

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Oran 1, Ahmed Ben Bella
Institut des Sciences et Techniques Appliquées

Thème

Conception d'un mini-laboratoire de cyber sécurité pour systèmes
industriels ICS

Par

BOUHACENE Zahera

Projet présenté à l'Institut des sciences et techniques appliquées
En vue de l'obtention du diplôme de Master professionnelle IM

Soutenu le 18 Juin 2026 devant le jury composé de :

M ^{me} DAHOU Nour El houda	MCB	Présidente
Mr BENSIKADDOUR El Habib	MCA	Examineur
M ^r CHERIET Mohammed El Amine	MCB	Encadreur
M ^{me} BOUBEKEUR Djamila	MCA	Co-Encadreur

Juin 2026

Résumé

Ce projet présente la conception et la validation d'un laboratoire de cybersécurité industrielle simulant une chaîne complète d'automatisation attaquée puis défendue.

Sur le plan opérationnel, un convoyeur automatisé est simulé sous Factory I/O et piloté par l'automate logiciel OpenPLC via le protocole Modbus TCP/IP. Le système détecte la présence d'un objet par capteur optique et commande l'arrêt du moteur en temps réel.

Sur le plan offensif, une attaque FDIA par inondation de requêtes Modbus FC5 est simulée à l'aide d'un script Python (pyModbusTCP). Elle sature le registre moteur et neutralise la logique d'arrêt locale, provoquant un incident physique réel.

Sur le plan défensif, deux mécanismes basés sur une analyse comportementale par fenêtre glissante sont déployés : un IDS qui détecte l'anomalie et alerte l'opérateur, et un IPS qui bloque activement les paquets hostiles avant qu'ils n'atteignent l'automate. Les résultats confirment l'efficacité de l'approche proxy Modbus comme couche de protection adaptée aux environnements OT

Abstract

This project presents the design and validation of an industrial cybersecurity laboratory simulating a complete automation chain under attack and subsequent defense.

On the operational level, an automated conveyor is simulated using Factory I/O and controlled by the OpenPLC softPLC via the Modbus TCP/IP protocol. The system detects the presence of an object using an optical sensor and commands the motor to stop in real time.

On the offensive level, a False Data Injection Attack (FDIA) via Modbus FC5 request flooding is simulated using a Python script (pyModbusTCP). It saturates the motor register and overrides the local stop logic, causing a real physical incident.

On the defensive level, two mechanisms based on rolling-window behavioral analysis are deployed: an IDS that detects the anomaly and alerts the operator, and an IPS that actively blocks hostile packets before they reach the PLC. The results confirm the effectiveness of the Modbus proxy approach as a tailored protection layer for OT environments.

ملخص المشروع

يقدم هذا المشروع تصميم واختبار مختبر للأمن السيبراني الصناعي يحاكي سلسلة أتمتة كاملة تعرضت لهجوم ثم جرى حيث يتم التحكم فيه ، Factory I/O الدفاع عنها. فمن الناحية التشغيلية، تمت محاكاة سير ناقل مؤتمت باستخدام برنامج ليقوم النظام بالكشف ، Modbus TCP/IP عبر بروتوكول OpenPLC بواسطة جهاز التحكم المنطقي المبرمج البرمجي عن القطع بواسطة مستشعر بصري ويصدر أمرًا بإيقاف المحرك في الوقت الفعلي. أما على المستوى الهجومي، فقد تم باستخدام سكرت بايثون Modbus FC5 عن طريق إغراق النظام بطلبات (FDIA) تنفيذ هجوم حقن البيانات الزائفة مما أدى إلى غمر سجل المحرك وتعطيل منطق الإيقاف المحلي متسببًا في وقوع حادث مادي ، (pyModbusTCP) حقيقي. وفي المقابل، تم نشر آليتين دفاعيتين تعتمدان على التحليل السلوكي عبر النافذة المنزلة؛ الأولى تمثلت في نظام لحظر الحزم المعادية بنشاط قبل (IPS) لرصد الشذوذ وتنبيه المشغل، والثانية في نظام منع التسلل (IDS) كشف التسلل كطبقة حماية متينة (Modbus Proxy) وصولها إلى جهاز التحكم. وتؤكد النتائج المستخلصة فعالية نهج وكيل مودبس (OT) ومناسبة لبيئات التكنولوجيا التشغيلية.

Remerciements

Nous remercions tout d'abord, Allah qui nous a donné la force Et le courage pour Terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos remerciements à notre encadreur : **Dr. CHERIET Mohammed El Amine** ET **Dr. BOUBEKEUR Djamila** pour la grande liberté de travail qu'il nous a accordée durant ce projet, ainsi que leurs conseils et encouragements.

Nos remerciements vont également aux membres du jury qui ont accepté de juger ce travail ainsi qu'à tous nos enseignants et enseignantes.

Table des matières

Abstract	iii
Table des matières	vi
Liste des figures	xi
Introduction générale	1
Chapitre 1 Systèmes de Contrôle Industriel (ICS)	3
1.1 Introduction	4
1.2 Définition des Systèmes de Contrôle Industriel (ICS)	4
1.3 Programmable logic contrôler PLC	5
1.3.1 Définition	5
1.3.2 Rôle de PLC dans un ICS [20]	6
1.3.3 Architecture	8
1.3.4 Avantage et inconvénients	10
1.4 Système de contrôle distribué DCS	12
1.4.1 Définition	12
Figure 5 : Système de contrôle distribué DCS	12
1.4.2 Principale caractéristique DCS	13
1.4.3 Architecture DCS	13
1.4.4 Avantage DCS	14
1.5 Système SCADA	15
1.5.1 Définition du SCADA	15
1.5.2 Éléments d'un système SCADA	16
1.5.3 Architecture des systèmes SCADA	18
1.5.4 Avantages du système SCADA	19

1.6 Les systèmes instrumentés de sécurité (SIS)	19
1.6.1 Définition SIS	19
1.6.2 Constitution d'un système instrumenté de sécurité	20
1.6.3 L'indépendance de SIS	21
1.7 l'IIoT (Industrial Internet of Things)	21
1.7.1 Définition de l'IIoT (Industrial Internet of Things)	21
1.8 La convergence IT/OT	22
1.9 Conclusion	23
Chapitre 2 La cyber sécurité	24
2.1 Introduction	25
2.2 La cybersécurité	25
2.3 La cyber sécurité industrielle	26
2.4 Objectifs de la cybersécurité	26
2.5 Définition du modèle Purdue	28
2.5.1 Les niveaux du modèle Purdue	28
2.6 Définition l'OT (Operational Technology)	29
2.7 Définition de l'IT (Technologies de l'Information)	30
2.8 Différence entre l'IT et l'OT	30
2.8.1 Objet (fonction principale)	30
2.8.2 Environnement	31
2.8.3 Sécurité	31
2.8.4 Mises à jour et maintenance	31
2.9 Définition des cyberattaques	31
2.10 Exemples concrets	32
2.11 Principaux types de cyberattaques	32
2.12 La défense en profondeur	33
2.13 Les différents éléments d'un système de défense en profondeur	35
2.14 Conclusion	35
Chapitre 3 Développement d'un laboratoire pour la cybersécurité	37

3.1 Introduction	38
3.2 Architecture du Système Développé	38
3.3 Les Bloc de Simulation (Environnement Virtuel)	39
3.4 Les Bloc de Sécurité	39
ce bloc centralise la surveillance et la protection du réseau :	39
3.5. Etape de réalisation	40
3.5.1 Usine virtuelle	40
3.5.2. Analyse Détaillée des l'Attaque	43
3.5.2.2.Impact de l'Attaque par Sabotage d'Interface	45
3.3.3.1.Techniques de Détection de l'IDS	47
➤ Détection par Signatures (Misuse Detection)	47
➤ Détection d'Anomalies (Anomaly Detection)	47
➤ Inspection Profonde des Paquets & Analyse d'État (DPI / Process-Aware)	47
3.3.3.3.Techniques de IPS:	50
➤ Le Filtrage Actif en Ligne (<i>Inline Packet Dropping</i>)	50
➤ La Réinitialisation de Connexion (<i>TCP Reset / Connection Termination</i>)	50
➤ La Reconfiguration Dynamique du Pare-feu (<i>Firewall Rate-Limiting & Shunning</i>)	51
➤ La Normalisation de Protocole (<i>Traffic Scrubbing / Protocol Sanity</i>)	51
3.3.3.5. Implémentation sur wireshark	53
3.4. validation pratique	54
3.5 Conclusion	57
Conclusion générale	59
1. Annexe A : Script Python de simulation offensive (Attaque FDIA)	61
2. Annexe B : Script Python de détection passive (Système IDS)	61
3. Annexe C : Script Python de prévention active (Système IPS)	62
Bibliographie	64

Liste des abréviations

ICS	Industrial Control Systems (Systèmes de Contrôle Industriel)
PLC / API	Programmable Logic Controller / Automate Programmable Industriel
DCS	Distributed Control System (Système de Contrôle Distribué)
SCADA	Supervisory Control And Data Acquisition (Supervision, Contrôle et Acquisition de Données)
SIS	Safety Instrumented System (Système Instrumenté de Sécurité)
SIF	Safety Instrumented Function (Fonction Instrumentée de Sécurité)
OT	Operational Technology (Technologies Opérationnelles)
IT	Information Technology (Technologies de l'Information)
IIoT	Industrial Internet of Things (Internet des Objets Industriels)
RTU	Remote Terminal Unit (Unité Terminale Distante)
MTU	Master Terminal Unit (Unité Terminale Maître)
HMI / IHM	Human Machine Interface / Interface Homme-Machine
BPCS	Basic Process Control System (Système de Contrôle de Procédé de Base)
CPU	Central Processing Unit (Unité Centrale de Traitement)
PID	Proportional Integral Derivative (Correcteur Proportionnel Intégral Dérivé)
DMZ	Demilitarized Zone (Zone Démilitarisée)
MES	Manufacturing Execution System (Système d'Exécution de Production)
ERP	Enterprise Resource Planning (Progiciel de Gestion Intégré)
CNC	Computer Numerical Control (Commande Numérique par Ordinateur)
LAN	Local Area Network (Réseau Local)
WAN	Wide Area Network (Réseau Étendu)
IP	Internet Protocol (Protocole Internet)
TCP/IP	Transmission Control Protocol / Internet Protocol
Modbus	Protocole de communication industriel Modbus
PROFIBUS	Process Field Bus
CIA	Confidentiality, Integrity, Availability (Confidentialité, Intégrité, Disponibilité)

DoS / DDoS Denial of Service / Distributed Denial of Service

Liste des figures

Figure 1 : BUT ICS[17]	5
Figure 2 : Programmable logic contrôler PLC	6
Figure 3 : Rôle PLC dans un ICS[19]	8
Figure 4 : Architecture PLC[21]	10
Figure 5 : Système de contrôle distribué DCS	12
Figure 6 : Architecture DCS	14
Figure 7 : Schéma général d'un RTU	17
Figure 8 : Schéma général d'un MTU.....	18
Figure 9 : Structure d'un SIS	21
Figure 10 : La convergence OT IT	22
Figure 11 : La triade C.I.A	27
Figure 12 : Le modèle Perdue	29
Figure 16 : Logiciel factoryIO	33
Figure 20 : La communication entre OpenPLC et Factory I/O est stabl.....	34
Figure 20 : La communication entre OpenPLC et Factory I/O est stable.....	38
Figure 21 : Le moteur s'arrête immédiatement lors de la détection.....	43
Figure 22 : organigramme de attaque DOS (<i>première mention</i>).....	43
Figure 22 : organigramme de attaque injection (<i>deuxième mention dans le texte sous le même numéro</i>).....	44

Figure 23 : interface sabotage.....	46
Figure 24 : colis tombe.....	46
Figure 25 : IDS en mode fonctionnement normale.....	49
Figure 26 : IDS dans le cas de sabotage.....	50
Figure 27 : IPS en mode fonctionnement normale.....	52
Figure 28 : IPS dans le cas de sabotage.....	53
Figure 29 : Résultat sur wireshark.....	54
Figure 30 : architecture de system.....	55
Figure 31 : Connexion établie avec succès.....	56
Figure 32 : l'Interface de Sabotage (Modbus TCP DoS Attacker).....	57

Introduction générale

La transformation numérique des environnements industriels a profondément modifié la nature des systèmes de production. L'intégration croissante entre les réseaux informatiques (IT) et les réseaux opérationnels (OT) a permis des gains considérables en termes de performance, de supervision et de réactivité. Cependant, cette convergence expose les systèmes de contrôle industriel (ICS) à des cyber menaces autrefois réservées au monde de l'informatique classique.

Les protocoles industriels tels que Modbus TCP/IP, conçus à une époque où la sécurité n'était pas une priorité, ne disposent d'aucun mécanisme natif d'authentification ou de chiffrement. Ils constituent ainsi des vecteurs d'attaque exploitables par tout acteur malveillant ayant accès au réseau. Les conséquences d'une intrusion dans un environnement industriel ne se limitent pas à une fuite de données : elles peuvent se traduire par des incidents physiques, des arrêts de production, des dommages matériels ou des risques pour la sécurité des personnes.

C'est dans ce contexte que s'inscrit ce projet, dont l'objectif est de concevoir, implémenter et évaluer un laboratoire de cybersécurité industrielle en environnement simulé. Il vise à démontrer, de manière concrète et reproductible, à la fois la vulnérabilité des réseaux OT face à une attaque par injection de fausses données (FDIA), et l'efficacité d'une défense comportementale par proxy Modbus intégrant un IDS et un IPS.

Ce mémoire est divisé en trois chapitres ; le premier présente les fondamentaux des systèmes de contrôle industriel : PLC, DCS, SCADA, SIS et IIoT. Le second aborde les concepts essentiels de la cybersécurité, notamment la triade CIA, le modèle Purdue et la défense en profondeur et finalement le troisième décrit en détail le développement du laboratoire : conception du convoyeur automatisé, simulation de l'attaque FDIA, et mise en œuvre des mécanismes de détection et de prévention d'intrusion.

Chapitre 1

Systèmes de Contrôle Industriel (ICS)

1.1 Introduction

Les systèmes industriels modernes reposent de plus en plus sur des infrastructures automatisées permettant d'assurer la continuité, la sécurité et l'efficacité des processus de production. Ces systèmes, appelés Systèmes de Contrôle Industriel (ICS), jouent un rôle central dans la gestion et la supervision des installations critiques.

Avec l'évolution des technologies et la convergence entre les réseaux informatiques (IT) et les réseaux industriels (OT), les ICS sont devenus des cibles potentielles pour diverses menaces cybernétiques. Il devient donc essentiel de comprendre leur architecture, leurs composants ainsi que leur fonctionnement afin d'identifier les risques et de mettre en place des mécanismes de protection adaptés.

Ce chapitre présente les fondamentaux des ICS, en détaillant leurs composants, leurs architectures ainsi que leur structure globale.

1.2 Définition des Systèmes de Contrôle Industriel (ICS)

Les Systèmes de Contrôle Industriel (Industrial Control Systems – ICS) regroupent l'ensemble des matériels, logiciels, réseaux et procédures utilisés pour surveiller, piloter et automatiser des processus industriels. Ils sont déployés dans des secteurs critiques tels que l'énergie, l'eau, le transport, l'industrie manufacturière, la chimie ou encore le pétrole et le gaz.

Un ICS assure la collecte des données issues du terrain (capteurs), le traitement et la prise de décision via des algorithmes de contrôle, l'action sur le procédé à l'aide d'actionneurs, la supervision et l'intervention humaine grâce aux interfaces opérateurs. Les principales architectures d'ICS incluent les systèmes SCADA, DCS et PLC, chacun répondant à des besoins spécifiques en matière de contrôle, de distribution et de supervision et de

optimisation comme l'illustre la Figure 1. [1]

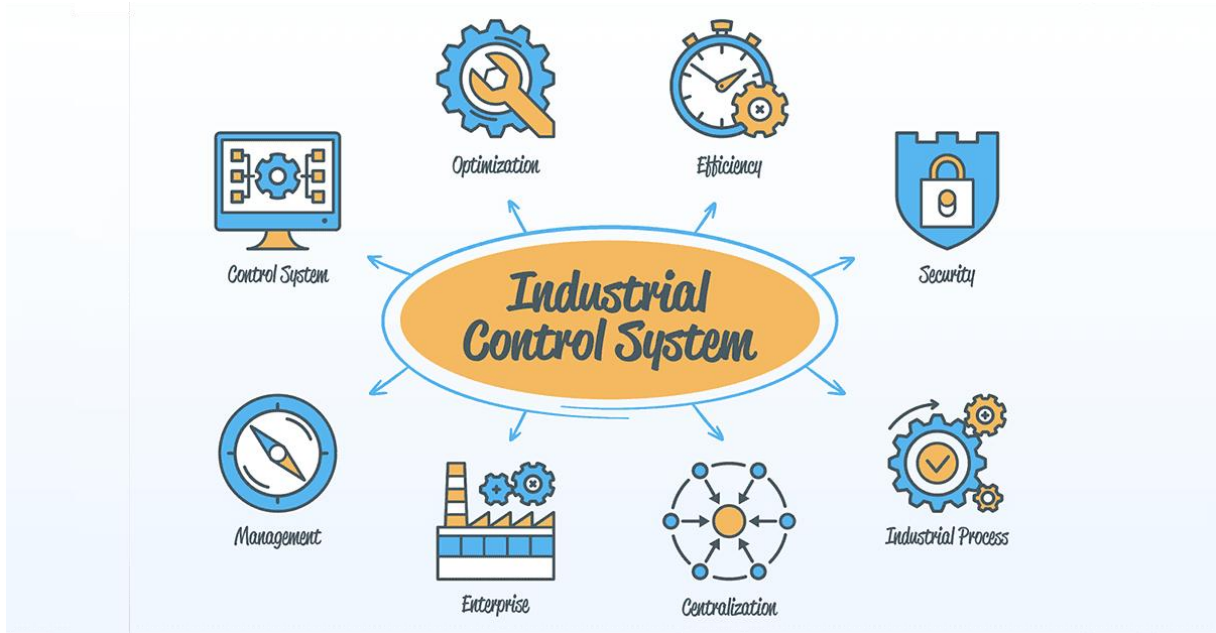


Figure 1 : BUT ICS[17]

1.3 Programmable logic contrôler PLC

1.3.1 Définition

L'automate programmable industriel (API), également appelé PLC (Programmable Logic Controller) ou contrôleur logique, est un dispositif informatique spécialisé utilisé dans les systèmes de contrôle industriels. Grâce à sa conception robuste, il est capable de fonctionner dans des environnements industriels sévères caractérisés par des températures extrêmes, des vibrations importantes, l'humidité ou encore les perturbations électriques. En plus de sa solidité, il offre des fonctionnalités essentielles telles que la gestion de séquences, les temporisations, les comptages et le contrôle automatisé des processus.

Facile à programmer et à exploiter, l'automate programmable assure un fonctionnement fiable des installations industrielles. Il est donc considéré comme un ordinateur dédié, spécialement conçu pour le pilotage des machines et des procédés industriels.

Bien que certaines industries utilisent le terme « PC » pour désigner ces dispositifs, cela peut prêter à confusion avec les ordinateurs personnels. C'est pourquoi la majorité des fabricants, comme Mitsubishi Electric, privilégient les appellations PLC ou API.

Enfin, l'utilisation des automates programmables ne se limite pas au domaine industriel. On les retrouve également dans des applications du quotidien telles que les machines à laver, les ascenseurs ou encore les systèmes de gestion des feux de circulation. En résumé, un API est un ordinateur basé sur un microprocesseur, dépourvu d'interfaces classiques comme le clavier, la souris ou l'écran, et conçu pour fonctionner efficacement dans des conditions difficiles comme illustre la figure 2. [1]



Figure 2 : Programmable logic contrôler PLC

1.3.2 Rôle de PLC dans un ICS [20]

- Contrôle séquentiel et logique conditionnelle

Les automates programmables industriels assurent la gestion des enchaînements d'opérations (comme les convoyeurs ou les bras robotisés) tout en prenant des décisions en fonction de conditions précises. Par exemple, ils peuvent déclencher un moteur lorsque qu'un capteur est activé comme illustre la figure 3.

- **Flexibilité et facilité de reprogrammation**

Contrairement aux systèmes câblés à relais, les PLC offrent une grande souplesse. Il est possible de modifier ou d'adapter le processus industriel simplement en changeant le programme, sans intervention matérielle complexe.

- **Supervision en temps réel**

Ils permettent de surveiller en continu différents paramètres tels que la température, la vitesse ou l'état des équipements, et peuvent générer des alertes en cas d'anomalie ou de panne.

- **Capacité de communication**

Les PLC s'intègrent facilement dans les réseaux industriels. Ils peuvent communiquer avec des interfaces homme-machine (IHM/HMI) et des systèmes de supervision comme le SCADA, facilitant ainsi le contrôle et la gestion à distance.

- **Robustesse et fiabilité**

Conçus pour les environnements industriels exigeants, ils résistent aux conditions difficiles telles que les vibrations, les températures élevées et les perturbations électromagnétiques.

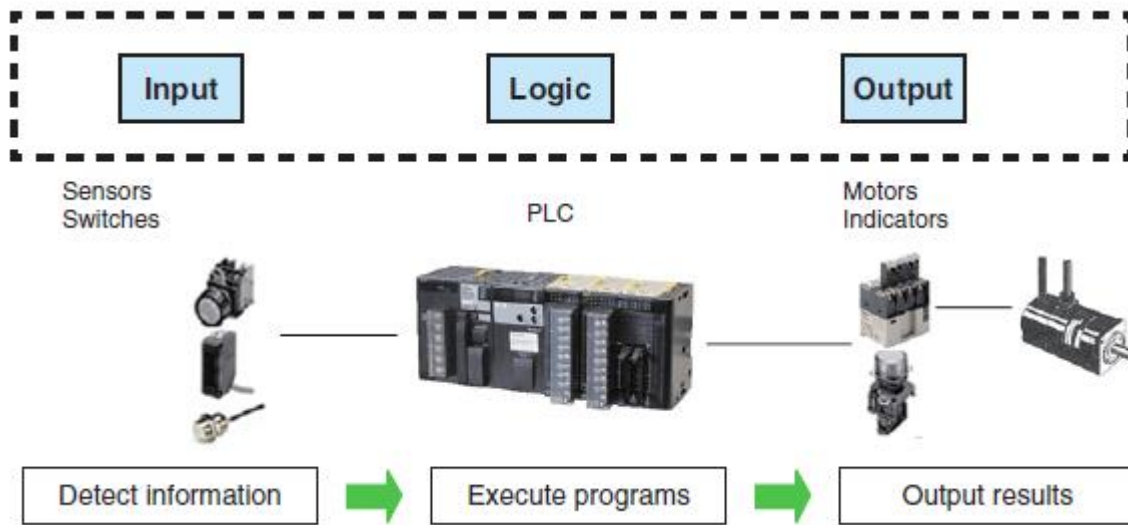


Figure 3 : Rôle PLC dans un ICS[19]

1.3.3 Architecture

L'architecture d'un PLC repose sur un ensemble de modules matériels et logiciels permettant d'assurer le contrôle et l'automatisation des processus industriels. Elle est généralement modulaire afin de faciliter l'installation, la maintenance et l'évolution du système comme illustre la figure 4.

1.3.3.1 Unité Centrale (CPU)

La CPU constitue le cœur de l'automate. Elle exécute le programme utilisateur, traite les données provenant des entrées et prend les décisions en fonction de la logique programmée. Elle assure également la gestion globale du fonctionnement du PLC.

1.3.3.2 Modules d'Entrées

Ces modules permettent de recevoir les signaux provenant des capteurs (boutons, détecteurs, capteurs de température, etc.). Ils convertissent ces signaux physiques en données exploitables par la CPU.

1.3.3.3 Modules de Sorties

Ils envoient des signaux de commande vers les actionneurs (moteurs, relais, voyants, vérins...). Ces signaux sont générés par la CPU selon le programme exécuté.

1.3.3.4 Mémoire

Le PLC dispose de différentes zones mémoire :

- Mémoire programme : stocke le programme utilisateur
- Mémoire données : contient les variables et états du système
- Mémoire système : utilisée pour le fonctionnement interne

1.3.3.5 Alimentation

Le module d'alimentation fournit l'énergie nécessaire au fonctionnement de tous les composants du PLC, en assurant une tension stable et adaptée.

1.3.3.6 Interfaces de Communication

Ces interfaces permettent au PLC de communiquer avec d'autres équipements industriels (IHM, systèmes SCADA, autres automates) via des protocoles comme Modbus, Ethernet ou Profibus. [1]

PLC Architecture

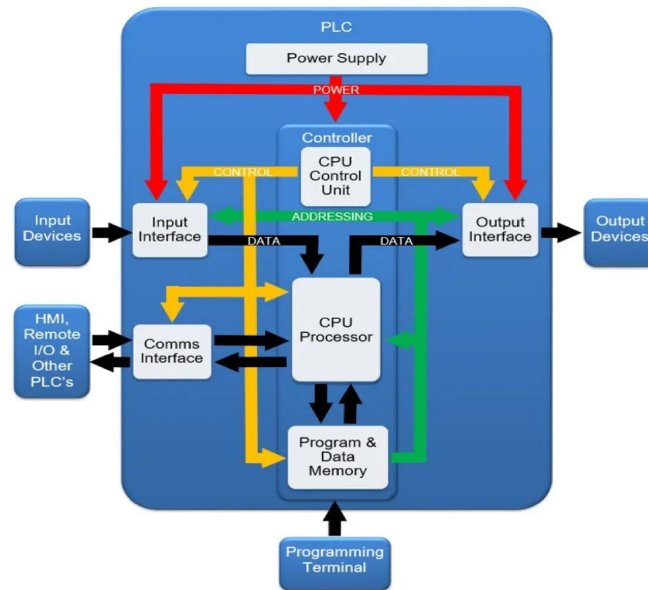


Figure 4 : Architecture PLC[21]

1.3.4 Avantage et inconvénients

1.3.4.1 Avantages des PLC

- **Grande robustesse**

Les automates programmables sont conçus pour fonctionner dans des environnements industriels difficiles, tels que la présence de poussière, les interférences électromagnétiques, les vibrations ou encore les variations de température.

- **Performances en temps réel**

Ils intègrent des circuits électroniques optimisés pour l'interface avec les entrées et sorties physiques, garantissant un temps d'exécution rapide et un fonctionnement efficace en temps réel.

- **Maintenance simplifiée**

Leur conception modulaire permet de remplacer rapidement les composants, ce qui facilite les opérations de maintenance et réduit les temps d'arrêt.

1.3.4.2 Inconvénients des PLC

- **Coût élevé**

Les PLC sont généralement plus coûteux que les solutions informatiques classiques, notamment celles basées sur des microcontrôleurs.

- **Coût variable selon les caractéristiques**

Le prix dépend de plusieurs facteurs, tels que le nombre d'entrées/sorties, la capacité mémoire disponible pour la programmation, ainsi que la présence de modules spécifiques à certaines industries.

- **Nécessité de formation**

L'utilisation des PLC requiert des compétences spécifiques en programmation. Toutefois, les langages utilisés sont souvent considérés comme plus intuitifs et visuels que les langages de programmation traditionnels.

- **Diversité des systèmes**

La multiplicité des marques et des modèles entraîne une diversité de langages et de méthodes de gestion des variables, malgré l'existence de la norme IEC 1131. [1]

1.4 Système de contrôle distribué DCS

1.4.1 Définition

DCS (Distributed Control System) est un système d'automatisation industrielle conçu pour surveiller et contrôler des processus complexes et continus à travers une infrastructure distribuée de contrôleurs et de postes opérateurs reliés par un réseau de communication industriel comme illustre la figure 5 . Contrairement aux systèmes centralisés, où un seul contrôleur gère l'ensemble du processus, le DCS répartit les fonctions de commande sur plusieurs unités locales, appelées stations de contrôle ou contrôleurs de terrain, permettant une meilleure fiabilité, flexibilité et tolérance aux pannes.[9]

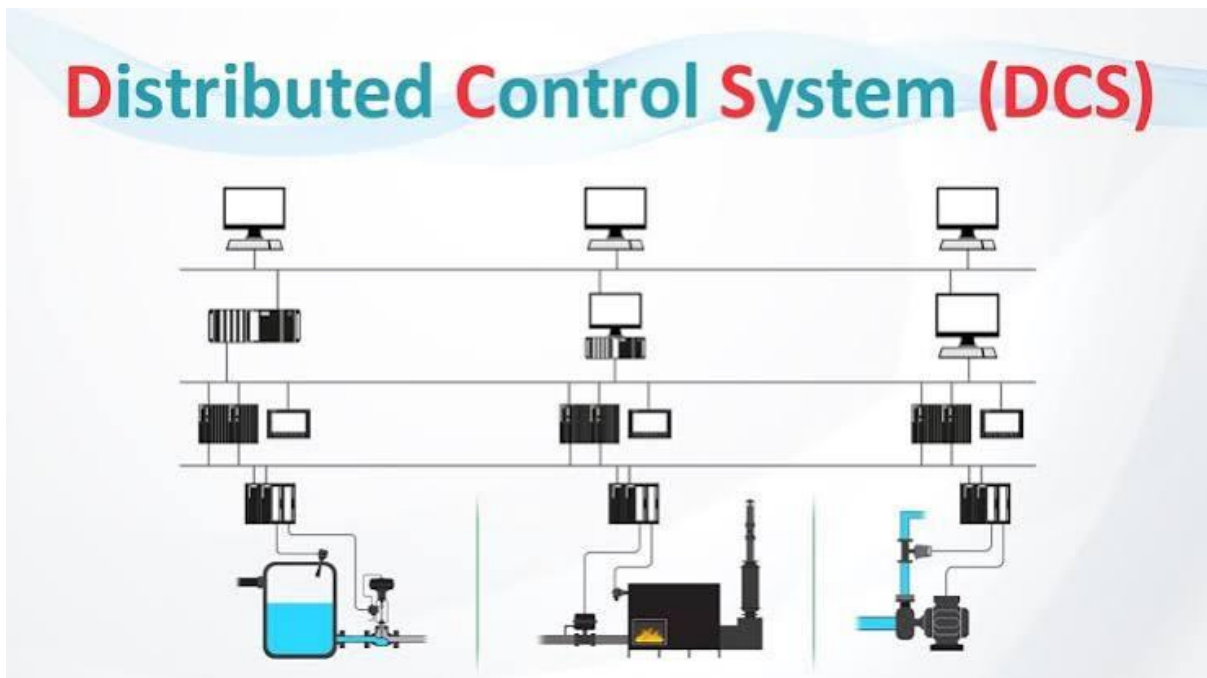


Figure 5 : Système de contrôle distribué DCS

1.4.2 Principale caractéristique DCS

La caractéristique essentielle d'un système DCS (*Distributed Control System* ou système de contrôle distribué) réside dans la distribution des fonctions de contrôle à travers différents contrôleurs implantés au sein du procédé industriel. Cette organisation permet d'assurer une grande fiabilité ainsi qu'un pilotage précis des procédés complexes. Contrairement aux systèmes centralisés, une panne localisée n'affecte pas l'ensemble de l'installation. [9]

Les principales caractéristiques d'un DCS sont les suivantes :

- **Architecture distribuée** : Les contrôleurs sont répartis sur différentes zones du procédé et assurent localement le traitement des entrées/sorties, ce qui améliore la rapidité de réponse du système.
- **Intégration globale** : Le DCS regroupe dans une même plateforme le contrôle des procédés, les interfaces homme-machine (IHM), la gestion des alarmes ainsi que l'enregistrement des données.
- **Fiabilité et redondance** : Conçu pour des applications critiques en fonctionnement continu, il intègre des mécanismes de redondance (matérielle et réseau) afin de garantir la continuité de service.
- **Gestion de procédés complexes** : Il est particulièrement adapté aux grandes installations industrielles (comme la pétrochimie ou la production d'énergie) nécessitant le contrôle de multiples boucles PID interconnectées. [9]

1.4.3 Architecture DCS

L'architecture d'un système de contrôle distribué (DCS) repose sur la répartition intelligente des fonctions de contrôle entre plusieurs contrôleurs interconnectés via des réseaux industriels. Contrairement à une architecture centralisée, cette organisation permet de réduire les points de défaillance uniques, d'améliorer la disponibilité du système et d'optimiser les performances globales du procédé industriel.

L'architecture de base d'un système DCS s'organise généralement en quatre niveaux distincts comme illustre la figure 6:

- **Niveau 1** : il correspond au terrain et regroupe l'ensemble des instruments de mesure et d'action installés sur le procédé, similaires à ceux utilisés dans les systèmes traditionnels.
- **Niveau 2** : il concerne les équipements d'automatisation situés dans le local technique, notamment les modules d'entrées/sorties qui assurent l'interface avec le terrain.
- **Niveau 3** : ce niveau est dédié à la conduite du procédé. Il inclut les stations opérateurs permettant de surveiller et de piloter le système.
- **Niveau 4** : il représente la couche supérieure, dédiée à la supervision globale et à la gestion de l'ensemble de l'installation industrielle.[9]

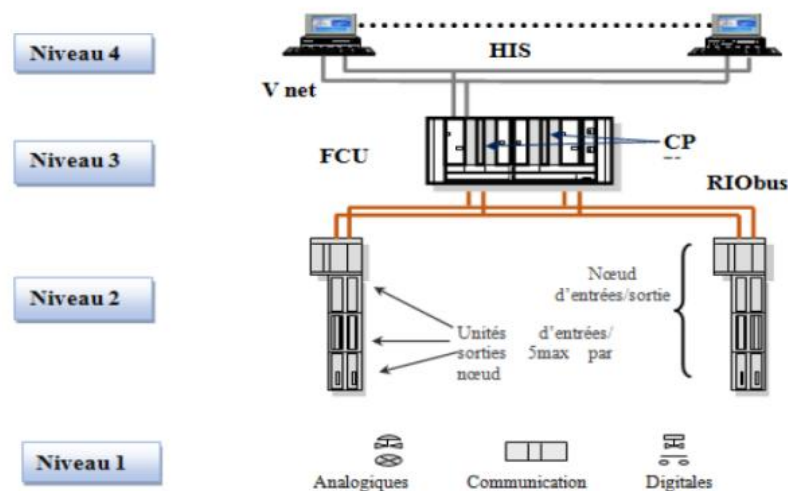


Figure 6 : Architecture DCS

1.4.4 Avantage DCS

Le système DCS offre de nombreux avantages par rapport aux anciens systèmes de contrôle, ce qui explique son adoption croissante dans l'industrie. Parmi ces avantages, on peut citer :

- **La distribution des fonctions** : les fonctions essentielles de pilotage du procédé sont réparties sur plusieurs stations. Cela garantit la continuité du fonctionnement même en cas de défaillance d'un élément.
- **La redondance** : la duplication des stations et des réseaux permet d'améliorer la fiabilité globale du système et de limiter les arrêts ou déclenchements non souhaités.
- **L'ouverture du système** : le DCS est conçu pour être compatible avec d'autres systèmes indépendants, tels que les systèmes SCADA ou ESD, facilitant ainsi l'intégration et la communication.
- **Les capacités d'analyse et d'optimisation** : grâce à des outils mathématiques avancés et à la commande évoluée, le DCS permet d'analyser et d'optimiser les procédés pour améliorer leurs performances.
- **La simplicité d'utilisation** : l'interface homme-machine repose sur des outils standards comme les ordinateurs et les imprimantes. Les opérateurs peuvent superviser et piloter les procédés via des interfaces graphiques conviviales, tandis que les ingénieurs peuvent assurer facilement la maintenance et le développement à l'aide de logiciels dédiés. [9]

1.5 Système SCADA

1.5.1 Définition du SCADA

Le SCADA, acronyme de *Supervisory Control and Data Acquisition* (Supervision, Contrôle et Acquisition de Données), est un système permettant de centraliser et de visualiser les informations issues d'une installation industrielle.

Il assure la collecte des données provenant de différents équipements (capteurs, automates, etc.), puis les transmet à un poste central, local ou distant, chargé de superviser et de contrôler le fonctionnement global du système. Les informations sont généralement présentées sous forme graphique sur des interfaces opérateurs, facilitant ainsi la surveillance et la prise de décision. [10]

1.5.2 Éléments d'un système SCADA

Un système SCADA est généralement composé des éléments principaux suivants :

1. **Site central (station de supervision)** : il constitue le centre de contrôle du système. Il offre à l'utilisateur une interface permettant de visualiser les données et de piloter les installations distantes.
2. **RTU (Remote Terminal Unit) / PLC** : ces équipements assurent la collecte des données provenant des capteurs sur le terrain et leur transmission vers l'unité centrale via le réseau de communication.

Le RTU (ou automate programmable) est une unité basée sur un microprocesseur dédié à l'acquisition de données et au contrôle local. Il supervise les équipements d'un site distant, collecte les informations issues des capteurs et les transmet au centre de contrôle.

Il peut également recevoir des instructions du système central et exécuter les actions correspondantes. Les RTU disposent généralement comme illustre la figure 7:

- D'entrées pour les capteurs,
- De sorties pour le contrôle et les alarmes,
- D'un port de communication pour l'échange de données. [10]

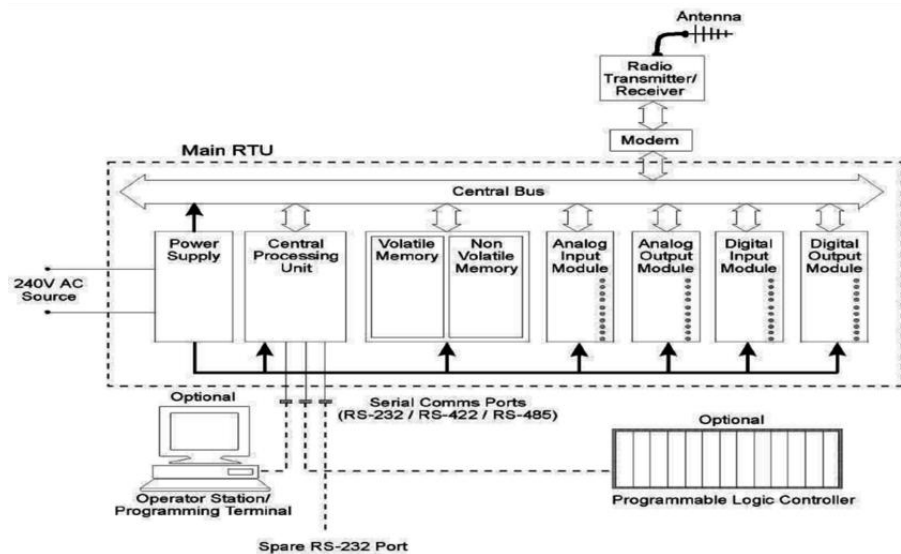


Figure 7 : Schéma général d'un RTU[14]

3. **MTU (Master Terminal Unit)** : il centralise les informations reçues des RTU, les rend accessibles via l'interface homme-machine (HMI) et transmet les commandes des opérateurs vers le terrain.

Le MTU correspond à une station centrale composée de plusieurs postes opérateurs connectés via un réseau local comme illustre la figure 8 Il assure :

- La collecte périodique des données provenant des RTU,
- La supervision globale du système,
- Le contrôle à distance des équipements.

Il permet également de configurer et programmer les RTU, ainsi que de diagnostiquer les éventuels problèmes de communication ou de fonctionnement. [10]

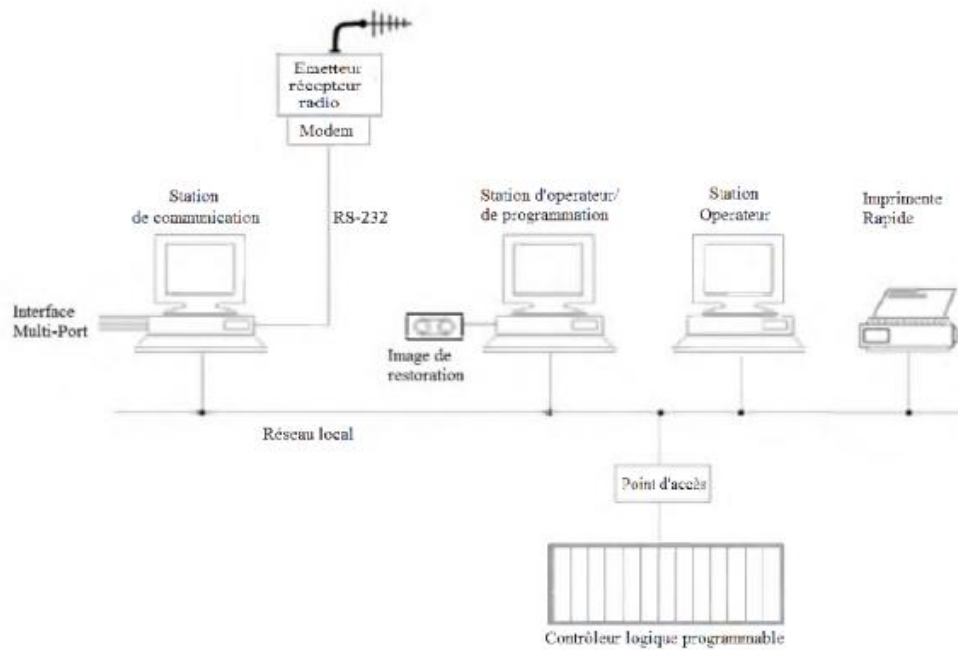


Figure 8 : Schéma général d'un MTU[14]

4. **Système de communication** : il assure la liaison entre le MTU et les différentes RTU. Cette communication peut s'effectuer à travers divers supports comme Internet, les réseaux filaires ou sans fil, ou encore le réseau téléphonique.

1.5.3 Architecture des systèmes SCADA

Les systèmes SCADA ont évolué en trois générations principales :

1. **Première génération (monolithique)** : systèmes centralisés, sans interconnexion avec d'autres systèmes. La redondance est assurée par une unité de secours.
2. **Deuxième génération (distribuée)** : traitement réparti sur plusieurs stations reliées par un réseau local, améliorant les performances et la fiabilité.
3. **Troisième génération (en réseau)** : systèmes ouverts utilisant des protocoles standards (comme IP), permettant une meilleure interopérabilité mais introduisant des risques liés à la cybersécurité.

1.5.4 Avantages du système SCADA

Le système SCADA présente de nombreux avantages dans la supervision et le contrôle des procédés industriels, parmi lesquels :

1. **Surveillance en temps réel** : il permet de suivre en continu l'état de fonctionnement du procédé à travers des interfaces graphiques, même lorsque les installations sont situées à distance.
2. **Contrôle des performances** : le SCADA assure le suivi des performances du système en temps réel. En cas de dégradation ou d'écart par rapport aux objectifs, des alarmes sont automatiquement déclenchées pour alerter l'opérateur.
3. **Détection et localisation des défauts** : il génère des alertes en cas de panne et permet d'identifier rapidement l'emplacement ainsi que l'équipement défaillant, facilitant ainsi le diagnostic et les interventions.
4. **Aide à la prise de décision** : grâce aux nombreuses informations fournies sur le système, il assiste l'opérateur dans ses choix et réduit les risques d'erreur lors des interventions.
5. **Optimisation des ressources humaines** : il permet de centraliser la supervision dans une salle de contrôle, réduisant ainsi les besoins en personnel sur le terrain.
6. **Réduction des déplacements** : la supervision à distance, via des interfaces graphiques, limite les visites sur les sites éloignés, tout en garantissant un suivi permanent de l'installation.

1.6 Les systèmes instrumentés de sécurité (SIS)

1.6.1 Définition SIS

Les systèmes instrumentés de sécurité (SIS) constituent un élément fondamental dans la prévention des risques au sein des installations industrielles. Leur conception, leur exploitation, leur maintenance ainsi que leurs modifications doivent garantir en permanence la disponibilité et la fiabilité des fonctions de sécurité.

Selon cette norme, un SIS est un système instrumenté destiné à assurer une ou plusieurs fonctions instrumentées de sécurité (SIF). Il est composé d'une combinaison de capteurs, d'unités logiques et d'éléments finaux.

1.6.2 Constitution d'un système instrumenté de sécurité

Un SIS a pour objectif de placer un procédé industriel dans un état sûr lorsqu'une situation dangereuse est détectée (incendie, explosion, etc.).

Il est généralement constitué de trois parties principales comme illustre la figure 9:

- **La partie capteur (Sensor) :**

Elle regroupe les dispositifs d'entrée tels que les capteurs et détecteurs, chargés de surveiller les paramètres physiques ou chimiques du procédé (température, pression, niveau, etc.).

- **L'unité logique (Logic Solver - LS) :**

Ce sous-système assure le traitement des informations reçues et prend les décisions nécessaires. Il peut s'agir d'un automate programmable industriel (API) ou d'un système informatique équipé de logiciels spécifiques.

- **La partie actionneur (Final Element - FE) :**

Elle intervient directement ou indirectement sur le procédé afin de le ramener à un état sûr. Par exemple, il peut s'agir de vannes d'arrêt d'urgence ou de vannes solénoïdes. L'action doit être réalisée dans un délai défini pour chaque fonction de sécurité.

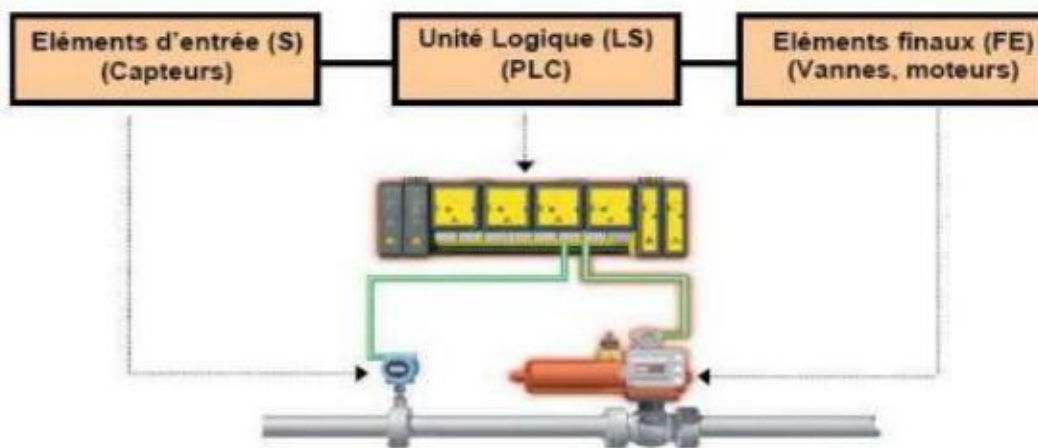


Figure 9 : Structure d'un SIS[23]

1.6.3 L'indépendance de SIS

L'indépendance entre le Safety Instrumented System (SIS) et le Basic Process Control System (BPCS) constitue un principe essentiel pour assurer la sécurité des installations industrielles. Le BPCS gère le fonctionnement normal du procédé, tandis que le SIS n'intervient que lors de situations anormales ou dangereuses afin de ramener le système vers un état sûr. Cette séparation, à la fois fonctionnelle et physique, permet d'éviter qu'une défaillance du BPCS n'impacte le bon fonctionnement du SIS.

1.7 l'IIoT (Industrial Internet of Things)

1.7.1 Définition de l'IIoT (Industrial Internet of Things)

L'Internet des Objets Industriel (IIoT) représente l'application des technologies de l'IoT au secteur industriel (Usine 4.0). Il se définit comme l'intégration synergique de capteurs intelligents, d'actionneurs et de machines connectées au cœur des infrastructures de production. L'objectif principal est de créer un écosystème interconnecté capable de collecter, transmettre et analyser des données massives (Big\ Data) en temps réel, avec une intervention humaine minimale.

Cette transition numérique permet de transformer des données brutes en indicateurs stratégiques grâce à des technologies de pointe telles que le *Cloud/Edge Computing*, l'Intelligence Artificielle (IA) et le *Machine Learning*. L'IIoT sert ainsi de catalyseur pour :

- **L'optimisation des processus** : Maximisation du rendement global des équipements (Taux de Rendement Global - TRG).
- **La maintenance prédictive** : Anticipation des pannes avant qu'elles ne provoquent un arrêt de production.
- **La gestion énergétique** : Suivi précis et réduction de l'empreinte carbone et des coûts opérationnels. [13]

1.8 La convergence IT/OT

Les entreprises de taille intermédiaire font face aujourd'hui à des cybermenaces comparables à celles des grandes organisations, sans toutefois disposer des mêmes ressources financières pour y faire face. La convergence entre les systèmes IT (technologies de l'information) et OT (technologies opérationnelles) permet d'unifier la visibilité sur l'ensemble des infrastructures. Grâce à l'intégration de plateformes Open XDR et de solutions basées sur l'intelligence artificielle au sein des SOC, ces organisations peuvent bénéficier d'une protection globale et plus efficace. La figure 10 montre un diagramme qui illustre la convergence entre l'automatisation industrielle (OT) et l'informatique connectée (IT). Leur intersection met en évidence l'IIoT (Internet des Objets Industriel), qui sert de pont technologique au cœur de l'Industrie 4.0.

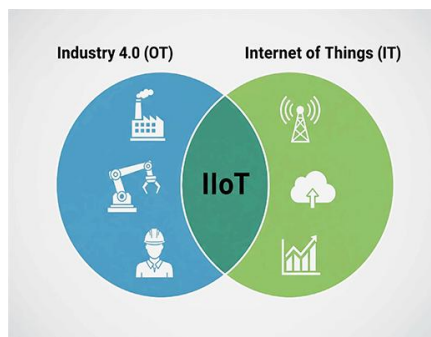


Figure 10 : La convergence OT IT[16]

1.9 Conclusion

Ce premier chapitre a permis de dresser un panorama complet des architectures de contrôle commande industriel (ICS). Nous avons mis en évidence la complémentarité entre les PLC (organes d'exécution locale), les systèmes DCS (dédiés aux régulations complexes distribuées) et les architectures SCADA (centrées sur la supervision longue distance). De plus, l'importance vitale de l'indépendance des systèmes de sécurité (SIS) a été soulignée face aux mutations technologiques actuelles, notamment l'introduction de l'IIoT et la convergence IT/OT.

Si cette transformation numérique vers l'Industrie 4.0 apporte des gains majeurs en matière de productivité et de flexibilité, elle interconnecte des réseaux autrefois isolés du monde extérieur, introduisant ainsi d'importantes vulnérabilités.

Le Chapitre suivant sera donc entièrement dédié à l'étude de la Cybersécurité Industrielle. Nous y analyserons en détail la nature des cybermenaces ciblant l'environnement OT, les vulnérabilités propres aux protocoles industriels, ainsi que les modèles de structuration défensive de référence, à l'instar du Modèle de Purdue et des stratégies de Défense en Profondeur.

Chapitre 2

La cyber sécurité

2.1 Introduction

Dans un contexte de transformation numérique accélérée et d'interconnexion croissante des systèmes, la cybersécurité est devenue un enjeu majeur pour les organisations industrielles et informatiques. Les infrastructures modernes reposent aujourd'hui sur une forte intégration entre les technologies de l'information (IT) et les technologies opérationnelles (OT), ce qui augmente leur efficacité mais également leur exposition aux cybermenaces.

Ce chapitre vise à présenter les concepts fondamentaux liés à la cybersécurité, en mettant en évidence ses objectifs principaux, ses domaines d'application ainsi que les différences entre les environnements IT et OT. Il aborde également les systèmes industriels tels que les ICS et SCADA, les cyberattaques les plus courantes, ainsi que les modèles de sécurité comme le modèle perdue et la défense en profondeur.

2.2 La cybersécurité

La cybersécurité regroupe l'ensemble des méthodes, processus, outils et comportements visant à protéger les systèmes informatiques, les réseaux ainsi que les données contre les cyberattaques et les accès non autorisés. Bien qu'elle repose fortement sur les solutions technologiques mises en place, son efficacité dépend également de manière significative du facteur humain.

En effet, les erreurs humaines, la négligence ou le manque de connaissances peuvent introduire des failles de sécurité exploitables par des cybercriminels. Ainsi, le respect des bonnes pratiques, la sensibilisation continue et l'application rigoureuse des protocoles de sécurité font des employés des acteurs essentiels dans la prévention des incidents et la protection des systèmes informatiques. [2]

2.3 La cyber sécurité industrielle

La cybersécurité industrielle concerne la protection des environnements de production ainsi que des systèmes de contrôle industriel, tels que les ICS et les systèmes SCADA. Contrairement à la cybersécurité classique orientée vers les systèmes informatiques (IT), elle se concentre sur les technologies opérationnelles (OT), directement liées au fonctionnement des machines, des procédés et des infrastructures physiques.

Son objectif principal est de sécuriser l'ensemble des composants industriels : équipements (automates programmables, capteurs, actionneurs), réseaux de communication et processus de production. Elle vise à prévenir les cyberattaques susceptibles de perturber les opérations, provoquer des arrêts de production, altérer la qualité des produits, ou même causer des dommages matériels et des risques pour la sécurité des personnes.

2.4 Objectifs de la cybersécurité

Les principales fonctions de sécurité visent à protéger les systèmes d'information selon la triade CIA qui est un modèle fondamental en cybersécurité utilisé pour protéger les systèmes d'information, les données et les échanges numériques. Elle constitue une base essentielle dans des normes comme **ISO 27001** et dans les stratégies de gestion des risques.

Elle repose sur trois principes complémentaires ce qui illustre la figure 11 :

- **Confidentialité** : limiter l'accès aux informations uniquement aux personnes autorisées.
- **Intégrité** : garantir que les données restent exactes et non modifiées.
- **Disponibilité** : assurer que les informations sont accessibles au bon moment.

CIA Triad

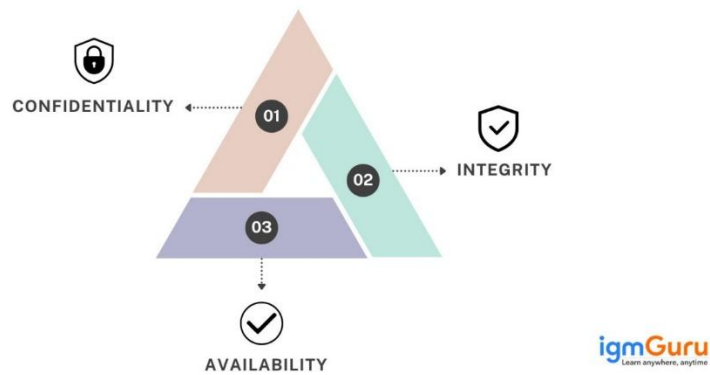


Figure 11 : La triade C.I.A[24]

1. Confidentialité

Elle protège les informations sensibles contre tout accès non autorisé. Elle repose sur :

- Le contrôle des accès,
- L'authentification forte,
- Le chiffrement des données,
- La sensibilisation des utilisateurs.

2. Intégrité

Elle garantit la fiabilité et l'exactitude des données. Elle est assurée par :

- La signature électronique,
- Les certificats numériques,
- L'horodatage,
- Les journaux d'audit.

Elle est essentielle pour la valeur juridique des documents.

3. Disponibilité

Elle assure l'accès continu aux systèmes et aux données. Elle nécessite :

- Des sauvegardes régulières,
- Des infrastructures fiables,
- Des plans de continuité et de reprise,
- Une surveillance constante. [3]

2.5 Définition du modèle Purdue

Le modèle Purdue est une architecture de référence utilisée pour organiser et sécuriser les systèmes de contrôle industriel (ICS). Il structure les réseaux industriels en plusieurs niveaux hiérarchiques afin de séparer les environnements **OT (opérationnels)** et **IT (informatiques)**, tout en contrôlant les échanges de données entre eux.

Son objectif principal est de :

- Segmenter le réseau industriel,
- Limiter la propagation des cyberattaques,
- Assurer un flux de données sécurisé et contrôlé,
- Protéger les processus industriels critiques.

2.5.1 Les niveaux du modèle Purdue

Le modèle est composé de plusieurs couches, allant du terrain jusqu'au système d'entreprise ce qui illustre la figure 12:

- **Niveau 4/5 (Entreprise – IT)** : systèmes de gestion (ERP), planification, logistique.
- **Niveau 3.5 (DMZ)** : zone intermédiaire sécurisée (pare-feu, proxys) qui sépare IT et OT.
- **Niveau 3 (Supervision)** : systèmes de gestion de production (MES, MOM, historiens).

- **Niveau 2 (Contrôle)** : systèmes SCADA, DCS, interfaces homme-machine (IHM).
- **Niveau 1 (Commande)** : automates programmables (PLC) et unités distantes (RTU).
- **Niveau 0 (Terrain)** : capteurs, actionneurs et processus physiques. [4]

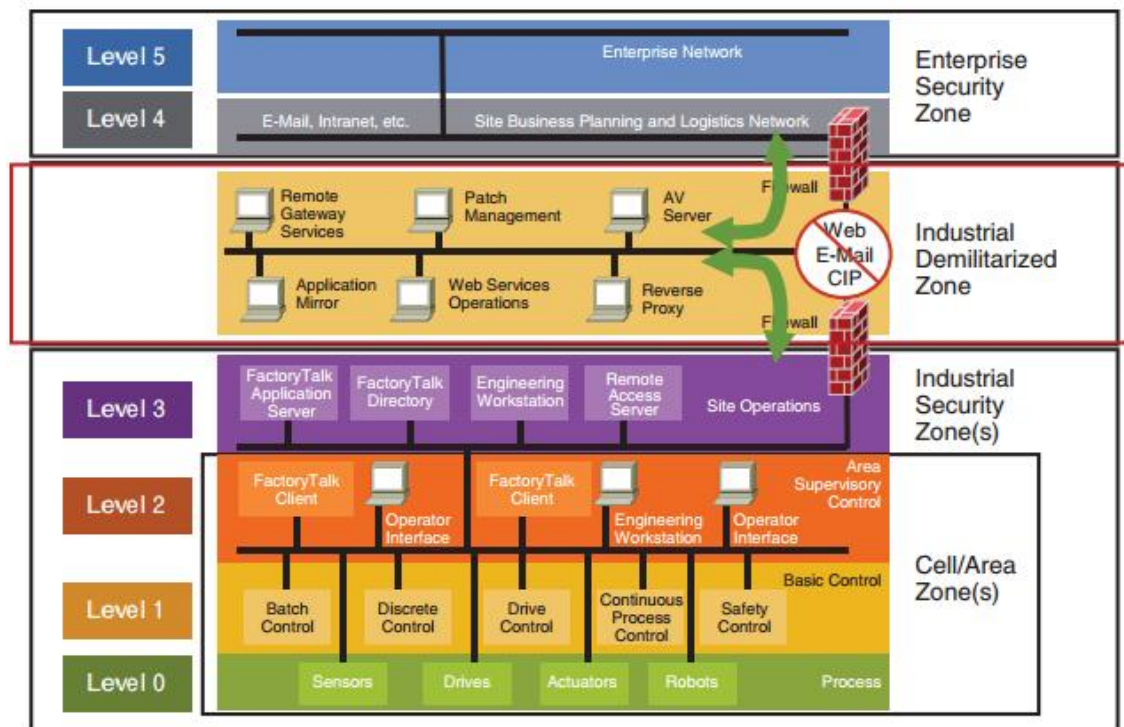


Figure 12 : Le modèle Perdue[15]

2.6 Définition l'OT (Operational Technology)

L'OT, ou technologie opérationnelle, regroupe l'ensemble des systèmes utilisés pour surveiller, contrôler et piloter des processus physiques dans les environnements industriels. Ces systèmes permettent d'observer en temps réel le fonctionnement des équipements et d'agir automatiquement pour ajuster les opérations.

Dans le secteur de la production, l'OT inclut notamment :

- Les machines industrielles comme les systèmes de commande numérique (CNC),
- Les systèmes de contrôle industriel, tels que les systèmes SCADA,

- Ainsi que les équipements qui interagissent directement avec le terrain (capteurs, actionneurs, automates[25])

2.7 Définition de l'IT (Technologies de l'Information)

L'IT, ou technologies de l'information (également appelées TIC), désigne l'ensemble des outils, systèmes et méthodes permettant de **créer, traiter, stocker, sécuriser et transmettre des informations** sous différentes formes : texte, image, audio ou vidéo.

Elle englobe un large éventail de technologies, notamment :

- Les ordinateurs et serveurs,
- Les réseaux informatiques (Internet, intranet),
- Les logiciels et applications,
- Les bases de données,
- Ainsi que les systèmes de communication numérique

2.8 Différence entre l'IT et l'OT

L'IT (technologies de l'information) et l'OT (technologies opérationnelles) sont toutes deux essentielles au fonctionnement des entreprises, mais elles ont des rôles et des objectifs très différents.

2.8.1 Objet (fonction principale)

- **IT** : se concentre sur la gestion de l'information. Elle traite les données, assure leur stockage, leur circulation et leur sécurité, et soutient les activités de l'entreprise comme la finance, les ressources humaines ou la communication.
- **OT** : se concentre sur les processus physiques. Elle contrôle et supervise les machines et les équipements industriels afin de garantir le bon déroulement de la production, la sécurité et la continuité des opérations.

2.8.2 Environnement

- **IT** : opère dans des environnements numériques classiques tels que les centres de données, le cloud, ainsi que sur les ordinateurs et les appareils mobiles des utilisateurs.
- **OT** : évolue dans des environnements industriels (usines, centrales, infrastructures), en interaction directe avec des équipements comme les automates programmables (PLC), les systèmes SCADA ou les robots.

2.8.3 Sécurité

- **Sécurité IT** : vise principalement à protéger les données (confidentialité, intégrité, disponibilité). L'objectif est d'empêcher les accès non autorisés et les fuites d'informations.
- **Sécurité OT** : met l'accent sur la sécurité des processus physiques. Une faille peut entraîner des arrêts de production, des dommages matériels ou des risques pour les personnes. La priorité est donc le fonctionnement sûr et continu des systèmes.

2.8.4 Mises à jour et maintenance

- **IT** : les systèmes sont mis à jour régulièrement pour corriger les vulnérabilités et améliorer les performances. Ces mises à jour sont souvent automatisées.
- **OT** : les systèmes ont une durée de vie plus longue et sont mis à jour moins fréquemment. Les interventions sont soigneusement planifiées pour éviter toute interruption. [5]

2.9 Définition des cyberattaques

Une cyberattaque est une action malveillante visant à accéder de manière non autorisée à un système informatique, un réseau ou des données, généralement dans le but de les voler, les exploiter ou perturber leur fonctionnement. Elle constitue souvent la première étape d'une intrusion plus grave, comme une violation de données.

Les objectifs d'une cyberattaque peuvent être :

- Voler des informations sensibles,
- Perturber ou arrêter un système,
- Infiltrer un réseau pour étendre l'attaque,
- Prendre le contrôle d'équipements ou de services.

Ces attaques peuvent être simples ou très sophistiquées, et peuvent cibler aussi bien des individus que des entreprises.

2.10 Exemples concrets

- **Malware (logiciel malveillant)** : un utilisateur visite un site frauduleux qui installe un programme malveillant permettant un accès à distance au système.
- **Phishing** : un faux e-mail incite une victime à fournir ses informations personnelles (mot de passe, données bancaires) via un site frauduleux.

Un exemple réel est l'attaque subie par l'entreprise CMA CGM, où un malware a compromis des serveurs, entraînant l'arrêt temporaire de certains services en ligne.

2.11 Principaux types de cyberattaques

- **Malware** : virus, vers, chevaux de Troie qui endommagent ou contrôlent les systèmes.
- **Phishing** : tromperie pour récupérer des données sensibles.
- **Ransomware** : blocage des données avec demande de rançon.
- **Déni de service (DoS/DDoS)** : saturation d'un service pour le rendre indisponible.
- **Man-in-the-Middle (MITM)** : interception des communications entre deux parties.
- **Cryptojacking** : utilisation des ressources d'un appareil pour miner de la cryptomonnaie.
- **Injection SQL** : exploitation de failles pour accéder aux bases de données.

- **Zero-day** : exploitation de vulnérabilités inconnues des développeurs.
- **Tunneling DNS** : utilisation détournée du protocole DNS pour exfiltrer des données.

Ce qui illustre dans la figure 13 les Type de cyberattaque

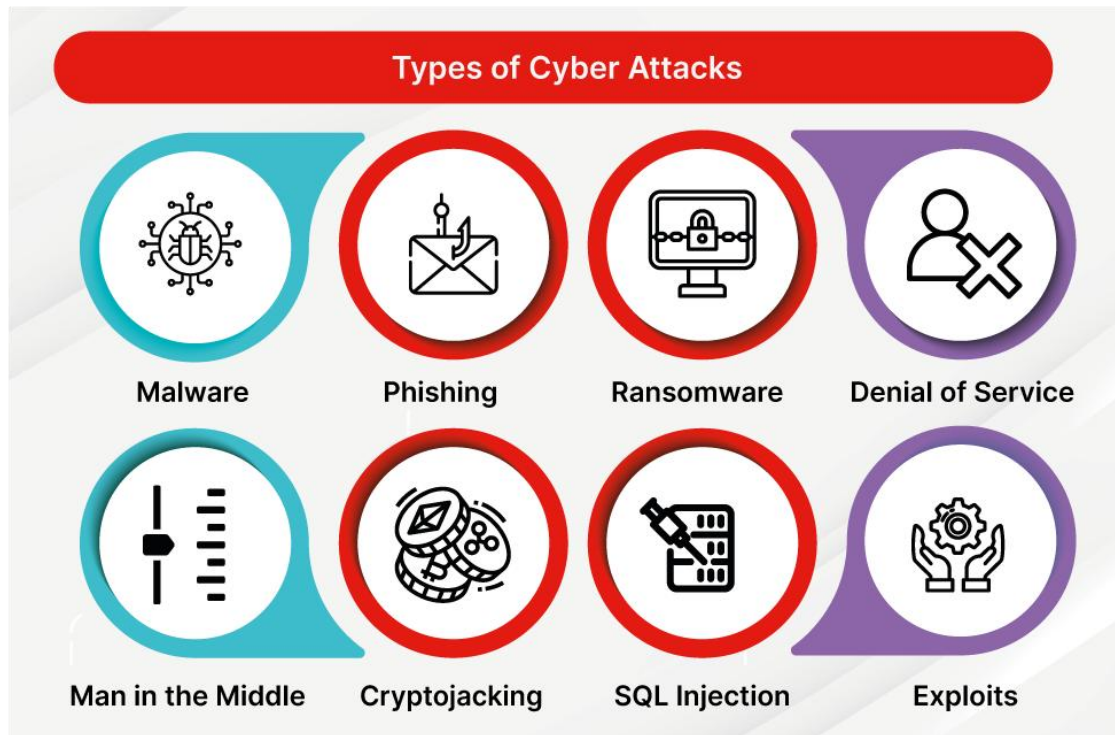


Figure 13 : Type de cyberattaque

2.12 La défense en profondeur

La défense en profondeur est une approche de sécurité qui consiste à superposer plusieurs mécanismes de protection afin de sécuriser les ressources d'une organisation. Le principe repose sur l'existence de plusieurs couches de défense : si l'une d'elles est contournée, les autres prennent le relais pour bloquer ou limiter la progression de la menace. Cette stratégie ne se limite pas aux aspects techniques (matériel et logiciels), mais prend également en compte le facteur humain, souvent à l'origine de failles liées à des erreurs ou à un manque de vigilance.

Face à l'évolution rapide des cybermenaces, de plus en plus complexes et étendues, la défense en profondeur s'impose comme une solution globale. Elle combine différents outils et techniques de sécurité pour protéger les terminaux, les données, les applications et les infrastructures réseau. Son objectif principal est de prévenir les attaques avant qu'elles ne surviennent, tout en étant capable de détecter et de contenir efficacement celles déjà en cours afin de réduire leur impact.

Les solutions classiques comme l'antivirus, les pare-feux, les passerelles sécurisées ou encore les réseaux privés virtuels (VPN) restent des éléments fondamentaux de cette stratégie. Toutefois, elles sont aujourd'hui complétées par des technologies plus avancées, telles que le machine learning, qui permet d'analyser les comportements et de détecter des anomalies au niveau des utilisateurs et des équipements, renforçant ainsi l'efficacité globale du dispositif de sécurité.[8]

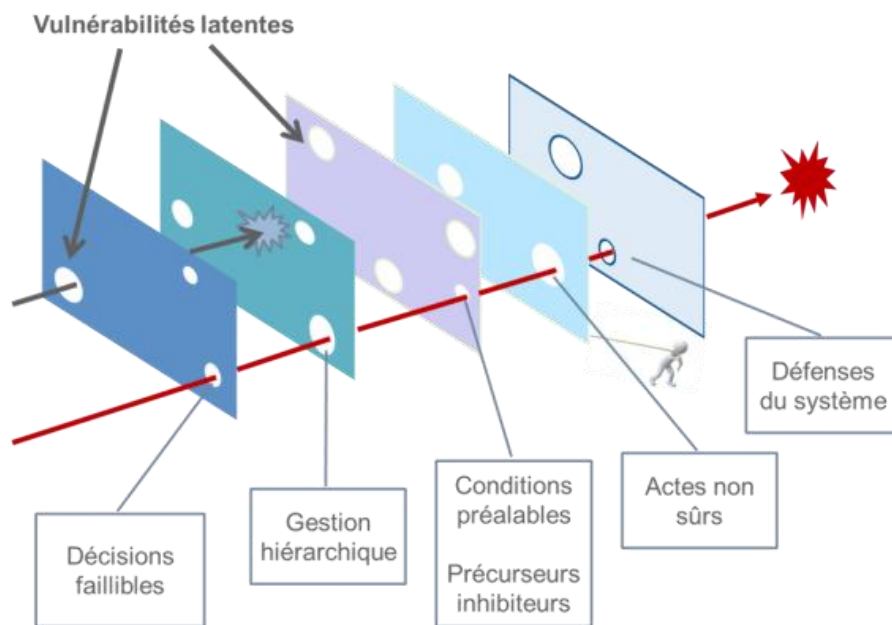


Figure 14 : Système de défense en profondeur [26].

2.13 Les différents éléments d'un système de défense en profondeur

Reposent sur une approche multicouche de la sécurité, qui combine plusieurs types de contrôles issus de domaines complémentaires.

- Les contrôles physiques regroupent les mesures destinées à protéger l'accès aux infrastructures, comme les cartes d'accès sécurisées pour entrer dans un bâtiment ou les dispositifs biométriques tels que les lecteurs d'empreintes digitales.
- Les contrôles de sécurité réseau concernent les mécanismes d'authentification permettant de vérifier l'identité des utilisateurs avant de leur donner accès au réseau, aux applications ou aux ressources internes.
- Les contrôles administratifs définissent les règles d'autorisation et limitent les accès des employés uniquement aux systèmes, applications ou zones du réseau nécessaires à leurs fonctions, une fois leur identité validée.
- Les solutions antivirus jouent un rôle essentiel en détectant et en bloquant les logiciels malveillants afin d'éviter leur introduction et leur propagation au sein du système informatique.
- L'analyse comportementale s'appuie sur des algorithmes et des techniques de machine learning pour identifier des activités inhabituelles, que ce soit au niveau des utilisateurs, des applications ou des équipements, permettant ainsi de détecter rapidement des comportements suspects.[8]

2.14 Conclusion

Ce chapitre pose les bases théoriques de la cybersécurité en distinguant l'IT (priorité à la confidentialité des données) de l'OT (priorité à la disponibilité et à la sécurité des procédés physiques). Il introduit le **modèle Purdue** pour segmenter les réseaux industriels et l'approche de la **défense en profondeur** pour contrer les menaces (malwares, injections) via plusieurs couches de contrôle. Ce cadre conceptuel est indispensable pour justifier

l'architecture dans laboratoire avec communication le protocole (Modbus TCP/IP) et les outils de protection (SIEM, IPS) déployés dans le laboratoire pratique du chapitre suivant.

Chapitre 3

Développement d'un laboratoire pour la cybersécurité

3.1 Introduction

Ce chapitre présente la conception et la validation d'une plateforme de simulation dédiée à la cybersécurité des systèmes industriels opérationnels. L'infrastructure repose sur un jumeau numérique simulant un convoyeur automatisé sous *Factory I/O*, piloté en temps réel par l'automate logiciel *OpenPLC*. La communication entre ces deux entités est assurée par le protocole standard *Modbus TCP/IP*, reflétant ainsi l'architecture classique d'une ligne de production moderne. À travers ce laboratoire, l'objectif est d'analyser la vulnérabilité de ces flux face à des menaces ciblées et de déployer des mécanismes de protection adaptés.

3.2 Architecture du Système Développé

l'architecture complète du laboratoire de cybersécurité industrielle mis en œuvre dans ce projet. Au centre, une machine virtuelle simule l'environnement opérationnel où l'automate (PLC) échange des données avec l'usine virtuelle *Factory I/O* via le protocole Modbus TCP. En amont, un script offensif injecte du trafic malveillant pour perturber cette communication en temps réel. En aval, une passerelle de sécurité intercepte ce flux réseau pour l'analyser et le neutraliser à l'aide de quatre modules complémentaires : un SIEM, un IPS global, l'outil de capture Wireshark et un IDS ce qui illustre la figure 15.

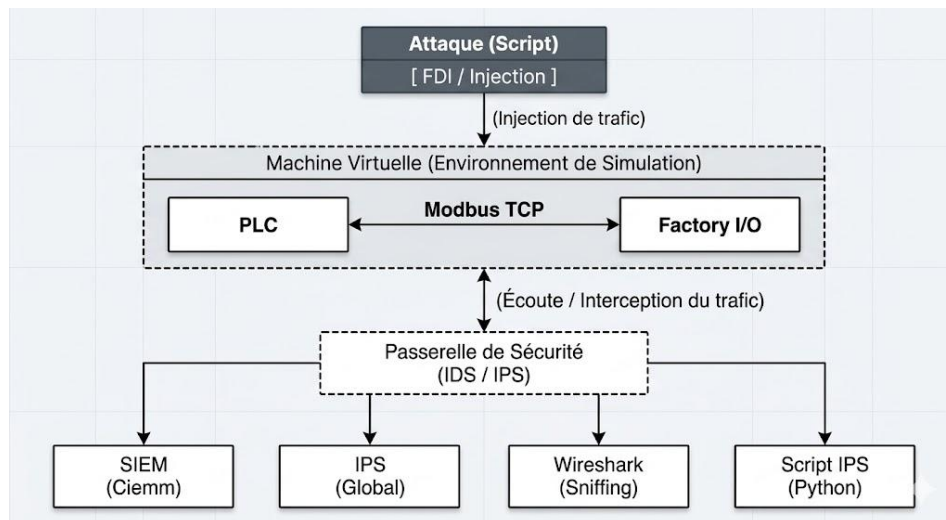


Figure 15 : Architecture du Système Développé

3.3 Les Bloc de Simulation (Environnement Virtuel)

Encadré par une zone virtuelle, ce bloc simule le cœur opérationnel de l'installation industrielle :

3.3.1. PLC (Automate Programmable Industriel) : Assure le contrôle-commande du procédé en exécutant la logique métier (ex. via OpenPLC).

3.3.2. Factory I/O : Assure la simulation physique et visuelle en temps réel du procédé industriel (ex. une ligne de convoyage, gestion de niveau).

3.3.3. Communication : L'échange de données entre le PLC et Factory I/O s'effectue via un protocole industriel standard (généralement Modbus TCP).

3.4 Les Bloc de Sécurité

ce bloc centralise la surveillance et la protection du réseau :

3.4.1. Le Système de Détection des Invasions IDS : il analyse le comportement des trames réseau en tâche de fond à l'aide d'un algorithme de fenêtre glissante pour lever une alerte dès qu'un écart par rapport au trafic nominal est détecté.

3.4.2. Le Systèmede Prévention des Invasions IPS: il passe d'une posture passive à une posture active en bloquant instantanément les paquets identifiés comme hostiles avant qu'ils ne corrompent les registres de l'automate.

3.4.3. L'Analyseur de Protocoles Wireshark (Sniffing) : Ce module est dédié à la capture de paquets en temps réel.

3.4.4.Le Gestionnaire d'Événements SIEM : Ce composant centralise l'ensemble des logs (journaux d'événements) et des alertes générés par la passerelle de sécurité. Il offre à

l'opérateur une interface de supervision (Tableau de bord) permettant de corréler les événements de sécurité avec l'état de la chaîne d'automatisation.

3.5. Etape de réalisation

3.5.1 Usine virtuelle

Ce projet présente la conception et la validation d'un système de convoyeur automatisé dont l'objectif est d'assurer le transport d'un objet, de détecter sa présence via un capteur, puis d'ordonner l'arrêt automatique du moteur.

Pour concevoir et valider cette logique de commande sans matériel physique, une architecture numérique combinant deux outils majeurs a été mise en place : le logiciel de simulation 3D **Factory I/O** pour reproduire l'environnement industriel virtuel (convoyeur, capteur et moteur)ce qui illustre la figure16 et l'automate programmable open-source **OpenPLC** pour l'exécution en temps réel du programme de contrôle (notamment en langage *Ladder Diagram*) ce qui illustre la figure 17.

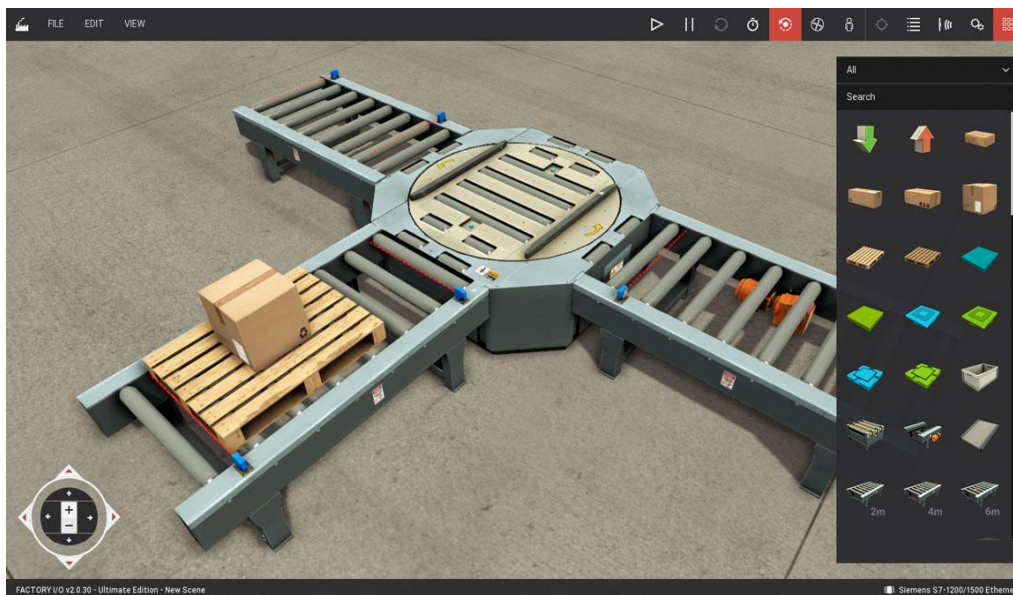


Figure 16 : Logiciel factoryIO

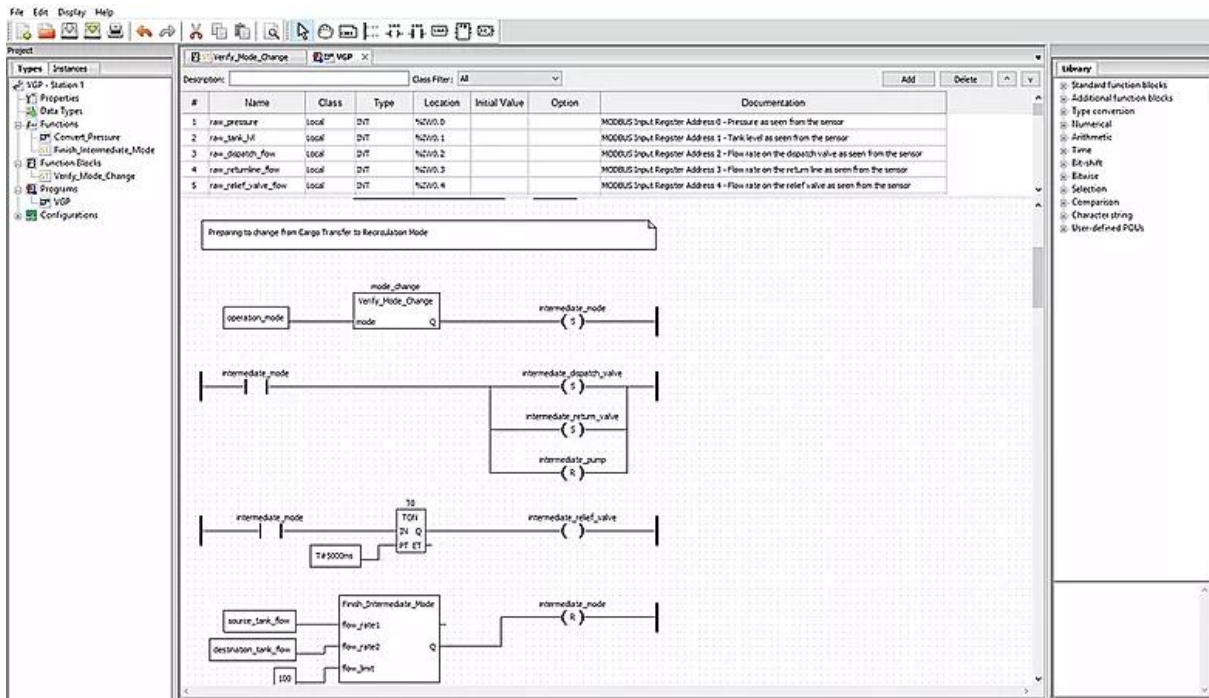


Figure 17: Logiciel open PLC[17]

La liaison et l'échange de données en temps réel entre ces deux entités sont assurés par le protocole de communication industriel **Modbus TCP/IP** sur réseau Ethernet, configuré après la création du projet *ce qui illustre dans la figure 18* et la connexion de l'éditeur OpenPLC à son service *Runtime ce qui illustre dans la figure 19*.

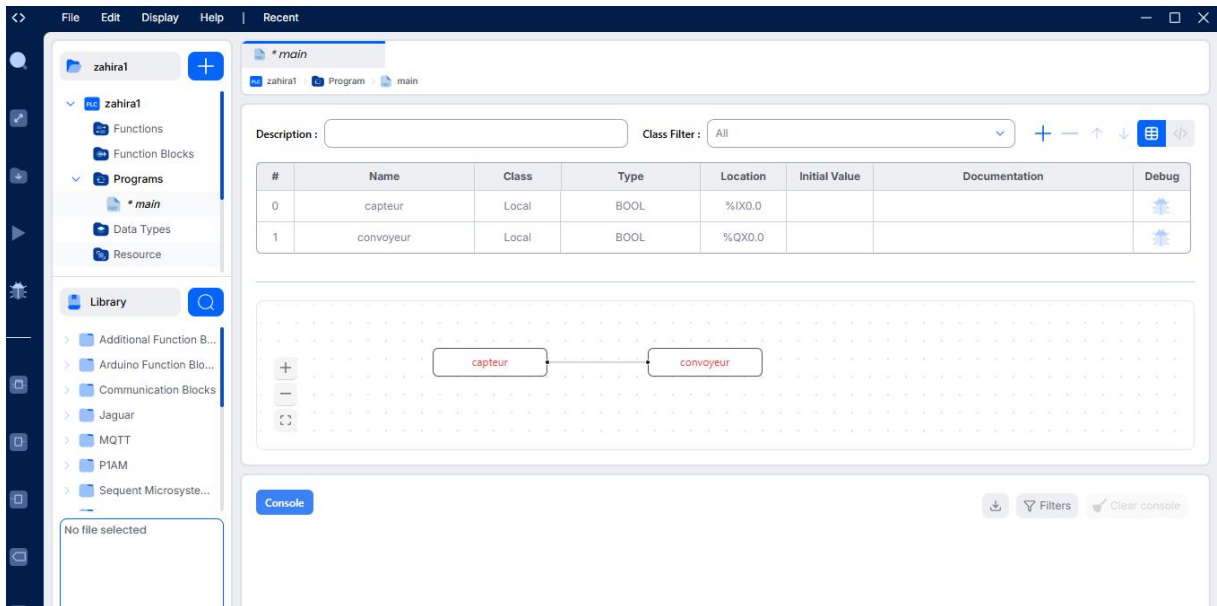


Figure 18 : Création du projet sur logiciel open PLC

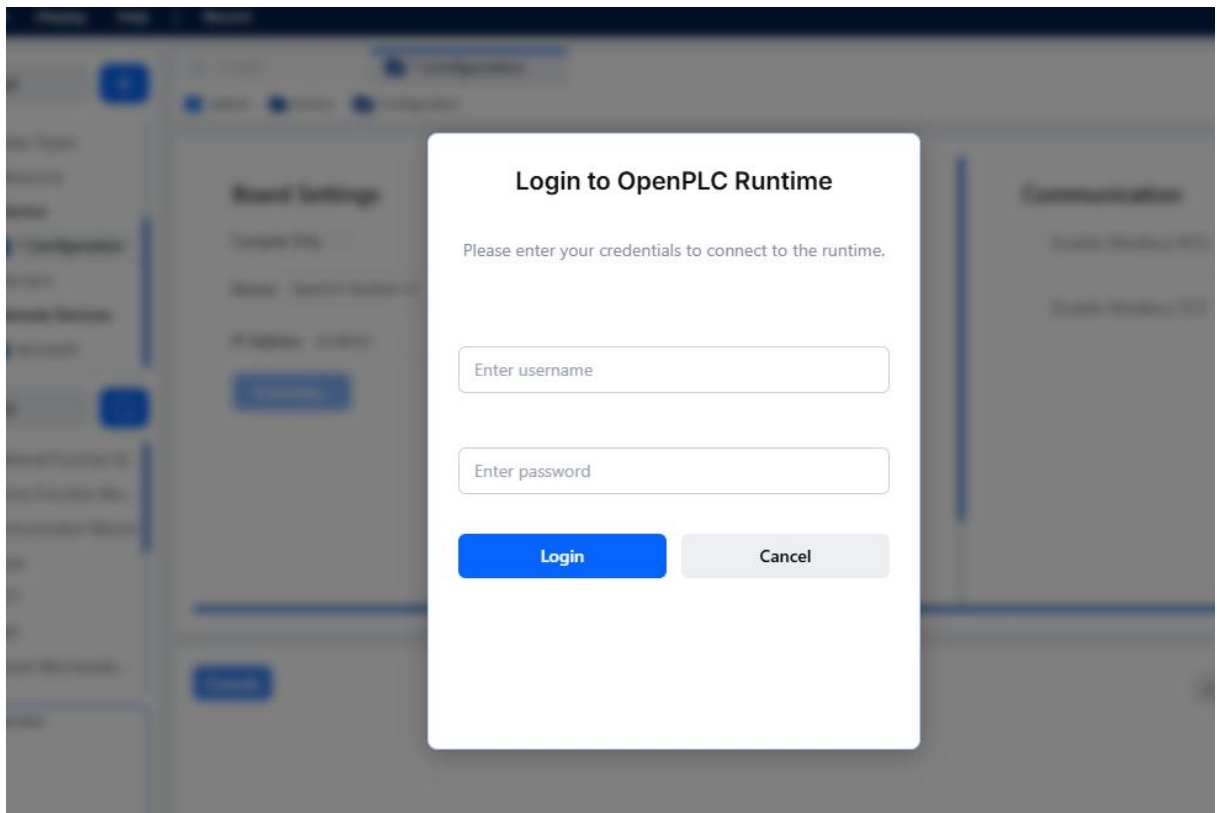


Figure 19 : Connecter OpenPLC runtime

Les résultats expérimentaux confirment la viabilité du système : la communication s'est révélée parfaitement stable ce qui illustre la figure 20 permettant au capteur de détecter précisément les objets et de déclencher l'arrêt instantané du moteur, validant ainsi la conformité de la logique de contrôle avant son implémentation physique ce qui illustre la figure 21.

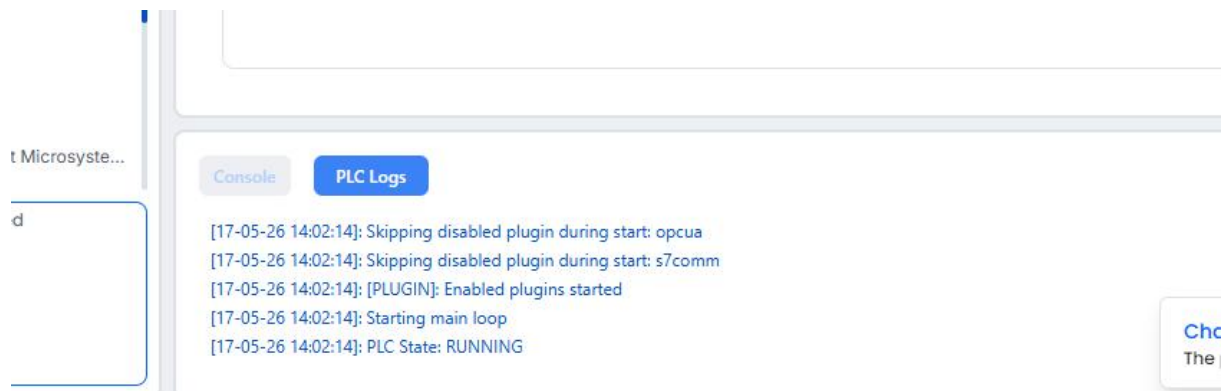


Figure 20 : La communication entre OpenPLC et Factory I/O est stable



Figure 21 : Le moteur s'arrête immédiatement lors de la détection

3.5.2. Analyse Détaillée des l'Attaque

3.5.2.1. Description des Techniques Utilisées

L'attaque conçue pour ce sabotage repose sur la combinaison stratégique de deux techniques

- **L'Attaque par Déni de Service (DoS - Denial of Service) par inondation :** Cette technique consiste à envoyer un flux massif et continu de requêtes réseau vers l'automate (OpenPLC). En submergeant le canal de communication, l'attaquant sature la pile TCP/IP et les capacités de traitement de la cible et la figure 22 montre son organigramme:

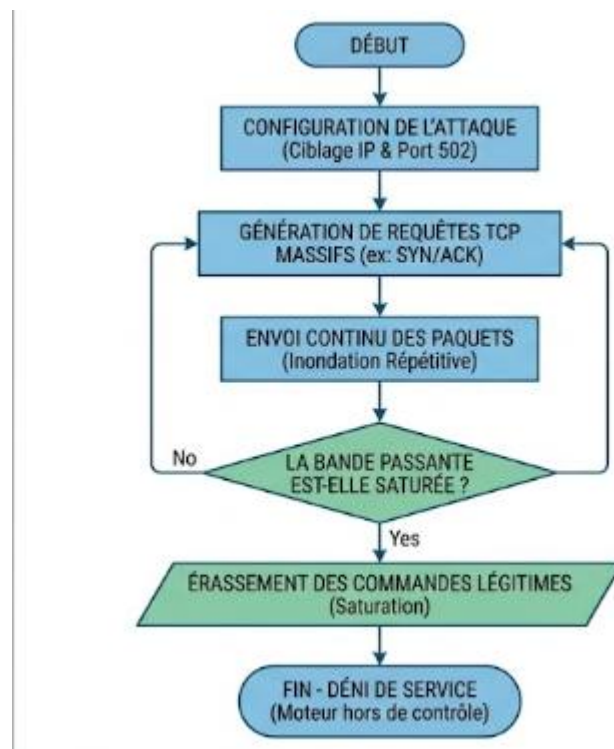


Figure 22 :organigramme de attaque DOS

- **L'Attaque par Injection de Fausses Données (FDIA - False Data Injection Attack) :** Contrairement à un DoS classique qui cherche uniquement à déconnecter un équipement, la FDIA est une attaque ciblée sur l'intégrité des données. À l'aide de la bibliothèque Python pyModbusTCP, l'attaquant forge des requêtes d'écriture spécifiques (Write Single Coil) orientées vers l'adresse du registre qui contrôle le moteur. L'objectif est d'injecter continuellement la valeur True la figure 22 montre son organigramme

ORGANIGRAMME : ATTAQUE FDIA (INJECTION DE FAUSSES DONNÉES)

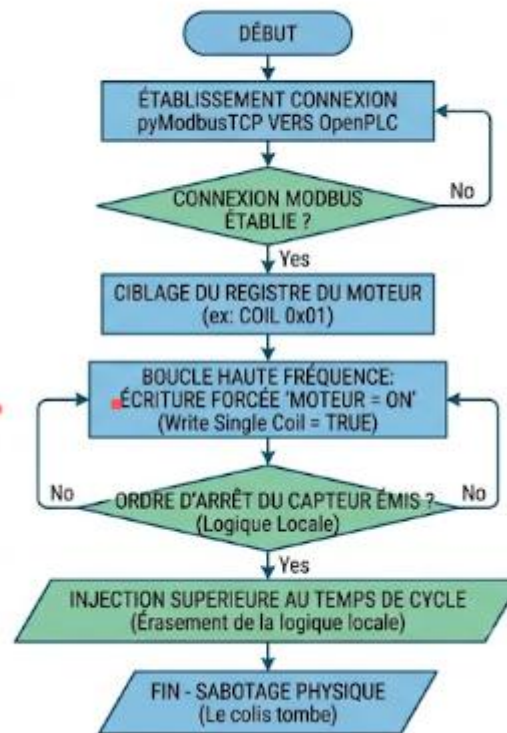


Figure 23 :organigramme de attaque injection

3.5.2.2.Impact de l'Attaque par Sabotage d'Interface

L'attaque par sabotage d'interface repose sur l'injection d'ordres d'allumage à une fréquence critique, nettement supérieure au temps de cycle normal d'OpenPLC, ce qui provoque la saturation immédiate de son registre. En raison de ce flux massif de données, l'automate réécrit instantanément la valeur *True* (marche), empêchant ainsi la logique locale de sécurité d'exécuter l'ordre d'arrêt et de stabiliser l'état du système ce qui illustre la figure 23 Ce conflit logique se traduit par une défaillance physique directe : le convoyeur ignore totalement les commandes de sécurité et le moteur continue de tourner sans interruption. En conséquence, les colis finissent par tomber de la bande transporteuse, entraînant un incident de production majeur et matérialisant le succès d'une action de sabotage industriels ce illustre la figure24

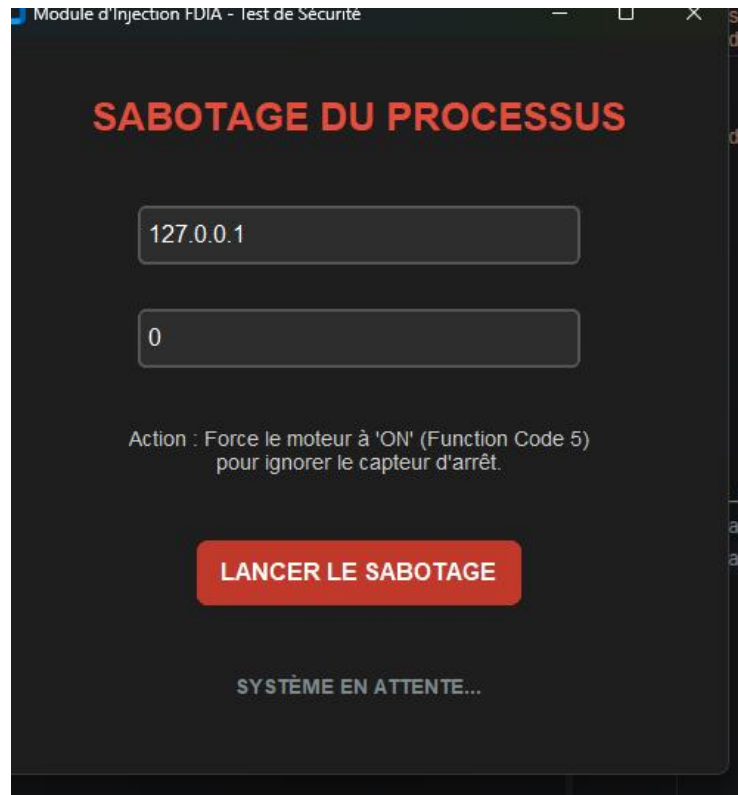


Figure 23: interface sabotage



Figure 24: colis tombe

3.3.3.Le Bloc de Sécurité

Dans le cadre de la sécurisation des systèmes industriels (OT), les **IDS** (Systèmes de Détection d'Intrusions) et les **IPS** (Systèmes de Prévention d'Intrusions) s'appuient sur plusieurs techniques complémentaires pour identifier et bloquer les activités suspectes, comme les injections de fausses données (FDIA) ou les saturations de registres.

3.3.3.1.Techniques de Détection de l'IDS

Pour assurer la sécurité du réseau industriel (Modbus TCP/IP) et protéger l'automate OpenPLC contre des attaques telles que le sabotage par injection de commandes à haute fréquence, l'IDS s'appuie sur trois approches complémentaires :

➤ **Détection par Signatures (Misuse Detection)**

Analyse du trafic réseau en le comparant à une base de données d'empreintes ou de règles prédéfinies d'attaques connues. Permet le Blocage immédiat des adresses IP non autorisées (listes noires) ou rejet des paquets Modbus contenant des codes fonctions interdits en production.

➤ **Détection d'Anomalies (Anomaly Detection)**

Modélisation du comportement normal du réseau (*baseline*) afin de détecter tout écart statistique ou comportemental suspect Permet Identification de l'attaque de sabotage grâce à l'analyse de la fréquence : l'IDS détecte un volume anormal d'ordres d'allumage par seconde, dépassant largement le temps de cycle standard de l'automate.

➤ **Inspection Profonde des Paquets & Analyse d'État (DPI / Process-Aware)**

Analyse minutieuse de la structure interne des protocoles industriels et vérification de la cohérence logique du processus physique permet L'IDS ne vérifie pas seulement la conformité du paquet Modbus TCP, il valide aussi la cohérence de la commande par rapport à l'état des capteurs physiques

3.3.3.2. La Technique Utilisée La Détection d'Anomalies Basée sur le Seuil de Fréquence

Il analyse le *comportement* du protocole Modbus TCP. Il sait qu'en fonctionnement normal, le taux de requêtes d'écriture (Force Single Coil - FC5) est bas. Une explosion soudaine de la fréquence (plus de 5 paquets par seconde) rompt la *baseline* (le comportement de référence) et déclenche l'alerte.

La logique de détection de l'IDS repose sur l'application d'une règle d'analyse temporelle stricte, adossée à une fenêtre glissante d'une seconde. Le comportement du système est régi par deux états distincts :

En fonctionnement nominal : Le trafic Modbus TCP d'écriture demeure faible, prévisible et parfaitement synchrone avec les cycles du procédé. L'analyse comportementale valide la légitimité du flux, et l'interface de supervision de l'IDS affiche un statut global **VERT**, matérialisant un « **TRAFFIC SAIN** » (*comme illustré sur la Figure 25*)

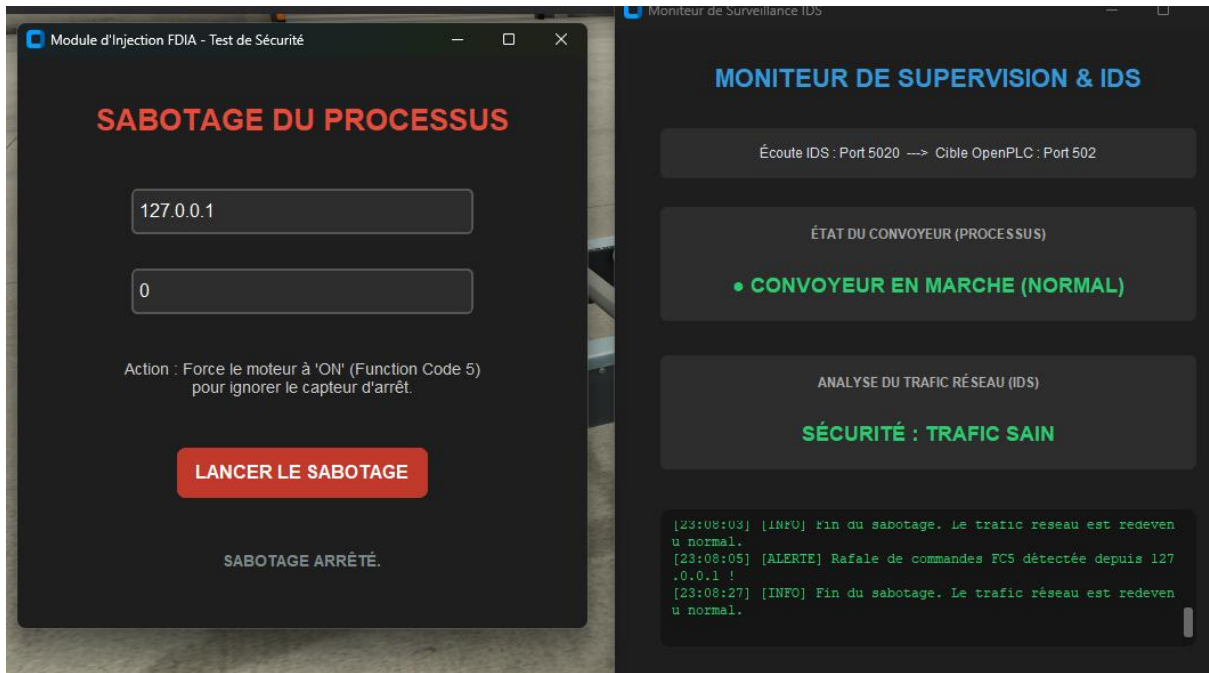


Figure 25 : IDS en mode fonctionnement normale

En phase d'attaque (Sabotage) : Dès l'activation de l'injection massive par l'attaquant, la fréquence des requêtes s'effondre logiquement hors des limites tolérées. L'IDS identifie le franchissement du seuil d'anomalie dès lors que plus de 5 requêtes d'écriture de type Write Single Coil (Code Fonction FC5) sont enregistrées en moins d'une seconde. Cette rupture statistique déclenche instantanément la levée d'une alerte : l'interface graphique bascule en **ROUGE FLASH**, doublée d'un signal visuel et sonore critique (*voir Figure 26*).

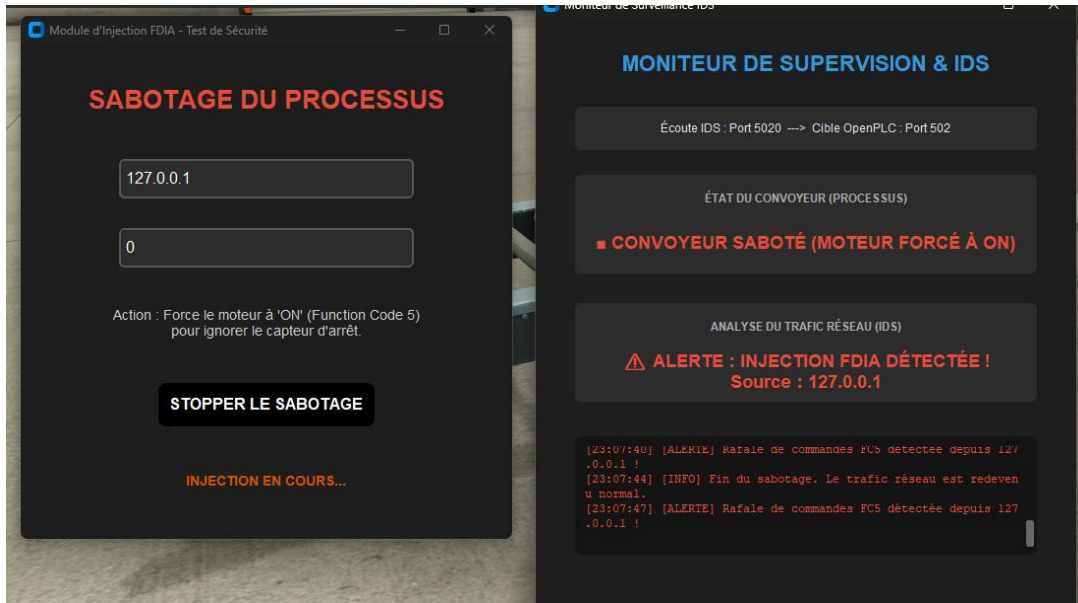


Figure 26: IDS dans le cas de sabotage

3.3.3.3. Techniques de IPS:

➤ Le Filtrage Actif en Ligne (*Inline Packet Dropping*)

C'est la technique reine pour un IPS configuré en mode proxy ou pont applicatif, L'IPS examine le paquet en temps réel. Si le paquet est jugé malveillant (par exemple, s'il dépasse le seuil de fréquence de ton attaque de sabotage), l'IPS décide simplement de ne pas le retransmettre et de le détruire (*drop*).

➤ La Réinitialisation de Connexion (*TCP Reset / Connection Termination*)

Cette technique est utilisée lorsque l'IPS ne bloque pas directement le flux physique mais envoie des commandes pour tuer la communication. Dès qu'une anomalie ou une signature d'attaque est détectée, l'IPS génère et injecte de faux paquets TCP avec le flag **RST (Reset)** en se faisant passer pour l'automate ou pour la station de supervision. Cela force la fermeture immédiate et brutale de la session TCP entre l'attaquant et la cible.

➤ **La Reconfiguration Dynamique du Pare-feu (*Firewall Rate-Limiting & Shunning*)**

L'IPS agit ici en donneur d'ordres pour l'infrastructure réseau. Lorsque l'IPS détecte un comportement suspect, il communique instantanément avec le pare-feu local (ou des règles de routage comme `iptables` sous Linux) via une API ou un script. Il lui ordonne de bannir l'IP de l'attaquant (*Shunning*) ou de limiter drastiquement son débit (*Rate-Limiting*).

➤ **La Normalisation de Protocole (*Traffic Scrubbing / Protocol Sanity*)**

Une technique axée sur la conformité stricte des protocoles industriels. L'IPS nettoie le trafic réseau en éliminant les paquets qui violent les spécifications standards du protocole (options TCP invalides, structures de paquets Modbus corrompues ou payloads anormalement longs). Il s'assure que seules des requêtes "propres" parviennent à l'automate.

3.3.3.4. La Technique Utilisée : Le Filtrage Actif en Ligne avec Blocage par Adresse IP (*Inline Packet Dropping & Stateful Host Shunning*)

L'IPS utilise une combinaison de deux techniques de prévention avancées :

- **Le Filtrage Actif en Ligne (*Inline Packet Dropping*)** : L'IPS est placé directement sur le chemin de communication (mode *Inline*). Il intercepte et inspecte le paquet *avant* de décider s'il doit le relayer ou non à l'automate OpenPLC.
- **Le Bannissement Dynamique de l'Hôte (*Host Shunning / Blacklisting*)** : C'est l'évolution clé par rapport au simple filtrage par paquet. Au lieu de jeter les paquets d'attaque un par un, l'IPS change d'état dès que le seuil de 5 requêtes par seconde est franchi. Il marque l'adresse IP de l'attaquant comme "**hostile**" et applique une politique de sécurité stricte : le blocage systématique de tout flux provenant de cette source.
- **En fonctionnement nominal (Figure 27)** : Les flux de communication s'effectuent sans aucune restriction. L'IPS valide la conformité et la fréquence des requêtes, permettant aux

colis de transiter normalement sur le convoyeur. L'interface graphique de l'IPS confirme la transparence du pont réseau en affichant un statut stable.

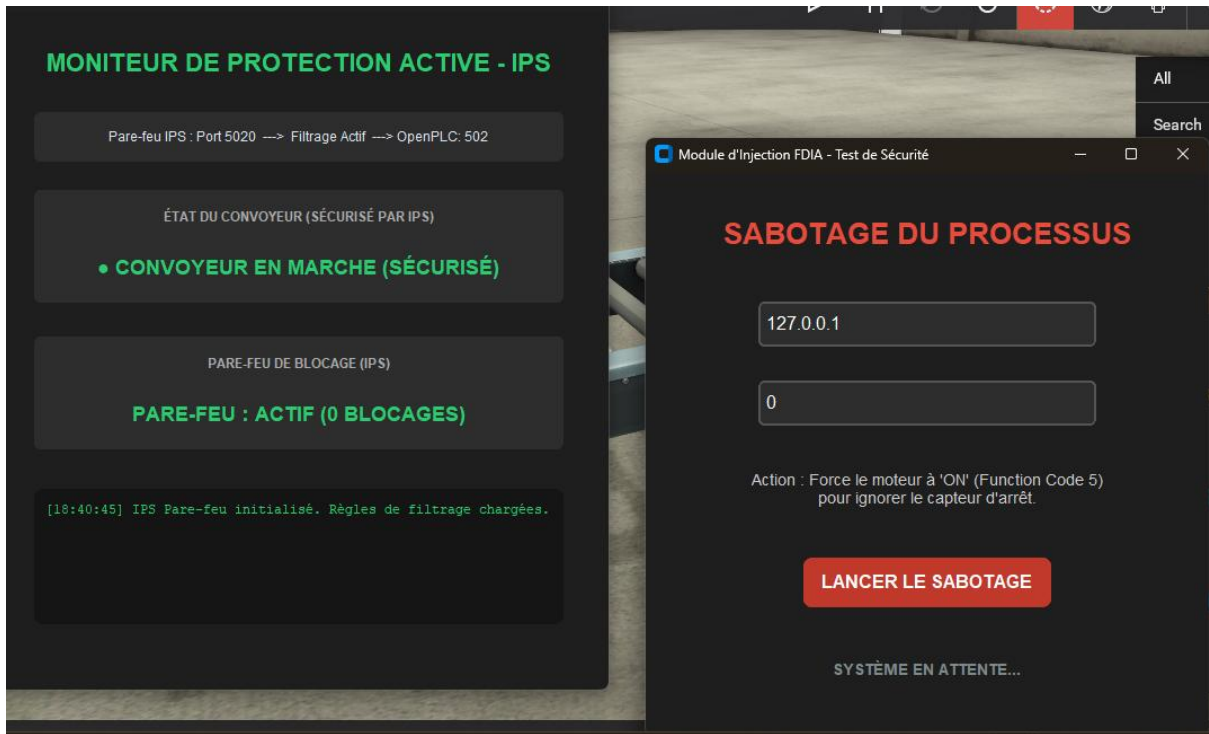


Figure 27: IPS en mode fonctionnement normale

En phase de mitigation du sabotage (Figure 28) : Dès que l'attaquant exécute son script d'injection, l'IPS comptabilise plus de 5 requêtes d'écriture (FC5) en l'espace d'une seconde. Le franchissement de ce seuil critique modifie instantanément la politique de sécurité : l'IPS déclare l'adresse IP source comme « hostile » et bascule en mode blocage strict (*Drop*). Tous les paquets ultérieurs provenant de cette adresse IP sont immédiatement détruits à la périphérie du système et ne sont jamais relayés au port standard 502 d'OpenPLC.

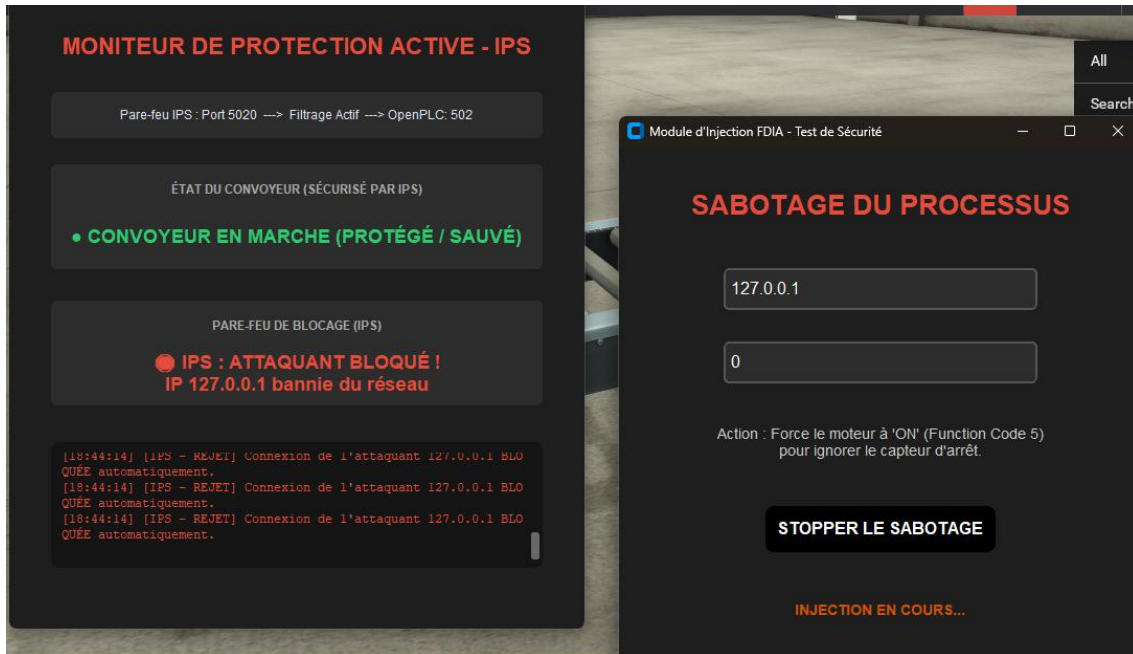


Figure 28: IPS dans le cas de sabotage

3.3.3.5. Implémentation sur wireshark

l'analyse des communications réseau à l'aide du logiciel Wireshark. Les paquets échangés entre OpenPLC et Factory I/O sont capturés et analysés afin de vérifier la transmission correcte des données et le bon fonctionnement du protocole de communication industriel ce qui illustre la figure 29.

No.	Time	Source	Destination	Protocol	Length	Info
2343	32.105832400	127.0.0.1	127.0.0.1	Modbus...	56	Response: Trans: 1368; Unit: 1, Func: 5: Write Single Coil
2345	32.209822500	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1369; Unit: 1, Func: 2: Read Discrete Inputs
2347	32.218386200	127.0.0.1	127.0.0.1	Modbus...	54	Response: Trans: 1369; Unit: 1, Func: 2: Read Discrete Inputs
2349	32.212532300	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1370; Unit: 1, Func: 5: Write Single Coil
2351	32.214256100	127.0.0.1	127.0.0.1	Modbus...	56	Response: Trans: 1370; Unit: 1, Func: 5: Write Single Coil
2353	32.321546300	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1371; Unit: 1, Func: 2: Read Discrete Inputs
2355	32.322862000	127.0.0.1	127.0.0.1	Modbus...	54	Response: Trans: 1371; Unit: 1, Func: 2: Read Discrete Inputs
2357	32.325595100	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1372; Unit: 1, Func: 5: Write Single Coil
2359	32.326686300	127.0.0.1	127.0.0.1	Modbus...	56	Response: Trans: 1372; Unit: 1, Func: 5: Write Single Coil
2361	32.431889600	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1373; Unit: 1, Func: 2: Read Discrete Inputs
2363	32.432592600	127.0.0.1	127.0.0.1	Modbus...	54	Response: Trans: 1373; Unit: 1, Func: 2: Read Discrete Inputs
2365	32.435734700	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1374; Unit: 1, Func: 5: Write Single Coil
2367	32.438687500	127.0.0.1	127.0.0.1	Modbus...	56	Response: Trans: 1374; Unit: 1, Func: 5: Write Single Coil
2369	32.544227100	127.0.0.1	127.0.0.1	Modbus...	56	Query: Trans: 1375; Unit: 1, Func: 2: Read Discrete Inputs

Frame 1: Packet, 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF{...}	0000	02 00 00 00 45 00 00 34	d0 d1 40 00 00 06 2b f0	E-4 ..@..+
> Null/loopback	0010	7f 00 00 01 7f 00 00 01	dc 3d 01 f6 67 67 bb 4f	*..ggO
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1	0020	27 05 8b 0b 50 18 00 de	f9 cc 00 00 03 0f 00 00	*...P... ..
> Transmission Control Protocol, Src Port: 56381, Dst Port: 502, Seq: 1, Ack: 1, Len: 12	0030	00 06 01 02 00 00 00 01		
> Modbus/TCP				
> Modbus				

Figure 29: Résultat sur wireshark

3.4. validation pratique

3.4.1. description de système

Cette architecture industrielle multicouche décrit un système cyber-physique de gestion et de distribution de carburant. Le niveau supérieur est articulé autour d'un serveur SCADA BR qui assure la supervision et le contrôle depuis la salle de commande. Les données et instructions opérationnelles transitent de manière bidirectionnelle via un réseau hybride combinant Modbus TCP/IP et liaisons Wi-Fi. Au cœur du système, un microcontrôleur intelligent ESP32 traite localement la logique algorithmique et les alarmes. Enfin, cette unité contrôle directement les équipements de terrain, notamment un capteur ultrasonique HC-SR04 et un relais statique (SSR) pilotant la pompe de distribution reliée au stockage principal.figure30

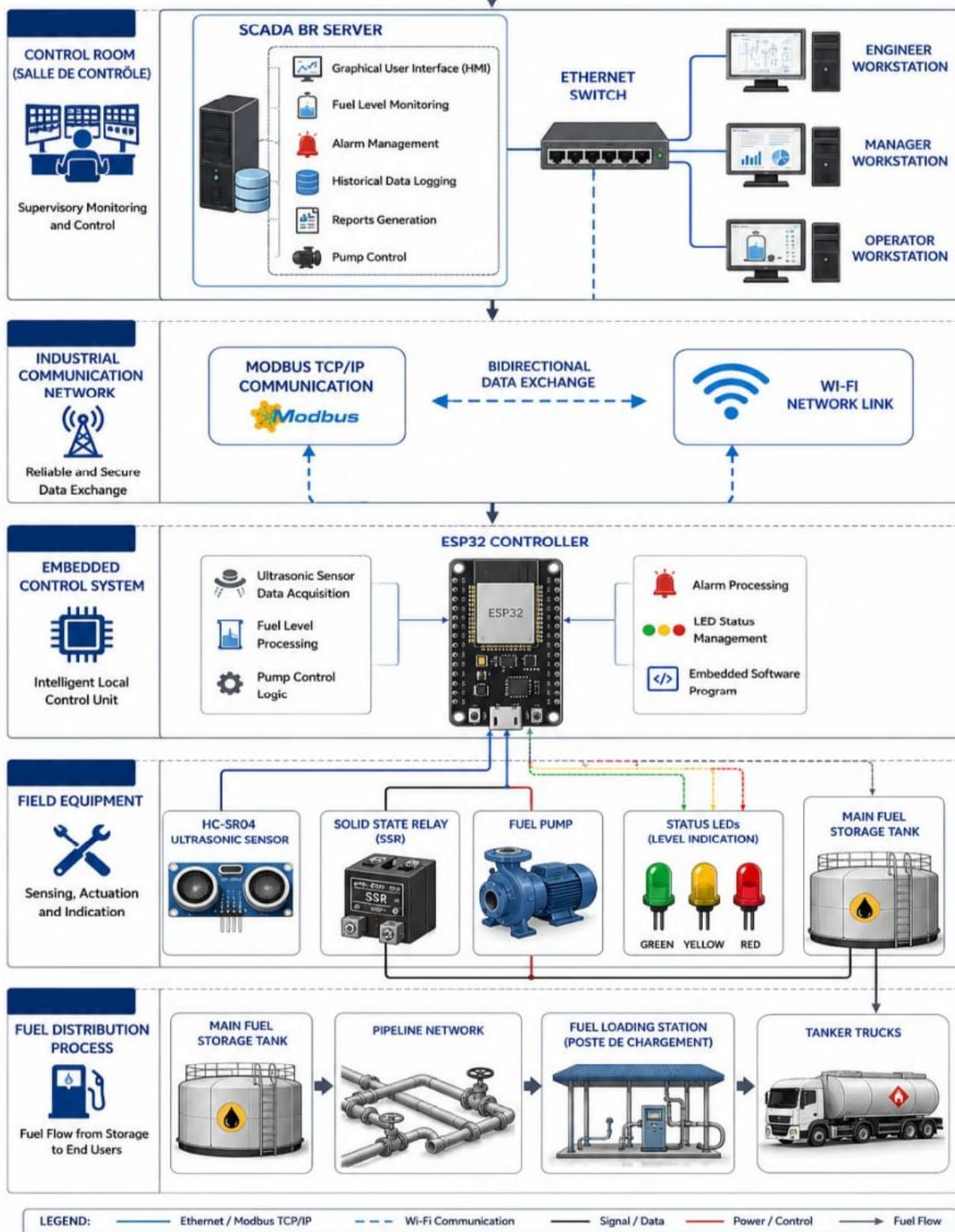


Figure 30: architecture de system

3.4.2. Mécanisme de l'Attaque par Déni de Service (DoS)

L'évaluation de la sécurité du système cyber-physique repose sur la simulation d'une menace combinant une interception de type homme du milieu (**Man-in-the-Middle - MitM**) et une inondation applicative ciblée. À l'aide de l'application graphique « MODBUS TCP DoS ATTACKER » développée en Python

l'attaquant valide d'abord son positionnement transparent sur le réseau en établissant une liaison préalable avec l'automate OpenPLC via le port de transit 5020. Cette phase de reconnaissance réseau est cruciale pour le saboteur, car elle confirme l'accessibilité de la cible et l'absence de filtrage défensif ce qui illustre la figure 31.

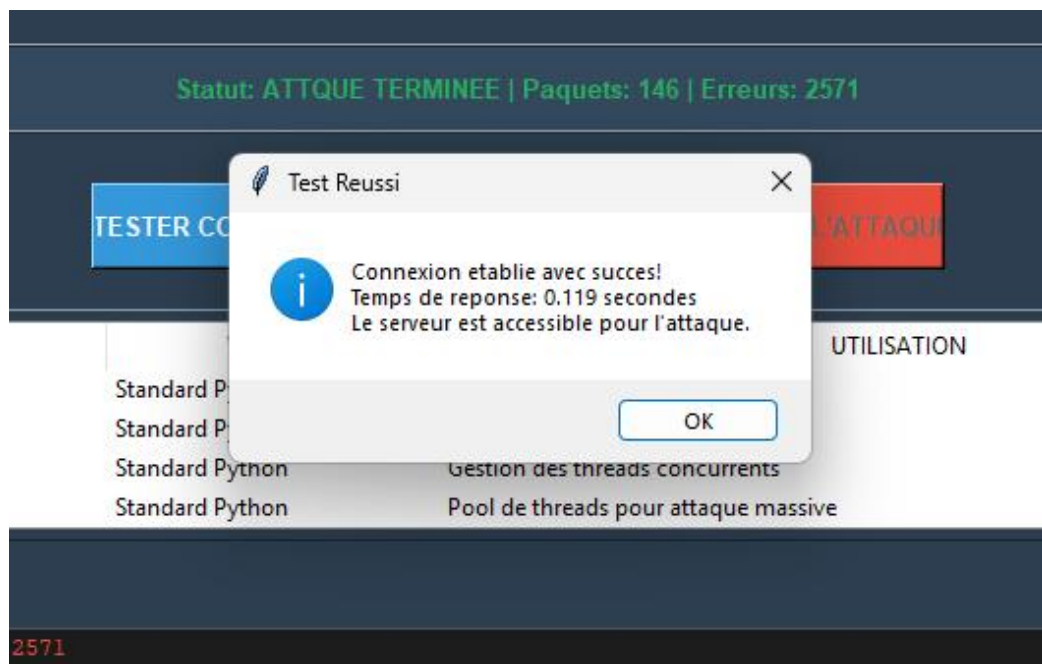


Figure 31: Connexion établie avec succès

Une fois cette connectivité validée, le déclenchement de l'attaque par déni de service (DoS) sature (figure 32) la pile réseau de l'automate par l'injection massive et continue de requêtes Modbus frauduleuses. Submergé par ce flux, l'automate consacre l'intégralité de ses ressources CPU au trafic malveillant, provoquant la rupture des communications légitimes, l'aveuglement total de la salle de contrôle SCADA BR et l'incapacité à stabiliser le procédé physique.

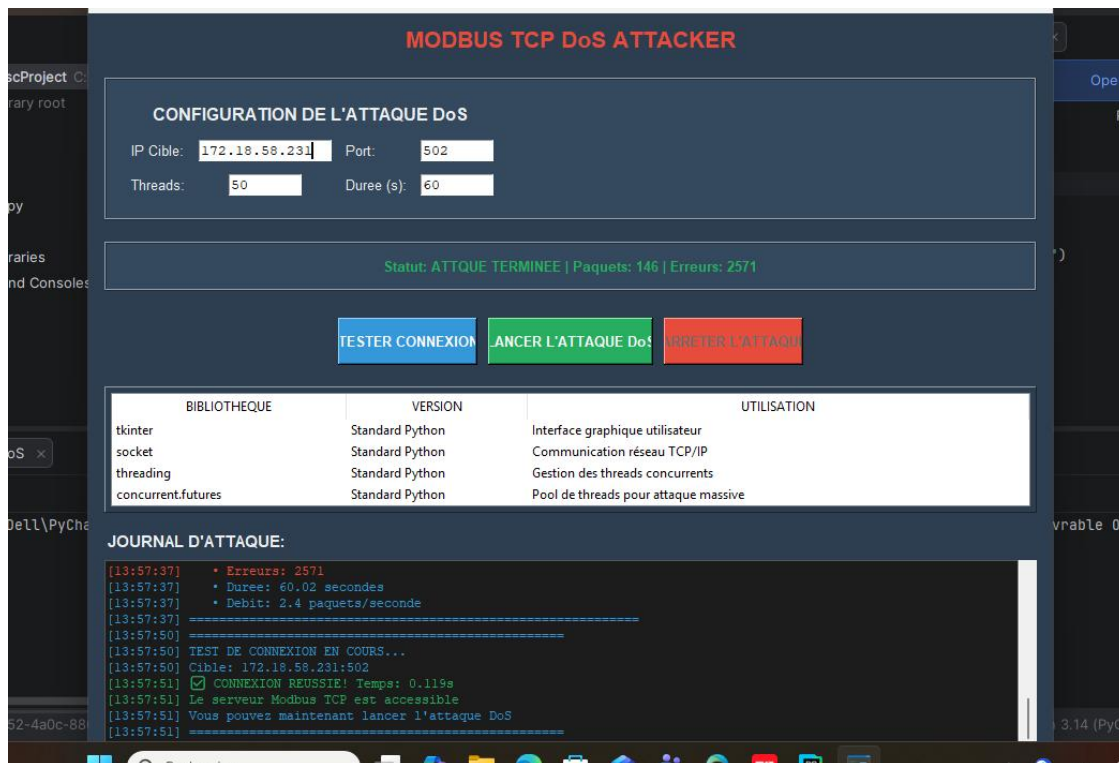


Figure 32: l'Interface de Sabotage (Modbus TCP DoS Attacker)

3.5 Conclusion

En conclusion, l'impact physique de l'attaque par injection de données a matérialisé le manque de sécurité inhérent aux protocoles industriels historiques. La mise en place d'une passerelle défensive basée sur un IDS/IPS comportemental a permis de sécuriser le procédé

en bloquant les requêtes de forçage avant toute altération des registres de l'automate. Les perspectives s'orientent désormais vers l'intégration d'un **SIEM** centralisé pour corréler les événements de sécurité et durcir la supervision globale.

Conclusion générale

Ce projet de fin d'études a abouti à la conception, la mise en œuvre et la validation d'une plateforme d'expérimentation complète dédiée à la cybersécurité des systèmes de contrôle-commande industriels (ICS). Structurée autour d'un triptyque interconnecté — opérationnel, offensif et défensif —, cette démarche holistique a permis d'appréhender à 360 degrés les vecteurs de vulnérabilité et les impératifs de résilience propres aux technologies opérationnelles (OT) modernes.

Sur le plan opérationnel, l'environnement de simulation développé associe de manière transparente le logiciel d'usine virtuelle Factory I/O et l'automate programmable OpenPLC. Les tests d'intégration ont mis en évidence la stabilité et la robustesse de la logique locale de contrôle-commande. L'exploitation du protocole Modbus TCP/IP s'est avérée fluide et exempte de latence impactante, validant la synchronisation parfaite entre la détection par le capteur optique et l'actionnement instantané du moteur du convoyeur.

Sur le plan offensif, l'implémentation concrète d'une attaque par injection de fausses données (FDIA) par déni de service (inondation de paquets) a mis en exergue la fragilité structurelle des infrastructures industrielles isolées. En submergeant le registre de commande du moteur par des requêtes de forçage d'écriture de bobines (FC5) à une fréquence supérieure à la vitesse de scrutation de l'automate, le script attaquant a réussi à paralyser la routine de sécurité d'OpenPLC. Cet assaut a mis en évidence le lien direct entre une faille numérique et un dommage physique majeur : le maintien en fonctionnement forcé du moteur et le déraillement (chute) du colis.

Sur le plan défensif, la stratégie de remédiation architecturale articulée autour d'un proxy Modbus applicatif s'est avérée pleinement concluante à travers deux niveaux de sécurité :

L'IDS comportemental remplit parfaitement son rôle d'observateur en analysant le trafic sur une fenêtre glissante d'une seconde. Il lève instantanément une alerte dès le franchissement du seuil anormal de 5 requêtes FC5, offrant une visibilité en temps réel à l'opérateur.

L'IPS comportemental apporte une réponse proactive et autonome en interceptant et en éliminant les trames malveillantes en amont de la pile réseau de l'automate. Ce filtrage chirurgical préserve l'intégrité opérationnelle du procédé physique sans dégrader les performances du trafic légitime et sans nécessiter d'arbitrage humain.

En somme, ces travaux mettent en relief un paradigme critique de la cybersécurité industrielle : conçus historiquement à des fins de performance et de disponibilité au détriment de mécanismes d'authentification ou de chiffrement, les protocoles OT natifs tels que Modbus TCP/IP exigent impérativement l'adjonction de dispositifs de protection périmétrique dédiés. La solution logicielle développée — légère, économique et non intrusive — démontre qu'une approche par inspection comportementale est viable et directement transposable à des scénarios industriels réels. Ce mini-laboratoire pose ainsi les fondations d'un environnement d'émulation pérenne, propice à l'audit, à la formation et au durcissement des infrastructures critiques face aux cybermenaces futures.

ANNEXES

1. Annexe A : Script Python de simulation offensive (Attaque FDIA)

Ce script implémente l'outil de sabotage industriel. Il exploite la bibliothèque `pyModbusTCP` pour injecter des requêtes d'écriture de bobines (**Function Code 5**) à haute fréquence vers le registre du moteur, simulant une attaque par injection de fausses données (False Data Injection Attack).

```
import customtkinter as ctk
from pyModbusTCP.client import ModbusClient
import threading
import time

# Configuration globale du style sombre
ctk.set_appearance_mode("dark")
ctk.set_default_color_theme("blue")

class InjectionFDIAApp(ctk.CTk): 1 usage

    def __init__(self):
        super().__init__()

        # Propriétés de la fenêtre principale
        self.title("Module d'Injection FDIA - Test de Sécurité")
        self.geometry("500x500")
        self.configure(fg_color="#1E1E1E") # Fond très sombre / noir

        self.injection_active = False
        self.modbus_client = None

        # 1. Titre Principal
        self.title_label = ctk.CTkLabel(
```

2. Annexe B : Script Python de détection passive (Système IDS)

Ce script configure un système de détection d'intrusions (IDS) basé sur le comportement réseau. Il intercepte le trafic à destination de l'automate, calcule la fréquence des requêtes de forçage applicatif sur une fenêtre glissante d'une seconde, et lève une alerte visuelle rouge sans interrompre le trafic.

```

def __init__(self):
    self.convoyeur_frame,
    text="● CONVOYEUR EN MARCHÉ (NORMAL)",
    font=("Arial", 18, "bold"),
    text_color="#2ECC71" # Vert
    )
    self.convoyeur_status.pack(expand=True)

    # 4. Section Analyse Réseau (IDS)
    self.ids_frame = ctk.CTkFrame(self, fg_color="#202D2D", height=100)
    self.ids_frame.pack(pady=15, padx=40, fill="x")
    self.ids_frame.pack_propagate(False)

    self.ids_title = ctk.CTkLabel(self.ids_frame, text="ANALYSE DU TRAFIC RÉSEAU (IDS)", font=
                                text_color="#AAAAAA")
    self.ids_title.pack(pady=(10, 0))

    self.ids_status = ctk.CTkLabel(
        self.ids_frame,
        text="SÉCURITÉ : TRAFIC SAIN",
        font=("Arial", 18, "bold"),
        text_color="#2ECC71" # Vert
    )
    self.ids_status.pack(expand=True)

```

3. Annexe C : Script Python de prévention active (Système IPS)

Ce script implémente le module de mitigation proactive (IPS). Contrairement à l'IDS, dès que le comportement anormal franchit le seuil critique, le proxy applique une politique restrictive de blocage coupe les sockets de communication de l'attaquant et l'inscrit dans une liste noire de bannissement temporaire, maintenant le processus physique en sécurité complète.

```

0      class MoniteurIPSApp(ctk.CTk): 1 usage
1
2      def __init__(self):
3
4          self.convoyeur_status = ctk.CTkLabel(
5              self.convoyeur_frame,
6              text="● CONVOYEUR EN MARCHÉ (SÉCURISÉ)",
7              font=("Arial", 18, "bold"),
8              text_color="#2ECC71"
9          )
10         self.convoyeur_status.pack(expand=True)
11
12         # 4. Section Système de Prévention (IPS)
13         self.ips_frame = ctk.CTkFrame(self, fg_color="#2D2D2D", height=100)
14         self.ips_frame.pack(pady=15, padx=40, fill="x")
15         self.ips_frame.pack_propagate(False)
16
17         self.ips_title = ctk.CTkLabel(self.ips_frame, text="PARE-FEU DE BLOCAGE",
18                                     text_color="#AAAAAA")
19         self.ips_title.pack(pady=(10, 0))
20
21         self.ips_status = ctk.CTkLabel(
22             self.ips_frame,
23             text="PARE-FEU : ACTIF (0 BLOCAGES)",
24             font=("Arial", 18, "bold"),

```

Bibliographie

- [1] [IP Systèmes](#) : « Qu'est-ce qu'un automate programmable industriel ? », consulté le 26/04/2026.
- [2] [Fortinet](#) : « Qu'est-ce que la cybersécurité ? ». ([Fortinet](#))
- [3] [ChamberSign France](#) : « La triade CIA ».
- [4] [Zscaler](#) : « What is Purdue Model ICS Security ».
- [5] [Tulip](#) : « IT vs OT : différence entre les technologies de l'information et les technologies opérationnelles ».
- [6] [Selceon](#) : « IT : définition des technologies de l'information ».
- [7] [ServiceNow](#) : « OT vs IT ».
- [8] [Fortinet Defense in Depth](#) : « Defense in Depth ».
- [9] KAHHOUL, Z., SARHANI : *Configuration, Interfaçage et Surveillance de DCS et RTU Schneider Saitel DP (SCADA) Utilisant le Logiciel Easergy Builder*, Mémoire de Master en Automatique et Informatique Industrielle, Département de Génie Électrique, Faculté des Sciences et de la Technologie, Université Mohamed Khider de Biskra, année universitaire 2019-2020, disponible sur [Archives Univ Biskra](#).
- [10] LAOUN, A., LOUBER, N. A. : *Étude et Simulation d'un Système SCADA au niveau de la Station ONA d'Ain Sefra*, Mémoire de Master en Maintenance, Fiabilité et Qualité, Département de Maintenance en Électromécanique, Université Oran 2 Mohamed Ben Ahmed, année universitaire 2020-2021. disponible sur [DS Univ Oran2](#).
- [11] BOUNAB, Z. : *Étude d'un système de supervision et de contrôle SCADA de la région de transport Est RTE Skikda*, Mémoire de Master en Automatique Avancée, Département de Génie Électrique, Faculté des Sciences et de la Technologie, Université Mohamed Khider de Biskra, année universitaire 2013-2014, disponible sur [Mémoire Biskra PDF](#).
- [12] FELIDJ, A. : *L'étude d'un système instrumenté de sécurité au niveau du complexe GPI/Z*, Mémoire de Master en Prévention et Intervention, Filière Hygiène et Sécurité Industrielle, Département de Sécurité Industrielle et Environnement, Institut de Maintenance et de Sécurité Industrielle, juin 2019. disponible sur [Mémoire ASMA FELIDJ](#).

- [13] SHAKYA, S. R., JHA, S. : « *Introduction to Industrial Internet of Things (IIoT) – toward the future internet* », dans *Quality Assessment and Security in Industrial Internet of Things*, Routledge Taylor & Francis Group, octobre 2024, pp. 1-19. disponible sur [ResearchGate IIoT](#).
- [14] Google Images : « CHEME RTU », disponible sur [Google Images CHEME RTU](#).
- [15] Google Images : illustration du modèle Purdue, disponible sur [Google Images Purdue](#).
- [16] Google Images : illustration IT/OT, disponible sur [Google Images IT OT](#)..
- [17] Google Images : « Open PLC », disponible sur [Google Images Open PLC](#).
- [18] Technologue Pro. *Introduction aux systèmes de contrôle industriel (ICS) et solutions d'automatisation*.
- [19] Schneider Electric. *Le rôle des Automates Programmables Industriels (PLC) au sein des architectures ICS*.
- [20] GHERBI, H. (2018). *Modélisation et sécurisation des architectures de réseaux industriels contre les cyberattaques*. Mémoire académique, Université d'Annaba.
- [21] Automation Sense. *Architecture interne, traitement des données et cycles d'exécution d'un PLC*.
- [22] Instrumentation Actu. *Topologies des réseaux de communication et modes d'échange des systèmes SCADA*.
- [23] INERIS. *Structure, composants et exigences de sécurité des Systèmes Instrumentés de Sécurité (SIS)*.
- [24] Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN). *Guide des bonnes pratiques de sécurité pour la triade C.I.A.*
- [25] NetBeOpen. *Qu'est-ce que l'Operational Technology (OT) et ses spécificités face à l'IT ?*
- [26] ANSSI. *Guide de la cybersécurité des systèmes industriels et application de la défense en profondeur*