REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARRA
BOUMERDES
FACULTE DES SCIENCES DE L'INGENIEUR

Département de maintenance industrielle
Option génie électrique

Mémoire de fin d'études

En vue de l'obtention du diplôme de master en automatique

Thème

Cyber sécurité pour le réseau de connexions du système de conduite automatisé hiérarchisé des ateliers de production
Cas : Cimenterie MEFTAH

Réalisé par :
- M[r]. KHALFI Nacim

Promoteur:
D[r] M.S. BOUMEDIENE

Président

Examinateur

Examinateur

Promotion: 2015/2016

ملخص

خلال الخمسة عشر عاما الأولى من القرن الحادي والعشرين عرف العالم توسعا كبيرا في مجال العلوم ، عالم السيارات، تكنولوجيا المعلومات و حتى تكنولوجيا الاتصال . شمل هذا التطور المجال الصناعي فازدهرت الصناعة كونها استجابة لمطالب ورغبات المنتجين لتحقيق المزيد من الأرباح و النتائج.

تغيّر شكل المصانع من مُنْشَآةٍ معزولة إلى أخرى مهيّأة بأحدث الأجهزة ذات التقنيات العالية, أسهل استعمالا وأكثر إتاحةً و وصولا لجميع أنحاء العالم، و هذا استجابة لمتطلّبات التّكنولوجيا الاتصال الحديثة.

التطوّر نحو تبسيط الصناعات و أنظمتها لا يخلو من إضعاف أمن و تهديد السّير الحسن للأجهزة و لورشات الإنتاج.

صحوة العالم الصناعي لمشكلة الأمن المرتبطة بإتّصال الأجهزة والتّركيبات أدّى إلى ظهور تخصص جديد هو cyber-security لأنظمة التحكم الصناعية.

Abstract

We are almost reaching the fifth of the 21th century, the world knows an amazing expansion and evolution concerning sciences, automotive, IT and even in the connectivity field.

The industry was also there, to live that evolution that touched her in an extraordinary way, being part of the answers to the increasing demands, requests and to the wishes of the producers to get more results and benefits.

The factories and production workshops changed status from an isolated plan to a hi-tech facility, easier to use and way more reachable, answering again to nowadays connectivity requirements.

The development towards simpler industries and their systems was not without blow against, weakening their security and jeopardizing the proper functioning of facilities and production workshops.

The awakening of the industrial world to this issue linked to the facilities connectivity gave birth to a new discipline which is the Cyber-security of industrial control systems.

Résumé

Durant la première quinzaine d'années du 21ème siècle, le monde a connu une folle expansion et cela concernant les sciences, le monde de l'automobile, celui des technologies de l'information et même de la connectivité.

L'industrie n'a pas non plus faillit au rendez-vous de l'évolution, qui l'a atteinte d'une façon vertigineuse, étant bien sur une réponse aux demandes croissantes et aux envies des producteurs à vouloir toujours plus de bénéfices et de résultats.

Les usines ont changé de statut, passant d'une installation isolée à vers une installation Hi-Tech plus simples d'utilisations et bien plus accessibles et ce même des quatre coins du globe, ceci répondant aux exigences actuelles de connectivité.

Les évolutions vers la simplicité des industries et leurs systèmes n'a pas été sans contre coup, fragilisant leurs sécurité et mettant en péril le bon fonctionnement des installations et ateliers de production.

L'éveil du monde industriel à ce souci de sécurité lié à la connectivité des installations a donné naissance à une nouvelle discipline étant la Cyber-sécurité des systèmes de contrôle industriels.

Remerciements

J'adresse mes sincères remerciements à tout premièrement dieu tout puissant m'ayant donné la santé, la volonté et la patience afin de pouvoir réaliser ce travail.

Je tiens à remercier le département de maintenance industrielle de la Faculté des sciences de l'ingénieur pour m'avoir accordé la chance de prendre part à ce master.

En particulier : Dr K.KHALFI

Je tiens à remercier mes enseignants du département Automatisation et électrification des procédés industriels de la Faculté des hydrocarbures et de la chimie qui ont contribués à ma formation le long de mon cursus universitaire, et à qui je dois le plus grand des respects.

. En particulier mon promoteur de thèse : Dr M.S.BOUMEDIENE.

Je tiens à remercier d'une part le directeur de formation de la cimenterie SCMI Mr. Riche A, le responsable des stagiaires Mr. HAMMOUCHE K. et d'une autre part, tout le staff technique de la SCMI tout particulièrement :

Mr.ABBAD C.

Mes remerciements s'adressent également à tous mes amis.

DEDICACE

A qui puis-je dédier ce travail si ce n'est à mes très chers parents, dont le sacrifice, la tendresse, l'amour, la patience, le soutien, l'aide et les encouragements sont le secret de ma réussite. Sans qui, je n'aurais pas accompli tout cela.

Je le dédie également

A mon cher frère Mohamed Amine

A ma très chère sœur Selma

A mon beau frère Anis

A mes oncles Abderrahmane, Abdelkader, Nabil et surtout Kamel

A tous mes enseignants tout au long de mon cursus.

A tous mes amis

Je dédie enfin ce travail à toute personne ayant contribué de prés ou de loin à sa concrétisation.

K.Nacim

Sommaire

SOMMAIRE

Liste des figures I

Liste des abréviations II

Introduction générale 1

Problématique 2

CHAPITRE I : Contrôle et système de contrôle industriel

I.1. Introduction 4

I.2. Contrôle industriel 4

I.3. Systèmes de contrôles Industriels (S.C.I) 5

I.3.1. Définition 5

I.3.2. Historique 5

I.3.3. Le fonctionnement d'un ICS 7

I.3.4. Les composantes d'un ICS 9

I.3.4.1. Composants de contrôle 9

I.3.4.2. Composants réseau 11

I.4. Systèmes Informatiques (IT systems) 13

I.5. SCADA (Supervisory Control And Data Aquisition) 15

I.5.1. Fonctionnement 15

I.5.2. Architectures SCADA 16

I.6. DCS (Distributed Control Systems) 17

I.6.1. Architecture 18

I.6.2. Gestion des niveaux de commande 20

I.7. Comparatif DCS et SCADA 20

I.8. Conclusion 21

CHAPITRE II : Les vulnérabilités des systèmes de contrôle industriels

II.1. Introduction 22

II.2. Comparatif ICS et IT 22

II.3. Les menaces: Agents de menaces et définitions 28

II.4. Les vulnérabilités potentielles des ICS 30

II.4.A. Vulnérabilités des politiques et procédures 30

II.4.B. Les Vulnérabilités par plateformes 32

II.4.B.1.Configuration 32

II.4.B.2. Matériel (Hardware) 34

II.4.B.3.Logiciels (Software) 35

II.4.B.4. Logiciels Malveillants (Malware) 36

II.4.C- Les vulnérabilités réseaux 37

II.4.C.1.Vulnérabilités des configurations réseaux 37

II.4.C.2. Vulnérabilités du matériel réseau (Hardware) 37

II.4.C.3. Vulnérabilités du périmètre réseaux 38

II.4.C.4. Vulnérabilités l'enregistrement et de la surveillance 38

II.4.C.5. Vulnérabilités de communication 39

II.4.C.6. Vulnérabilités des connexions sans-fil 39

II.5. Facteurs de risque 39

II.5.a. Technologies et protocoles standardisées 40

II.5.b. Connectivités 40

II.5.c. Connexions non-sécurisées. 42

5.d. L'information publique 43

II.6. Les cyber-incidents (ou incidents de cyber-sécurité) 44

III.6.a. Sources d'incidents 44

III.6.b. Scénarios d'incidents possibles 44

II.7.Conclusion 45

CHAPITRE III : Programme de cyber-sécurité des systèmes de contrôle industriels

III.1.Introduction 46

III.2. Programme de sécurité 46

III.2.1. Définir et faire l'inventaire des atouts ICS 46

III.2.2.Procéder à une évaluation des risques et vulnérabilités 47

III.2.3.Définir les contrôles d'atténuation et de réduction 49

III.2.3.1. Sécurisation fonctionnelle 49

III.2.3.1.A. Les architectures réseaux 49

III.2.3.1.B. Réseaux de contrôle logiquement séparés 50

III.2.3.1.C. Séparation des réseaux 51

III.2.3.2. Sécurisation technique 57

III.2.3.2.A. Pare-feu (Firewalls) 57

III.2.3.2.B. Pré-configuration du pare-feu 57

III.4. Plan économique 58

III.5. Conclusion 58

CHAPITRE IV : Représentation de la cimenterie de MEFTAH

IV.1. Introduction 59

IV.2. La situation géographique de la cimenterie 59

IV.3. Le processus de fabrication 60

IV.4. Description de la ligne de production 60

IV.4.1. La zone carrière 61

IV.4.2. La zone CRU 62

IV.4.3. La zone cuisson 64

IV.4.4. La zone Ciment 65

IV.4.5. La zone expédition 66

IV.5. Conclusion 67

CHAPITRE V : ETUDE DE CAS « Système de contrôle de la SCMI »

V.1. Introduction 68

V.2. Architecture réseau du système de contrôle de la SCMI 68

V.3. Inventaire des atouts de l'ICS 73

V.3.1. Logiciel d'inventaire réseau Open-audiT 73

V.3.2. Instrumentation 76

V.3.3. Interface logiciels et HMI 81

V.3.4. Normes et protocoles de communication 82

V.4. Analyse des vulnérabilités du réseau 83

V.4.1. Logiciel SNORT 84

V.4.2. Liste des vulnérabilités 85

V.5. Implémentation de la solution 86

V.5.1. La sécurisation fonctionnelle 86

V.5.2. La sécurisation technique 86

V.5.2.1.1. Pare-feu FL MGUARD 86

V.5.2.1.2. Logique de la programmation 87

V.5.2.1.2. Etapes de la programmation 88

V.6. Conclusion 92

Conclusion générale 93

Références bibliographiques III

Annexe IV

Liste des figures

Liste des figures

Figure I.1 : PAC Programmable Automation Controller 7

Figure I.2 : Fonctionnement d'un ICS 9

Figure I.3 : Un exemple d'une salle de contrôle SCADA réalisé par la firme « RGB spectrum » 14

Figure I.4 : Un exemple d'implémentation d'un système SCADA (Contrôle et surveillance distribuées) 16

Figure I.5 : Salle de contrôle DCS réalisée par la firme « Yokogawa » 17

Figure I.6 : Composants et configuration générale d'un DCS 19

Figure III.1 : Fonction du DMZ entre les réseaux ICS et d'entreprise 53

Figure III.2 : Pare-feu entre le réseau de contrôle et le réseau d'entreprise 54

Figure.III.3 : Combinaison pare-feu/routeur entre le réseau de contrôle et le réseau d'entreprise 55

Figure III.4 : Pare-feu avec DMZ entre le réseau de contrôle et le réseau d'entreprise 56

Figure III.5 : Paire de pare-feu entre le réseau de contrôle et le réseau d'entreprise 58

Figure IV.1 : Situation géographique de la cimenterie de MEFTAH 60

Figure IV.2 : Schéma de processus de fabrication du ciment 61

Figure IV.3 : Extraction et transport de la matière première 62

Figure IV.4 : Concassage et transport 63

Figure IV.5 : Hall de pré homogénéisation 64

Figure IV.7 : La cuisson 65

Figure IV.8 : Le four rotatif 66

Figure IV.9 : Broyage ciment 67

Figure IV.10 : Expédition en sac ou vrac 67

Figure V.1 : Architecture du réseau globale du système de contrôle de la SCMI 69

Figure V.2 : Zone 1 « Réseau de contrôle » 70

Figure V.3 : Zone 2 « Réseau d'entreprise » 71

Figure V.4 : Niveau 1 du système de contrôle « Supervision » 71

Figure V.5 : Niveau 2 du système de contrôle « Contrôle Commande » 72

Figure V.6.1 : Niveau 3 du système de contrôle « Automates programmables » 73

Figure V.6.2 : Niveau 3 du système de contrôle « Automates programmables » 73

Figure V.7 : Niveau 4 du système de contrôle « Site de terrain » 74

Figure V.8 : Fenêtre d'identification au Panel d'Open-AudiT 75

Figure V.9 : Accès à la fonction découverte 75

Figure V.10 : Fenêtre de sélection des sous réseaux à scanner 76

Figure V.11 : Précision du rang d'adresse IP 76

Figure V.12 : Introduction des identifiants 77

Figure V.13 : Le démarrage de l'inventaire 77

Figure V.14: API S7 416-3DP 78

Figure V.15 : API S7 315 78

Figure V.16 : ET 200M avec connexion PROFINET et CPU S7-300 79

Figure V.17 : ET 200S avec connexion PROFINET, modules E/S et départs-moteurs 80

Figure V.18 : Convertisseur PROFIBUS-Fibre (ICF-1180l) 80

Figure V.19 : Répéteur de PROFIBUS 81

Figure V.20: Borne Wifi Industrielle fonctionnant en point d'accès 81

Figure V.21 : Variateur de vitesse 82

Figure V.22 : Vue d'un projet sous SIMATIC PCS7 82

Figure V.23 : Création d'une vue de Supervision sous WinCC Graphics designer 83

Figure V.24 : Lancement de SNORT 85

Figure V.25 : Démarrage de l'écoute passive 85

Figure V.26 : Détection d'activité avec SNORT 86

Figure V.27. : Pare-feu de sécurité FL MGUARD de la firme PHOENIX CONTACT 88

Figure V.28 : Principe de fonctionnement du pare-feu FL MGUARD 88

Figure V.29 : Accès au panel du FL MGUARD par le biais de son adresse IP par défaut. . 89

Figure V.30 : Panel de configuration du FL MGUARD 89

Figure V.31 : Accès aux options d'interfaces de réseau sur le panel du FL MGUARD. . . . 90

Figure V.32 : Définition d'adresse IP et masque réseau au FL MGUARD 90

Figure V.33 : Copie de la nouvelle adresse IP du FL MGUARD 91

Figure V.34 : Accès aux options d'utilisateurs du pare-feu sur le panel du FL MGUARD. . 91

Figure V.35 : Création d'un modèle d'utilisateur pare-feu 92

Figure V.36 : Création d'un modèle d'utilisateur 92

Figure V.37 : Définition des règles pare-feu adéquates 92

Figure V.38 : Accès aux options d'authentification d'utilisateur pare-feu 93

Figure V.39: Etape finale de la création d'un utilisateur pare-feu 93

Liste des abréviations

Liste des abréviations :

ICS: Industrial Control Systems

IT: Information Technology

SCADA: Supervisory Control And Data Acquisition

SNCC: Système Numérique de Contrôle Commande

DCS: Distributed Control Systems

PAC: Process Automation Controller

PLC: Programmable Logic Controller

HMI: Human Machine Interface

IHM: Interface Homme-Machine

RTU: Remote terminal Unit

MTU: Master Terminal Unit

TCP: Transmission Control Protocol

IP: Internet Protocol

CPU: Central Processing Unit

RAM: Random Access Memory

OS: Operating System

SE: Système d'exploitation

MAJ: Mise à jour

SPOF: Single Point Of Failure

DOS: Denial Of service

DDOS: Direct Denial Of Service

OPC: OLE for Process Control / Open Platform Communication

LAN: Local Area Network

WAN: Wide Area Network

DMZ: Demilitarized zone

Analyse de la codification LAFARGE de l'architecture réseau de la SCMI :

AF : Tablier métallique

AG : Analyseur de gaz

AM : Répartiteur analogique

CP : Condensateur, correcteur de facteur de puissance

CR : Concasseur (mobile et fixe)

DH : Cellule de distribution MT/Medium voltage distribution center

DM : Répartiteur logique

DR : Groupe de commande

EC : Tableau Electrique (Contrôle, protection, comptage, éclairage)

FA : Ventilateur

IN : Réseau informatique

KI : Four

LM : Emetteur (en sortie de silo)

LP : Protection contre la foudre (ensemble du matériel)

LT : Eclairage prise courant

MC : Tableau de distribution basse Tension (LV distribution Center)

MN : Station opérateur (moniteur)

MP : Motopompe

MT : Moteur électrique

PL : Contrôleur Niv1, Automate, satellite, module de contrôle électronique

PM : Ensacheuse

QR : Gratteur

SC : Vis de transport matière

SM : Débitmètre matière

SP : Séparateur

SU : Main Substation (Sous station principale)

SV : Servomoteur

TC : Tour de conditionnement (tower conditionning)

TF : Transformateur (HT,BT, éclairage, auxiliaires)

VS : Variateur de vitesse

WF : Doseur

YZ : Capteur analogique de position

Introduction Générale

INTRODUCTION GENERALE

L'automatisation industrielle est l'art d'utiliser les machines afin de réduire la charge de travail des opérateurs tout en garantissant la qualité et la productivité. Elle fait appel à des systèmes électroniques qui englobent toute la hiérarchie de contrôle-commande depuis les capteurs de mesures en passant par les automates, les bus de communication, la visualisation, l'archivage et même jusqu'à la gestion de la production et des ressources de l'entreprise.

Les systèmes de contrôle industriels mis en œuvre afin d'automatiser l'industrie ont été et sont toujours en continuelle évolution où les Ingénieurs de contrôle cherchent toujours à concevoir et développer des systèmes plus simples, plus ouverts et plus efficaces.

Ceci n'aurait pas pu être accompli sans l'évolution du monde des technologies de l'information et de l'informatique, où beaucoup de facilitations ont pu être apportées aux systèmes de contrôle industriels, à leur conception et développement et surtout du point de vue connectivité.

Etant donné l'accroissement que connait l'industrie actuelle et les besoins qui ne cessent de grandir, les investissements dans des systèmes plus simples et plus compactes sont au jour d'aujourd'hui des pratiques très courantes chez les industriels qui en contre partie ont délaissé petit à petit les systèmes propriétaires pour laisser place à des systèmes plus ouverts et plus accessibles afin de répondre aux besoins actuels de connectivité, où nous pouvons introduire le principe « d'Usine connectée ».

L'industrie a aujourd'hui dépassé l'ère du réseau et a atteint l'ère de l'interconnexion, où nous avons maintenant des usines et installations connectées à internet et accessibles de partout dans le monde.

L'évolution vers la simplicité n'est pas toujours sans contre coup, dans le cas présent la simplification des systèmes a été faite sans la prise en compte d'un facteur essentiel et pas des moindres : La sécurité des systèmes de contrôle.

Beaucoup d'industries critiques s'intéressent aujourd'hui à la sécurité des systèmes de contrôle, facteur pouvant affecter positivement comme très négativement le bon fonctionnement de l'installation, de la production et l'industrie de façon générale.

PROBLEMATIQUE

Les systèmes de contrôle conçus à la base pour travailler dans un environnement fermé sans grandes ressources de sécurité, se retrouvent aujourd'hui dans un milieu connecté sans grande possibilité de se défendre face à tout type de menace. C'est là où l'on introduit les principes de « Cyber-Menaces » et donc de « Cyber-Sécurité ».

L'industrie étant en constante évolution ne peut donc plus se permettre aujourd'hui, de négliger de tels risques qui pourraient mener à des pertes et dégâts irréversibles. D'où ce besoin de développer et mettre au point la ou les solutions de cyber-sécurité aux systèmes de contrôle industriels.

Dans le cadre du mémoire de fin d'études, nous avons effectué un stage pratique au niveau de la cimenterie de « MEFTAH (SCMI) » sans oublier de citer l'important impact de l'industrie du ciment, mais aussi la demande continuellement croissante de la matière produite qui ont poussé les producteurs de cette dernière à investir dans l'automatisation des systèmes, dont la sécurité, la fiabilité, la disponibilité sont des facteurs extrêmement importants. De ce fait, le projet choisis est « L'amélioration de la cyber-sécurité du système de contrôle » consistant à étudier les systèmes de contrôle, leurs vulnérabilités, mettre le relief sur les solutions possibles afin de les appliquer à notre cas réel étant : L'architecture du système de contrôle industriel de la cimenterie de MEFTAH.

Afin de réaliser ce projet, nous avons divisé notre travail en cinq (05) chapitres à savoir :

- Chapitre I : Contrôle et systèmes de contrôle industriels

Dans ce chapitre, on exposera des généralités concernant tous les systèmes de contrôle, leurs composants et leurs fonctionnements.

- Chapitre II : Vulnérabilités des systèmes de contrôle industriels (ICS)

On exposera dans ce chapitre, les grandes lignes des vulnérabilités des ICS et les risques encourus.

Chapitre III : Programme de cyber-sécurité des ICS

Dans ce chapitre, on va présenter l'approche générale à un programme de sécurité des systèmes de contrôle industriel et la méthodologie à suivre.

- Chapitre IV : Présentation de la cimenterie de MEFTAH (SCMI)

Il sera question dans ce chapitre de présenter les étapes de fabrication du ciment et l'installation de la cimenterie, cas et objet de notre étude.

- Chapitre V : Etude de cas « Système de contrôle de la SCMI »

On va étudier en détails dans ce dernier chapitre, l'architecture du système de contrôle industriel de la SCMI et l'implémentation de la solution de cyber-sécurité.

Finalement, nous allons conclure par l'importance de l'amélioration de la cyber-sécurité des systèmes de contrôle de l'industrie actuelle en citant les aspects et apports positifs d'un tel changement.

Chapitre I:

Contrôle et systèmes de contrôle industriels

I.1. Introduction

Le contrôle industriel regroupe un ensemble d'activités techniques et de technologies destinées à l'automatisation des procédés et de systèmes de fabrication industrielle. Les domaines de compétence du contrôle industriel vont de la conception d'installations, à la réalisation, l'exploitation et la maintenance.

Ce chapitre va représenter une introduction aux systèmes de contrôle industriels afin de mieux comprendre leur fonctionnement.

I.2. Contrôle industriel

Le contrôle industriel a fortement évolué ces dernières années en accompagnant la progression des systèmes d'information (IT) omniprésents dans toutes les composantes de l'entreprise industrielle. Toutefois, la technologie et le développement des systèmes d'exécution de la production n'ont pas changé de façon significative la vision d'ensemble du contrôle industriel. On considère généralement que l'activité de production est réalisée par le biais de 3 entités :

- ***Les hommes :*** les personnes qui travaillent et l'entreprise à laquelle ils appartiennent
- ***Les équipements :*** les éléments physiques qui assurent l'activité ou dans lesquels l'activité se déroule
- ***Les systèmes :*** le système d'information et tous les éléments qui s'y rattachent. Le poids respectif de ces entités indique le degré relatif d'automatisation. Par exemple, si les investissements en termes d'équipements et de systèmes sont faibles, les hommes feront l'essentiel du travail. Inversement, des investissements élevés sur ces points entraîneront une part humaine relativement faible.

Les recouvrements entre ces 3 entités définissent 3 interfaces :

- ***L'interface entre les systèmes et les équipements*** **:** L'instrumentation ;
- ***L'interface entre les systèmes et les hommes :*** Les dispositifs de contrôle et de surveillance (IHM, superviseurs) ;
- ***L'interface entre les hommes et les équipements :*** les interactions physiques directes entre les opérateurs et les équipements dans les opérations manuelles d'exploitation.

Le contrôle industriel comprend les systèmes et leurs interfaces avec les hommes et les équipements.

Secteurs industriels concernés

Selon le métier, le contrôle industriel est souvent perçu et appliqué de façon spécifique. Les secteurs industriels suivants sont proposés (les services ou les infrastructures ne sont pas cités) :

Aérospatiale et aéronautique, Agroalimentaire, Automobile, Chimie, Communications et transport de données, Énergie et utilités, Eaux et retraitement des eaux usées, Environnement, Équipements et machinerie industriels, Instruments industriels et médicaux, Mines et métaux, Pétrole et raffinage, Pharmacie, Pulpe et papier, Textiles, Verre et céramique.

I.3. Systèmes de contrôles Industriels (S.C.I)

I.3.1. Définition

Système de contrôle industriel (ICS: Industrial Control Systems) est un terme général qui englobe plusieurs types de systèmes de contrôle utilisés dans la production industrielle, y compris contrôle et l'acquisition de données (SCADA) , les systèmes de contrôle distribué (DCS) et d'autres configurations de système de contrôle plus petit tels que les Automates Programmables Industriels (API) se trouvant très souvent dans les secteur industriels et infrastructure critiques.

Les ICS sont généralement utilisés dans des secteurs tels que l'électricité, l'eau, l'huile et le gaz. Basés sur les données reçues des stations distantes, automatisé ou sur commandes de contrôle de l'opérateur, qui sont souvent désignés comme des appareils de terrain (field devices). Les appareils de terrain contrôlent les opérations locales telles que les vannes et les disjoncteurs (ouverture/clôture), la collecte de données à partir de systèmes de détection, de surveillance de l'environnement local pour les conditions d'alarme.

I.3.2. Historique

Les technologies concernant les systèmes industriels ont évolué durant la dernière décennie. L'historique des SCADA (Supervisory Control and Data Aquisition / Système de contrôle supervisé et acquisition de données) dans les domaines de distribution : Energie, gaz naturel, canalisations des eaux, où il est nécessaire de recueillir des données à distance à travers des liens à faible bande passante, haute latence qui plus est potentiellement non fiables ou même intermittents. Un système SCADA utilise le contrôle à boucle-ouverte avec des sites qui sont grandement séparés géographiquement. Ces systèmes utilisent des RTU (Remote

Terminal units) ou des API (Automates Programmables Industriels) pour renvoyer les données de supervision et surveillance au centre de contrôle. La plupart des Systèmes RTU avaient des limites de capacité pour gérer le contrôle locale pendant que la station maîtresse n'était pas disponible. Toutefois, au fil des années, les système RTU ont évolué de plus et plus et sont maintenant câbles de gérer le contrôle local.

DCS (Distributed Control Systems) ou systèmes de contrôle distribué, fait généralement référence à la fonction particulière que désignent les DCS qui existe dans les installations de processus industriels. (Exemple: pétrole et gaz, raffinage, chimie, pharmaceutique, l'alimentaire, boisson, eaux et eaux usées, papiers, secteur d'alimentation en électricité, les exploitations minière, métallurgie). Le concept du DCS est né du besoin de recueillir les informations et les données tout en contrôlant les systèmes sur un grand campus en temps réel, à grande bande passante, sur des réseaux de faible latence. Sur un DCS, Il est plutôt commun pour une boucle de contrôle de s'étendre jusqu'au contrôleur de très haut niveau, où tout est temps réel. Ces systèmes ont largement évolué depuis le simple besoin d'étendre le contrôle d'un système pneumatique au delà d'une petite parcelle d'une raffinerie.

API (Automates Programmables Industriels) ont évolué du besoin de remplacer les racks de relais sous forme d'échelle. Ces derniers n'étaient pas particulièrement fiables, les installations électriques étaient difficiles à refaire, mais aussi très difficile à diagnostiquer. Le contrôle d'un API tend à être utiliser très régulièrement dans des contrôles binaire de grande vitesse. A la base, les API n'avaient pas les racks E/S et la plupart ne pouvait qu'offrir des contrôles analogiques très rudimentaires.

Les barrières se trouvant entre ces systèmes tendent à disparaître avec le temps. Les limites techniques qui ont poussé à la création et au développement de ces systèmes ne représentent plus grand soucis. La plupart des plateformes API peuvent maintenant effectuer certaines tâches aussi facilement qu'un petit DCS, utilisant des E/S à distances et suffisamment fiables, certains systèmes SCADA arrivent même à gérer des boucles fermées sur une longue distance. Avec l'augmentation de la vitesse des processeurs d'aujourd'hui, la plupart des produits DCS ont une ligne complète de sous système API qui n'était pas présente sur le marcher à leur apparitions.

Ce qui nous mène au concept du PAC (Programmable Automation controller/ Process Automation controller) qui veut dire en langue française: Contrôleur d'automatisation programmable ou Contrôleurs d'automatisation de processus, démontré sur la **Figure I.1**

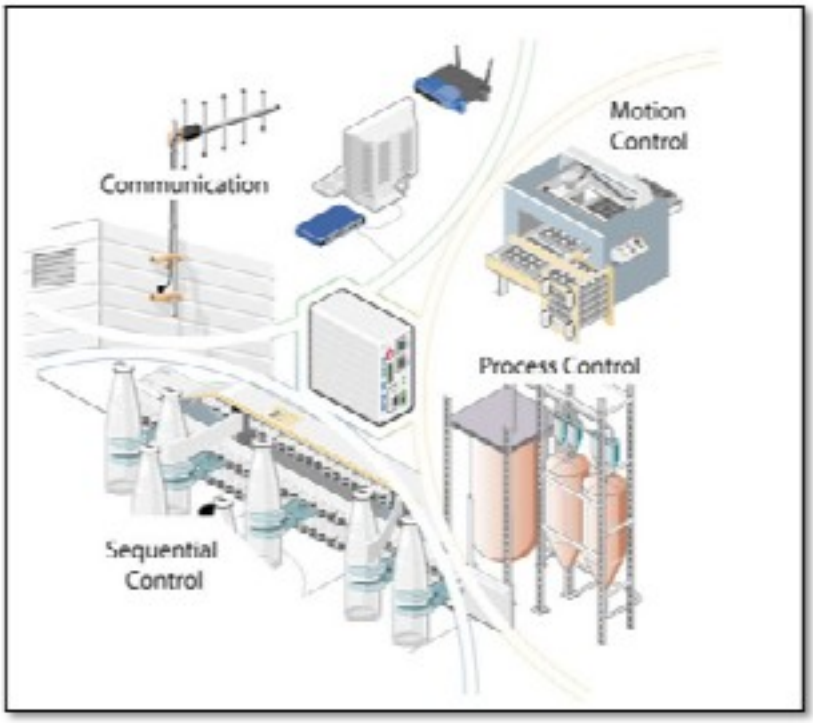


Figure I.1 : PAC Programmable Automation Controller, contraste entrain 3 terrains d'actions différents. [9]

Qui représente en réalité, une sorte de fusions des 3 concepts vus plus haut. Le temps et le marcher vont déterminer si oui ou non, certaines des terminologies et du flou entourant ces 3 concept se verra simplifier.

I .3.3. Le fonctionnement d'un ICS

- **Boucle de régulation:** Une boucle de régulation comporte d'une part le capteur transmetteur de mesure, du matériel de contrôle (API), actionneur (Valves, moteurs etc.) et réalise d'une autre part la communication avec les autres variables. Les variables régulées et contrôlées sont transmises aux régulateurs (dit contrôleur). Le contrôleur interprète les signaux et génère les commandes correspondantes, qu'il transmet aux actionneurs. Le processus change à cause des perturbations créant de nouveaux signaux émanant des capteurs, identifiant le nouvel état du processus, qui sera encore une fois retransmis au contrôleur.

- **Human-Machine Interface (HMI) ou Interface Homme-Machine (IHM):** Les opérateurs et les ingénieurs utilisent les HMI afin de configurer les consignes, les algorithmes de commande, ajuster et établir les paramètres au niveau du contrôleur.

L'HMI affiche aussi les informations concernant les états du processus mais aussi l'historique d'informations

- **Diagnostiques et utilitaires de maintenances à distance:** Diagnostiques et utilitaires de maintenances sont utilisées afin de prévenir, identifier et récupérer des échecs.

Un ICS typique contient une prolifération de boucle de contrôle, HMI, des outils de diagnostiques et de maintenance à distances construit en utilisant un tableau de protocoles de réseau sur une architecture de réseau en couche. Parfois, ces boucles de régulations et de contrôle peuvent être imbriquées et/ou en cascade où la consigne d'une boucle est basée sur la variable de processus déterminée par une autre boucle. Les boucles du niveau de supervision (supervisory-Level) et celles du niveau inférieur (Lower-Level) opèrent de façon continue sur les boucles Supervisory-level et les boucles de lower-level fonctionnent en continu pendant toute la durée d'un processus avec des temps de cycle allant de l'ordre de quelques millisecondes à quelques minutes.

La **Figure I.2** représente le fonctionnement de base d'un ICS:

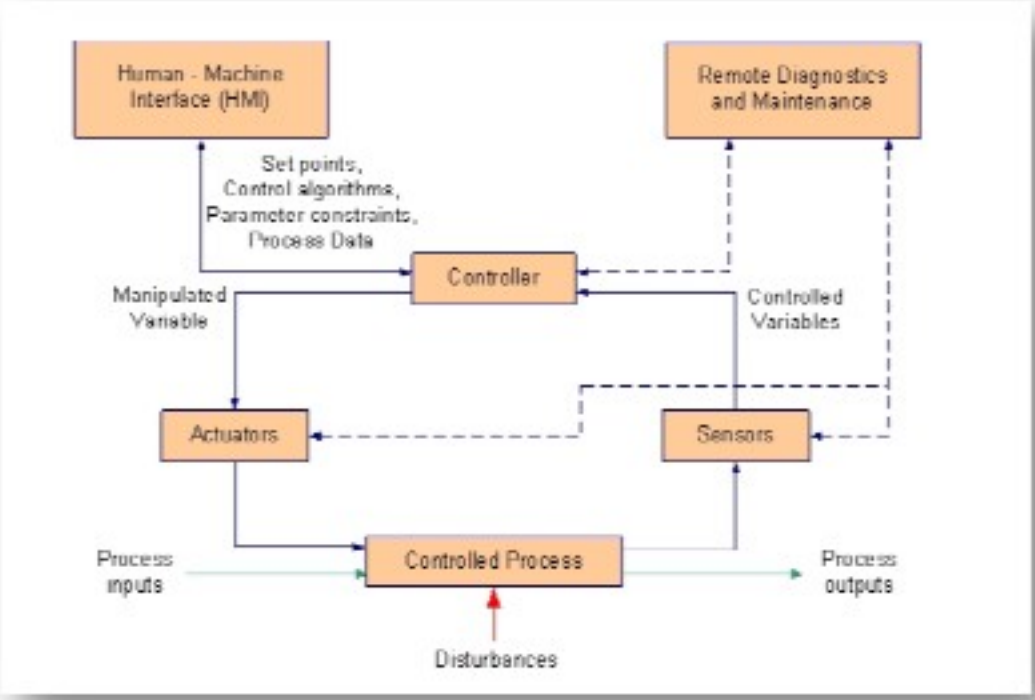


Figure I.2 : Fonctionnement d'un ICS. [9]

I.3.4. Les composantes d'un ICS

I.3.4.1. Composants de contrôle

Dans ce qui suit on a présenté la liste des composants majeurs de contrôle d'un ICS:

- **Serveur de contrôle:** Le serveur de contrôle héberge le logiciel de supervision de contrôle du DCS ou de l'API conçu pour communiquer avec les dispositifs de contrôle du niveau inférieur. Le contrôle a un accès au module de contrôle subordonné suivant le réseau de l'ICS.

- **Serveur SCADA, Unité Terminale Maîtresse (UTM):** ou Master Terminal Unit (MTU), le serveur SCADA est un dispositif qui agit comme étant maître dans le système SCADA. Les dispositifs RTU et API (décrits plus bas) se situent sur les sites de terrain à distance et agissent généralement comme esclaves.

- **Remote Terminal Unit (RTU):** L'RTU ou Unité terminale distante, aussi appelée Remote Telemetry Unit, est une unité dont la fonction spéciale est le contrôle et l'acquisition de données, conçue afin de soutenir les stations SCADA à distance. Les RTU sont des dispositifs de terrain souvent équipés d'une interface radio sans fil afin de rester fonctionnel dans le cas où les connexions câblées sont impossibles. Parfois, les API sont implémentées comme étant des dispositifs de terrain jouant le rôle d'un RTU.

- **Automates Programmables Industriels(API):** L'API est un petit ordinateur industriel conçu à l'origine pour effectuer les fonctions logiques exécutées par du matériel électrique (Relais, commutateurs de batteries, compteurs/minuteurs mécaniques). Les APIs ont évolué vers le statut de contrôleur avec la capacité de contrôler des processus complexes et sont essentiellement utilisés dans les systèmes SCADA et DCS. Les autres contrôleurs utilisés au niveau du terrain sont des contrôleurs de processus et RTU. Ils fournissent le même contrôle que l'API mais sont conçu pour des applications de contrôleurs spécifiques. Dans les environnements SCADA, l'API est souvent utilisé comme dispositif de terrain car ils sont plus économiques, versatiles, flexibles et configurable qu'un RTU à usage spécial.

- **Dispositifs Electronique Intelligents (DEI):** Ou Intelligent Electronic Devices (IED), les DEI sont des capteurs/actionneurs intelligents, contenant l'intelligence requise afin d'acquérir des données, les communiquer à d'autres dispositifs, et effectuer le contrôle et le traitement local. Un DEI pourrait combiner entre un capteur d'entrée analogique, sortie analogique, capacité de contrôle du niveau-inférieur, un système de communication et la mémoire de programme dans un seul dispositif. L'utilisation des DEI dans les systèmes SCADA et DCS permet d'avoir un contrôle automatique au niveau local.

- **Interface Homme-Machine (IHM):** ou Human-Machine Interface (HMI) est à la fois logiciel et matériel qui permet à l'opérateur humain de surveiller l'état du processus contrôlé, modifier les paramètres afin de changer l'objectif de contrôle et manuellement outrepasser les opérations de contrôle automatique dans le cas d'une urgence. L'HMI permet aussi à l'ingénieur de contrôle ou à l'opérateur de configurer les consignes et algorithmes de contrôle. Elle affiche les informations concernant l'état du processus, l'historique d'informations, rapports et autres aux opérateurs, administrateurs, manageur, partenaires et autres utilisateurs autorisés. L'emplacement, la plate-forme, et l'interface peuvent énormément varier. Par exemple, une HMI pourrait être une plate-forme dédiée au centre de contrôle, un ordinateur portable sur un réseau local sans fil ou un navigateur sur tout système connecté à Internet.

- **L'historique de données (Data Historian) :** L'historique de données est une base de données centralisée pour la connexion de toutes les informations de processus au sein d'un ICS. Les informations stockées dans cette base de données sont accessibles pour la réalisation de diverses analyses, de contrôle statistique du processus de planification à l'échelle de l'entreprise.

- **Serveur Entrée/Sortie(E/S):** Le serveur IO est un composant de contrôle responsable de la collecte, mise en mémoire tampon et autorisation d'accès aux informations de processus des sous-composants de contrôle tels que les automates, RTU et IED. Un serveur IO peut résider sur le serveur de commande ou sur une plate-forme informatique distincte. Les serveurs IO sont également utilisés pour l'interfaçage des composants de contrôle de tiers, comme un opérateur et un serveur de contrôle.

I.3.4 .2. Composants réseau

Il existe différents type de caractéristiques réseaux pour chaque couche, dans la hiérarchie d'un système de contrôle. La topologie des réseaux parmi les différentes implémentations des ICS vari avec les systèmes modernes utilisant les systèmes IT (information technology) basées sur internet et les stratégies d'intégration de l'entreprise. Les réseaux de contrôle ont émergé avec les réseaux informatiques afin de permettre aux ingénieurs de surveiller et contrôler des systèmes d'en dehors du réseau du système de contrôle. La connexion pourrait également permettre au niveau de l'entreprise (Entreprise-Level) c'est à dire les décideurs d'obtenir un accès pour le traitement de données. La liste suivante regroupe les composants majeurs des réseaux d'un ICS, indépendamment des topologies de réseau utilisées:

- **Réseau du bus de terrain (Fieldbus Network):** Le réseau du bus de terrain relie les capteurs et autres dispositif à un API ou bien à un autre contrôleur. L'utilisation de la technologie du bus de terrain élimine le besoin à un câblage point-à-point entre le contrôleur et chacun des dispositifs. Les capteurs communiquent avec le contrôleur du bus de terrain utilisant un protocole spécifique. Le message envoyé entre les capteurs et le contrôleur s'identifie comme étant unique et propre à chacun des capteurs.

- **Réseau de contrôle (Control Network):** Le réseau de contrôle connecte le niveau de supervision de contrôle (Supervisory control level) au module de contrôle de niveau inférieur (Lower-level control modules.)

- **Routeurs de communication:** Un routeur est un dispositif de communications qui transfert les messages entre deux réseaux. Les utilisations commune d'un routeur peuvent inclure la connexion d'un LAN (Local Area Network) à un WAN (Wide area Network), et connectant MTUs (Master Terminal Unit) et RTUs (Remote Terminal Units) à un support de réseau à grande distance pour la communication SCADA.

- **Pare-feu (Firewall):** Un pare-feu protège les dispositifs sur un réseau en surveillant et contrôlant les paquets de communication utilisant des politiques de filtrage prédéfinies. Les pare-feu sont également utiles dans la gestion de stratégies de ségrégation de réseau ICS.

- **Modems:** Un modem est dispositif qui convertit des données numériques de série et un signale approprié pour la transmission à travers une ligne téléphonique afin de permettre aux dispositifs de communiquer. Les modems sont souvent utilisés dans les systèmes SCADA afin de permettre les communications en série de longue distance entre les MTUs et les dispositifs de terrain distants. Sont aussi utilisés dans les systèmes SCADA, DCSs et APIs pour gagner en accès à distance pour les fonctions opérationnelle, par exemple pouvoir entrer une commande, modifier des paramètres ou à des butes de diagnostiques.

- **Points d'accès à distance (Remote Access points):** Sont des dispositifs distincts, des zones et des emplacements afin de pouvoir configurer un système de contrôle et avoir accès aux données de processus à distance. On pourrait citer comme exemple l'utilisation d'un PDA (Personal digital assistant) afin d'avoir accès aux données sur un réseau local via un point d'accès sans fil, ou bien en utilisant un lap top et une connexion modem afin d'avoir accès à un ICS à distance.

I.4. Systèmes Informatiques (IT systems)

L'informatique est un domaine d'activité scientifique, technique et industriel concernant le traitement automatique de l'information par l'exécution de programmes informatiques par des machines : des systèmes embarqués, des ordinateurs, des robots, des automates, etc.

Ces champs d'application peuvent être séparés en deux branches, l'une, de nature théorique, qui concerne la définition de concepts et modèles, et l'autre, de nature pratique, qui s'intéresse aux techniques concrètes de mise en œuvre. Certains domaines de l'informatique peuvent être très abstraits, comme la complexité algorithmique, et d'autres peuvent être plus proches d'un public profane. Ainsi, la théorie des langages demeure un domaine davantage accessible aux professionnels formés (description des ordinateurs et méthodes de programmation), tandis que les métiers liés aux interfaces homme-machine sont accessibles à un plus large public.

Protocoles de communications

Dans les réseaux informatiques et les télécommunications, un protocole de communication est une spécification de plusieurs règles pour un type de communication particulier.

Initialement, on nommait protocole ce qui est utilisé pour communiquer sur une même couche d'abstraction entre deux machines différentes. Par extension de langage, on utilise parfois ce mot aussi aujourd'hui pour désigner les règles de communication entre deux couches sur une même machine.

Les protocoles de communication les plus utilisés sont les protocoles réseau.

Concept

Communiquer consiste à transmettre des informations, mais tant que les interlocuteurs ne lui ont pas attribué un sens, il ne s'agit que de données et pas d'informations. Les interlocuteurs doivent donc non seulement parler un langage commun mais aussi maîtriser des règles minimales d'émission et de réception des données. C'est le rôle d'un protocole de s'assurer de tout cela.

Les protocoles peuvent être réparties en plusieurs couches, citons quelques exemples de différents protocoles de plusieurs couches :

- TCP/IP ;
- Ethernet/IP ;

I.5. SCADA (Supervisory Control And Data Aquisition)

Figure I.3 : Exemple d'une salle de contrôle SCADA réalisé par la firme « RGB spectrum » [12]

Les premiers systèmes SCADA sont apparus dans les années 1960. Pour la première fois il devenait possible d'actionner une commande de terrain (une vanne par exemple) depuis un centre de contrôle à distance, plutôt que par une intervention manuelle sur site. Aujourd'hui, les dispositifs SCADA ont intégré de nombreuses avancées technologiques (réseaux, électronique, informatique...) et sont devenus omniprésents sur les installations à caractère industriel. De ce fait, leur fiabilité et leur protection sont également devenues des enjeux importants.

Un système de contrôle et d'acquisition de données (anglais : Supervisory Control And Data Acquisition, sigle : SCADA) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.

Les systèmes SCADA sont grandement distribués, utilisés dans le contrôle d'atouts et actifs distribués géographiquement (de l'ordre du millier de km²) où la centralisation de l'acquisition de donnée et le contrôle sont des éléments critiques.

L'acquisition de données étant intégrée, un système de transmission de données et des

logiciels HMI qui fournissent une surveillance centralisée mais aussi le contrôle d'un grand nombre d'E/S (inputs/outputs).

I.5.1. Fonctionnement

Le système SCADA effectue de la surveillance centralisée et le contrôle des sites, grâce à des réseaux de communication de longue-distance, incluant la surveillance d'alarmes et le traitement des données des états.

Il peut être désigné pour la récolte de l'information sur terrain, son transfert à l'installation d'ordinateur centrale et l'affichage des informations à l'opérateur de façon graphique ou textuelle, puis permet à ce dernier de surveiller ou contrôler un système tout entier de l'emplacement de la centrale.

Le dispositif SCADA n'a pas vocation à se substituer entièrement à l'homme : le pilotage et la prise de décision restent dévolus à l'opérateur. C'est pourquoi les logiciels SCADA sont fortement dédiés à la surveillance et aux alarmes.

Le système SCADA inséré à la cimenterie, dans le contrôle du refroidissement du clinker:

- Permet à un opérateur de modifier la consigne d'écoulement (flux d'air froid dans le refroidisseur)
- Enregistre et affiche l'évolution des mesures (débit, température etc.) ;
- Détecte et affiche des conditions d'alarme (température clinker élevée etc.) ;

Exemples d'utilisation

On trouve par exemple des systèmes SCADA dans les contextes suivants :

- Surveillance de processus industriels ;
- Transport de produits chimiques ;
- Systèmes municipaux d'approvisionnement en eau ;
- Commande de la production d'énergie électrique ;
- Distribution électrique ;
- Canalisations de gaz et de pétrole ;
- Réseaux de chaleur ;
- Recherche et études scientifiques et industrielles ;

I.5.2. Architectures SCADA

Les différents types d'architectures utilisées sont les suivantes: point-to-point, series, series-star, et multi-drop. Point-to-point est la plus simple mais la plus couteuse à cause de la nécessité d'un Canal individuel pour chaque connexion

. La **Figure I.3** représente l'architecture réseau globale d'une implémentation SCADA avec l'exposition de ses différents composants et réseau.

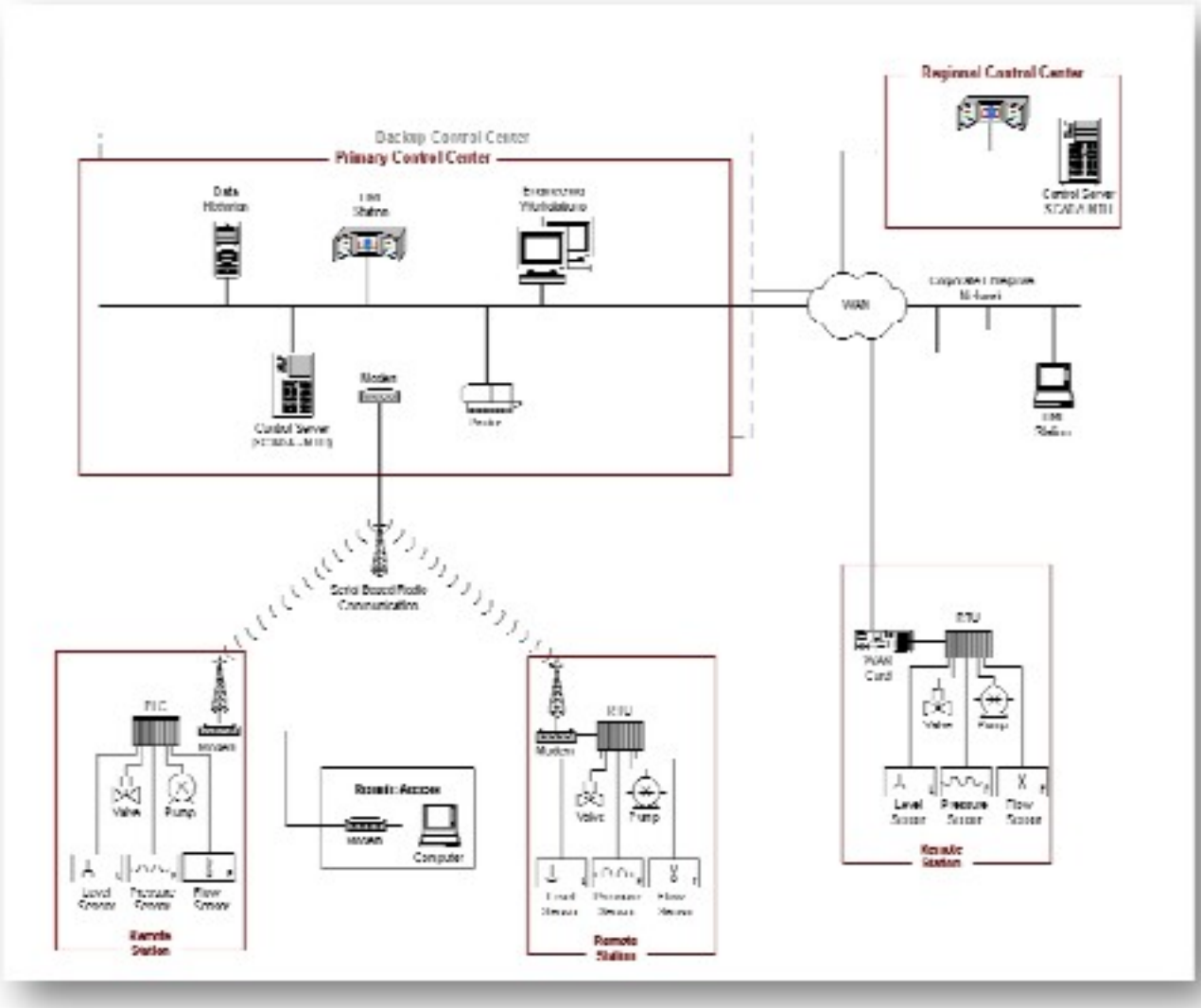


Figure I.4: Un exemple d'implémentation d'un système SCADA (Contrôle et surveillance distribuées). [9]

En conclusion: Les systèmes SCADA sont généralement conçus afin d'être des systèmes tolérant la panne avec une redondance importante construite dans l'architecture du système.

I.6. DCS (Distributed Control Systems)

Figure I.5 : Salle de contrôle DCS réalisée par la firme « Yokogawa » [13

Un système de commande réparti (DCS) ou SNCC (système numérique de commande et de contrôle) est un système de commande d'un processus ou d'une installation, dans lequel les éléments de commande sont répartis dans l'ensemble du système. Ceci est en contraste avec les systèmes non distribués, qui utilisent un seul contrôleur à un emplacement central ou salle de contrôle. Dans un DCS, une hiérarchie de contrôleurs est reliée par des réseaux de communication de commande et de contrôle.

Un DCS utilise généralement des processeurs conçus sur mesure en tant que contrôleurs et utilise les deux interconnexions propriétaires et protocole de communication standard pour la communication. Les modules d'entrée et de sortie constituent des parties constitutives du DCS. Le processeur reçoit des informations provenant des modules d'entrée et envoie des informations aux modules de sortie. Les modules d'entrée reçoivent des informations provenant des instruments d'entrée dans le procédé (ou champ) et les modules de sortie transmettent des instructions aux instruments de sortie dans le domaine. Les entrées et sorties peuvent être soit un signal analogique en constante variation ou signaux discrets qui ont 2 états Tout Ou Rien (TOR). Bus informatiques ou des bus électriques relient le processeur et les modules. Des bus relient également les contrôleurs distribués avec le contrôleur central et enfin à l'interface homme-machine (IHM) ou consoles de contrôle.

Les éléments d'un DCS peuvent se connecter directement à l'équipement physique tel que commutateurs, pompes et vannes et d'interface homme-machine (IHM) via SCADA. Les différences entre un DCS et SCADA sont souvent subtiles, surtout avec les progrès de la technologie permettant la fonctionnalité de chacun d'évoluer et de grandement s'élargir. L'avantage de ces systèmes est leur modularité, qui permet de les installer et de les modifier facilement.

Parmi les constructeurs de SNCC on peut citer: ABB, Emerson, Foxboro, Honeywell, Rockwell, Siemens, Yokogawa. Les DCS sont utilisé pour contrôler les systèmes de production dans la même zone géographique, se trouvant dans les industries suivantes:

- Les usines chimiques
- Pétrochimiques (pétrole) et les raffineries
- Pâtes et papiers
- Centrales nucléaires
- Systèmes de contrôle de l'environnement
- Systèmes de gestion de l'eau
- Usines de traitement métallurgiques
- Fabrication de produits pharmaceutiques
- Usines de raffinage de sucre
- Marchandises sèches en vrac et les navires de transport de l'huile

En modularisant le système de production, le DCS réduit l'impacte de la simple erreur sur tout le système. Dans la plupart des systèmes, le DCS est interfacé avec le réseau de l'entreprise afin de donner aux chargés des opérations une vue globale de production.

I.6.1 Architecture

La **Figure I.6** démontre les composantes et la configuration générale d'un DCS.

Ce DCS englobe tout un établissement, du plus bas niveau (processus de production) jusqu'au niveau (couche) d'entreprise. Dans cet exemple, un contrôleur de supervision (Control server) communique avec ses subordonnés à l'aide du réseau de contrôle. Le superviseur envoie des consignes et demandes directement les données au niveau des contrôleurs de terrain distribués. Les contrôleurs distribués contrôlent les actionneurs de leur processus se basant sur les commandes du serveur de contrôle et les feedback des capteurs.

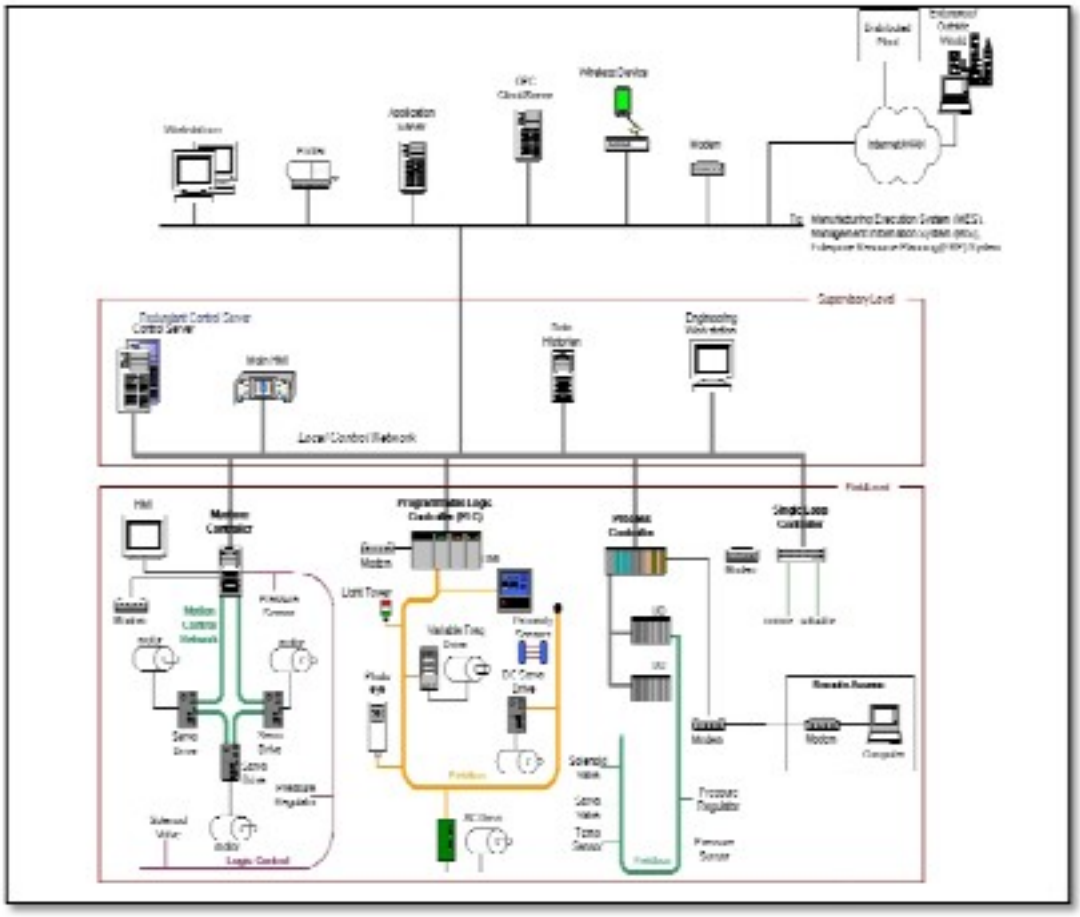


Figure I.6 : Composants et configuration générale d'un DCS. [9]

Cette figure est un exemple des contrôleurs de bas-niveau (Low-Lever controllers) pouvant se trouver sur un système DCS. Les dispositifs de control de terrain (Field control devices) démontrés pourraient être représentés par: un API, un contrôleur de processus, un contrôleur de boucle unique mais aussi un contrôleur de machine. Le contrôleur de boucle unique (Single loop controller) interface capteurs et actionneurs utilisant le câblage point à point. (Point to point wiring.) Pendant que les trois (03) autres dispositifs de terrain intègrent le réseau de bus de terrain afin d'être interfacer avec les capteurs et actionneurs du processus. Le réseau de bus de terrain élimine le besoin d'un câblage point à point entre un contrôleur et un unique capteur ou actionneur de terrain. Ajoutons que le bus de terrain permet beaucoup plus de fonctionnalités au-delà de celle du control, incluant les dispositifs de diagnostique de terrain, pouvant accomplir des algorithmes de contrôle dans le bus de terrain, ainsi éviter le routage du signale vers l'API à chaque opération de contrôle. Les normes de protocole de communication industrielle ont été conçu par groupe industriel tel que Modbus et FieldBus et sont très souvent utilisé dans les réseaux de contrôle et de bus de terrain.

1.6.2. Gestion des niveaux de commande

En plus des boucles de contrôle du niveau de supervision (Supervisory-Level) et le niveau de terrain (Field-Level), des niveaux de contrôle intermédiaires peuvent aussi exister. Par exemple, dans le cas d'un DCS contrôlant la partie discrète d'une unité de production, il pourrait y avoir un niveau de supervision intermédiaire pour chaque cellule au niveau de l'installation. Ce superviseur englobera une cellule de fabrication, contenant un contrôleur de machine qui traite une partie et un robot contrôleur qui gère les stocks de matière brute et le produit final. Il pourrait y avoir un certain nombre de ces cellules qui pourrait gérer les contrôleurs du niveau de terrain (Field-Level) sous la supervision de la boucle de contrôle du DCS.

I.7. Comparatif DCS et SCADA

Le **Tableau I.1** expose les grands points de différences entre les deux type de systèmes SCADA et DCS

Systèmes SCADA	Systèmes DCS
-Surveillance de processus distribués sur une grande zone géographique. -Intelligence distribuée permet le contrôle et la surveillance continue même quand la communication avec la salle de contrôle est coupée. (compromise.) -Orienté acquisition de données. (Data gathering) -Se concentre généralement sur le centre de contrôle mais aussi sur les opérations. -Peu importe quand la communication de terrain échoue, SCADA doit opérer raisonnablement.	-Se concentre grandement sur les évènements locaux. -Ne peut supporter temporairement des coupures de communications. -Orienté processus. -Se concentre et scanne le processus contrôlé que se soit sur une installation chimique ou autre puis présente l'information à l'opérateur. -Une station opérateur DCS est généralement connectée à ses E/S avec un câblage local, réseaux et bus de terrain (FieldBus). -L'opérateur fait une demande directement aux E/S terrains peu importe quand il a

-La principale préoccupation du fonctionnement du système SCADA est la qualité des données affichées à l'opérateur.	besoin d'information et reçoit une réponse, ceci veut dire que les évènements de terrain peuvent perturber le système et annuler l'opérateur.
-Ces systèmes suivent plutôt les évènements des processus.	-Système DCS est préoccupé par les tendances de processus.
-Maintien une base de données des dernières bonnes valeurs et sécurise les données peu importe quand il y a problème de communication ce qui le rend très rapide pour l'affichage à l'opérateur en cas d'urgence, gère la redondance d'une manière répartie.	-Ne garde pas de base de données étant donné qu'il est toujours connecté à sa source. -Dans le cas de redondance, des équipements parallèles prennent cela en main.
-Les boucles fermées sont indisponibles au niveau des systèmes SCADA mais on peut avoir accès au contrôle à travers l'HMI avec l'homme comme étant superviseur.	-L'opérateur a des boucles fermées de contrôle au niveau des API/RTU. -Tous els systèmes DCS d'aujourd'hui ont des HMI intégré et des installations de supervisions, connexions aux bases de données (data base) mais aussi avec toutes les installations basiques fournis dans un SCADA.

Tableau I.1 : Comparative SCADA/DCS

En contre partie à toutes les différences citées plus haut, la plupart des systèmes SCADA et DCS d'aujourd'hui sont accompagnés des mêmes normes d'installation, évènements, archivage, HMI, rapports, gestion de base de données et connexions, le contrôle à distance de la salle de contrôle.

La solution offerte par les deux systèmes dépend des besoins des clients et peut être personnalisée afin de répondre aux solutions attendus.

I.8. Conclusion

Ce chapitre représente une introduction aux différents systèmes de contrôle industriel, leurs composants et leurs fonctionnements, afin de mieux comprendre les vulnérabilités qui y sont liées, qui seront l'objet du chapitre suivant.

Chapitre II:

Vulnérabilités des systèmes de contrôle industriels

II.1. Introduction

Afin de faciliter la conception de la nouvelle solution d'automatisation et de cyber-sécurité, il est impératif de comprendre les vulnérabilités liées aux systèmes de contrôle de façon générale et les risques encourus.

II.2. Comparatif ICS (Industrial Control Systems) et IT (Information Technology)

Initialement, les ICS avaient très peu de ressemblance avec les systèmes IT, où les ICS étaient des systèmes isolés fonctionnant sous un protocole de contrôle propriétaire utilisant du matériel et logiciels (Hardware/software) spécialisé.

Grandement disponibles, les dispositifs IP (Internet Protocol) à bas coût (Low-cost) sont entrain de remplacer les solutions propriétaires ce qui augmente la possibilité d'avoir des vulnérabilités et incidents de cyber sécurité.

Les ICS sont entrain d'adopter des solutions informatique (IT) afin de promouvoir la connectivité d'entreprise et les capacités d'accès à distance ; sont maintenant aussi, conçus et implémentés utilisant des ordinateurs d'industries standard, systèmes d'exploitation (OS) et protocoles de réseaux ce qui le rends de plus en plus ressemblant aux systèmes I.T.

Cette intégration supporte de nouvelles capacités IT mais fournie de façon considérable une isolation beaucoup moins importante des ICS du monde extérieur en comparaison avec les ICS précédents, créant ainsi le grand besoin de les sécuriser d'avantage.

Pendant que des solutions sécuritaires ont été conçues pour les problèmes dans les systèmes IT typiques, des précautions particulières doivent être prises en proposant ces mêmes solutions à l'environnement des ICS. Dans certains cas, de nouvelles solutions de sécurité sont requises afin qu'elles soient adaptées à l'environnement ICS.

Les ICS possèdent un grand nombre de caractéristiques qui différèrent de ceux des systèmes IT traditionnels, incluant des risques et priorités totalement différentes. Parmi cela, citons un risque considérable à la santé et la sécurité des vies humaines, dégâts et dommages considérables à l'environnement, soucis financiers comme la perte de production, impactes négatifs sur l'économie de toute une nation mais aussi pouvant compromettre des informations propriétaires et confidentielles.

Les ICS ont des conditions de performances et de fiabilités différentes, utilisant des systèmes d'exploitation (OS) et applications pouvant être considérées comme –non-conventionnelle par rapport au personnel IT typiques.

Les buts de sécurité et d'efficacité peuvent parfois entrer en conflit avec la sécurité dans la conception et le fonctionnement des systèmes de contrôle. Exemple : La nécessité d'une authentification et autorisation par mot-de-passe ne devrait certainement pas entraver les actions en cas d'urgence au niveau des ICS.

Voici une liste des considérations particulières lors de l'examen de sécurités des ICS :

- ***Les exigences de performances***

Les ICS sont généralement à temps critique, le délai n'est donc pas acceptable pour la diffusion de l'information, le haut débit n'est généralement pas indispensable.

En contraste, les systèmes IT requièrent essentiellement du haut-débit mais peuvent supporter des niveaux substantiels de retards et de délai. Les ICS doivent présenter des réponses déterministes

- ***Exigences de disponibilité***

La plupart des processus des ICS sont de natures continues, les interruptions de services/coupures de courant du système qui contrôle les processus industriels ne sont pas acceptables.

Les tests de pré-déploiement exhaustif sont nécessaires afin d'assurer une grande disponibilité des ICS.

La plupart des systèmes de contrôles ne peuvent-être ARRÊTER et DEMARRER sans en affecter la production, dans certains cas le produit en cours de production ou l'équipement entrain d'être utiliser est plus important que l'information transmise ; donc dans ce cas l'utilisation de stratégies typiques d'un systèmes IT comme le redémarrage (reboot) d'un composant n'est donc pas acceptable à cause de l'impacte sur les conditions de grande disponibilité, fiabilité et maintenabilité du ICS.

- ***Les exigences en matière de gestion de risques***

Dans un système informatique (IT) typique, la préoccupation primaire est la confidentialité et l'intégralité des données.

Pour un ICS, les préoccupations primaires sont la sûreté humaine et la tolérance de faute et d'erreur afin d'éviter et prévenir les pertes de vie ou même la mise en danger de la sécurité publique, la perte d'équipement, la perte de propriété intellectuelle ou bien de produits perdus ou endommagés.

Le personnel responsable du fonctionnement, de la sécurisation et de l'entretien de l'ICS doit comprendre le lien entre sûreté et sécurité.

- ***Mise au point de la sécurité de l'architecture***

Dans les systèmes informatiques (IT) typiques, l'objectif principal de la sécurité est de protéger les actifs informatiques (IT asset), qu'ils soient centralisés ou distribués, et les informations qui y sont stockées.

Dans certaines architectures, l'information stockée et traitée centralement est plus critique et lui est accordée plus de protection.

En ce qui concerne les ICS, les clients de bord (API, station opérateur, contrôleur, DCS…) doivent-être soigneusement protégé du moment qu'ils sont responsables du contrôle des procédés finaux.

La protection du serveur centrale est tout aussi importante car ce dernier pourrait éventuellement avoir un impact très négatif sur les dispositifs de bord.

- ***Conséquences inattendues***

Les ICS (ou Système de Contrôle Industriels : SCI) ont des interactions très complexe avec le processus physique et les conséquences peuvent se manifester par des évènements physiques.

Toutes les fonctions de sécurité intégrées aux ICS doivent-être testé afin de confirmer quelle ne compromettront aucunement les fonctionnalités d'un ICS normal.

- ***Les réponses à temps critiques***

Dans un système IT typique, le contrôle d'accès peut-être mis en œuvre sans regard significatif sur le flux de données.

Pour certains ICS, les temps de réponses automatisées ou la réponse du système à une interaction humaine sont critiques.

Le flux de données et d'informations ne devrait surtout pas être interrompu ou corrompu.

L'accès à ces systèmes devrait être restreint et limité par des contrôles de sécurité très rigoureux.

- ***Le fonctionnement du système***

Les systèmes d'exploitation (OS) et applications des ICS ne peuvent tolérer des pratiques typiques de sécurités des systèmes IT.

Les anciens systèmes sont particulièrement vulnérables à l'indisponibilité de ressources et à la perturbation de timing et de cadencement.

Les réseaux de contrôle sont plus souvent complexes et nécessitent un niveau d'expertise différent. Exemple : Les réseaux de contrôle sont spécialement gérés par des Ingénieurs de contrôle et non des Informaticiens. (Personnel IT)

- ***Exigences et contraintes de ressources***

Les ICS et leur OS en temps sont souvent des systèmes à ressources contrainte qui n'incluent souvent pas les capacités sécuritaires typiques d'un système IT.

Il se peut qu'il n'y ait pas les ressources informatiques nécessaires afin de moderniser ces systèmes avec les capacités sécuritaires actuelles.

Dans certains cas, les solutions sécuritaires d'une tierce partie ne sont pas autorisées à cause des accords de licences des fournisseurs et la perte des services de dépannage et soutien pourrait arriver si la tierce partie se voit installée.

- ***Les communications***

Les protocoles de communication et média utilisés par les environnements des ICS pour le contrôle des appareils et dispositifs de terrain et la communication intra-processeur sont typiquement et généralement différentes de l'environnement informatique (IT) de base, et peuvent-être propriétaires.

- ***La gestion du changement***

La gestion du changement primordiale afin de maintenir l'intégrité des IT et des ICS. Les systèmes non-à-jour sont les plus vulnérables. Les mises-à-jour (MAJ) logicielles sur un système IT, y compris les correctifs de sécurité sont généralement appliquées en temps voulu en se basant sur les politiques et procédures de sécurité appropriées, ces procédures sont souvent automatiques et utilisent les outils serveurs. Les MAJ logicielles des ICS ne peuvent pas toujours être mise en œuvre en temps voulu, car ces MAJ doivent-être minutieusement testées par le fournisseur d'application de contrôle industriel et l'utilisateur final avant d'être implémentées, les arrêts des ICS doivent-être programmés des jours voir semaines à l'avance. Les ICS peuvent aussi nécessités une revalidation dans le cadre du processus de MAJ.

La gestion de changement est aussi applicable aux matériels et aux microprogrammes.

Le processus de gestion de changement appliqué aux ICS requiert un examen minutieux par des experts en ICS travaillant en conjonction avec le personnel IT.

- ***La gestion du support***

Les systèmes IT typiques permettent une diversification dans le style de supporter, peut-être afin de soutenir des architectures technologiques interconnectées mais complètement différentes.

Pour les ICS, le service support se fait essentiellement par un unique fournisseur, ne proposant pas des solutions de support diversifiées et interopérables par un autre fournisseur.

- ***Durée de vie des composants***

Les composants IT ont une durée de vie de 3-5 années avec brièveté due à l'évolution rapide de la technologie.

Pour les ICS, où la technologie a été développée dans différents cas pour des utilisations et implémentations spécifiques, la durée de vie d'une technologie mise en place est souvent de l'ordre de 15-20 ans et parfois plus.

- ***L'accès aux composants***

Les composants IT sont souvent au niveau local et facilement accessible.

Pour les ICS, les composants peuvent-être installés à distance et nécessitent des efforts physiques pour y accéder.

En résumé, les différences opérationnelles et des risques entre les ICS et les systèmes IT créent la nécessité d'accroitre la sophistication dans l'application de la cyber-sécurité et les stratégies opérationnelles.

Les ressources informatiques des ICS (CPU, RAM…) tendent à être limitées car ces systèmes ont été conçus afin de maximiser les ressources des systèmes de contrôle avec pratiquement aucun extra capacitaires pour une tierce partie de solution de cyber-sécurité.

En addition, dans certain cas les tierces parties des solutions de sécurité ne sont pas autorisées à cause d'une licence agrée du fournisseur, leur installations peuvent causer la perte du service support et dépannage du fournisseur.

La cyber-sécurité IT et l'expertise des systèmes de contrôle ne sont pas retrouvées dans le même groupe de personne. Une équipe inter fonctionnelle d'Ingénieurs de contrôle et professionnels IT a besoin de travailler en étroite collaboration afin de comprendre les conséquences possibles de l'installation, l'exploitation et la maintenance des solutions de sécurité en liaison avec le fonctionnement du système de contrôle.

Les professionnels IT travaillant sur les ICS doivent comprendre les impactes de fiabilité des technologies de sécurité de l'information avant tout déploiement.

Certains systèmes d'exploitation (OS) et applications fonctionnant sur ICS peuvent ne pas fonctionner avec les solutions improvisées de cyber-sécurité de l'IT à cause de l'environnement de l'architecture spécialisée de l'ICS.

II.3. Les menaces: Agents de menaces et définitions

Les menaces à l'encontre des systèmes de contrôle peuvent venir de différentes sources, notamment de gouvernement hostiles, de groupes terroristes, d'espions industriels, d'employés mécontents, intrus malveillants et de sources naturelles comme la complexité du système, erreurs humaines et accidents, échec d'équipement et catastrophes naturelles.

Afin de se protéger des menaces naturelles ou provenant de la concurrence, il est primordiales et nécessaire de créer une stratégie de défense approfondie pour l'ICS.

Agents de menace

La liste suivante regroupe les menaces possibles à l'encontre des ICS :

- **Les attaquants**

Pénètrent dans le réseau le plus souvent pour le plaisir du challenge ou à des fins financières. Il fût un temps où le hacking à distance nécessitait un certain amont considérable de connaissances, aujourd'hui ça n'est plus le cas, les attaquants peuvent maintenant télécharger des scripts d'attaque (Attack scripts) et protocoles d'internet et les lancer contre le site web de leurs victimes. Même si les outils d'attaques deviennent de plus en plus sophistiqués, ils en deviennent bien plus faciles à utiliser. Même si la plupart de ces attaquants n'ont pas d'expertise requise afin de menacer des cibles difficiles la plupart de ces derniers, avec les courtes coupures pouvant être provoquées sur les cibles isolées, représentent une très grande menace pouvant provoquer des dégâts considérables.

- **Opérateurs BOT de réseau (BOT-NETWORK)**

Représentant aussi des attaquants mais à la place de pénétrer à l'intérieur des systèmes, prenant le contrôle de plusieurs serveurs afin de coordonner une attaque et distribuer spam et attaque de logiciels malveillant.

- **Groupes criminels**

Attaquant le système à des fins d'argent de façon plus spécifique, les groupes criminels organisés utilisent les spam, hameçonnage et les logiciels Espions/Malveillants (Spyware/malware) afin de procéder à des vols d'identité et les fraudes en ligne.

Les espions d'entreprises internationales et les organisations de crime représentent aussi une menace à tout un pays à travers leur capacité à gérer et procéder à l'espionnage industriel et le détournement de fonds à grandes échelle afin d'embaucher les hackers talentueux.

- **Les intrus/éléments internes**

Les intrus mécontent sont une source de crime informatique, ces derniers n'ont pas grand besoin de connaissance sur le hacking car leur connaissance du système cible leur permet très souvent de réussir à obtenir des accès afin de causer certains dommage et dégâts au système ou bien voler des informations et données système. Ces éléments peuvent aussi inclure les fournisseurs proches ou même les employés pouvant accidentellement introduire un logiciel malveillant dans les systèmes. Les procédures, politiques et tests inadéquats peuvent et vont causer un gros impacte sur l'ICS.

La classification de ces impactes passent des plus insignifiants aux signifiant/voir catastrophiques à l'ICS et aux dispositifs de terrain. Les impactes non-intentionnels des insiders (des éléments internes.) représentent les plus grandes probabilités d'occurrence.

- **Le hameçonnage**

Représente des individus et de petits groupes exécutant des procédures d'hameçonnage afin de tenter le vol d'identités ou d'informations contre une rémunération monétaire.

Ils peuvent aussi avoir recourt aux spam et aux logiciels espions/malveillant afin d'accomplir leur objectifs.

- **Les Spammeurs**

Sont des individus ou de petits groupes qui distribuent des e-mail/courriels avec des informations cachées ou bien de fausses informations pour la vente de faux produits conduisant des procédure d'hameçonnage, distribuant des logiciels espions et malveillants ou attaques directes aux organisation (DoS/DDOS : Denial of service / Direct Denial of SERVICE [ang])

- **Les auteurs de logiciels espions et malveillants**

Ce sont des individus et organisations avec de mauvaises intentions, mettant en scène des attaques contre des utilisateurs en produisant et distribuant des logiciels espions et

malveillants. Un grand nombre de virus et ver informatiques destructeurs ont atteint et endommagés fichiers et disques dur.

II.4. Les vulnérabilités potentielles des ICS

Cette partie énumère les vulnérabilités qui pourraient se trouver au niveau d'un ICS typique. L'ordre suivant lequel ces vulnérabilités sont classées ne reflète aucune priorité d'occurrence et de l'impacte de sécurité.

Les vulnérabilités sont classées suivant les groupes suivants :

a) Vulnérabilités des politiques et procédures.
b) Vulnérabilités par plateformes.
c) Vulnérabilités des réseaux.

a. Vulnérabilités des politiques et procédures

Les vulnérabilités sont introduites dans l'ICS à cause de la documentation de sécurité qui est souvent incomplète, inappropriées ou inexistante, incluant les grandes procédures d'implémentation.

La documentation de sécurité avec le support de gestion représentent le noyau de n'importe quel programme de sécurité.

Les politiques de sécurité de l'entreprise peuvent réduire les vulnérabilités de façon considérable en mandatant la conduite comme les mot-de-passe d'usages ou de maintenances, conditions et exigence pour connecter les modems aux ICS, etc.

Liste des vulnérabilités et leur description :

1- ***Politiques de sécurité inadéquates pour l'ICS :*** Les vulnérabilités sont souvent introduites au niveau des ICS à cause de politiques inadéquates ou un manque de politiques tout particulièrement concernant la sécurité des systèmes de contrôle.

2- ***Absence de formation de sécurité des ICS et de programme de sensibilisation :*** Une formation et documentation formelle et un programme de sensibilisation sont conçues afin de permettre au staff de rester à jour sur les politiques organisationnelles de sécurité et les procédures ainsi que les normes en matière de cyber-sécurité de l'industrie et les meilleurs pratiques.
Sans formation sur les procédures et politiques des ICS adéquates, le staff/personnel ne pourra maintenir un environnement sécurisé de l'ICS.

3- ***Sécurité de l'architecture et la conception inadéquates :*** Les Ingénieurs de contrôle et automaticiens n'ont jusqu'à maintenant eu aucune formation concernant la sécurité et même jusqu'à très récemment où les fournisseurs n'incluaient toujours pas de fonctions de sécurité dans leurs produits.

4- ***Aucune procédure de sécurité suivie de documentation n'a été développée pour les ICS :*** Des procédures de sécurités adéquates devraient être développées pour l'ICS. Ils représentent les racines d'un programme de sécurité solide.

5- ***Directives d'application d'un matériel d'ICS absentes ou inadéquates :*** Les lignes directive de mise en œuvre de l'équipement doivent-être tenues à jour et facile d'accès. Ces dernières font partie intégrante des procédures de sécurité en cas de dysfonctionnement des ICS.

6- ***Peu ou pas de vérification de la sécurité des ICS :*** Les vérifications indépendantes de sécurité devraient revoir et examiner l'historique et les activités d'un système afin de vérifier et déterminer la pertinence/compétences/capacités du système de contrôle et assurer le respect des procédures et politiques de sécurité de l'ICS.
Les vérifications pourraient aussi permettre de détecter les brèches dans les services de sécurités des ICS et évidemment proposer et recommander des changements comme étant des contre-mesures choses qui pourrait permettre de rendre les contrôle de sécurité plus robustes et/ou l'ajout de nouveaux systèmes de contrôle de sécurité.

7- ***Manque de gestion spécifique du changement de configuration de l'ICS :*** Un processus de contrôle de modification de matériel (hardware), firmware, logiciel

(software) et documentation devrait être implémenté afin d'assurer la sécurité de l'ICS contre des modifications non conforme ou inadéquates avant, durant et après l'implémentation du système.

Un manque au niveau des procédures de gestion du changement de configuration pourrait conduire à des oublies ou erreurs de sécurité menant à une grande exposition aux risques.

b. Les Vulnérabilités par plateformes

Les vulnérabilités des ICS pouvant se produire à cause d'erreurs/défauts, mauvaises configurations ou à cause de la faiblesse de maintenance de leurs plateformes, incluant : Hardware, OS et les applications de l'ICS.

Ces vulnérabilités peuvent-être mitigées/atténuées/réduites à travers différents contrôle de sécurité, comme la MAJ de l'ICS et ses applications, contrôles d'accès physiques, logiciels de sécurité (Anti-virus).

La répartition est faite comme suit :

b.1.Configuration

1. ***Patches et MAJ OS et logiciels ne seront peut-être pas développé que jusqu'à a découverte des failles de sécurité :*** En raison de la complexité des logiciels ICS, d'éventuelles modifications au SE/OS en cours de fonctionnement et les changements doivent-être soumis à des testes approfondis. Le temps écoulé pour ces essaies et les distributions ultérieurs du logiciels mis-à-jour fournit une longue fenêtre de vulnérabilité.

2. ***Les patches OS et applications de sécurité non-maintenu :*** Les SE/OS et applications périmées peuvent contenir des vulnérabilités nouvellement découvertes qui pourrait être exploitées. Les procédures documentées devrait être développé sur comment les patches de sécurité pourrait-être maintenus.

3. ***Patches des SE/OS et applications de sécurité sont implémentés sans teste exhaustif :*** Les patches OS/applications de sécurité déployés sans testes pourrait compromettre les opérations et le fonctionnement normal de l'ICS. Les procédures documentées devrait-être développées sur les testes à effectuer sur les nouveaux patches de sécurité.

4. ***L'utilisation des configurations par défaut :*** Mène très souvent à des ports non sécurisés/ouvert et inutiles, serveurs et applications exploitable en plein fonctionnement.

5. ***Configurations critiques non sauvegardées ou stockées :*** Des procédures de restauration du paramétrage de configuration de l'ICS devraient-être disponible dans le cas de changement accidentels de configurations afin de maintenir la disponibilité du système et éviter les pertes de données.
Des procédures documentées devraient-être développées afin de maintenir le paramétrage des configurations de l'ICS.

6. ***Données non protégées sur les dispositifs portatifs :*** Si les données sensibles (Mot de passe…etc.) sont stockées en clair sur les appareils portables tels que les PC portables et PDA (Personnal Digital Assistant) et si ces dispositif sont perdus ou volés, la sécurité du système pourrait-être compromise.

7. ***Contrôle d'accès appliqués inadéquats :*** Les contrôles d'accès pauvrement configurés peuvent conduire à un utilisateur de l'ICS avec trop ou même peu de privilèges. La suite explique chaque cas en détail.
   - Système configuré avec un paramétrage de contrôle d'accès par défaut donne à l'opérateur des privilèges administratifs.
   - Les systèmes mauvaisement configurés, conduisent à un opérateur incapable à prendre en main les actions correctives durant les situations d'urgences.
   - Les politiques du contrôle d'accès devrait-être développées comme étant partie entière du programme de sécurité de l'ICS.

B.2. Matériel (Hardware)

1- ***Testes inadéquats des changements de sécurité :*** Beaucoup d'installation ICS et spécialement les plus petites ne possèdent pas d'installations de testes et donc les changements de sécurités doivent-être fait en utilisant le système opérationnel en live/plein fonctionnement.

2- ***Protections physiques inadéquates pour les systèmes critiques :*** Accès au centre de contrôle, dispositifs de terrain, dispositifs portatifs et les autres composants de l'ICS ont besoin d'être contrôlés.
La plupart des sites sont souvent non surveillés physiquement.

3- ***Le personnel non autorisé ayant l'accès physique à l'équipement :*** L'accès physique aux équipements de l'ICS devrait-être interdit sauf au personnel nécessaire, prenant en compte les conditions de sécurité comme les arrêts d'urgence ou démarrage.

Les accès physiques non autorisés peuvent conduire à :

- Vole physique de données/matériels.
- Dommages physiques, destructions de données/matériels.
- Changement non autorisés à l'environnement fonctionnel (connexions de données, utilisation non autorisées des média amovibles, ajouts/suppressions de ressources)
- déconnexion de liens de données physiques.
- Interception indétectable de données (Keylogger : Enregistreur de frappes et autres)

4- ***Accès à distance à l'ICS non-sécurisé :*** Les modems et autres dispositifs d'accès à distance qui permettant aux Ingénieurs de contrôle et aux fournisseurs d'avoir accès aux systèmes devrait-être déployés et mis en place avec des contrôles de sécurités afin de prévenir l'accès des individus non autorisé aux ICS.

5- ***Atouts et actifs non-listés :*** Afin de proprement sécurisé un ICS, il faut qu'il y ait une liste précise des actifs dans un système. Une représentation imprécise de l'ICS et de ses composants peut laisser un point d'accès non-autorisé ou une porte de derrière (Backdoor) au niveau de l'ICS.

6- ***Manque d'alimentation de secours :*** Sans alimentations de secours pour les actifs critiques, une perte générale d'alimentation arrêtera l'ICS et pourrait conduire à de nombreuses situations dangereuses ou à des paramètres par défaut non sécurisés.

7- ***Le manque de redondance des composants critiques :*** Pourrait fournir un point unique de possibilité d'échec et de défaillance (SPOF : Single Point Of Faillure)

B.3.Logiciels (Software)

1. ***Des capacités de sécurité installées mais non activés par défaut :*** Les capacités de sécurité installées avec le produit sont inutiles si elles ne sont pas activées ou du moins identifiées comme étant désactivées.

2. ***Dos : Denial of Service (Déni de service) :*** Les logiciels de l'ICS pourrait-être vulnérables à des attaques Dos, conduisant à l'interdiction des accès autorisés à une ressource système ou créant délais et retards au niveau des opérations et fonctions du système.

3. ***OLE pour Process Control (OPC : Open Platform Communication) :*** Sans patches et MAJ, OPC est vulnérable aux faiblesses et failles.

4. ***L'utilisation des larges protocoles industriels pour ICS :*** MODBUS, PROFIBUS et autres protocoles sont très communs à travers la pluparts des industries, les informations concernant ces protocoles sont gratuitement disponibles. Ces protocoles ont peu voir pas du tout de capacité sécuritaires.

5. ***L'utilisation d'un texte clair :*** La plupart des protocoles des ICS transmettent à travers les médias de transmissions des messages en textes clairs, les rendant susceptibles d'être lu par des concurrents.

6. ***Des services inutiles en fonctionnement :*** La plupart des plateformes ont une variété processus et services réseaux définit afin d'opérer par défaut. Les services inutiles sont très rarement désactivés et pourrait-être exploités par la suite.

7. ***L'utilisation de logiciels propriétaires dont le sujet a été abordée en conférences internationales :*** Les soucis des logiciels propriétaires sont très souvent sujets des discussions au niveau des conférences ICS internationales (incluant « Black Hat ») et disponibles à travers papiers, documentations et fiches techniques. Les manuels de maintenance des systèmes de contrôle sont disponibles au niveau des fournisseurs. Ces informations peuvent aider concurrents et adversaires à planifier et réussir une attaques contre l'ICS.

8. ***Authentifications et contrôles d'accès inadéquats pour la configuration et la programmation du logiciel :*** L'accès non-autorisé à la configuration et programmation du logiciel pourrait donner libre champ pour l'atteinte d'un dispositif et du système en entier.

B.4. Logiciels Malveillants (Malware)

1- ***Les logiciels de protection malware non installés ou non-à-jour:*** Les malware peuvent provoquer de lourdes dégradations de performances, pertes de la disponibilité du système, ajoutons à cela : capture, modification et suppression de données. Les logiciels de protections malware comme les Antivirus sont nécessaire afin d'éviter que les systèmes soient infectés par des logiciels malveillants ou malware.

2- ***Logiciels de protection malware implémenté sans testes rigoureux :*** Les logiciels non-testés peuvent en effet affecter le court des opérations et le fonctionnement normal d'un ICS.

C- Les vulnérabilités des réseaux

Les vulnérabilités au niveau d'un ICS peuvent se créer des défauts, mauvaises configurations ou la faible administration des réseaux ICS et leurs connexions avec les autres réseaux.

Ces vulnérabilités peuvent-être éliminées, réduites ou même atténuées à travers différents contrôles de sécurité, Les points suivant décrivent les vulnérabilités potentielles concernant les plateformes liées aux réseaux de l'ICS :

C.1.Vulnérabilités des configurations des réseaux

1- ***Faibles architectures de la sécurité du réseau :*** L'environnement de l'infrastructure au sein de l'ICS a souvent été développé puis modifiée en se basant sur les besoins de fonctionnement avec une très faible considération quant à l'impacte sécuritaire que pourrai avoir ces changements là. Avec le temps, les lacunes de sécurité peuvent-être introduites par inadvertance au niveau de certaines parties particulières de l'infrastructure.

2- ***Equipements informatiques de sécurités faiblement ou mal configurés:*** L'utilisation des configurations par défaut mène très souvent à des ports non sécurisés ouverts, non nécessaires et à des services réseau exploitables en cours d'exécution sur les serveurs. Les mauvaises configurations des règles pare-feu (Firewall) peuvent permettre un trafic non nécessaire.

3- ***Configurations des dispositifs réseaux non stockées ou sauvegardées :*** Les procédures de restauration de paramétrage de configurations des dispositifs réseau devraient-être disponibles dans le cas d'avènement de changement de configuration accidentel ou extérieur afin de maintenir la disponibilité du système et éviter les pertes de données.

C.2. Vulnérabilités du matériel du réseau (Hardware)

1. ***Protection physique inadéquate aux équipements réseaux :*** L'accès à ces équipements devrait être contrôlé afin d'éviter dommages, dégâts ou même destructions.

2. ***Personnel non-qualifié accédant aux équipements et connexions réseaux:*** L'accès physique aux équipements réseau ne devrait être autorisé qu'au personnel qualifié et nécessaire.

   L'accès inadéquat aux équipements réseau pourrait mener à :

   - Vole physique de données et de matériels.
   - Dégâts physique et destruction de données et/ou de matériel.
   - Des changements non-autorisés à l'environnement de sécurité.
   - Interceptions et manipulations non-autorisées des activités réseau.
   - Déconnexion des liens/câbles de données physiques.

3. ***Le manque de redondance pour les réseaux critiques :*** La redondance étant un dédoublement d'équipement critique où en cas de pannes, ces derniers se mettront en marche, aussi appelés périphériques de secours. Ce manque là pourrait fournir un point unique de défaillance. (SPOT : Single point of failure)

C.3. Vulnérabilités du périmètre réseaux

1. ***Aucun périmètre de sécurité défini :*** Si le réseau de contrôle n'a pas de périmètre de sécurité clairement défini, il ne sera donc pas possible de s'assurer que les contrôles de sécurité sont déployés et proprement configurés. Ceci peut conduire à des accès non-autorisés aux systèmes, aux données mais aussi à d'autres problèmes.

2. ***Pare-feu inexistants ou non-proprement configurés :*** Un manque de pare-feu proprement configurés pourrait permettre le passage de données non-nécessaires entre les réseaux comme les réseaux de contrôle et d'entreprise. Ceci pourrait causer beaucoup de problèmes notamment les attaques extérieurs, malwares qui vont se propager entre les réseaux, rendant les données importantes et sensibles susceptibles à la surveillance d'espionnage, donnant aussi des accès non autorisés aux systèmes.

C.4. Vulnérabilité de l'enregistrement et de la surveillance du réseau

Aucune surveillance de sécurité sur le réseau de l'ICS : Sans la surveillance de sécurité, les incidents peuvent passer inaperçus conduisant à des dégâts supplémentaires et à des perturbations de fonctionnement. La surveillance de sécurité normale est aussi requise afin d'identifier les problèmes avec le contrôle adéquat (Comme les mauvaises configurations et les pannes).

C.5. Vulnérabilités de communication

1. ***Chemins de contrôle et de surveillance critiques non-identifiés :*** Connexion inconnues aux ICS peuvent laisser une porte de derrière (Backdoor) pour des attaques futurs.

2. ***Protocoles de communication standard avec des documentations disponibles sont utilisés de façon brute :*** Concurrents et adversaire peuvent surveiller les réseaux ICS en utilisant un analyseur de protocole ou d'autres utilitaires afin de décoder les données transmise par les protocoles tels que Telnet (Telecom Net), FTP (File Transfert Protocol) ou NFS (Network File System). L'utilisation de tels protocoles rend la tâche plus facile à l'adversaire pour attaquer et manipuler les activités réseaux au niveau de l'ICS.

3. ***L'authentification des utilisateurs de données et de dispositif est non existante :*** La plupart des ICS n'ont pas d'authentification à aucun niveau. Sans aucune authentification, il y a risque de modification de données/dispositifs comme les capteurs ou les identités d'utilisateur.

C.6. Vulnérabilités des connexions sans-fils

Authentification et protection inadéquate entre les clients et les points d'accès : Une forte authentification mutuelle est nécessaire entre les clients sans fils et les points accès.

II.5. Facteurs de risque

Beaucoup de facteurs contribuent actuellement à l'augmentation du risque aux systèmes de contrôle.

a) L'adoption des protocoles et technologies standardisées avec des vulnérabilités connues.
b) La connectivité des systèmes de contrôles aux autres réseaux.
c) Connexion non-sécurisées.
d) La disponibilité répandue des informations techniques concernant les systèmes de contrôle.

5. a. Technologies et protocoles standardisés

Les vendeurs et les fournisseurs des ICS ont commencé à ouvrir leurs protocoles propriétaires et publier les spécifications de leurs protocoles afin de permettre à la tierce partie constituant les fabricants d'accessoires de mettre au point les dispositifs et accessoires adéquats et compatibles.

Les organisations et entreprises sont aussi en plein transition des systèmes propriétaires à d'autres moins coûteux, constituant des technologies standardisées comme exemple nous avons : Microsoft Windows et Unix Like OS/SE comme nous avons aussi les protocoles réseaux comme le TCP/IP afin de réduire les coûts et améliorer les performances.

Une contre contribution standard à cette évolution des systèmes open ou bien ouverts est le OPC (OLE for process control/Open platform communication) étant un protocole qui active les interactions entre le système de contrôle et les applications/programmes sur PC.

La transition vers l'utilisation de ces normes de protocoles ouverts fournit des avantages autant techniques qu'économiques mais augmente aussi en lourde contre partie la vulnérabilité des ICS aux cybers attaques.

Ces protocoles et technologies standardisées ont des vulnérabilités très connues qui sont sensibles à l'exploitation d'outils sophistiqués et efficaces étant largement disponibles et relativement facile d'usage.

5.b. Connectivités

Les ICS et les systèmes IT d'entreprise sont souvent interconnectés comme résultat de beaucoup de changements effectués aux niveaux des pratiques de gestion de l'information.

Le besoin d'un accès à distance a encouragé beaucoup d'entreprise à établir des connexions aux ICS qui permet aux Ingénieurs du système de contrôle et personnels support de surveiller et contrôler le système d'endroits se trouvent en dehors du réseau de contrôle.

Beaucoup d'entreprises et d'organisations ont aussi ajoutés des connexions entre les réseaux d'entreprise et le réseau de contrôle afin de permettre aux décideurs de l'organisation d'avoir accès aux données sensibles et critiques à propos des états de leurs systèmes opérationnels afin de pouvoir envoyer des instructions à la fabrique ou manufacture ou même aux points de distribution du produit.

Durant les premières implémentations, ceci a du être fait avec des applications personnalisées à travers un serveur/passerelle OPC (Open Platform communication). Souvent, ces implémentations sont faites sans une compréhension totale des risques de sécurité correspondant, ajoutons à cela le fait que les réseaux d'entreprise sont souvent connectées aux réseaux de partenaires stratégiques et surtout à Internet.

Les systèmes de contrôle font de plus en plus usage des WAN (Wide Area Network) et d'internet afin de transmettre les données aux stations locales ou à distance et aux dispositifs individuels.

Cette intégration des réseaux des systèmes de contrôle avec les réseaux publique et d'entreprise augmente l'accessibilité des vulnérabilités du système de contrôle, sans le déploiement des contrôles de sécurité appropriés, ces vulnérabilités peuvent exposer tous les niveaux de l'architecture du réseau de l'ICS, erreurs d'origines inconnues, une variété de cyber-menaces, incluant malware/ver etc.

A titre d'exemple de la variation de menaces aux systèmes de contrôle, une enquête interne d'une entreprise concernant l'Energie dont le nom reste non communiqué, a démontré ce qui suit :

- La majorité des unités de gestion de busines pensaient que leurs systèmes de contrôle n'étaient pas connectés au réseau d'entreprise.
- Une vérification a démontré que la plupart des systèmes de contrôle étaient connectés d'une certaine manière au réseau d'entreprise.
- Le réseau d'entreprise n'a été assuré que pour supporter des processus d'affaire et non les systèmes de sécurité critiques.

En plus de la complexité de la situation, le but des départements IT (d'informatique) sont fondamentalement différents de ceux des départements de contrôle de processus (Process control)

Le monde IT voit les performances, confidentialité et intégrité des données comme primordiales, pendant que le monde des ICS voit la sécurité de l'homme et de l'installation comme sa responsabilité primaire, puis viennent les priorités fondamentale étant la disponibilité du système et l'intégrité des données comme vu dans la **section II.1** précédente incluant les différentes conditions de fiabilité, l'impacte d'incidents, performances, protocoles de communication et architecture des systèmes ceci veut donc dire qu'il y a

clairement des différences significatives dans l'implémentation des pratiques de sécurité concernant les deux type de systèmes.

5.c. Connexions non-sécurisées

La plupart des fournisseurs des ICS délivrent les systèmes avec des modems qui fournissent l'accès à distance afin d'alléger le poids du personnel de support technique sur terrain.

L'accès à distance fournit au personnel et au staff technique le niveau administratif d'accès à un système, comme l'utilisation des informations d'identification de contrôle d'accès (exemple : Identificateurs/MDP valides)

Les MDP utilisés par l'accès à distance sont très souvent identiques pour toutes les implémentations des systèmes d'un seul fournisseur et n'ont peut-être pas été changé par l'utilisateur final. Ce genre de connexions peut laisser le système grandement vulnérable.

Les organisations et entreprises laissent très souvent des liens d'accès comme les routeurs/switch ouverts pour des diagnostiques à distance, maintenance et surveillance.

Les systèmes de contrôle utilisent grandement les systèmes de communication sans-fil ce qui peut les rendre très vulnérables.

Les liens et points d'accès non protégés par authentifications et encryptages ont augmenté le risque que le concurrents puissent utiliser ces connexion non-sécurisées afin d'accéder au système de contrôle à distance.

Sans mécanismes d'authentification afin de limiter l'accès, il y a vraiment très peu pouvant protéger la confidentialité et l'intégrité de l'information étant transmise.

Ceci pourrait résulter à des informations et données dont l'intégrité est compromise mais aussi la disponibilité du système aussi se verra affecter, dans les deux cas cela pourrait toucher à la sécurité de vies humaines et de l'installation en elle-même.

La plupart des interconnexions entre les réseaux d'entreprise et les ICS requièrent l'intégration de systèmes avec différentes normes de communication, le résultat serai une infrastructure qui est confectionnée par les Ingénieurs de contrôle de façon à transmettre en va et vient les données entre deux systèmes uniques.

En raison de la complexité de l'intégration de systèmes complètement différents, les Ingénieurs ne parviennent très souvent pas à répondre à la charge supplémentaire concernant les risques de sécurité. Beaucoup d'Ingénieur de contrôle ont peu et pas d'informations en matière de sécurité et souvent, les connaissances et ressources informatiques (IT) en réseaux ne sont impliquées dans la conception de la sécurité des ICS.

Par conséquent, le contrôle d'accès destiné à protéger les systèmes de contrôle d'accès non-autorisés à travers les réseaux d'entreprise sont souvent minimes.

Par ailleurs, le comportement des protocoles sous-jacent n'est souvent pas compris et donc les vulnérabilités peuvent toujours exister et peuvent mettre à l'échec les contre-mesures de sécurité avancées.

Les protocoles comme les TCP/IP et d'autres ont des caractéristiques qui sont souvent non activées et ceci peut aller à l'encontre de toute procédure de sécurité mise en place au niveau du réseau ou des applications.

5.d. L'information publique

Les informations en rapport avec les ICS : design/conception, maintenance, interconnexion et communication étant publique et facilement disponibles à travers Internet pour soutenir la concurrence dans le choix des produits ainsi que pour permettre l'utilisation des normes ouvertes. (Open standards)

Les fournisseurs et vendeurs des ICS vendent des boîtes à outils (toolkits) afin d'aider au développement de logiciels qui pourrait faciliter l'implémentation des différentes normes utilisées dans l'environnement ICS.

Il y a beaucoup d'anciens employés, vendeurs et autres utilisateurs finaux du même équipement de l'ICS à travers le monde entier ayant des connaissances internes concernant le fonctionnement des systèmes de contrôle.

Les ressources et informations sont disponibles aux concurrents et intrus potentiels de tout calibre. Avec ces informations, il est possible pour un individu avec très peu de connaissance sur le système de contrôle d'avoir l'accès non-autorisé au système avec l'utilisation d'outils d'attaque automatisé.

II.6. Les cyber-incidents (ou incidents de cyber-sécurité)

II.6.1. Définition

Tout acte ou évènement suspect qui compromet ou tentative de compromettre le périmètre de sécurité électronique ou le périmètre de sécurité physique d'un actif/dispositif électrique/électronique critiques, ou son fonctionnement.

II.6.2. Sources d'incidents

Une comptabilité précise des cyber-incidents sur les systèmes de contrôle est difficile à déterminer. Toutefois, les individus en industrie ayant mis l'accent sur la question remarquent des tendances de croissance similaires entre les vulnérabilités exposées dans les systèmes informatiques traditionnels (IT) et celles trouvées au niveau des systèmes de contrôles.

Il existe le « ISID : Industrial Security Incident Database » qui veut dire : Base de données des incidents de sécurité industriels, conçue afin de pister les incidents de nature de cyber-sécurité qui affectent directement les ICS et les processus.

Ceci inclut les évènements de cyber-sécurité accidentels comme délibérés (accès à distance non-autorisés), attaque DoS (déni de service), infiltration de logiciel malveillant.

Les données sont récoltées à travers les recherches menées sur les incidents publiques connus et aussi sur les rapports privés des membres de l'organisation ou l'entreprise souhaitant avoir accès à la base de données.

Chaque incident est passé sous enquête puis classé en fonction de la fiabilité (confirmé, probable mais non confirmé, peu probable ou inconnu, canular/légende urbaine).

Références. Il existe trois (03) grandes catégories d'incidents des systèmes de contrôle :

1- ***Attaques ciblées intentionnelles.***
2- ***Conséquences non-intentionnelles ou dégâts collatéraux.***
3- ***Conséquences non-intentionnelles de sécurité interne.***

II.6.3. Scénarios d'incidents possibles

Il existe plusieurs types de scénario possible pour un ICS citons :

- La perturbation du fonctionnement du système de contrôle causé par le retard ou blocage du flux d'information à travers les réseaux d'entreprise et de contrôle, ainsi niant toute disponibilité des réseaux aux opérateurs du système de contrôle ou causant le blocage total dans le transfert d'information ou un DoS.
- Des changements non-autorisés faits à des infrastructures programmées au niveau des API,RTU,DCS ou contrôleur SCADA, changement des seuils d'alarmes, problèmes de commandes non autorisées pour contrôler l'équipement qui pourrait endommager ce dernier (si les points de tolérances sont dépassés par exemple), extinction prématurée des processus (pouvant causer des incidents environnementaux ou complètement désactiver l'équipement de contrôle.)
- De fausses informations communiquées à l'opérateur du système de contrôle afin de déguiser les changements non autorisés ou pour lancer des actions inappropriées par les opérateurs systèmes.
- Modification du logiciel du système de contrôle ou de la configuration des paramètres, produisant des résultats inattendus.
- Le fonctionnement des systèmes de sécurité interféré.
- Les logiciels malveillants introduits dans le système.
- Instructions de travail modifiées afin de provoquer des dégâts aux produits, équipements ou même au personnel.

En addition, concernant les systèmes de contrôle recouvrant une grande zone géographique, les sites à distances sont souvent vides (sans personnel) donc sans aucune assistance ou surveillance physique. Si de tels systèmes sont physiquement violés et atteints, les concurrents peuvent établir une connexion retour vers le réseau de contrôle.

II.7. Conclusion

Nous avons au cours de ce chapitre étudié et mis l'accent sur les vulnérabilités connues des systèmes de contrôle et les risques que ces dernières peuvent faire courir à nos systèmes ; afin de mieux les comprendre et pouvoir mettre en place les solutions d'atténuations qui seront l'objet du chapitre suivant.

Chapitre III:

Programme de cyber-sécurité des systèmes de contrôle industriels (ICS)

III.1.Introduction

Comme mentionné dans la **section II.1** du chapitre précédent, il existe des différences critiques entre les ICS et les systèmes IT qui influencent comment les contrôles de sécurité doivent-être spécifiés et appliqués aux ICS.

Ce chapitre va comporter la méthodologie à suivre de façon générale afin de développer et mettre en place la ou les contre-mesures d'automatisation et de sécurité à notre système de contrôle.

III.2. Programme de sécurité

Intégrer de façon efficace la sécurité à un ICS nécessite le respect de certains points notamment définir et exécuter un programme compréhensif qui touche à tous les aspects de la sécurité, allant d'identifier les objectifs aux opérations au jour le jour et les surveillances en temps réel des améliorations et dégradations.

Ce qui suit représente les points essentiels au processus de développement d'un programme de sécurité :

1. Définir et faire l'inventaire des atouts ICS.
2. Procéder à une évaluation des risques et des vulnérabilités.
3. Définir les contrôles de réduction et d'atténuation des risques.

III.2.1.Définir et faire l'inventaire des atouts ICS

L'équipe de Cyber-sécurité se doit d'identifier les applications et les ordinateurs systèmes à l'intérieur de l'ICS et des réseaux en question.

Tout d'abord la concentration se doit d'être diriger un peu plus sur les systèmes que sur les dispositifs incluant API, DCS, SCADA et les systèmes basés sur instruments utilisant un dispositif d'affichage (surveillance/monitorage, exemple : HMI).

Après l'identification des atouts ICS, l'information doit-être enregistrée et devrait être revue et mise à jour de façon annuelle.

Logiciels et outils d'inventaires d'atouts des réseaux ICS

Il existe différentes entreprises offrant et proposant des logiciels outils d'inventaire pouvant identifier et mettre en documents tous les éléments d'un réseau et ceci concernant les parties hardware et software.

Exemple : Open – AudIT

Il faut néanmoins agir avec précaution en utilisant ces outils là pour identifier les atouts de l'ICS. L'équipe concernée devrait d'abord procéder à une évaluation approfondie de la façon dont ces outils fonctionnent et l'impacte qu'ils pourraient peut-être avoir sur les équipements de commande connectés. Cette évaluation peut inclure des testes sur les systèmes similaire à caractère non productif afin de s'assurer que ces outils ne vont pas affecter négativement les systèmes de commande/contrôle de production. Ajoutons que si l'impacte pourrait être acceptable sur les systèmes IT, il ne le sera très probablement pas sur les ICS.

III.2.2.Procéder à une évaluation des risques et vulnérabilités

Parce que la plupart des entreprises possèdent un amont de ressources limitées, ils se doivent de procéder à une évaluation de risques pour les ICS et en utiliser les résultats afin de mettre en priorités les systèmes basés sur le principe de l'ICS concernant l'impacte potentiel sur chaque système.

Une évaluation de vulnérabilités détaillée devrait-être faite pour les systèmes à « HAUTE-PRIORITE » et ceux à moins importante priorité comme jugé de la façon la plus prudente mais aussi en fonction des ressources.

Cette évaluation de vulnérabilités permettra d'identifier quelconque faiblesse et failles pouvant être présente sur les systèmes qui pourraient causer une atteinte la confidentialité, intégrité et disponibilité des systèmes et des données mais aussi les autres risques de cyber-sécurité et les approches d'atténuation pour diminuer et réduire les risques.

En raison du risque de perturbation des dispositifs et appareils, les scanner de vulnérabilités devraient-être utilisés avec précaution sur les réseaux ICS de production. Les scanner de vulnérabilités tentent souvent de vérifier la vulnérabilité d'un tel appareil en procédant à un ensemble représentatif d'attaques contre cet appareil ou ce réseau. Etant donné que les ICS ont été conçu pour contrôler et automatiser les processus ou les équipements du monde réel,

recevant les mauvaises instructions, ils pourraient effectuer des actions incorrectes causant perte d'équipements, dégâts, blessures ou même la mort.

L'identification des vulnérabilités au sein d'un ICS requiert une approche différente de celle sur un système IT typique. Dans la plupart des cas, les appareils et dispositif sur un système IT peuvent-être rebootés (redémarrés) ou remplacés avec une très courte interruption de service. L'ICS quant à lui contrôle un processus physique et a donc des conséquences dans le monde réel associées à certaines actions.

Pendant qu'un inventaire ou qu'un scan de vulnérabilités est effectué, il existe un certain nombre d'étapes à suivre. Le tableau suivant décrit en détails chacune de ces étapes avec la comparaison directe de son application sur un système IT. Ces techniques peuvent rendre le travail relativement plus compliqué mais devrait aider à diminuer les problèmes liés au scan actif.

A Identifier	Actions suggérer sur ICS	Actions sur IT
Hôtes et réseaux	-Procéder à une vérification physique (suivre les câblages) -Procéder à une écoute passive ou une détection d'intrusion sur le réseau (exemple : snort) -Spécifier des adresses IP à être scanner de façon programmée.	Balayage réseau (exemple : nmap)
Services	-Faire la vérification locale des ports.	Scanner les ports (exemple : nmap)

Tableau III.1 : Etapes à suivre sur l'ICS pour lister les vulnérabilités.

Les points communs entre les actions suggérer sur un ICS est le fait qu'elles ne génèrent aucun trafic sur le réseau opérationnel de production ou bien contre les systèmes de production.

Ces méthodes peuvent regrouper la plupart voir toutes les mêmes informations qu'une méthode plus active sans le risque de causer des failles durant les testes.

Un autre facteur à prendre en compte pendant le choix des méthodes de testes ICS est que ces systèmes ont très peu de capacité de secours comparés aux systèmes IT. Les systèmes ICS ont quant à eux, une plus grande longévité que les systèmes IT, donc leur hardware et bien au-delà de l'état de l'art et peut-être très facilement surchargé.

III.2.3.Définir les contrôles d'atténuation et de réduction

Les contrôles d'atténuation d'un certain risque spécifique pourraient varier parmi les différents types de systèmes. Il existe certains risques pouvant être atténués et réduit à l'aide de méthodes « Quick fixes » faible coût et à grande valeur pratique qui peuvent grandement réduire le risque. Les exemples de ces solutions peuvent-être la restriction d'accès à internet, éliminer l'accès e-mail sur les stations opérateurs.

On peut déduire deux approches :

Sécurisation fonctionnelle : Cette approche concerne essentiellement l'architecture réseau du système de contrôle, et toutes les modifications pouvant y être apportées.

Sécurisation technique : Cette partie regroupe tout ce qui concerne les équipements dédiés à l'amélioration de la cyber-sécurité et leurs programmations (pare-feu, point d'accès Wifi etc.)

III.2.3.1. Sécurisation fonctionnelle

III.2.3.1.A. Les architectures des réseaux

Lors de la conception d'une architecture réseau pour un ICS, il est souvent recommandé de séparer le réseau ICS et le réseau d'entreprise. La nature du trafic réseau sur ces deux derniers est différente : Accès Internet, e-mail et accès à distance seront naturellement permis sur le réseau d'entreprise et ne devraient pas l'être sur le réseau ICS. En ayant des réseaux séparés, les problèmes de sécurité et de performances sur le réseau d'entreprise ne devraient pas être en mesure d'affecter le réseau ICS.

Pour des raisons pratiques, la connexion entre les réseaux ICS et d'entreprise est souvent requise. Cette connexion représente néanmoins un risque de sécurité significatif, une précaution considérable devrait être prise lors de la conception concernant ce point.

Si les réseaux doivent-être connectés, il est fortement recommandé qu'il y ait un minimum (voir unique si possible) connexion permis et que cette dernière soit faite à travers un « pare-feu » et un « DMZ ». Un « DMZ » est un segment séparé du réseau se connectant directement au pare-feu. Les serveurs qui contiennent les données provenant de l'ICS qui doivent être accédés du réseau d'entreprise sont placés sur ce segment. Seulement ces systèmes devraient être accessibles du réseau d'entreprise.

Avec la moindre connexion extérieure, l'accès minimum devrait être mis à travers le pare-feu, incluant l'ouverture des ports requis à la communication en question

III.2.3.1.B. Réseaux de contrôle logiquement séparés

Le réseau de l'ICS devrait-être à un minimum logiquement séparé du réseau d'entreprise sur des dispositifs réseau physiquement séparés. Lorsque la connectivité d'entreprise est requise :

- Il devrait y avoir un nombre de point d'accès minimale (voir unique) entre le réseau ICS et celui de l'entreprise.
- Les règles du pare-feu devraient à un minimum fournir le filtrage de la source et de la destination.

Il existe une autre approche acceptable lorsque l'on permet la connexion entre le réseau ICS et celui d'entreprise qui est d'implémenter un réseau intermédiaire DMZ (zone démilitarisée : Demilitarized zone) qui est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

Comme on peut le voir sur la **Figure III.1** le DMZ devrait donc être connecté au pare-feu de façon à ce que la seule connexion à pouvoir se faire sera entre le réseau d'entreprise et le réseau ICS est le DMZ.

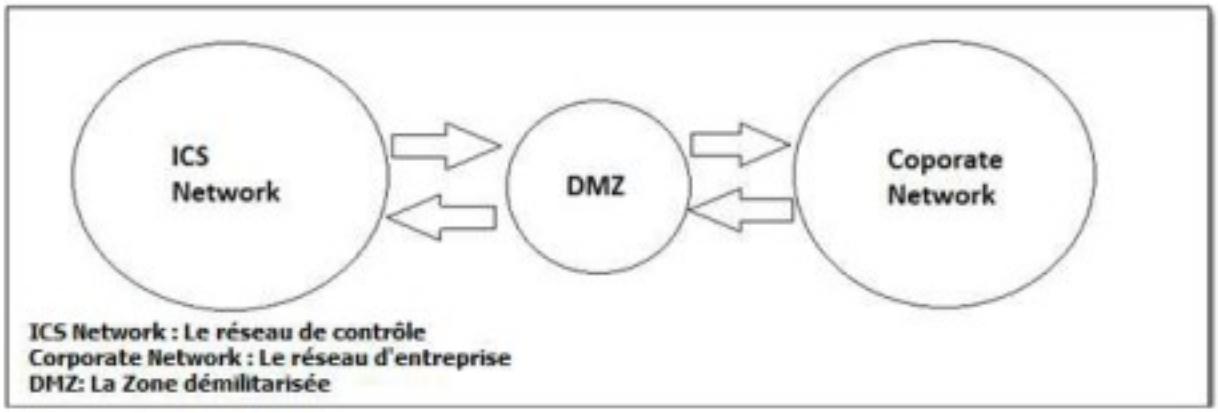


Figure III.1 : Fonction du DMZ entre les réseaux ICS et d'entreprise.

Le réseau d'entreprise et celui de l'ICS ne devrait pas être en mesure de communiquer directement entre eux.

III.2.3.1.C. Séparation des réseaux

Les réseaux ICS et d'entreprise peuvent-être séparés afin d'améliorer la cyber sécurité en utilisant différentes architectures. Il existe différentes approches de séparation des réseaux :

1. Type 2 zones.
2. Type 3 zones.

Parmi celles du type 2 zones, citons :

1.1. Pare-feu entre le réseau de contrôle et le réseau d'entreprise

En introduisant un simple pare-feu à deux ports entre le réseau de contrôle et le réseau d'entreprise, comme démontré sur la figure qui suit, une amélioration sécuritaire peut-être accomplie. Démontré sur la **Figure III.2 ;**

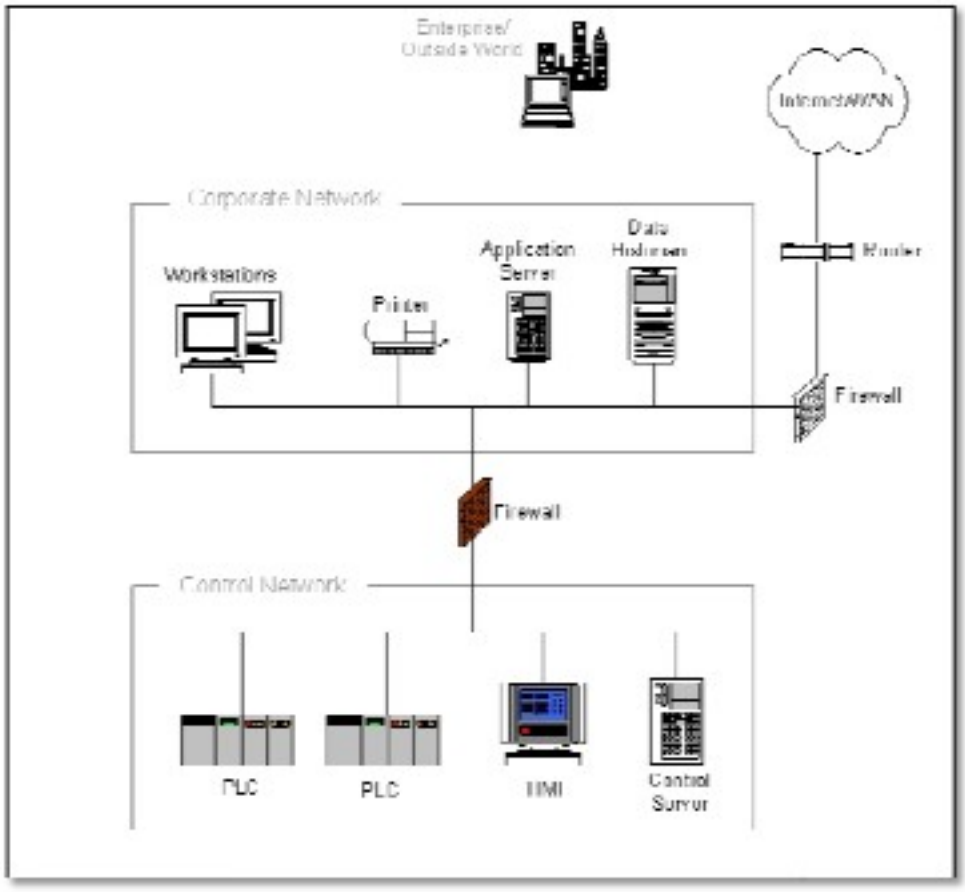


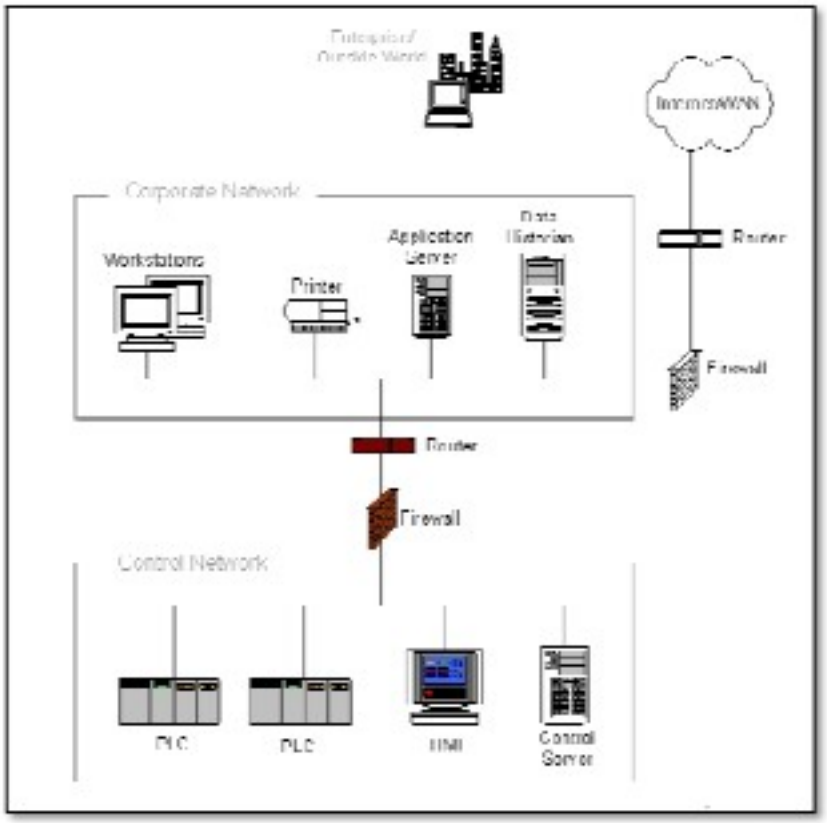
Figure III.2 : Pare-feu entre le réseau de contrôle et le réseau d'entreprise. [9]

NB : Tous les éléments présents sur le réseau de contrôle et d'entreprise ne sont pas tous représentés.

En résumé, cette architecture peut représenter un bon nombre d'améliorations en comparaison avec les réseaux non séparés, elle nécessite l'utilisation de règles de pare-feu permettant les communications directes entre le réseau d'entreprise et les appareils/dispositifs du réseau de contrôle. Ceci pourrait tout autant résulter en des brèches sécuritaires si la conception et la surveillance ne sont pas minutieuses.

1.2. Pare-feu et routeur entre le réseau de contrôle et le réseau d'entreprise

Une architecture un tout petit peu amélioré est démontrée sur la figure qui va suivre, améliorations qui résident en l'utilisation de la combinaison routeur/pare-feu. Le routeur se trouve en face du pare-feu offrant des services de filtrage de paquets de base, pendant que le pare-feu se charge des soucis plus complexes, on peut clairement le voir sur la **Figure III.3**



Figures III.3 : Combinaison pare-feu/routeur entre le réseau de contrôle et le réseau d'entreprise. [9]

Procédons maintenant aux approches du type 3 zones, qui représentent les solutions les plus optimales :

2.1. Pare-feu avec DMZ entre le réseau de contrôle et le réseau d'entreprise

Une amélioration significative sera l'utilisation de pare-feu avec la capacité d'établir un DMZ entre le réseau de contrôle et le réseau d'entreprise. Chaque DMZ peut englober un ou plus d'éléments sensibles (critiques), par exemple : L'historique de données, les points d'accès Wifi, le système d'accès tierce/à distance.

En pratique l'utilisation d'un DMZ avec pare-feu possible permet la création d'un réseau intermédiaire.

La **Figure III.4** démontre un exemple de cette architecture :

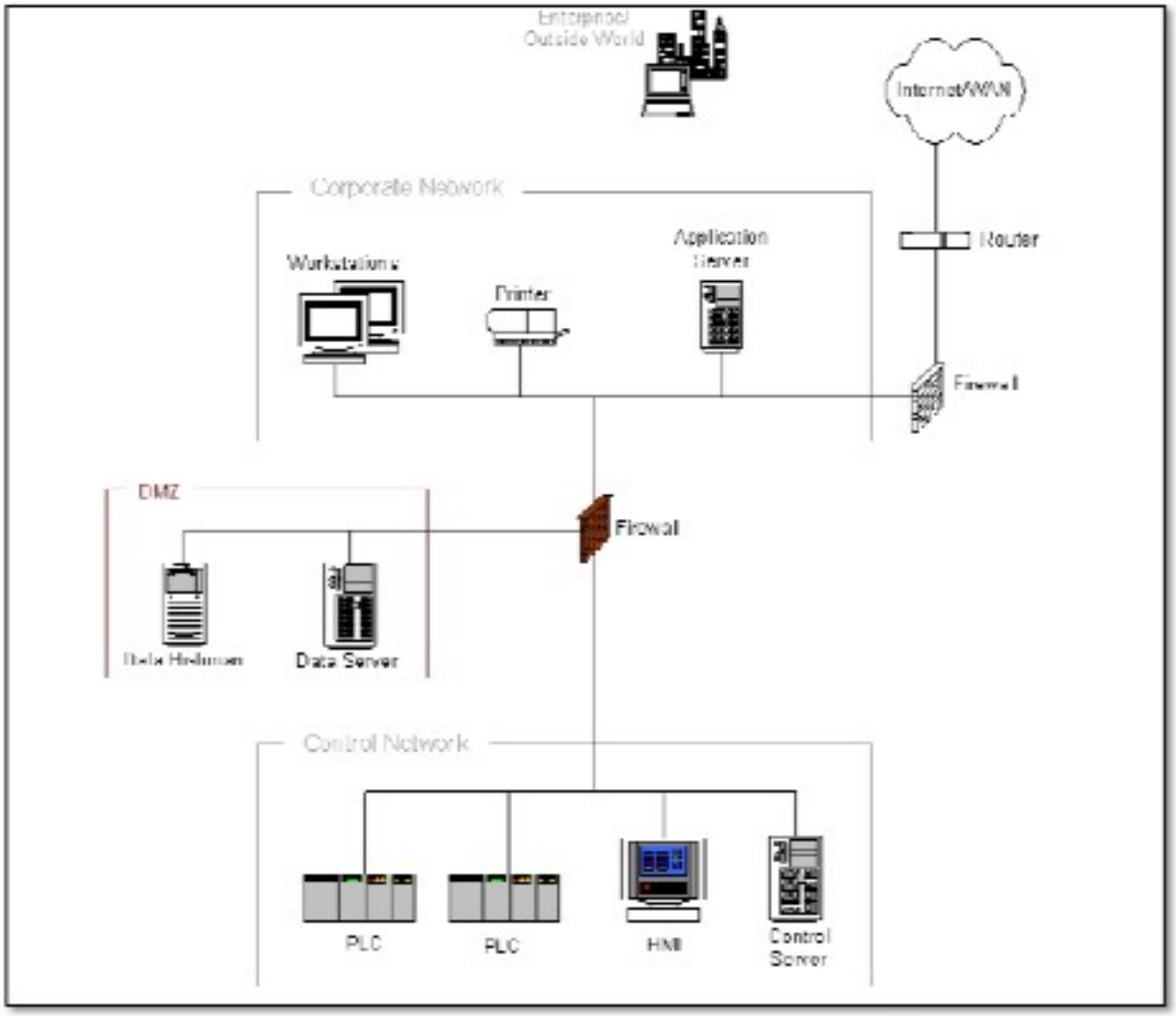


Figure III.4 : Pare-feu avec DMZ entre le réseau de contrôle et le réseau d'entreprise. [9]

En plaçant au niveau du DMZ des composants accessible de l'entreprise, aucun chemin de communication directe n'est requis du réseau d'entreprise au réseau de contrôle, chaque chemin se termine au niveau du DMZ. La plupart des pare-feu peuvent permettre plusieurs DMZ et peuvent spécifier quel type de trafic peut-être transmis entre les zones.

Avec un ensemble de règles bien planifiées, une séparation claire peut-être maintenu entre le réseau de contrôle et les autres réseaux, avec très peu voir aucun trafic entre le réseau d'entreprise et le réseau de contrôle.

Il serait meilleur aussi de choisir un antivirus différents dans le réseau de contrôle et celui d'entreprise. Par exemple, si un incident de logiciel malveillants se voit arriver et qu'un

produit Antivirus ne le détecte pas, il se peut qu'il ne passe pas inaperçu chez le second produit et qu'il puisse d'ailleurs l'arrêter.

Le risque de sécurité primaire sur ce genre d'architecture est que si un ordinateur sur le DMZ se voit compromis, il pourrait être par la suite utilisé pour déclencher une attaque contre le réseau de contrôle à l'aide du trafic permis entre ce dernier et le DMZ. Ce risque peut-être gratuitement réduit si des efforts supplémentaires sont fournis afin de renforcer et mettre à jour de façon active les serveurs sur le DMZ, et si les règles de pare-feu ne permettent que les connexions entre le réseau de contrôle et le DMZ utilisées par les dispositifs et appareils de contrôle.

Un autre souci lié à cette architecture est une complexité ajoutée et le risque potentiel d'augmentation du coût des pare-feu avec les différents ports.

Pour les systèmes critiques et sensibles, la sécurité améliorée compense largement ces avantages.

2.2. Paire de Pare-feu entre le réseau d'entreprise et le réseau de contrôle

Une variation sur la solution pare-feu avec le DMZ est l'utilisation d'une paire de pare-feu positionnée entre les réseaux ICS et le réseau d'entreprise, comme démontré sur **Figure III.5.**

Les serveurs commun comme l'historique de données sont situés entre les pare-feu dans le un réseau style DMZ. Comme c'est le cas aussi pour les architectures décrites plutôt, le premier pare-feu bloque des paquets arbitraires d'accès au réseau de contrôle et aux données partagées. Le deuxième pare-feu peut prévenir l'accès d'un trafic non-désiré d'un serveur compromis vers le réseau de contrôle, mais aussi éviter que le trafic du réseau de contrôle n'ait un impacte sur le serveur partagé.

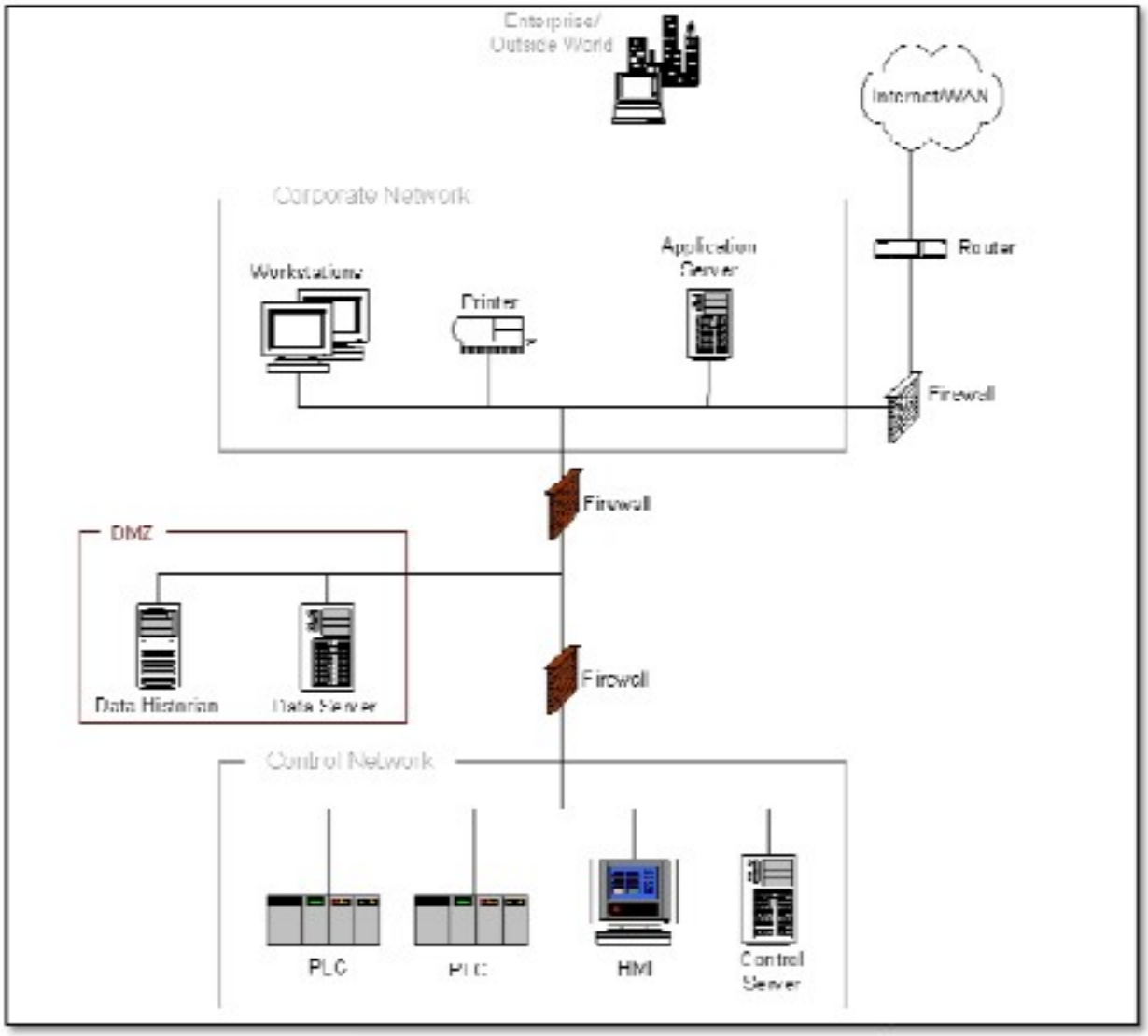


Figure III.5 : Paire de pare-feu entre le réseau de contrôle et le réseau d'entreprise [9]

Si des pare-feu de deux constructeurs différents sont utilisés, cela peut offrir certains avantages. Cela permettra aussi au groupe de contrôle et celui d'informatique (IT) d'avoir une responsabilité clairement séparée des appareillages et dispositifs, du moment que chacun peut gérer un pare-feu, si évidemment il en est décidé ainsi.

Le 1er désavantage de l'utilisation d'une architecture à deux pare-feu est l'augmentation du coût et la complexité de gestion. Pour les environnements avec des exigences de sécurité strictes, cette architecture a de gros avantages.

En résumé, les solutions sans pare-feu ne fourniront certainement pas une isolation adéquate entre les réseaux de contrôle et le réseau d'entreprise. Les solutions à deux zones (sans DMZ) sont marginalement acceptables et ne devrait être déployées qu'avec extrême soin.

III.2.3.2. Sécurisation technique

III.2.3.2.A. Pare-feu (Firewalls)

Les pare-feu réseaux sont des appareils/dispositifs ou systèmes qui contrôlent le flux du trafic réseau entre des réseaux employant différentes postures de sécurité.

Dans la plupart des applications modernes, pare-feu et leur environnement sont sujets à des discussions dans le contexte de la connectivité d'internet et le protocole TCP/IP. Néanmoins, les pare-feu peuvent être utilisés dans l'environnement réseau qui ne possède pas ou ne nécessite pas forcément une connexion à Internet. Par exemple, beaucoup de réseau d'entreprise emploient des pare-feu afin de restreindre la connectivité à des réseaux interne se chargeant de fonctions plus sensibles. Avec l'emploi des pare-feu afin de contrôler la connectivité au niveau de ces zones là, l'entreprise peut prévenir les accès non autorisés aux systèmes et ressources à l'intérieur des zones sensibles.

III.2.3.2.B. Pré-configuration du pare-feu

Etant donné l'existence de pare-feu dans le marcher qui sont déjà préprogrammé et fournit avec des logiciels internes (firmware) permettant la modification des règles de pare-feu selon le besoin.

Il est nécessaire de bien connaître les protocoles de communication adéquats, il existe d'ailleurs différents types et modèles de pare-feu industriels :

Pare-feu multi-protocoles : Avec une programmation rigoureuse autorisera les protocoles voulues et bloquera ceux non autorisé, selon évidemment le respect des adressages déjà présent au niveau l'architecture réseau. (Exemple : MDS Orbit)

Pare-feu Ethernet : Ce second type est strictement limité au contrôle d'accès des connexions sous le protocole Ethernet industriel. (Exemple : Pheonix Contact mGuard)

III.4. Plan économique

La première étape pour la mise en œuvre d'un programme de cyber-sécurité pour l'ICS est de développer une analyse de rentabilisation convaincante pour les besoins uniques de l'entreprise. Cette analyse devrait saisir les préoccupations des entreprises de la haute direction tout en étant fondée dans l'expérience de ceux qui sont déjà entrain de gérer beaucoup de risques du genre.

III.4.1. Bénéfices

La menace contre les ICS doit être mesurée et contrôlée afin de protéger les intérêts des employés, les actionnaires, clients, fournisseurs et l'entreprise en générale.

En addition à la réduction de risque, l'exercice de diligence raisonnable et afficher de la responsabilité aussi aide les entreprise afin d'atteindre les points et objectifs suivants :

- L'amélioration de la fiabilité et la disponibilité des systèmes de contrôle.
- L'amélioration de la confiance des investisseurs.
- L'amélioration de l'image et de la réputation de L'entreprise.
- Aide avec les couvertures d'assurance.
- L'amélioration des relations avec les investisseurs bancaires.

Un fort programme de gestion de sureté et cyber-sécurité est fondamental à un modèle d'entreprise durable.

III.5. Conclusion

Nous avons au court de ce chapitre, exposé et explicité de façon générale l'approche et les solutions d'atténuation possibles aux problèmes de cyber-sécurité. Notre étude sera basée sur le cas d'un système réel qui est : Le système de contrôle de la Cimenterie de MEFTAH (SCMI) objet des chapitres suivants.

Chapitre IV:

Présentation de la cimenterie de MEFTAH

IV.1. Introduction

La Société des Ciments de la Mitidja (S.C.MI) est une filiale du Groupe Industriel des ciments de l'Algérie (G.I.C.A.). Elle comprend une seule unité : la cimenterie de MEFTAH. La S.C.M.I a été réalisé dans le cadre du plan quadriennal de « 1970-1973 ». Elle fait partir des premières cimenteries installées en Algérie.

Ce chapitre va comporter une présentation de la cimenterie de MEFTAH afin de donner une idée générale sur les différentes étapes de la production de ciment.

IV.2. La situation géographique de la cimenterie

La Cimenterie de MEFTAH est localisée à proximité de la route nationale n°29, reliant la commune de MEFTAH à celle de Khemis-El-Khechna. Elle est implantée dans la commune de MEFTAH, Daira de Meftah, Wilaya de Blida. Elle est située à 27km au sud-est d'Alger. Elle est à une dizaine de kilomètres de la gare d'Oued-Smar et à une quinzaine de kilomètres de l'aéroport international d'Alger.

Figure IV.1 : Situation géographique de la cimenterie de MEFTAH. [6]

IV.3. Le processus de fabrication

Le ciment est un produit industriel fabriqué par broyage, mélange du clinker, du gypse et d'ajouts. Le clinker qui est le principal constituant des ciments est un produit semi fini obtenu par la cuisson d'un mélange des matières premières à haute température (1450 °C).

Ce mélange des matières premières est broyé finement avant la cuisson pour obtenir une farine qui contient certains composants (éléments chimiques) dont les propriétés sont bien définies.

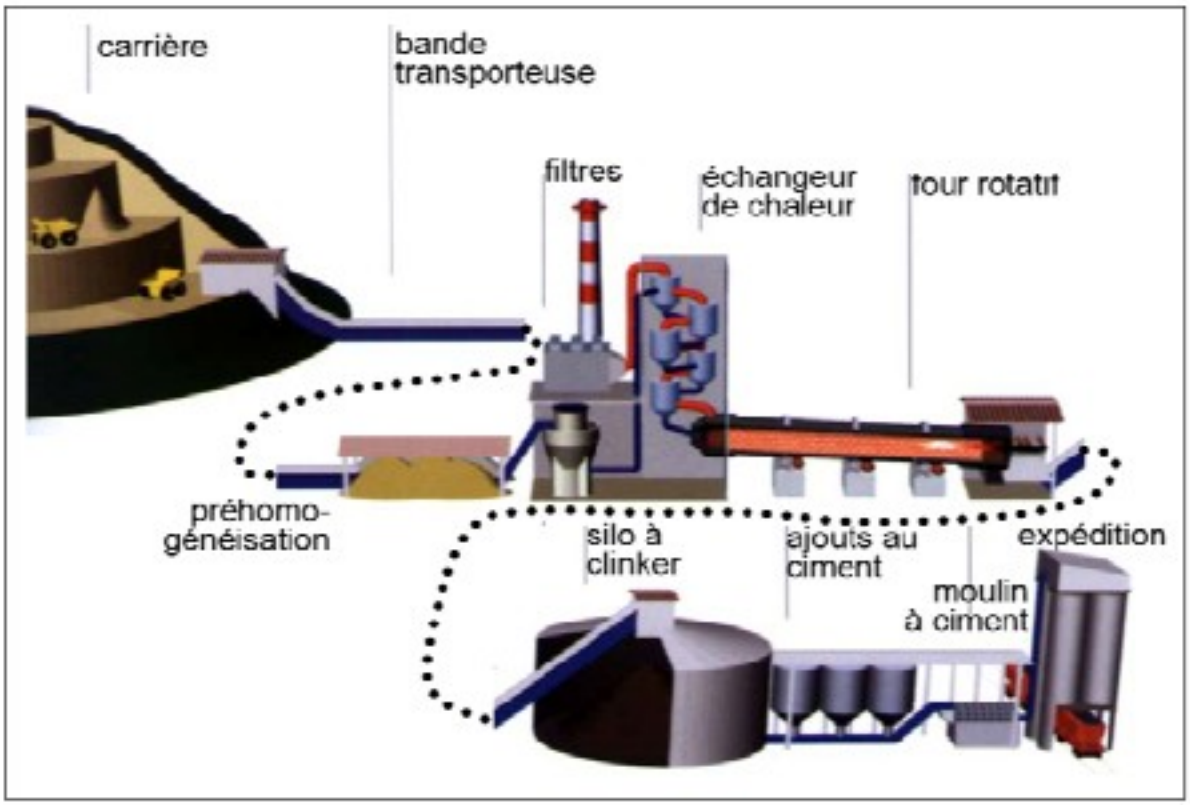


Figure IV.2 : Schéma de processus de fabrication du ciment. [6]

IV.4. Description de la ligne de production

L'usine possède une seule ligne de production, par voie sèche. Cette dernière est divisée en cinq zones, comme suit :

- Zone I : Carrières de calcaire/argile.
- Zone II : Cru.
- Zone III : Cuisson.
- Zone IV : Ciment.

- Zone V : Expédition.

IV.4.1. La zone carrière

Dans cette zone, on trouve :

a. Extraction et transport de la matière première

La cimenterie de MEFTAH exploite deux carrières à ciel ouvert par des pelles mécaniques ou encore par ripage au bulldozer :

- Une carrière de calcaire qui se situe à 1 km de l'usine.
- Une carrière d'argile qui se situe à 4km de l'usine.

Figure IV.3 : Extraction et transport de la matière première. [5]

b. Le concassage

Le calcaire est envoyé vers l'atelier de concassage. Les deux concasseurs FCB 450 T/h et KHD 1000 T/h réduisent les matériaux à une taille maximum de 80 mm. La roche est ensuite échantillonnée en continu pour déterminer la quantité des différents ajouts nécessaires (oxyde de fer, alumine, silice) et atteindre ainsi la composition chimique idéale. Le calcaire et l'argile sont ensuite transportés par les tapis T0, T1, T2 et T3 vers deux halls différents de pré-homogénéisation où la matière est stockée en couches horizontales superposées puis reprise verticalement.

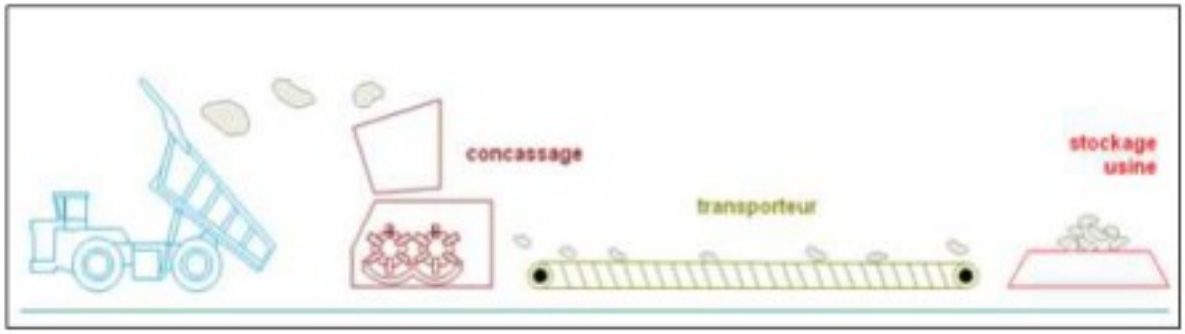


Figure IV.4 : Concassage et transport. [5]

IV.4.2. La zone CRU

a. La pré-homogénéisation

En général, deux constituants sont utilisés pour la préparation du cru : le calcaire et l'argile. Apres le concassage de ces deux constituants de base on obtient une granulométrie de « 0 à 25mm ». Une prise d'échantillon sera réalisée pour effectuer les analyses afin de déterminer la composition. Les deux composants sont acheminés vers l'usine par des transporteurs couverts, puis les matières premières sont stockées dans deux halls de pré-homogénéisation.

- ***Hall calcaire :*** Le gratteur portique sert à gratter le calcaire, il se déplace en translation de tas en tas et jetant la matière sur un tapis afin de la transporter à la trémie calcaire.
- ***Hall ajout :*** On trouve deux gratteurs semi portiques qui servent à gratter les ajouts (argile, fer et sable). Ils jettent les produits sur deux bandes transporteuses différentes.

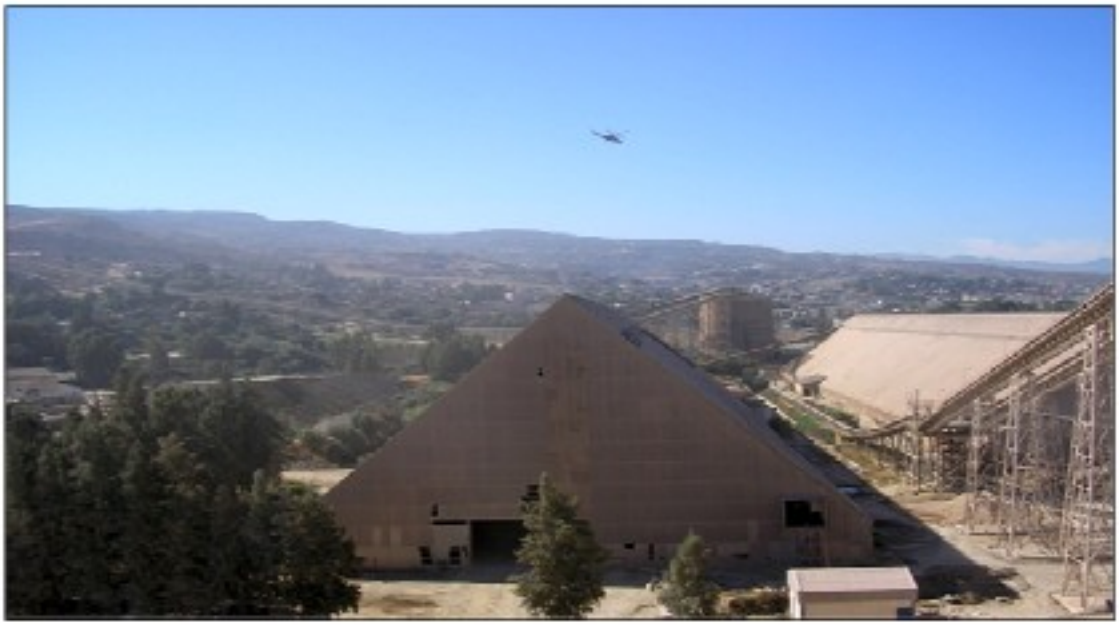


Figure IV.5 : Hall de pré homogénéisation. [6]

b. Broyeurs a cru

Pour favoriser les réactions chimiques ultérieures, les matières premières doivent être séchées et broyées très finement (quelques microns) dans un broyeur à boulets. A la sortie de broyeur, les matières premières sont parfaitement homogénéisées et séchées afin d'obtenir la farine. Celle-ci peut-être introduite directement dans le four sous forme pulvérulente.

Figure IV.6 : Broyage a cru. [6]

IV.4.3. La zone cuisson

La ligne de cuisson est constituée :

- D'un pré chauffeur.
- D'un four rotatif.
- D'un refroidissement.

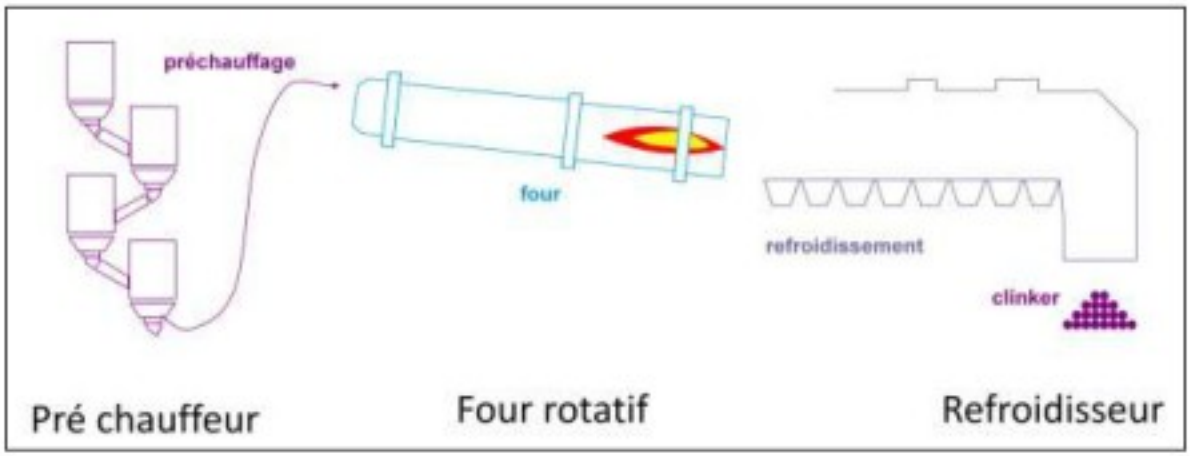


Figure IV.7 : La cuisson [5]

a. Préchauffage ou cyclones

Les gazes réchauffent la poudre cru qui circule dans les cyclones. La poudre s'échauffe jusqu'à 800°C environ et perd donc son gaz carbonique (CO_2) et son eau.

b. Four rotatif

La cuisson se fait à une température voisine des 1450 °C dans un four rotatif, long cylindre tournant de 1,5 à 3 tours/minute et légèrement incliné. A cette température appelée température de clientélisation, des réactions physico-chimiques se produisent et donnent lieu à la formation d'un produit qu'on appelle le clinker.

Figure IV.8 : Le four rotatif [6]

c. *Refroidissement*

Le clinker à sa sortie du four est encore chaud (800°C), pour le manutentionner dans les bonnes conditions, il est nécessaire de le refroidir jusqu'à une température permettant sa manipulation.

Un refroidisseur à grille permet d'assurer la trempe des nodules incandescents et de les ramener à une température d'environ 100 degrés.

IV.4.4. La zone Ciment

a. Le remplissage des trémies

Le gypse est transporté vers la trémie de récupération par des camions. Il sera transporté sur le tapis T19 qui déverse sur T20. A l'aide d'un élévateur gypse, ce dernier sera stocké dans le silo de stockage gypse de capacité de 5000 T.

b. Broyage ciment

Le broyage de clinker qui se fait au niveau de l'atelier de broyage Ciment, est l'opération qui consiste à moudre le mélange principalement clinker et gypse dont les proportions déterminées aussi finement que possible pour obtenir un produit appelé ciment artificiel, c'est-à-dire un liant hydraulique. Plus le ciment est fin, meilleure sera sa résistance

une fois mis en œuvre. Donc, le paramètre auquel une attention particulière doit être portée pendant l'opération de broyage, c'est le contrôle de la finesse du produit.

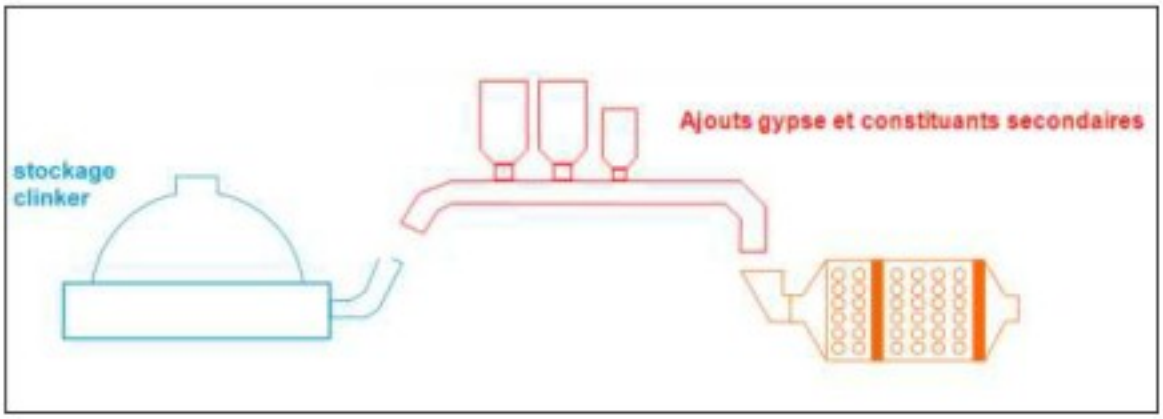


Figure IV.9 : Broyage ciment. [5]

IV.4.5. La zone expédition

Le ciment est stocké dans huit silos avec une capacité de 500T chacun. L'expédition du ciment se fait en sac ou en vrac.

- **Expédition en sac :** Elle est réalisée par quatre ensacheuses avec un débit de 90 T/h. chacune possède huit becs pour le remplissage des sacs. Les sacs de 50 Kg sont chargés sur des camions à bennes.
- **Expédition en vrac :** Le remplissage se fait par un flexible branché au font d'une trémie et qui est dirigé par l'opérateur pour mettre a l'intérieur de la bouche de cocotte des camions pour les remplir.

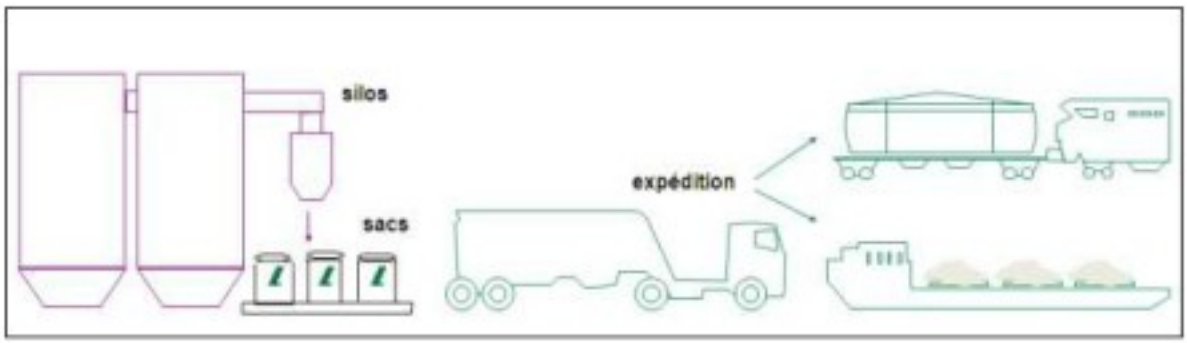


Figure IV.10 : Expédition en sac ou vrac. [5]

IV.5. Conclusion

Dans ce chapitre, nous avons décrit le processus de fabrication du ciment qu'on a pu voir au sein de la cimenterie de MEFTAH. Notre étude est basée sur le système de contrôle mis en œuvre au niveau de cette installation et son amélioration, objet du chapitre suivant et final.

Chapitre V:

Etude de cas : « Système de contrôle de la SCMI »

V.1. Introduction

A la suite de l'étude approfondie des systèmes de contrôle, des vulnérabilités qui y existent déjà et des solutions possibles de façons générales vu dans les trois premiers chapitres, il sera question dans ce celui-ci d'une application de notre solution de cyber sécurité à un cas réel : Système de contrôle de la ligne de production de la cimenterie de MEFTAH.

V.2. Architecture du réseau du système de contrôle de la SCMI

La ligne de production de la SCMI est gérée par un système de contrôle distribué ou plus communément appelé : Réseau d'AUTOMATES.

La **Figure V.1** suivante représente cette architecture :

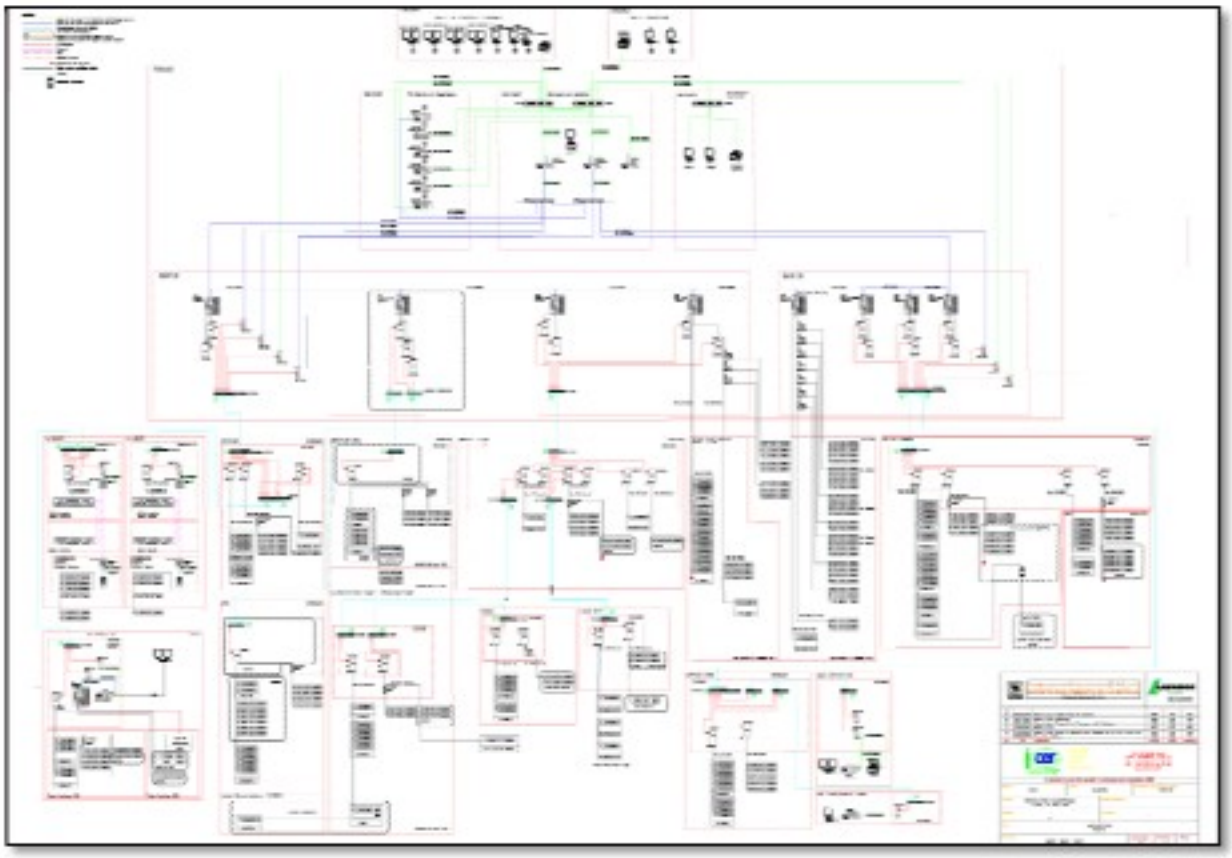


Figure V.1 : Architecture du réseau globale du système de contrôle de la SCMI [4]

Répartition du réseau

Ce réseau est réparti en 2 zones et 4 niveaux, comme suit:

- Zone 1 : Réseau de contrôle.
- Zone 2 : Réseau d'entreprise.

- Niveau 1 : Supervision
- Niveau 2 : Contrôle Commande
- Niveau 3 : Automates programmables
- Niveau 4 : Site de terrain (Field site).

Zone 1 : Réseau de contrôle

La première zone est représentée par tout le réseau de contrôle, incluant supervision, contrôle commande, automates et même le site de terrain. La **Figure V.2** expose la première zone qui est : « Le réseau de contrôle »

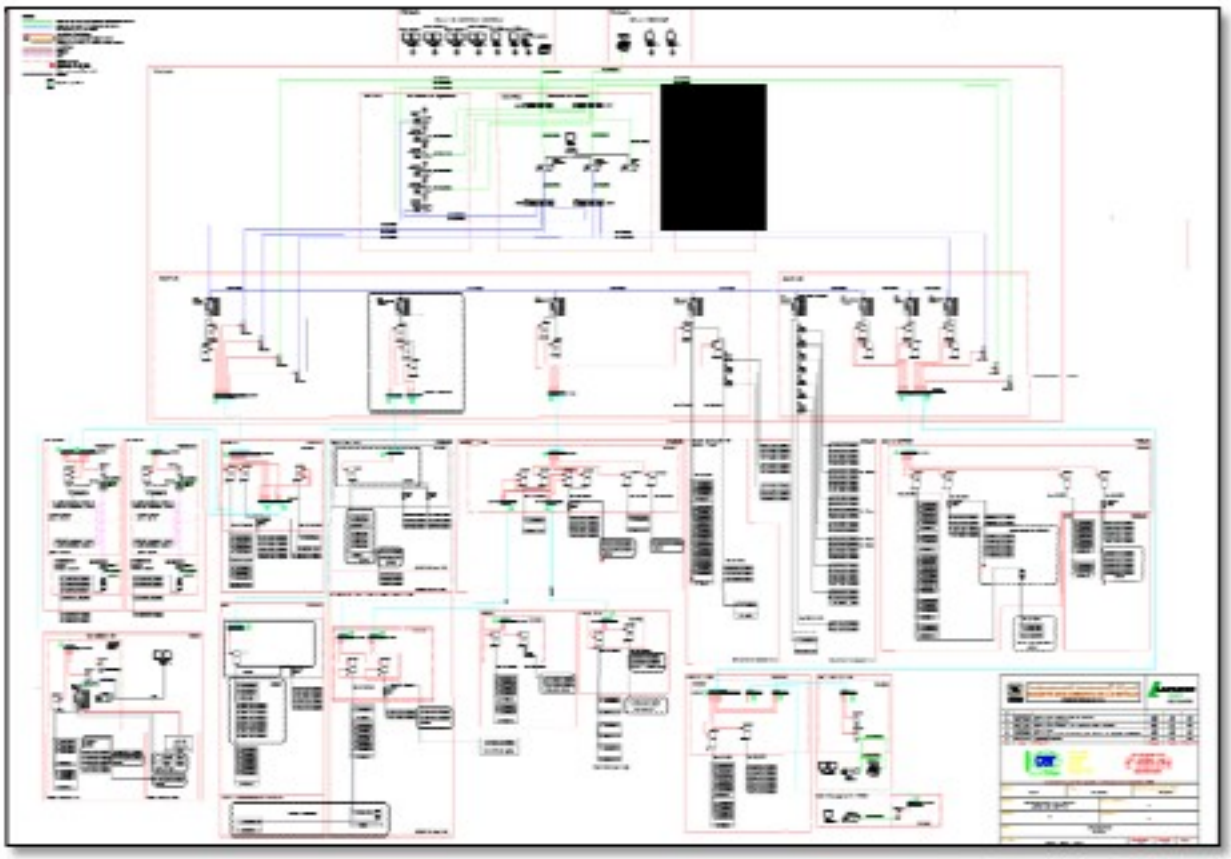


Figure V.2 : Zone 1 « Réseau de contrôle » [4]

Zone 2 : Réseau d'entreprise

La seconde zone est représentée par tout ce qui reste de l'architecture étant le réseau d'Entreprise. La **Figure V.3** expose la seconde zone qui est le réseau d'entreprise :

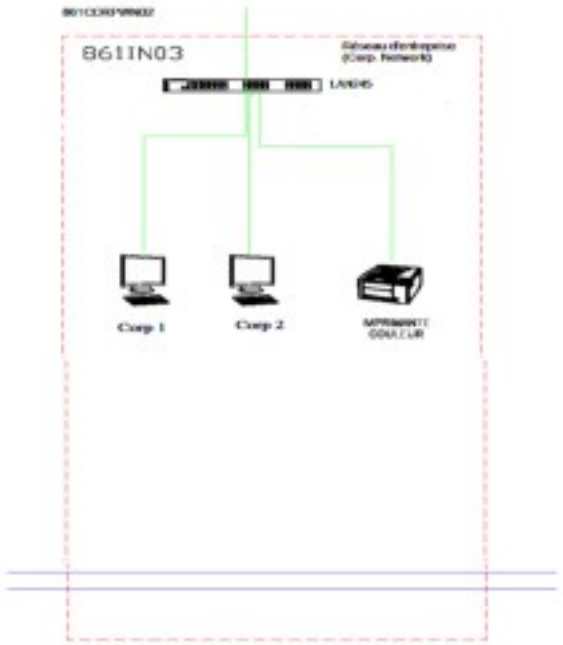


Figure V.3 : Zone 2 « Réseau d'entreprise » [4]

Les 4 niveaux de l'architecture réseau sont présentés comme suit :

Niveau 1 : Supervision

Ce niveau contient deux salles de contrôle

- Salle de contrôle centrale : **731SU01 ;**
- Salle Ingénieurs : **731SU03** ;

La **Figure V.4** représente le premier niveau du système de contrôle :

Figure V.4 : Niveau 1 du système de contrôle « Supervision » [4]

Niveau 2 : Contrôle Commande

Ce niveau est composé de 3 parties :

- PC Clients et Ingénieurs
- Serveurs et Switches
- Réseau d'entreprise

La **Figure V.5** expose en détails le deuxième niveau de notre système de contrôle :

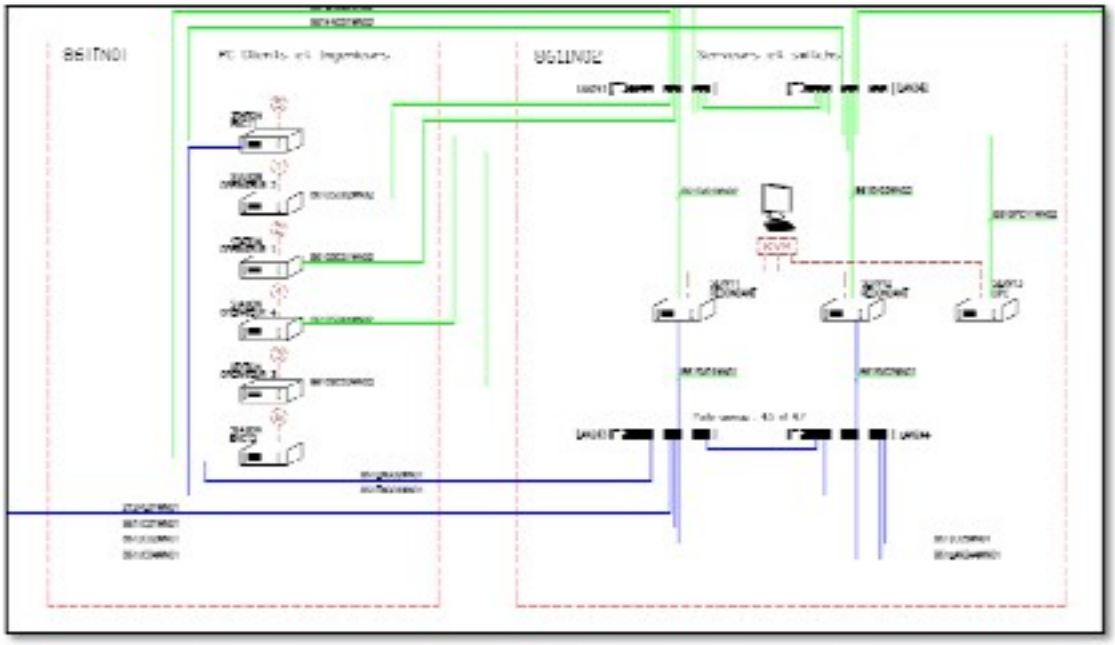


Figure V.5 : Niveau 2 du système de contrôle « Contrôle Commande »

Niveau 3 : Automates programmables : (861PL01)

Ce niveau est composé de 8 parties :

- CPU Reprise ;
- CPU Broyeur cru ;
- CPU Amont four ;
- CPU Aval four ;
- CPU utilités ;
- CPU BK1 et communs ;
- CPU BK2 ;

- CPU Expéditions ;

Les deux **Figure V.6.1 et V.6.2** suivantes représentent le niveau 3 de notre ICS

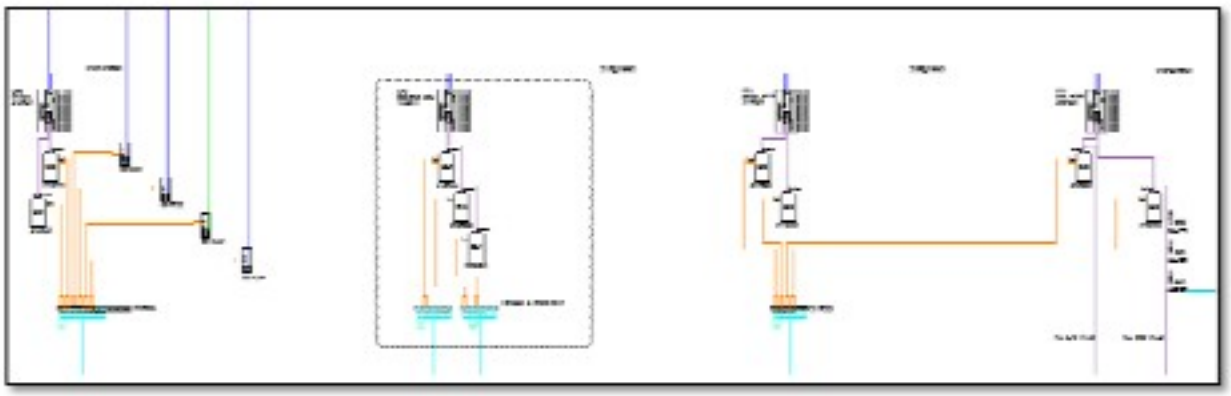


Figure V.6.1 : Niveau 3 du système de contrôle « Automates programmables » [4]

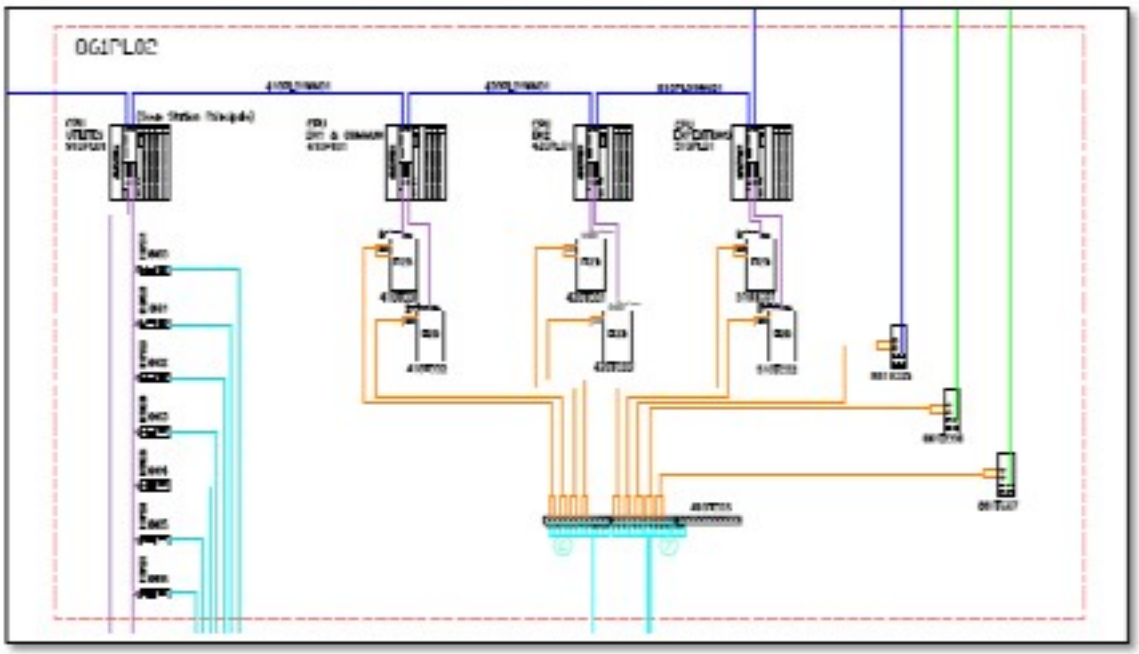


Figure V.6.2 : Niveau 3 du système de contrôle « Automates programmables » [4]

Niveau 4 : Site de terrain

Ce dernier niveau est composé de 14 parties, comme suit :

- Reprise ;

- Hall Calcaire ;
- Hall Ajouts ;
- Broyeur cru ;
- Massif Four ;
- Sous-station P0 ;
- BK1 et communs ;
- SdC Carrière FCB ;
- APS ;
- Alimentation FOUR + PRECHAUFFEUR ;
- IMASA ;
- Expéditions ;
- SdC expéditions ;
- SdC Chargement Vrac ;

La **Figure V.7** illustre de façon globale toutes les parties qui composent le 4ème niveau du système de contrôle la cimenterie de MEFTAH :

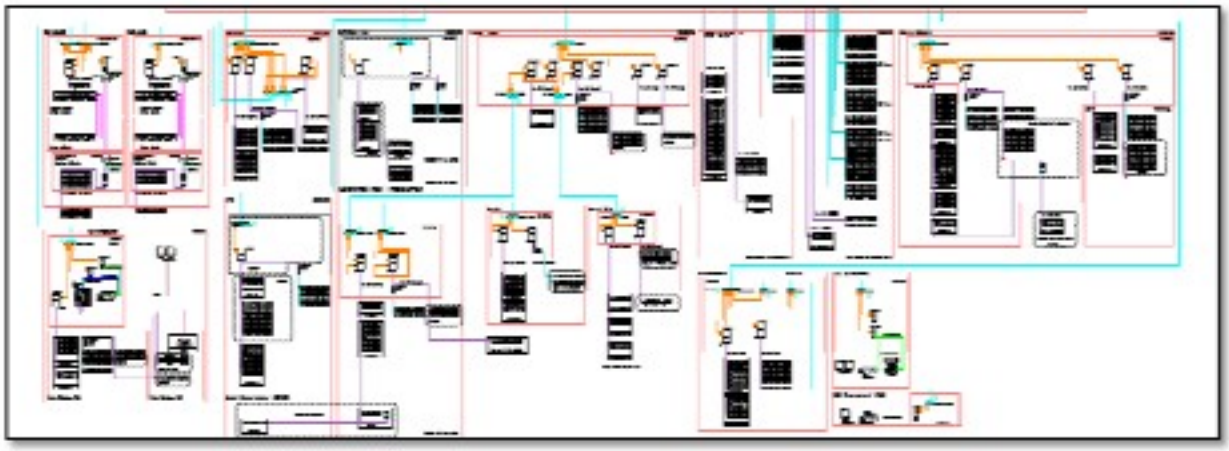


Figure V.7 : Niveau 4 du système de contrôle « Site de terrain » [4]

V. 3. Inventaire des atouts de l'ICS

V.3.1. Logiciel d'inventaire Open-audiT du réseau

Afin de détecter tous les éléments que regroupe notre réseau d'automates, nous avons utilisé le logiciel d'inventaire « Open-audiT ». C'est un outil d'inventaire, de vérification, documentation et de gestion d'un réseau. Les étapes d'utilisation sont les suivantes :

1- Se connecter au serveur Open-AudiT

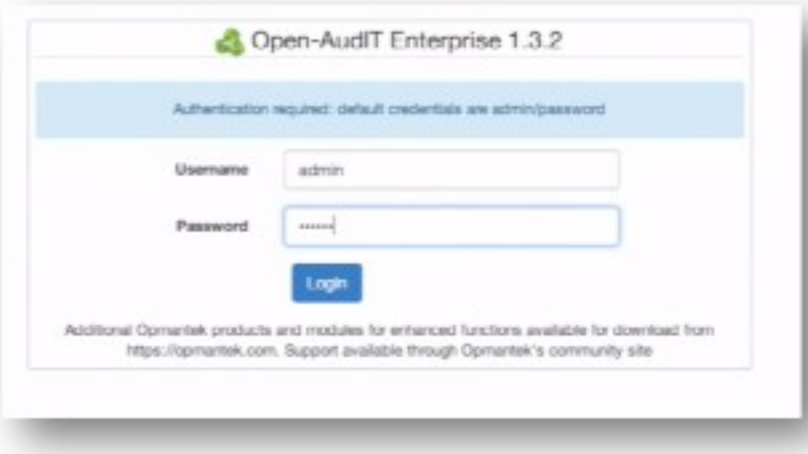


Figure V.8 : Fenêtre d'identification au Panel d'Open-AudiT

2- Accéder à la fonction découverte : View >> Discovery

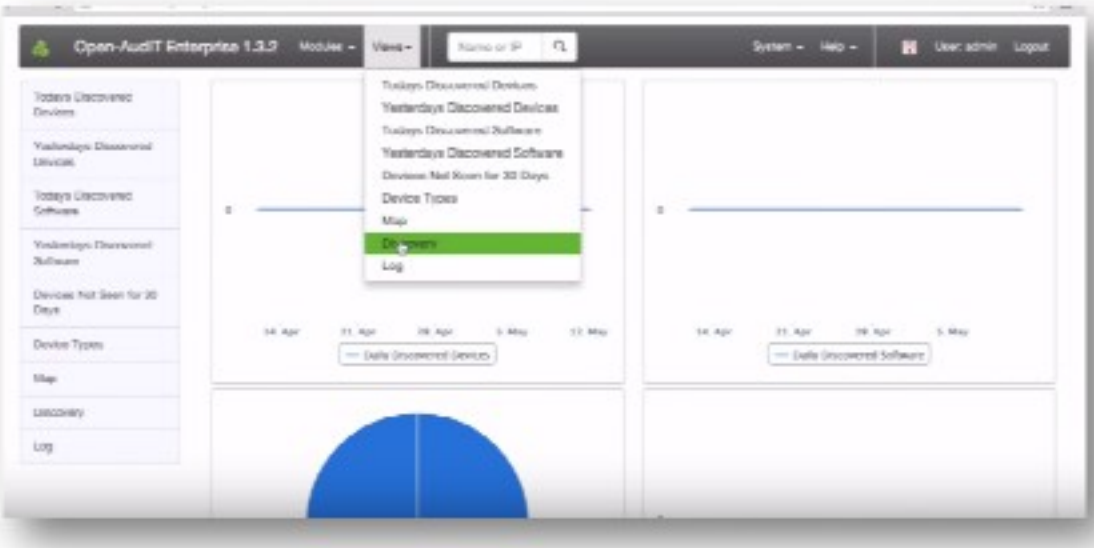


Figure V.9 : Accès à la fonction découverte

3- Scanne d'un sous réseau : Il faudra sélectionner avec précision le rang d'adresse IP à scanner au niveau de notre réseau. Voir **Figure V.10**

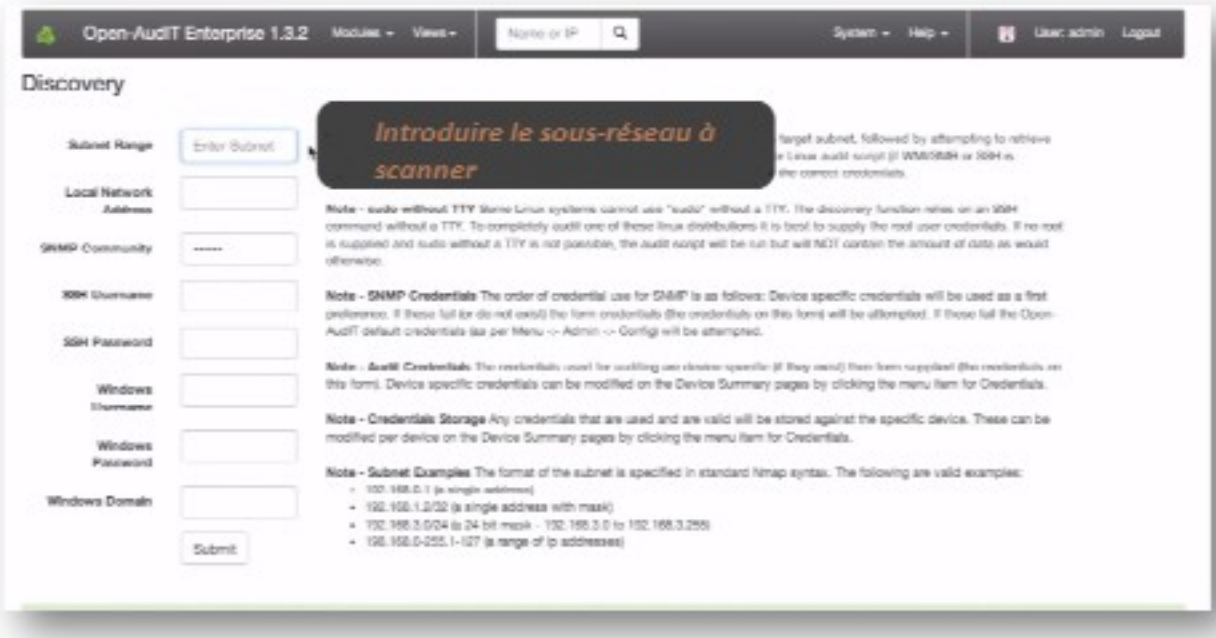


Figure V.10 : Fenêtre de sélection des sous réseaux à scanner

Il faudra introduire avec précision le rang d'adresse IP à scanner au niveau de notre réseau, comme suit :

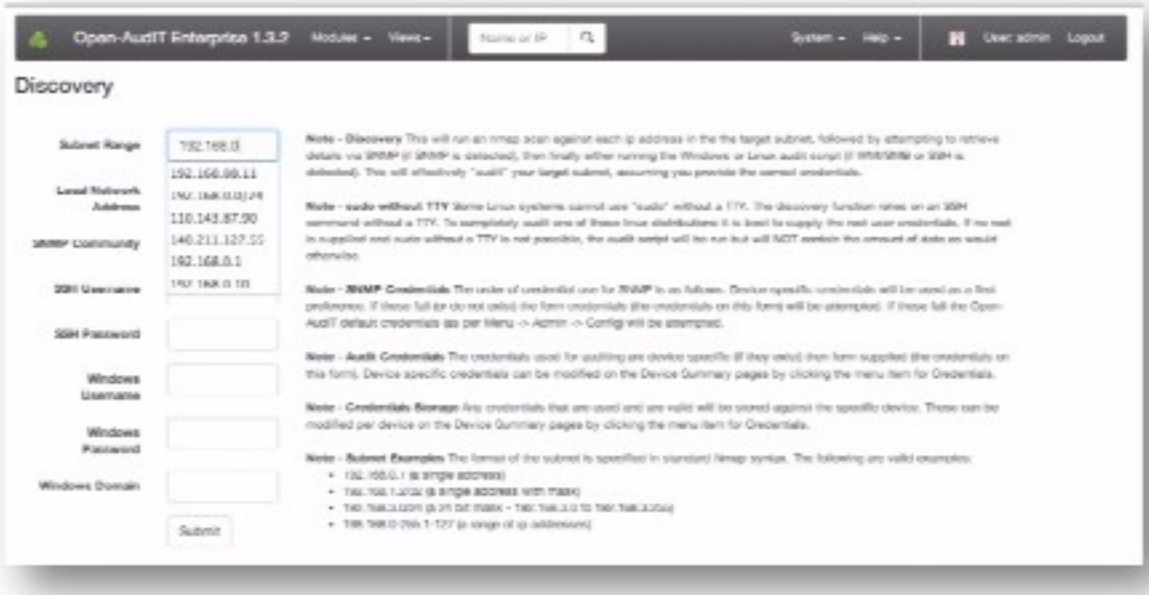


Figure V.11 : Précision du rang d'adresse IP

4- Introduction des identifiants (ou login) :

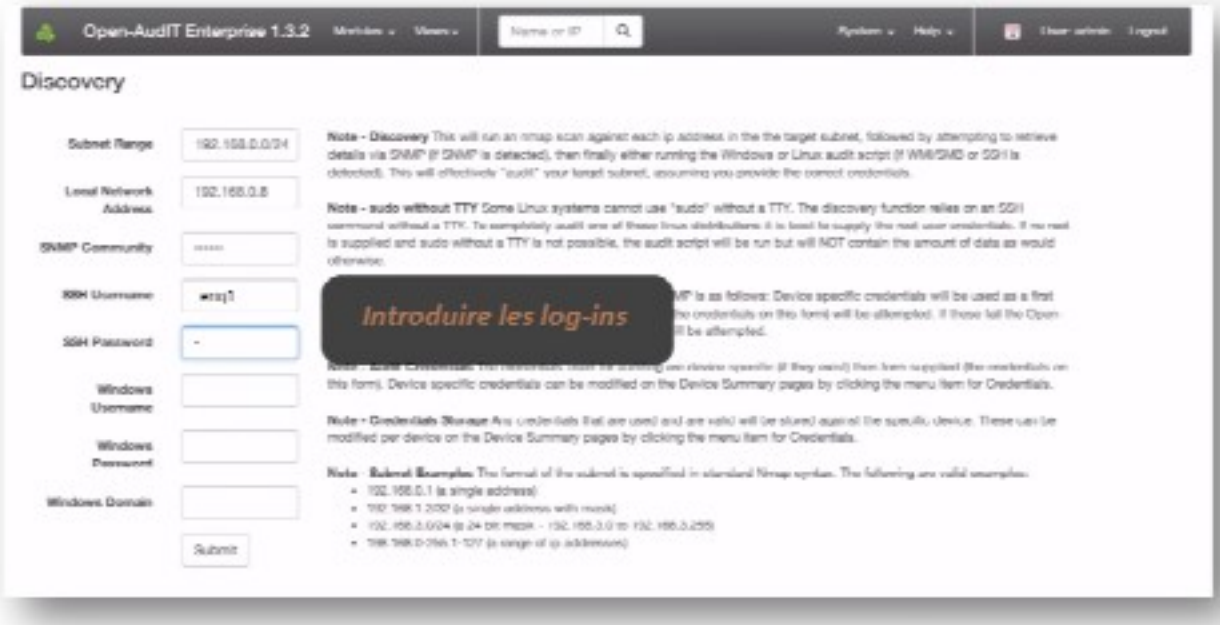


Figure V.12 : Introduction des identifiants

5- Démarrage de l'inventaire :

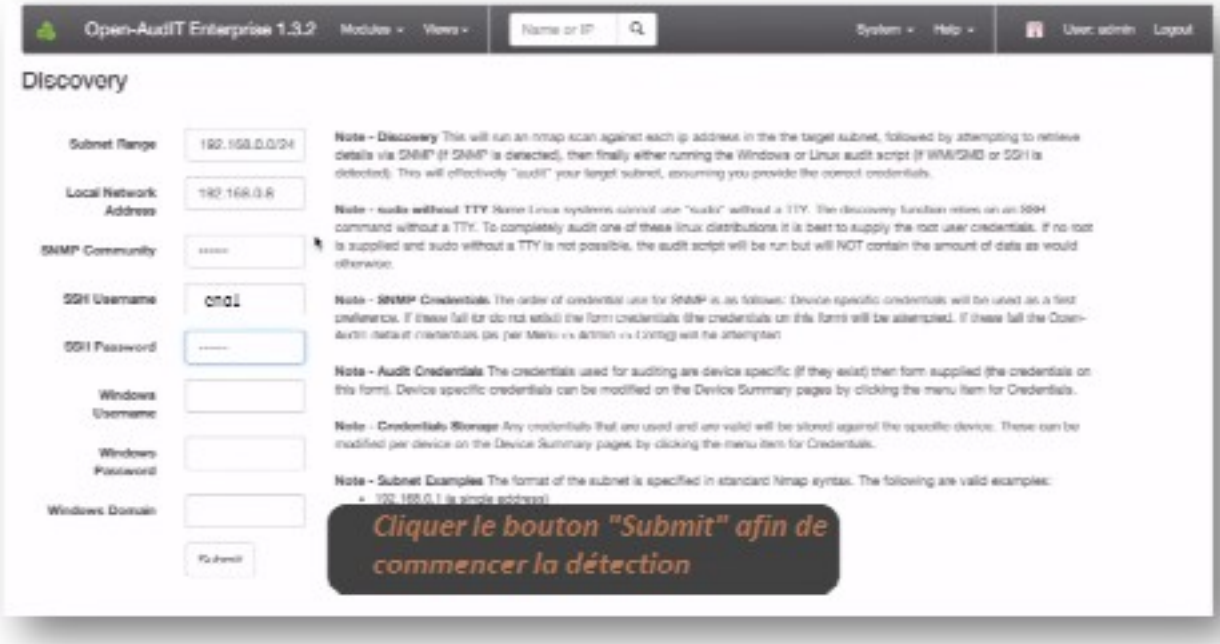


Figure V.13 : Le démarrage de l'inventaire

V.3.2. Instrumentation

A la suite de l'inventaire réussi, ce qui suit met du relief sur les grandes lignes, instrumentations importantes et logiciels de notre système de contrôle :

- ***API SIEMENS S7 CPU 416-3DP***

Figure V.14 : API S7 416-3DP[5]

Cette automate possède les fonctionnalités du PROFINET avec les caractéristiques suivantes :

- RAM 11.2 MB ;
- L'interface maître-DP MPI/PROFIBUS ;
- Interface additionnelle PROFIBUS DP ;
- Interface additionnelle PROFINET ;
- Slot additionnelle pour un module IF ;
- Slot pour carte mémoire ;

- ***APU SIEMENS S7 CPU 315***

Figure V.15 : API S7 315[5]

Cette CPU offre les sous réseaux suivants :

- MPI ou PROFIBUS-DP ;

➢ ***STATION ET200***

SIMATIC ET 200 est une famille de stations périphériques décentralisées très diversifiée pour l'installation en armoire ou le montage direct sur la machine sans armoire, ou encore pour l'emploi en zone à atmosphère explosible.

La modularité des stations ET 200 favorise leur adaptabilité et leur extensibilité graduelle : entrées/sorties TOR et analogiques, modules intelligents à fonction CPU, constituants de sécurité, départs-moteurs, dispositifs pneumatiques, variateurs de vitesse et divers modules technologiques.

- ET 200M :

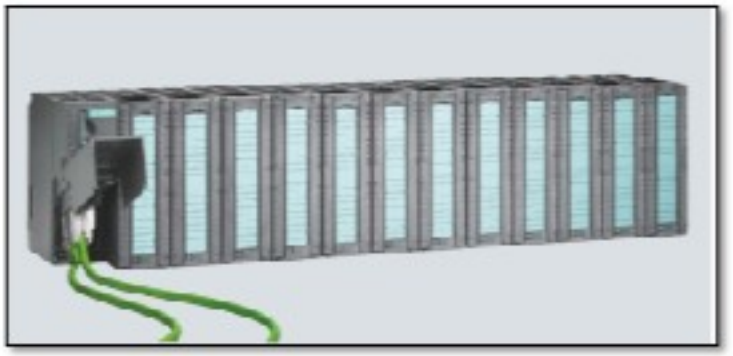


Figure V.16 : ET 200M avec connexion PROFINET et CPU S7-300 [8]

Le système de périphérie décentralisée ET 200M est de conception modulaire. Elle peut être configurée avec 12 modules de périphérie : des modules d'entrées/sorties haute densité (par ex. 64 entrées TOR) ou des modules de fonction ou encore des processeurs de communication S7-300. Il n'y a pas de règles pour l'emplacement des modules. La configuration avec des modules de bus actifs permet de remplacer et d'ajouter des modules en cours de fonctionnement, voir **Figure V.16.**

- *ET 200S :*

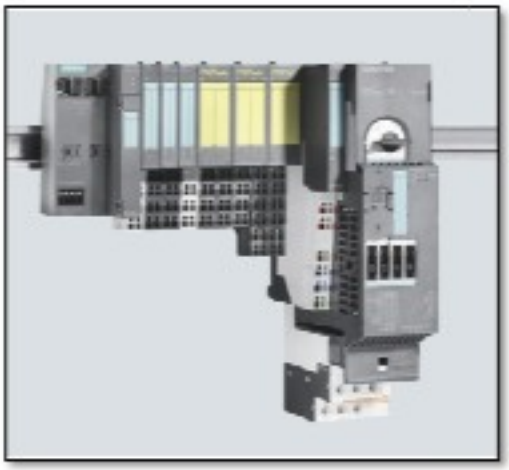


Figure V.17 : ET 200S avec connexion PROFINET, modules E/S et départs-moteurs. [8]

SIMATIC ET 200S est la station de périphérie multifonctionnelle, qui s'adapte exactement à la tâche d'automatisation. Sa construction robuste lui permet de supporter des sollicitations mécaniques élevées. Voir **Figure V.17.**

➢ ***Convertisseur PROFIBUS – Fibre optique***

Figure V.18 : Convertisseur PROFIBUS-Fibre (ICF-1180I) [11]

Les convertisseurs PROFIBUS vers fibre industriels de la série ICF-1180I servent à convertir des signaux PROFIBUS du cuivre vers la fibre optique, voir **Figure V.18**

- ***Répéteur de PROFIBUS***

Figure V.19 : Répéteur de PROFIBUS [11]

Les répéteurs PROFIBUS DP permettent de s'affranchir des limitations liées aux spécifications du réseau et de s'adapter à vos contraintes usine. Ils offrent de nombreux bénéfices dans l'architecture de vos installations : liberté de topologie pour votre réseau : les configurations arbre ou étoile deviennent possible, dérivations possibles, extension du nombre d'équipements sur un réseau, extension de la longueur du réseau, protection contre les courts-circuits sur chaque voie, insertion / suppression d'équipements à chaud, intégration de fonctions de diagnostic. Voir **Figure V.19**

- ***Borne Wifi Industrielle***

Figure V.20: Borne Wifi Industrielle fonctionnant en point d'accès [11]

➢ *Variateur de vitesse*

Figure V.21 : Variateur de vitesse [11]

Un variateur électronique de vitesse est un dispositif destiné à régler la vitesse et le moment d'un moteur électrique à courant alternatif en faisant varier la fréquence et la tension, respectivement le courant, délivrées à la sortie de celui-ci. Voir **Figure V.21**

V.3.3. Interface logiciels et HMI

V.3. 3.1. Progiciel SIEMENS SIMATIC PCS7

C'est un système de conduite de processus qui, grâce à de nombreuses fonctions automatiques, la création d'un projet sera facile, il nous offre parallèlement de nombreuses possibilités de créer des solutions individuelles et spécifiques aux projets, adaptés a nos besoins. Utile et facilite grandement tout type de programmation sur les automates Siemens

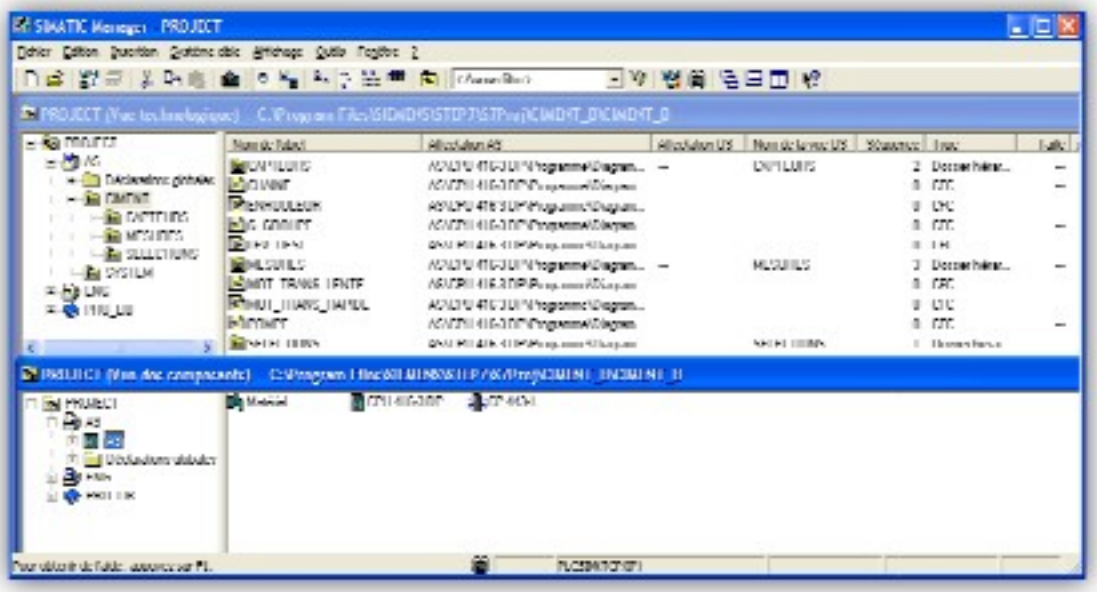


Figure V.22 : Vue d'un projet sous SIMATIC PCS7 [15]

V.3. 3.2. Interface Homme Machine (IHM) Supervision WinCC

Le WinCC est une HMI performante, c'est l'interface utilisée pour le contrôle commande des processus par API. Le WinCC nous permet de visualiser le processus et de concevoir l'interface utilisateur graphique destinée à l'opérateur. Voir **Figure V.23**

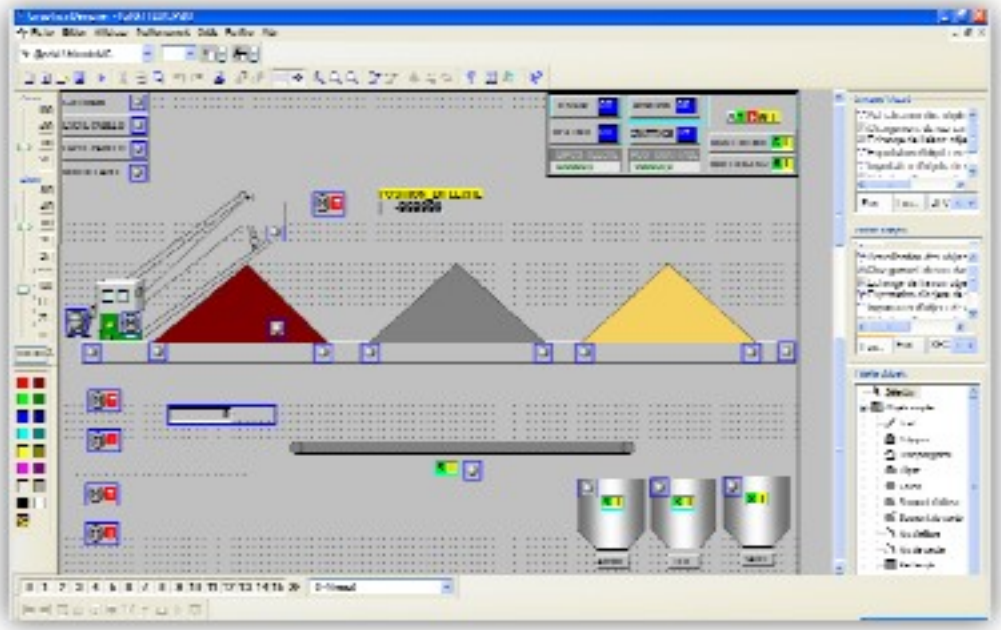


Figure V.23 : Création d'une vue de Supervision sous WinCC Graphics designer [15]

V.3.4. Normes et protocoles de communication

Différents réseaux sont proposés en fonction des exigences de la communication industrielle, ils sont listés ci après par niveau de performance croissant :

V.3.4.a. MPI (Multipoint Interface)

Le réseau MPI (Multi Point Interface) est utilisé pour les interconnections de faible étendue aux niveaux terrain et cellule. Il ne peut cependant être utilisé qu'avec les automates SIMATIC S7.

Celle-ci a été conçue comme interface de programmation, elle atteint rapidement ces limites lorsque les exigences de la communication sont sévères.

a. PROFIBUS

Le réseau PROFIBUS (Process Field Bus) est le nom d'un type de bus de terrain propriétaire et de son protocole, inter-automates et de supervisions. Il est devenu peu à peu une norme de communication dans le monde de l'industrie ces dix dernières années, mais son usage tend à disparaître au profit d'autre bus de terrain ou de réseaux.

Un bus de terrain est un système d'interconnexion d'appareils de mesures, capteurs, actionneurs, etc.

b. Industriel Ethernet

Réfère à l'utilisation des protocoles Ethernet standards avec ses connecteurs robustes et les commutateurs de température étendue dans un environnement industriel pour l'automatisation ou le contrôle de processus. Les composants utilisés dans les zones de traitement de l'usine doivent-être conçus pour fonctionner dans des environnements difficiles, d'extrêmes températures, d'humidité et des vibrations dépassent les plages limite des équipements de technologie de l'information destinés à être utilisé dans des environnements contrôlés. Il est le réseau le plus puissant pour la communication industrielle, il nécessite peu de manipulation, de configuration et aisément extensible.

c. MODBUS

C'est est un protocole de communication non-propriétaire, créé en 1979 par Modicon, utilisé pour des réseaux d'automates programmables, relevant du niveau 7 (applicatif) du Modèle OSI. Ce protocole a rencontré beaucoup de succès depuis sa création du fait de sa simplicité et de sa bonne fiabilité. Un regain d'intérêt lui confère un certain avenir depuis son encapsulation dans les trames Ethernet grâce à MODBUS over TCP/IP.

V.4. Analyse des vulnérabilités du réseau

Afin de détecter et lister les vulnérabilités présentes au niveau de notre système de contrôle, nous avons suivis les étapes suivantes :

- ✓ Etude de l'architecture réseau d'un point de vue sécuritaire ;
- ✓ Vérification physique du câblage ;
- ✓ Ecoutes passives du réseau à l'aide d'un détecteur d'intrusion.

V.4.1. Logiciel SNORT

La détection d'intrusion a été faite à l'aide d'un des logiciels disponibles sur le marché étant « SNORT » comme suit :

1- Lancement de SNORT

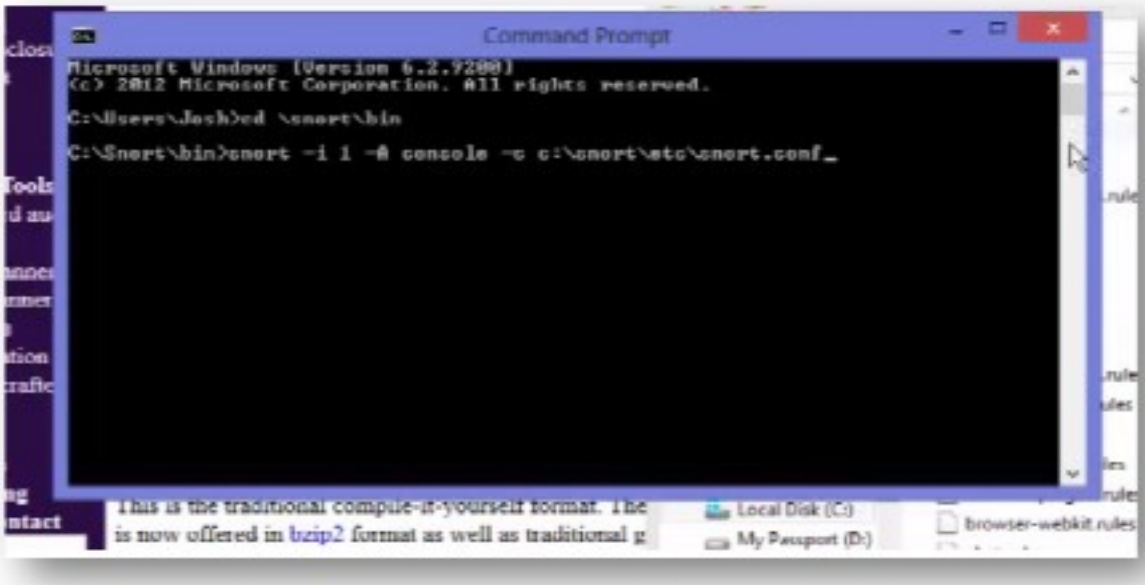


Figure V.24 : Lancement de SNORT

2- Démarrage de l'écoute passive :

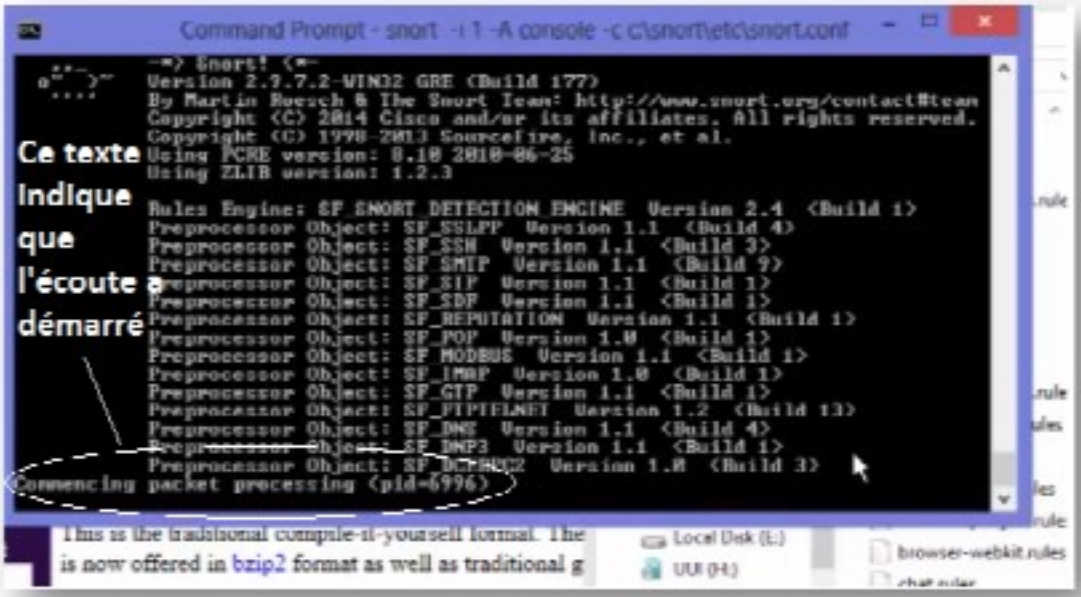


Figure V.25 : Démarrage de l'écoute passive

3- Vérification de tout type d'activité :

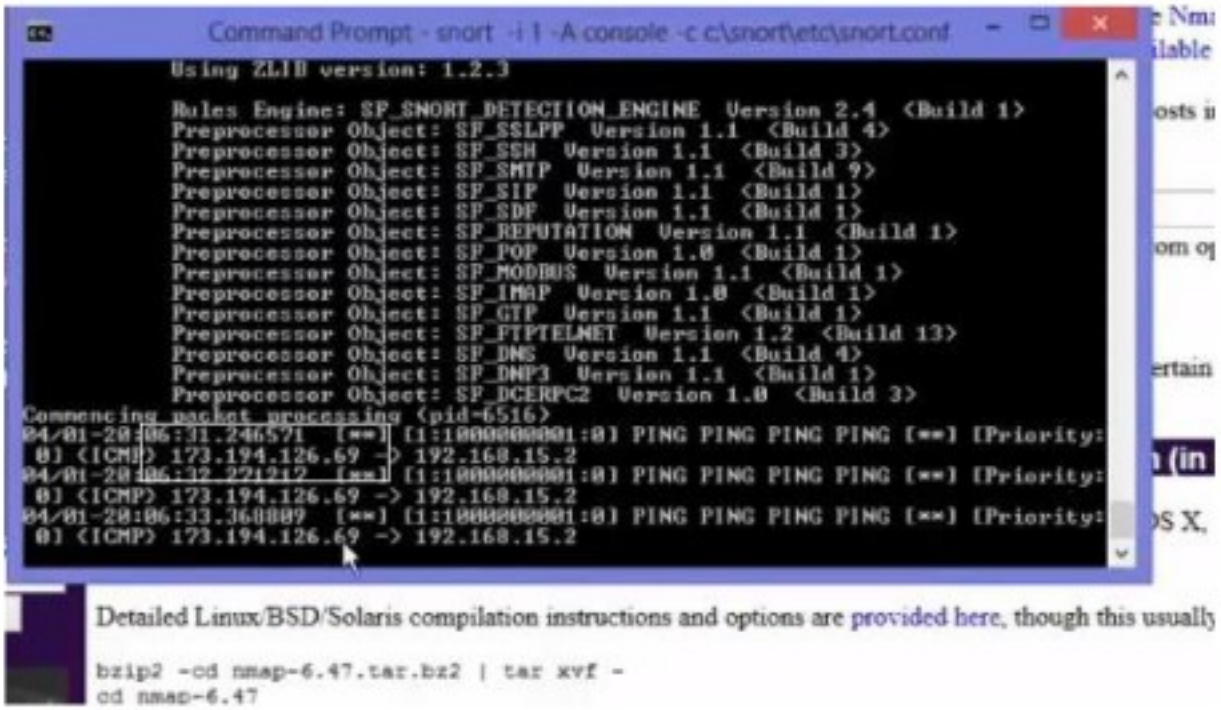


Figure V.26 : Détection d'activité avec SNORT

Comme on peut le voir sur la **Figure V.26**, SNORT détecte tout type d'activité sur le réseau avec précision de l'adresse IP du dispositif en cours d'activité (cadre blanc.)

V.4.2. Liste des vulnérabilités

A la suite de l'analyse de vulnérabilité faite sur notre système de contrôle, nous avons listé les vulnérabilités suivantes :

- Réseau en 2 zones ;
- Connexions directes entre le réseau de contrôle et le réseau d'entreprise ;
- Aucune présence de pare-feu ou de dispositifs de sécurité ;

V.5. Implémentation de la solution

L'amélioration du réseau d'automates a été faite suivant deux approches et aspects à la fois différents et complémentaires, comme vu à la **section III.2.3.**

V.5.1. La sécurisation fonctionnelle

Nous avons effectué des modifications sur notre architecture réseau avec l'addition d'un sous réseau « DMZ » qui regroupe des éléments clés de notre système de contrôle.

V.5.2. La sécurisation technique

V.5.2.1. Pare-feu

Nous visons à créer une isolation totale du réseau de contrôle de celui de l'entreprise et de tout type de menaces extérieures. Afin de parfaire les modifications de l'aspect fonctionnel, nous avons placé et configuré des pare-feu à des endroits stratégiques, afin qu'il n'y ait aucune connexion directe entre le réseau de contrôle et celui de l'entreprise.

Le choix du pare-feu s'est tourné vers un « FL mGuard » de la firme Pheonix Contact

V.5.2.1.1. Pare-feu FL MGUARD [14]

Le pare-feu FL de la série « mGuard » de la firme Phenoix Contact, voir **Figure V.27.**

Offre énormément de possibilité notamment :

- Performances élevées avec un débit de données maximal de 99 MBit/s ;
- Configuration simple et rapide avec le pare-feu ;
- DMZ pour plus de sécurité ;
- Les réseaux séparés pour les applications séparées sont protégés conjointement ;

Figure V.27. : Pare-feu de sécurité FL MGUARD de la firme PHOENIX CONTACT [14]

V.5.2.1.2. Logique de programmation

Comme l'explique la **Figure V.28**, il sera question en premier lieu de bloquer tout type de connexions non-désirées entre les dispositifs critiques et un ou des ordinateurs du réseau d'entreprise, ou même n'importe quel un ordinateur connecté au switch du réseau.

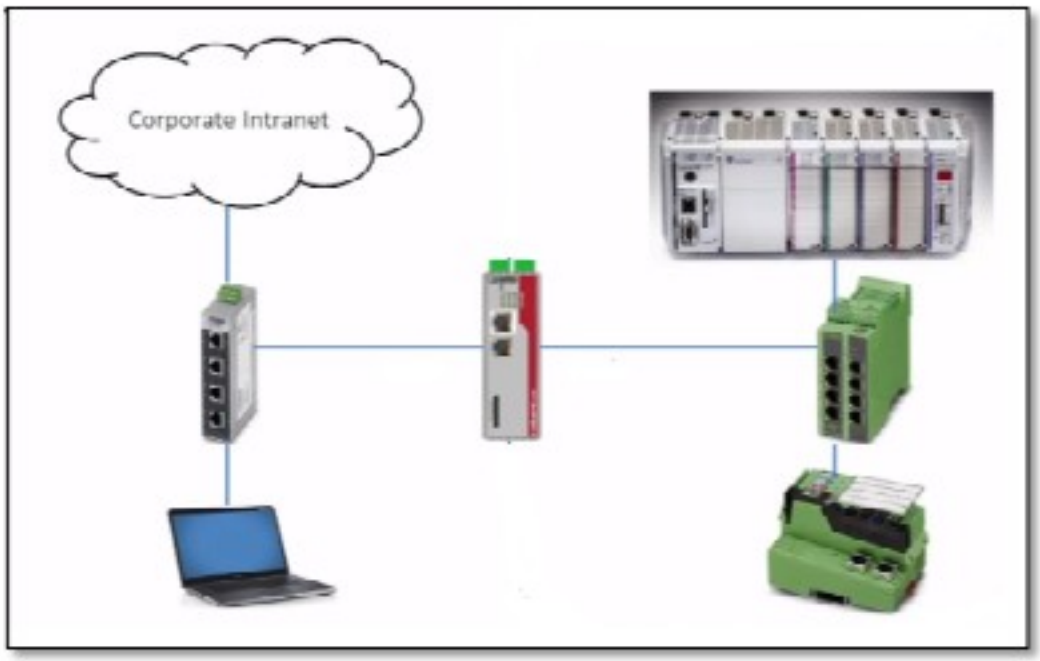


Figure V.28 : Principe de fonctionnement du pare-feu FL MGUARD

Il faut tout d'abord :

- Déterminer les points d'accès de nos éléments critiques ;
- Lister les adresses IP autorisées ou utilisateurs autorisés;
- Définir les règles de pare-feu adéquates en respectant les protocoles et adresses IP ;

V.5.2.1.2. Etapes de programmation

Afin de programmer correctement notre pare-feu FL MGUARD, il faut suivre les étapes suivantes :

1- Définir une adresse IP au pare-feu dans le réseau du système de contrôle

Il faut tout d'abord, accéder au panel de configuration du FL MGUARD avec son adresse IP par défaut, étant : « 1.1.1.1 » comme on peut le voir sur la **Figure V.29**

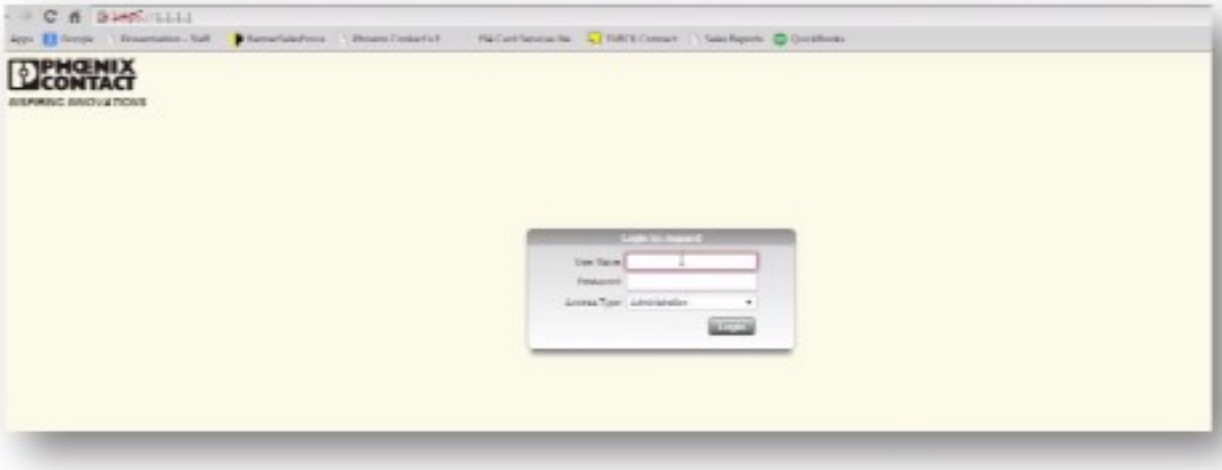


Figure V.29 : Accès au panel du FL MGUARD par le biais de son adresse IP par défaut.

Il faudra par la suite, entre l'identifiant et le mot de passe, panel visible sur la **Figure V.30**

Figure V.30 : Panel de configuration du FL MGUARD

Pour définir une adresse IP au FL MGUARD, il faut accéder sur la gauche à

Network > Interfaces, comment on peut le voir sur la **Figure V.31**

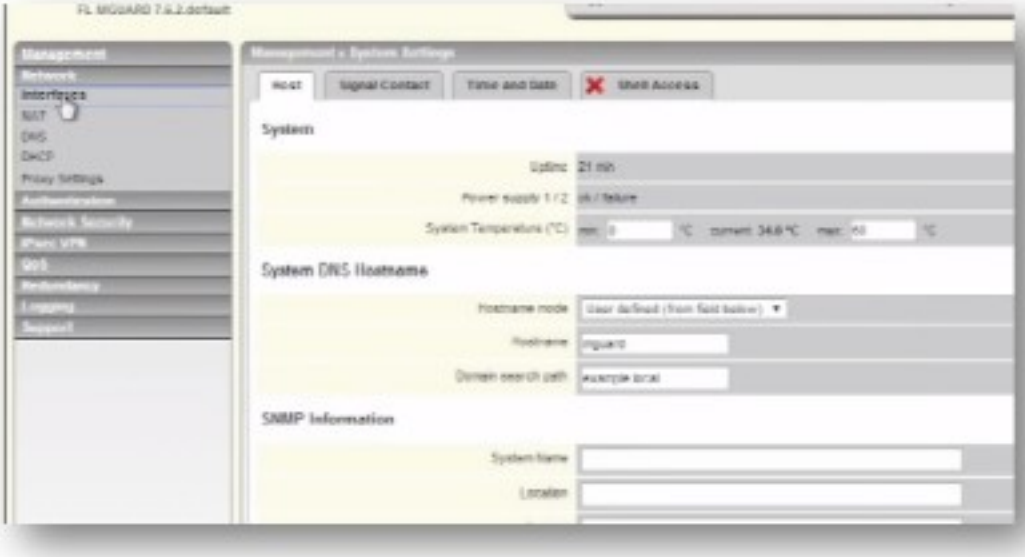


Figure V.31 : Accès aux options d'interfaces de réseau sur le panel du FL MGUARD

Puis nous définissons l'adresse IP et le masque réseau du pare-feu, voir **Figure V. 32**

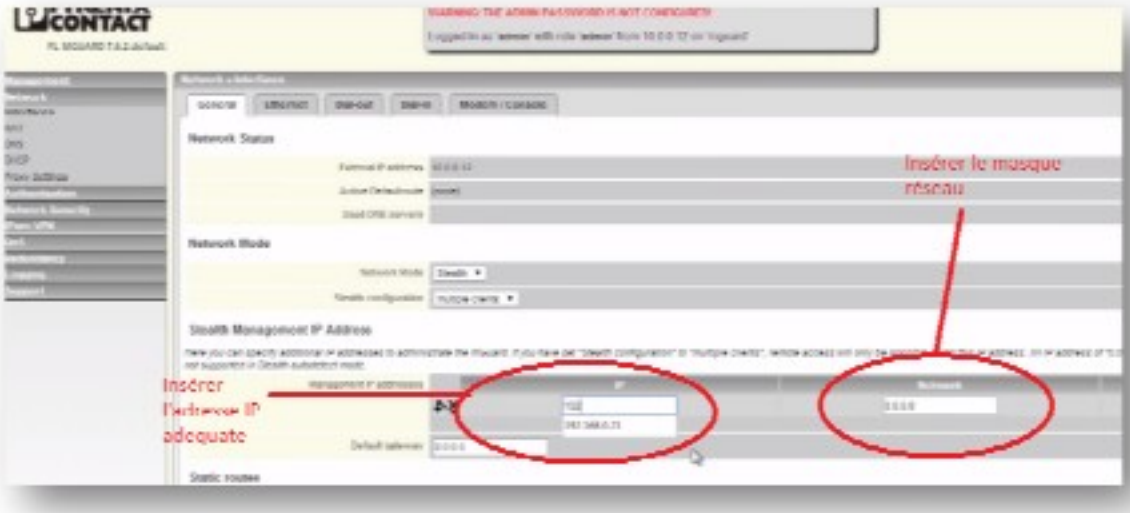


Figure V.32 : Définition d'adresse IP et masque réseau au FL MGUARD

Nous validons puis copions la nouvelle adresse IP du pare-feu, voir **Figure V. 33**

Figure V.33 : Copie de la nouvelle adresse IP du FL MGUARD

Après cela, nous branchons notre pare-feu dans la partie adéquate, le pare-feu est maintenant installé et bloquera toute connexion.

Afin de permettre les connexions voulues et adéquates, nous passons à l'étape suivante

2- **Création d'un utilisateur Pare-feu**

L'utilisateur va permettre l'accès aux dispositifs seulement avec les identifiants pare-feu.

Il faut tout d'abord aller à la section Network Security > User Firewall, comme on peut le voir sur la **Figure V.34**

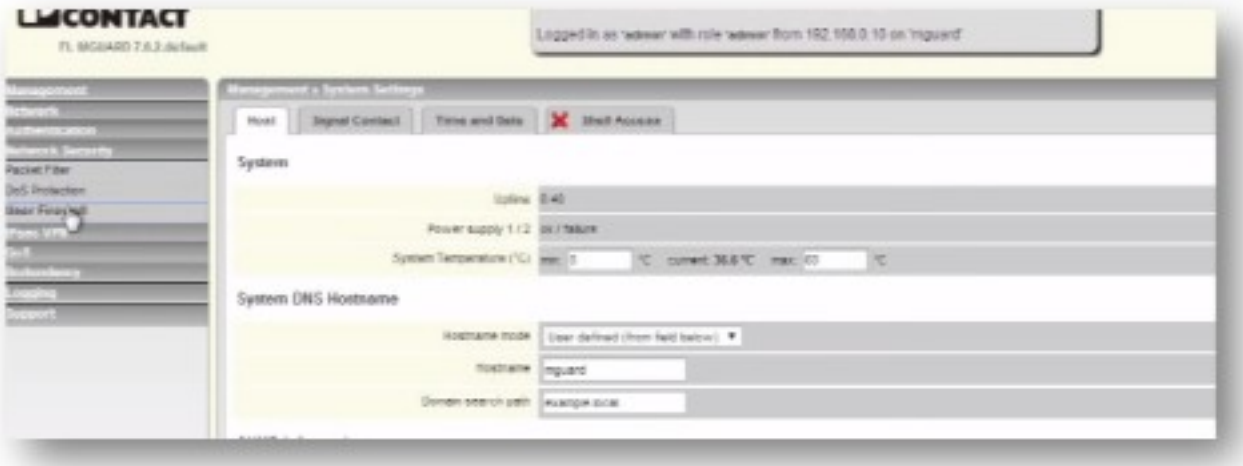


Figure V.34 : Accès aux options d'utilisateurs du pare-feu sur le panel du FL MGUARD

Nous l'allons par la suite créer un modèle d'utilisateur pare-feu que l'on nome « PLC ACCESS » Voir **Figure V. 35**

Figure V.35 : Création d'un modèle d'utilisateur pare-feu

Les **Figure V.36 et V. 37** qui suivent sont explicatives des conduites à suivre afin de créer un modèle d'utilisateur et configurer les règles de pare-feu selon nos besoins.

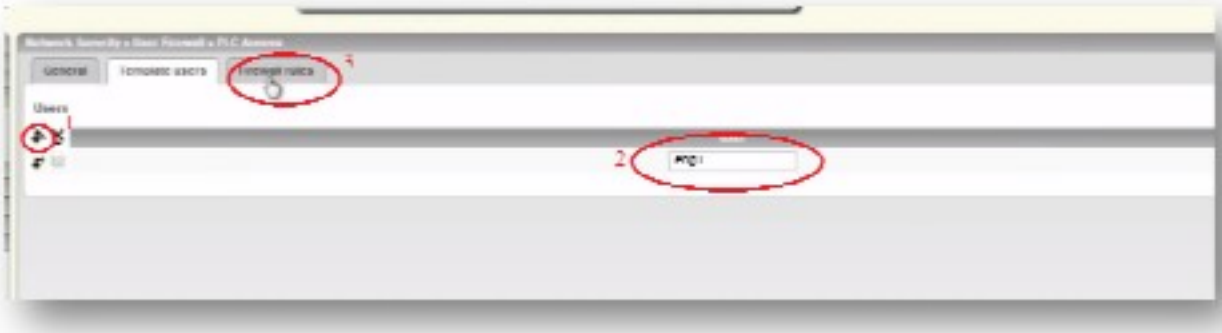


Figure V.36 : Création d'un modèle d'utilisateur

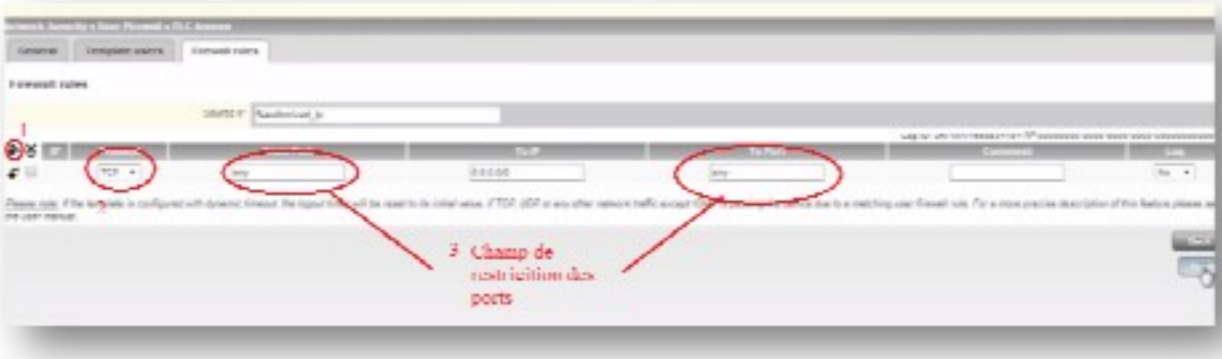


Figure V.37 : Définition des règles pare-feu adéquates

Il faudra par la suite créer notre utilisateur, les étapes sont clairement expliquées sur les **Figures V.38 et V.39**

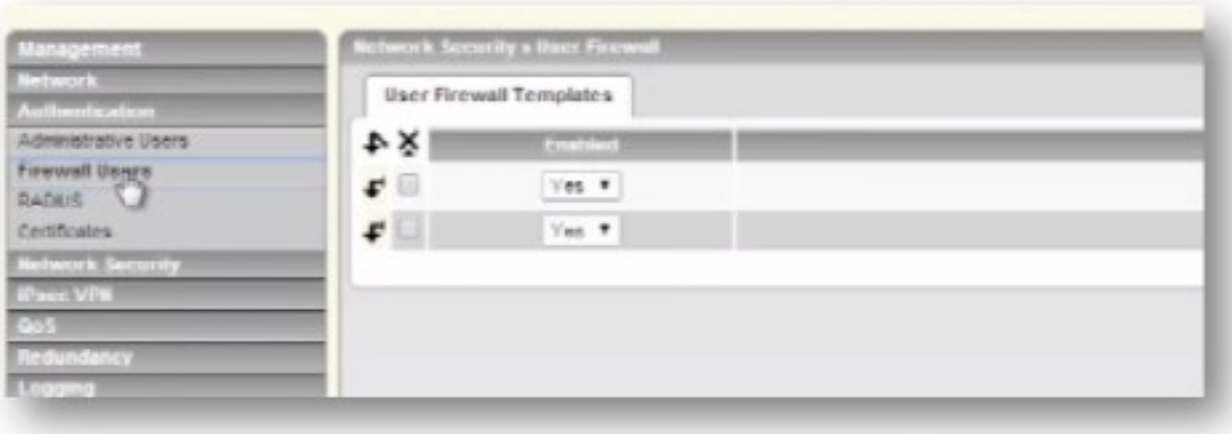


Figure V.38 : Accès aux options d'authentification d'utilisateur pare-feu

Figure V.39: Etape finale de la création d'un utilisateur pare-feu.

Il sera possible à ce moment d'avoir accès au dispositif protégé par le pare-feu qu'en se connectant d'abord au pare-feu par le biais de la machine utilisée.

V.6. Conclusion

Nous avons dans ce chapitre étudié l'architecture du système de contrôle de la cimenterie de MEFTAH, ses atouts et instrumentations, ses vulnérabilités et mis le relief sur les approches prises en compte dans l'implémentation de notre solution de cyber-sécurité.

Conclusion Générale

Conclusion générale

A la suite du stage effectué à la cimenterie SCMI de MEFTAH, expérience très enrichissante qui nous a permis de comprendre les lignes de fabrication de ciment, les aspects du rôle d'un Ingénieur automaticien et quelques bonnes pratiques d'industrie, en concluant de tout cela que:

- La compréhension et l'étude des systèmes de contrôle industriels et de leurs vulnérabilités nous a permis d'avoir une meilleure perception du fond de notre problème afin procéder au développement de sa solution.
- La sécurité des systèmes de contrôle est devenue aujourd'hui une priorité.
- Les systèmes automatisés sous Siemens SIMATIC PCS7 sont très plus fiables d'un point de vue sécuritaire et permettent une amélioration continue du système.
- La mise en évidence de notre projet se base sur le choix d'une architecture du système de contrôle améliorée, jouant sur les deux aspects fonctionnelle et technique.
- Tout en respectant la logique de fonctionnement de notre système, la création, développement et testes de notre solution nous a permis d'apprendre à choisir l'approche adéquate face à n'importe quel type de système de contrôle tout en respectant évidemment le processus et son fonctionnement.
- Grace à l'amélioration de la cyber-sécurité du système de contrôle, ce dernier est devenu mieux protégé et beaucoup plus isolé permettant de maintenir son fonctionnement et de le protéger de façon acceptable face aux grandes cyber-menaces.

Dans l'espoir de rester à jour avec les avancements technologiques et pouvoir améliorer ce travail et arriver à de meilleures résultats et solutions.

Références Bibliographiques

✓ **Documentation offerte par la cimenterie de MEFTAH**

[1] : F.HAMMOUCHE A.SABIL/ SCMI MEFTAH, 2011. « Codification, Formation et Maintenance ». Document interne à l'entreprise

[2]: P.Walk/ LAFARGE, 2000 « Coding Level 5 and 6 », 11/2000

EQUIPEMENT, SYSTEMS AND COMPONENTS

[3] : CENTRE TECHNIQUE INTER-UNITES, 2002. « Maintenance, codification et kit outil.A3.carte.n3 » 13/05/2002

Codification du périmètre CTI

[4] : F.GUILLAUME/ICEP, 2012. «MEF-861-N01_RevF », 06/05/2013

Architecture réseau automates

[5] : SCMI MEFTAH/2013. « MEF-861-N06» 05/2013

Manuel Opérateur

[6] : M.BENAZZOUZ/SCMI MEFTAH, 2012. « SOCIETE-DES-CIMENTS-DE-LA-MITIDJA » 25/10/2012

Présentation de la Cimenterie

✓ **Documentation offerte par SIEMENS**

[7] : SIEMENS AG, 2009 « Système de conduite de processus PCS7 - Getting Started – Part 1 (V7.1) » 03/2009

Numéro : A5E02122224-0

[8] : SIEMENS AG, 2012 « SIMATIC ET 200 pour solutions d'automatisation distribuée » 11/2012

✓ **Documentation Enligne**

[9]: Keith Stouffer, Joe Falco, Karen Scarfone/NIST, 2011 « Guide to Industrial Control Systems (ICS) Security » [pdf]. 06/2011. Disponible à l'adresse : http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[10]: Groupe CGI 2011 «La cyber-sécurité des infrastructures essentielles modernes » [pdf]. 06/2011. Disponible à l'adresse : https://www.cgi.com/sites/default/files/white-papers/la_cybersecurite_des_infrastructures.pdf

[11]: M.GERIN/Schneider Electric 2002, « Les bus et les réseaux de terrain en automatisation industriel » [pdf]. 11/2002. Disponible à l'adresse : https://www.schneider-electric.fr/documents/enseignement/intersection-guides/GT2002-les-bus-et-reseaux-industriels.pdf

[12] : RGB SPECTRUM, 2016. Utilities RGB Spectrum.01/2016. Disponible à l'adresse : http://www.rgb.com/markets/utilities

[13]: PTOA Segment, 2015. Process Tech & Operator academy – Many DCS benefits, processtechacademy.com. 25/04/2015. Disponible à l'adresse : http://www.processtechacademy.com/contrast-between-old-and-new-control-technologies/

[14] : PHOENIX CONTACT, 2016. PHOENIX CONTACT | Routeurs et pare-feu de sécurité, www.phoenixcontact.com. Disponible à l'adresse : https://www.phoenixcontact.com/online/portal/pi?1dmy&urile=wcm:path:/pifr/web/main/products/subcategory_pages/security_routers_and_firewalls_p-03-09/3bd0489c-fcd0-4c5f-84e6-8d02e094bbcb

✓ **Mémoires de fin d'études :**

[15] : N.KHALFI, S. AITCHALLAH/ FHC-UMBB, 2015. « Migration de la commande d'un pont gratteur de l'automate S5 à l'automate S7 400 sous PCS7 », 07/2015.