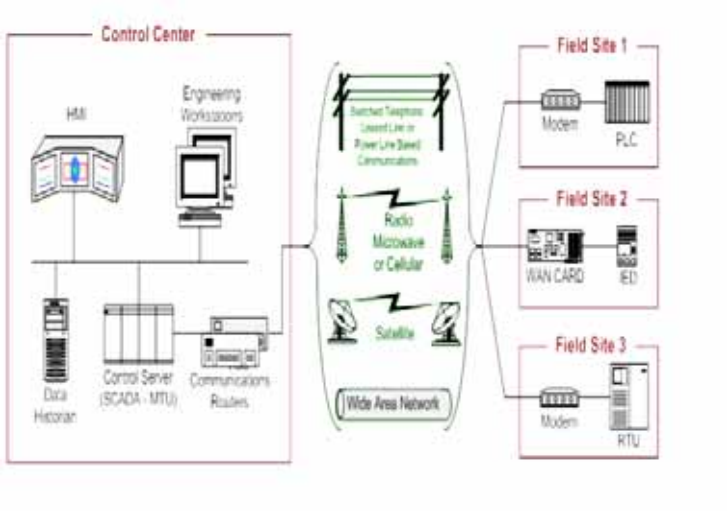


Figure III-1 : Schéma général d'un système SCADA [24]

III-3 /Eléments du système SCADA :

Principalement un système SCADA se compose de :

1. RTU (Remote Terminal Unit) : il sert à collecter les informations à partir de l'instrumentation du terrain et les transmettre au MTU à travers le système de communication.
2. MTU (Master Terminal Unit) : il recueille les données provenant des RTU, les rendre accessibles aux opérateurs via l'HMI et transmet les commandes nécessaires des opérateurs vers l'instrumentation du terrain.
3. Système de communication : moyen de communication entre MTU et les différents RTU, la communication peut être par le biais de l'Internet, réseaux sans fil ou câblé, ou le réseau téléphonique public….etc. [25], [26], [27]

III-3 -1/ RTU :

C'est une entité d'acquisition de données et de commande généralement à base de microprocesseur (actuellement on utilise des automates programmables). Il sert à contrôler et superviser localement l'instrumentation d'un site éloigné et transférer les données requises vers la salle de contrôle principal ou parfois à d'autres RTU. Il se compose de contrôleur, des cartes d'entrées et sorties (analogique, tout ou rien, impulsions) et des modules de communication.

La figure suivante représente un schéma typique d'un RTU. [25], [27]

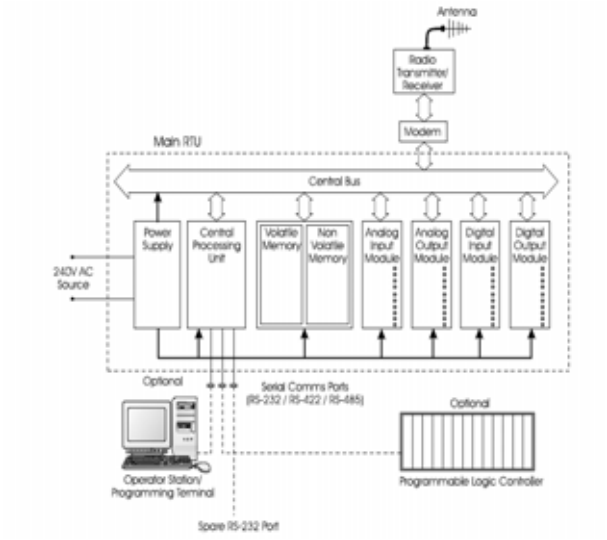


Figure III-2 : Schéma général d'un RTU [25]

III-3 -2/ MTU :

Il peut être décrit comme une station ayant plusieurs postes opérateur (liés ensemble avec un réseau local) connecté à un système de communication, comme on vient d'aborder l'MTU recueille les données de l'instrumentation du terrain périodiquement à partir des stations RTU et permet la commande à distance par le biais des postes opérateurs. En général l'MTU sert à configurer et programmer les RTU, diagnostiquer la communication et les stations RTU, la figure ci-dessous montre un schéma général d'un MTU . [25], [26], [27]

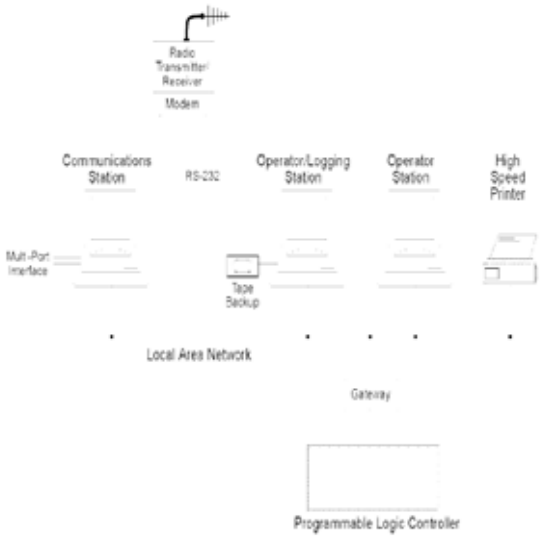


Figure III-3 : Schéma général d'un MTU [25]

III-3 -3/Communication :

Différentes architectures de communication pour un système SCADA sont disponibles, la plus simple est la communication point à point où 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 ci-dessous :

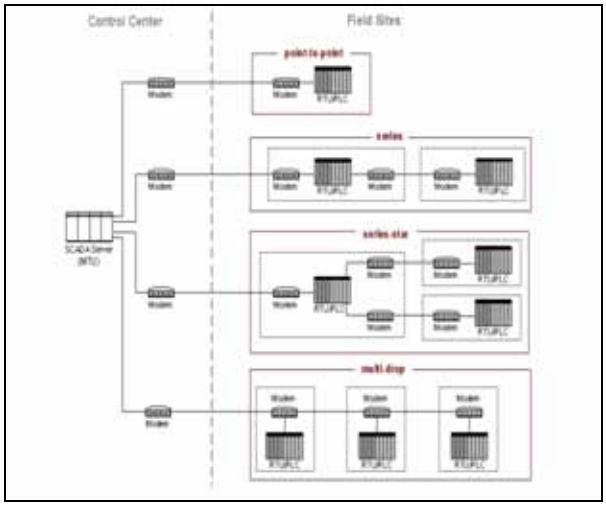


Figure III-4 : Topologie de différents modes de communication SCADA [24]

La communication peut être classifiée selon deux approches, la première qui se base sur l'approche d'interrogation et la deuxième est l'approche paire à paire (peer to peer). [28], [29]

III-3 -3-1/ 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 à la demande du maitre. [28], [30]

III-3 -3-2/ Approche paire à paire (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 qu'il doit avoir un contrôle d'accès et collision du réseau. Autrement dit il faut écouter tout d'abord avant d'entamer la communication. [29], [30]

III-3 -3-3/ Protocole employés dans un environnement SCADA :

Les protocoles de communication dans un environnement SCADA évoluent suite à la nécessité d'envoyer et de recevoir des données jugées critiques généralement pour de longues distances et en temps réel, cette optique a donné naissance de plusieurs protocoles dont on va développer les plus utilisés [28]

III-3 -3-3-1/ Le protocole Modbus :

Le protocole MODBUS [29] est un protocole de transmission de données régissant le dialogue entre une station "Maitre" et des stations "Esclaves".L'échange Maitre-Esclave s'effectue par l'envoi de trames MODBUS 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 (CRC16) 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.

Modbus (marque déposée par Modicon) est un protocole de communication utilisé pour des réseaux d'automates programmables.

III-3 -3-3-2/ Le protocole DNP3 :

Le protocole DNP3 [30] est un protocole de communication multipoint qui 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.

DNP3 est construit sur le profil EPA (Enhanced Performance Architecture) qui est une version simplifiée du modèle OSI (Open System Interconnection).

L'EPA comporte seulement 3 couches :

1. Physique
2. liaison
3. application.

Toutefois, pour permettre la transmission de messages de taille importante (2 kilo-octets ou plus), des fonctions de segmentation et de réassemblage de données ont été ajoutées. L'ensemble de ces fonctions constitue une pseudo-couche Transport. [29]

III-3 -3-3-3/ <u>Le protocole PROFIBUS</u> :

PROFIBUS est un 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. De même, selon l'application, il peut emprunter trois supports de transmission ou supports physiques (RS 485, CEI 1158-2 ou fibre optique).

PROFIBUS répond à des normes internationales unanimement reconnues. Son architecture repose sur 3 couches inspirées du modèle en 7 couches de l'OSI, la couche 1, physique, décrit les caractéristiques physiques de la transmission. La couche 2, liaison de données, spécifie les règles d'accès au bus. Enfin, la couche 7, application, définit les mécanismes communs utiles aux applications réparties et la signification des informations échangées, la figure suivante représente l'architecture de la communication PROFIBUS. [26], [29], [30]

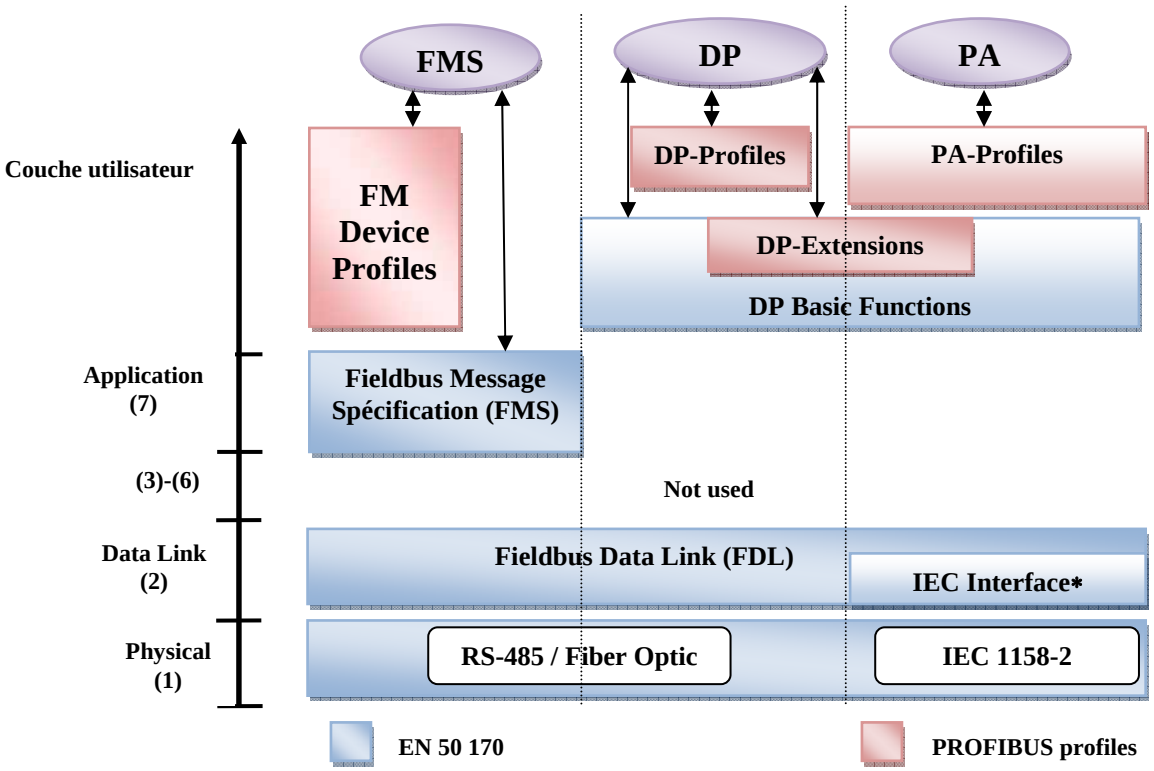


Figure III-5 : Architecture de communication PROFIBUS [28]

III-4/ Le logiciel SCADA

Le logiciel d'interface homme/procédé SCADA fournit à la fois des vues graphiques de l'état des terminaux à distance et leurs historiques d'alarmes. Il permet de visualiser l'ensemble des données du procédé et d'intervenir à distance sur les machines, il génère des rapports d'exploitation et de contrôle de données environnementales. Il archive la synthèse des données dans ses bases d'historiques.

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
- La capture des notifications d'alarme adressées au personnel d'exploitation et de maintenance par message texte ou par voie vocale.

- La génération des rapports d'exploitation et les rapports réglementaires régulièrement
- La gestion de la sécurité des processus et des procédés à travers l'ensemble des installations et l'administration des authentifications et les habilitations pour l'accès des personnels

En plus l'interface graphique doit faciliter aux opérateurs toute ces taches citées, l'HMI du SCADA est très important pour le bon déroulement de la procédure d'aide à la décision, il est le seul point d'interaction entre l'opérateur et les algorithmes d'aide à la décision. Ainsi, il aide l'opérateur 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. [23], [25]

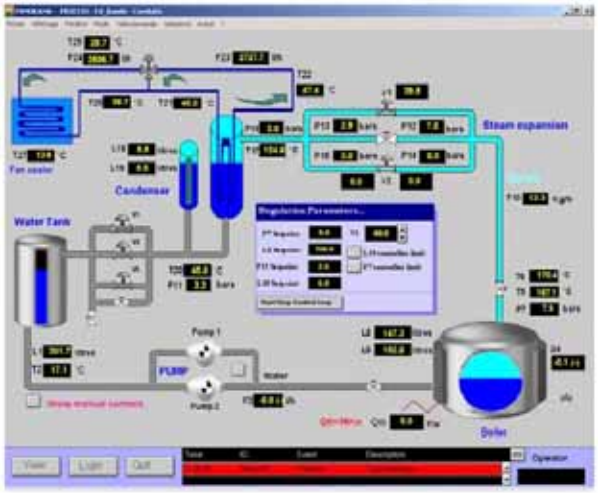


Figure III-6 : Exemple de logiciel SCADA/IHM [22]

III-5/ <u>Conclusion</u> :

Dans ce chapitre nous avons étudié le système SCADA en détaillant ses éléments, en passant par les protocoles de communication les plus utilisés dans un tel système et en terminant avec ses logiciels.

Le système SCADA 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 si jamais un accident survient et aussi réduit énormément le nombre de visite au site.

CHAPITRE (IV)

IV-1/ Introduction

La sécurité est une fonction incontournable des réseaux. Puisqu'on ne voit pas son correspondant directement, il faut l'authentifier. Puisqu'on ne sait pas par où passent les données, il faut les chiffrer. Puisqu'on ne sait pas si quelqu'un ne va pas modifier les informations émises, il faut vérifier leur intégrité. Nous pourrions ajouter une longue suite de requêtes du même genre qui doivent être prises en charge par les réseaux.

Globalement, on peut scinder la sécurité en deux parties : la sécurité à l'ouverture de la session et la sécurité lors du transport de l'information. Les techniques pour réaliser ces deux formes de sécurité sont extrêmement diverses, et il s'en invente de nouvelles tous les jours [1].

Nous nous intéressons beaucoup plus à la sécurité au réseau INTERNET mais il est indispensable de voir la sécurité d'une manière générale.

IV-2/ Concepts généraux :

IV-2-1/ Les services de sécurité :

En informatique, le terme sécurité recouvre tout ce qui concerne la protection des informations, cette fonctionnalité est assurée par cinq types de service de sécurité comme suit [31]:

- La confidentialité, qui doit assurer la protection des données contre les attaques non autorisées.
- L'authentification, qui doit permettre de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué.
- L'intégrité, qui garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.
- La non-répudiation, qui assure qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.
- Le contrôle d'accès, qui a pour fonction de prévenir l'accès à des ressources sous des conditions définies et par des utilisateurs spécifiés.

Dans chacun de ces services, il peut exister des conditions particulières, si l'on reprend les cinq services de sécurité présentés précédemment en étudiant les besoins de l'émetteur et du récepteur et en les répertoriant, on obtient le processus suivant :

1. Le message ne doit parvenir qu'au destinataire.
2. Le message doit parvenir au bon destinataire.
3. L'émetteur du message doit pouvoir être connu avec certitude.
4. Il doit y avoir identité entre le message reçu et le message émis.
5. Le destinataire ne peut contester la réception du message.
6. L'émetteur ne peut contester l'émission du message.
7. L'émetteur ne peut accéder à certaines ressources que s'il en a l'autorisation.

Le besoin 1 correspond à un service de confidentialité, les besoins 2 et 3 à un service d'authentification, le besoin 4 à un service d'intégrité des données, les besoins 5 et 6 à un service de non-répudiation, et le besoin 7 au contrôle d'accès. [32]

IV-2-2/ Les Mécanismes De Chiffrement :

Le chiffrement est un mécanisme issu d'une transformation cryptographique et le mécanisme inverse du chiffrement est le déchiffrement. [33]

Les principaux mécanismes de chiffrement normalisés par l'ISO sont les suivants:

- Le mécanisme de bourrage de trafic consiste à envoyer de l'information en permanence en complément de celle déjà utilisée de façon à empêcher les fraudeurs de repérer si une communication entre deux utilisateurs est en cours ou non.
- L'authentification qui en général utilise des techniques de chiffrement symétrique et à clés publiques.
- L'intégrité des informations
- La signature numérique est un mécanisme appelé à se développer de plus en plus.

IV-2-2-1 / Les Algorithmes De Chiffrement :

Les algorithmes de chiffrement permettent de transformer un message écrit en clair en un message chiffré, appelé cryptogramme. Cette transformation se fonde sur une ou plusieurs clés, le cas le plus simple est celui d'une clé unique et secrète, que seuls l'émetteur et le récepteur connaissent.

Les systèmes à clés secrètes sont caractérisés par une transformation f et une transformation inverse f^{-1}, qui s'effectuent à l'aide de la même clé. C'est la raison pour laquelle on appelle ce système « à chiffrement symétrique » [31].

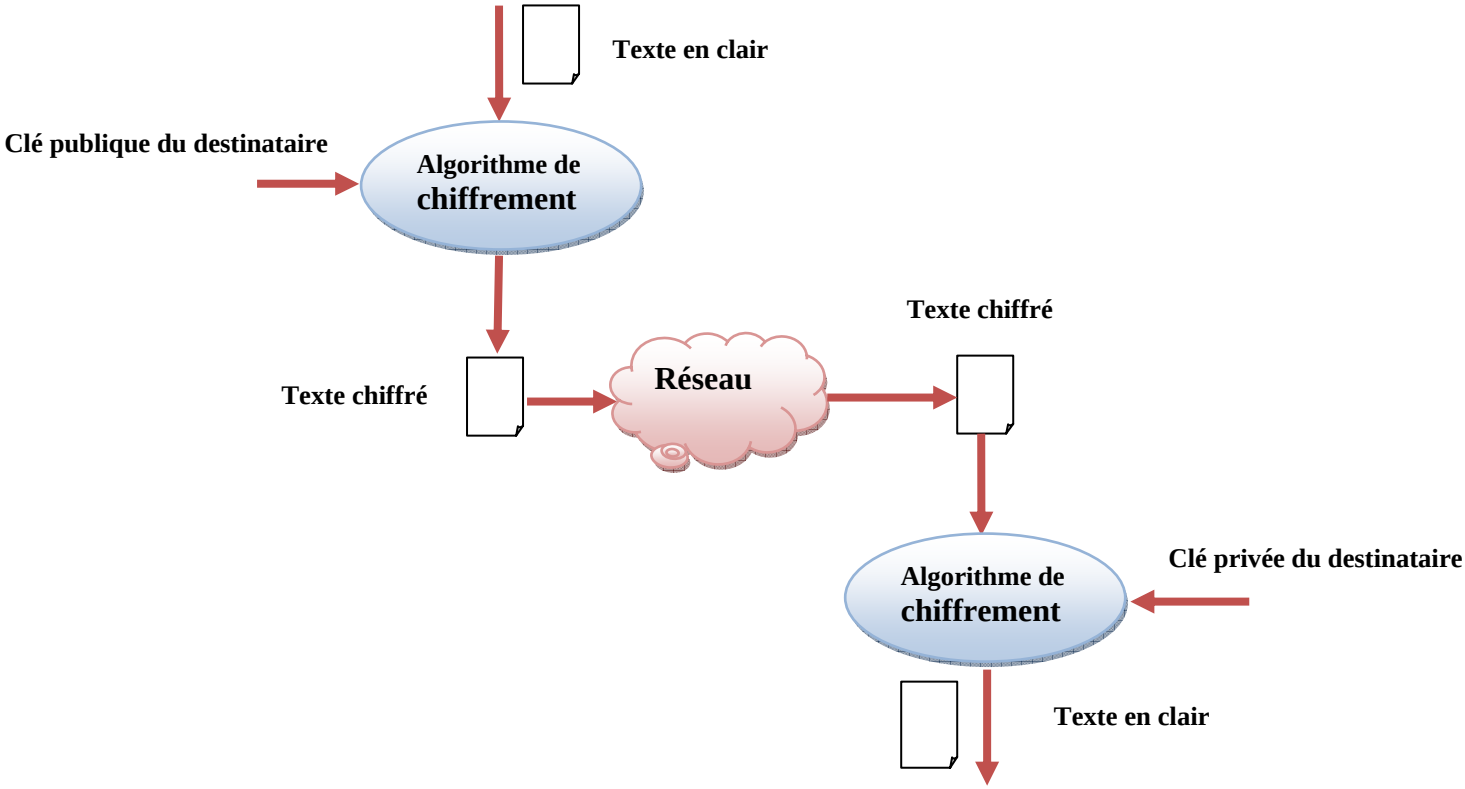


Figure IV-1 : Algorithme de chiffrement symétrique [1]

Les signatures électroniques font également partie de la panoplie des mécanismes indispensables à la transmission de documents dans un réseau. La signature a pour fonction d'authentifier l'émetteur, celui-ci code le message de signature par une clé qu'il est le seul à connaître, la vérification d'une signature s'effectue par le biais d'une clé publique [2].

IV-2-2-2 / Les Certificats :

Une difficulté qui s'impose à la station d'un réseau qui communique avec beaucoup d'interlocuteurs consiste à se rappeler de toutes les clés publiques dont elle a besoin pour récupérer les clés secrètes de session. Pour cela, il faut utiliser un service sécurisé et fiable, qui délivre des certificats. Un organisme offrant un service de gestion de clés publiques est une autorité de certification, appelée tiers de confiance, cet organisme émet des certificats au sujet de clés permettant à une entreprise de les utiliser avec confiance [2].

Un certificat est constitué d'une suite de symboles (document M) et d'une signature.

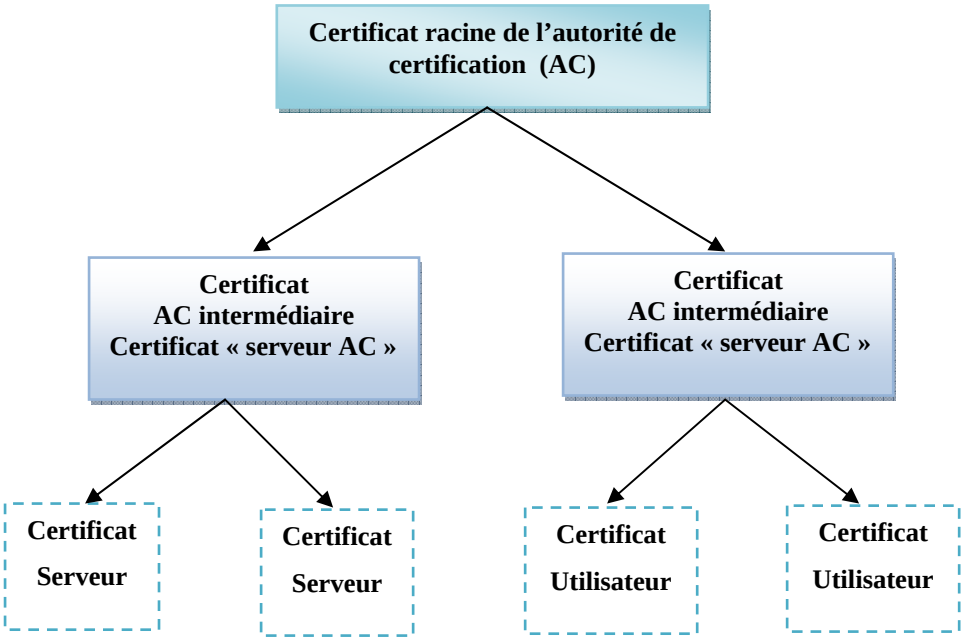


Figure IV-2 : Exemple de chemin de certification [2]

IV-2-3 / La Sécurité Dans Un Environnement IP :

Un environnement IP n'est pas à l'abri des attaques qu'on peut diviser en deux grands champs : celles qui visent les équipements terminaux et celles qui visent le réseau Internet lui-même, elles ne sont pas totalement indépendantes puisque les attaques des machines terminales par Internet utilisent souvent ses défauts.

Les attaques du réseau Internet lui-même consistent à essayer de dérégler un équipement de routage ou un serveur, comme les serveurs DNS, ou à obstruer les lignes de communication par contre les attaques des machines terminales consistent à prendre le contrôle de la machine pour effectuer des opérations non-conformes.

Très souvent, ces attaques s'effectuent par le biais des logiciels réseau qui se trouvent dans la machine terminale [3].

IV-2-3-1/ Les attaques :

Le réseau internet est le sujet de multiples attaques, on va voir quelques unes : les plus connues.

IV-2-3-1-1/ Les attaques par ICMP :

Le protocole ICMP (Internet Control Message Protocol) est utilisé par les routeurs pour transmettre des messages de supervision permettant. Par exemple, d'indiquer à un utilisateur la raison d'un problème. Un premier type d'attaque contre un routeur ou un serveur réseau consiste à générer des messages ICMP en grande quantité et à les envoyer vers la machine à attaquer à partir d'un nombre de sites important.

Pour inonder un équipement de réseau, le moyen le plus simple est de lui envoyer des messages de type Ping lui demandant de renvoyer une réponse. On peut également inonder un serveur par des messages de contrôle ICMP d'autres types [34].

IV-2-3-1-2/ Les attaques par TCP :

Le protocole TCP travaille avec des numéros de port qui permettent de déterminer une adresse de socket, c'est-à-dire d'un point d'accès au réseau. Cette adresse de socket est formée par la concaténation de l'adresse IP et de l'adresse de port, à chaque application correspond un numéro de port, par exemple 80 pour une application http [34].

Une attaque par TCP revient à utiliser un point d'accès pour faire autre chose que ce pour quoi il a été défini. En particulier, un pirate peut utiliser un port classique pour entrer dans un ordinateur ou dans le réseau d'une entreprise. La figure IV-3 illustre une telle attaque. L'utilisateur ouvre une connexion TCP sur un port correspondant à l'application qu'il projette de dérouler. Le pirate commence à utiliser le même port en se faisant passer pour l'utilisateur et se fait envoyer les réponses. Éventuellement, le pirate peut prolonger les réponses vers l'utilisateur de telle sorte que celui-ci reçoive bien l'information demandée et ne puisse se douter de quelque chose.

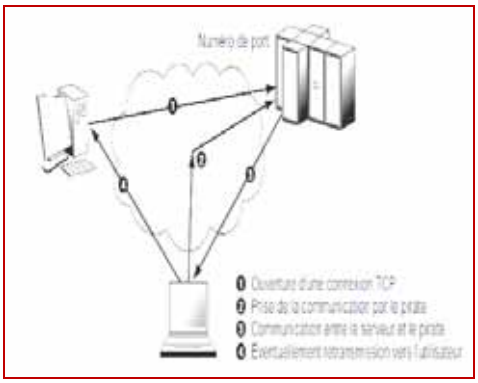


Figure IV-3 : Les attaques par TCP [34]

IV-2-3-1-3/ Les attaques par cheval de Troie :

Dans l'attaque par cheval de Troie, le pirate introduit dans la station terminale un programme qui permet de mémoriser le login et le mot de passe de l'utilisateur [34]. Ces informations sont envoyées à l'extérieur par le biais d'un message vers une boîte aux lettres anonyme.

Diverses techniques peuvent être utilisées pour cela, allant d'un programme qui remplace le gestionnaire de login jusqu'à un programme pirate qui espionne ce qui se passe dans le terminal [34].

IV-2-3-1-4/ Les attaques par dictionnaire

Beaucoup de mots de passe étant choisis dans le dictionnaire, il est très simple pour un automate de les essayer tous. De nombreuses expériences ont démontré la facilité de cette attaque et ont mesuré que la découverte de la moitié des mots de passe des employés d'une grande entreprise s'effectuait en moins de deux heures.

Une solution simple pour remédier à cette attaque est de complexifier les mots de passe en leur ajoutant des lettres majuscules, des chiffres et des signes comme !, ?, &, etc. [33]

IV-2-3-1-5/ Les autres attaques :

Le nombre d'attaques possibles est bien trop grand pour que nous puissions les citer toutes. De plus, de nouvelles procédures d'attaque s'inventent chaque jour.
Les attaques par écoute consistent, pour un pirate, à écouter une ligne de communication et à interpréter les éléments binaires qu'il intercepte. Les attaques par fragmentation utilisent le fait que les informations de supervision se trouvent dans la première partie du paquet à un emplacement parfaitement déterminé. Un pirate peut modifier la valeur du bit de fragmentation, ce qui a pour effet de faire croire que le message se continue alors qu'il aurait dû se terminer. Le pare-feu voit donc arriver une succession de fragments qui suivent les fragments de l'utilisateur sans se douter que ces fragments complémentaires ont été ajoutés par le pirate.

Les algorithmes de routage sont à la base de nombreuses attaques. En effectuant des modifications sur les tables de routage, le pirate peut récupérer de nombreuses informations qui ne lui sont pas destinées ou dérouter les paquets,

lesquels, par exemple, vont effectuer des boucles et saturer le réseau [32]. De la même façon, de nombreuses attaques sont possibles en perturbant un protocole comme ARP (Address Resolution Protocol), soit pour prendre la place d'un utilisateur, soit en captant des données destinées à un autre.

IV-2-3-2/ Les parades :

Les parades aux attaques sont nombreuses, elles relèvent autant du comportement humain que de techniques spécifiques. Nous allons examiner les principales : l'authentification, l'intégrité du flux, la non-répudiation, la confidentialité du flux et la confidentialité au niveau de l'application [32].

IV-2-3-2-1/ L'authentification :

Une des 5 premières parades visant à empêcher qu'un terminal autre que celui prévu ne se connecte ou bien qu'un terminal ne se connecte sur un serveur pirate, est offerte par les méthodes d'authentification. L'authentification peut être simple, et ne concerne que l'utilisateur, ou mutuelle, et implique à la fois le client et le serveur, dans des applications de type Telnet ou e-mail, le client s'authentifie avec un mot de passe auprès du serveur pour établir ses droits, dans une application HTTP, il est nécessaire d'authentifier le serveur puis le client, généralement à l'aide d'un mot de passe [31].

L'authentification Windows utilise le protocole de sécurité Kerberos, met en œuvre des stratégies de mot de passe portant sur la validation de la complexité des mots de passe forts et prend en charge le verrouillage des comptes et l'expiration des mots de passe. [1]

Kerberos est un algorithme d'authentification fondé sur une cryptographie, l'utilisation de cet algorithme ne permet pas à une personne qui écoute le dialogue d'un client à l'insu de ce dernier de se faire passer pour lui plus tard, ce système permet à un processus client travaillant pour un utilisateur donné de prouver son identité à un serveur sans avoir à envoyer de données dans le réseau.

L'idée sous-jacente est que le processus client doit prouver qu'il possède la clé de chiffrement qui est connue des seuls utilisateurs de base et du serveur, le client et le processus client ne connaissent pas la clé de chiffrement de base utilisée pour l'authentification, quand un client doit répondre à une demande d'authentification, il se met en contact avec le serveur pour générer une nouvelle clé de chiffrement et se la

faire envoyer de façon sécurisée, cette nouvelle clé est appelée clé de session, le serveur utilise un ticket Kerberos pour envoyer la clé de session au vérificateur par l'intermédiaire du client.

Le ticket Kerberos est un certificat provenant, comme nous venons de le voir, du serveur d'authentification, il est chiffré avec la clé de base que ne connaît pas le client, le ticket contient des informations, parmi lesquelles la clé de session qui est utilisée pour l'authentification, le nom de l'utilisateur de base a un temps d'expiration après lequel la clé de session n'est plus valide, puisque le ticket est chiffré avec la clé de base, connue seulement du serveur et du vérificateur, il est impossible au client de modifier le ticket sans que cela passe inaperçu, à la réception du ticket Kerberos, le vérificateur le déchiffre, extrait la clé de session et utilise celle-ci pour déchiffrer le nom du serveur.

IV-2-3-2-2/ <u>L'intégrité du flux de données</u> :

L'intégrité d'un flux de données demande qu'il ne puisse y avoir une altération des informations transportées. Un pirate pourrait en effet modifier une information pour tromper le récepteur. Il est à noter qu'intégrité ne signifie pas confidentialité. En effet, il est possible que l'information ne soit pas confidentielle et qu'elle puisse être recopiée, sans que cela pose de problème à l'utilisateur. Cependant, l'utilisateur veut que son information arrive intègre au récepteur [31].

La solution classique à ce genre de problème consiste à utiliser une empreinte. À partir de l'ensemble des éléments binaires dont on souhaite assurer l'intégrité, on calcule une valeur, qui ne peut être modifiée sans que le récepteur s'en rende compte. Les empreintes regroupent les solutions de type empreinte digitale, signature électronique, analyse rétinienne, reconnaissance faciale et, d'une manière générale, tout ce qui permet de signer de façon unique un document. Ces différentes techniques de signature proviennent de techniques d'authentification puisque, sous une signature, se cache une authentification. Dans les réseaux IP, la pratique de la signature électronique est de plus en plus mise en œuvre pour faciliter le commerce et les transactions financières [31].

IV-2-3-2-3/ <u>La non-répudiation</u> :

La non-répudiation consiste à empêcher l'éventuel refus d'un récepteur d'effectuer une tâche suite à un démenti de réception. Si la valeur juridique d'un fax

est reconnue, celle d'un message électronique ne l'est pas encore. Pour qu'elle le soit, il faut un système de non-répudiation. Les parades visant à éviter qu'un utilisateur répudie un message reçu proviennent essentiellement d'une signature unique sur le message et sur son accusé de réception, c'est-à-dire une signature qui ne serait valable qu'une seule fois et serait liée à la transmission du message qui a été répudié. Un système de chiffrement à clés publiques peut être utilisé dans ce contexte.

Une autre solution, qui se développe, consiste à passer par un notaire électronique, qui, par un degré de confiance qui lui est attribué, peut certifier que le message a bien été envoyé et reçu. Une difficulté importante de la non-répudiation dans une messagerie électronique provient de la vérification que le récepteur en a pris possession et a lu le message, il n'existe pas de règle aujourd'hui sur Internet pour envoyer des messages de type lettre recommandée. Le récepteur peut, par exemple, recevoir le message dans sa boîte aux lettres électronique mais ne pas le récupérer. Il peut également recopier le message dans la boite aux lettres de son terminal et le supprimer sans le lire [31].

Les techniques de non-répudiation ne sont pas encore vraiment développées dans le monde IP. En effet, cette fonction de sécurité est souvent jugée moins utile que les autres, cependant, elle est loin d'être absente. En effet, dans le commerce électronique elle est capitale pour qu'un achat ne puisse être décommandé sans certaines conditions déterminées dans le contrat d'achat. Cette fonction serait également utile dans des applications telles que la messagerie électronique, où l'on aimerait être sûr qu'un message est bien arrivé. [31]

IV-2-3-2-4/ <u>La confidentialité</u> :

La confidentialité désigne la capacité de garder une information secrète. Le flux, même s'il est intercepté, ne doit pas pouvoir être interprété. La principale solution permettant d'assurer la confidentialité d'un flux consiste à le chiffrer.

Aujourd'hui, étant donné la puissance des machines qui peuvent être mises en jeu pour casser un code, il faut utiliser de très longues clés. Les clés de 40 bits peuvent être percées en quelques secondes et celles de 128 bits en quelques minutes sur une très grosse machine. Une clé RSA de 128 bits a été cassée en quelques heures par un ensemble de machines certes important mais accessible à une entreprise.

Pour casser une clé, il faut récupérer des données chiffrées, parfois en quantité importante, ce qui peut nécessiter plusieurs heures d'écoute, voire plusieurs

jours si la ligne est à faible débit. Une solution à ce problème de plus en plus souvent utilisée consiste à changer de clé régulièrement de telle sorte que l'attaquant n'ait jamais assez de données disponibles pour casser la clé [31].

Dans la réalité, il est plus facile de pirater une clé que d'effectuer son déchiffrement. Une parade pour contrer les pirates réside dans ce cas dans un contrôle d'accès sophistiqué des bases de données de clés.

IV-2-4/ Les pare-feu

Un pare-feu est un équipement de réseau, la plupart du temps de type routeur, placé à l'entrée d'une entreprise afin d'empêcher l'entrée ou la sortie de paquets non autorisés par l'entreprise [33]. La situation géographique d'un pare-feu est illustrée à la figure IV-4

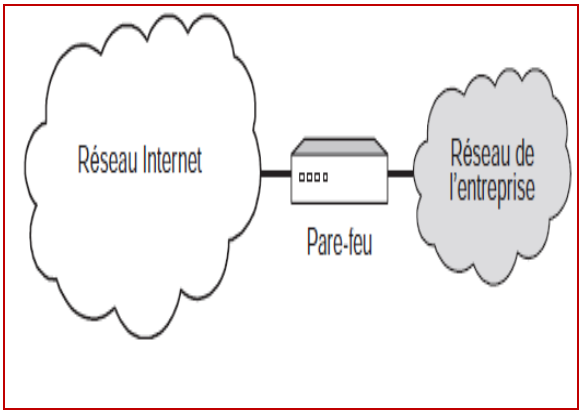


Figure IV-4 : Situation d'un pare-feu dans l'entreprise [33]

Toute la question est de savoir comment reconnaître les paquets à accepter et à refuser, il est possible de travailler de deux façons [33] :

- 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 [33]. 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 [33].

IV-2-5 / <u>Les filtres</u> :

Comme expliqué précédemment, les filtres sont essentiellement appliqués sur les numéros de port. La gestion de ces numéros de port n'est toutefois pas simple. En effet, de plus en plus de ports sont dynamiques. Avec ces ports, l'émetteur envoie une demande sur le port standard, mais le récepteur choisit un nouveau port disponible pour effectuer la communication. Par exemple, l'application RPC (Remote Procedure Call) affecte dynamiquement les numéros de port. La plupart des applications P2P (Peer-to-Peer) ou de signalisation de la téléphonie sont également dynamiques [31].
L'affectation dynamique de port peut être contrôlée par un pare-feu qui se comporte astucieusement. La communication peut ainsi être suivie à la trace, et il est possible de découvrir la nouvelle valeur du port lors du retour de la demande de transmission d'un message TCP. À l'arrivée de la réponse indiquant le nouveau port, il faut détecter le numéro du port qui remplace le port standard. Un cas beaucoup plus complexe est possible, dans lequel l'émetteur et le récepteur se mettent directement d'accord sur un numéro de port. Dans ce cas, le pare-feu ne peut détecter la communication, sauf si

tous les ports sont bloqués. C'est la raison essentielle pour laquelle les pare-feu n'acceptent que des communications déterminées à l'avance [31].

Cette solution de filtrage et de reconnaissance des ports dynamiques n'est toutefois pas suffisante, car il est toujours possible pour un pirate de transporter ses propres données à l'intérieur d'une application standard sur un port ouvert. Par exemple, un tunnel peut être réalisé sur le port 80, qui gère le protocole HTTP. À l'intérieur de l'application HTTP, un flot de paquets d'une autre application peut passer. Le pare-feu voit entrer une application HTTP, qui, en réalité, délivre des paquets d'une autre application, une entreprise ne peut pas bloquer tous les ports, sans quoi ses applications ne pourraient plus se dérouler. On peut bien sûr essayer d'ajouter d'autres facteurs de détection, comme l'appartenance à des groupes d'adresses IP connues, c'est-à-dire à des ensembles d'adresses IP qui ont été définies à l'avance. De nouveau, l'emprunt d'une adresse connue est assez facile à mettre en œuvre.

De plus, les attaques les plus dangereuses s'effectuent par des ports qu'il est impossible de bloquer, comme le port DNS. Une des attaques les plus dangereuses s'effectue par un tunnel sur le port DNS [31]. Encore faut-il que la machine réseau de l'entreprise qui gère le DNS ait des faiblesses pour que le tunnel puisse se terminer et que l'application pirate s'exprime dans l'entreprise. Pour sécuriser l'accès à un réseau d'entreprise, une solution beaucoup plus puissante consiste à filtrer non plus aux niveaux 3 ou 4 (adresse IP ou adresse de port) mais au niveau applicatif. Cela s'appelle un filtre applicatif. L'idée est de reconnaître directement sur le flot de paquets l'identité de l'application plutôt que de se fier à des numéros de port.

Cette solution permet d'identifier une application insérée dans une autre et de reconnaître les applications sur des ports non conformes. La difficulté avec ce type de filtre réside dans la mise à jour des filtres chaque fois qu'une nouvelle application apparaît. Le pare-feu muni d'un tel filtre applicatif peut toutefois interdire toute application non reconnue, ce qui permet de rester à un niveau de sécurité élevé [31].

IV-2-6/ La sécurité autour du pare-feu

Comme nous l'avons vu, le pare-feu vise à filtrer les flots de paquets sans empêcher le passage des flots utiles à l'entreprise, flots que peut essayer d'utiliser un pirate. La structure de l'entreprise peut être conçue de différentes façons. Deux solutions générales sont mises en œuvre [32].

La première est illustrée à la figure IV-5, dans ce cas la communication, après avoir traversé le pare-feu, se dirige au travers du réseau d'entreprise vers le poste de travail de l'utilisateur. Alors, il faut que les postes de travail de l'utilisateur soient des machines sécurisées afin d'empêcher les flots pirates qui auraient réussi à passer le pare-feu d'entrer dans des failles du système de la station.

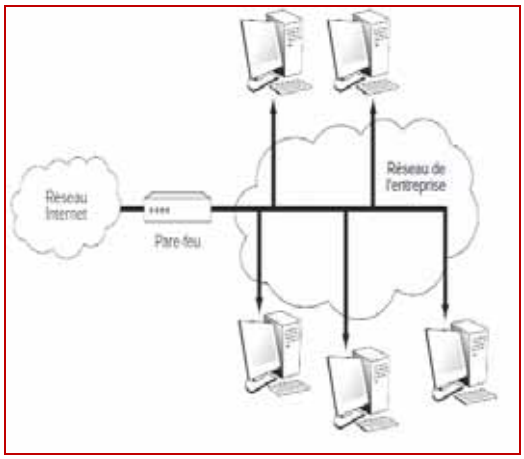


Figure IV-5 : Place d'un pare-feu dans l'infrastructure réseau [32]

La seconde est représentée à la figure IV-6, puisque la première solution est très difficile à sécuriser, car elle dépend de l'ensemble des utilisateurs d'une entreprise, la plupart des architectes réseau préfèrent mettre en entrée de réseau une machine sécurisée, que l'on appelle machine bastion.

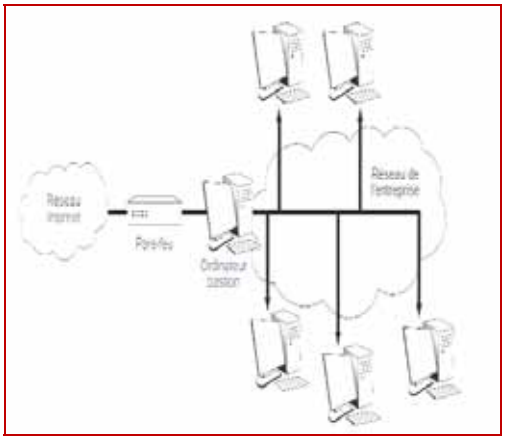


Figure IV-6 : Pare-feu associé à une machine bastion [32]

La machine bastion apporte quelques difficultés supplémentaires de gestion. En effet, elle prend en charge l'ouverture et la fermeture des communications d'un

utilisateur avec l'extérieur. Par exemple, un client avec son navigateur ne peut plus accéder à un serveur externe puisque la machine bastion l'arrête automatiquement. Le bastion doit être équipé d'un serveur proxy, et chaque navigateur être configuré pour utiliser le proxy. La communication se fait donc en deux temps. L'utilisateur communique avec son proxy, et celui-ci ouvre une communication avec le serveur distant. Lorsqu'une page parvient au proxy, ce dernier peut la distribuer au client. Le bastion peut d'ailleurs servir de cache pour les pages standards utilisées par une entreprise [33].

Le défaut de cette dernière architecture provient de sa relative lourdeur, puisqu'il est demandé à une machine spécifique d'effectuer le travail réseau pour toutes les machines de l'entreprise. De plus, la sécurité de toute l'entreprise peut être menacée si l'ordinateur bastion n'est pas parfaitement sécurisé, car un pirate externe peut avoir accès à l'ensemble des ressources de l'entreprise. De fait, l'architecture de sécurité peut s'avérer plus complexe lorsqu'un ordinateur bastion est mis en place. [33]

IV-3/ La sécurité dans un environnement SCADA :

La sécurité dans les réseaux SCADA est presque la même dans les réseaux OSI ou TCP/IP seulement, les réseaux SCADA doivent prendre en considération les contraintes additionnelles suivantes [26] :

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

On va commencer d'abord à introduire les attaques et les menaces qui ciblent un système SCADA puis on verra les mesures à prendre.

IV-3-1/ Vulnérabilités et attaques :

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 sous les attaques conventionnelles du monde informatique, les risques majeurs pour un système SCADA sont [26] :

1. Emploi de matériels et logiciels standards qui présentent des vulnérabilités connues
2. Retard d'exécution suite à l'implémentation de la sécurité

IV-3-1-1/ Les menaces:

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 [24]:

1. Les virus
2. Les chevaux de Troie
3. L'erreur humaine
4. Les accidents
5. Toute interruption des services publics
6. Le bruit sur les lignes électriques
7. L'interdépendance avec d'autres réseaux

IV-3-1-2/ Chemins d'attaques :

Pour qu'une menace soit réalisée, il doit avoir un moyen d'accéder au système SCADA, et comme ce dernier est lié à l'Internet, ou aux réseaux d'entreprise, il existe une variété de chemins pour y accéder, certains chemins typiques d'attaque SCADA sont cités ici [35]:

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

IV-3-1-3/ Cibles préférées:

Généralement si un attaquant arrive à pénétrer à un système SCADA, son but sera l'accès au contrôle du système afin de faire des modifications nuisibles. Quelques actions possibles lors d'une attaque sont les suivantes [35] :

1. Contrôle du MTU
2. Obtention du mot de passe
3. Arrêt des unités
4. Modification des programmes des RTU
5. Neutralisation de la communication entre MTU et les différents RTU

IV-3-2/ <u>Cyber-sécurité des systèmes SCADA</u>:

La cyber-sécurité des systèmes SCADA est assurée par un processus qui consiste en 21 étapes (figure IV-7) [26] :

1. identifier toutes les connexions au réseau SCADA
2. déconnecter les connexions non nécessaires
3. évaluer et renforcer la sécurité des connexions restantes
4. renforcer les systèmes SCADA en enlevant ou en neutralisant les services non nécessaires
5. ne pas compter uniquement sur les protocoles internes pour protéger les systèmes SCADA
6. mettre en place les dispositifs de sécurité fournis par des services externes
7. établir des contrôles forts des éléments des systèmes SCADA pouvant servir de porte d'entrée
8. implémenter des systèmes de détection d'intrusion internes et externes et surveiller 24 heures sur 24 les incidents
9. effectuer des audits techniques du système SCADA et des réseaux reliés pour identifier les problèmes de sécurité
10. effectuer des enquêtes de la sécurité physique du système SCADA et des réseaux connectés
11. établir des équipes (SCADA Red Teams) pour identifier et évaluer des scénarios possibles d'attaques
12. définir clairement les rôles et les responsabilités des gestionnaires, administrateurs système et utilisateurs du système SCADA
13. documenter l'architecture réseau et identifier les systèmes servant aux fonctions critiques ou contenant de l'information sensible requérant des niveaux supplémentaires de protection
14. établir un processus rigoureux de gestion des risques

15. établir une stratégie de protection du réseau basée sur le principe de défense en profondeur
16. identifier clairement les besoins en cyber-sécurité ;
17. établir des processus de gestion effective de la configuration du système SCADA
18. effectuer des évaluations régulières du système SCADA
19. effectuer des copies de sauvegarde et développer des plans de rétablissement du système SCADA
20. établir des attentes précises pour les performances de cyber-sécurité et s'assurer que le personnel soit responsabilisé face à l'atteinte de ces niveaux
21. développer des politiques et effectuer des entraînements pour minimiser la possibilité que le personnel dévoile par inadvertance de l'information sensible en ce qui a trait à la conception, les opérations et les mesures de sécurité du système SCADA

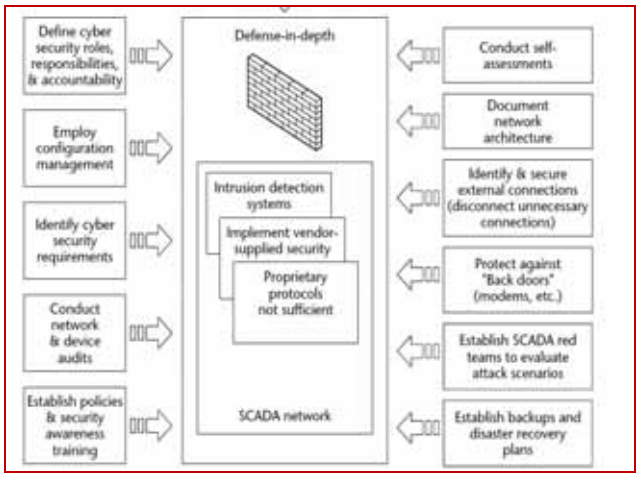


Figure IV-7: Cyber-sécurité du SCADA [26]

IV-4/ Conclusion:

La sécurité dans Internet est un besoin impératif vu la vulnérabilité de ce dernier, elle a comme fonction principale la mise en œuvre de cinq types d'opération :

- Identification d'un utilisateur.
- Authentification d'un utilisateur.
- Intégrité des données.
- Confidentialité des données.
- Non-répudiation.

Dans ce chapitre nous avons vu les outils à prévoir pour assurer ces opérations et dans un environnement Internet et dans un environnement SCADA.

Les systèmes SCADA peuvent être efficacement protégés contre les attaques et les intrusions, si les méthodes classiques de sécurité de systèmes d'informations sont modifiées et adaptées.

Il est vrai que les efforts fournis pour sécuriser les environnements Internet et SCADA sont énormes mais sans qu'ils soient invulnérables.

CHAPITRE (V)

ETUDE EXPERIMENTALE

V-1/ Introduction :

Avant d'aborder le sujet de télégestion, il est à rappeler que de nos jours l'automatique a connu une grande évolution, il s'agit surtout de l'informatique industrielle utilisant les systèmes de communication numériques. Afin de pouvoir expliquer cette évolution nous avons la fameuse pyramide CIM (Computer Integrated Manufacturing).

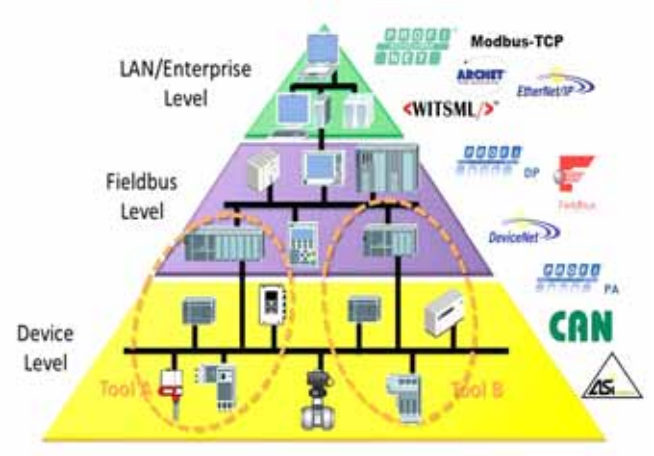


Figure V-1 : Pyramide CIM [36]

Il s'agit d'un concept décrivant l'automatisation complète des processus de fabrication. Ainsi, tous les équipements de l'usine fonctionnent sous le contrôle permanent des ordinateurs, des automates programmables et autres systèmes numériques. La pyramide CIM est donc une représentation hiérarchique logique organisée en plusieurs niveaux dont un niveau supérieur décide ce qu'un niveau inférieur exécute. A titre d'exemples les actions relatives à chaque niveau peuvent être définit comme suit :

- Niveau 3 : niveau entreprise utilisant les réseaux de communications tel que les LAN et peuvent être interconnectés avec le monde extérieur à travers les réseaux MAN et/ou WAN.
- Niveau 2 : les automates programmables utilisant les réseaux de terrain comme moyens de communication.

- Niveau 1 : l'instrumentation de terrain comme les capteurs et les actionneurs.

De nos jours les niveaux 1 et 2 sont relativement maitrisés surtout au niveau professionnel. L'intérêt est de plus en plus focalisé sur les couches supérieures utilisant essentiellement les outils informatiques et les systèmes de communication comme les réseaux informatiques et l'internet. Or, ces systèmes de communications posent beaucoup de problèmes liés essentiellement à la sécurité et la qualité de service (QoS : Quality of Service).

Dans notre travail nous nous sommes intéressés à l'étude et la conception d'un système de télégestion des stations d'épurations des eaux usées. Ces stations, comme tant d'autres installations industrielles, sont souvent réparties sur de vastes zones géographiques. Nous avons donc mis en œuvre une HMI pour cette application. Ensuite nous avons étudié ses performances en termes de qualité de service en utilisant des logiciels en open source. Comme une HMI est le plus souvent associée à des automates programmables industriels nous avons utilisés des programmes déjà fonctionnels. En effet, les programmes d'automatisation (programmes exécutés par les automates programmables industriels) que nous avons utilisés sont des réalisations professionnelles fonctionnant réellement sur certaines stations d'épurations des eaux usées. Ces programmes sont écrits en step7 qui est un logiciel de programmation des automates programmables industriels de Siemens S7-300 et S7-400.

V-2/ Description de la télégestion

La télégestion permet de gérer à distance des installations industrielles géographiquement réparties. Elle assemble les équipements matériels et logiciels nécessaires au fonctionnement de cette dernière. La télégestion est composée essentiellement de postes clients (locaux et distants) et de postes serveurs. [36] (figure V-2)

Ses éléments sont :

- Postes centraux : Supervision générale du réseau.
- Postes locaux : Installés sur les ouvrages techniques.
- Réseaux de communications industrielles et publiques.
- Eléments physiques de communication (conducteurs électriques, sans fils, fibre optique …etc)
- Appareillage d'interconnexion (commutateurs, concentrateurs, routeurs, …etc)

La télégestion se concrétise par:

- L'électronique: Pour récolter les informations.
- L'informatique: Pour le traitement des informations.
- Les télécommunications: Pour émettre les informations.

La télégestion garantit le bon fonctionnement des installations industrielles géographiquement réparties, notamment :

- La Sécurité.
- La Surveillance permanente.
- Le Contrôle et commande à distance.
- …etc

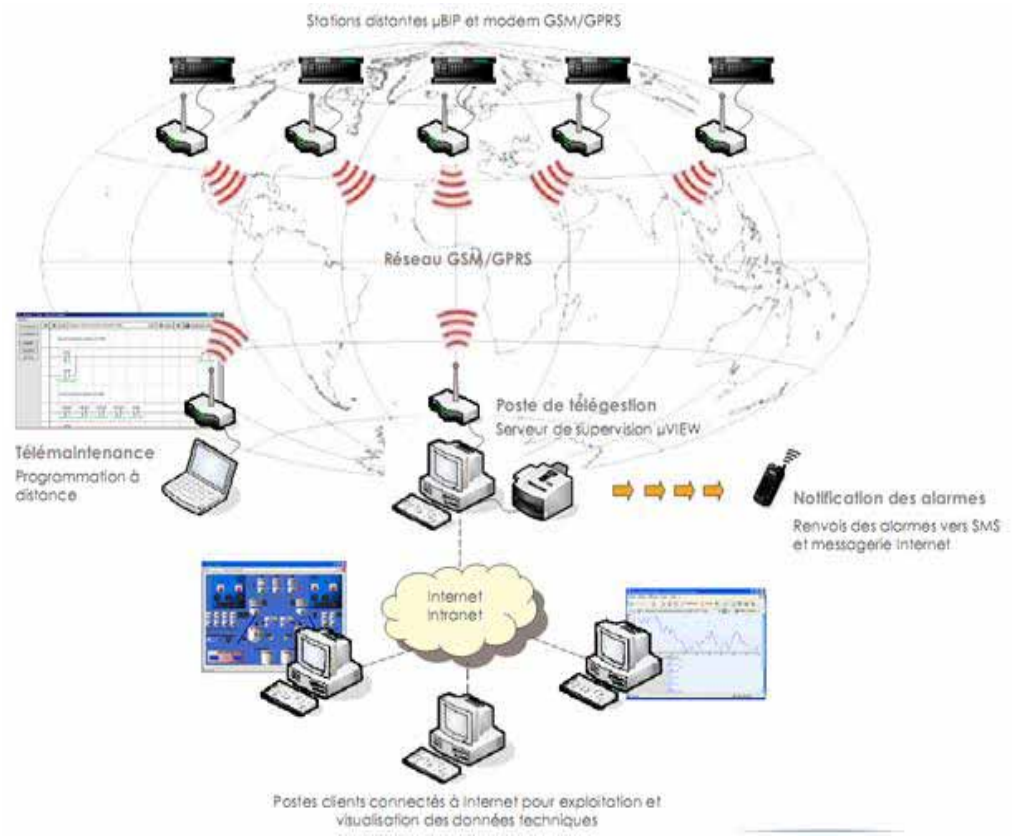


Figure V-2 : Equipements de télégestion [36]

Dans ce thème nous analysons la possibilité et les apports techniques d'une télégestion de stations d'épurations des eaux usées à boue activée. Ce choix est motivé par deux facteurs majeurs :

- La protection de l'environnement de la pollution qui est devenue ces dernières années un sujet critique, car cette pollution contamine le milieu naturel.
- La nécessité de surveiller ces stations d'épuration en installant un système de contrôle fiable permettant la supervision des sites géographiquement répartis.

V-3/ Station d'épuration des Eaux Usées :

Une vue d'ensemble d'une station d'épuration des eaux usées à boue activée peut être décrite par la figure V- 3 :

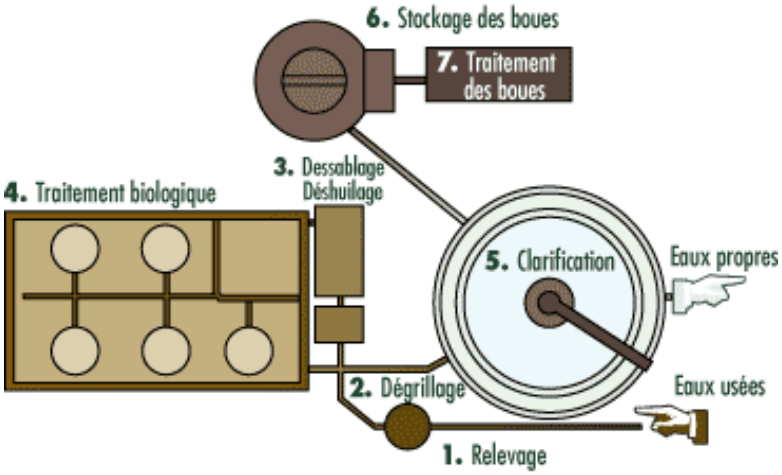


Figure V-3 : Vue d'ensemble d'une station d'épuration

Les eaux usées brutes passent par une vanne qui adapte automatiquement le débit d'entrée à la capacité hydraulique de la station. Les eaux en excès sont déversées directement dans les milieux naturels. Dans ce procédé d'épuration des eaux, nous définissons trois phases essentielles illustrées sur la figure ci-dessous :

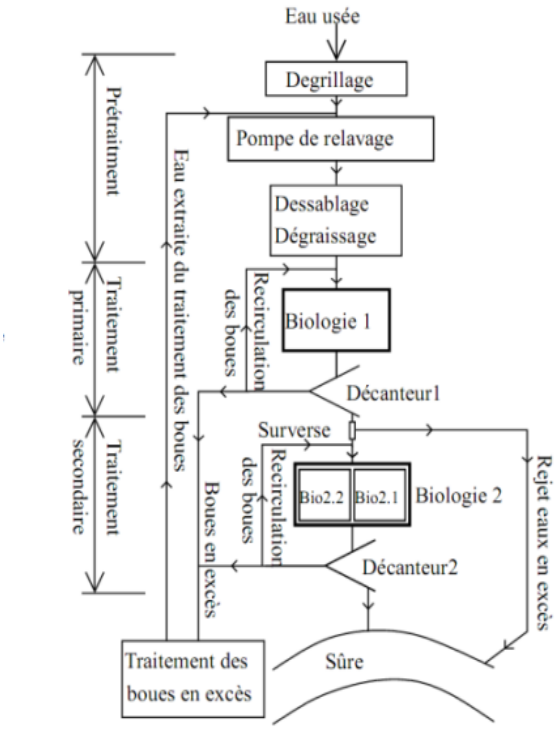


Figure V-4 : Structure d'une station d'épuration

Chacune de ces trois phases est composée de plusieurs parties d'instrumentations automatisées. L'automatisation d'une station d'épuration des eaux usées à boue activée est le plus souvent assurée par des API (Automates Programmables Industriels ou PLC). L'API assure, sous sa forme basique, les trois taches fondamentales à savoir :

- Acquisitions et mesures : il s'agit des entrées ou capteurs de l'API. Généralement des entrées tout ou rien ou TOR (DI : Digital Input) et des entrées analogiques (AI : Analog Input).
- Traitement numérique : souvent ce sont des procédures de régulation et de contrôle numériques
- Prise de décision : ce sont les différentes actions que l'API aura à effectuer à partir de ses sorties TOR (DO : Digital Output) et analogiques (AO : Analog Output).

Dans le cas d'une station d'épuration des eaux usées de taille moyenne le nombre des entrées/sorties, est relativement élevé (plusieurs centaines). L'instrumentation utilisée dans les stations d'épuration est très diversifiée. Cependant, nous trouvons habituellement rencontrés comme instrumentation au niveau des stations d'épurations des eaux usées:

- Des variateurs de vitesse pour moteurs et pompes Des capteurs de niveau par exemple à ultrasons
- Des débits mètres
- Des capteurs de vitesse pour moteur
- Des capteurs de taux d'oxygène
- Des vannes motorisées et des électrovannes
- Autres actionneurs et préactionneurs
- Autres capteurs TOR (Tout Ou Rien) comme des les boutons poussoirs
- …etc

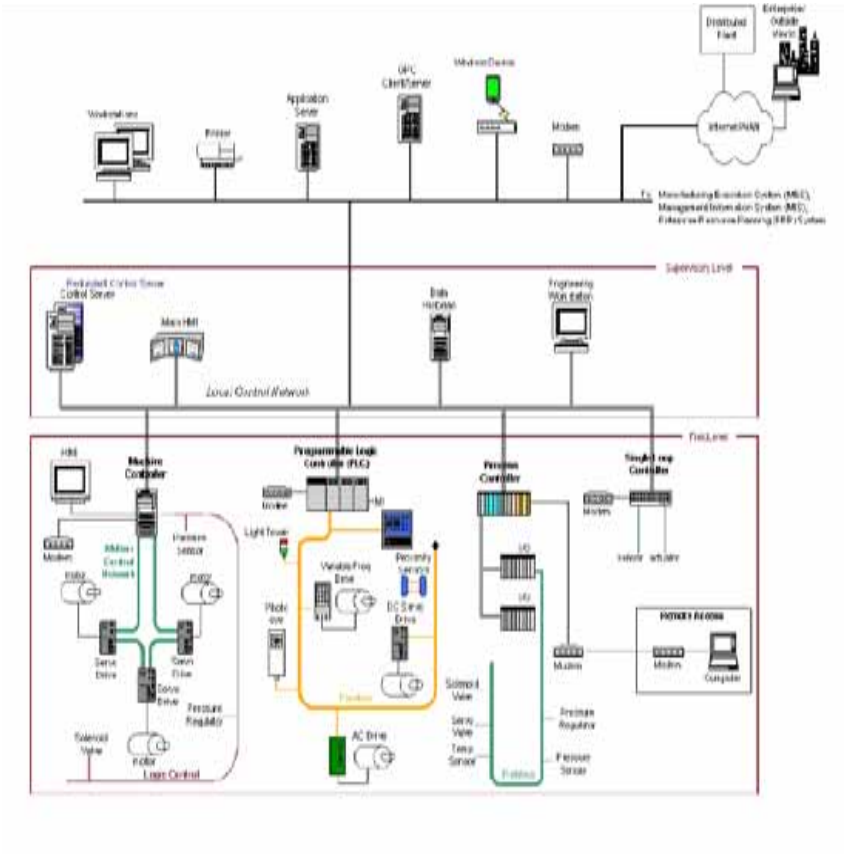


Figure V-5 : Architecture de système de contrôle de la station d'épuration

V-4/ Implémentation de la Télégestion:

Avant d'entamer l'étude de la télégestion, tout d'abord il faut implémenter la HMI en utilisant, par exemple, le progiciel WinCC [36]. Nous pouvons également faire appel à ses extensions notamment des systèmes ''Client/serveur'', avec toutes les fonctions SCADA Incluses. WinCC est un système software modulaire permettant de développer à la fois des HMI et de garantir des applications multiutilisateurs. Le progiciel WinCC, sous sa forme basique, fournit tous les composants et fonctions permettant de produire les vues, aussi complexes qu'elles soient, des installations industrielles à superviser.

Les options SIMATIC WinCC sont conçues de manières à permettre aux postes clients l'accès via Internet vers des postes. Parmi ces options nous pouvons citer :

- WinCC / Server : Pour la mise en place d'un système client / serveur.
- WinCC / Web Navigator : Pour la visualisation et la télégestion des installations industrielles à partir du Web.

- WinCC / Messenger : Pour l'envoi automatique des messages, sous forme de textes, vocaux et/ou graphiques directement à partir de WinCC vers les utilisateurs.
- WinCC / Data monitor : Pour le transfert de données procès via internet/intranet.
- WinCC / Guardian : Pour le contrôle de l'installation industrielle en utilisant des images en direct

  … etc.

L'option WinCC / Web Navigator permet la visualisation instantanée de l'installation industrielle, sous forme de vues, au niveau des postes utilisateurs distants via l'Internet, il suffit juste d'avoir une adresse IP statique au niveau du poste serveur.

La solution adoptée dans notre cas pour cette réalisation est basée sur un service très connue à savoir DynDNS. Ce service permet de faire la liaison entre un nom de domaine et son adresse IP alors que cette dernière est dynamique. En effet Il est possible de mettre en place un serveur (FTP, HTTP) sans la disposition d'adresse IP fixe. L'idée est de créer un hôte auprès des services gratuits en l'occurence www.dlinkddns.com (Figure V-6). A l'aide de ce procédé nous avons pu héberger notre HMI dans un serveur d'application http alors que notre connexion internet possède une adresse IP publique, fournie par le FAI (Fournisseur d'Accès Internet), dynamique. Cette opération est effectuée à partir d'un abonnement particulier dans un service internet et aussi par la redirection des ports de notre modem/routeur.

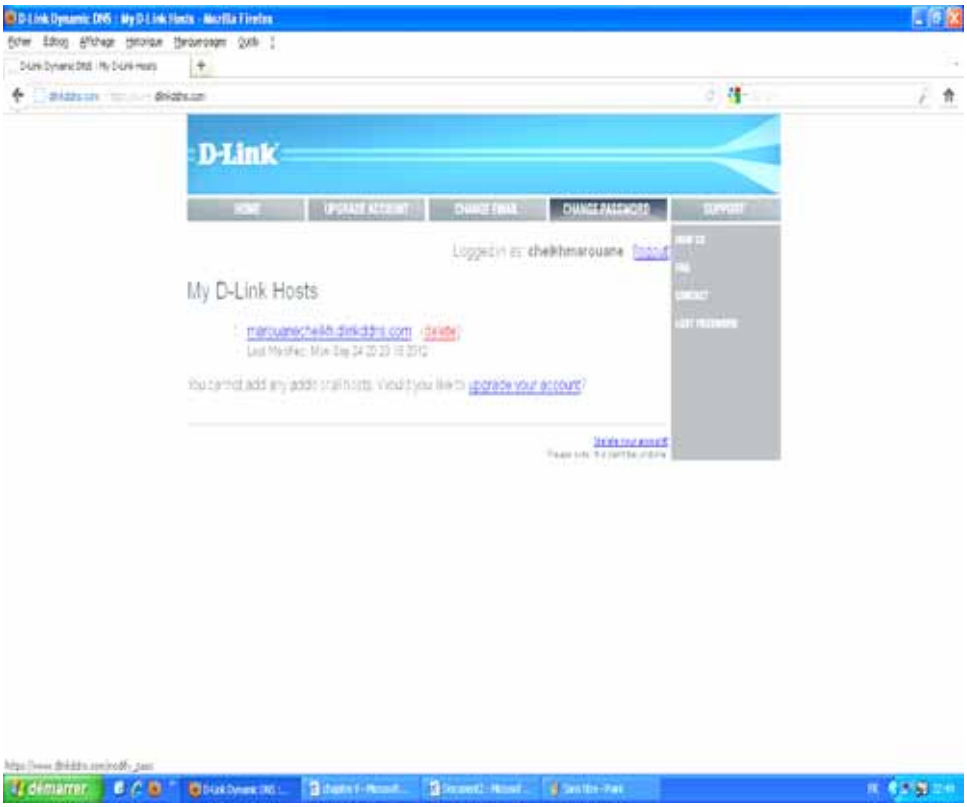


Figure V-6 : Création d'hôte

La redirection des ports (Port Forwarding) de notre routeur (dans notre cas le DSL2640Rde Dlink) est réalisée à partir de son menu interne de configuration :

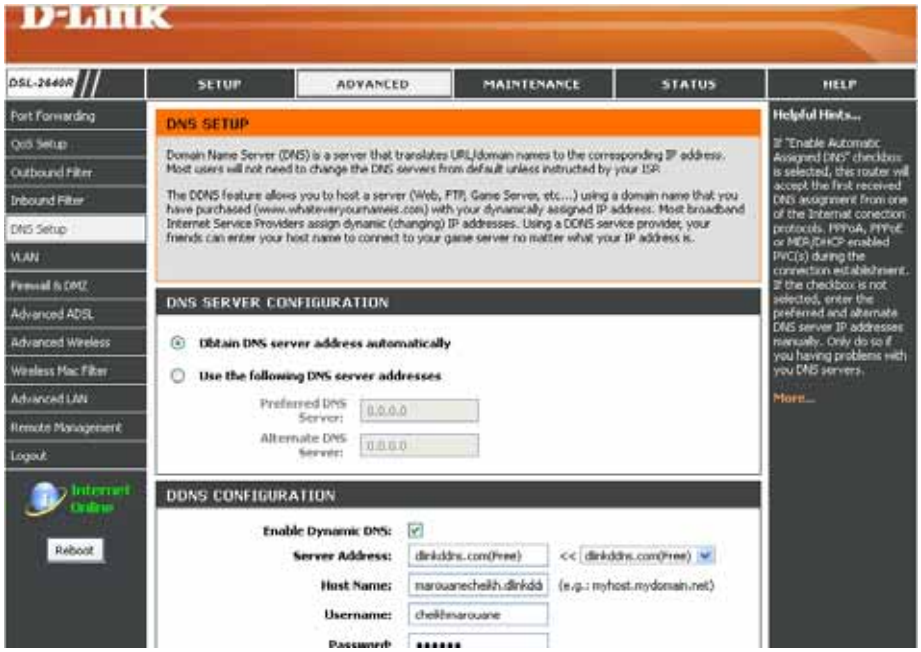


Figure V-7 : Configuration de l'hôte

Après cette étape l'adresse privée du serveur HMI devient accessible à partir du réseau Internet.

Quant à la configuration du projet HMI pour le rendre accessible à partir du réseau Internet nous avons des étapes à effectuer au niveau du WinCC :

On lance le projet WinCC et on choisit l'option Web Navigator puis Web configurator pour attribuer l'adresse IP et le numéro de port utilisé, également il faut choisir MainControl.asp comme site web standard. (Figure V-8)

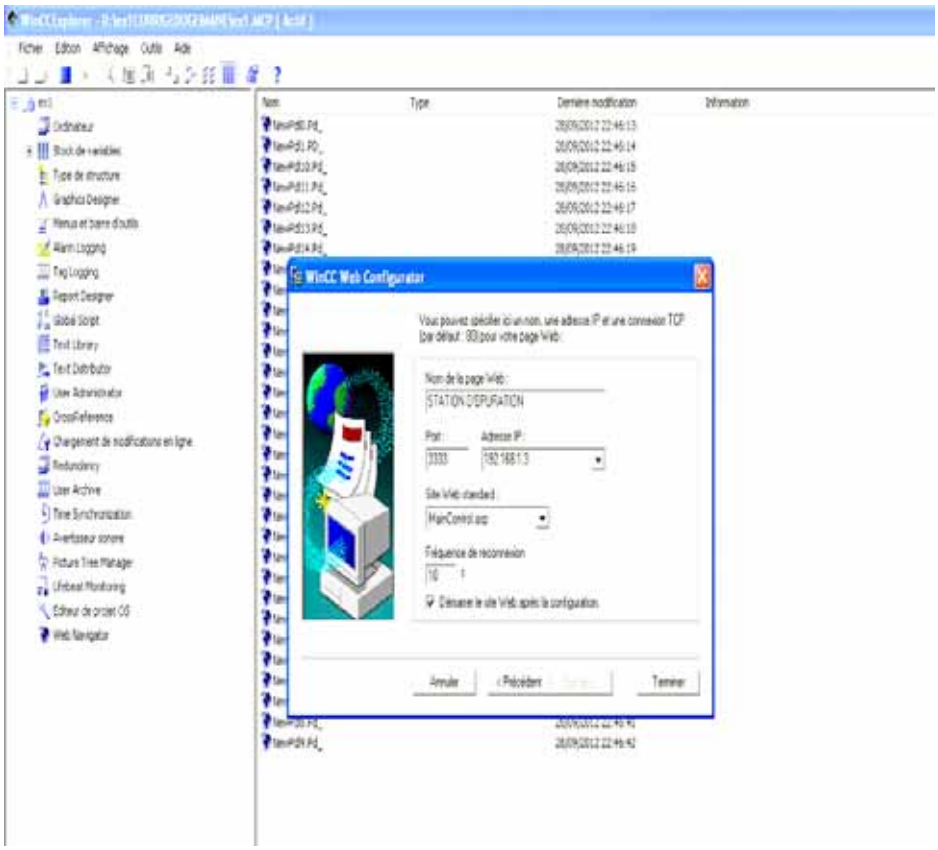


Figure V-8 : Paramétrage d'adresse IP et numéro de port

On procède à la publication des vues qui constituent le projet en utilisant l'option Web View Publisher, ensuite on crée un compte pour l'application afin de la sécuriser en matière d'accessibilité en faisant appelle à l'option User Administrator.

L'étape finale est celle de modifier les options Internet en adaptant l'option Sécurité au besoin de l'application (activation des options de Contrôle Active X).

Finalement le projet est prêt à être exploité à distance via le réseau Internet, il suffit de lancer l'installation systématique de WinCC Web Navigator Client au niveau du poste client et on obtient la vue d'accueil qui s'affiche sur l'écran.

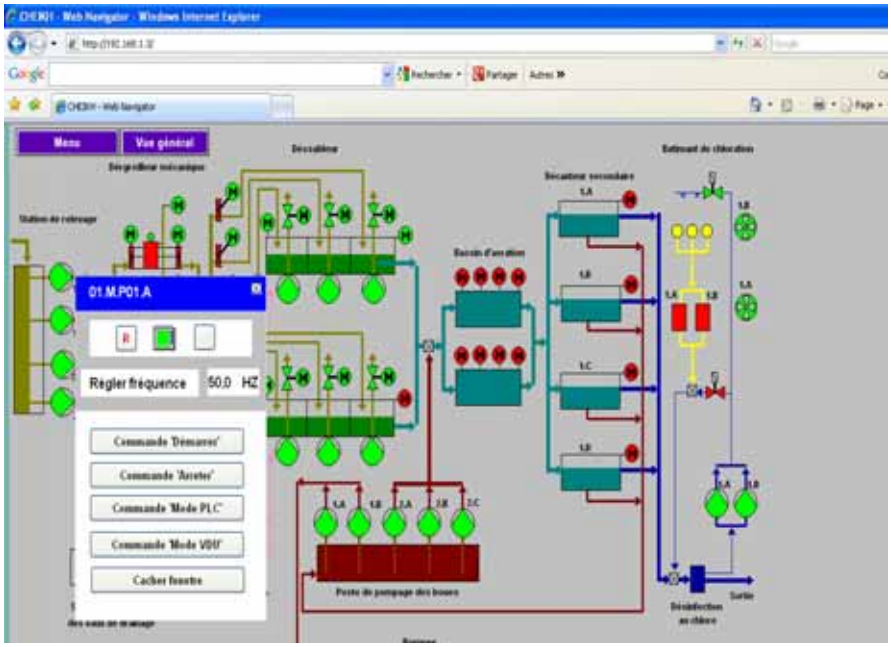


Figure V-9 : Page d'accueil du projet WinCC

V-5/ Mise en œuvre des vues du système de télégestion:

Il s'agit de créer des vues, au niveau de la HMI, représentant l'installation industrielle de point de vue instrumentation et procès. Cette HMI contient entre autres :

- des formes, des courbes,
- des champs de saisies,
- des tableaux,
- des alarmes,
- des archives,
- des symboles
- …etc

Tout ceci est alors dynamisé en les associant aux différentes variables des API (entrées, sorties, variables internes …etc). Dans notre cas nous avons eu à réaliser plusieurs dizaines de vues. Ces vues ont utilisé plusieurs centaines de variables (entrées, sorties, variables internes …etc) se trouvant dans le programme de l'automatisation de cette station d'épuration des eaux usées. Parmi les vues que nous avons développées nous allons essayer de présenter les plus pertinentes :

A. Vue générale

La vue principale (Figure 10) est un schéma fonctionnel général représentant les différentes unités de la station (dégrilleur, soufflerie, les bassins d'aération, poste de pompage, décanteur, bâtiment de chloration ….etc). Ainsi, chaque unité permet de visualiser en temps réel les mesures et les actions analogiques des équipements les plus pertinents :

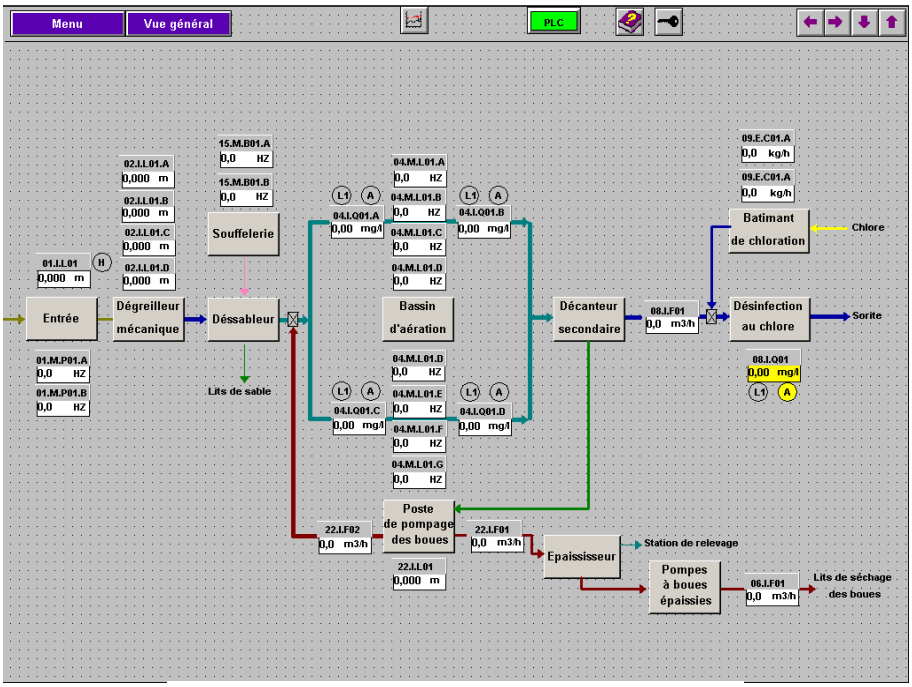


Figure V-10 : Schéma fonctionnel général

Parmi les paramètres visualisés dans cette vue :

- Les fréquences des variateurs de vitesse des moteurs pompes.
- Les mesures des capteurs de niveau à ultrason.
- un débitmètre au niveau de la sortie de pompes à boues épaississies,
- …etc

A partir de cette vue principale nous pouvons appeler les autres vues, représentant les différentes unités de la station.

B. Vue d'ensemble

Cette vue représente une vue d'ensemble numérique des unités de toute la station (Figure 11).

Les états de différents équipements sont visualisés en temps réel. A titre d'exemple et pour chacune des unités de la station nous avons :

- Unité de relevage : Quatres pompes, possédant chacune quatre états (marche, arrêt, défaut et absence d'informations) représentés respectivement par quatres couleurs, le rouge, le vert, le jaune et le gris.
- Dégrilleur mécanique : Huit vannes batardeaux motorisées et un moteur entraînant le racleur, possédant chacun quatre états (marche, arrêt, défaut et absence d'informations) représentés respectivement par quatres couleurs, le rouge, le vert, le jaune et gris.
- Déssableur : Deux bassins rectangulaires, chacun équipé de trois vannes à opercules motorisées et trois pompes et deux moteurs pour enraîner les ponts roulants. Leurs états aussi sont associés à quatre couleurs selon le même principe.
- Souffelerie : Mesures des fréquences délivrées par les capteurs de vitesse pour les deux moteurs des pompes. Même principe pour la visualisation des états.
- Bassins d'aération : Huit moteurs d'aération, quatres sondes de mesure d'oxygène dissous. Même principe pour la visualisation des états.
- Poste de pompage des boues : Cinq pompes avec le même principe de visualisation des différents états.
- Décanteur secondaire : Quatre bassins équipés chacun d'un moteur entraînant un pont roulant.
- Unité de chloration : Deux pompes pouvant être activées. Elles deviennent en rouge lorsqu'une faible concentration du chlore gazeux est détecée. Trois fûts de chlore liquifé haute pression, deux vannes électromagnétiques pour le système d'arosage.
- Les différentes flèches présentes dans cette vue représentent le parcours d'écoulement de l'eau à traiter vers les différentes unités de la station .

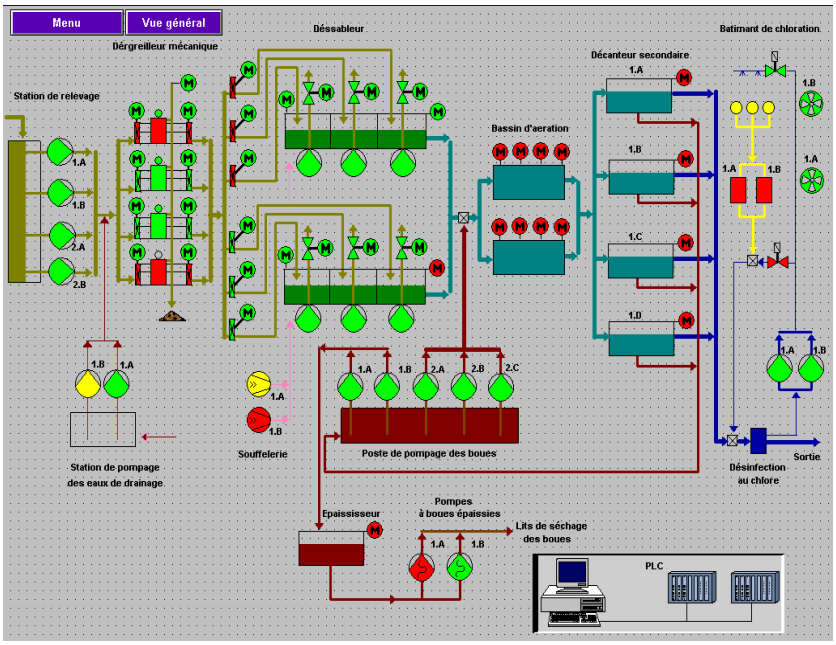


Figure V-11 : Vue d'ensemble

C. Vue de l'unité relevage dégrillage

Cette vue représente l'unité de relevage et dégrillage (Figure 12). Elle permet de visualiser et/ou d'actionner en temps réel les paramètres les plus pertinents:

- Les valeurs des mesures analogiques délivrées par les différents capteurs, comme le capteur de niveau, les deux capteurs de vitesse des deux moteurs pompes et aussi les deux commutateurs de niveau
- Les états des quatre pompes submersibles dans le bassin de relevage.
- Les fréquences des variateurs de vitesse des moteurs peuvent être visualisées et/ou modifiées.

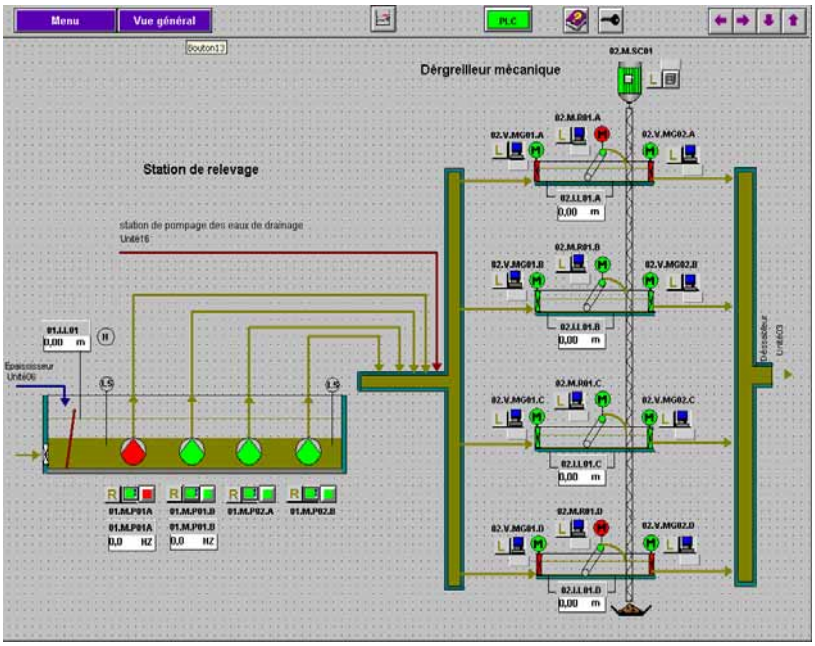


Figure V-12: Station de relevage + Dégrilleur mécanique

D. Vue de l'unité dessablage déshuilage

Cette vue représente l'unité de dessablage/déshuilage (Figure 13):

- Deux bassins à trois chambres , chacun équipé de trois vannes à opercules motorisées et trois pompes submersibles au fond et deux moteurs pour enraîner les ponts roulant. Leurs états aussi sont associés à quatre couleurs.
- Les moteurs des pompes peuvent être mis en marche ou arrêter à partir de cette vue.
- Les vannes peuvent être ouvertes ou fermées toujours à partir de cette vue.
- Le niveau de la soufflerie et les deux mesures des fréquences délivrés par les capteurs de vitesse pour les deux moteurs des pompes sont visualisés dans cette vue.
- Les flèches indiquent le parcours d'écoulement des eaux à traiter vers les différentes unités de la station.

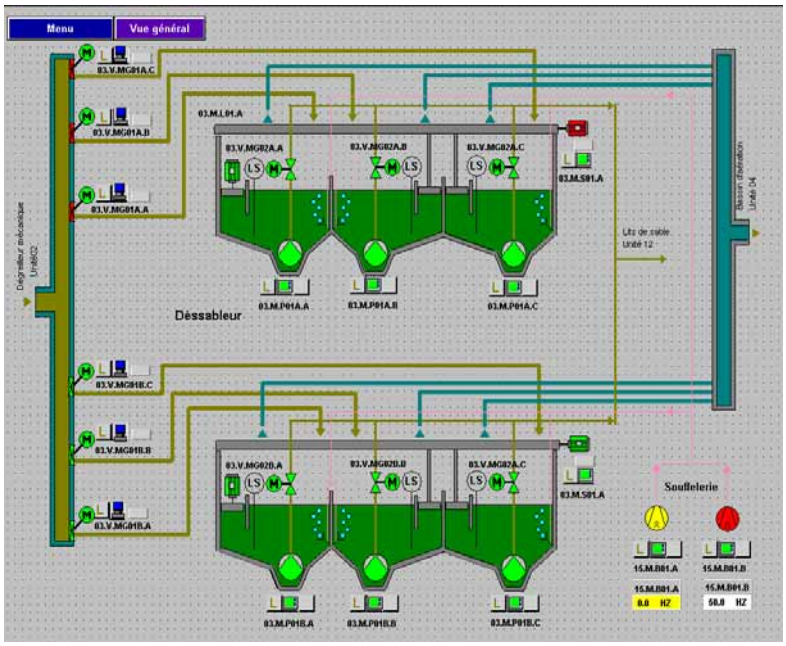


Figure V-13 : Dessableur/Déshuileur

E. Vue de l'unité d'aération et décantation

Cette vue représente l'unité d'aération (Figure 14):

- Deux bassins rectangulaires, chacun équipé de quatre moteurs pour enraîner les ventilateurs. Leurs états sont associés à quatre couleurs.
- Les valeurs analogiques des mesures du taux de l'O_2 dissous dans chaque bassin, ainsi que les valeurs de fréquence pour chaque moteur des aérateurs sont visualisées en temps réel dans cette vue.
- Quatre bassins de décantation, chacun équipé d'un moteur qui entraîne le pont roulant.
- La valeur analogique de débit, mesuré par le débitmètre, est visualisée en permanence dans cette vue**.**
- Tous les moteurs peuvent être démarrés, arrêtés tout en changeant leurs vitesses à partir de cette vue.

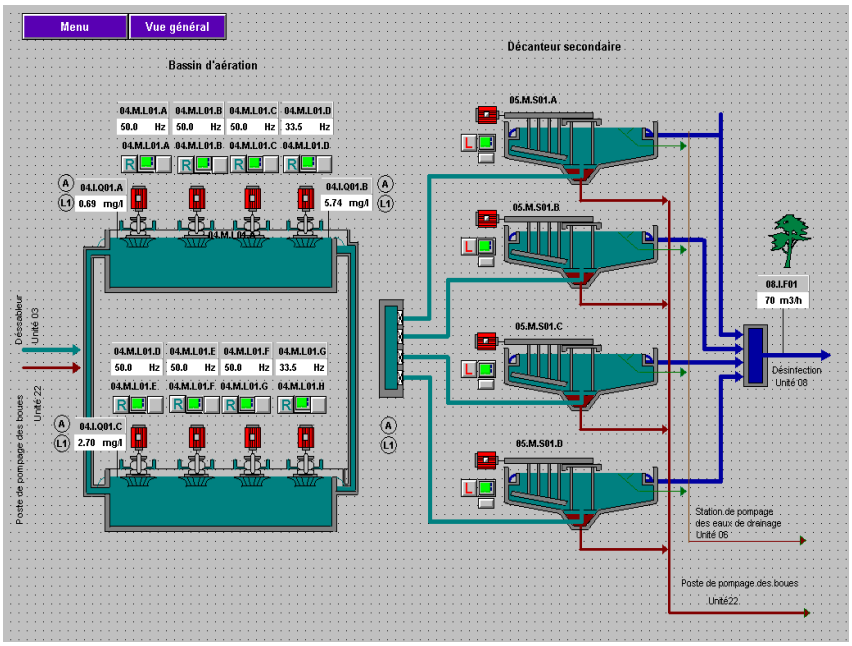


Figure V-14 : Bassins d'aération +Décanteur secondaire.

F. Vue de l'unité des boues

Cette vue représente l'unité de pompage des boues, les eaux de drainage et l'épaississeur (Figure 15):

- Un bassin rectangulaire pour le poste de pompage des boues, équipé de cinq pompes. Les états de ces moteurs sont associés à cinq couleurs.
- Les valeurs analogiques des mesures de niveau, de débit par les capteurs de niveau et les débimètres sont visualisées dans cette vue.
- Les bassins d'épaississage de formes coniques, équipés chaun d'un moteur entraînant la herse, commandable à partir de cette vue.
- Un bassin rectangulaire pour le poste de pompage des eaux de drainage équipé de deux pompes. Leurs moteurs sont à vitesse fixe. Nous pouvons démarrer ces moteurs ou les arrêter à partir de cette vue
- Deux pompes pour le pompage de boues vers les lits de séchage, à vitesses fixes peuvent être commandées à partir de cette vue.

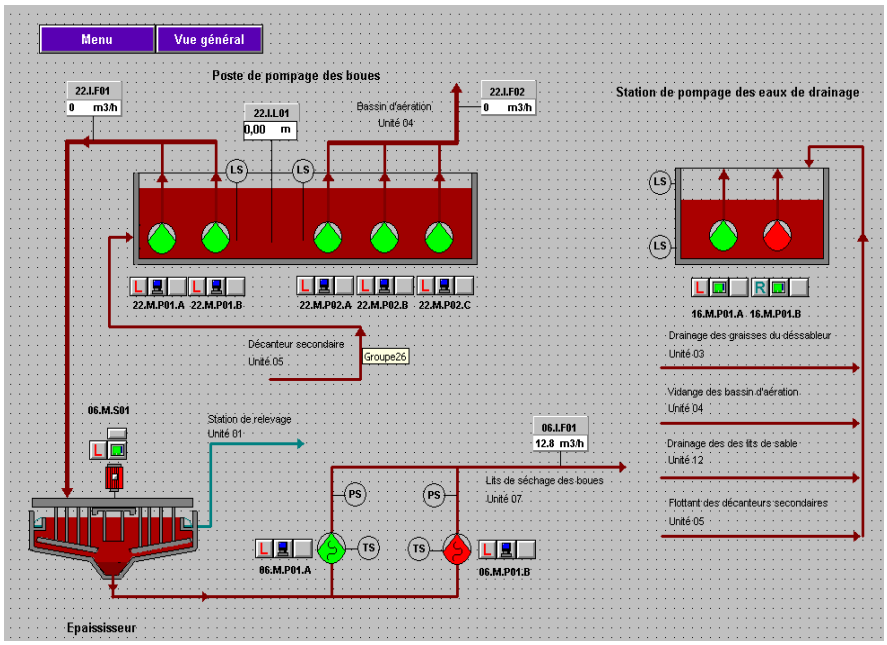


Figure V-15 : Unité de pompage des boues, les aux de drainage et l'épaississeur

G. Vue de l'unité de chloration

Cette vue représente l'unité de désinfection au chlore et le bâtiment de chloration (Figure 16):

- Un bassin de contact où se fait le traitement final des eaux à traiter par la chloration avant d'être rejetées vers le milieu naturel.
- Deux pompes pouvant être activées à partir de cette vue. Elles deviennent en rouge lorsqu'une faible concentration du chlore gazeux est détecté, trois fûts de chlore liquéfié haute pression, deux vannes électromagnétiques pour le système d'arrosage.

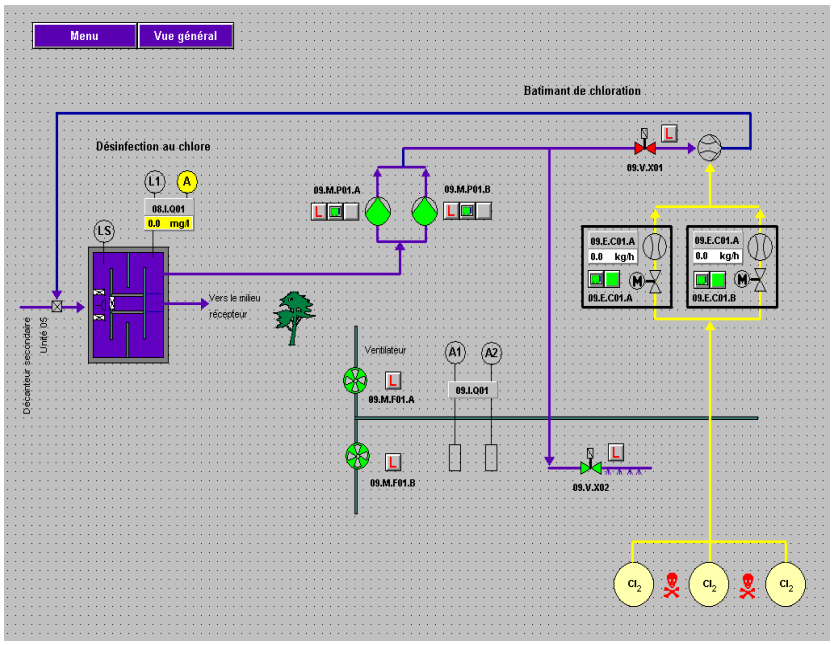


Figure V-16 : Unité de chloration

V-6/ Etude des performances de la Télégestion :

L'objectif de notre thème est d'aborder de manière optimale la question de télégestion d'une implémentation sous réseau Internet, qui est largement utilisé dans plusieurs domaines et applications. Ceci est dû essentiellement à son faible coût et sa flexibilité en matière de configuration.

Comme il est construit à l'aide de différentes architectures de réseaux hétérogènes, l'information, transmise sous forme de paquets IP, au sein du réseau Internet est sujette à plusieurs problèmes et limitations notamment le retard et la perte de certains paquets. Ceci est dû essentiellement à la bande passante utilisée et à d'éventuelles congestions. Pour cette raison on définit ce que l'on appelle habituellement la QoS (Quality of Service) dans les systèmes de communication par IP. Elle désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante. Elle est appliquée aux réseaux à commutation de paquets (réseaux basés sur l'utilisation de routeurs). Les principaux critères permettant d'apprécier la qualité de service sont les suivants :

- **Débit** : Il dépend essentiellement de la bande passante du support.
- **Gigue** (jitter en anglais) : c'est la variation du délai de transmission, et elle influe sur la forme du trafic.

- **Latence**, **délai** ou **temps de réponse** (en anglais delay) : retard entre l'émission et la réception d'un paquet.
- **Perte de paquet** (en anglais packet loss): elle correspond au non réception d'un paquet de données, dû surtout à un encombrement du réseau ou congestion.
- **…etc**

Le retard qui dépend principalement du matériel du réseau, des protocoles utilisés, et de la charge du réseau. La complexité du réseau Internet a rendu la tache de sa modélisation très délicate [37], plusieurs approches ont été adoptées telle que le modèle du poisson, modèles statistiques, modèles basés sur le comportement TCP/IP….etc.

Dans ce travail nous allons étudier les performances de transmission des données de l'application implémentée [38] (ouverture d'une vanne, démarrage d'une pompe, changement de consigne ou des paramètres de régulateur PID…..) en s'intéressant au TCP. TCP/IP est le protocole le plus utilisé sur Internet qui permet de fiabiliser les communications en offrant un contrôle de la transmission des paquets.

V-6-1/Principe de la modélisation analytique différentielle du TCP :

Notre but est de réaliser des mesures réelles du trafic Internet afin d'évaluer la qualité de l'exploitation à distance de l'installation via le réseau Internet (un poste client est sensé gérer la station d'épuration d'eau en temps réel), quoi que la métrologie pour Internet nécessite des moyens considérables et des outils très avancés [39] nous avons adopté une méthodologie de travail basée sur la modélisation analytique différentielle de TCP/IP [40]qui nous permet d'estimer le délai de bout en bout (RTT, paramètre capital pour l'exploitation à distance représentant l'axe de cette étude), et la mesure pratique de RTT moyennant les commandes classiques et très connues à savoir PING et TRACERT[38].

Le principe de la modélisation différentielle est de décrire l'évolution du débit d'une source TCP/IP en fonction du temps pour chaque mode d'opération. En effet TCP/IP assure le contrôle de flux de bout en bout, d'erreur et de congestion, en utilisant trois modes de transmission:

- Slow Start : Dans ce mode TCP/IP découvre la bande passante disponible en augmentant sa fenêtre de congestion CWND exponentiellement (et par

conséquent son crédit d´´emission) jusqu'a qu'une congestion ait lieu (une erreur ou une perte).

- Fast Retransmit : Dans ce mode TCP/IP retransmet les paquets perdus lors de la congestion un par un.
- Congestion Avoidance : Dans ce mode TCP/IP stabilise le taux d´´emission tout en essayant de découvrir plus lentement la bande passante disponible.

Le modèle différentiel fournit une expression analytique différentielle de la valeur de CWND(t) et RTT(t) pour chaque mode d'opération de TCP/IP [40]. Le passage d'une équation différentielle à une autre se fait par des évènements de contrôle qui sont liés à la détection d'une perte lors d'une transmission.

L'établissement de la connexion TCP/IP commence toujours par l'émission d'un paquet de synchronisation SYN et la réception de son acquittement ACK, cela donne à la source le crédit de transmettre deux paquets de données, la réception d'un acquittement incrémente le crédit d'émission et la transmission le décrémente selon l'équation ci-après mentionnée [40]:

$$\text{CREDIT} = \text{ACK} + \min(\text{CWND}, \text{RWND}) - \text{SEQ} + \text{NDUP} * \text{MSS} \quad (1)$$

avec

MSS (Maximum Segment Size): est la taille maximum de paquet de données dans une fenêtre.

SEQ : adresse de paquet suivant à transmettre.

ACK : acquittement, la valeur de dernier ACK correspond à l'adresse prochaine du paquet à transmettre.

CWND : volume maximum de données présent dans un réseau entre un émetteur et récepteur.

RWND : correspond au volume maximum de données que peut être pris en charge par le récepteur.

NDUP : est un compteur d'acquittements identiques reçus par un émetteur.

RTT : délai entre l'émission d'un paquet et son acquittement ACK.

RTO : le délai maximum permis entre l'émission d'un paquet et son acquittement.

CREDIT : nombre de paquet qu'un émetteur peut transmettre.

Comme nous l'avons déjà indiqué TCP/IP fonctionne selon trois modes d'opérations, au départ le mode SLOW START actif, la source commence à émettre un flot de paquets qui dépend des acquittements reçus. La fenêtre de congestion

CWND est initialisée à 1, après la transmission du premier segment et la réception de son acquittement CWND est incrémentée de 1 et deux segment peuvent être transmis, une fois transmis et leurs acquittements sont reçus CWND est incrémentée de 2 et 4 segments peuvent être transmis et ainsi de suite, CWND évolue selon une forme exponentielle, en pratique le récepteur met du temps pour acquitter les donnés reçues et en général ce délai appelé b est de l'ordre de 2 (le récepteur émet un ACK pour chaque deux segments), de ce fait la progression de CWND suit approximativement une suite géométrique de raison b+1/b.

Le mode CONGESTION AVOIDANCE est implémenté pour assurer des transmissions sans qu'il y ait une perte de données, en mode congestion un TIME OUT ou un triple ACK dupliqué sont signalés, si la congestion est due à un triple ACK dupliqué CWND/2 est enregistré comme SSTHRESH (SSTHRESH : Slow Start THRESHold size), par contre si TIME OUT est à l'origine de la congestion CWND est mise à 1, et son incrémentation est de (b+1 /CWND) pour chaque ACK reçu.

Lorsqu' une perte au niveau des paquets est signalée TCP/IP passe au mode FAST RETRANSMIT, la source doit réémettre tous les paquets, et le mode SLOW START ne peut être activé qu'après la commutation au mode CONGESTION AVOIDANCE. (Figure V-17)

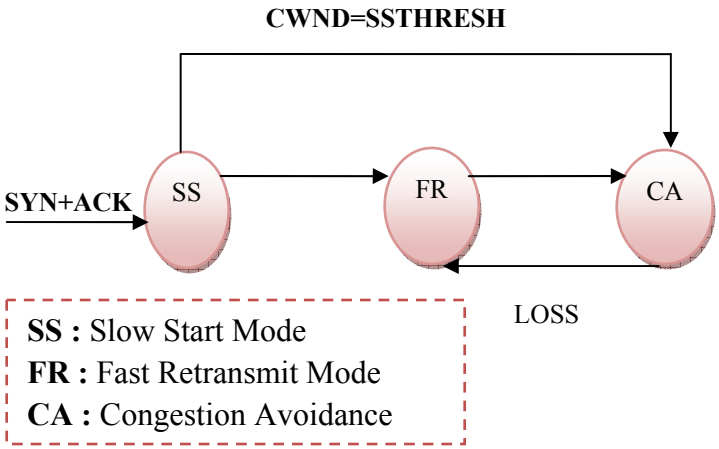


Figure V-17 : Commutation de modes TCP/IP [40]

V-6-2/ Equations de propagation:

L'idée de base est d'écrire l'équation (1) sous forme d'équation différentielle afin de décrire l'évolution du trafic TCP/IP dans le réseau Internet c'est-à-dire écrire

le CREDIT en fonction des ACK et les évènements qui provoquent la commutation d'un mode à un autre mode.

Soit $\boldsymbol{\lambda}_s$ (t) le débit d'émission de données d'une source s et $N_s(t)$ le nombre de paquets émis par cette source alors on a [41] :

$$N_s(t) = \int_0^t \lambda_s(t)\,dt \qquad (2)$$

De la même manière pour le nœud récepteur nous aurons [41]:

$$N_{s,r}(t) = \int_0^t \lambda_{s,r}(t)dt \qquad (3)$$

où $\boldsymbol{\lambda}_{s,r}$ (t), $N_{s,r}(t)$ débit et nombre de paquets reçus par le nœud récepteur respectivement, et $\boldsymbol{\lambda}_{s,l}$ (t) et $N_{s,l}(t)$ débit et nombre de paquets perdus avec :

$$N_{s,l}(t) = \int_0^t \lambda_{s,l}(t)dt \qquad (4)$$

Le modèle différentiel suppose la propagation des valeurs de variables d'un nœud à un autre nœud selon l'équation suivante :

$F(t+\Delta t)=F(t)+F'(t)*\Delta t$

(5)

avec : $F'(t)=K=$Constante, $\forall\, t\in [t, t+\Delta t]$.

V-6-2-1/ <u>Mode START SLOW:</u>

Comme nous avons vu dans ce mode, le flot de paquets émis suit une suite géométrique de raison (b+1)/b, on écrit le taux de paquets émis à t_{k+1} en fonction de celui à t_k :

$$\boldsymbol{\lambda\big((K+1).RTT\big) = \frac{b+1}{b}\lambda(K.RTT)} \qquad (6)$$

et comme $\lambda_k = \lambda_0 \left(\frac{b+1}{b}\right)^{\frac{K}{RTT}}$ avec λ_0 =b/RTT, on obtient :

$$\boldsymbol{\lambda(t) = \frac{b}{RTT(t)} \cdot e^{\frac{\ln\left(\frac{b+1}{b}\right)}{RTT(t)}t}} \qquad (7)$$

Après dérivation on a :

$$\boldsymbol{\dot{\lambda}(t) = \frac{\lambda(t)}{RTT(t)} \cdot \ln\left(\frac{b+1}{b}\right)} \qquad (8)$$

A vrai dire le transfert est géré par le débit des acquittements reçus du nœud récepteur (pour chaque ACK reçu la source émis b+1 paquets), et donc nous aurons :

$$\boldsymbol{\lambda_{r-max} = (b+1).\lambda_{ack} = \mu_{min}\ \frac{b+1}{b}} \qquad (9).$$

Où μ_{min} est le taux de service du routeur le plus lent et $\boldsymbol{\lambda}_{ack} = \mu_{min}/b$.

V-6-2-2/ Mode CONGESTION AVOIDANCE:

Dans ce mode le débit moyen est $\lambda(t) = \frac{CWND(t)}{RTT(t)}$, et de même façon ce débit est limité par le débit des acquittements reçus (un ACK pour chaque [b+ (1/CWND)]) d'où [40]:

$$\lambda_{r-max}(t) = \left(b + \frac{1}{CWND(t)}\right). \lambda_{ack} \quad (10)$$

On remplace $\lambda_{ack} = \mu_{min}/b$ par sa valeur et on trouve

$$\lambda_{r-max}(t) = \left(1 + \frac{1}{b.CWND(t)}\right). \mu_{min} \quad (11)$$

V-6-2-3/ Mode FAST RETRANSMIT:

Les paquets perdus sont retransmis avec un débit :

$$\lambda_s(t) = \frac{1}{RTT_s(t)} \quad (12)$$

V-6-2-4/ Evolution de CWND:

L'évolution de CWND peut être résumée de la manière suivante :

$$CWNDs(t) = \begin{cases} CWNDs(t) + 1 & SS \\ CWNDs(t) + \frac{1}{CWNDs(t)} & CA \\ 0 & FR \\ \frac{CWNDs(t)}{2} & LOSS \end{cases} \quad (13)$$

V-6-2-5/ Débit des acquittements:

Le débit des acquittements reçus détermine le débit de transfert des paquets. Soit $\lambda_j(t)$ le débit des ACK reçus, et $\lambda_i(t)$ le débit de l'émission :

$$\lambda_j(t) = \begin{cases} \lambda_i(t) & FR \\ \frac{\lambda_i(t)}{b} & SINON \end{cases} \quad (14)$$

V-6-2-6 Estimation de RTT :

La valeur de RTT dépend du chemin des paquets, soit D_i le délai de connexion d'un routeur à un autre, T_i le délai de transfert d'un paquet à partir d'une source i, RTT est calculé par la formule suivante :

$$RTT(t) = \sum_{i \in R} T_i(t) + D_i \quad (15)$$

R est l'ensemble de routeurs, et $T_i(t)$ égal à :

$$T_i(t) = \begin{cases} \frac{1}{\mu_{min}} & n(t) = 0 \\ \frac{n(t)}{\mu_{min}} & n(t) > 0 \end{cases} \quad (16)$$

$n(t)$ représente le nombre de paquets dans la file d'attente.

Partant des données μ_{min}= 500000, capacité de la file d'attente 35, délai de chaque routeur égal 1ms [40], et notant que $n(t)$ suit une distribution gaussienne [39], on détermine le RTT.

Le nombre de routeurs (deux routeurs) est déterminé avec la commande TRACERT. Le schéma qui décrit l'expérience est le suivant :

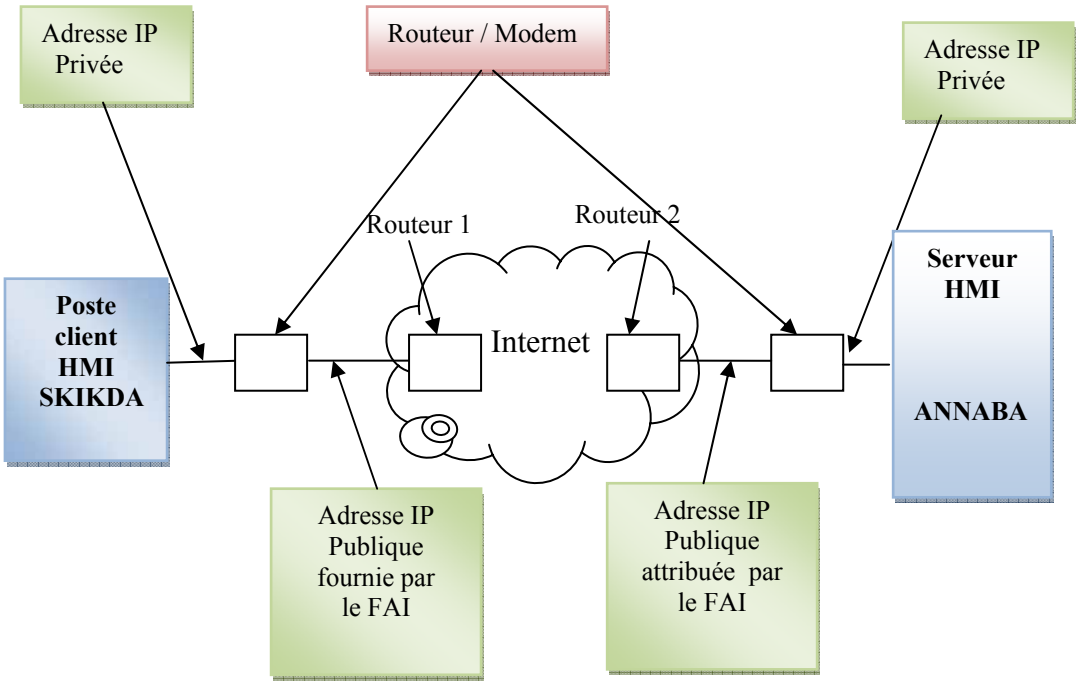


Figure V-18 : Schéma du principe de l'expérimentation

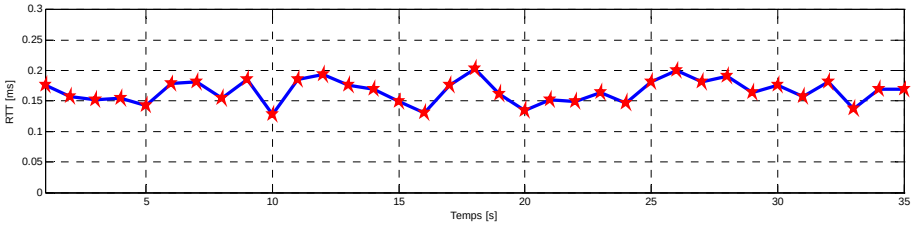


Figure V-19 : Estimation de délai de traitement au niveau du premier routeur

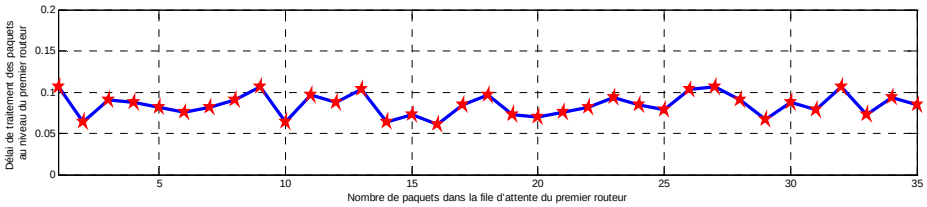


Figure V-20: Estimation de délai de traitement au niveau du deuxième routeur

Les deux courbes ci-dessus représentent les délais de traitement et de routage du premier et deuxième routeur respectivement. En effet, ces routeurs schématisent d'une manière simple et assez réaliste ce qui se passe au niveau des réseaux WAN (Wide Area Network) en particulier l'internet. Ces délais dépendent essentiellement du nombre de paquets dans la file d'attente (expression (16)) :

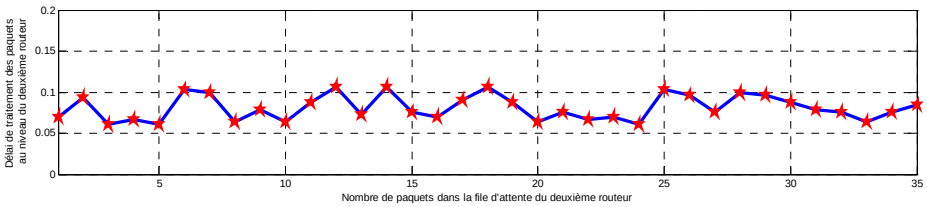


Figure V-21: Estimation de RTT avec le modèle

Quant à la courbe de la figure V-21, elle représente la mesure du délai entre l'envoi d'un paquet et la réception de son acquittement. Ce délai est calculé à partir de l'expression (15).

V-6-3/ Mesures expérimentales:

A partir du poste client plusieurs commandes Ping (Figure V-22) ayant comme cible l'adresse du serveur ont été effectuées à des intervalles séparés, la commande Tracert était utilisée pour connaitre le nombre de commutation nécessaires (routeurs) pour accéder au serveur [38], les mesures faites sont enregistrées au tableau ci-dessous.

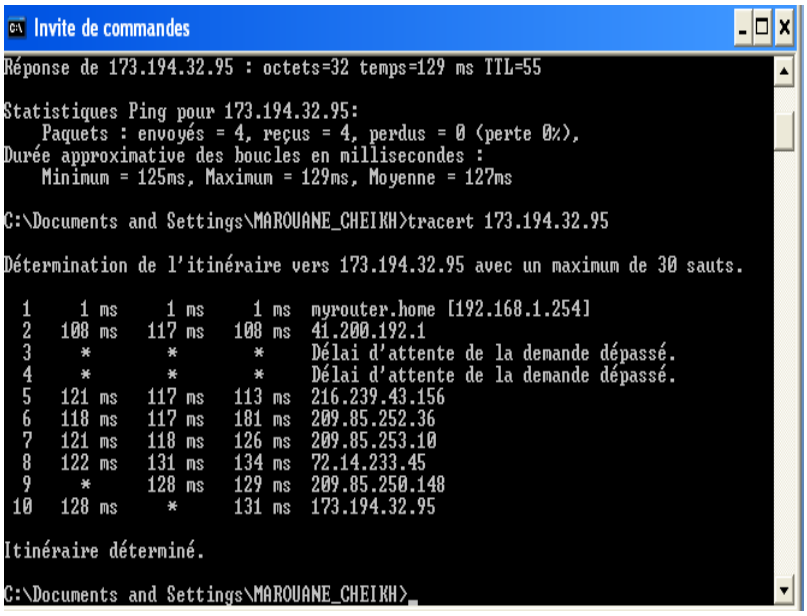


Figure V-22 : Estimation du délai de bout en bout

DATE	HEURE	RTT
23/11/2012	09H00	187 ms
23/11/2012	13H00	183 ms
23/11/2012	22H00	171 ms
24/11/2012	10H00	136 ms
24/11/2012	15H00	147 ms
24/11/2012	21H00	125 ms
25/11/2012	09H30	186 ms
25/11/2012	14H00	185 ms
25/11/2012	22H30	171 ms
26/11/2012	09H00	138 ms
26/11/2012	13H30	147 ms
26/11/2012	23H30	128 ms
27/11/2012	08H30	174 ms
27/11/2012	15H30	163 ms
27/11/2012	22H30	157 ms

Tableau V-1 : Mesures du RTT

Une différence légère est à remarquer entre le RTT en jour et en nuit puisque le nombre d'utilisateurs diminue relativement, la courbe suivante illustre les valeurs de RTT pour chaque commande effectuée.

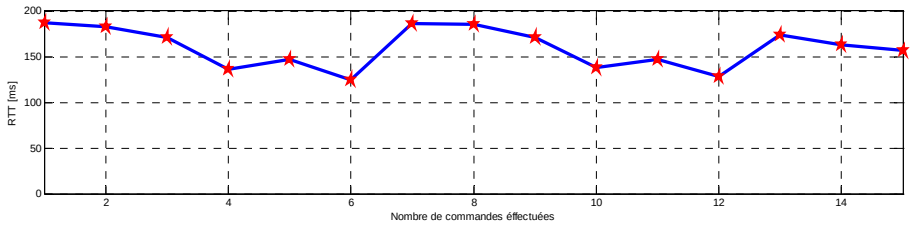


Figure V-23 : Mesures de RTT avec la commande Ping

Quoique la mesure estimée et la mesure réelle ne sont pas parfaitement identique nous remarquons que la différence est relativement faible cette différence est due principalement à la non détermination exacte du nombre de paquets dans la file d'attente.

V-7 / Surveillance du trafic de communication dans le système de télégestion :

Pour mieux évaluer les performances de la télégestion nous avons utilisé un logiciel « Open Source » le Wireshark [42].Wireshark est un analyseur de trames, ou encore analyseur de protocoles. Il permet de lire toutes les trames passant sur l'interface réseau de votre machine dans le but d'analyser les échanges sur le réseau [43].

Wireshark analyse le trafic passant sur les interfaces Ethernet et WiFi. Il repose sur la commande unix tcpdump, qui permet de sniffer le trafic en mode commandes ; le logiciel fournit juste une interface graphique à tcpdump pour faciliter la lecture [43]. Il dispose en plus de nombreux outils permettant de simplifier et affiner l'analyse du trafic.

V-7-1 / Présentation de Wireshark:

Wireshark est un logiciel qui visualise le transfert des paquets circulant dans un réseau, il est conçu pour travailler dans un environnement Windows, Linux, Solaris et Mac OS X [44]. Il permet d'examiner des trames à partir d'un fichier ou directement en les capturant sur le réseau. Pour chaque paquet, il est possible d'obtenir un résumé ainsi qu'un décodage détaillé.

En outre, le logiciel possède des fonctionnalités très utiles comme les filtres de capture et d'affichage et la reconstitution du flux d'une session TCP. De plus, le nombre de protocoles reconnus par l'analyseur est très élevé.

Utilisé dans un environnement Windows sa mise en service nécessite l'installation de WinPCap qui permet la capture des paquets sous Windows afin d'être analysés par le biais de Wireshark. L'installation de Wireshark [45] est simple et ne demande que suivre les instructions de l'interface de l'installation (Figure V-24).

Figure V-24 : Interface d'installation de Wireshark

L'activation d'une capture se fait dans le menu Capture → Interfaces : sélectionnez l'interface réseau sur laquelle vous souhaitez observer le trafic (Figure V-25).

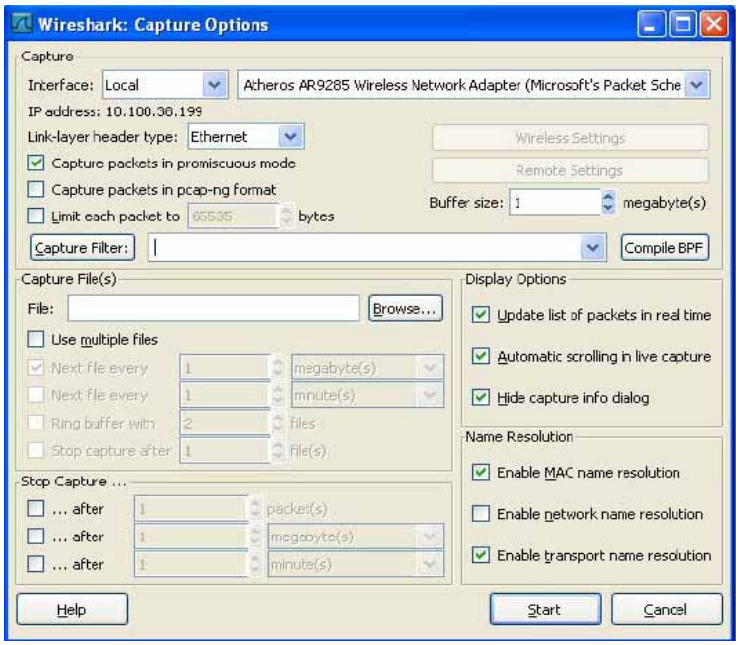


Figure V-25 : Réglage de l'interface de la capture

L'interface graphique présente trois fenêtres (Figure V-26).

- Fenêtre du haut : liste des paquets capturés avec résumé de leurs caractéristiques. En cliquant sur un paquet de cette fenêtre, on modifie le contenu des deux autres.
- Fenêtre du milieu : contenu du paquet, en-tête par en-tête (des couches basses vers les couches hautes)
- Fenêtre du bas : représentation hexadécimale du paquet sélectionné. Les champs sélectionnés dans la fenêtre du milieu y sont affichés en caractères gras.

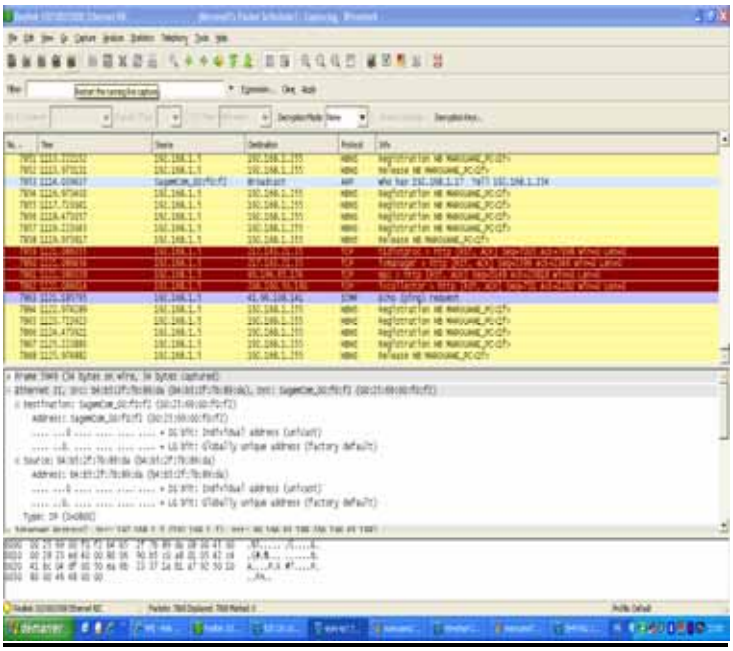


Figure V-26 : Capture des paquets

V-7-2 / Exemple de capture de WireShark:

Notre système de télégestion est installé. Nous avons commencé à évaluer ses performances en termes de qualité de transmission. Nous avons alors utilisé le wireshark afin d'étudier et de tracer les différents paquets mis en œuvre. Le montage utilisé est schématisé par la figure suivante :

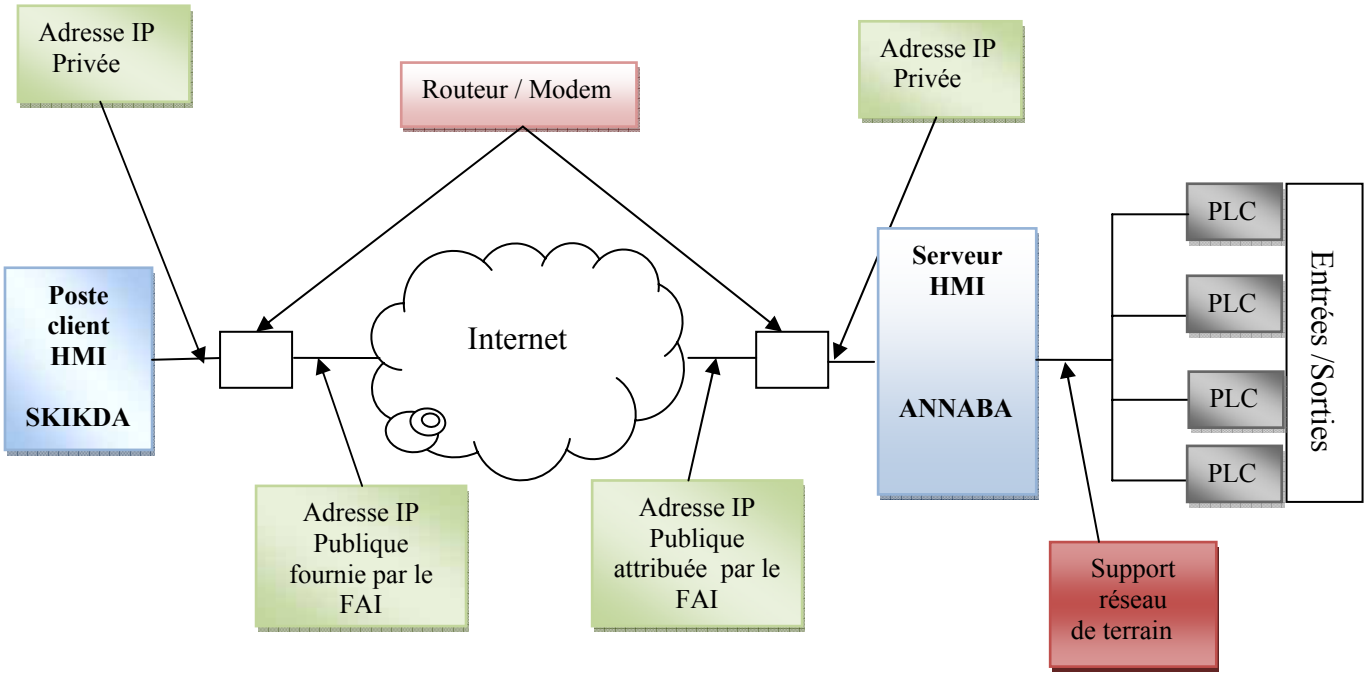


Figure V-27: Schéma du principe de l'expérimentation

A travers cette expérience nous avons pu faire fonctionner notre système de télégestion expérimental. Au niveau du poste HMI client nous avons procédé à la capture et l'analyse de paquets échangés entre HMI client et HMI serveur en utilisant le wireshark. A noter que la connexion entre le client et le serveur s'établit par un simple navigateur internet. La durée de cette expérience ainsi que les moments de son application sont très pertinents. En effet, la durée doit être relativement importante afin de pouvoir réaliser des statistiques de communications assez significatives. Les moments de connexion sont également d'une grande importance afin d'évaluer tous les cas de figure relatifs représentant le trafic internet. Les résultats obtenus de cette étude sont représentés ci-dessous.

La représentation du trafic de réseau Internet sous forme de courbe est nettement sensible aux commandes effectuées au niveau de l'HMI client, la figure ci-dessous illustre le trafic en absence de manipulation de la supervision.

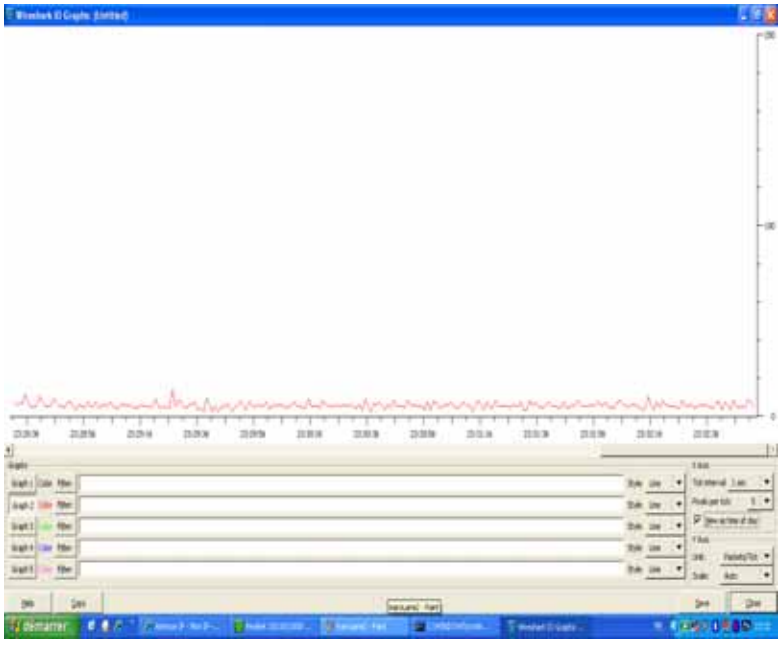


Figure V-28 : Représentation du trafic Internet sans manipulation

Dés que nous commençons à manipuler l'HMI (changer une valeur de champ de saisie, lancer une fenêtre, démarrer une pompe, ouvrir une vanne……etc), la courbe qui représente le trafic enregistre un pic au moment de la manipulation comme le montre la figure V-29.

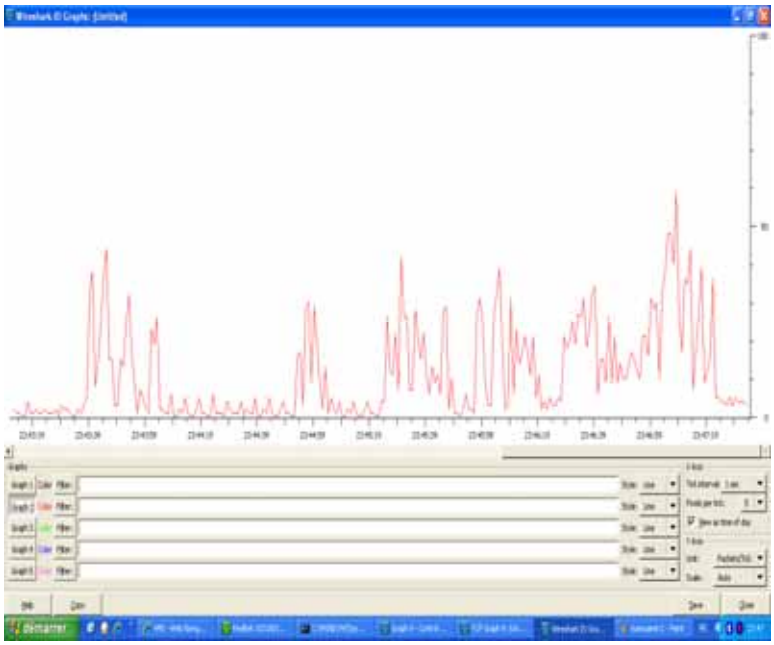


Figure V-29 : Représentation du trafic Internet durant la manipulation

Wireshark permet la visualisation de transfert des paquets sous forme brute, des trames Ethernet, des datagrammes IP et des segments TCP. Dans chaque forme citée il nous fourni des informations importantes relative à chaque niveau, comme illustré à la Figure V-30.

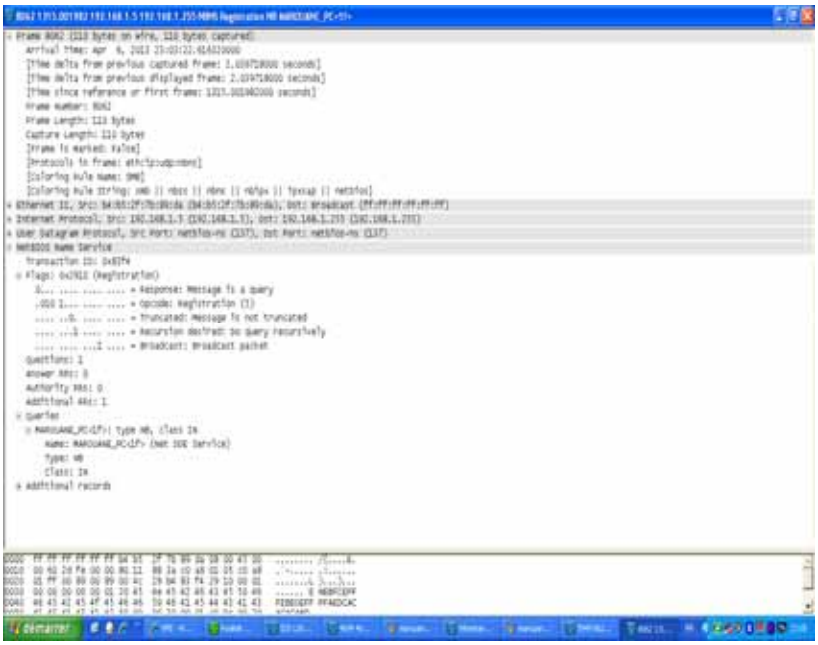


Figure V-30 : Représentation du trafic Internet durant la manipulation

Wireshark possède également l'avantage de représenter sous forme de débit de graphe la connexion entre le nœud source et le nœud destination en montrant le segment TCP avec ses paramètres les plus importants tel que SEQ, ACK …etc.

La Figure ci-dessous montre un exemple de cette représentation entre la source (HMI serveur ayant l'adresse IP 41.69.108.141) et la destination (HMI client représenté par son adresse IP privée 192.168.1.5)

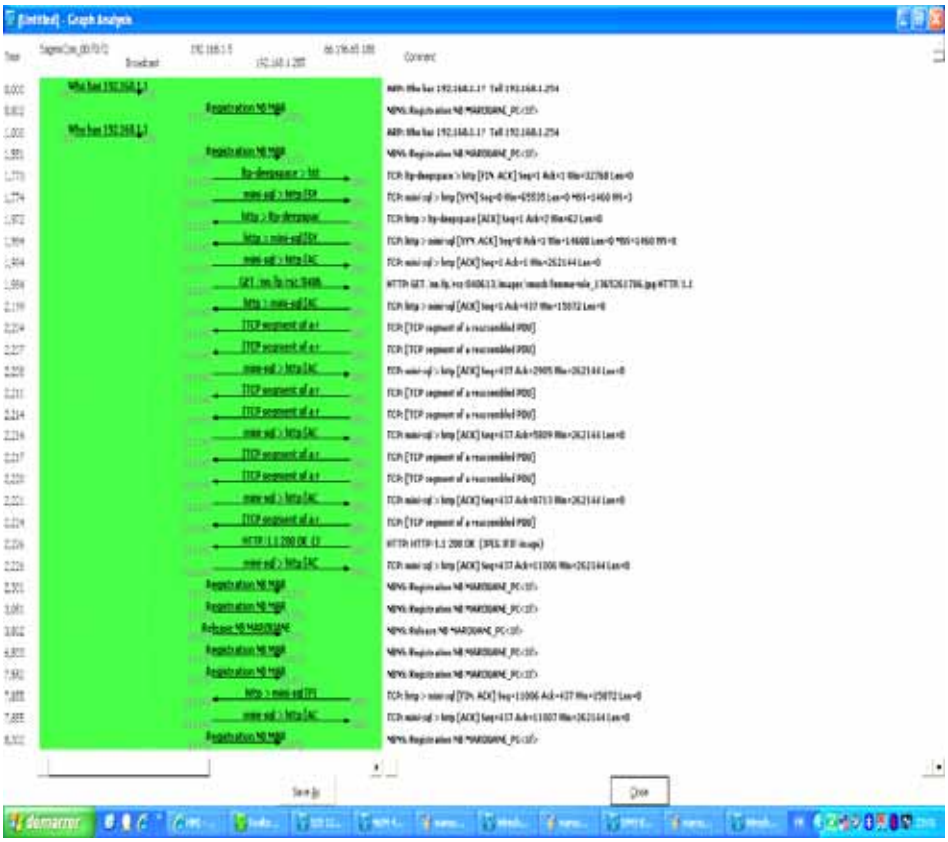


Figure V-31 : Représentation du trafic Internet sous forme de débit de graphe

En plus Wireshark permet de visualiser les paquets perdus et les délais effectués, donc c'est un outil très puissant pour étudier la QoS du réseau.

V-8 / RESULTATS ET DISCUSSION

Toute l'implémentation du HMI étant réalisée, à partir du logiciel Simatic WinCC, selon l'architecture décrite ci-dessus nous avons ensuite configuré notre télégestion, à partir du Web Navigator du WinCC, avec une liaison clients/serveur via des connexions selon le standard http.

Une trentaine de vues comprenant plus de 200 variables (entrées, sorties et alarmes) ont été implémentées, dynamisées au niveau du HMI. Toutes ces variables

ont pu être télégérées selon le standard http. Ces variables sont contrôlées et surveillées à distance à partir du HMI via http sous forme de textes, de couleurs, de courbes, de tableaux, de formes et/ou d'objets. La mise à jour de ces variables à partir du standard http prend moins d'une seconde pour un réseau LAN sans fils de 56kbs, et de l'ordre de 1s, pour une liaison http via une connexion internet ADSL.

Notons, que la télégestion à l'aide des technologies du web en utilisant les protocoles TCP/IP, aussi bien sous LAN (Local Area Network) ou WAN (Wide Area Network), bénéficie de tous les services et protocoles utilisés sous Windows. Parmi, les services et protocoles que l'on pourra solliciter nous avons :

- Les services de messagerie électronique en particulier SMTP et POP3
- Le service DHCP (Dynamic Host Configuration protocol) pour l'attribution des adresses IP aux différents clients en particulier dans le cas du LAN
- Les services IIS, WEB, et le service FTP (File Transfert Protocol).

L'approche analytique différentielle du protocole TCP/IP nous a permis d'estimer le délai de bout en bout avec une erreur relativement faible, l'erreur entre les valeurs estimées et mesurées est due au choix des paramètres des routeurs d'un coté et la distribution de la file d'attente d'un autre coté, cette approche peut nous servir à déterminer d'autres paramètres tel que le débit de transfert des données, ou l'évolution de la taille de la fenêtre.

De même, Wireshark nous a permis d'étudier les paramètres les plus importants de la QoS à savoir le débit, le délai et les pertes de données. Il est à remarquer que le temps d'une vue (une fenêtre) à une autre vue de l'HMI est relativement important alors que la manipulation des variables au sein de la même vue est quasiment instantané.

L'administration des différents clients, à partir du serveur, permet d'attribuer aux clients des droits d'accès différents. Certains clients, par exemple, peuvent avoir la possibilité de contrôler et de commander alors que d'autres auront seulement la possibilité de suivre l'évolution des différents paramètres de l'installation.

En effet la dernière version de WinCC utilise l'authentification Windows, qui offre une sécurité très supérieure à l'authentification SQL Server [46] (voir chapitre 4).

V-9 / Conclusion :

Dans ce thème nous avons étudié et évalué les performances du fonctionnement d'une télégestion d'une station d'épuration des eaux usées à boue activée, cette dernière est automatisée, il s'agit de la station de Khenchela (Est Algérie). En utilisant les technologies du Web, nous avons donc opté pour un HMI Simatic WinCC. La télégestion adoptée est assurée grâce à l'option Web Navigator du WinCC.

L'implémentation du HMI a pu fonctionner convenablement malgré le nombre élevé des variables pertinentes (entrées, sorties et alarmes). La télégestion adoptée par l'utilisation de la technologie Web (WebNavigator) démontre la qualité et la fiabilité d'une surveillance à distance des installations industrielles géographiquement réparties. A cet effet, le délai entre serveurs et clients est relativement faible ainsi la sécurité est largement suffisante.

Conclusion Générale

Conclusion générale :

Dans notre travail de magister nous nous sommes intéressés à la télégestion des installations industrielles géographiquement réparties. Nous avons essayé d'apporter une contribution dans ce domaine, devenu vital, en utilisant des réseaux de communication notamment Internet. Nous avons donc commencé par donner un aperçu succinct sur les notions fondamentales des réseaux informatiques. Nous avons ensuite présenté certaines méthodes de conception des HMI en tenant compte de l'analyse et la modélisation des taches humaines et les spécifications de la conception d'un système interactif. L'architecture des systèmes SCADA a été développée y compris la communication entre le terminal principal et les autres terminaux déportés. La sécurité, qui représente le point le plus pertinent des systèmes SCADA, a également été discutée en se basant sur les risques et attaques visant le réseau Internet et l'environnement SCADA.

Enfin nous avons réalisé et étudié une télégestion, utilisant comme support de communication le réseau Internet. Ainsi, la distance entre l'installation et le poste client peut être arbitraire puisqu'il suffit uniquement d'avoir l'accès à Internet.

Au cours de ce travail, nous avons étudié et évalué la possibilité et les apports d'une télégestion dans des stations d'épurations des eaux usées à boue activées. En effet, ces stations d'épurations des eaux usées sont devenues une nécessité compte tenu des contraintes liées à la sauvegarde de l'environnement d'une part. D'autre part, elles représentent un exemple typique d'installation répartie sur de vastes zones géographiques et nécessitant une télégestion. Dans cette étude nous avons pris un exemple particulier d'une station d'épuration des eaux usées, afin d'étudier l'impact de l'utilisation de ces technologies et plus précisément le Web Navigator. Ce dernier est un module du progiciel WinCC assurant la télégestion. La télégestion est composée généralement de plusieurs postes, clients et/ou serveurs, qui sont:

- Des postes locaux : Répartis sur les ouvrages techniques
- D'un ou deux postes centraux : Pour disposer d'une vue d'ensemble du réseau.
- Des réseaux de communications industriels et publics
- Différents types de supports de communication (conducteurs électriques, sans fils, fibre optique …etc)

- Des équipements d'interconnexion (commutateurs, concentrateurs, points d'accès, routeurs, …etc)

Afin de mieux étudier la télégestion nous avons adopté la modélisation analytique différentielle de TCP/IP qui nous a permis d'estimer un paramètre important de la QoS, et faire des mesures réelles en utilisant les commandes classique PING et TRACERT.

Avec l'utilitaire Wireshark qui est un analyseur de trames, ou encore analyseur de protocoles permettant de lire toutes les trames passant sur l'interface réseau d'une machine dans le but d'analyser les échanges sur le réseau, nous avons pu réaliser une étude expérimentale des performances de la télégestion à savoir le taux de perte, le mouvement des paquets transférés, la mesure de débit…etc.

La télégestion est une discipline qui dépend essentiellement de l'électronique, de l'informatique et des télécommunications. Elle permet d'assurer le bon fonctionnement des installations industrielles géographiquement réparties en garantissant entre autres sa sécurité, sa surveillance et le contrôle et commande locale et à distance …etc.

L'implémentation du HMI, malgré un nombre relativement élevé des variables pertinentes (entrées, sorties et alarmes), a pu fonctionner correctement. La télégestion adoptée, en utilisant la technologie Web (standard http), grâce au Web/Navigator montre bien la puissance et la robustesse d'une surveillance à distance de telles installations industrielles géographiquement réparties. En effet, le temps de réponse entre serveurs et clients est relativement faible et la sécurité est suffisamment assurée.

PERSPECTIVES :

Le travail que nous avons présenté est seulement l'achèvement d'une première phase. En effet, il y'a plusieurs perspectives qui sont ouvertes dont les plus pertinentes :

- Etude et mise en œuvre d'une sécurité du SCADA
- Etude et évaluation de la QoS

BIBLIOGRAPHIE

Bibliographie :

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

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

[03] Gilbert Held « Network Design: Principles and applications» CRC Press LLC 2000.

[04] Kurose & Ross, «Analyse structurée des réseaux », Pearson Education 2003.

[05] Craig Hunt «TCP/IP : Administration de réseaux», O'Reilly, 2002.

[06] Charles M. Kozieirok «The TCP/IP guide», Aquarelle, 2003.

[07] D.Kofman et M. Gagnaire «Réseaux haut débits », Tome 1. 2ème édition Dunod 1999

[08] Alexis Ferréro «Les réseaux locaux commutés et ATM », Inter Editions 1998.

[09] Charles Spurgeon. «Guide Pratique des Réseaux Ethernet », Vuibert 1998

[10] Christian Huitema «Le routage dans l'Internet» - Edition Eyrolles, 2002

[11] Christophe Kolski «Interfaces homme-machine, application aux systèmes industriels complexes ». Éditions Hermès, 1997.

[12] Kolski C. «Interfaces Homme-Machine», Hermès. 1997

[13] Coutaz J. «Interfaces Homme-Ordinateur», Dunod.1990.

[14] Frank Tarpin-Bernard «Interaction homme-machine adaptative », Thèse d'habilitation, L'institut national des sciences appliquées de Lyon et l'université Claude Bernard Lyon I, 2006

[15] Millot .P «Supervision des procédés automatisés et ergonomie ». Éditions Hermès, 1988

[16] Christophe Kolski et Houcine Ezzedine Lamih, «Conception et évaluation des IHM de supervision : éléments méthodologiques », Revue Génie Logiciel, 2003

[17] BENAISSA.M «Une démarche de conception, réalisation et évaluation d'IHM : Application au projet ferroviaire ASTREE ». Thèse de doctorat, université de Valenciennes, décembre 1993.

[18] Dans Boy, G.A. (Ed.). «L'ingénierie cognitive : IHM et Cognition». Hermès, 2005.

[19] GALITZ, Wilbert O «The Essential Guide to User Interface Design», John Wiley & Sons; 2nd edition, June 15, 2002.

[20] L.Nigay, «Conception et modélisation logicielles des systèmes interactifs : application aux interfaces multimodales», PhD dissertation, Université de Grenoble, France, 1994.

[21] M.David Julien «Goliath: un environnement à base de modèles et agents pour la conception d'interface utilisateurs » Thèse de doctorat de l'université Paris 6, 2004

[22] Ikhlef Boualem «contribution à l'étude de supervision industrielle automatique dans un

environnement SCADA » mémoire magistère université M'HAMED BOUGARA de BOUMERDES 2009.

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

[24] Keith Stouffer, Joe Falco, Karen Kent «Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security» NIST Special Publication 800-82

[25] David Bailey,Edwin wright «Practical SCADA for Industry», Edition Newnes 2003

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

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

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

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

[30] John Park, Steve Mackay, Edwin wright, Deon Reynders «Practical Industrial Data Networks», Edition Newnes 2003

[31] Omar Santos «End to end network security defense in deptht», Cisco Press2008.

[32]Ronald L. Mendell, Ms, Cissp, Cli «Document security», Charles C Thomas Publisher, Ltd 2007

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

[34] Stuart McClure, Joel Scambray , George Kurtz «Halte aux hackers», Eyrolles 2003.

[35] Yongge Wang, Bei-Tseng Chu «sSCADA: Securing SCADA Infrastructure Communications», International Journal of Communication Networks and Distributed Systems , August 5, 2004.

[36] www.siemens.com: Siemens company web site.

[37] Bruno Tuffin'' Modélisation mathématique pour la conception, l'analyse quantitative et le contrôle de la qualité de service des systèmes", Habilitation à diriger les recherches, université de Rennes I, 2006.

[38] Nicolas Larrieu, '' Contrôle de congestion et gestion du trafic à partir de mesures pour l'optimisation de la QdS dans l'Internet''. Thèse doctorat, université TOULOUSEIII, 2005.

[39] Frederico Larroca,'' Techniques d'Ingénierie de Trafic Dynamique pour l'Internet''. Thèse de doctorat, Ecole doctorale d'informatique, télécommunication et électronique de Paris.

[40] Hassan Hassan, “Modélisation et analyse de performances du trafic multimédia dans les réseaux hétérogènes”, Thèse de doctorat, université de TOULOUSEIII, 2006.

[41] Gauchard David, “Simulation hybride des réseaux IP-DiffServ-MPLS multiservices sur environnement d’exécution distribuée”, Thèse de doctorat, université de TOULOUSEIII, 2003.

[42] www.wireshark.org

[43] Stephan Robert “Laboratoire de téléinformatique : Introduction à l’analyseur de réseau wireshark”, haute école d’ingénierie et de gestion du canton de Vaud

[44] Sivanantharasa Panchadcharam “Information and Communications Technology Infrastructure for Smart Distribution Network Application”, Master of philosophy, Burnel University UK.

[45] Chris Sanders “Practical Packet Analysis: using wireshark to solve real-world network problems”, No Starch Press. Inc, 2007.

[46] ICS-CERT, ‘ICSA-12-205-01—Siemens Simatic Wincc Insecure SQL server authentification ’’. 13/07/2012