REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département de Génie Electrotechnique et Automatique

Réf: ..... /2024

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**
AcadémiqueDomaine : Sciences et Technologie

Filière : Automatique
Spécialité : Automatique et Informatique industrielle

Par :

BOUDRA Fares Abdelbasset **RAMDANI Khayreddine**

Thème

Cybersécurité des systèmes de contrôle industriel grâce à des systèmes de détection et de prévention des intrusions

Soutenu publiquement, le 28/10/2024, devant le jury composé de :

Mme. KECHIDA Sihem	Professeur	Univ. Guelma	Présidente/ Examinatrice
M. **MOUSSAOUI Abdelkrim**	Professeur	Univ. Guelma	Encadrant
M. GRIOUZ Badreddine	MCB	Univ. Guelma	Examinateur
M. BENKIRAT Abdelaziz	MAA	Univ. Guelma	Examinateur
M. MADI Sami	Ingénieur	Algérie Télécom	Examinateur

Année Universitaire : 2023/2024


بسم الله الرحمن الرحيم

RESUME

L'intégration croissante des systèmes de contrôle industriel (ICS) au sein des infrastructures critiques a accru le besoin de solutions de cybersécurité robustes, car ces systèmes sont essentiels à la gestion des processus industriels dans des secteurs tels que l'énergie, la fabrication et le transport. Ce Mémoire étudie les défis de cybersécurité spécifiques aux ICS et à la technologie opérationnelle (OT), en se concentrant sur la manière dont les systèmes de détection et de prévention des intrusions (IDS/IPS) de nouvelle génération peuvent améliorer la posture de sécurité de ces systèmes critiques.

L'objectif principal de ce mémoire est d'explorer les techniques avancées de segmentation du réseau, la surveillance du trafic réseau en temps réel et la mise en œuvre d'une solution de tableau de bord spécialisée appelée « THE PROTECTOR ». Cette plate-forme offre une visualisation et une gestion complètes des alertes de sécurité, adaptées aux besoins uniques des environnements ICS. Grâce à une analyse détaillée du déploiement des IDS/IPS au sein des infrastructures critiques, la recherche présente à la fois des perspectives théoriques et des applications pratiques, en mettant l'accent sur la protection des actifs clés contre les cybermenaces sophistiquées.

Le mémoire porte également sur le développement et la personnalisation des contrôles de sécurité pour les environnements ICS, conformément au cadre de gestion des risques du NIST (RMF). Ce cadre s'applique spécifiquement aux systèmes OT, répondant aux défis uniques de la disponibilité, des opérations en temps réel et de la tolérance au risque dans les environnements industriels.

En présentant une combinaison d'outils et de méthodologies innovants, ce travail contribue au développement de solutions de cybersécurité de nouvelle génération qui non seulement détectent et préviennent les intrusions, mais fournissent également des renseignements exploitables pour l'atténuation des risques dans les systèmes ICS/OT.

ABSTRACT

The increasing integration of industrial control systems (ICS) within critical infrastructures has increased the need for robust cybersecurity solutions, as these systems are essential to the management of industrial processes in sectors such as energy, manufacturing, and transportation. This thesis explores the cybersecurity challenges specific to ICS and operational technology (OT), focusing on how next-generation intrusion detection and prevention systems (IDS/IPS) can improve the security posture of these critical systems.

The main objective of this Master thesis is to explore advanced network segmentation techniques, real-time network traffic monitoring, and the implementation of a specialized dashboard solution called “THE PROTECTOR”. This platform provides comprehensive visualization and management of security alerts, tailored to the unique needs of ICS environments. Through a detailed analysis of IDS/IPS deployment within critical infrastructures, the research presents both theoretical perspectives and practical applications, with a focus on protecting key assets from sophisticated cyber threats.

The thesis also addresses the development and customization of security controls for ICS environments, in line with the NIST Risk Management Framework (RMF). This framework is specifically applicable to OT systems, addressing the unique challenges of availability, real-time operations, and risk tolerance in industrial environments.

By presenting a combination of innovative tools and methodologies, this work contributes to the development of next-generation cybersecurity solutions that not only detect and prevent intrusions but also provide actionable intelligence for risk mitigation in ICS/OT systems.

ملخص

أدى التكامل المتزايد لأنظمة التحكم الصناعية (ICS) ضمن البنية التحتية الحيوية إلى زيادة الحاجة إلى حلول قوية للأمن السيبراني، حيث أن هذه الأنظمة ضرورية لإدارة العمليات الصناعية في قطاعات مثل الطاقة والتصنيع والنقل. تستكشف هذه المذكرة تحديات الأمن السيبراني الخاصة بـ ICS والتكنولوجيا التشغيلية (OT)، مع التركيز على كيف يمكن للجيل الجديد من أنظمة كشف التسلل والوقاية (IDS/IPS) تحسين الوضع الأمني لهذه الأنظمة الحيوية.

الهدف الرئيسي من مذكرة الماستر هذه هو استكشاف تقنيات تجزئة الشبكة المتقدمة ومراقبة حركة مرور الشبكة في الوقت الفعلي وتنفيذ حل يتمثل في لوحة تحكم متخصصة تسمى "THE PROTECTOR". توفر هذه المنصة تصورًا شاملاً وإدارة التنبيهات الأمنية، المصممة خصيصًا لتلبية الاحتياجات الفريدة لبيئات ICS. ومن خلال التحليل التفصيلي لنشر IDS/IPS داخل البنى التحتية الحيوية، يقدم البحث رؤى نظرية وتطبيقات عملية، مع التركيز على حماية الأصول الرئيسية ضد التهديدات السيبرانية المتطورة.

وتغطي المذكرة أيضًا تطوير وتخصيص الضوابط الأمنية لبيئات ICS، بما يتوافق مع إطار إدارة المخاطر NIST (RMF). وينطبق هذا الإطار بشكل خاص على أنظمة التكنولوجيا التشغيلية، حيث يعالج التحديات الفريدة المتمثلة في التوفر والعمليات في الوقت الفعلي وتحمل المخاطر في البيئات الصناعية.

ومن خلال تقديم مجموعة من الأدوات والمنهجيات المبتكرة، يساهم هذا العمل في تطوير حلول الأمن السيبراني من الجيل التالي التي لا تكتشف عمليات التطفل وتمنعها فحسب، بل توفر أيضًا معلومات استخبارية قابلة للتنفيذ لتخفيف المخاطر في أنظمة ICS/التكنولوجيا التشغيلية.

REMERCIEMENTS

« Il faut trois conditions pour faire le thé : le temps, les braises et les amis. »
(Proverbe touareg)

Comme dans ce proverbe, ce mémoire a nécessité du temps, de l'énergie, et surtout le soutien de nombreuses personnes sans qui ce projet n'aurait pu aboutir. Ainsi, nous tenons à exprimer notre profonde gratitude à **Pr. MOUSSAOUI Abdelkrim**, pour la qualité de son encadrement tout au long de ce travail. Sa confiance en notre capacité à mener à bien ce projet et ses précieux conseils ont été d'une immense aide. Il a su allier génie, optimisme et bienveillance, et nous a apporté autant sur le plan professionnel que personnel.

Nous souhaitons exprimer nos sincères remerciements à **M. BENKIRAT Abdelaziz**, directeur de **l'incubateur de l'université 8 Mai 1945**, pour son soutien précieux et son accompagnement tout au long de notre parcours entrepreneurial. Grâce à sa vision et à ses conseils, nous avons pu concrétiser nos projets avec succès. Nous lui en sommes profondément reconnaissants.

Nous remercions chaleureusement les membres de jurys pour l'honneur qu'ils nous ont fait en acceptent d'évaluer notre projet.

Nous tenons à remercier **BOUSSAHA Abderrahmen**, notre camarade, pour son engagement et son esprit de collaboration. Travailler ensemble sur ce projet a été une expérience enrichissante.

Nous tenons également à exprimer notre gratitude à **nos familles**, qui ont toujours su nous soutenir dans les moments les plus exigeants. Leur amour, leur patience, et leurs encouragements inconditionnels ont été essentiels à notre réussite.

Enfin, un grand merci à **nos amis** et proches pour leur soutien moral et leurs précieux encouragements tout au long de cette période. Leur présence a apporté une motivation supplémentaire qui a fait la différence.

Ce travail est le fruit d'un effort collectif, et chacun de vous a contribué, d'une manière ou d'une autre, à ce succès. Nous vous en sommes profondément reconnaissants.

Fares Abdelbasset BOUDRA
Khayreddine RAMDANI

ABRÉVIATIONS ET ACRONYMES

800-82-r2, "Guide to Industrial Control System (ICS) Security" International guidelines for implementing cybersecurity in Industrial Control Systems.

800-61-r2, "Computer Security Incident Handling Guide" A NIST Special Publication designed to guide organizations in the process of incident response using a four-phase lifecycle approach.

800-115, "Technical Guide to Information Security Testing and Assessment" A NIST Special Publication designed to assist organizations in planning and conducting penetration tests, analyzing findings, and developing mitigation strategies.

800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" A NIST Special Publication designed to guide organizations in their efforts to conduct continuous security monitoring operations.

800-161, "Supply Chain Risk Management Practices for Federal Information Systems and-Organizations" A NIST Special Publication designed to guide organizations in their efforts to identify, assess, and mitigate their IT/OT supply chain risks.

Abréviations et Acronymes sélectionnés utilisés dans cet ouvrage :

ACL	Access Control List
ARP	Address Resolution Protocol
CIP	Critical Infrastructure Protection
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSRC	Computer Security Resource Center
CSSC	Control System Security Center
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control System(s)
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNP3	DNP3 Distributed Network Protocol (published as IEEE 1815)
DNS	Domain Name System
DoS	Denial of Service
DRP	Disaster Recovery Plan
EAP	Extensible Authentication Protocol
EMS	Energy Management System
EPRI	Electric Power Research Institute
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GPS	Global Positioning System

HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
I/O	Input/Output
I3P	Institute for Information Infrastructure Protection
IACS	Industrial Automation and Control System
IAONA	Industrial Automation Open Networking Association
ICCP	Inter-control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control System(s)
ICS-CERT	Industrial Control Systems - Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISA	International Society of Automation
ISID	Industrial Security Incident Database
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
MAC	Media Access Control
MES	Manufacturing Execution System
MIB	Management Information Base
MTU	Master Terminal Unit (also Master Telemetry Unit)
NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NCSD	National Cyber Security Division
NFS	Network File System
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSTB	National SCADA Testbed
OLE	Object Linking and Embedding
OMB	Office of Management and Budget
OPC	OLE for Process Control
OS	Operating System
OSI	Open Systems Interconnection
PCII	Protected Critical Infrastructure Information
PIN	Personal Identification Number

PID	Proportional – Integral - Derivative
PIV	Personal Identity Verification
PLC	Programmable Logic Controller
PP	Protection Profile
PPP	Point-to-Point Protocol
R&D	Research and Development
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
RMA	Reliability, Maintainability, and Availability
RMF	Risk Management Framework
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTU	Remote Terminal Unit (also Remote Telemetry Unit)
SC	Security Category
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SPP-ICS	System Protection Profile for Industrial Control Systems
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

TABLE DES ILLUSTRATIONS

LISTE DES FIGURES :

Chapitre 1

Figure 1 : Les 16 secteurs d'infrastructures critiques 7

Chapitre 2

Figure 2. 1 : Architecture typique d'un ICS (Bai & Liu, 2023) 14
Figure 2. 2 : Unité terminale (RTU) et PLC (Mondi Anderson, 2018) 15
Figure 2. 3 : Composants d'un PLC (Schweber, 2019) 16
Figure 2. 4 : Diagramme de communication dans un PLC (LadderLW, s.d.) 16
Figure 2. 5 : Architecture d'un DCS 20
Figure 2. 6 : Architecture SCADA de première génération 21
Figure 2. 7 : Architecture SCADA de deuxième génération 21
Figure 2. 8 : Architecture SCADA de troisième génération 22
Figure 2. 9 : Architecture SCADA de quatrième génération (SCADA / IOT) 23
Figure 2. 10 : Structure du type d'informations du champ de controle 24
Figure 2. 11 : IEC 60870-5-104 APDU & ASDU 24
Figure 2. 12 : Groupes de types de codes 25
Figure 2. 13 : Architecture maître/esclave DNP3 (Ortega, 2013) 25
Figure 2. 14 : ENCAPSULATION DE DNP3 SUR TCP/IP (Ortega, 2013) 26
Figure 2. 15 : Trame de liaison de données DNP3 27
Figure 2. 16 : Modbus Client/Server communication model 27
Figure 2. 17 : Modbus RTU Client/Server communication model (General Industrial Automation, 2021) 28
Figure 2. 18 : Architecture de communication MODBUS TCP/IP (General Industrial Automation, 2021) 28
Figure 2. 19 : Trame de messagerie Modbus TCP/IP vs RTU 29
Figure 2. 20 : Modèle OSI pour Modbus TCP (General Industrial Automation, 2021) 29
Figure 2. 21 : Interrelations entre les normes IEC TC57 et IEC 62351 (Ersan Kabalci, 2019) 33

Chapitre 3

Figure 3. 1 : MODELE DE PURDUE DE L'ARCHITECTURE D'UN ICS (Wainstein, 2024) 41
Figure 3. 2 : Convergence IT-OT 42
Figure 3. 3 : Taxonomie des attaques des ICSs 44
Figure 3. 4 : Chronologie des cyberattaques impactant les entreprises industrielles 46
Figure 3. 5 : Priorités de la triade de la CIA 47
Figure 3. 6 : Architecture pour la detection et supervision (BOOZ ALLEN HAMILTON INC, 2020) 54

Chapitre 4

Figure 4. 1 : Processus de gestion des risques : encadrer, évaluer, réagir et surveiller..... 59
Figure 4. 2 : Niveaux de gestion des risques : organisation, mission et processus opérationnels, et système (Keith, Michael, & CheeYee, 2023) 60
Figure 4. 3 : Etapes du cadre de gestion des risques 65

Chapitre 5

Figure 5. 1 : Architecture de l'application "THE PROTECTOR"..... 80
Figure 5. 2 : Tableau de bord (dashboard) en mode sombre..... 82
Figure 5. 3 : En mode claire 82
Figure 5. 4 : Tableau des alertes..... 83
Figure 5. 5 : Tableau des évènements 84
Figure 5. 6 : Installation de la solution THE PROTECTOR au niveau 3 85
Figure 5. 7 : Simulation..... 88
Figure 5. 8 : SCADABR (HMI) 89
Figure 5. 9 : Workstation..... 89
Figure 5. 10 : Logiciel OPENPLC dans la machine Workstation..... 90
Figure 5. 11 : Utilisation d'arp-scan 91
Figure 5. 12 : Première analyse avec Wireshark..... 91
Figure 5. 13 : Vue de SCADABR (HMI)..... 92
Figure 5. 14 : Le filtrage des résultats de scan Wireshark 93
Figure 5. 15 : La lecture de la valeur d'adresse 40 93
Figure 5. 16 : L'écriture de la valeur "1" dans l'adresse 40..... 93
Figure 5. 17 : La chute de plus de 1000 kPa en moins d'une minute 94
Figure 5. 18 : Réussite de l'attaque..... 94
Figure 5. 19 : Affichage de l'alerte..... 95
Figure 5. 20 : Affichage de l'alerte..... 95

Annexe A

Figure A 1 : Types des IDS..... 108
Figure A 2 : Installation de l’IPS en série 108
Figure A 3 : Types des IPS..... 109
Figure A 4 : Configurations correctes et incorrectes, ainsi que des exemples de conduits.... 113
Figure A 5 : Conduits (basé sur IEC documentation) 114
Figure A 6 : Traffics normal et trafics avec NGFW..... 116
Figure A 7 : Architecture Zero-Trust Securite dans les ICS/OT..... 117

Annexe B

Figure B 1 : Architecture de base du systèmes de contrôle..... 121
Figure B 2 : Architecture de sécurité avec IDS..... 123
Figure B 3 : Architecture de sécurité avec IPS 124
Figure B 4 : Architecture de sécurité avec SIEM..... 125
Figure B 5 : Architecture de sécurité avec IDS/IPS, SIEM 126

LISTE DES TABLEAUX :

Chapitre 2

Tableau 2. 1 : Différence entre MODBUS RTU et MODBUS TCP (General Industrial Automation, 2021) 29
Tableau 2. 2 : Différence entre DNP3 et Modbus 34

Liste des figures :

Chapitre 3

Tableau 3. 1 : Les différents niveaux du modèle Purdue 39

Chapitre 4

Tableau 4. 1 : Définition possible des niveaux d'impact pour les systèmes OT en fonction du produit, de l'industrie, et des préoccupations de sécurité (Keith, Michael, & CheeYee, 2023) 61
Tableau 4. 2 : Évaluation de la probabilité d'occurrence d'un évènement (Keith, Michael, & CheeYee, 2023) 62
Tableau 4. 3 : Catégories de composants de contrôle non numériques pour les OT 63
Tableau 4. 4 : Application de l'étape de préparation du RMF à l'OT (Keith, Michael, & CheeYee, 2023) 66
Tableau 4. 5 : Application de l'étape de catégorisation RMF à l'OT (Keith, Michael, & CheeYee, 2023) 70
Tableau 4. 6 : Application de l'étape évaluer du RMF aux systèmes OT 71
Tableau 4. 7 : Application de l'étape autoriser du RMF aux systèmes OT 73
Tableau 4. 8 : Application de l'étape surveiller du RMF aux systèmes OT 74

Annexe A

Tableau A 1 : Différence entre IDS et IPS 109
Tableau A 2 : Les points clés entre la segmentation et la micro-segmentation 114
Tableau A 3 : Bonnes pratiques pour mettre en œuvre la micro-segmentation 115

Annexe B

Tableau B 1 : Différence entre Snort et Suricata dans les ICS 129

SOMMAIRE

Résumé III
Abstract IV
Remerciements VI
Abréviations et acronymes VII
Table des illustrations X
Liste des figures : X
Liste des tableaux : XII

Chapitre 1 Introduction 6
1.1. Aperçu sur les infrastructures critiques (CI) 6
1.2. Aperçu des différents types d'infrastructures critiques en Algérie 7
1.3. Contexte et enjeux 9
1.3.1 Importance de la cybersécurité pour les infrastructures critiques 9
1.3.2 Les menaces spécifiques aux systèmes de contrôle industriels (ICS) 10
1.4 Problématique 10
1.4.1 Vulnérabilités dans les systèmes industriels et leur exposition croissante aux cyberattaques 10
1.4.2 Les IDS/IPS de nouvelle génération sont une réponse nécessaire 10
1.5 Objectifs du mémoire 10
1.6 Méthodologie 11
Chapitre 2 La technologie utilisée dans les systèmes de contrôle industriels (ics) et scada 13
2.1 Architecture des Systèmes de Contrôle Industriel 13
2.1.1 Composants Principaux 13
2.1.2 Types de Systèmes 13
2.1.3 Interfaces 13
2.1.4 Évolution Technologique 13
2.1.5 Exigences Spécifiques 13
2.2 Architecture Générale des Automates Programmables Industriels (PLC) 14
2.2.1 Composants Principaux des PLC 14
2.2.2 Structure Modulaire des PLC 15
2.2.3 Communication Interne 16
2.3 Fonctionnalités Clés des PLC 17
2.4 Architecture des Systèmes de Contrôle Distribués (DCS) 17
2.4.1 Composants Principaux des DCS 18

2.4.2 Structure Hiérarchique d'un DCS 18
2.4.3 Redondance et Fiabilité 19
2.4.4 Modularité et Scalabilité 19
2.4.5 Exigences Spécifiques des DCS 19
2.5 Architecture SCADA 20
2.5.1 Première génération – Systèmes SCADA monolithiques 21
2.5.2 Deuxième génération – Systèmes SCADA distribués 21
2.5.3 Systèmes SCADA en réseau (Troisième génération) 22
2.5.4 Quatrième génération – Systèmes SCADA basés sur l'Internet des objets (IoT) 22
2.6 Protocoles de communication SCADA 23
2.6.1 IEC 60870-5-104 23
2.6.2 DNP3 25
2.6.3 Modbus 27
2.7 Vulnérabilités et Problèmes de sécurité dans les protocoles 31
2.7.1 IEC 60870-5-104 32
2.7.2 DNP3 32
2.7.3 Modbus TCP 32
2.7.4 IEC 62351 33
2.7.5 Différence entre DNP3 et Modbus 34
2.8 Sécurité des ICS/SCADA 34
2.8.1 Vulnérabilités des systèmes SCADA 35
Chapitre 3 Cybersécurité des Systèmes de contrôle industriel (ICSs) : spécificités, enjeux et défis associés 38
3.1 Systèmes de contrôle industriels (ICS) et cyberattaques 38
3.1.1 Introduction 38
3.1.2 Systèmes de contrôle industriels (ICSs) 38
3.1.3 ICS/OT et défis de sécurité 41
3.2 Vecteurs d'Attaque dans les Environnements ICS/OT 43
3.2.1 Techniques d'Attaque Courantes : 43
3.2.2 Cybers incidents survenus aux systèmes SCADA 45
3.3 La sécurité des technologies opérationnelles (OT) est différente de celle des technologies de l'information (IT) 47
3.3.1 Principales mesures de cybersécurité 48
3.3.2 Sécurité opérationnelle OPSEC (OPerationnelle SEC-urity) 50
3.3.3 Établir un programme de détection et de réponse aux menaces ICS/OT 51
Chapitre 4 GESTION DES RISQUES POUR LES SYSTEMES ICS/OT 58

4.1 Gestion de la sécurité ICS/OT 58
4.1.1 Encadrement des risques liés aux OT 60
4.1.2 Évaluation des risques dans un environnement OT 62
4.1.3 Réponse au risque dans un environnement OT 64
4.1.4 Surveillance du risque dans un environnement OT 64
4.2 Domaines particuliers à prendre en compte 64
4.2.1. Gestion des risques de la chaîne d'approvisionnement 64
4.2.2. Systèmes de sécurité 64
4.3 Application du Cadre de Gestion des Risques aux Systèmes OT 65
4.3.1 Préparation 66
4.3.2 Catégorisation 69
4.3.3 Sélection 70
4.3.4 Implémentation 71
4.3.5 Évaluation 71
4.3.6 Autorisation 73
4.3.7 Surveillance 74
Chapitre 5 ..... THE PROTECTOR : Application de surveillance, détection et prévention des intrusions 77
5.1 Introduction 77
5.2 Objectifs du Projet 77
5.3 Périmètre Fonctionnel 78
5.4 Exigences Techniques et Technologies Utilisées 79
5.5 Avantages de l'interface web "THE PROTECTOR v.1" : 81
5.5.1 Une Accessibilité Totale et Compatibilité avec "THE PROTECTOR" 81
5.5.2 Visualisation des Données de Sécurité Simplifiée et Personnalisée pour une Analyse Efficace 81
5.5.3 Intégration Transparente et Collaboration Renforcée pour une Synergie Sécuritaire Totale 83
5.5.4 Gestion Centralisée et Évolutivité Illimitée pour les Entreprises de Toutes Tailles 83
5.6 Test et scénarios d'application 87
5.6.1 Présentation du Lab GRFICS 87
5.6.2 Objectifs du Test 90
5.6.3 Méthodologie 90
5.6.4 Arrêt du processus 90
5.6.5 Résultats Attendus 94
5.6.6 Conclusion 95
Conclusion Générale 97

Bibliographie 98
Annexe A ..... Segmentation Réseau et Rôle des IDS/IPS dans la Cybersécurité des ICS 106
A.1 Introduction 106
A.1.1 Aperçu sur la Segmentation Réseau 106
A.1.2 Importance de la Segmentation Réseau dans les ICS 106
A.2 Rôle des IDS/IPS dans les ICS 107
A.2.1 Présentation de l'IDS (Système de Détection d'Intrusion) 107
A.2.2 Présentation de l'IPS (Système de Prévention d'Intrusion) 108
A.2.3 Différences entre IDS et IPS 109
A.2.4 Défis de l'Utilisation des IDS/IPS dans les ICS 110
A.3 Stratégies de Segmentation Réseau dans les Systèmes de Contrôle Industriels (ICS) 110
A.3.1 Modèles de Segmentation 110
A.3.2 Segmentation et Zones de Sécurité dans les ICS 111
A.3.3 La segmentation du réseau ICS/OT, pourquoi est-ce important ? 111
A.3.4 Comment les réseaux ICS/OT doivent-ils être segmentés ? 112
A.4 Architecture ZERO-TRUST dans les ICS 116
Annexe B ..... Conception et configuration d'IDS/IPS dans les systèmes de contrôle industriel 120
B.1 Architecture de Base du Système de Contrôle 120
B.2 Architectures de sécurité pour les systèmes de contrôle 120
b.3 Outils de Détection d'Intrusions Efficaces pour les Systèmes ICS 127
B.3.1 Snort : 127
B.3.2 Suricata : 127
B.3.3 OSSEC 127
B.3.4 Zeek (anciennement Bro) 127
B.3.5 Systèmes de Détection d'Intrusions Basés sur l'Apprentissage Automatique 127
B.4 SNORT vs SURICATA 128
B.4.1 Snort 128
B.4.2 Suricata 128

CHAPITRE 1
INTRODUCTION

CHAPITRE 1 INTRODUCTION

1.1. APERÇU SUR LES INFRASTRUCTURES CRITIQUES (CI)

Le terme "infrastructure critique" désigne l'ensemble des systèmes, réseaux et ouvrages publics qu'un gouvernement considère comme essentiels au bon fonctionnement et à la sécurité de ses citoyens. Ces infrastructures englobent généralement les transports, les systèmes de communications, les services bancaires et financiers, les réseaux électriques, l'approvisionnement en eau et les services publics. Une attention particulière doit être accordée à la protection des infrastructures critiques. Assurer la protection de ces infrastructures critiques contre les cyberattaques est crucial pour garantir la continuité des services essentiels et le bien-être du pays. (Wright, 2023)

Les infrastructures critiques peuvent être classées dans différents secteurs, selon le pays ou la région. Par exemple, le gouvernement fédéral canadien identifie dix secteurs d'infrastructure critique, notamment l'énergie et les services publics, les technologies de l'information et de la communication, la finance, la santé, l'alimentation, l'eau, les transports, la sécurité, le gouvernement et la fabrication. En revanche, le Programme européen pour la protection des infrastructures critiques (EPCIP) fait référence à la doctrine ou aux programmes spécifiques créés pour la protection de l'énergie, des transports et de la navigation, de la banque et de la finance, de l'industrie chimique et des matières dangereuses, des postes, des monuments et icônes nationaux, de la fabrication critique et des services d'urgence.

Le Plan national de protection des infrastructures (NIPP) des États-Unis définit les secteurs d'infrastructure critique comme étant la chimie, les installations commerciales, les communications, la fabrication critique, les barrages, la base industrielle de défense, les services d'urgence, l'énergie, les services financiers, l'alimentation et l'agriculture, les installations gouvernementales, les soins de santé et la santé publique, les technologies de l'information, les réacteurs nucléaires, les matériaux et les déchets, les systèmes de transport et les systèmes d'eau et d'assainissement.

La protection des infrastructures critiques implique diverses mesures, notamment la sécurité physique, la cybersécurité, l'évaluation des risques, la planification de la réponse en cas d'urgence et les partenariats public-privé. Le Département de la sécurité intérieure des États-Unis (DHS) a mis en place le Centre national d'intégration de la cybersécurité et des communications (NCCIC) pour renforcer la protection des infrastructures critiques et la cybersécurité. (Moteff, 2015, June 10) (Critical infrastructure, 2023).

La protection des infrastructures critiques est un domaine complexe et en constante évolution, avec divers défis et risques, notamment les catastrophes naturelles, les erreurs humaines, les cyber-attaques et les menaces terroristes.

La protection des infrastructures critiques nécessite une approche globale et coordonnée, impliquant divers acteurs, notamment les agences gouvernementales, les entités du secteur privé et le public.

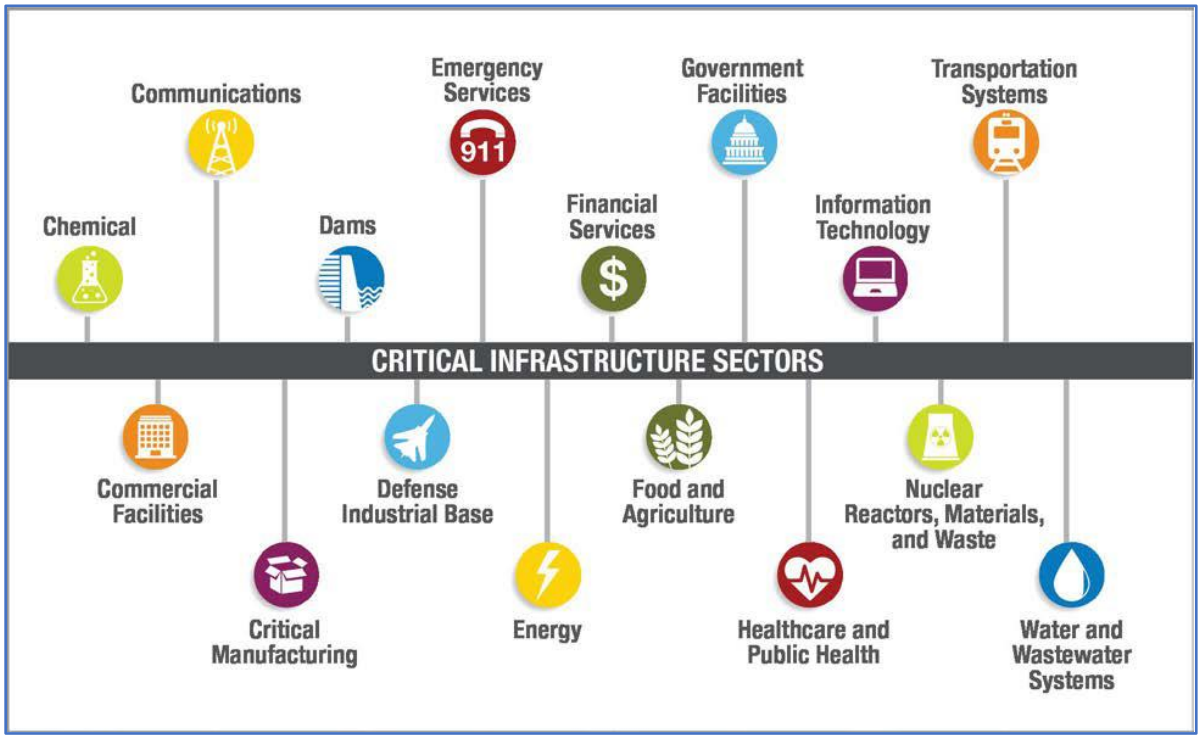


FIGURE 1 : Les 16 secteurs d'infrastructures critiques

1.2. APERÇU DES DIFFERENTS TYPES D'INFRASTRUCTURES CRITIQUES EN ALGERIE

Les infrastructures en Algérie englobent divers secteurs et domaines qui représentent l'axe de développement et de fonctionnement de l'écosystème du pays. Ces secteurs comprennent :

Infrastructure de transport : L'Algérie se concentre sur la modernisation de ses infrastructures de transport, notamment les systèmes ferroviaires, les routes, les aéroports et les ports. Le pays investit de manière significative dans des projets tels que l'autoroute transsaharienne et l'expansion de son réseau ferroviaire (Algeria - Safety and Security, s.d.) (Dumouza, 2018).

Secteur de l'énergie : Le secteur énergétique algérien, dirigé par des entreprises publiques comme Sonatrach et Sonelgaz, joue un rôle vital dans l'économie du pays. Les investissements dans de nouvelles centrales énergétiques, des logements et des infrastructures font partie d'un plan de 50 milliards de dollars visant à améliorer la production et la distribution d'énergie (Algeria - Safety and Security, s.d.).

Développement du logement : Avec une croissance démographique et une urbanisation rapide, le développement du logement est une priorité clé. Le gouvernement a alloué des fonds substantiels à des projets de logement, visant à répondre à la demande croissante.

Gestion des ressources en eau : L'Algérie investit dans des projets de gestion de l'eau pour répondre à la demande croissante en ressources en eau. Cela comprend l'amélioration de la distribution d'eau potable, le traitement des eaux usées, la construction de barrages et

l'amélioration des systèmes de transfert d'eau (Algeria - Safety and Security, s.d.) (Dumouza, 2018).

Sûreté et sécurité : Le secteur de la sûreté et de la sécurité en Algérie se concentre sur la protection des frontières, des infrastructures critiques telles que les installations pétrolières et gazières, les bâtiments gouvernementaux et sur la mise en œuvre de technologies de cybersurveillance. Le pays dispose d'un budget de défense important et donne la priorité aux solutions de sécurité (Algeria Country Report, 2023).

Infrastructure touristique : L'Algérie investit dans son secteur touristique pour attirer davantage de touristes et améliorer les infrastructures pour soutenir l'industrie. Cela comprend la construction de nouveaux hôtels, l'agrandissement des aéroports et le développement de réseaux de transport pour améliorer les expériences touristiques (Dumouza, 2018).

Construction industrielle : Les investissements dans la construction industrielle, y compris les usines chimiques et pharmaceutiques, les installations de fabrication et les usines de traitement des déchets, font partie des plans de développement de l'Algérie visant à stimuler la croissance industrielle et à diversifier l'économie (Securing Critical Infrastructure: Concerns for Businesses, 2024).

Ces secteurs d'infrastructures critiques sont essentiels à la croissance économique, au développement social et à la résilience globale de l'Algérie face à divers défis et opportunités.

Les infrastructures critiques de l'écosystème algérien comprennent :

1) Installations pétrolières et gazières : L'Algérie dépend fortement des exportations de pétrole et de gaz, ce qui rend les installations liées à leur extraction, leur traitement et leur transport essentielles à l'économie.
2) Pôles de transport : Les aéroports, les ports maritimes et les postes frontaliers servent de points d'entrée et de sortie essentiels pour les marchandises et les personnes, nécessitant une protection contre les menaces potentielles pour la sécurité.
3) Systèmes de surveillance des frontières : Étant donné les vastes frontières de l'Algérie avec les pays voisins tels que le Maroc, la Mauritanie, le Mali, le Niger, la Libye et la Tunisie, les systèmes de surveillance sont essentiels pour surveiller et se protéger contre les activités illégales.
4) Bâtiments gouvernementaux : Les infrastructures protégeant les bâtiments gouvernementaux assurent la continuité des services essentiels et le fonctionnement de l'État.
5) Systèmes de cybersécurité : Avec la numérisation croissante des services et des communications, la cybersécurité est devenue cruciale pour se protéger contre les cybermenaces ciblant les institutions gouvernementales et les infrastructures critiques.
6) Infrastructure énergétique : Outre le pétrole et le gaz, d'autres infrastructures énergétiques telles que les centrales électriques et les réseaux électriques sont essentielles au maintien des opérations industrielles et des services publics.

7) Systèmes d'approvisionnement en eau : Garantir la disponibilité d'eau potable via les systèmes d'approvisionnement en eau est essentiel pour la santé publique et le maintien de la stabilité de la société.
8) Réseaux de communication : Des réseaux de communication robustes, y compris des infrastructures de télécommunications et Internet, sont essentiels pour faciliter le commerce, les interventions d'urgence et la diffusion de l'information.

Selon les résultats, les principales préoccupations en matière de sûreté et de sécurité liées aux infrastructures critiques en Algérie comprennent :

- Surveiller et protéger ses larges frontières avec les pays voisins tels que le Maroc, la Mauritanie, le Mali, le Niger, la Libye et la Tunisie (Algeria - Safety and Security, s.d.).
- Protéger des milliers de kilomètres d'oléoducs et d'installations de gaz naturel dans des zones désertiques isolées (Algeria - Safety and Security, s.d.). Protéger ces actifs énergétiques critiques contre d'éventuelles attaques ou sabotages est une priorité essentielle.
- Protéger les bâtiments gouvernementaux, les infrastructures et les points d'entrée clés tels que les aéroports et les ports (Algeria - Safety and Security, s.d.). Assurer la sûreté et la sécurité de ces installations vitales est crucial.
- Faire face à la menace de cyberattaques et à la nécessité de techniques de cybersurveillance robustes (Algeria - Safety and Security, s.d.). Alors que l'Algérie s'appuie de plus en plus sur les infrastructures numériques, les cyberattaques sont devenues une préoccupation majeure. Cela nécessite une renaissance et un bond en avant dans la cybersécurité pour suivre le rythme de développements dans le domaine.

Dans l'ensemble, les résultats soulignent que l'Algérie est confrontée à un ensemble complexe de défis en matière de sûreté et de sécurité pour protéger ses infrastructures critiques en raison de la nécessité de sécuriser les actifs physiques et numériques sur une vaste zone.

1.3. CONTEXTE ET ENJEUX

1.3.1 Importance de la cybersécurité pour les infrastructures critiques

Les infrastructures critiques (CI) incluent des systèmes essentiels au bon fonctionnement de la société, tels que les réseaux d'énergie, d'eau, de transport, ainsi que les systèmes de santé et financiers. Ces infrastructures reposent sur des systèmes de contrôle industriels (ICS) pour automatiser et superviser des processus vitaux. La cybersécurité de ces systèmes est cruciale, car une cyberattaque pourrait entraîner des répercussions graves sur l'économie, la sécurité publique et la santé.

Avec l'évolution de la connectivité et l'intégration de l'Internet des objets (IoT) dans les environnements industriels, les ICS deviennent de plus en plus vulnérables. Les réseaux historiquement isolés sont désormais accessibles via Internet, créant des vecteurs d'attaques supplémentaires pour les cybercriminels. De plus, les ICS utilisent souvent des technologies obsolètes, peu mises à jour, qui présentent des vulnérabilités connues.

Dans ce contexte, la cybersécurité joue un rôle clé dans la protection de ces systèmes contre des attaques visant à perturber les infrastructures critiques.

1.3.2 Les menaces spécifiques aux systèmes de contrôle industriels (ICS)

Les systèmes de contrôle industriels (ICS) sont exposés et vulnérables à un large éventail de menaces cybernétiques, y compris :

1) Les attaques par ransomware : Ces attaques chiffrent les données critiques des systèmes et exigent une rançon pour restaurer l'accès.
2) Les attaques APT (Advanced Persistent Threat) : Les cyberattaquants ciblent des infrastructures spécifiques et cherchent à rester cachés dans le système pendant une longue période, compromettant les systèmes sans se faire remarquer.
3) Les attaques sur les protocoles industriels : De nombreux ICS utilisent des protocoles de communication spécifiques comme Modbus ou DNP3, qui manquent de mécanismes de sécurité intégrés.

Ces menaces incluent également des attaques de type "Man-in-the-Middle" (MitM) et des attaques par rediffusion, qui permettent aux cybercriminels de manipuler les communications entre les systèmes pour infliger des dommages ou prendre le contrôle des processus industriels.

Les incidents notoires tels que Stuxnet et Triton illustrent à quel point les ICS sont des cibles vulnérables. Ces menaces nécessitent donc des solutions de cybersécurité adaptées à la spécificité des environnements industriels.

1.4 PROBLEMATIQUE

1.4.1 Vulnérabilités dans les systèmes industriels et leur exposition croissante aux cyberattaques

Les ICS souffrent de plusieurs vulnérabilités intrinsèques, notamment l'absence de mécanismes de sécurité intégrés, l'utilisation de logiciels et équipements vieillissants, et la difficulté à mettre à jour les systèmes sans interrompre les processus industriels. Ces systèmes étant traditionnellement isolés, la sécurité n'était pas une priorité lors de leur conception. Cependant, avec la convergence entre les technologies de l'information (IT) et les technologies opérationnelles (OT), les ICS sont de plus en plus interconnectés à des réseaux plus larges, augmentant leur surface d'attaque.

1.4.2 Les IDS/IPS de nouvelle génération sont une réponse nécessaire

Les systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) de nouvelle génération sont essentiels pour pallier ces vulnérabilités. Contrairement aux solutions traditionnelles, les IDS/IPS de nouvelle génération sont capables de détecter des menaces complexes, telles que les comportements anormaux dans les réseaux industriels, et d'intervenir automatiquement pour bloquer les attaques avant qu'elles n'impactent le fonctionnement des ICS. Ces systèmes peuvent analyser des protocoles spécifiques aux ICS, offrir une visibilité en temps réel sur les menaces, et s'adapter à des environnements uniques, ce qui en fait une solution clé pour la cybersécurité des infrastructures critiques.

1.5 OBJECTIFS DU MEMOIRE

Développer une compréhension approfondie de l'intégration des IDS/IPS dans les ICS

L'objectif principal est d'étudier comment les IDS/IPS peuvent être intégrés efficacement dans les infrastructures critiques, en tenant compte des exigences spécifiques des ICS, comme la latence faible, la fiabilité, et la compatibilité avec les protocoles industriels.

Proposer des solutions pour renforcer la sécurité des ICS grâce à ces technologies

Ce mémoire vise à identifier et à tester des solutions pratiques basées sur des IDS/IPS de nouvelle génération pour améliorer la sécurité des systèmes industriels. Cela inclut le déploiement de stratégies de détection proactive, l'analyse de scénarios de menace, et l'évaluation des performances de ces solutions dans des environnements réels ou simulés.

1.6 METHODOLOGIE

Étude des systèmes actuels

- Une analyse des architectures actuelles des ICS et de leurs vulnérabilités.
- Étude des différents protocoles industriels utilisés et de leur impact sur la sécurité.
- Examen des systèmes de défense utilisés aujourd'hui dans les ICS, incluant les systèmes traditionnels de détection et prévention d'intrusions.

Analyse des solutions basées sur IDS/IPS

- Étude approfondie des IDS/IPS de nouvelle génération disponibles sur le marché (ex Suricata, Snort, Zeek).
- Comparaison des fonctionnalités, des performances, et de la capacité à répondre aux besoins spécifiques des ICS.
- Analyse de l'intégration de ces solutions dans les infrastructures critiques, en mettant en avant les défis techniques et les avantages.

Déploiement et simulation d'une architecture sécurisée

- Conception d'une architecture réseau sécurisée intégrant des IDS/IPS de nouvelle génération.
- Mise en place d'une simulation d'attaques pour tester la robustesse des solutions déployées.
- Analyse des résultats en termes d'efficacité de détection, de prévention, et de réduction des faux positifs/négatifs.
- Proposition d'améliorations et d'ajustements pour une meilleure personnalisation des solutions aux besoins spécifiques des ICS.

Ce plan méthodologique assurera une approche complète, allant de la théorie à la pratique, en vue de démontrer l'efficacité des IDS/IPS de nouvelle génération dans la protection des ICS contre les cybermenaces

CHAPITRE 2
LA TECHNOLOGIE UTILISEE DANS LES SYSTEMES DE CONTROLE INDUSTRIEL (ICSS) ET SCADA

CHAPITRE 2 LA TECHNOLOGIE UTILISEE DANS LES SYSTEMES DE CONTROLE INDUSTRIELS (ICS) ET SCADA

2.1 ARCHITECTURE DES SYSTEMES DE CONTROLE INDUSTRIEL

2.1.1 Composants Principaux

- **Système de Traitement de l'Information** : Comprend des postes de travail, des serveurs, des équipements réseau, et des systèmes de stockage. Ces éléments permettent la gestion et l'analyse des données collectées.

- **Équipements Spécifiques** : Inclut les automates programmables (PLC), les unités terminales (RTU), les capteurs, et les actionneurs qui interagissent directement avec le système physique.

Ces dispositifs sont essentiels pour mesurer des grandeurs physiques et contrôler les opérations (Flaus J.-M. , Cybersécurité des systèmes industriels, 2018) (Wikipédia, 2022).

2.1.2 Types de Systèmes

- **Systèmes Centralisés** : Dans ces systèmes, toutes les données sont transmises à une salle de contrôle centrale. Bien que cela offre une vue d'ensemble, il peut être inflexible et difficile à reconfigurer (HARTING Technology Group, 2024).

- **Systèmes Distribués** : Ces systèmes répartissent les fonctions de contrôle à travers plusieurs unités autonomes, permettant une plus grande fiabilité et une gestion décentralisée (HARTING Technology Group, 2024) (TechTarget, 2016).

2.1.3 Interfaces

- **Interfaces Homme-Machine (IHM)** : Permettent aux opérateurs d'interagir avec le système. Cela inclut des dispositifs de contrôle et de surveillance qui facilitent la gestion des processus (Wikipédia, 2022).

- **Systèmes SCADA** : Utilisés pour la supervision et le contrôle à distance, ces systèmes intègrent divers équipements et logiciels pour assurer le bon fonctionnement des installations industrielles (Flaus J.-M. , Cybersécurité des systèmes industriels, 2018) (TechTarget, 2016).

2.1.4 Évolution Technologique

L'architecture des ICS a évolué avec l'avènement de l'Internet des Objets (IoT), intégrant davantage d'équipements non informatiques dans un réseau interconnecté.

Cette convergence entre technologies opérationnelles (OT) et technologies de l'information (IT) pose également des défis en matière de cybersécurité (TechTarget, 2016).

2.1.5 Exigences Spécifiques

Les systèmes de contrôle industriel doivent répondre à des contraintes spécifiques telles que la nécessité d'un traitement en temps réel, la fiabilité, et la sécurité.

Ces exigences sont essentielles pour garantir une opération efficace dans des environnements industriels souvent critiques (Flaus J.-M. , Cybersécurité des systèmes industriels, 2018) (Wikipédia, 2022).

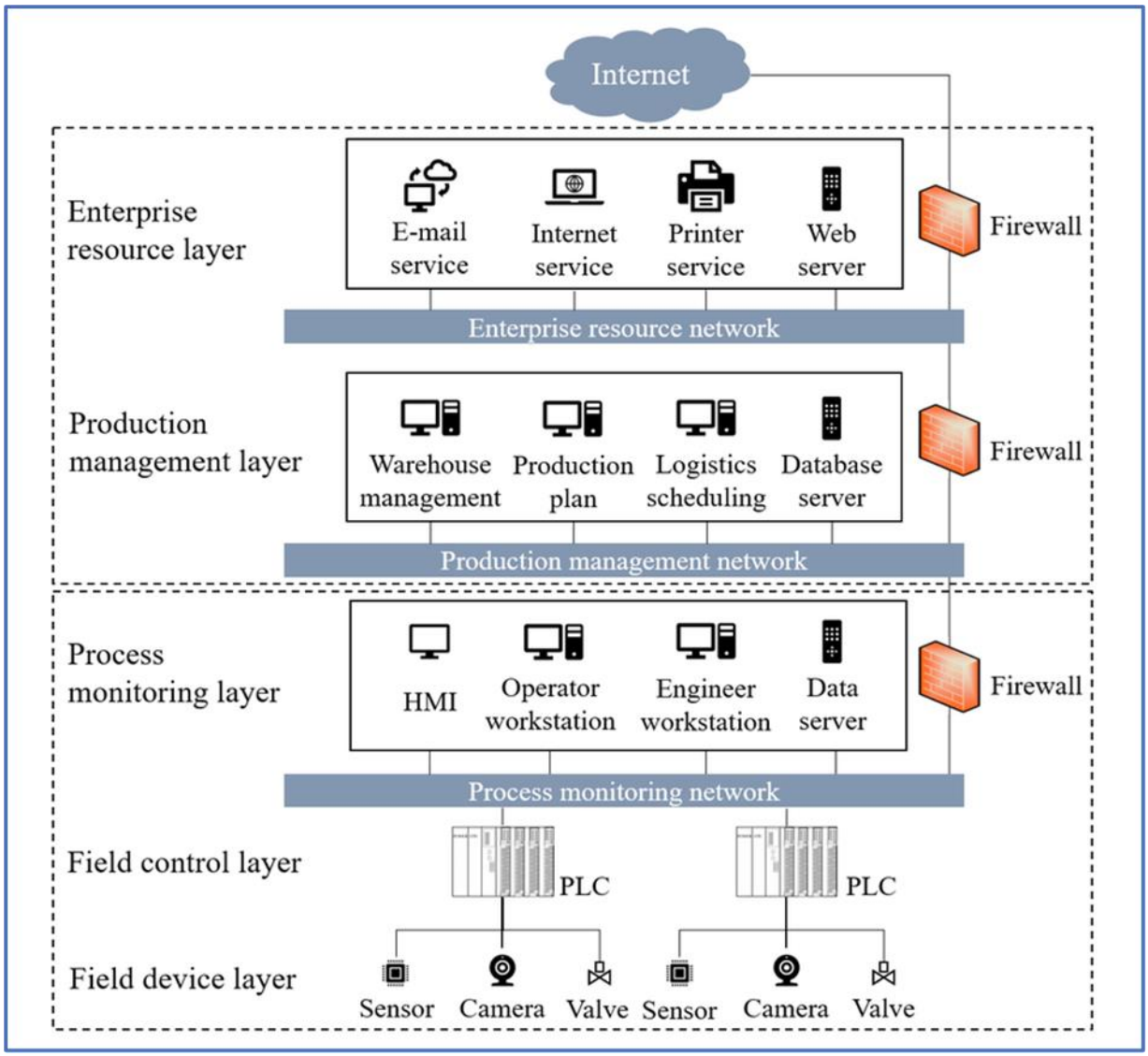


FIGURE 2. 1 : Architecture typique d'un ICS (BAI & LIU, 2023)

2.2 ARCHITECTURE GENERALE DES AUTOMATES PROGRAMMABLES INDUSTRIELS (PLC)

Les automates programmables industriels, ou PLC, sont des dispositifs électroniques spécialisés qui permettent de contrôler et d'automatiser des processus industriels tels que la gestion de machines, des chaînes de production ou des systèmes de sécurité.

Comprendre leur architecture permet de saisir comment ils fonctionnent et comment ils s'intègrent dans les systèmes industriels.

2.2.1 Composants Principaux des PLC

Unité Centrale (UC)

L'unité centrale est le cerveau du PLC. Elle comprend :

Le processeur : Il exécute les programmes logiques qui contrôlent le système. Le processeur analyse les signaux provenant des capteurs, prend des décisions logiques basées sur des instructions programmées, et commande des actions.

Mémoire : Elle stocke les instructions du programme et les données nécessaires. Le programme, souvent écrit en langage ladder ou en langage de bloc de fonctions, est chargé dans la mémoire du PLC.

Il peut également contenir les valeurs temporaires de certains calculs ou paramètres du processus.

Modules d'Entrées/Sorties (E/S) :

Les modules d'E/S connectent le PLC avec les appareils extérieurs :

- Entrées : Les capteurs, boutons-poussoirs, et autres dispositifs d'entrée envoient des signaux au PLC via ces modules. Par exemple, un capteur de température pourrait envoyer un signal indiquant que la température dépasse un certain seuil.
- Sorties : Le PLC envoie des signaux à des actionneurs (comme des moteurs, des vannes, ou des relais) pour effectuer des actions spécifiques en fonction des décisions prises par le programme.

Alimentation :

L'alimentation électrique fournit l'énergie nécessaire au fonctionnement de tous les composants du PLC.

Elle est souvent convertie en des tensions adaptées à chaque composant (comme 24V DC ou 220V AC).

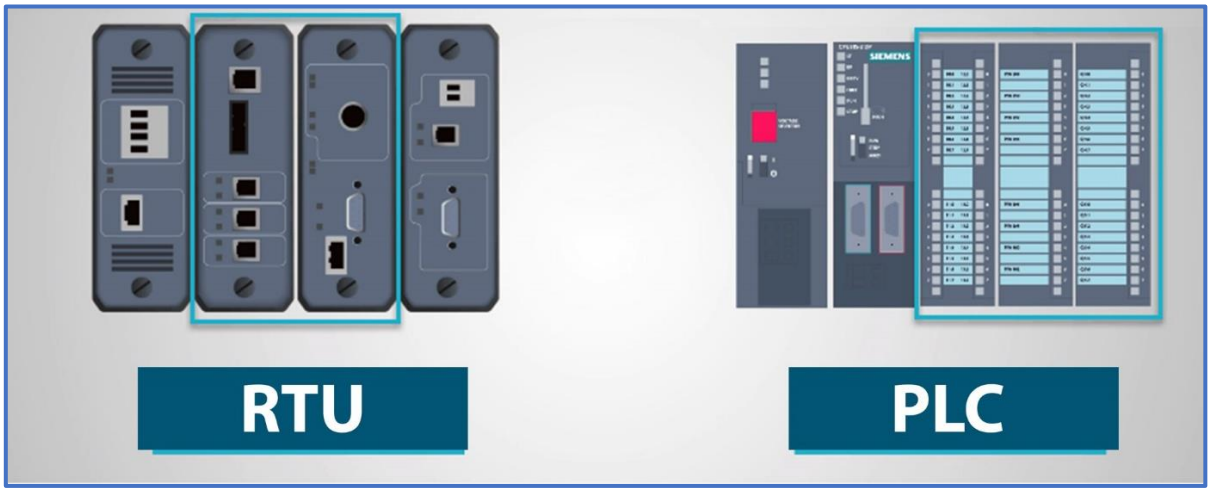


FIGURE 2. 2 : Unité terminale (RTU) et PLC (MONDI ANDERSON, 2018)

2.2.2 Structure Modulaire des PLC

Les PLC modernes sont souvent construits de manière modulaire, ce qui signifie que l'on peut ajouter ou retirer des modules selon les besoins de l'application. Par exemple : Si un système nécessite plus d'entrées ou de sorties, il suffit d'ajouter des modules supplémentaires au PLC. Cette modularité permet une grande flexibilité, car on peut adapter le PLC aux exigences spécifiques de chaque processus industriel.

Les systèmes modulaires sont aussi plus faciles à entretenir. Si un module tombe en panne, il peut être remplacé sans affecter les autres parties du système.

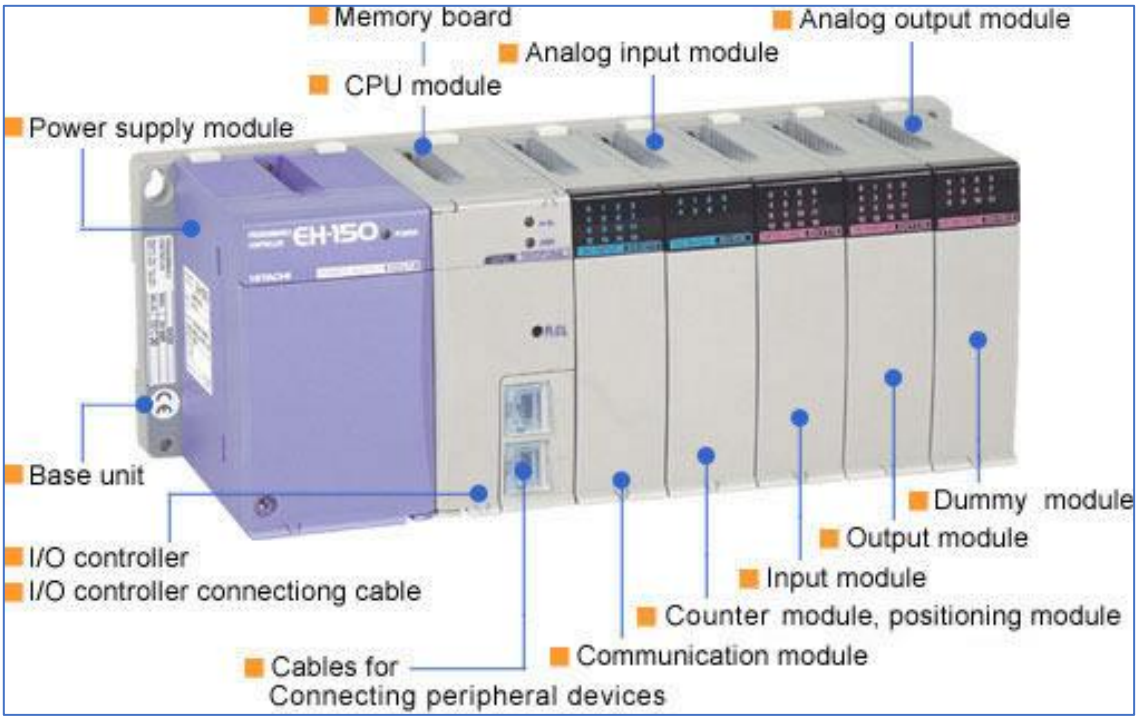


FIGURE 2. 3 : Composants d'un PLC (SCHWEBER, 2019)

2.2.3 Communication Interne

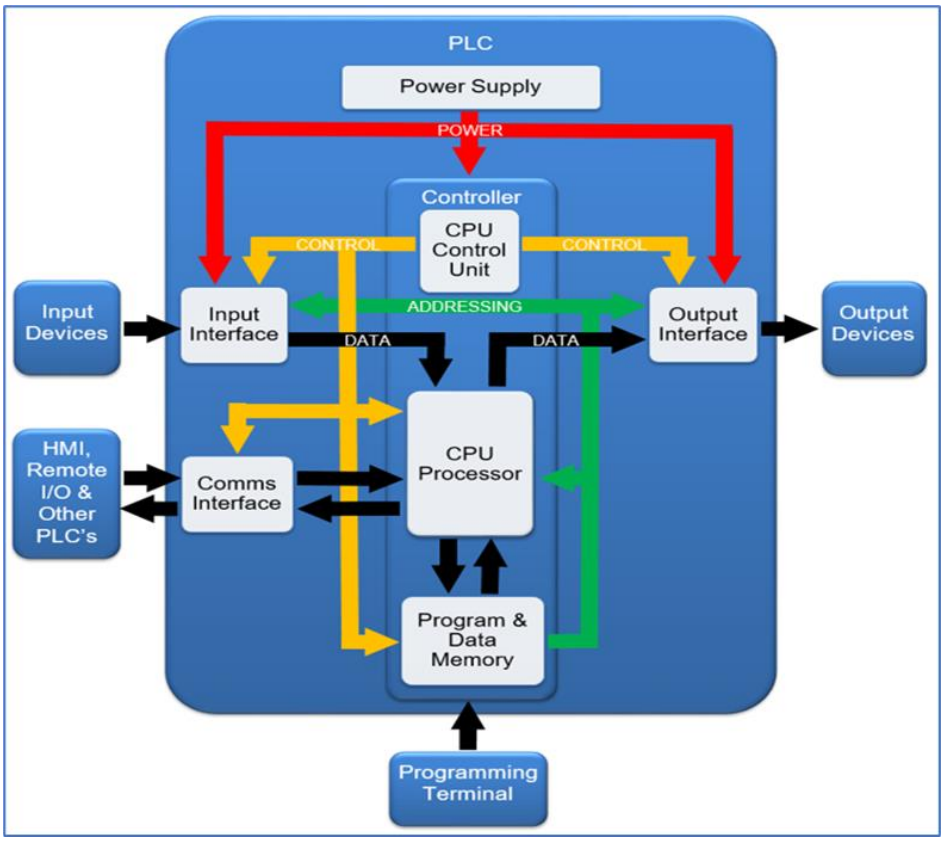


FIGURE 2. 4 : Diagramme de communication dans un PLC (LADDERLW, S.D.)

Les différents composants d'un PLC, l'unité centrale et les modules E/S, communiquent entre eux via un bus de données :

Bus de données : Il s'agit d'un canal par lequel les informations sont échangées. Selon l'architecture du PLC, ce bus peut être unibussé (tous les composants partagent un même canal) ou multibussé (différents canaux pour différentes fonctions).

Cela permet de gérer efficacement le transfert des informations entre les modules, notamment entre les entrées et le processeur, et entre le processeur et les sorties.

2.3 FONCTIONNALITES CLES DES PLC

1) Traitement Séquentiel :

Le traitement des instructions dans un PLC se fait de manière séquentielle.

Cela signifie que le PLC lit et exécute chaque instruction l'une après l'autre dans l'ordre où elles apparaissent dans le programme. Cette capacité à traiter des milliers d'entrées et de sorties dans un laps de temps très court est cruciale pour le contrôle en temps réel des processus industriels.

2) Interface Utilisateur (HMI) :

Les systèmes avec PLC incluent souvent une interface homme-machine (HMI) pour permettre aux opérateurs de surveiller et contrôler les processus automatisés. L'HMI peut afficher des graphiques en temps réel, des valeurs de capteurs, et même des alarmes visuelles ou sonores pour signaler des anomalies ou des pannes dans le système.

3) Intégration de Capteurs et Actionneurs

Le PLC s'appuie sur des capteurs pour obtenir des informations sur le processus industriel (comme la température, la pression ou la vitesse), puis sur des actionneurs pour contrôler des dispositifs mécaniques ou électriques en fonction des données reçues. Par exemple, si un capteur de niveau d'eau détecte que le niveau est trop bas, le PLC peut activer une pompe via un actionneur pour ajouter de l'eau dans le réservoir.

En générale, l'architecture des PLC est spécialement conçue pour répondre aux exigences de l'automatisation industrielle. Grâce à leur structure modulaire, leur capacité à traiter des données en temps réel, et leur facilité d'intégration avec des capteurs et actionneurs, les PLC sont des éléments essentiels pour rendre les processus industriels plus efficaces, sûrs, et flexibles. Ils sont au cœur de la modernisation des systèmes industriels, permettant un meilleur contrôle, une maintenance plus facile, et une réponse rapide aux changements ou aux pannes du système.

2.4 ARCHITECTURE DES SYSTEMES DE CONTROLE DISTRIBUES (DCS)

Les systèmes de contrôle distribués (DCS) sont des infrastructures essentielles pour l'automatisation des processus industriels complexes. Ils se distinguent par leur architecture répartie et hiérarchisée, permettant de contrôler et superviser de vastes réseaux d'équipements tout en assurant une flexibilité et une fiabilité maximales.

2.4.1 Composants Principaux des DCS

Contrôleurs (Process Controllers)

Les contrôleurs sont au cœur des systèmes DCS. Leur fonction principale est d'exécuter les **algorithmes de contrôle** qui régissent le processus industriel. Voici leurs rôles :

- **Traitement des données d'entrée** : Ils reçoivent des informations des capteurs qui mesurent diverses variables du processus (température, pression, débit, etc.).
- **Décisions et commandes** : En fonction des algorithmes programmés, les contrôleurs analysent ces données et prennent des décisions qui sont ensuite transmises aux **actionneurs** (comme des vannes ou des moteurs) pour ajuster le processus en temps réel.

Modules d'Entrées/Sorties (E/S)

Ces modules servent d'interface entre le DCS et les équipements externes. Ils sont essentiels pour la communication bidirectionnelle avec les capteurs et actionneurs :

- **Entrées** : Les capteurs envoient des signaux au DCS via ces modules, permettant au système de suivre en temps réel l'état du processus.
- **Sorties** : Les modules envoient des commandes aux actionneurs afin de contrôler les éléments du système en fonction des décisions prises par les contrôleurs.

Réseaux de Communication

Les réseaux de communication assurent l'échange de données entre les différents composants du DCS (contrôleurs, modules E/S, stations de supervision). Ces réseaux doivent être :

- **Fiables** : La stabilité est essentielle pour éviter toute interruption de communication, qui pourrait affecter le processus.
- **À faible latence** : Les décisions doivent être prises et exécutées en temps réel, ce qui impose un délai de communication minimal entre les différents éléments du système.

2.4.2 Structure Hiérarchique d'un DCS

Les DCS sont souvent organisés selon une **structure hiérarchique**, divisée en plusieurs niveaux pour faciliter la gestion du système.

Niveau Supervisoire (Supervisory Level)

C'est le **niveau supérieur** du DCS. Il inclut :

- **Stations de supervision (SCADA, IHM)** : Ces interfaces homme-machine permettent aux opérateurs de visualiser le processus dans son ensemble et d'intervenir si nécessaire. Elles offrent des graphiques en temps réel, des tableaux de bord et des alarmes.

- **Stations d'ingénierie** : Les ingénieurs peuvent y modifier les paramètres de contrôle, télécharger des programmes de contrôle mis à jour, et effectuer des diagnostics à distance.

Niveau de Contrôle (Control Level)

C'est le **niveau intermédiaire** où se trouvent les contrôleurs et les modules E/S. Il est chargé d'exécuter en temps réel les **algorithmes de contrôle** nécessaires pour assurer la régulation du processus industriel. Ce niveau garantit que les actions de contrôle se déroulent de manière autonome et continue.

2.4.3 Redondance et Fiabilité

Une caractéristique fondamentale des DCS est leur **redondance** intégrée, qui garantit un haut niveau de fiabilité :

- **Redondance des contrôleurs** : Chaque contrôleur peut avoir un contrôleur de secours prêt à prendre la relève en cas de défaillance. Cela garantit que le processus continue de fonctionner sans interruption, même si un composant critique tombe en panne.
- **Redondance des réseaux** : Plusieurs réseaux peuvent être configurés pour assurer une communication ininterrompue en cas de défaillance d'un canal de communication.
- **Redondance des modules E/S** : Des modules E/S de secours peuvent être installés pour prendre le relais en cas de panne.

2.4.4 Modularité et Scalabilité

Modularité

Les systèmes DCS sont conçus de manière **modulaire**, ce qui permet de les adapter facilement aux besoins spécifiques d'une installation industrielle :

- **Ajout ou retrait de modules** : En fonction des évolutions du processus ou de l'agrandissement d'une usine, des modules supplémentaires peuvent être ajoutés ou retirés, sans nécessiter de modifications majeures du système.

Scalabilité

Les DCS peuvent être facilement **évolutifs**, ce qui signifie qu'ils peuvent s'adapter à la croissance d'une installation :

- **Intégration avec des technologies émergentes** : Par exemple, ils peuvent se connecter à des solutions de l'Internet des objets industriels (IIoT) pour améliorer la surveillance et l'efficacité du processus.

2.4.5 Exigences Spécifiques des DCS

Les DCS doivent répondre à plusieurs **exigences spécifiques** pour fonctionner efficacement dans des environnements industriels :

- **Traitement en temps réel** : Les systèmes doivent répondre rapidement aux changements de processus pour assurer un contrôle précis et immédiat.
- **Durabilité** : Les composants doivent être robustes pour résister à des environnements industriels souvent difficiles (températures extrêmes, humidité, vibrations).

- **Sécurité** : Les DCS doivent être conformes à des normes strictes en matière de **sécurité industrielle** et de **cybersécurité** pour protéger les processus critiques contre les défaillances ou les cyberattaques.

L'architecture des systèmes de contrôle distribués (DCS) est conçue pour gérer de manière fiable et efficace des processus industriels complexes.

Grâce à leur structure hiérarchique, leur modularité, leur redondance, et leur capacité à évoluer avec les besoins de l'industrie, les DCS assurent un contrôle optimal et une supervision en temps réel, tout en garantissant la sécurité et la résilience du système.

Ils sont un pilier essentiel de l'automatisation moderne dans divers secteurs industriels.

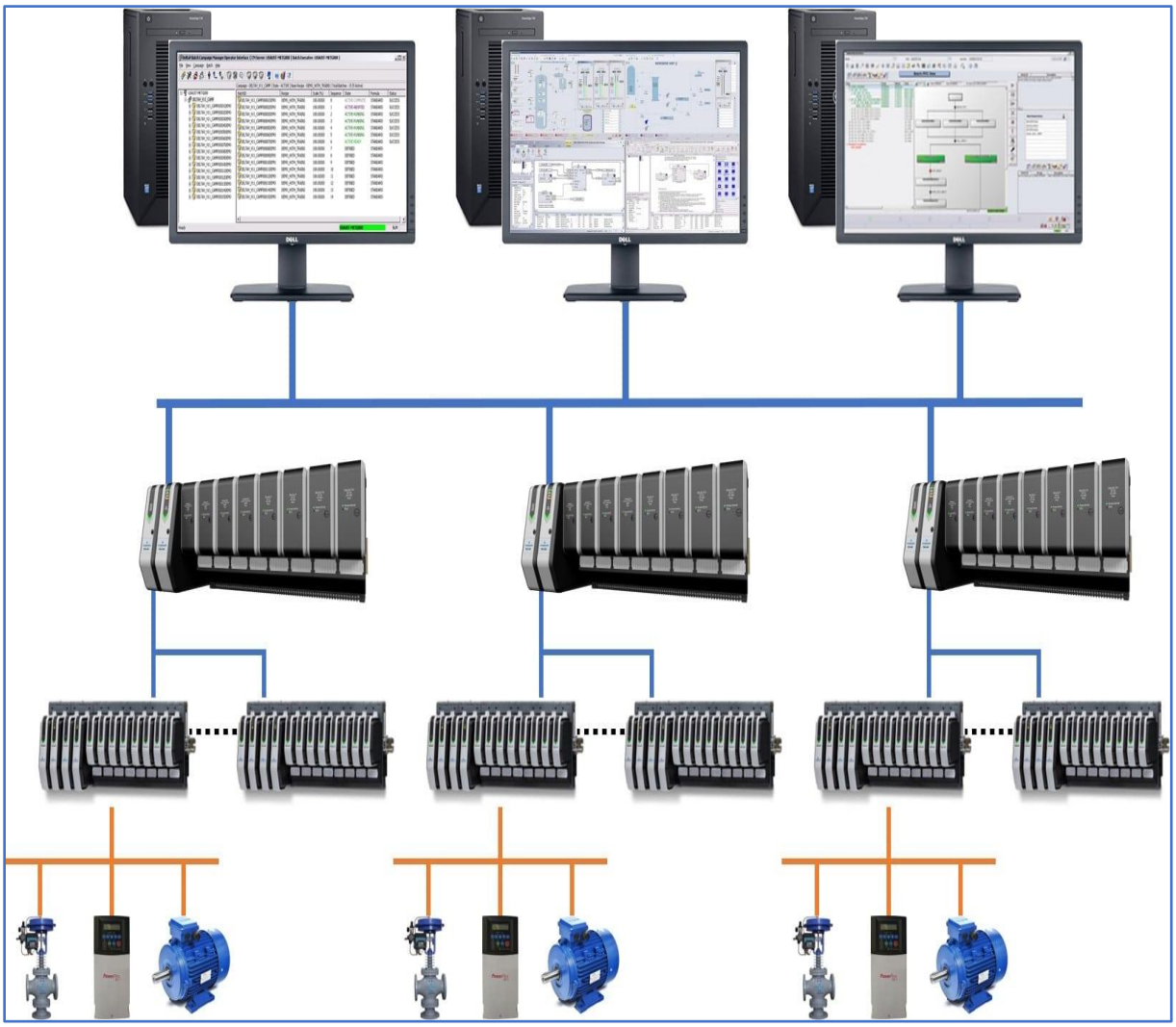


FIGURE 2. 5 : Architecture d'un DCS

2.5 ARCHITECTURE SCADA

Les premiers systèmes SCADA ont été déployés dans les années 1960 et ont évolué au fil des décennies. On peut distinguer quatre générations d'architectures SCADA.

2.5.1 Première génération – Systèmes SCADA monolithiques

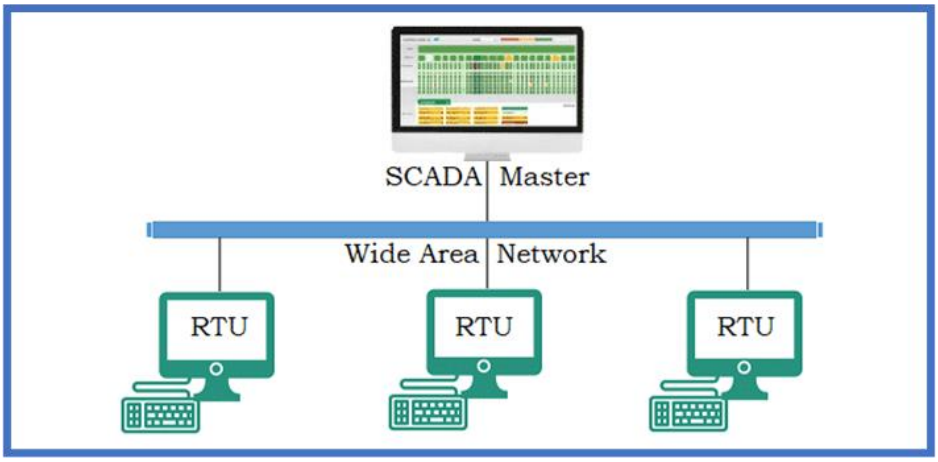


FIGURE 2. 6 : Architecture SCADA de première génération

Lorsque les premiers systèmes SCADA ont été développés, ils étaient conçus comme des systèmes autonomes. Ces systèmes communiquaient avec les RTU (Remote Terminal Units) via des réseaux étendus (WAN).

Les protocoles de communication utilisés dans les réseaux SCADA étaient créés par les fabricants d'équipements RTU et étaient souvent propriétaires. La connexion au poste maître SCADA s'effectuait au niveau du bus à l'aide d'un adaptateur propriétaire.

2.5.2 Deuxième génération – Systèmes SCADA distribués

La deuxième génération de systèmes SCADA a été conçue pour répartir le traitement des données entre plusieurs systèmes, connectés via un réseau local (LAN). Ces stations distribuées remplissaient différentes fonctions. Certaines agissaient comme processeurs de communication entre les dispositifs de terrain, tels que les RTU. D'autres servaient d'interface opérateur, offrant l'interface homme-machine (HMI) aux opérateurs du système. Certaines stations étaient également dédiées aux calculs et aux services de bases de données. La répartition des fonctionnalités du système a permis d'augmenter la puissance de traitement, d'améliorer la redondance et la fiabilité du système. Comme dans la première génération, le système communiquait avec les RTU via des réseaux étendus (WAN).

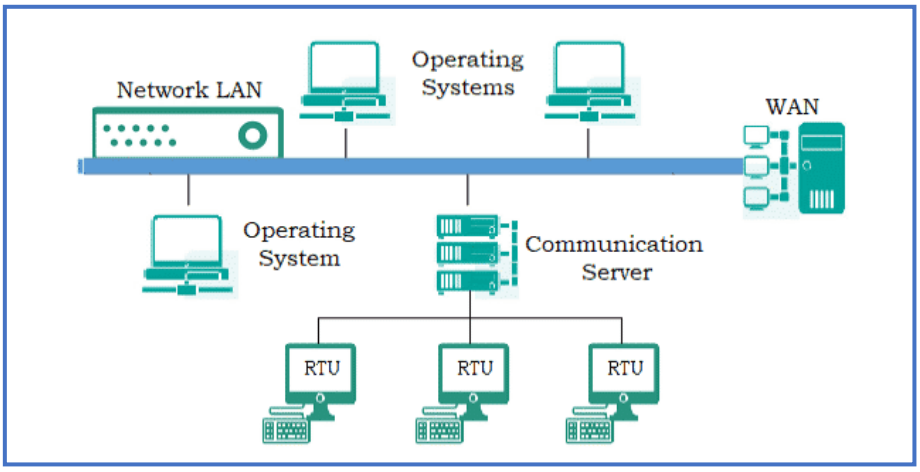


FIGURE 2. 7 : Architecture SCADA de deuxième génération

2.5.3 Systèmes SCADA en réseau (Troisième génération)

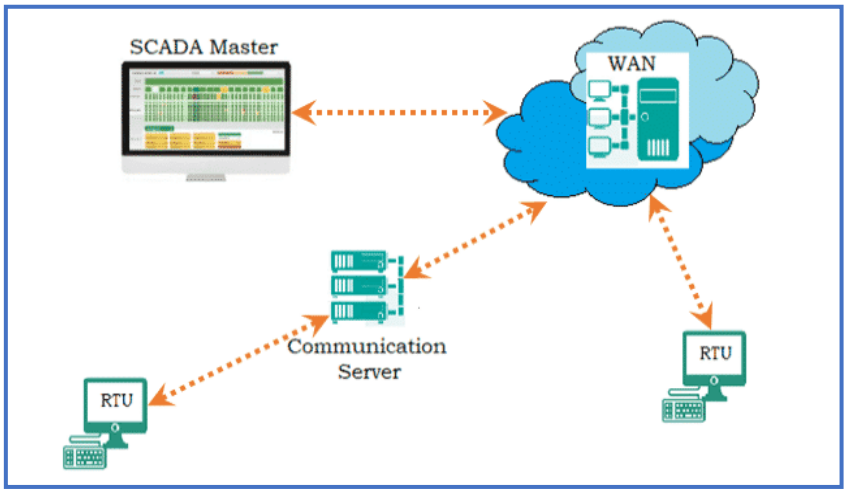


FIGURE 2. 8 : Architecture SCADA de troisième génération

Les systèmes de contrôle et acquisition de données (SCADA) sont en réseau et communiquent via des réseaux étendus (WAN) par des lignes téléphoniques ou de données.

Les connexions en fibre optique ou Ethernet sont utilisées pour la transmission des données entre les nœuds. Ces systèmes utilisent des automates programmables (PLC) pour ajuster et surveiller les opérations uniquement lorsqu'une décision importante doit être prise (Mondi, 2019).

Les systèmes SCADA de première et deuxième génération étaient limités à des réseaux sur un seul site ou à un seul bâtiment, appelés systèmes fermés. Dans ces anciens systèmes, les risques de sécurité étaient quasi inexistants, contrairement aux systèmes SCADA de troisième génération, qui sont connectés à Internet et donc plus vulnérables aux risques de sécurité.

La nouvelle architecture réseau permet à plusieurs systèmes SCADA distribués de fonctionner en parallèle sous la supervision d'un seul poste maître (Flaus J.-M. , Cybersécurité des systèmes industriels, 2018).

2.5.4 Quatrième génération – Systèmes SCADA basés sur l'Internet des objets (IoT)

La quatrième génération d'architecture SCADA a incorporé les technologies de l'Internet des objets (IoT) ainsi que les services cloud commerciaux, facilitant ainsi la maintenance et l'intégration des systèmes SCADA.

Cette évolution technologique offre plusieurs avantages significatifs, tels qu'une meilleure accessibilité des données, une réduction des coûts, une flexibilité accrue, une optimisation des processus, une disponibilité continue et une scalabilité améliorée des infrastructures.

Toutefois, cette transition vers des solutions connectées introduit également de nouveaux défis en matière de sécurité, en raison de la dépendance aux environnements cloud et à l'interconnexion croissante des dispositifs industriels.

En somme, bien que cette architecture apporte une modernisation indéniable, elle exige également une vigilance accrue face aux risques émergents pour garantir la sécurité des systèmes critiques (Raghvendra, s.d.) (Mondi, 2019).

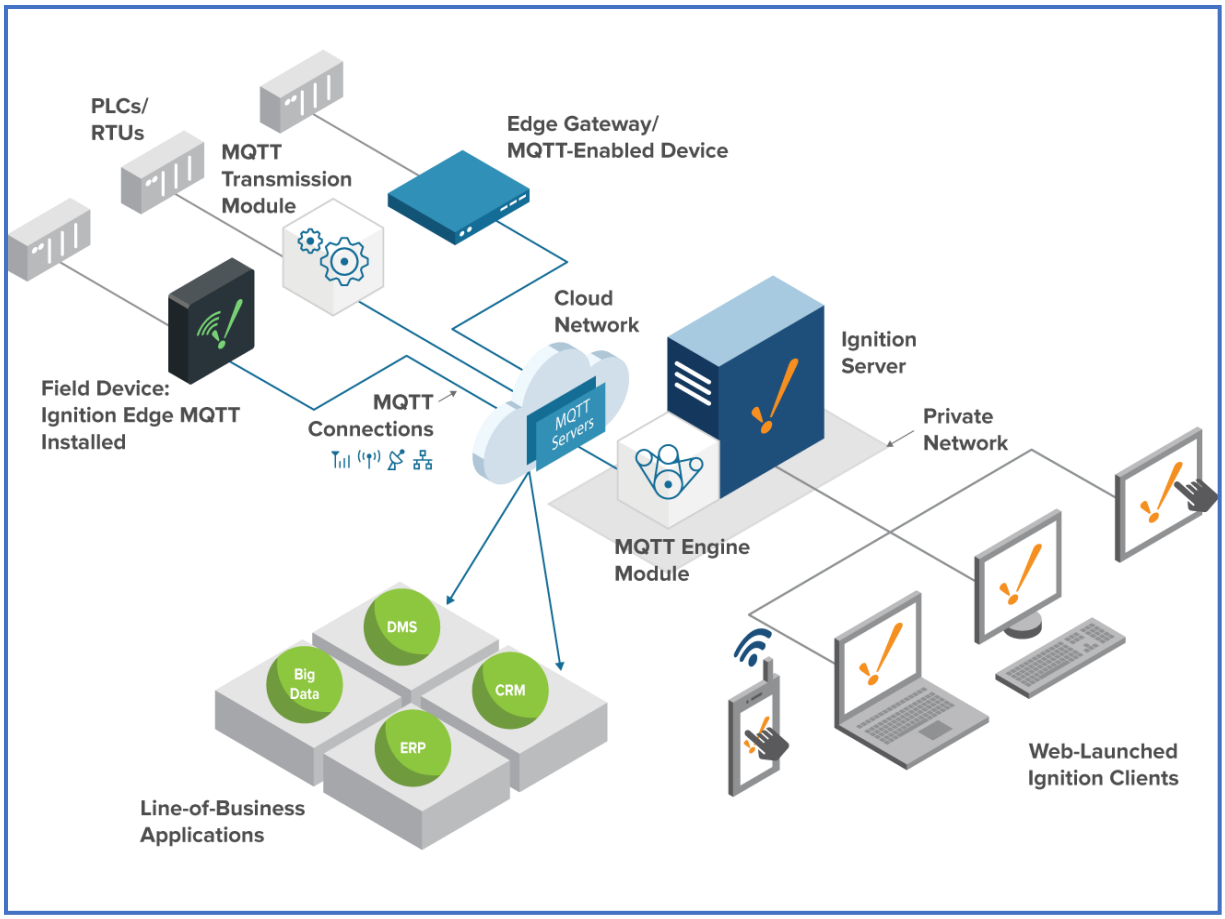


FIGURE 2. 9 : Architecture SCADA de quatrième génération (SCADA / IOT)

2.6 PROTOCOLES DE COMMUNICATION SCADA

Les systèmes SCADA utilisés dans le secteur de l'énergie englobent la collecte d'informations via les RTU, leur transfert vers le site central, l'analyse et le contrôle nécessaires, puis l'affichage des informations dans une interface homme-machine (IHM). Un protocole de communication SCADA est une norme pour la représentation et le transfert de données sur un canal de communication en mode maître/esclave. IEC 60870-5-104 et DNP3 sont deux des protocoles de communication SCADA les plus couramment utilisés dans l'industrie énergétique. L'IEC 60870-5 est largement utilisé en Europe, tandis que le DNP3 est répandu en Amérique du Nord. Un autre protocole SCADA largement utilisé est Modbus, couramment employé dans diverses industries, notamment les usines de traitement des eaux et des eaux usées. Ces protocoles sont implémentés au niveau de la couche application, qui correspond à la couche 5 du modèle TCP/IP.

2.6.1 IEC 60870-5-104

L'IEC 60870 est un ensemble de normes de la Commission électrotechnique internationale (IEC) pour la transmission de données et le contrôle de télémétrie SCADA, principalement utilisé dans la surveillance et le contrôle des systèmes électriques. L'IEC 60870-5-101, lancé en 1995, est conçu pour la communication série, tandis que l'IEC 60870-5-104, introduit en 2004, est une extension permettant la transmission des trames série sur TCP/IP. La **figure 11** illustre la structure de la trame du protocole, appelée Unité de Données du Protocole d'Application (APDU), composée de l'APCI (Informations de Contrôle du Protocole d'Application) et de l'ASDU (Unité de Données du Service d'Application).

L'APCI correspond aux six premiers octets de l'APDU et inclut un caractère de début (68H), un champ de longueur et un champ de contrôle. Ce champ de contrôle, comme indiqué dans la **figure 2.10**, peut-être de trois types : Information, Supervisory ou Unnumbered. Les deux derniers bits déterminent le type : 10 pour Supervisory, 11 pour Unnumbered, et 00 pour Information.

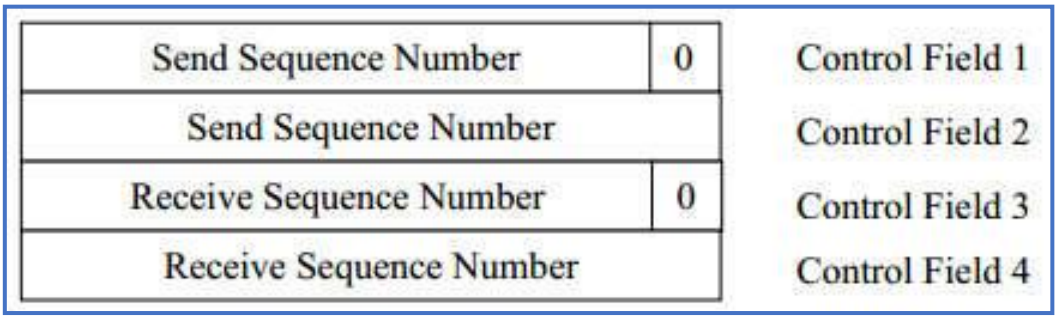


FIGURE 2. 10 : Structure du type d'informations du champ de controle

L'ASDU (illustré à la **figure 2.11**) contient l'identifiant de l'unité de données ainsi que la charge utile de données de un ou plusieurs objets d'information. Le champ d'identification de type (TI) définit les types de données en se référant aux codes sur 8 bits. La **figure 2.12** montre les groupes TI actuellement définis par l'IEC. Par exemple, le TI numéro 9 correspond au code de référence M_ME_NA_1, qui indique "Valeur mesurée, Valeur normalisée".

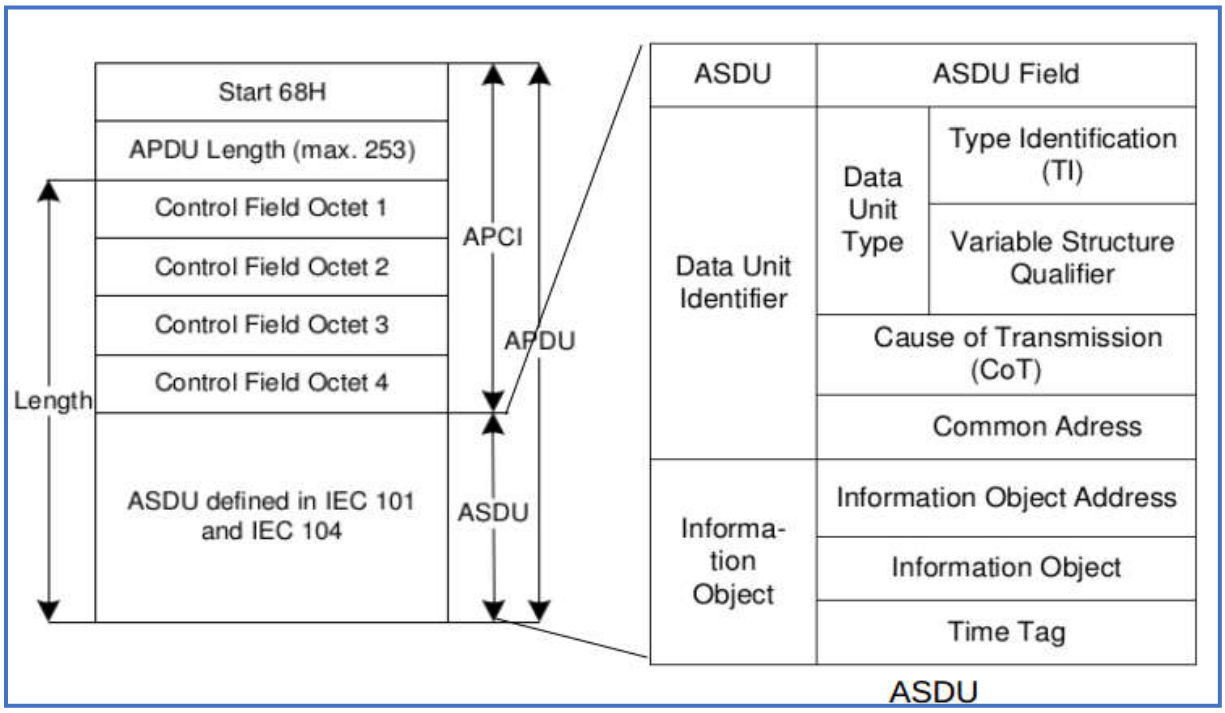


FIGURE 2. 11 : IEC 60870-5-104 APDU & ASDU

Le qualificateur de structure variable indique si la charge utile contient plusieurs objets d'information ou non (jusqu'à un maximum de 127). Le champ "Cause of Transmission" (CoT) précise la raison de la transmission. Par exemple, une valeur CoT de "1" indiquerait une transmission périodique, tandis qu'une valeur de "3" indiquerait une transmission spontanée. L'adresse commune est associée à tous les objets dans un ASDU, et toutes les stations d'un

système spécifique diffusent à cette adresse commune. L'adresse de l'objet d'information est utilisée comme adresse de destination pour les communications de contrôle et comme adresse source pour la surveillance. Par défaut, le protocole IEC 60870-5-104 utilise le port TCP 2404.

CODE TYPE RANGE	GROUP
1-21, 30-40	Process information in monitor direction
45-51	Process information in control direction
70	System information in monitor direction
100-106	System information in control direction
110-113	Parameter in control direction
120-126	File Transfer

FIGURE 2. 12 : Groupes de types de codes

2.6.2 DNP3

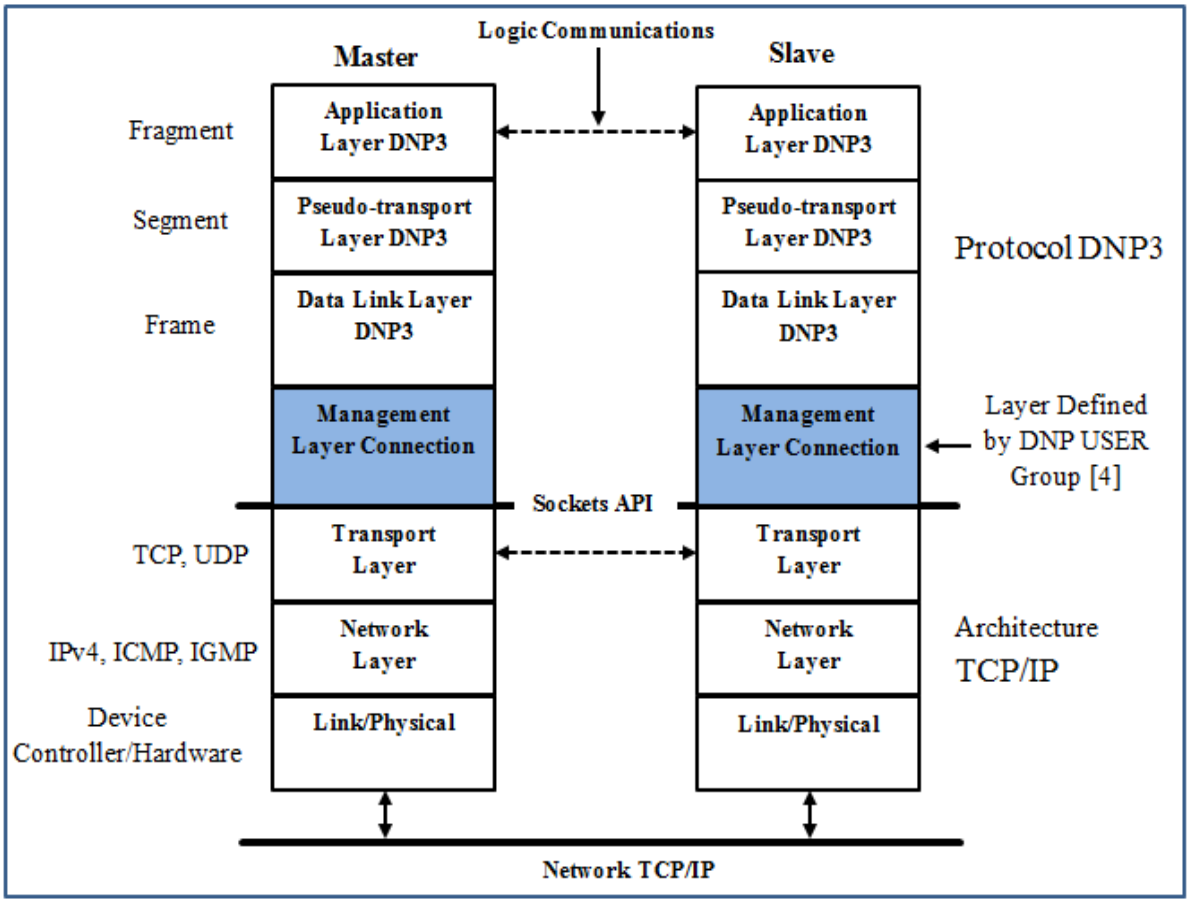


FIGURE 2. 13 : ARCHITECTURE MAITRE/ESCLAVE DNP3 (ORTEGA, 2013)

Le protocole Distributed Network Protocol Version 3 (DNP3) est une norme de protocole qui définit les communications entre les RTU (Remote Terminal Units) et les stations maîtresses. À l'origine, DNP3 était un protocole propriétaire développé par la division Harris Controls, mais il a ensuite été adopté par l'IEEE en tant que norme ouverte. DNP3 est un protocole de contrôle maître/esclave, généralement configuré avec une station maître et plusieurs dispositifs distants.

Le protocole DNP3 a initialement été conçu pour établir une connexion série point à point. Cependant, avec l'amélioration des réseaux en termes de vitesse et de bande passante, il a été adapté pour fonctionner avec le protocole TCP/IP. Comme illustré dans la **Figure 2.13**, la mise en œuvre du standard DNP3 sur TCP/IP ne change pas la structure des couches, à l'exception de la synchronisation temporelle. Le message envoyé reste indépendant du protocole TCP/IP, et les accusés de réception dans la couche de liaison ne sont plus utilisés, étant remplacés par des confirmations au niveau de la couche application, comme dans la transmission série. L'interface entre les couches de gestion et contrôle du protocole TCP/IP est mise en œuvre via une API (interface de programmation d'applications), et le port attribué pour cette communication est le numéro 20000.

Le DNP3 encapsulé dans TCP/IP est divisé en trois niveaux : le niveau 1 gère les fonctions de base, le niveau 2 ajoute des fonctions et variations pour la communication avec des dispositifs intelligents (IED), et le niveau 3 prend en charge toutes les fonctionnalités du protocole.

Le DNP3 utilise TCP/IP pour transporter ses messages sur des réseaux LAN, MAN ou WAN, et il est recommandé de désactiver les accusés de réception dans la couche de liaison, car le protocole TCP garantit une connexion fiable (Ortega, 2013).

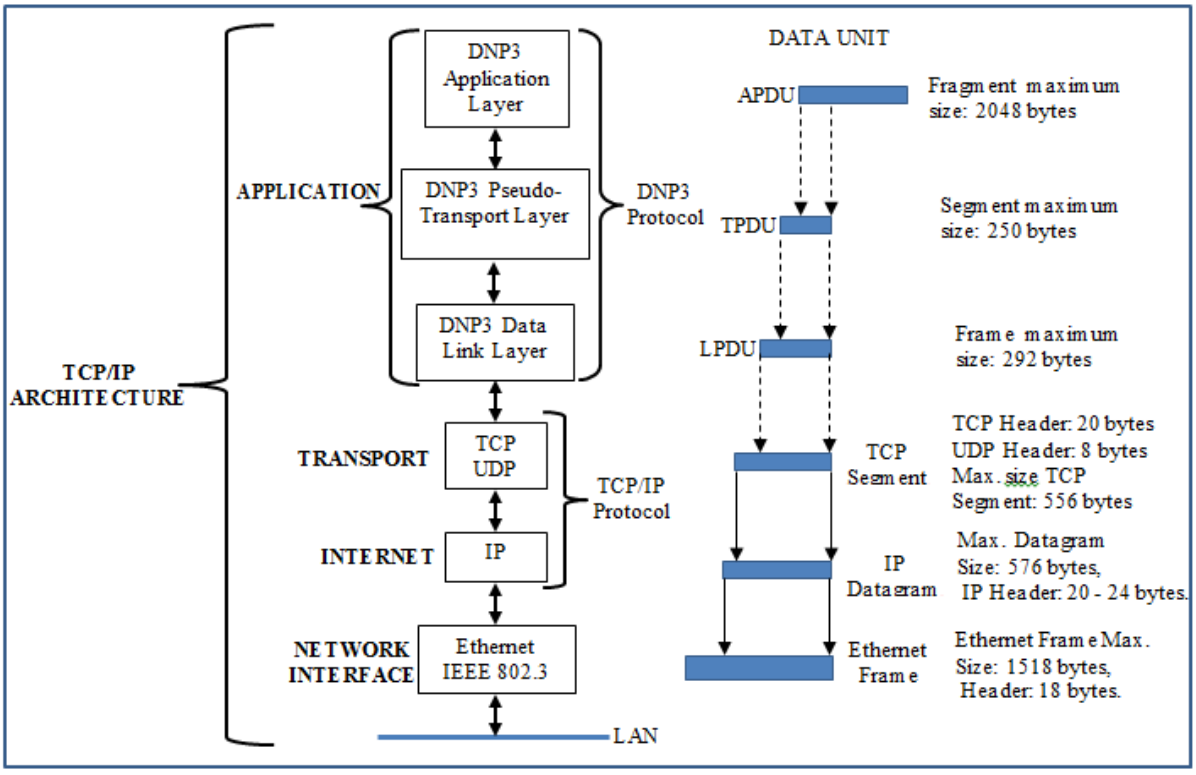


FIGURE 2. 14 : ENCAPSULATION DE DNP3 SUR TCP/IP (ORTEGA, 2013)

Lors de l'encapsulation des données DNP3, un message DNP3, construit dans la couche application, est encapsulé dans un segment TCP avec une taille maximale de 292 octets. Ensuite, il est encapsulé dans un datagramme IP, portant la taille maximale à 576 octets. Finalement, le message est encapsulé dans une trame Ethernet, atteignant une taille maximale de 1 518 octets. Cette adaptation permet au DNP3 de tirer parti des avantages des réseaux modernes tout en conservant ses fonctionnalités essentielles (Ortega, 2013).

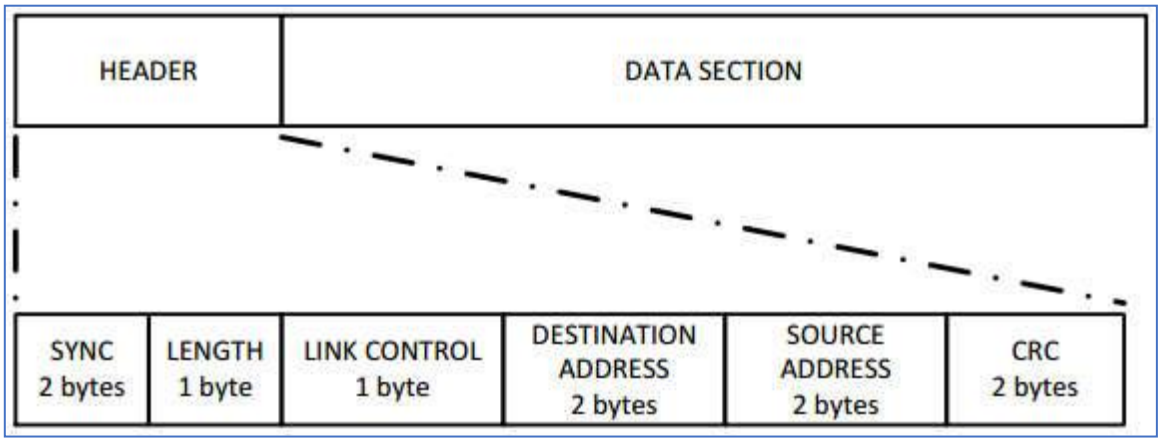


FIGURE 2. 15 : TRAME DE LIAISON DE DONNEES DNP3

La couche pseudo-transport a pour responsabilité de diviser les longs messages de la couche application en paquets plus petits, adaptés à la taille de la couche de liaison pour la transmission. Lors de la réception, elle doit également réassembler les trames en un message plus long de la couche application. La couche application fragmente un message en fonction de la taille du tampon du destinataire, qui peut varier de 2048 à 4096 octets. Un fragment de taille 2048 doit être divisé en 9 trames par la couche de transport avant d'être transmis à la couche de liaison de données. Par défaut, DNP3 utilise le port TCP numéro 20000.

2.6.3 Modbus

Modbus est un protocole de communication série open source développé par Modicon (aujourd'hui Schneider Electric) en 1979. Il est utilisé pour établir une communication maître/esclave ou client/serveur entre un ordinateur de supervision et une unité terminale distante (RTU) dans un système de contrôle et d'acquisition de données (SCADA). Il existe plusieurs versions des protocoles Modbus, notamment Modbus RTU et Modbus ASCII pour les lignes série, ainsi que Modbus TCP pour la communication Ethernet. Ce mémoire se concentre sur Modbus sur TCP.

Le protocole Modbus fournit quatre types de messages utilisés dans la communication client/serveur : demande, confirmation, indication et réponse.

FIGURE 2. 16 : MODBUS CLIENT/SERVER COMMUNICATION MODEL

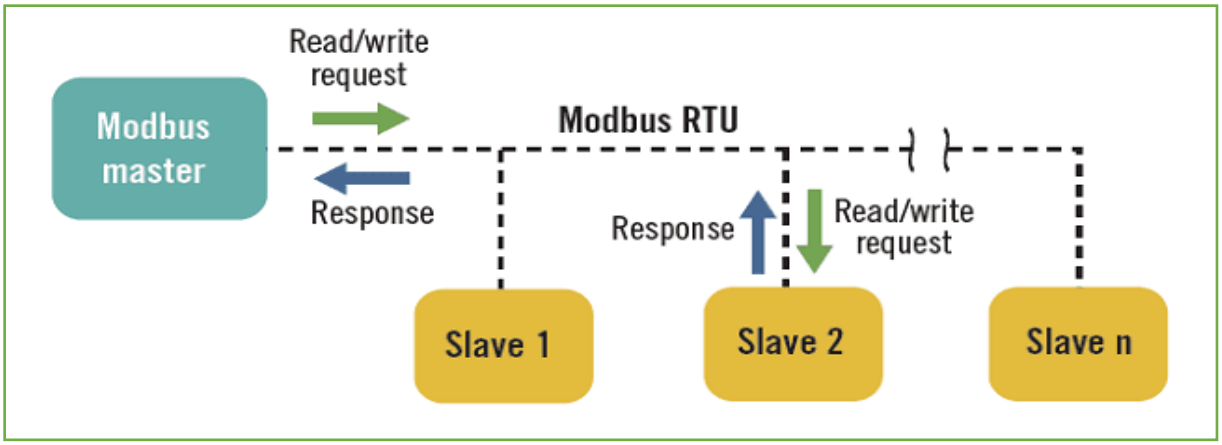


FIGURE 2. 17 : MODBUS RTU CLIENT/SERVER COMMUNICATION MODEL (GENERAL INDUSTRIAL AUTOMATION, 2021)

Un système de communication utilisant Modbus TCP peut inclure différents types de dispositifs. La plupart de ces dispositifs sont directement connectés à l'Ethernet. Des dispositifs interconnectés, tels que des ponts, des routeurs et des passerelles, peuvent également être utilisés pour relier des appareils sur des lignes série au réseau Modbus.

La trame Modbus est composée d'une Unité de Données d'Application (ADU), qui encapsule une Unité de Données de Protocole (PDU). L'ADU comprend un champ d'adresse, la PDU et un mécanisme de vérification d'erreur. La PDU contient un champ de code de fonction et un champ de données. Le code de fonction indique le type d'action à effectuer.

La trame Modbus utilisée dans Modbus TCP diffère de la trame générale. La principale différence réside dans l'ajout d'un nouvel en-tête de 7 octets, appelé en-tête MBAP (Modbus Application Header), au début du message.

La vérification de redondance cyclique (CRC) pour le contrôle d'erreur a été supprimée du message. La vérification d'erreur est désormais effectuée par le protocole TCP au niveau de la couche de transport (couche 4).

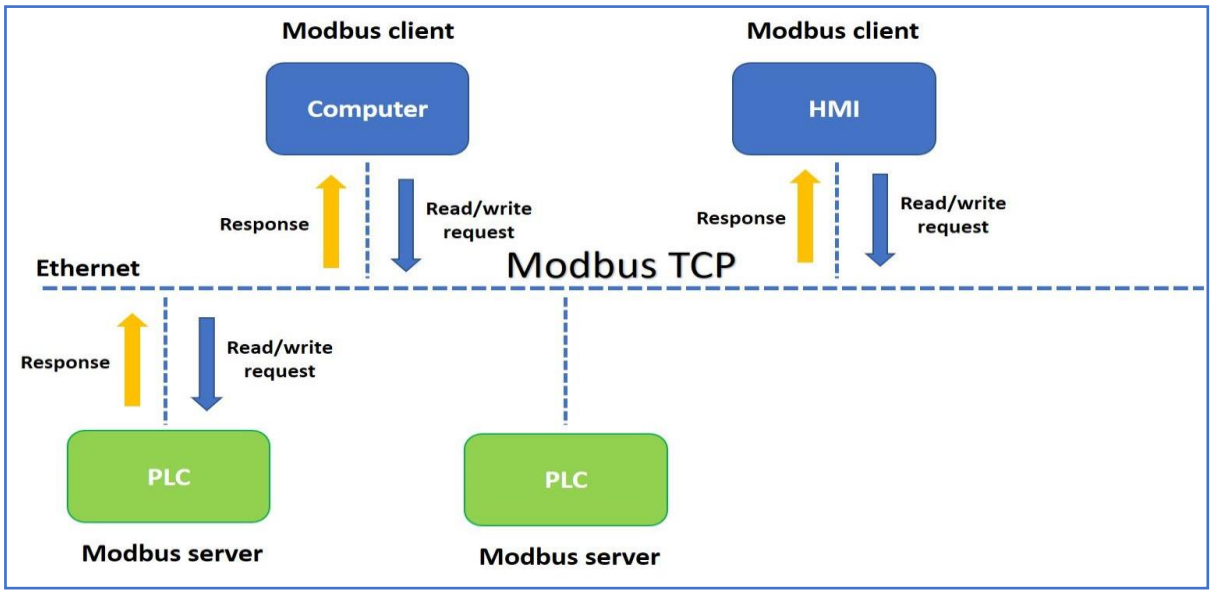


FIGURE 2. 18 : Architecture de communication MODBUS TCP/IP (GENERAL INDUSTRIAL AUTOMATION, 2021)

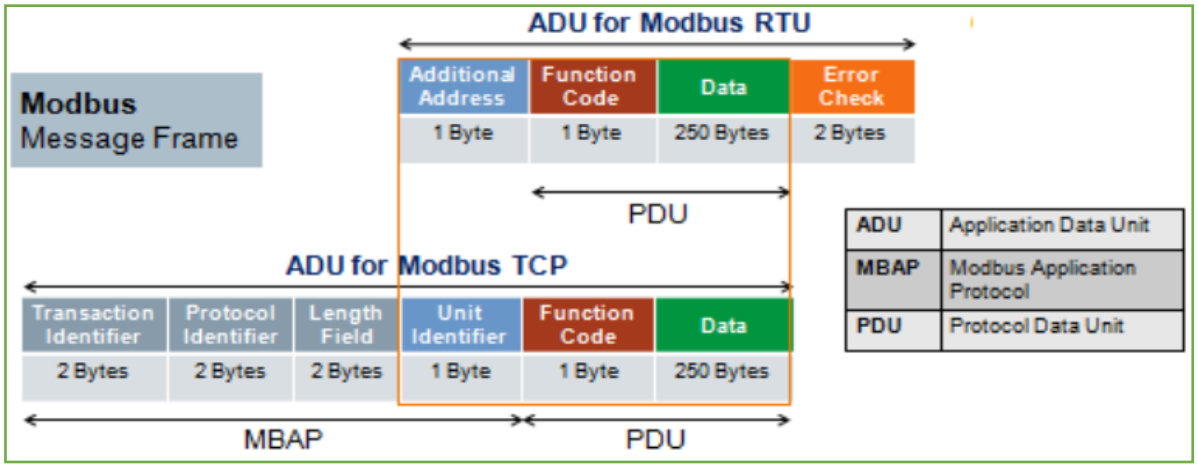


FIGURE 2. 19 : Trame de messagerie MODBUS TCP/IP VS RTU

TABLEAU 2. 1 : Différence entre MODBUS RTU et MODBUS TCP (GENERAL INDUSTRIAL AUTOMATION, 2021)

#	**Modbus RTU**	**Modbus TCP**
Physical Layer	Serial RS485 - RS422 - 2/4 wire	Ethernet, Cat5,6,7
Multi Clients (Master)	Only One	Multi-Client Support
Multi Servers (Slave)	Supported	Supported
Speed	9600-19200 bps	10 Mbps
Distance	Limited, usually not more than 1000m	Unlimited with fiber and satellite

Modèle OSI pour Modbus TCP

Layer	Layer Name	Description	Protocols
7	Application	The application layer is exposed to the end-user like web browsers or applications.	Modbus
6	Presentation	The Presentation layer prepares the translation of the application data and format into network format (encryption/decryption of data for secure transmission).	
5	Session	A session occurs between two devices. This layer connects the application to the network.	
4	Transport	layer is also called the Transmission Control Protocol or TCP. The TCP is built on top of the Network layer (IP).	TCP
3	Network	The network layer (IP) is where packet forwarding (routing), setup and creation of connections occur	IP,ARP,RARP
2	Data Link	The data link layer is responsible for data transfer.	Ethernet, CSMA/CD, MAC
1	Physical	The Physical layer is where physical components connect. This includes the cables, sufficient voltages and frequencies.	Ethernet Physical layer – Cat5,6,7 for example

FIGURE 2. 20 : Modèle OSI pour MODBUS TCP (GENERAL INDUSTRIAL AUTOMATION, 2021)

Pour mieux comprendre la structure de Modbus TCP/IP, il est nécessaire d'examiner le modèle d'interconnexion des systèmes ouverts (OSI) :

Les couches supérieures, 5 à 7, sont généralement unies pour former la cinquième couche, la couche Application. Lorsque Modbus est mentionné en tant que couche d'application, nous faisons référence à Modbus TCP.

Les quatre premières couches sont identiques pour chaque protocole basé sur Ethernet.

Couche Application

Il existe plusieurs protocoles dans la couche application, tels que FTP, DNS, SMTP, HTTP, et bien d'autres. Chacun de ces protocoles a un objectif spécifique. Pour Modbus TCP, le principal protocole d'application d'intérêt est Modbus.

Les fonctions Modbus opèrent sur des registres de mémoire pour surveiller et contrôler les dispositifs sur le réseau. Les fabricants de dispositifs Modbus publient généralement une carte de registre. Avant d'essayer de communiquer avec un dispositif, il est conseillé de se référer à la carte de registre de ce dispositif pour comprendre son fonctionnement.

La structure du modèle de données Modbus se compose de quatre types de données de base :

- **Entrées discrètes** – 0xxxx
- **Bobines (Sorties)** – 1xxxx
- **Registres d'entrée (Données d'entrée)** – 3xxxx
- **Registres de maintien (Données de sortie)** – 4xxxx

La requête de service (Unité de Données de Protocole Modbus) se compose d'un code de fonction et d'octets de données supplémentaires, selon la fonction. Dans la plupart des cas, les données supplémentaires incluent généralement une référence variable, comme une adresse de registre, car la plupart des fonctions Modbus opèrent sur des registres.

Fonctions et Registres Modbus

Le client (maître) fournit au serveur (esclave) des informations supplémentaires requises par l'esclave pour compléter l'opération spécifiée par le code de fonction. Les données de la requête incluent généralement des adresses de registre, des valeurs de décalage et des données à écrire.

- **Lire l'état de la bobine (01)** – Cette commande lira l'état ON/OFF des sorties discrètes ou des bobines (adresses de référence 0xxxx) dans l'esclave/serveur.
- **Lire les registres de maintien (03)** – Lit le contenu binaire des registres de maintien (adresses de référence 4x) dans le dispositif esclave.

- **Lire les registres d'entrée (04)** – Cette commande lira le contenu binaire des registres d'entrée (adresses de référence 3x) dans le dispositif esclave.
- **Forcer une seule bobine (05)** – Force une seule bobine/sortie (adresse de référence 0x) à être ON ou OFF.
- **Préciser un registre unique (06)** – Cette commande va définir un registre de maintien unique (adresse de référence 4x) à une valeur spécifique.
- **Forcer plusieurs bobines (15)** – Force simultanément une série de bobines (adresse de référence 0x) à être ON ou OFF.
- **Préciser plusieurs registres (16)** – Précise un bloc de registres de maintien (adresses de référence 4x) à des valeurs spécifiques.
- **Rapporter l'ID de l'esclave (17)** – Cette commande retourne le modèle, le numéro de série et le firmware.

Pour qu'une fonction fonctionne, il faut spécifier le registre de départ et la quantité de registres à lire/écrire.

Exceptions Modbus

Lorsque le dispositif serveur répond au client, il utilise le code de fonction pour indiquer soit une réponse normale, soit une réponse d'exception si une erreur s'est produite.

Une réponse normale renvoie simplement le code de fonction original de la requête, tandis qu'une réponse d'exception retourne le code de fonction original avec son bit le plus significatif défini à '1'.

Les communications Modbus sont, par défaut, initiées sur le port TCP 502, qui est spécifiquement réservé à ce protocole, garantissant ainsi une connexion standardisée et sécurisée pour l'échange de données entre les dispositifs connectés.

2.7 VULNERABILITES ET PROBLEMES DE SECURITE DANS LES PROTOCOLES

Les systèmes SCADA font souvent partie des infrastructures critiques (IC), rendant la sécurité de ces systèmes et des protocoles de communication utilisés pour l'échange de données primordiale pour prévenir les cyberattaques. De nombreux systèmes manquent de fonctionnalités de surveillance. En l'absence de surveillance réseau, il devient impossible de détecter les activités suspectes et d'identifier les menaces potentielles.

Un autre problème majeur est que certains systèmes sont rarement ou jamais mis à jour, ce qui signifie qu'ils peuvent contenir des vulnérabilités dans le firmware ou le logiciel, exploitables par des attaquants. Certains fournisseurs autorisent même les dispositifs SCADA à communiquer à distance via des connexions non chiffrées.

De plus, les solutions d'authentification sont souvent configurées avec de faibles mots de passe, voire avec des mots de passe par défaut. Ces derniers, disponibles sur Internet, laissent

le système complètement ouvert aux attaquants. Les sections suivantes abordent les problèmes de sécurité rencontrés dans les protocoles SCADA, notamment l'IEC 60870-5-104, le DNP3 et le Modbus TCP. Bien que de nombreux protocoles SCADA soient conçus pour être ouverts, robustes, fiables et faciles à utiliser, ils ne sont pas nécessairement orientés vers la fourniture d'une communication sécurisée.

2.7.1 IEC 60870-5-104

Le protocole IEC 60870-5-104 ne réalise aucun calcul de somme de contrôle (checksum). Celui-ci était inclus dans la trame IEC 60870-5-101 utilisée pour la communication asynchrone. Désormais, le calcul de la somme de contrôle n'est plus effectué au niveau de la couche application (couche 5) mais est délégué à la couche transport (couche 4).

- **Absence de Confidentialité :** Tous les messages IEC 60870-5-104 sont transmis en clair sur le réseau.
- **Absence d'Intégrité :** Aucune vérification d'intégrité n'est intégrée au protocole IEC 60870-5-104.
- **Absence d'Authentification :** Le protocole IEC 60870-5-104 ne comporte aucun mécanisme d'authentification.

2.7.2 DNP3

Le protocole DNP3 transmet toutes les données en clair sur le réseau. À la différence de l'IEC 60870-5-104 et du Modbus, DNP3 effectue un contrôle de redondance cyclique (CRC) en divisant les données en blocs, chaque bloc contenant une paire d'octets CRC pour chaque 16 octets de données, à l'exception du dernier bloc.

- **Absence de Confidentialité :** Tous les messages DNP3 sont transmis en clair sur le réseau.
- **Absence d'Authentification :** Le protocole DNP3 ne comporte aucun mécanisme d'authentification.
- **Absence d'Intégrité :** Le CRC ne détecte que les défauts aléatoires. Si un attaquant modifie intentionnellement le contenu d'une trame DNP3, le champ CRC peut être recalculé.

2.7.3 Modbus TCP

Le protocole Modbus TCP présente de nombreuses vulnérabilités qui pourraient permettre à un attaquant de mener des activités de reconnaissance ou d'envoyer des commandes arbitraires.

- **Absence de Confidentialité :** Tous les messages Modbus sont transmis en clair sur le réseau.
- **Absence d'Intégrité :** Aucune vérification d'intégrité n'est intégrée au protocole Modbus.
- **Absence d'Authentification :** Il n'y a aucun mécanisme d'authentification à quelque niveau que ce soit du protocole Modbus.
- **Encadrement Simpliste :** Les trames Modbus sont envoyées via des connexions TCP établies. Bien que ces connexions soient généralement fiables, elles présentent un inconvénient majeur car TCP ne préserve pas les limites des enregistrements.

- **Absence de Structure de Session :** Le protocole Modbus TCP est composé de transactions courtes, où le client initie une requête qui entraîne une action unique du serveur. Combiné à l'absence d'authentification et à la faible génération de numéros de séquence initiale TCP (ISN) dans de nombreux dispositifs embarqués, il devient possible pour des attaquants d'injecter des commandes sans connaître la session en cours.

2.7.4 IEC 62351

L'IEC 62351 est un ensemble de normes créé par la Commission Électrotechnique Internationale (IEC) pour traiter les problèmes de sécurité dans les protocoles de communication SCADA, y compris les protocoles IEC 60870-5-104 et DNP3. Ces normes visent différents objectifs de sécurité, notamment l'authentification et le chiffrement des données.

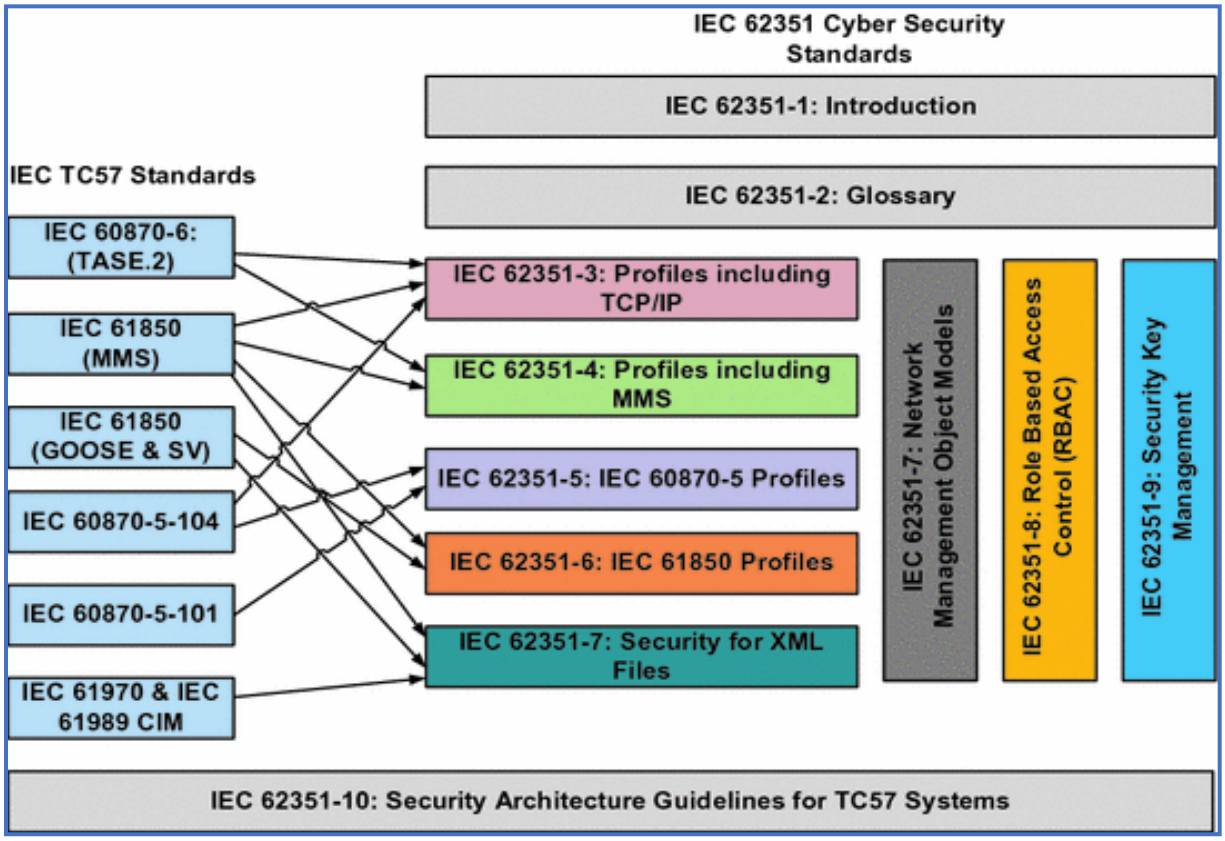


FIGURE 2. 21 : Interrelations entre les normes IEC TC57 et IEC 62351 (ERSAN KABALCI, 2019)

- **Authentification :** L'authentification des entités, grâce à l'utilisation de signatures numériques, garantit que seuls les utilisateurs autorisés peuvent accéder aux systèmes.
- **Chiffrement TLS :** Ce mécanisme empêche les attaques d'écoute clandestine en chiffrant les données échangées entre les entités de communication.
- **Protection contre les attaques de type Man-in-the-Middle :** L'authentification des entités prévient ce type d'attaque en s'assurant que les parties qui communiquent sont bien celles qu'elles prétendent être.
- **Protection contre le spoofing :** L'utilisation de certificats de sécurité prévient l'usurpation d'identité en garantissant l'authenticité des entités.

- **Protection contre les attaques par rejeu :** Le chiffrement TLS empêche ces attaques, qui consistent à réutiliser des messages anciens pour tromper le système.

Cependant, le chiffrement TLS ne protège pas contre les attaques par déni de service (DoS).

La figure 23 montre la relation entre les standards de communication IEC et les normes de sécurité IEC.

2.7.5 Différence entre DNP3 et Modbus

TABLEAU 2. 2 : Différence entre DNP3 et MODBUS

DNP3	Modbus
Développé en 1993 par Harris	Développé en 1979 par Modicon
Utilise des bits pour la communication	Utilise des descriptions textuelles pour la transmission des données
Composé de trois couches : physique, liaison de données et application	Composé uniquement de la couche application
Supporte plusieurs esclaves, plusieurs maîtres et la communication de pair à pair	Supporte uniquement la communication de pair à pair
Les paramètres de configuration incluent le débit en bauds, la taille des fragments et les adresses des dispositifs	Les paramètres de configuration incluent le mode parité, le mode ASCII/RTU, et le débit en bauds

2.8 SECURITE DES ICS/SCADA

Avec l'évolution des architectures SCADA et des technologies de communication, les systèmes SCADA modernes deviennent de plus en plus vulnérables aux cyberattaques physiques, ciblant non seulement les infrastructures matérielles, mais également les réseaux de communication et les centres de contrôle. Les cyberattaques sont devenues une option privilégiée pour des adversaires malveillants cherchant à saboter des infrastructures critiques, car elles sont moins coûteuses, plus sûres, et plus simples à exécuter que les attaques physiques traditionnelles. Dans certains cas, les attaquants coordonnent les actions cybernétiques et physiques pour maximiser les dégâts (Fouladirad, 2005).

Des efforts de recherche considérables ont été menés pour améliorer la sécurité des systèmes SCADA contre ces cybermenaces. Par exemple, Nazir, (Nazir & Shushma Patel, 2017) proposent une classification des différentes méthodes de sécurisation des SCADA. Pour élaborer une stratégie efficace de protection contre les attaques malveillantes, il est essentiel d'évaluer les vulnérabilités des systèmes SCADA et d'analyser les cyberattaques déjà survenues. L'étude des vulnérabilités permet d'identifier les points faibles du système et la manière dont ils pourraient être exploités. Parallèlement, l'analyse des cyber incidents passés permet de mieux comprendre les méthodes utilisées lors d'attaques antérieures, facilitant ainsi le développement de mesures de protection visant à prévenir les futures attaques.

2.8.1 Vulnérabilités des systèmes SCADA

Les vulnérabilités dans les protocoles de communication des composantes SCADA, ont amplifié les risques de cyberattaques. Ces nouvelles menaces ciblent des infrastructures critiques qui s'appuient sur des réseaux SCADA. Durant la dernière décennie, plusieurs cyberattaques intentionnelles ont exploité les vulnérabilités de ces systèmes industriels, permettant aux attaquants d'obtenir un accès non autorisé aux réseaux SCADA, de collecter des données sensibles échangées entre les installations et les opérateurs, et de déployer des malwares perturbant les processus.

Quelques vulnérabilités majeures des SCADA sont identifiées par (Fovino, 2013):

1) Les vulnérabilités architecturales :

Les architectures SCADA modernes restent fondamentalement similaires à celles des années 80 et 90, mais avec un passage d'un environnement isolé à un environnement ouvert. Cette évolution rend les SCADA modernes plus exposés aux cyberattaques. Par exemple, les réseaux SCADA stockent souvent les données des processus dans des unités d'historisation accessibles via le réseau de l'entreprise, ce qui peut ouvrir une porte aux malwares depuis ce réseau. De plus, l'utilisation d'applications web pour surveiller les processus physiques crée une connexion directe à Internet, augmentant le risque d'intrusion. Les points d'accès locaux aux appareils de terrain représentent aussi une faille potentielle pour des attaques. Enfin, les attaquants peuvent accéder aux systèmes SCADA via le réseau du fournisseur, souvent intégré aux systèmes SCADA modernes (Y. Yuan, 2011).

2) Les vulnérabilités des protocoles de communication :

Historiquement, les concepteurs de SCADA n'ont pas suffisamment pris en compte les mécanismes de sécurité tels que l'intégrité des données, l'authentification ou la protection contre les attaques de rejeu, car ces systèmes étaient initialement isolés. Les protocoles de communication SCADA, tels que Modbus, DNP3, et Allen-Bradley Ethernet/IP, manquent souvent de fonctions d'authentification garantissant l'origine et la validité des données réseau (Reaves, 2009).

Cette absence rend ces systèmes vulnérables à des attaques par déni de service (DoS), des attaques de type "man-in-the-middle" et des attaques par rediffusion. Alors que les anciens systèmes SCADA, basés sur des protocoles propriétaires, étaient considérés comme sûrs grâce à la "sécurité par obscurité", cette approche est désormais obsolète dans les infrastructures modernes, où des protocoles communs comme Ethernet, TCP/IP et des réseaux sans fil sont utilisés (Wei Gao et Morris, 2010).

3) Les vulnérabilités des logiciels et du matériel :

La complexité croissante des systèmes SCADA en termes de logiciels et de matériel a conduit à l'apparition de nombreuses vulnérabilités. Parmi les failles logicielles courantes, on trouve les dépassements de tampon, les injections SQL et les erreurs de format de chaîne (Zhu, 2011). Par exemple, certains incidents de cybersécurité ont été provoqués par des vulnérabilités dans le logiciel MS-SQL. De plus, étant des systèmes en temps réel, les SCADA ne peuvent pas facilement implémenter des algorithmes de chiffrement traditionnels, ce qui expose ces systèmes à des attaques d'intégrité.

4) Les vulnérabilités des politiques de sécurité :

Certaines politiques de sécurité, comme l'application de correctifs et les mises à jour antivirus, peuvent affaiblir les systèmes SCADA. Par exemple, accéder à Internet pour ces mises à jour peut introduire des logiciels malveillants, et le redémarrage nécessaire après une mise à jour peut perturber des systèmes critiques. Un exemple notable est l'arrêt d'une centrale nucléaire suite à une mise à jour logicielle (Tolo, 2019). Il est donc conseillé d'appliquer ces correctifs avec prudence pour préserver l'isolement des réseaux SCADA.

CHAPITRE 3
CYBERSECURITE DES SYSTEMES DE CONTROLE INDUSTRIEL (ICSS): spécificités, enjeux et défis associés

CHAPITRE 3 CYBERSECURITE DES SYSTEMES DE CONTROLE INDUSTRIEL (ICSS) : SPECIFICITES, ENJEUX ET DEFIS ASSOCIES

3.1 SYSTEMES DE CONTROLE INDUSTRIELS (ICS) ET CYBERATTAQUES

3.1.1 Introduction

La cybersécurité dans les installations industrielles est devenue une préoccupation très importante au cours de la dernière décennie (Schwab, 2018). La fréquence et la gravité des cyberattaques contre les infrastructures critiques ont considérablement augmenté (par exemple, l'attaque Stuxnet en 2010, l'attaque Flame en 2012 (Flaus J.-M. , 2018). De plus, de nombreux systèmes informatiques de traitement de l'information (TI) sont victimes d'attaques qui peuvent se propager rapidement et avoir un impact important, comme Wanacry (Flaus J.-M. , 2018). De plus, les professionnels de la sécurité identifient régulièrement des vulnérabilités dans les systèmes de contrôle. Les systèmes informatiques sont utilisés pour contrôler les systèmes physiques depuis les années 1960.

Cependant, ces systèmes étaient difficiles à mettre en place et à programmer. Pour cette raison, un nouveau dispositif appelé « PLC » a été développé par Modicon en 1968 (Flaus J.-M. , 2018). Cela simplifie l'installation du matériel et permet l'utilisation de langages de programmation plus simples. Ces systèmes étaient à l'origine utilisés pour contrôler de grands systèmes. Plus tard, dans le cadre de la miniaturisation, ces systèmes ont été intégrés dans des systèmes physiques, pour finalement aboutir à des dispositifs de dimensions compactes dotés de certaines capacités de traitement et de communication, appelés systèmes cyber-physiques.

Dans de nombreux cas, ces systèmes peuvent se connecter directement à Internet à l'aide de protocoles de communication du monde informatique, créant ainsi l'Internet des objets. Les problèmes de sécurité informatique deviennent donc de plus en plus graves.

Ce bref rappel historique illustre la différence de philosophie entre les mondes IT et OT, et comment le monde OT, initialement peu intéressé par les questions de sécurité informatique, est finalement devenu obsédé par ces questions.

C'est très réel maintenant et cela prend de plus en plus d'ampleur. De nombreux fabricants sont influencés par la modernisation et la numérisation de leurs systèmes de contrôle et de gestion. Ces industries abritent des fabricants de systèmes critiques qui ont un impact direct sur les utilisateurs, tels que les voitures, les avions, les trains et les implants médicaux.

Certaines entreprises possèdent des infrastructures à grande échelle telles que des centrales électriques et des raffineries de pétrole. Même si c'est différent., toutes ces industries partagent aujourd'hui le même défi de protéger leurs systèmes critiques des risques de cybersécurité qui peuvent engendrer des impacts sur la sûreté de fonctionnement.

3.1.2 Systèmes de contrôle industriels (ICSs)

« Système de contrôle industriel » est un terme ou une désignation générale qui regroupe plusieurs systèmes tels que (Riad, 2021) :

Contrôle de surveillance et acquisition de données (SCADA) Un système de contrôle et d'acquisition de données couramment utilisé pour les systèmes géographiquement étendus. Ceux-ci sont constitués de matériel et de logiciels provenant de différents fournisseurs et sont combinés en un seul système par un intégrateur.

Les systèmes de contrôle distribués (DCS) relèvent généralement de la responsabilité d'un seul fournisseur.

Les ICS sont constitués de plusieurs systèmes physiques (électriques, mécaniques, hydrauliques, pneumatiques, etc.) qui doivent réaliser conjointement des tâches et des fonctions industrielles (chaînes de production, systèmes de transport, production d'énergie, etc.). Ces ICS sont utilisés pour contrôler et surveiller les infrastructures critiques telles que les centrales nucléaires et les installations de production de pétrole et de gaz.

Les systèmes de contrôle industriels sont généralement constitués de dispositifs et de systèmes spécialisés ou conventionnels qui peuvent être classés comme suit (Flaus J.-M. , 2018):

- **Premièrement**, les systèmes informatiques qui ressemblent aux systèmes traditionnels (ordinateurs de bureau traditionnels, serveurs et réseaux, imprimantes, systèmes de stockage).
- **Le second** est un ensemble de dispositifs spéciaux qui permettent de prendre des mesures, de répondre aux systèmes physiques et de communiquer avec les manipulateurs.
  Cette catégorie comprend, entre autres, les automates programmables (PLC - programmable logic contrôleurs), les systèmes de surveillance (HMI - interface homme machine, SCADA), les systèmes de diagnostic de télémaintenance industrielle, les capteurs et actionneurs.

Le terme « IACS – Industrial Automation Control System » a été proposé par l'ISA dans les années 2000 et adopté sous la forme simplifiée « ICS » en 2008 NIST (National Institute of Standards and Technology) Guide 800-82 (NIST (SP) 800-82, 2011). Cependant, la définition ICS de la norme CEI 62443 est plus large et inclut également des éléments logiciels et matériels qui assurent le bon fonctionnement des processus industriels, tels que : SCADA, DCS, HMI, PLC, RTU (Remote Terminal Unit), dispositif électronique intelligent (IED), système d'instrumentation de sécurité (SIS) et systèmes d'information associés, etc. À mesure que la connectivité au monde Internet s'est développée à des fins commerciales, ICS a adopté des technologies basées sur Internet et la plupart des protocoles de communication ont été repensés pour fonctionner sur Protocole IP. Cette ouverture expose les composants ICS et les protocoles de communication aux cyberattaques, créant un risque plus élevé que les attaques contre les systèmes informatiques traditionnels.

La norme IEC 62264-1 donne et propose un modèle d'architecture en cinq niveaux clés pour l'entreprise basés sur la hiérarchie fonctionnelle (Kriaa, 2016) :

TABLEAU 3. 1 : Les différents niveaux du modèle purdue

Nom	Description
Niveau 0 : Cellule et zone	Le niveau 0 est constitué d'un large éventail de capteurs, d'actionneurs et de dispositifs impliqués dans le processus de fabrication de base. Ces

	dispositifs exécutent les fonctions de base du système industriel d'automatisation et de contrôle, telles que : - Entraînement d'un moteur - Mesure de variables - Définition d'une sortie - Exécution de fonctions clés (par exemple peinture, soudage et pliage)
Niveau 1 : Contrôle du processus	Le niveau 1 comprend des contrôleurs intégrés qui contrôlent et manipulent le processus de fabrication et dont la fonction principale est de communiquer avec les dispositifs de niveau 0. En production discrète, ces dispositifs sont des contrôleurs logiques programmables (PLC) ou des unités de télémétrie à distance (RTU). Dans l'industrie de type process, le contrôleur de base est appelé un système de contrôle distribué (DC).
Niveau 2 : Supervision	Le niveau 2 représente les systèmes et fonctions associés à la supervision et à l'exploitation du runtime d'une zone d'une installation de production. Il s'agit généralement des éléments suivants : - Interfaces d'opérateur ou interfaces homme-machine (IHM) - Alarmes ou systèmes d'alerte - Historique des processus et systèmes de gestion des lots - Stations de travail de la salle de contrôle Ces systèmes communiquent avec les PLC et les RTU du niveau 1. Dans certains cas, ils communiquent ou partagent des données avec les systèmes et les applications du site ou de l'entreprise (niveau 4 et 5). Ces systèmes sont principalement basés sur des équipements informatiques et des systèmes d'exploitation standard (Unix ou Microsoft Windows).
Niveaux 3 et 3,5 : Niveau de site et réseau de périmètre industriel	Le niveau de site représente le niveau le plus élevé de systèmes d'automatisation et de contrôle industriels. Les systèmes et les applications qui existent à ce niveau gèrent les fonctions d'automatisation et de contrôle industrielles à l'échelle du site. Les niveaux 0 à 3 sont considérés comme critiques pour les opérations du site. Les systèmes et fonctions qui existent à ce niveau peuvent inclure les éléments suivants : - Rapports de production (par exemple durées de cycle, index de qualité et maintenance prédictive) - Historique de l'usine - Planification détaillée de la production - Gestion des opérations au niveau du site – Gestion des dispositifs et du matériel - Serveur de lancement des correctifs - Serveur de fichiers - Domaine industriel, Active Directory et serveur de terminal Ces systèmes communiquent avec la zone de production et partagent des données avec les systèmes et applications de l'entreprise (niveau 4 et 5).
Niveaux 4 et 5 : Réseaux de l'entreprise	Les niveaux 4 et 5 représentent le réseau du site ou de l'entreprise sur lequel se trouvent les fonctions et les systèmes informatiques centralisés. L'organisation informatique gère directement les services, les systèmes et les applications à ces niveaux.

- **Niveau 0** (Processus physique) : le niveau du bus de terrain est consacré au contrôle (mesure avec les capteurs) et à la commande (avec les actionneurs) du système physique.
- **Niveau 1** (Contrôle local) : le niveau du procédé est dédié à la supervision et à la prise de décision, il permet donc de piloter les équipements de niveau 0. Ce niveau contient des dispositifs qui interviennent directement dans le processus de contrôle industriel comme le PLC et RTU, etc. Ces appareils permettent de lire les mesures des capteurs, exécuter des algorithmes, commander les actionneurs et enregistrer l'état du système physique.
- **Niveau 2** (Supervision) : il comprend les interfaces homme-machine (IHM), les systèmes de contrôle et d'acquisition de données (SCADA) et les systèmes distribués (DCS).
- **Niveau 3** (Gestion des opérations) : le niveau usine est destiné à la gestion de la production en fonction de la demande d'ateliers (le plus souvent, par le biais d'un système MES - Manufacturing Execution System). Une partie du système de supervision peut aussi se situer à ce niveau (Flaus J.-M. , 2018).
- **Niveau 4 et 5** (Entreprise) : le niveau entreprise concerne les fonctions impliquées dans les activités liées à l'entreprise nécessaires afin de gérer l'organisation de la fabrication.

Les dispositifs qui sont directement impliqués dans le processus de contrôle industriel sont particulièrement situés aux niveaux 0, 1 et 2.

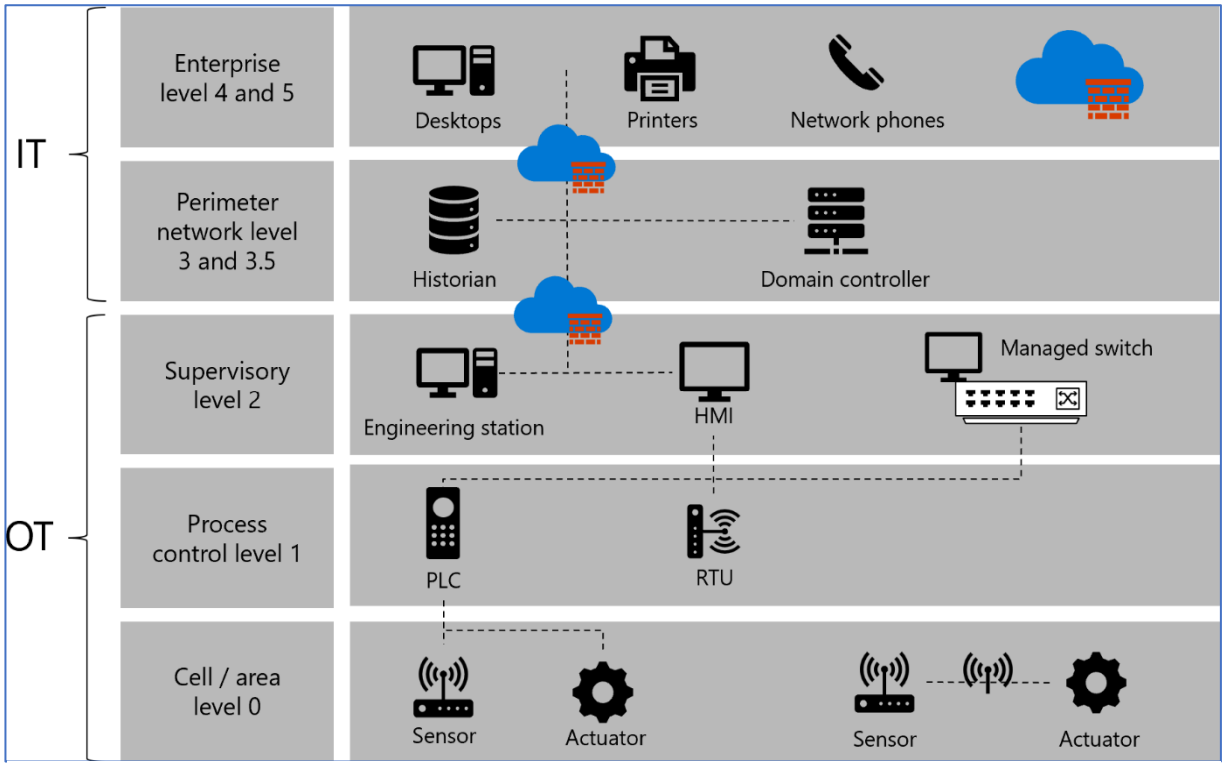


FIGURE 3. 1 : MODELE DE PURDUE DE L'ARCHITECTURE D'UN ICS (WAINSTEIN, 2024)

3.1.3 ICS/OT et défis de sécurité

Différences entre la sécurité des systèmes IT et OT

La sécurisation des environnements ICS/OT pose des défis uniques en raison de plusieurs différences clés avec les systèmes IT traditionnels :

- **Disponibilité continue :** Contrairement aux systèmes IT où les arrêts temporaires pour maintenance et mises à jour sont fréquents, les systèmes OT nécessitent une opération continue. Toute interruption peut gravement affecter la production ou les services critiques.
- **Longévité des systèmes :** Les environnements OT dépendent souvent de systèmes fonctionnant sur plusieurs décennies. Par conséquent, ces systèmes utilisent fréquemment des technologies obsolètes, dépourvues des fonctionnalités de sécurité modernes, les rendant vulnérables aux menaces actuelles (VERVE, 2024).
- **Opérations en temps réel :** Les systèmes ICS/OT nécessitent des communications instantanées et hautement disponibles pour répondre rapidement aux changements opérationnels. Cette exigence de faible latence implique que certaines mesures de sécurité, telles que le chiffrement ou la détection d'intrusions, peuvent introduire des délais inacceptables (Balbix, Inc, 2024).

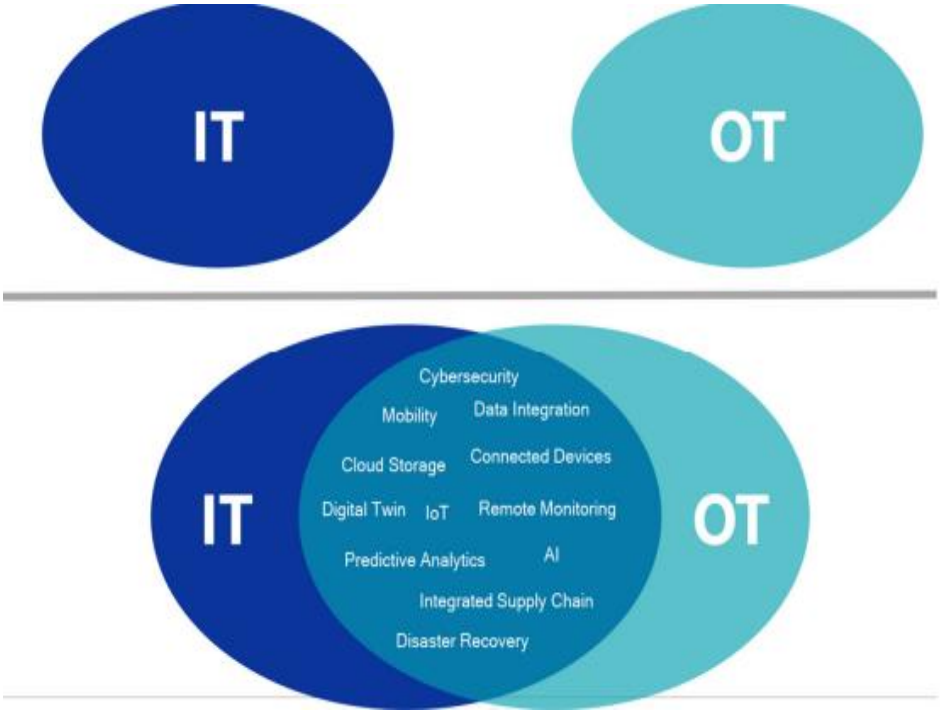


FIGURE 3. 2 : Convergence IT-OT

Défis de sécurité courants

- **Systèmes hérités :** De nombreux environnements ICS/OT utilisent des systèmes anciens avec des matériels et logiciels obsolètes, conçus sans tenir compte des exigences de cybersécurité modernes, ce qui les rend difficiles à sécuriser contre les menaces actuelles (Ruchi Bisht in InfoSecTrain, 2024).
- **Absence de chiffrement :** Les protocoles de communication industrielle n'intègrent souvent pas de mécanismes de chiffrement.
- **Limites des correctifs :** L'application de correctifs de sécurité est complexe dans les systèmes ICS/OT en raison des préoccupations liées à la stabilité des systèmes et à la nécessité d'une exploitation continue. Cela ralentit considérablement la correction des vulnérabilités (VERVE, 2024).

- **Dépendance à la sécurité physique :** Historiquement, les systèmes ICS/OT se sont appuyés sur des mesures de sécurité physique pour empêcher tout accès non autorisé. Cependant, l'introduction de technologies d'accès à distance les a exposés à de nouvelles menaces numériques (Nozomi Networks, 2023).

3.2 VECTEURS D'ATTAQUE DANS LES ENVIRONNEMENTS ICS/OT

3.2.1 Techniques d'Attaque Courantes :

- **Hameçonnage (Phishing) et Ingénierie Sociale :** Les attaques par hameçonnage représentent une menace prévalente dans les environnements ICS, ciblant souvent les employés ayant accès à des systèmes critiques. Les cybercriminels envoient des courriels trompeurs pour inciter les individus à révéler des informations sensibles ou à télécharger des logiciels malveillants, qui peuvent ensuite se propager dans le réseau ICS, perturbant les opérations et pouvant causer des dommages matériels.
- **Malwares (par exemple, Stuxnet, Triton/Trisis) :** Les malwares spécifiquement conçus pour les environnements ICS posent des risques significatifs. Des exemples notables incluent Stuxnet, qui a ciblé les installations nucléaires iraniennes, et Triton/Trisis, qui visait à manipuler les systèmes de sécurité dans des installations industrielles. Ces variantes de malwares peuvent altérer les commandes de contrôle et perturber les processus industriels, mettant en évidence les vulnérabilités des systèmes hérités souvent dépourvus de fonctionnalités de sécurité modernes.
- **Attaques par Déni de Service (DoS) :** Les attaques par déni de service visent à perturber la disponibilité des services dans les environnements ICS en saturant les systèmes avec un trafic excessif ou en exploitant des vulnérabilités pour les faire tomber. De telles attaques peuvent paralyser les opérations et créer des dangers pour la sécurité, les rendant particulièrement nuisibles dans le contexte des infrastructures critiques.
- **Menaces Internes :** Les menaces internes constituent un défi unique pour la sécurité des systèmes ICS, en raison de l'accès légitime que les employés ou les contractuels ont aux systèmes sensibles. Les employés malveillants peuvent tirer parti de leurs connaissances et de leur accès pour un gain personnel ou par vengeance, entraînant d'importantes perturbations opérationnelles.
- **Attaques sur la Chaîne d'Approvisionnement :** Les vulnérabilités de la chaîne d'approvisionnement peuvent être exploitées par des attaquants sophistiqués qui compromettent les réseaux informatiques des fournisseurs fournissant de l'équipement aux environnements ICS. En insérant des composants malveillants lors de la livraison ou de l'installation, les attaquants peuvent accéder de manière non autorisée à des systèmes critiques et manipuler les opérations sans être détectés.

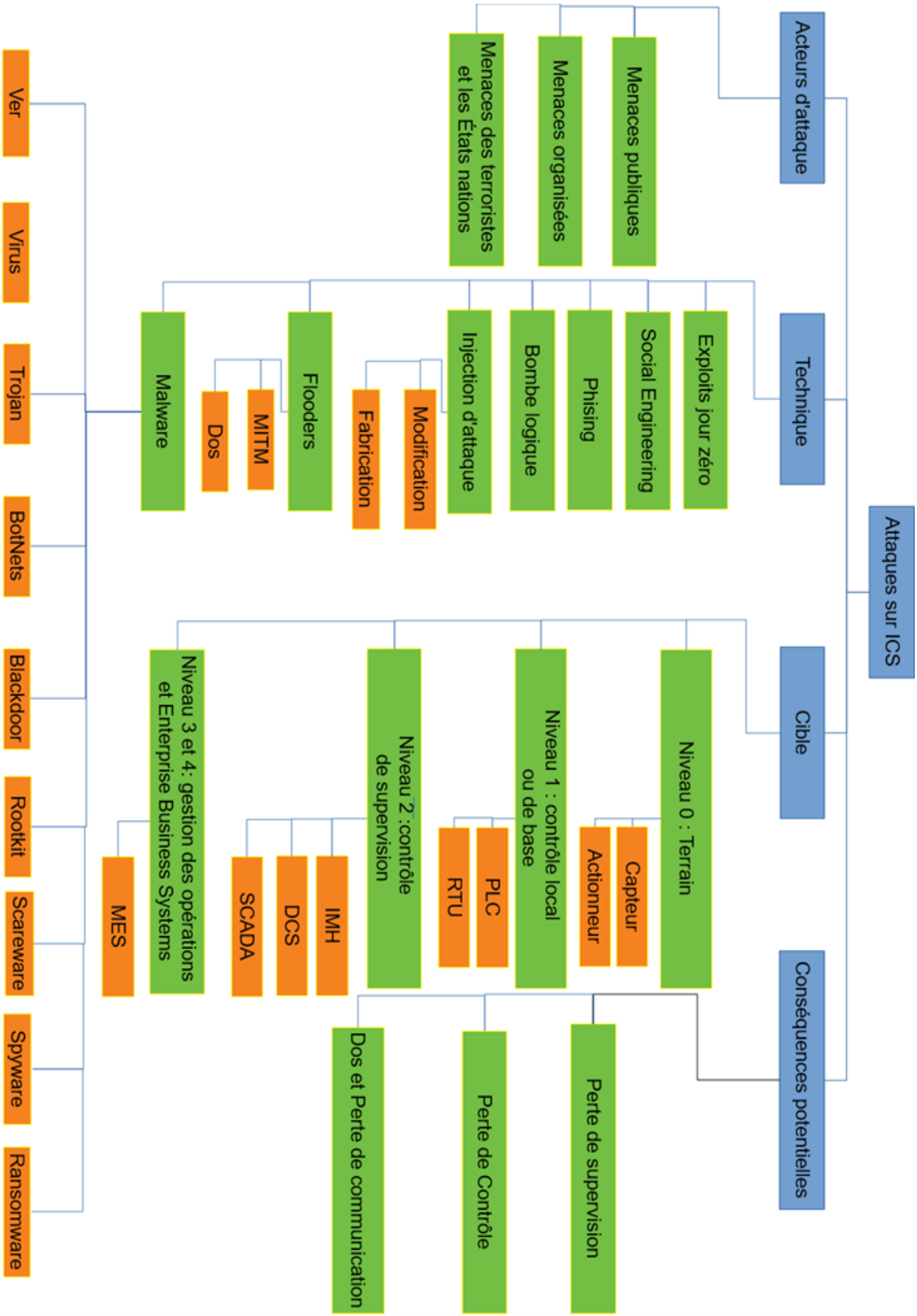


FIGURE 3. 3 : Taxonomie des attaques des ICSS

3.2.2 Cybers incidents survenus aux systèmes SCADA

La dépendance croissante des systèmes SCADA à Internet les expose à des menaces significatives de cyberattaques, principalement en raison des vulnérabilités inhérentes aux protocoles de communication utilisés dans ces réseaux.

Voici une chronologie des principaux cyber-incidents impliquant des systèmes SCADA :

- **Explosion d'un pipeline en Russie (1999) :** En 1999, des pirates informatiques ont infiltré Gazprom, la plus grande entreprise de gaz russe, grâce à un complice parmi les employés. Ils ont utilisé un cheval de Troie pour prendre le contrôle du tableau de distribution central régissant le flux de gaz, un incident rapporté en 2000 par le ministère de l'Intérieur Russie.
- **Maroochy, Australie (2000) :** En 2000, un ancien employé mécontent a utilisé un ordinateur portable et un émetteur radio pour manipuler 150 stations de pompage des eaux usées dans le comté de Maroochy, Queensland. Pendant trois mois, il a déversé un million de litres d'eaux usées non traitées dans les cours d'eau locaux, motivé par sa colère après avoir échoué à obtenir un emploi au Conseil du comté de Maroochy.
- **Infection par ver dans une centrale nucléaire - Slammer aux États-Unis (2003) :** En janvier 2003, le ver Slammer a infiltré un réseau privé de la centrale nucléaire de Davis-Besse, dans l'Ohio, désactivant un système de surveillance de sécurité pendant près de cinq heures. Malgré la croyance que le réseau était protégé par un pare-feu, le ver a exploité les vulnérabilités du MS-SQL, perturbant considérablement les opérations de la centrale.
- **Panne de la centrale de production hydroélectrique de Taum Sauk aux États-Unis (2005) :** Bien que cet incident du 14 décembre 2005 n'ait pas été causé par une attaque, il a mis en lumière des défaillances dans la conception, l'instrumentation et la gestion humaine, entraînant l'effondrement d'un réservoir. Ce type de faiblesse peut être exploité pour mener des attaques indétectables dans des infrastructures critiques.
- **Stuxnet en Iran (2010) :** Découvert en 2010, le malware Stuxnet a ciblé les automates des centrifugeuses nucléaires iraniennes. Il a réussi à installer un programme malveillant en remplaçant de manière indétectable le fichier original des automates, provoquant des fluctuations de vitesse entraînant la destruction des centrifugeuses.
- **Telvent au Canada (2012) :** Une brèche dans les systèmes de sécurité de Telvent Canada, une entreprise fournissant des outils de surveillance au secteur de l'énergie, a été découverte le 10 septembre 2012. Les intrus ont volé des fichiers de projets liés à OASyS SCADA, ce qui pourrait avoir permis de mieux préparer des attaques futures.
- **Shamoon en Arabie Saoudite (2012) :** En 2012, le logiciel malveillant Shamoon a été utilisé pour des cyberespionnage ciblant une entreprise pétrochimique au Moyen-Orient. L'attaque a effacé les données de milliers de postes de travail, rendant les systèmes inaccessibles en altérant le Master Boot Record (MBR).
- **Empoisonnement de l'eau potable aux États-Unis (2013) :** Le 26 avril 2013, un incident à la station d'épuration de Carters Lake a vu quelqu'un manipuler les niveaux de chlore et de fluorure, soulignant le potentiel de cyberattaques dans les systèmes d'eau connectés à Internet.
- **BlackEnergy en Ukraine (2015) :** Utilisé pour des attaques DDoS et de cyberespionnage, le cheval de Troie BlackEnergy a été déployé contre des systèmes SCADA dans le secteur

de l'énergie, montrant un niveau de compétence supérieur à celui des attaques de DDoS traditionnelles

- **Attaque d'un pipeline aux États-Unis (2018) :** En mars 2018, une attaque massive a compromis les systèmes de données des gazoducs américains, exploitant un système de communication électronique d'un fournisseur.

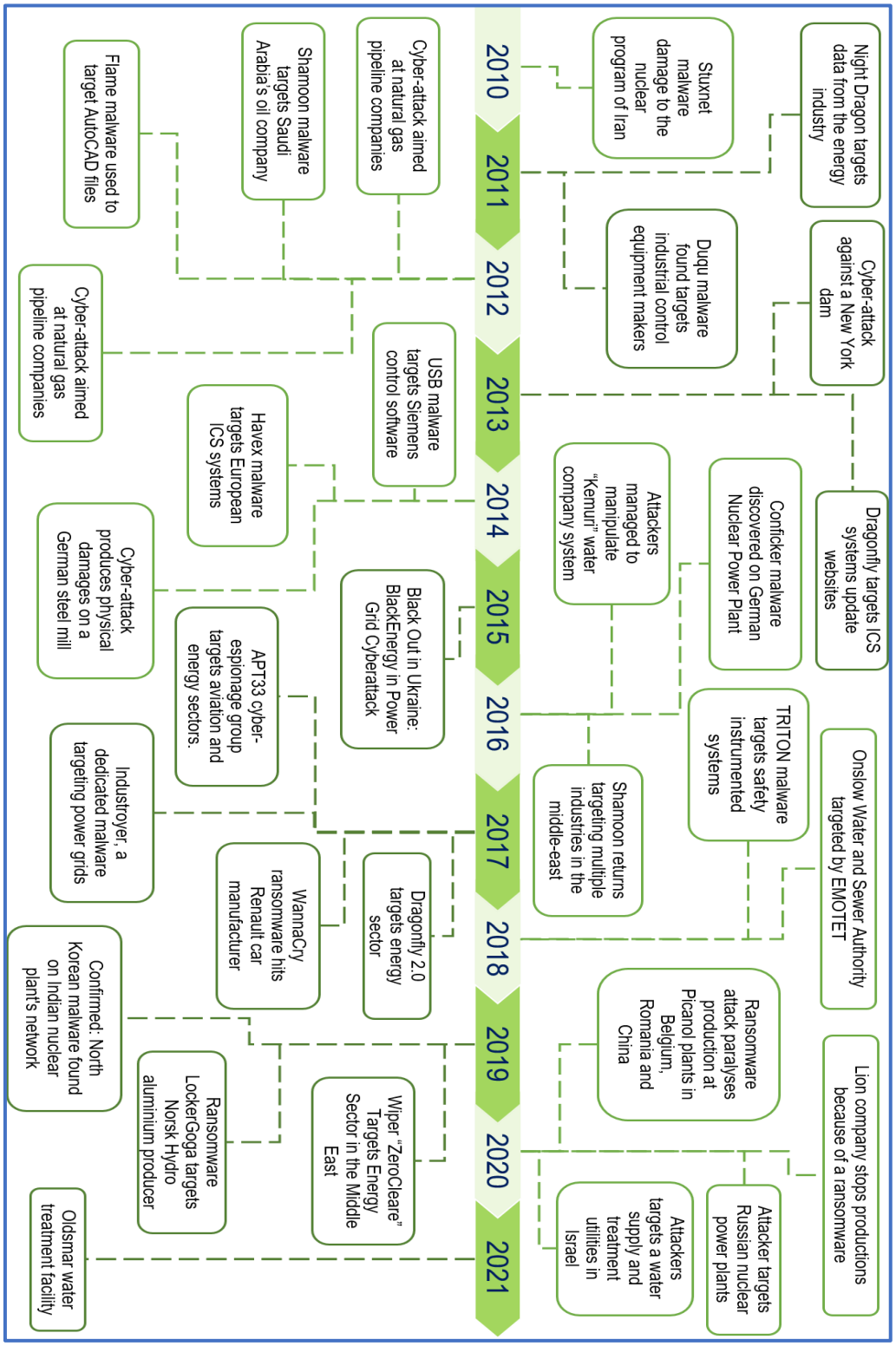


FIGURE 3. 4 : Chronologie des cyberattaques impactant les entreprises industrielles

3.3 LA SECURITE DES TECHNOLOGIES OPERATIONNELLES (OT) EST DIFFERENTE DE CELLE DES TECHNOLOGIES DE L'INFORMATION (IT)

Il est fréquent de croire, à tort, que la sécurité des systèmes de contrôle industriel (ICS) n'est qu'une extension de la sécurité des réseaux informatiques (IT), bien maîtrisée et pour laquelle il existe de nombreux outils. Cependant, bien que les ICS fonctionnent souvent au sein de réseaux IT, les composants matériels et logiciels qui commandent les systèmes industriels, désignés sous le terme de technologies opérationnelles (OT), posent des défis de cybersécurité fondamentalement distincts de ceux des systèmes IT traditionnels.

Tout d'abord, les objectifs de la sécurité IT et de la sécurité OT sont différents : la sécurité IT vise à garantir l'intégrité et la disponibilité des données, tandis que la sécurité OT se concentre sur le bon fonctionnement et la sécurité des systèmes industriels physiques. De plus, les protocoles de communication entre les composants des ICS ne sont souvent pas standardisés, contrairement aux réseaux IT, ce qui rend difficile l'automatisation des approches de sécurité.

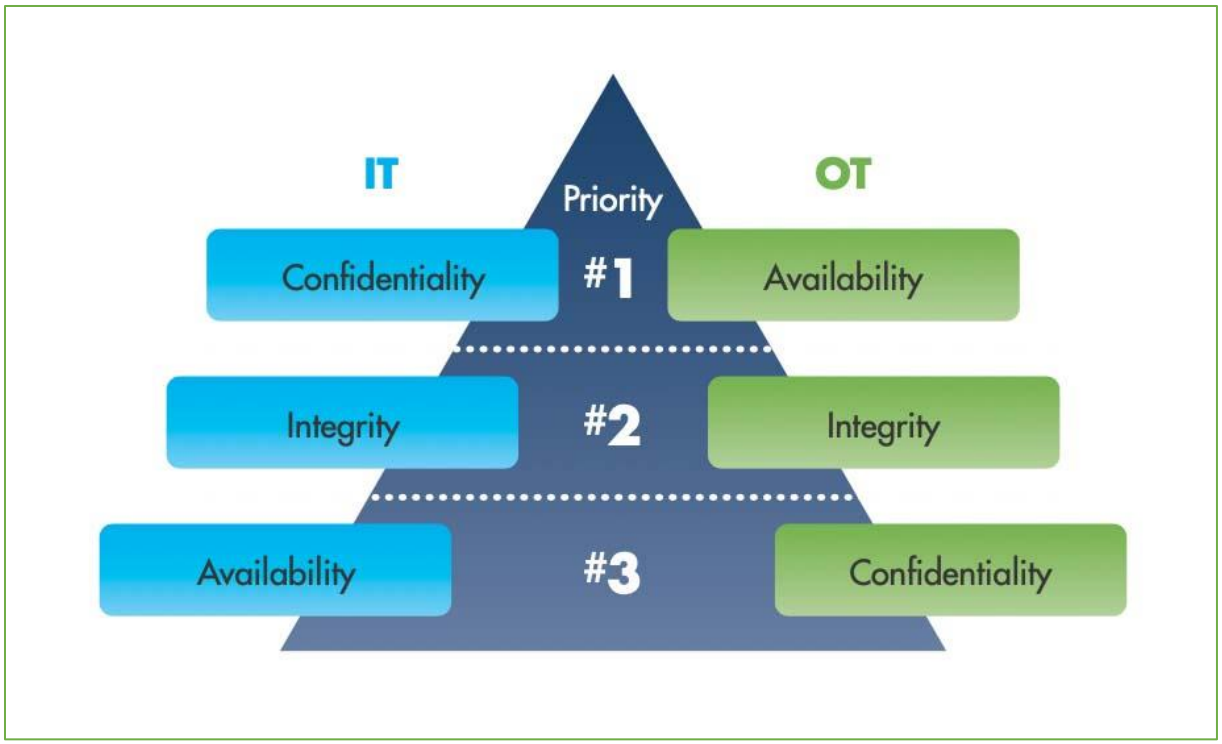


FIGURE 3. 5 : Priorités de la triade de la CIA

De nombreux processus industriels exigent une coordination précise et ne tolèrent pas les délais de latence, ce qui rend problématique l'utilisation de fonctions de sécurité courantes dans l'IT, telles que le chiffrement et l'authentification des paquets. En outre, toute modification d'un ICS en fonctionnement introduit un risque dans le système de manière difficile à prévoir, ce qui pousse souvent les ingénieurs à résister aux mises à jour ou correctifs de sécurité, par crainte de provoquer des pannes inattendues ou d'ajouter de la latence.

Cela signifie que de nombreuses mesures de sécurité IT de base, comme des pare-feux stricts, des politiques restrictives d'accès utilisateur local, et des mises à jour fréquentes de sécurité, sont souvent inadaptées pour un ICS. Contrairement aux infrastructures IT qui utilisent

des protocoles cohérents et bien définis et fonctionnent avec un nombre relativement limité de types de matériels tels que les routeurs, commutateurs réseau, serveurs et postes de travail, les écosystèmes ICS sont beaucoup plus variés et il existe bien moins d'outils de sécurité commerciaux adaptés à ces environnements.

Les modèles et outils de sécurité IT ne pouvant être facilement appliqués aux environnements ICS en raison de leur fragilité, complexité et diversité, les responsables des installations se retrouvent souvent avec peu d'outils efficaces pour obtenir une visibilité claire sur leurs inventaires ICS, analyser les opérations ICS pour distinguer l'activité normale des anomalies, et intervenir en cas d'attaque. Pour de nombreuses installations, il est même difficile de savoir par où commencer les efforts de réduction des risques, étant donné l'ampleur et la portée de leurs opérations ICS. Il devient donc évident pour de nombreux composants du DoD que la sécurité des ICS nécessite une approche plus globale et adaptée.

3.3.1 Principales mesures de cybersécurité

Les spécifications jouent un rôle crucial dans la conception des systèmes de contrôle industriel (ICS). Des spécifications bien définies permettent d'intégrer des mesures de sécurité efficaces dès la phase de conception, renforçant ainsi la protection globale du système. Dans cette section, nous présenterons certaines des principales mesures mises en place en matière de cybersécurité pour les ICS, en gardant à l'esprit que cette liste n'est pas exhaustive.

Cryptographie

La cryptographie est un élément essentiel pour garantir la confidentialité, l'intégrité et l'authentification des données dans les systèmes industriels. Cependant, son application dans les systèmes de contrôle industriel (ICS) peut poser des défis en raison des limitations des ressources et de la nécessité de respecter les contraintes de temps réel. Par exemple, le chiffrement peut entraîner une surcharge des performances, et la vérification de l'intégrité des firmwares est complexe à cause de la nature propriétaire des automates programmables (PLC). Malgré ces défis, le contrôle d'authentification est réalisable avec certains protocoles de communication tels que DNPSec et OPC. Toutefois, l'authenticité des firmwares reste préoccupante, car de nombreux fabricants ne signent pas leurs produits, ce qui expose les systèmes à des vulnérabilités, comme celles exploitées lors de l'attaque Stuxnet.

Mises à jour régulières

Les mises à jour régulières (matérielles, logicielles, correctifs) dans les systèmes industriels peuvent être longues et coûteuses. Cette lenteur est due au fait que les mises à jour doivent être soigneusement testées pour éviter toute dégradation du système. Par conséquent, des évaluations des risques doivent être réalisées avant le déploiement des mises à jour, afin de peser les avantages de la réduction des risques de cybersécurité par rapport aux coûts potentiels, tels que les interruptions de production. Dans certains cas, les mises à jour peuvent être reportées et des mesures correctives alternatives mises en place si le risque est jugé acceptable.

Sauvegardes régulières

Les sauvegardes régulières sont essentielles pour restaurer les systèmes après des incidents, qu'ils soient causés par des cyberattaques ou des défaillances matérielles. Bien que des solutions existent pour sauvegarder les disques durs des serveurs SCADA, la sauvegarde des programmes des automates (PLC) est plus complexe en raison des protocoles propriétaires utilisés.

Antivirus

Les logiciels antivirus sont une mesure de cybersécurité de base. Toutefois, la détection traditionnelle basée sur les signatures est limitée, car de nouveaux virus, notamment les virus polymorphes, changent constamment. La détection heuristique est plus avancée, mais elle nécessite une quantité importante de mémoire et de ressources de traitement, ce qui peut entraîner des faux positifs. Dans les environnements ICS, ces faux positifs sont intolérables, car la suppression d'un fichier critique sur un serveur SCADA pourrait interrompre la production pendant des jours, voire entraîner des conséquences graves.

Contrôle d'accès logique

Les mesures de contrôle d'accès permettent de garantir le principe du moindre privilège, n'accordant l'accès qu'aux personnes qui en ont réellement besoin. Elles offrent également la traçabilité des activités des utilisateurs, ce qui est crucial pour les audits et la responsabilité.

Dispositifs de filtrage du réseau (pare-feu)

Les pare-feu filtrent le trafic réseau en fonction de règles prédéfinies, mais leur capacité à analyser les protocoles industriels est souvent limitée. Bien que Modbus TCP soit pris en charge par la plupart des pare-feu, il ne couvre qu'une fraction du marché des ICS. De plus, le filtrage ajoute de la latence, ce qui peut interférer avec les exigences strictes de temps de réponse des systèmes ICS, en particulier dans les couches 0 et 1 du modèle Purdue.

Système de détection d'intrusion (IDS)

Les systèmes de détection d'intrusion (IDS) offrent une protection puissante pour la cybersécurité dans les environnements où les changements sont peu fréquents, ce qui facilite la détection des anomalies. L'implémentation des IDS dans les ICS est cependant difficile, en raison des ressources mémoire et de calcul limitées dont disposent de nombreux dispositifs industriels. Les IDS surveillent les réseaux en temps réel à la recherche de comportements suspects ou de tentatives d'intrusion, en comparant les actions actuelles avec des modèles préétablis d'activités normales (détection d'anomalies) ou en utilisant des bases de données de menaces connues (détection basée

sur les signatures). Toutefois, les contraintes de performance des systèmes ICS peuvent limiter l'efficacité de ces solutions, car les délais introduits par la détection d'intrusions doivent être minimisés pour ne pas perturber les opérations. Malgré cela, les IDS sont essentiels pour identifier rapidement des attaques potentielles, prévenir les dommages et protéger les infrastructures critiques.

Systèmes de supervision

Les systèmes de supervision permettent de surveiller et de contrôler les événements en temps réel, en envoyant des alertes pour assurer des réponses rapides et efficaces en cas d'incidents imprévus. Ils collectent les données des outils de sécurité, tels que les pare-feu et les IDS. Toutefois, les informations fournies par les PLC sont souvent limitées en matière de cybersécurité, ce qui peut compliquer une détection complète des menaces.

3.3.2 Sécurité opérationnelle OPSEC (OPerationnelle SEC-urity)

L'un des objectifs principaux de l'OPSEC (Operations Security) est de protéger les informations sensibles d'une infrastructure, en empêchant leur exploitation par des adversaires. En ralentissant la capacité d'un attaquant à obtenir des informations critiques, on gagne du temps pour détecter les problèmes et restreindre l'accès aux informations et aux installations. Le processus OPSEC se décompose en cinq étapes essentielles :

- **Identification de l'information critique :** Déterminer quelles informations doivent être protégées.
- **Analyse de la menace :** Évaluer les menaces potentielles qui pèsent sur ces informations.
- **Analyse des vulnérabilités :** Identifier les faiblesses qui pourraient être exploitées par une menace.
- **Évaluation du risque :** Estimer le niveau de risque en fonction des menaces et des vulnérabilités identifiées.
- **Mise en œuvre de contre-mesures :** Appliquer des mesures pour réduire ou éliminer le risque.

Il est crucial de comprendre que l'OPSEC est un processus continu et dynamique. Les étapes ne suivent pas nécessairement un ordre fixe et peuvent être revisitées à tout moment pour s'adapter aux évolutions du contexte.

Évaluation des Risques

Le risque dans le contexte industriel et de la cybersécurité se réfère à la probabilité qu'une menace exploite une vulnérabilité, avec des conséquences négatives pour les installations. Les différentes organisations peuvent définir le risque de manière légèrement différente, mais dans la plupart des disciplines d'ingénierie, comme l'illustre la norme EN50126, le risque est généralement calculé comme suit :

$$\textit{Risque} = \textit{Probabilité de l'incident} \times \textit{Impact}$$

En cybersécurité, l'agence américaine de sécurité des infrastructures (CISA, s.d.) propose une version adaptée de cette formule, où la probabilité est décrite comme un produit scalaire de la menace et de la gravité de la vulnérabilité :

$$\boldsymbol{Risque = Menace \times Vulnérabilité \times Impact}$$

- ***Impact :*** Le dommage ou la perte subie par l'organisation en cas de réussite d'une attaque.
- ***Menace :*** Par exemple, un hacker cherchant à exploiter des failles dans un système.
- ***Vulnérabilité :*** Une faiblesse exploitable, comme une faille de sécurité dans un logiciel bancaire.
- ***Conséquence :*** L'issue d'une attaque, comme le vol de données sensibles.

Il est important de noter que toutes les menaces ne sont pas intentionnelles. Des facteurs externes tels que les conditions météorologiques, la dégradation des matériaux, ou les erreurs humaines peuvent également augmenter les risques, parfois avec des conséquences plus graves que celles causées par des menaces intentionnelles. Cependant, dans ce cadre, nous nous concentrerons sur les menaces intentionnelles.

3.3.3 Établir un programme de détection et de réponse aux menaces ICS/OT

Défis de la Détection des Menaces ICS

1. **Hétérogénéité des Environnements** : Les systèmes ICS/OT sont souvent composés de divers équipements et technologies provenant de différents fournisseurs, ce qui rend leur intégration et leur surveillance complexes.
2. **Absence de Standards** : L'absence de normes uniformes dans la sécurité des systèmes industriels rend difficile l'application de solutions de détection des menaces cohérentes et efficaces.
3. **Ancien Matériel et Logiciels :** De nombreux systèmes ICS reposent sur du matériel et des logiciels obsolètes qui ne sont pas conçus pour faire face aux menaces modernes, limitant ainsi les capacités de détection et de réponse.
4. **Pressions sur la Continuité des Opérations :** La nécessité de maintenir un fonctionnement ininterrompu des opérations complique la mise en œuvre de mises à jour de sécurité ou de nouvelles technologies.
5. **Manque de Visibilité :** Les environnements ICS manquent souvent de visibilité sur le réseau, ce qui rend difficile la détection des activités anormales ou malveillantes.
6. **Sensibilité aux Délais :** Les systèmes doivent répondre en temps réel, et l'introduction de processus de sécurité peut introduire des délais, compromettant ainsi l'efficacité opérationnelle.
7. **Culture de Résistance au Changement :** Les employés peuvent être réticents à adopter de nouvelles technologies ou processus, ce qui complique la mise en œuvre de solutions de détection des menaces.
8. **Volume Élevé d'Alerte :** Les outils de détection peuvent générer un grand nombre d'alertes, ce qui peut entraîner la fatigue des équipes de sécurité et le risque d'ignorer des menaces réelles.

9. **Compétences Limités en Sécurité :** Il y a souvent un manque d'expertise en cybersécurité dans les équipes travaillant sur des systèmes ICS, rendant la gestion des menaces plus difficile.
10. **Coordination Inter-Équipes :** La nécessité de collaboration entre les équipes IT et OT pour répondre efficacement aux menaces est un défi en raison de différences culturelles et opérationnelles.

Ces défis soulignent la nécessité d'une approche intégrée et proactive pour la détection et la réponse aux menaces dans les environnements ICS/OT.

Le coût des licences logicielles et du travail en ingénierie dépasse celui du matériel dans le cadre des systèmes de contrôle industriel (ICS/OT). Modifier les équipements existants pour intégrer de nouveaux outils est souvent déconseillé par les fournisseurs, car cela peut entraîner des conséquences imprévues. Cette réticence à mettre à jour la technologie engendre l'utilisation de dispositifs obsolètes ou non pris en charge. De plus, l'équipement OT conçu pour la communication en temps réel ne tolère pas les retards dus à la sécurité, ce qui a freiné l'implémentation de certaines mesures de sécurité jusqu'à récemment.

L'augmentation de l'interconnectivité et la réticence au changement rendent la détection des menaces essentielle pour éviter des risques perturbateurs. De nouveaux outils de sécurité visent à répondre à ce besoin, mais ils doivent être accompagnés de processus adaptés et d'une équipe compétente. Un programme efficace de détection et de réponse aux menaces ICS/OT repose sur la collecte de données à différents niveaux, l'enrichissement de ces données pour identifier les alertes prioritaires, et la réponse rapide d'experts (Booz Allen Hamilton Inc, 2020).

APPROCHE

Il est essentiel que l'organisation s'engage à établir un programme complet de détection et de réponse aux menaces ICS/OT, comprenant des éléments tels que l'effectif suffisant pour les opérations de sécurité, l'examen des données existantes pour leur intégration, l'investissement dans des outils de sécurité, l'optimisation des processus existants, la création de cas d'utilisation appropriés, et l'élaboration de manuels de réponse. Bien que chaque organisation puisse choisir un chemin différent pour son programme de détection et de réponse aux menaces ICS/OT, plusieurs objectifs doivent être atteints pour réduire le risque cybernétique.

CRÉER UNE STRATÉGIE

La première étape de tout nouveau projet est la planification. Une stratégie de haut niveau doit être établie avant tout changement lié aux personnes, aux processus ou à la technologie. Bien qu'il puisse être tentant de commencer le plus tôt possible pour voir des résultats rapidement, agir sans stratégie peut entraîner des pertes de temps et des mauvaises décisions dues à un manque d'information. Une stratégie bien réfléchie inclut une première liste de cas d'utilisation ciblés, une stratégie de déploiement comprenant une phase de preuve de concept, les compétences nécessaires pour mener à bien le travail, le personnel requis pour faciliter le travail sur le site, et un calendrier de

base. Par exemple, les cas d'utilisation peuvent inclure l'alerte lorsqu'une clé USB est insérée dans des serveurs critiques ou lorsque certains contrôleurs commencent à envoyer un volume de trafic supérieur à la normale. Lors de cette planification, l'organisation doit commencer à identifier si elle aura besoin de soutien supplémentaire et de visibilité à travers une capacité de détection et de réponse gérée (MDR). Il existe plusieurs façons pour une organisation de tirer parti d'un MDR ; cependant, la solution optimale équilibre les besoins de l'organisation en termes d'échelle et de contrôle tout en renforçant les investissements en cybersécurité mis en place dans le cadre du programme global de détection des menaces OT (Booz Allen Hamilton Inc, 2020).

ÉLARGIR LA VISIBILITÉ

Les environnements ICS/OT nécessitent une disponibilité continue, ce qui rend difficile la mise en place d'outils de sécurité sans perturber les opérations. Cependant, la visibilité est essentielle pour la détection et la réponse aux menaces, car les organisations ne peuvent pas protéger ce qu'elles ne connaissent pas.

Sources existantes

Avant d'introduire de nouvelles technologies, les organisations doivent évaluer les données déjà disponibles et leur alignement avec leurs cas d'utilisation. Les environnements ICS/OT, tout comme les environnements informatiques traditionnels, disposent de nombreuses sources de données qui, si elles sont correctement configurées, peuvent offrir une meilleure visibilité. Les infrastructures ICS/OT utilisent souvent des réseaux Ethernet avec des commutateurs, des pare-feu, des serveurs et des postes de travail. Ces dispositifs peuvent être configurés pour envoyer des journaux vers un dépôt centralisé pour analyse.

En outre, les environnements ICS/OT génèrent des millions de points de données nécessaires à leur fonctionnement. Des logiciels comme les serveurs Open Platform Communications (OPC) et les historiens peuvent être configurés pour maximiser ces données et les transmettre à un dépôt centralisé pour corrélation.

Nouvelles sources

Si une organisation manque de visibilité sur son réseau, elle ne pourra pas détecter efficacement les menaces et atténuer les risques dans son environnement ICS/OT. Il est donc nécessaire d'introduire de nouveaux outils de sécurité pour combler les lacunes. Dans les environnements ICS/OT, des outils passifs sont préférables car ils n'ajoutent pas de trafic supplémentaire sur le réseau, évitant ainsi de surcharger les dispositifs OT. Ces outils doivent être configurés pour enregistrer les événements sans répondre activement, bien que certains paramètres actifs puissent être activés après une longue période d'analyse des données passives pour garantir la compréhension des impacts potentiels.

Le point clé ici est qu'il n'existe pas d'outil unique pour assurer la visibilité dans les environnements ICS/OT. Il faut un ensemble d'outils et de tactiques. Chaque outil a ses forces et ses faiblesses, et son efficacité dépend de sa configuration. Par exemple, les

pare-feu sont des outils très utiles, mais s'ils ne sont pas installés correctement ou configurés pour bloquer le trafic, ils deviennent simplement des routeurs coûteux.

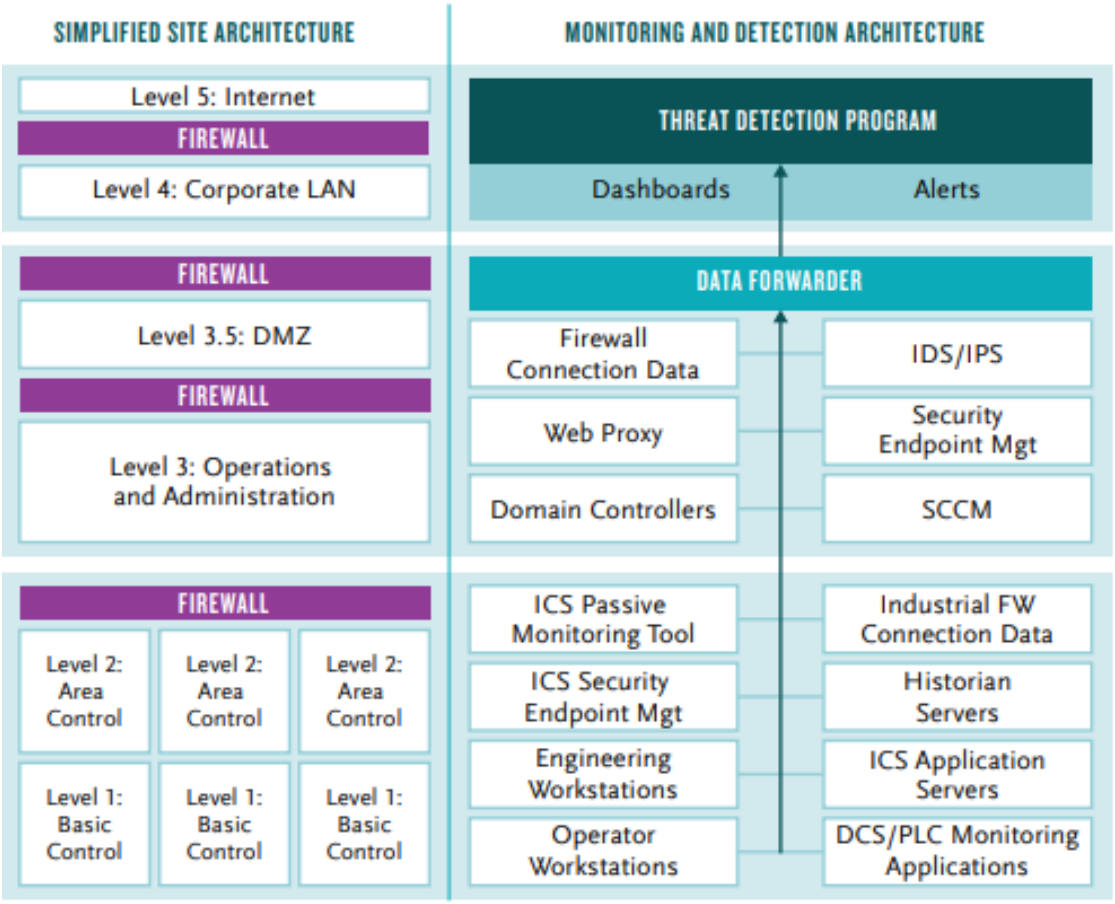


FIGURE 3. 6 : Architecture pour la detection et supervision (BOOZ ALLEN HAMILTON INC, 2020)

Il existe plusieurs options de logiciels passifs de gestion d'actifs OT sur le marché. Sélectionner le bon outil peut être difficile, d'où l'importance d'un processus d'évaluation rigoureux. Le processus de sélection doit commencer par la création d'une liste de critères de sélection, divisée en deux catégories : les fonctionnalités souhaitées et les fonctionnalités essentielles. Ces critères doivent ensuite être priorisés selon leur importance pour la mission. Le processus de sélection peut être résumé en six étapes :

1) Développer une liste de critères,
2) Contacter les fournisseurs approuvés et leur soumettre un questionnaire,
3) Organiser des entretiens techniques avec les fournisseurs,
4) Évaluer les fournisseurs selon un mécanisme de notation,
5) Sélectionner la solution recommandée pour un projet pilote,
6) Évaluer les solutions en fonction des réponses et de leur scalabilité.

Il est important de choisir les fournisseurs en fonction des besoins spécifiques du client, de leur expérience dans l'industrie, et de la démonstration technique de leurs produits. Après la sélection, la communication avec l'équipe opérationnelle est cruciale pour garantir leur compréhension des bénéfices de l'outil, son impact potentiel sur les opérations, et leur adhésion au processus de sécurisation de l'environnement.

PERMETTRE L'ACTION

La fonction la plus importante de tout programme de sécurité est la capacité à détecter et à répondre en continu aux menaces potentielles dès leurs débuts. Pour que la détection des menaces soit efficace et efficiente, les alertes des outils de sécurité et les journaux système doivent être centralisés dans un dépôt. L'agrégation des données provenant de diverses sources permet de les corréler et de les contextualiser pour en faire des tâches exploitables. Cependant, de nombreux outils peuvent générer un grand nombre d'alertes pour chaque changement mineur, et tous les journaux ne sont pas pertinents. Il est donc crucial de sélectionner les bonnes données nécessaires au développement précis de cas d'utilisation ou d'alertes. C'est ici qu'un changement de mentalité de la sécurité réactive à proactive doit se produire.

Le développement de cas d'utilisation ou d'alertes doit être une activité coordonnée entre le personnel de l'automatisation sur site, l'informatique et le Centre des opérations de sécurité (SOC). Le personnel sur site doit contribuer à la définition des cas d'utilisation concernant ce qui doit être surveillé et les indicateurs courants d'anomalies. Ensuite, le personnel informatique peut évaluer la faisabilité des sources de données existantes pour le cas d'utilisation, tandis que le personnel du SOC développe la logique de détection pertinente et les requêtes qui relient les sources de données disponibles. Sans cette collaboration, des alertes non pertinentes peuvent survenir, entraînant frustration et ignorance des menaces potentielles.

Bien que certains professionnels de la sécurité soient dédiés à la réponse aux incidents, le volume d'alertes et les autres tâches réduisent le temps disponible pour y répondre. De plus, le personnel nécessaire pour aider à l'investigation et à la gestion des incidents a ses propres tâches quotidiennes qui ne se concentrent pas sur la sécurité. Il est donc essentiel de prioriser les alertes selon l'importance de l'actif par rapport aux opérations, afin que les alertes concernant des dispositifs critiques soient mises en avant. Pour permettre cette priorisation, un effort unifié doit être fait pour identifier et caractériser les dispositifs qui soutiennent les opérations. Ces informations peuvent ensuite être envoyées au dépôt centralisé en tant que nouvelle source de données (Booz Allen Hamilton Inc, 2020).

FACILITER LA RÉPONSE

Les cyberattaques dans les environnements ICS/OT sont de plus en plus sophistiquées, et un processus de réponse solide est essentiel pour gérer efficacement les incidents, identifier le vecteur d'attaque et améliorer les méthodes de détection. Une intégration continue entre le personnel et des workflows de réponse prédéterminés est cruciale pour minimiser les délais d'action. Avant qu'une alerte ne devienne active, il est important de déterminer le public cible et d'établir un processus de réponse approprié. Par exemple, une alerte sur un comportement anormal d'un PLC doit être envoyée au personnel d'automatisation approprié pour un suivi rapide.

Les contraintes budgétaires et le manque de personnel peuvent entraver la capacité de réponse. Une solution efficace est de recourir à un service de détection et de réponse gérée (MDR) spécialisé dans les environnements ICS/OT. Cela offre des avantages comme une expertise en cybersécurité, une couverture 24/7 et des rapports exploitables. Contrairement aux services MDR traditionnels, un MDR pour l'ICS/OT doit équilibrer la réponse aux incidents et la continuité des opérations critiques. Une coordination avec le personnel sur site et un analyste hybride comprenant les spécificités ICS/OT peuvent faciliter les plans de remédiation et améliorer l'efficacité de la réponse aux événements.

RÉDUCTION DES RISQUES CYBERNÉTIQUES

Le parcours pour sécuriser les systèmes ICS/OT est un processus continu, car les menaces évoluent tout comme les techniques de défense. L'introduction de nouvelles technologies nécessite une itération constante des capacités de détection et de réponse aux menaces, ce qui peut inclure l'ajustement des analyses et le développement de nouveaux cas d'utilisation. Les programmes efficaces suivent un processus de cycle de vie pour s'assurer qu'ils évoluent avec les menaces (Booz Allen Hamilton Inc, 2020).

Ce cycle de vie commence par l'ingénierie et l'architecture des solutions visant à offrir une visibilité sur les opérations technologiques (OT). Une fois le design achevé, la technologie est déployée et les données générées sont intégrées dans l'environnement centralisé. Ces événements servent alors à développer des cas d'utilisation et des procédures de réponse. Les alertes, tableaux de bord et rapports doivent ensuite être surveillés, analysés et catalogués pour fournir des données de tendance. Ce processus aide à ajuster les analyses, développer de nouveaux cas d'utilisation ou identifier des solutions pouvant atténuer davantage les menaces.

Dans une industrie où l'efficacité opérationnelle et la chaîne d'approvisionnement sont cruciales, il est essentiel de changer la mentalité pour reconnaître l'importance d'un programme de détection et de réponse aux menaces ICS/OT afin de maintenir l'efficacité.

CHAPITRE 4

GESTION DES RISQUES POUR LES SYSTEMES ICS/OT

CHAPITRE 4 GESTION DES RISQUES POUR LES SYSTEMES ICS/OT

Pour atteindre leurs objectifs commerciaux, les entreprises gèrent quotidiennement des risques tels que les pertes financières, les pannes d'équipement et la sécurité des employés. Les organisations développent des processus pour évaluer les risques associés à leur activité et déterminer comment gérer ces risques en fonction des priorités de l'organisation, de sa tolérance au risque et des contraintes internes et externes. Cette gestion des risques est un processus continu et interactif qui fait partie des opérations commerciales normales. Les entreprises utilisant des systèmes OT gèrent traditionnellement les risques grâce à de bonnes pratiques technologiques et de sécurité. Les évaluations de sécurité sont bien établies dans la plupart des secteurs et sont souvent intégrées aux exigences réglementaires.

La gestion des risques liés à la sécurité de l'information constitue une dimension supplémentaire potentiellement complémentaire. Les processus et cadres de gestion des risques décrits dans cette section peuvent être appliqués à la gestion des risques liés à la sécurité, à la sécurité de l'information et à la cyber-chaîne d'approvisionnement. Pour certains systèmes OT, la confidentialité est également un risque à prendre en compte. Pour des conseils supplémentaires sur la gestion des risques liés à la confidentialité, consultez le cadre de gestion des risques du (NIST (SP) 800-37r2, 2018)et le cadre de confidentialité [PF]. Le processus de gestion des risques est déployé dans toute l'organisation en utilisant une approche à trois niveaux pour gérer les risques : (i) *au niveau organisationnel*, (ii) *au niveau de la mission et des processus métier*, et (iii) *au niveau du système (IT et OT)*.

Le processus de gestion des risques se déroule de manière transparente aux trois niveaux, avec pour objectif général l'amélioration continue des activités liées aux risques de l'organisation et une collaboration inter-niveaux entre toutes les parties prenantes ayant un intérêt commun dans le succès de l'organisation et une communication efficace au sein de chaque niveau.

Bien que cette section se concentre principalement sur les considérations OT au niveau du système, les activités, informations et artefacts de gestion des risques de chaque niveau ont un impact et informent les autres niveaux. Cette section aborde également les considérations relatives au système OT et la manière dont ces considérations affectent le processus de gestion des risques.

4.1 GESTION DE LA SECURITE ICS/OT

Bien que le processus de gestion des risques décrit dans le NIST SP 800-39 (NIST (SP) 800-39, 2011) s'applique à tous les types de systèmes, certaines considérations uniques doivent être prises en compte lorsqu'il s'agit de gérer les risques liés à la sécurité des systèmes OT.

Comme la montre Figure 4. 1 le processus de gestion des risques se compose de quatre éléments : un cadre de risque (c'est-à-dire la définition du contexte pour une prise de décision basée sur le risque), une évaluation des risques, une réponse au risque et une surveillance des risques. Ces activités sont interdépendantes et se déroulent souvent simultanément au sein d'une organisation. Par exemple, les résultats d'un composant de suivi sont intégrés dans un

composant de cadre. L'environnement dans lequel une organisation évolue en constante évolution, la gestion des risques doit être un processus continu dans lequel toutes les composantes ont des activités continues. Il est important de rappeler que ces éléments s'appliquent à la gestion de tous les types de risques, notamment la cybersécurité, la sécurité physique, la sécurité et la finance.

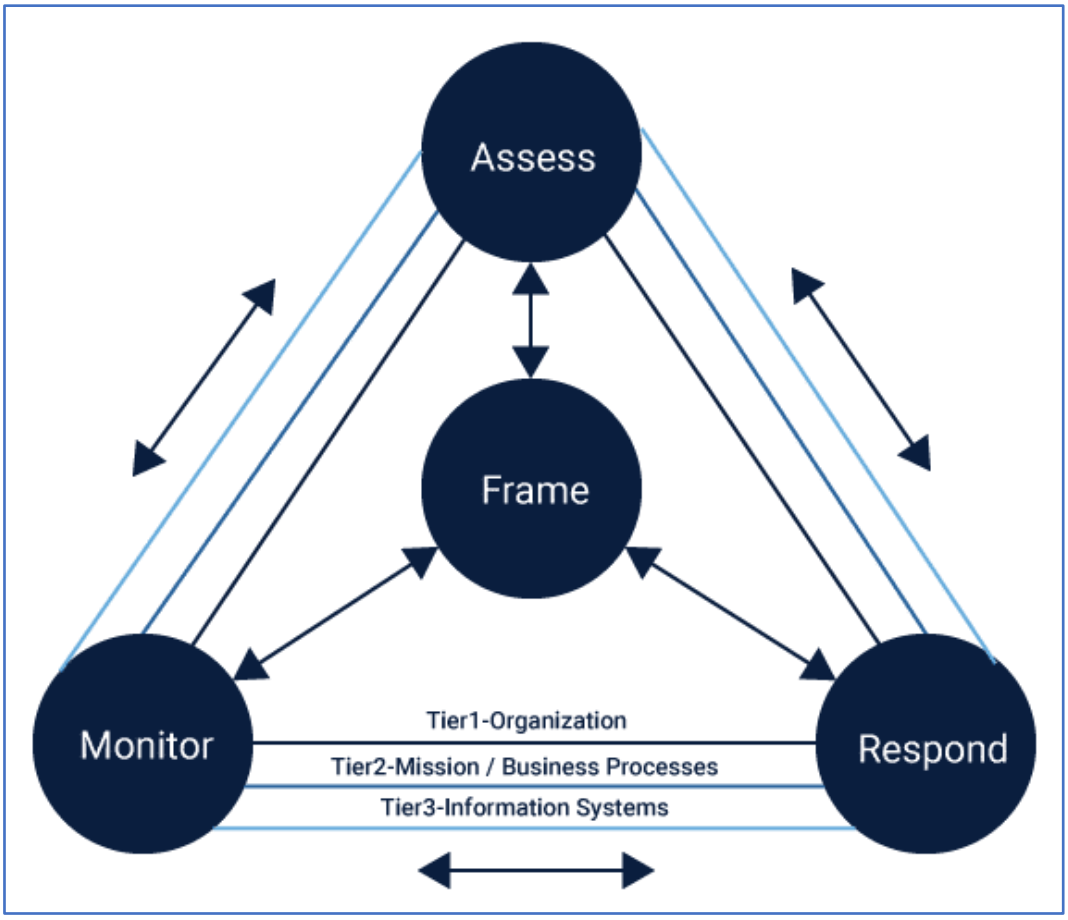


FIGURE 4. 1 : Processus de gestion des risques : encadrer, évaluer, réagir et surveiller

La gestion des risques à l'échelle organisationnelle s'effectue sur trois niveaux, comme illustré à la Figure 4. 2.

Le premier niveau traite des risques d'un point de vue global, en établissant le cadre de gestion des risques et en fournissant un contexte pour toutes les activités dans l'organisation. Le deuxième niveau se concentre sur les risques liés à la mission et aux processus opérationnels, s'appuyant sur le cadre défini au niveau 1. Le troisième niveau concerne la gestion des risques au niveau des systèmes, en tenant compte des résultats des deux premiers niveaux (Keith, Michael, & CheeYee, 2023).

Ces trois niveaux, intégrés aux différentes phases de gestion des risques (cadrage, évaluation, réponse et surveillance), assurent une vision globale des risques à travers toute l'organisation, tout en garantissant la transparence et la traçabilité des décisions prises en matière de gestion des risques.

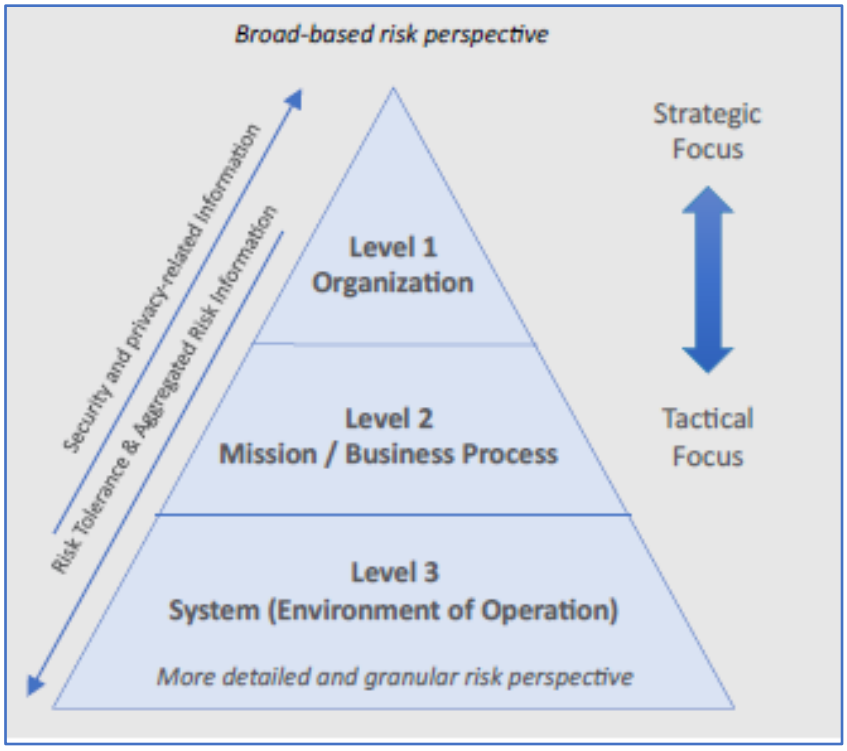


FIGURE 4. 2 : Niveaux de gestion des risques : organisation, mission et processus opérationnels, et système (KEITH, MICHAEL, & CHEEYEE, 2023)

4.1.1 Encadrement des risques liés aux OT

L'encadrement des risques pour les systèmes OT (Technologies Opérationnelles) consiste à définir les hypothèses, contraintes, tolérances au risque et stratégies permettant aux organisations de gérer efficacement les risques.

Ce processus soutient la stratégie globale de gestion des risques en tenant compte de la structure de gouvernance, des environnements réglementaires, et d'autres facteurs essentiels. Il aide les organisations à évaluer, répondre et surveiller les risques liés aux systèmes informatiques et OT.

La CISA (Cybersecurity and Infrastructure Security Agency) encourage une collaboration entre le gouvernement et l'industrie pour mieux anticiper et gérer les risques liés aux OT au niveau national. Elle aide les opérateurs et fournisseurs d'infrastructures critiques à identifier les vulnérabilités et à développer des stratégies d'atténuation afin de renforcer leur posture de cybersécurité.

Lors de l'encadrement des risques, il est crucial pour les organisations de choisir des méthodologies d'évaluation des risques adaptées aux OT.

Cela inclut l'analyse des impacts potentiels des incidents cybernétiques sur les systèmes physiques, la résilience des systèmes OT en place, et les possibilités d'incidents physiques résultant d'attaques cybernétiques.

Le Tableau 4. 1 offre des exemples de catégories d'impact que les organisations peuvent ajuster selon leurs besoins spécifiques, notamment la gravité des pannes ou interruptions.

TABLEAU 4. 1 : Définition possible des niveaux d'impact pour les systèmes OT en fonction du produit, de l'industrie, et des préoccupations de sécurité (KEITH, MICHAEL, & CHEEYEE, 2023)

Catégorie	Impact Élevé	Impact Modéré	Impact Faible
Panne sur plusieurs sites	Perturbation majeure des opérations sur plusieurs sites, avec une restauration nécessitant un ou plusieurs jours	Perturbation opérationnelle sur plusieurs sites, avec une restauration nécessitant plus d'une heure	Perturbation partielle des opérations sur plusieurs sites, avec restauration complète en moins d'une heure
Infrastructure et services nationaux	Impact sur plusieurs secteurs ou perturbation des services communautaires de manière significative	Potentiel d'impact au-delà de l'entreprise dans le secteur concerné	Impact minimal voire nul sur les secteurs en dehors de l'entreprise et impact négligeable sur la communauté
Coût (% du revenu)	> 25 %	> 5 %	< 5 %
Légal	Infraction criminelle de type "crime" ou violation de conformité affectant la licence d'exploitation	Infraction criminelle de type "délit" ou violation de conformité entraînant des amendes	Aucun
Confiance du public	Perte d'image de marque	Perte de confiance des clients	Aucune
Personnel sur site	Décès	Perte de journée de travail ou blessure grave	Premiers soins ou blessure enregistrable
Personnel hors site	Décès ou incident majeur dans la communauté	Plaintes ou impact sur la communauté locale	Aucune plainte
Environnement	Citation par une agence régionale ou dommage significatif à long terme sur une grande zone	Citation par une agence locale	Petit déversement contenu sous les limites déclarables

Pour soutenir l'évaluation des risques, les organisations doivent définir la manière de déterminer la probabilité d'occurrence des événements de cybersécurité afin de garantir la cohérence du processus. La norme NIST SP 800-30, propose des orientations pour développer des facteurs de risque pondérés selon la probabilité. Il est recommandé de pondérer ces facteurs en fonction de l'analyse de la capacité d'une menace à exploiter une vulnérabilité, du déclenchement de l'événement et des impacts négatifs potentiels. Pour les menaces adverses, la probabilité est évaluée en fonction de l'intention, des capacités et du ciblage de l'adversaire. Pour d'autres menaces, la probabilité repose sur des données historiques, empiriques, et d'autres critères. Si les organisations disposent de peu de données historiques, elles peuvent s'appuyer sur des informations sectorielles. La probabilité d'une menace dépend également de l'état de l'organisation, de son architecture de sécurité et de l'efficacité des contrôles de sécurité, ainsi que de sa résilience face aux événements indésirables dans les systèmes OT.

TABLEAU 4. 2 : Évaluation de la probabilité d'occurrence d'un évènement (KEITH, MICHAEL, & CHEEYEE, 2023)

Probabilité d'initiation ou d'occurrence d'un événement de menace	Probabilité que les événements de menace entraînent des impacts négatifs
Très élevée	Faible
Élevée	Faible
Modérée	Faible
Faible	Très faible
Très faible	Très faible

4.1.2 Évaluation des risques dans un environnement OT

L'évaluation des risques dans un environnement OT s'appuie sur les résultats obtenus lors de la définition des risques, tels que les méthodologies d'évaluation acceptées, les stratégies de gestion des risques et les niveaux de tolérance au risque. Elle vise à identifier, estimer et hiérarchiser les risques pour les opérations, les actifs, les individus et d'autres organisations. Ces évaluations peuvent se faire à différents niveaux, que ce soit au niveau de l'organisation, des missions, des fonctions commerciales, ou des systèmes, et les résultats obtenus peuvent éclairer les évaluations de risques à d'autres niveaux.

L'évaluation des risques dans les systèmes OT inclut des spécificités non présentes dans les évaluations des systèmes informatiques classiques, comme l'impact physique potentiel d'un cyber-incident sur un OT, en plus des effets numériques.

De plus, cette évaluation nécessite l'analyse des mécanismes, numériques ou non, mis en place pour minimiser les impacts des incidents. Les systèmes OT intègrent souvent des dispositifs non numériques, comme des systèmes de tolérance aux pannes ou des mécanismes physiques, qui empêchent l'OT de dépasser certains seuils de sécurité. Ces mécanismes non numériques, tels que des soupapes de sécurité ou des compteurs analogiques, aident à limiter

les conséquences des incidents et doivent être pris en compte dans le processus d'évaluation des risques. Ces dispositifs permettent de contrôler l'état du système physique, fournissant aux opérateurs des données fiables même en cas de défaillance ou de corruption des systèmes numériques. Le Tableau 4. 3 présente une classification des mécanismes non numériques qui peuvent réduire l'impact d'un incident OT.

TABLEAU 4. 3 : CATEGORIES DE COMPOSANTS DE CONTROLE NON NUMERIQUES POUR LES OT

Type de contrôle	Description
Affichages ou alarmes analogiques	Des mécanismes non numériques mesurent et affichent l'état du système physique (par ex., température, pression, tension, courant) et peuvent fournir à l'opérateur des informations précises lorsque les affichages numériques sont indisponibles ou corrompus. Ces informations peuvent être fournies à l'opérateur via des affichages non numériques (par ex., thermomètres, manomètres) ou par des alarmes sonores.
Mécanismes de contrôle manuels	Les mécanismes de contrôle manuels (par ex., contrôles de valve manuelle, interrupteurs physiques) permettent aux opérateurs de contrôler manuellement un actionneur sans dépendre du système OT numérique. Cela garantit que l'actionneur peut être contrôlé même si le système OT est indisponible ou compromis.
Systèmes de contrôle analogiques	Les systèmes de contrôle analogiques utilisent des capteurs et des actionneurs non numériques pour surveiller et contrôler un processus physique. Ils peuvent empêcher le processus physique d'atteindre un état indésirable lorsque le système OT numérique est indisponible ou corrompu. Les contrôles analogiques incluent des dispositifs tels que des régulateurs, des régulateurs de vitesse, et des relais électromécaniques. Un exemple est un dispositif conçu pour s'ouvrir en cas d'urgence ou de conditions anormales afin de prévenir l'augmentation de la pression interne du fluide au-delà d'une valeur spécifiée, ramenant ainsi le processus à un état plus sûr. Le dispositif peut aussi être conçu pour prévenir un vide interne excessif, comme une soupape de décharge de pression, un dispositif de décharge non refermable (par ex., disque de rupture) ou une soupape de dépression.

De plus, les organisations doivent parfois inclure la confidentialité dans leur évaluation des risques, ce qui peut nécessiter une approche distincte. Le NIST propose la méthodologie d'évaluation des risques de confidentialité ((NIST Privacy Risk Assessment Methodology, s.d.) (PRAM)), un outil basé sur le modèle de risque du NIST IR 8062. Cet outil aide les organisations à analyser, évaluer et prioriser les risques liés à la confidentialité afin de définir des réponses appropriées et choisir les solutions adéquates.

4.1.3 Réponse au risque dans un environnement OT

La réponse au risque dans un environnement OT consiste à élaborer des mesures organisationnelles pour gérer les risques identifiés. Ces mesures sont choisies en tenant compte de la tolérance au risque de l'organisation et des éléments définis lors du cadrage du risque. Les options incluent l'acceptation, l'évitement, l'atténuation, le partage ou le transfert du risque, ou une combinaison de ces actions. Le processus implique la sélection et l'exécution du plan d'action le plus adapté pour traiter les risques identifiés.

4.1.4 Surveillance du risque dans un environnement OT

La surveillance du risque est une composante essentielle de la gestion continue du risque. Elle consiste à suivre en permanence les risques, y compris l'efficacité des stratégies mises en place pour réduire ces risques, les changements dans l'environnement qui pourraient modifier l'évaluation initiale, ainsi que la performance des mesures de gestion du risque. Cette surveillance influence les autres aspects de la gestion des risques et permet d'adapter les actions en fonction de nouvelles menaces ou vulnérabilités.

4.2 DOMAINES PARTICULIERS A PRENDRE EN COMPTE

La gestion des risques de la chaîne d'approvisionnement et la gestion des risques pour la sécurité sont des aspects essentiels de la gestion des risques de cybersécurité des OT.

4.2.1. Gestion des risques de la chaîne d'approvisionnement

Les risques de cybersécurité peuvent provenir des produits ou services acquis pour les OT et peuvent être introduits à n'importe quelle étape de la chaîne d'approvisionnement. Ces risques, qu'ils soient malveillants, accidentels ou naturels, peuvent compromettre la disponibilité, l'intégrité des systèmes et des composants OT critiques ainsi que la confidentialité des données. Les organisations OT, souvent dépendantes des fournisseurs et prestataires tiers, doivent comprendre et atténuer les risques inhérents à leur chaîne d'approvisionnement. Cela inclut la gestion proactive des risques dans la chaîne d'approvisionnement de la cybersécurité (C-SCRM) via des politiques et pratiques spécifiques (Keith, Michael, & CheeYee, 2023).

Les organisations doivent évaluer les capacités, la fiabilité et les pratiques de sécurité des fournisseurs et prestataires, ainsi que la provenance et l'authenticité des produits. De plus, il est crucial de considérer la difficulté potentielle à obtenir des pièces de rechange ou des mises à jour d'origine tout au long du cycle de vie du produit. Les normes telles que NIST SP 800-161 fournissent des directives sur les pratiques C-SCRM, incluant une approche progressive pour établir un programme efficace de gestion des risques de la chaîne d'approvisionnement.

4.2.2. Systèmes de sécurité

La gestion des risques de sécurité physique est déjà bien intégrée dans les environnements OT, mais les organisations doivent également intégrer les évaluations des risques de cybersécurité, car le monde numérique et physique sont intimement liés dans ces environnements. Les évaluations de sécurité physique et numérique doivent donc être combinées pour identifier les risques croisés.

Les systèmes de sécurité, qui surveillent et contrôlent les processus pour garantir la sécurité des personnes et des actifs, jouent un rôle clé dans la réduction des impacts d'un incident cybernétique. Bien que ces systèmes soient souvent redondants et séparés de l'OT principal, certaines architectures les combinent, augmentant ainsi le risque d'attaque si l'OT est compromis. Il est essentiel que les organisations maintiennent une séparation adéquate des composants et évaluent l'impact des contrôles de sécurité sur le système pour éviter tout risque supplémentaire (Keith, Michael, & CheeYee, 2023).

4.3 APPLICATION DU CADRE DE GESTION DES RISQUES AUX SYSTEMES OT

Le cadre de gestion des risques ((NIST Risk Management Framework, s.d.)(RMF)) applique les processus et concepts de gestion des risques—tels que la définition, l'évaluation, la réponse et la surveillance des risques aux systèmes et aux organisations. Les sous-sections suivantes expliquent comment appliquer le RMF à l'OT, en fournissant une description succincte de chaque étape et tâche, ainsi que des résultats attendus, des liens avec d'autres normes et directives pertinentes pour l'OT (comme le cadre de cybersécurité et la norme CEI 62443), et des recommandations d'implémentation spécifiques à l'OT. Il est à noter que certaines tâches sont optionnelles et que toutes ne comportent pas nécessairement des considérations ou des conseils propres à l'OT.

Bien que les étapes du RMF, comme illustré dans la Figure 4. 3, soient présentées de manière séquentielle, leur mise en œuvre peut se faire dans un ordre différent pour s'aligner avec les processus établis de gestion et de cycle de vie du développement des systèmes.

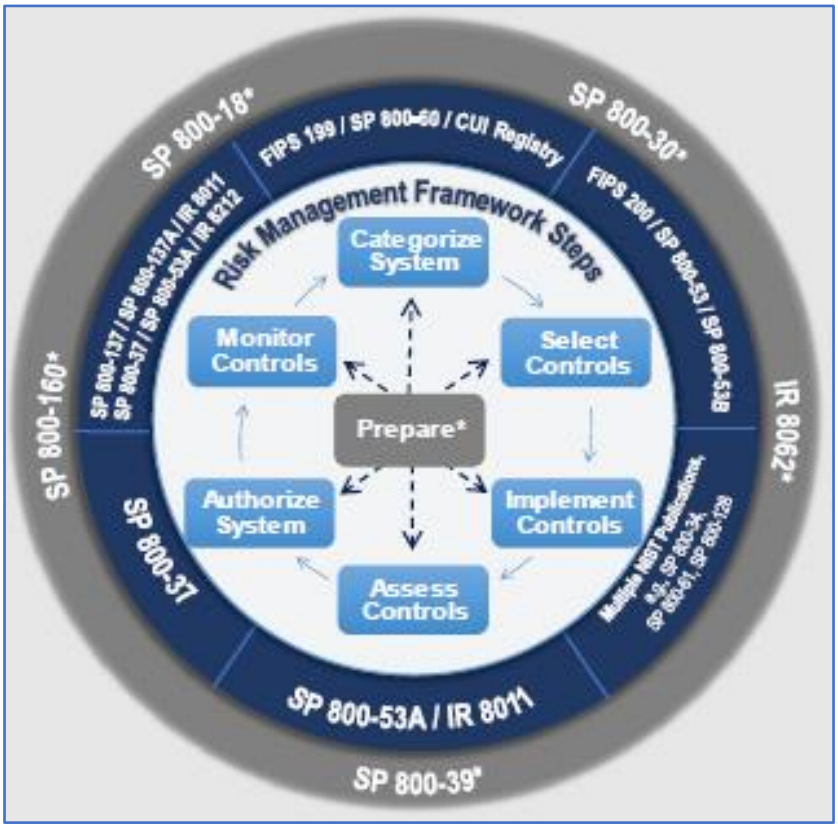


FIGURE 4. 3 : Etapes du cadre de gestion des risques

4.3.1 Préparation

L'objectif de l'étape Préparation est de réaliser des activités essentielles au niveau de l'organisation, de la mission, des processus opérationnels et du système pour aider l'organisation à gérer ses risques de sécurité et de confidentialité à l'aide du RMF. L'étape Préparation s'appuie sur les activités déjà menées dans le cadre des programmes de cybersécurité pour souligner l'importance de mettre en place une gouvernance et des ressources à l'échelle de l'organisation pour soutenir la gestion des risques. Le Tableau 4. 4 fournit des détails sur l'application de l'étape Préparation à la TO.

TABLEAU 4. 4 : Application de l'étape de préparation du RMF à l'OT (KEITH, MICHAEL, & CHEEYEE, 2023)

Tâches	Résultats	Orientations spécifiques à l'OT
Niveaux organisationnels et de processus métier		
TÂCHE P-1 ROLES DE GESTION DES RISQUES	Les individus sont identifiés et se voient attribuer des rôles clés pour l'exécution du RMF. [Cadre de cybersécurité : ID.AM-6 ; ID.GV-2] [IEC 62443-2-1 : ORG 1.3]	Établir et maintenir les rôles et responsabilités en matière de cybersécurité pour les systèmes IT et OT. Inclure les rôles et responsabilités en cybersécurité des fournisseurs tiers. Des exemples de personnel OT incluent le Responsable de Processus/Usine, l'Ingénieur en Contrôle de Processus, l'Opérateur, l'Ingénieur en Sécurité Fonctionnelle, le Personnel de Maintenance et le Responsable de Sécurité de Processus.
TÂCHE P-2 STRATÉGIE DE GESTION DES RISQUES	Une stratégie de gestion des risques pour l'organisation qui inclut une détermination et une expression de la tolérance au risque organisationnelle est établie. [Cadre de cybersécurité : ID.RM ; ID.SC] [IEC 62443-2-1 : ORG 2.1]	La stratégie de gestion des risques englobe l'ensemble de l'organisation. Considérer les exigences réglementaires uniques liées aux organisations disposant de systèmes OT.
TÂCHE P-3 ÉVALUATION DES RISQUES — ORGANISATION	Une évaluation des risques à l'échelle de l'organisation est	

	complétée ou une évaluation existante est mise à jour. [Cadre de cybersécurité : ID.RA ; ID.SC-2] [IEC 62443-2-1 : Event1.9 ; ORG 1.3 ; 2.1]	
TÂCHE P-4 BASES DE CONTROLE TAILLÉES ORGANISATIONNELLEMENT ET PROFILS DE CADRE DE CYBERSÉCURITÉ (OPTIONNEL)	Des bases de contrôle taillées organisationnellement et/ou des profils de cadre de cybersécurité sont établis et rendus disponibles. [Cadre de cybersécurité : Profil]	Une base de contrôle taillée organisationnellement pour les systèmes OT peut être développée pour répondre aux besoins de mission et d'affaires, aux environnements opérationnels uniques et/ou à d'autres exigences.
TÂCHE P-5 IDENTIFICATION DES CONTROLES COMMUNS	Des contrôles communs disponibles pour héritage par les systèmes organisationnels sont identifiés, documentés et publiés.	Les contrôles communs disponibles pour héritage peuvent avoir un impact négatif sur le fonctionnement des systèmes OT. Considérer si les contrôles communs peuvent être appliqués efficacement, en toute sécurité, et sans impact négatif sur le fonctionnement des systèmes OT.
TÂCHE P-6 PRIORISATION PAR NIVEAU D'IMPACT (OPTIONNEL)	Une priorisation des systèmes organisationnels avec le même niveau d'impact est effectuée. [Cadre de cybersécurité : ID.AM-5] [IEC 62443-2-1 : DATA 1.1]	Des critères tels que la sécurité ou la livraison de services critiques peuvent être utilisés dans la priorisation par niveau d'impact.
TÂCHE P-7 STRATÉGIE DE SURVEILLANCE CONTINUE – ORGANISATION	Une stratégie organisationnelle pour surveiller l'efficacité des contrôles est développée et mise en œuvre.	
Niveau Système		
TÂCHE P-8 FOCUS SUR LA MISSION OU LES AFFAIRES	Les missions, fonctions commerciales et processus missionnels et	Lors de la cartographie des processus OT et IT, les flux d'information et les

	commerciaux que le système est censé soutenir sont identifiés. [Cadre de cybersécurité : Profil ; Niveaux de mise en œuvre ; ID.BE] [IEC 62443-2-1 : ORG1.6 ; AVAIL 1.2 ; AVAIL 1.1]	protocoles doivent également être documentés.
TÂCHE P-9 PARTIES PRENANTES DU SYSTÈME	Les parties prenantes intéressées par le système sont identifiées. [Cadre de cybersécurité : ID.AM ; ID.BE]	Des exemples de personnel OT incluent le Responsable de Processus/Usine, l'Ingénieur en Contrôle de Processus, l'Opérateur, l'Ingénieur en Sécurité Fonctionnelle et le Responsable de Sécurité de Processus.
TÂCHE P-10 IDENTIFICATION DES ACTIFS	Les actifs des parties prenantes sont identifiés et priorisés. [Cadre de cybersécurité : ID.AM]	Les composants des systèmes OT peuvent inclure des PLC, des capteurs, des actionneurs, des robots, des outils de machine, des firmwares, des commutateurs réseau, des routeurs, des alimentations et d'autres composants ou dispositifs réseau.
TÂCHE P-11 LIMITES D'AUTORISATION	La limite d'autorisation (c'est-à-dire le système) est déterminée.	
TÂCHE P-12 TYPES D'INFORMATIONS	Les types d'informations traitées, stockées et transmises par le système sont identifiés. [Cadre de cybersécurité : ID.AM-5]	
TÂCHE P-13 CYCLE DE VIE DE L'INFORMATION	Toutes les étapes du cycle de vie de l'information sont identifiées et comprises pour chaque type d'information traitée, stockée ou transmise par le système [Cadre de cybersécurité : ID.AM-3 ; ID.AM-4].	

TÂCHE P-14 ÉVALUATION DES RISQUES – SYSTÈME	Une évaluation des risques au niveau du système est complétée ou une évaluation existante est mise à jour. [Cadre de cybersécurité : ID.RA ; ID.SC-2]	Les évaluations des risques, y compris les tests de performance/de charge et les tests de pénétration, sont menées sur les systèmes OT avec soin pour s'assurer que les opérations OT ne sont pas impactées négativement par le processus de test.
TÂCHE P-15 DÉFINITION DES EXIGENCES	Les exigences de sécurité et de confidentialité sont définies et priorisées. [Cadre de cybersécurité : ID.GV ; PR.IP]	
TÂCHE P-16 ARCHITECTURE D'ENTREPRISE	Le placement du système au sein de l'architecture d'entreprise est déterminé.	Grouper les composants OT par fonction ou niveau de sensibilité pour optimiser la mise en œuvre des contrôles de cybersécurité.
TÂCHE P-17 ALLOCATION DES EXIGENCES	Les exigences de sécurité et de confidentialité sont allouées au système et à l'environnement dans lequel le système opère. [Cadre de cybersécurité : ID.GV]	Lors de l'allocation des exigences de sécurité et de confidentialité au système OT, des considérations telles que l'impact sur la performance et la sécurité sont prises en compte.
TÂCHE P-18 ENREGISTREMENT DU SYSTÈME	Le système est enregistré à des fins de gestion, de responsabilité, de coordination et de supervision. [Cadre de cybersécurité : ID.GV]	

4.3.2 Catégorisation

Lors de la phase de catégorisation, on évalue les impacts négatifs potentiels liés à la perte de confidentialité, d'intégrité, et de disponibilité des informations et des systèmes. Pour chaque type d'information et système concernés, les trois objectifs de sécurité (confidentialité, intégrité, et disponibilité) sont associés à un des trois niveaux de gravité des conséquences en cas de violation de sécurité. Dans les systèmes OT, la disponibilité est souvent la principale préoccupation. Les normes FIPS 199 et NIST SP 800-60 fournissent les directives et standards

pour ce processus de catégorisation. Le Tableau 4. 5 fournit des détails sur l'application de l'étape de catégorisation RMF à l'OT (Keith, Michael, & CheeYee, 2023).

TABLEAU 4. 5 : Application de l'étape de catégorisation RMF à l'OT (KEITH, MICHAEL, & CHEEYEE, 2023)

Tâches	Résultats	Conseils Spécifiques aux OT
Tâche C-1 DESCRIPTION DU SYSTÈME	La description et la documentation des caractéristiques du système sont effectuées. [Cadre de cybersécurité : Profil]	
Tâche C-2 CATÉGORISATION DE SÉCURITÉ	Une catégorisation de la sécurité du système, y compris les informations traitées par le système représentées par les types d'informations identifiés par l'organisation, est complétée. [Cadre de cybersécurité : ID.AM-1 ; ID.AM-2 ; ID.AM-3 ; ID.AM-4 ; ID.AM-5] Les résultats de la catégorisation de la sécurité sont documentés dans les plans de sécurité, de confidentialité et de gestion des risques de la chaîne d'approvisionnement (SCRM). Les résultats de la catégorisation de la sécurité sont cohérents avec l'architecture d'entreprise et l'engagement à protéger les missions, les fonctions commerciales, et les processus associés. Les résultats de la catégorisation de la sécurité reflètent la stratégie de gestion des risques de l'organisation.	Les systèmes OT et IT peuvent avoir des critères de catégorisation différents. Les informations du système et le processus du système (par exemple, la production chimique) doivent être pris en compte lors de la catégorisation de la sécurité.
Tâche C-3 EXAMEN ET APPROBATION DE LA CATÉGORISATION DE SÉCURITÉ	Les résultats de la catégorisation de la sécurité sont examinés et la décision de catégorisation est approuvée par les dirigeants de l'organisation.	

4.3.3 Sélection

L'étape de sélection vise à choisir les contrôles initiaux nécessaires pour protéger le système en fonction des risques identifiés. Les lignes de base de contrôle servent de point de départ pour ce processus et sont déterminées en fonction de la catégorisation de sécurité et du niveau d'impact associé aux systèmes identifiés lors de l'étape de catégorisation.La norme NIST SP 800-53B propose des lignes de base de contrôle recommandées pour les systèmes et les informations du gouvernement fédéral (Keith, Michael, & CheeYee, 2023).

Pour répondre à la nécessité de créer des ensembles de contrôles adaptés aux communautés et aux systèmes spécifiques, le concept de superpositions est introduit. Une superposition est un ensemble complet de contrôles, d'améliorations de contrôle et de recommandations supplémentaires, résultant de l'application de conseils d'adaptation aux lignes de base de contrôle de sécurité spécifiées dans la norme NIST SP 800-53B.

Les propriétaires de systèmes OT peuvent ajuster ces superpositions à partir de l'annexe F de la norme NIST SP 800-82r3 (Keith, Michael, & CheeYee, 2023) lorsque la mise en œuvre de contrôles spécifiques s'avère impossible ou peu pratique.

4.3.4 Implémentation

L'étape d'implémentation consiste à mettre en œuvre des contrôles au sein de systèmes nouveaux ou existants. Le processus de sélection des contrôles, décrit dans cette section, peut s'appliquer aux systèmes OT sous deux angles : le développement de nouveaux systèmes et la gestion de systèmes existants. Pour les nouveaux systèmes, le processus de sélection est orienté vers la définition des exigences, car ces systèmes sont encore en phase de conception. À ce stade, les organisations réalisent des catégorisations de sécurité initiales. Les contrôles identifiés dans les plans de sécurité des systèmes servent alors de spécifications de sécurité, devant être intégrés durant les phases de développement et d'implémentation du cycle de vie du système.

En revanche, pour les systèmes existants, le processus de sélection des contrôles de sécurité se base sur une analyse des écarts, surtout lorsque des changements significatifs sont envisagés (par exemple, lors de mises à niveau majeures, de modifications ou d'externalisation). Comme ces systèmes sont déjà en place, les organisations ont probablement déjà achevé les processus de catégorisation de sécurité et de sélection des contrôles, ce qui a permis d'établir des contrôles convenus dans les plans de sécurité respectifs et de les mettre en œuvre dans les systèmes (Keith, Michael, & CheeYee, 2023).

4.3.5 Évaluation

L'étape d'évaluation du cadre de gestion des risques (RMF) vise à déterminer l'efficacité des contrôles appliqués au système et à vérifier s'ils produisent les résultats attendus. La norme NIST SP 800-53A offre des directives pour l'évaluation des contrôles sélectionnés de la norme NIST SP 800-53. Ces directives visent à s'assurer que les contrôles sont correctement mis en œuvre, fonctionnent comme prévu et atteignent les résultats souhaités en matière de conformité aux exigences de sécurité du système.

Le Tableau 4. 6 fournit des détails supplémentaires sur l'application de l'étape d'évaluation à l'ergothérapie.

TABLEAU 4. 6 : Application de l'étape évaluer du RMF aux systèmes OT

Tâches	Résultats	Conseils spécifiques à l'OT
TÂCHE A-1 : SÉLECTION DE L'ÉVALUATEUR	Un évaluateur ou une équipe d'évaluation est sélectionné pour mener les évaluations des contrôles. Un niveau d'indépendance approprié est atteint pour l'évaluateur ou l'équipe d'évaluation sélectionnée.	Incluez le personnel des systèmes OT et l'opérateur dans l'équipe d'évaluation.

Tâches	Résultats	Conseils spécifiques à l'OT
TÂCHE A-2 : PLAN D'ÉVALUATION	La documentation nécessaire pour effectuer les évaluations est fournie à l'évaluateur ou à l'équipe d'évaluation.	Des plans d'évaluation de la sécurité et de la vie privée sont développés et documentés. Ces plans sont examinés et approuvés pour établir les attentes concernant les évaluations des contrôles et le niveau d'effort requis.
TÂCHE A-3 : ÉVALUATIONS DES CONTRÔLES	Les évaluations des contrôles sont effectuées conformément aux plans d'évaluation de la sécurité et de la vie privée.	Considérez les opportunités de réutiliser les résultats des évaluations précédentes pour rendre le processus de gestion des risques plus efficace en termes de temps et de coûts. Maximisez l'utilisation de l'automatisation pour accélérer, rendre efficace et efficient les évaluations. Envisagez d'utiliser des exercices de simulation pour réduire l'impact sur la production OT. Utilisez des outils automatisés pour effectuer des évaluations tout en veillant à ce que le système OT ne soit pas affecté négativement par le processus de test.
TÂCHE A-4 : RAPPORTS D'ÉVALUATION	Des rapports d'évaluation de la sécurité et de la vie privée, fournissant des constatations et des recommandations, sont complétés.	[Cybersecurity Framework : ID.RA-1 et ID.RA-3]
TÂCHE A-5 : ACTIONS DE REMÉDIATION	Des actions de remédiation sont prises pour traiter les lacunes des contrôles mis en œuvre dans le système et l'environnement opérationnel. Les plans de sécurité et de vie privée sont mis à jour pour refléter les changements apportés à l'implémentation des contrôles basés sur les évaluations et les actions de remédiation subséquentes.	Assurez-vous que les actions de remédiation n'impactent pas négativement l'efficacité et la sécurité des opérations OT. Envisagez l'utilisation de contrôles compensatoires comme l'une des actions de remédiation.
TÂCHE A-6 : PLAN D'ACTION ET ÉTAPES	Un plan d'action et des étapes détaillant les plans de remédiation pour les risques inacceptables identifiés dans les rapports d'évaluation de la sécurité et de la vie privée est élaboré.	Tenez compte des contraintes temporelles uniques du système OT dans le plan d'action et des étapes, et prenez en considération les opérations de maintenance

Tâches	Résultats	Conseils spécifiques à l'OT
		programmées ou les arrêts du système OT.

4.3.6 Autorisation

L'étape d'autorisation implique une décision de gestion visant à autoriser le fonctionnement d'un système tout en acceptant explicitement les risques liés aux opérations, aux actifs et aux individus, en fonction de la mise en œuvre d'un ensemble de contrôles convenu. Un nouveau système ne peut pas être mis en production ou en opération tant qu'il n'est pas autorisé.

TABLEAU 4. 7 : Application de l'étape autoriser du RMF aux systèmes OT

Tâches	Résultats	Conseils spécifiques à l'OT
TÂCHE R-1 : PACKAGE D'AUTORISATION	Un package d'autorisation est élaboré pour soumission à l'autorité d'autorisation.	
TÂCHE R-2 : ANALYSE ET DÉTERMINATION DES RISQUES	Une détermination des risques par l'autorité d'autorisation est effectuée, reflétant la stratégie de gestion des risques, y compris la tolérance au risque.	
TÂCHE R-3 : RÉPONSE AUX RISQUES	Des réponses aux risques déterminés sont fournies.	[Cybersecurity Framework : ID.RA-6] Développez et mettez en œuvre une stratégie complète pour gérer les risques du système OT, incluant l'identification et la priorisation des réponses aux risques.
TÂCHE R-4 : DÉCISION D'AUTORISATION	L'autorisation du système ou des contrôles communs est approuvée ou refusée.	Les organisations peuvent avoir besoin de déterminer des stratégies de remédiation lorsque les risques du système sortent de la plage acceptable, en tenant compte des dépendances spécifiques à l'OT, telles que l'incapacité de mettre hors ligne un système ou un composant jusqu'à remédiation.
TÂCHE R-5 : RAPPORT D'AUTORISATION	Les décisions d'autorisation, les vulnérabilités significatives et les risques sont rapportés aux	Assurez-vous que les décisions, les vulnérabilités et les risques sont rapportés au personnel OT et aux opérations.

Tâches	Résultats	Conseils spécifiques à l'OT
	responsables organisationnels.	

4.3.7 Surveillance

L'étape de surveillance consiste à suivre en continu les changements apportés au système qui pourraient affecter les contrôles et à évaluer l'efficacité de ces contrôles. La norme NIST SP 800-37, Rév. 2, fournit des orientations sur la surveillance continue en matière de cybersécurité [SP800-37r2].

TABLEAU 4. 8 : Application de l'étape surveiller du RMF aux systèmes OT

Tâches	Résultats	Conseils spécifiques à l'OT
TÂCHE M-1 : CHANGEMENTS DU SYSTÈME ET DE L'ENVIRONNEMENT	Le système et l'environnement d'opération sont surveillés conformément à la stratégie de surveillance continue. [Cybersecurity Framework : DE.CM; ID.GV]	Exploitez la stratégie de surveillance continue spécifique à l'OT qui prend en compte les impacts sur la performance et considère les systèmes de sécurité comme critiques.
TÂCHE M-2 : ÉVALUATIONS CONTINUES	Des évaluations continues de l'efficacité des contrôles sont réalisées conformément à la stratégie de surveillance continue. [Cybersecurity Framework : ID.SC-4]	Réalisez des évaluations continues qui tiennent compte des impacts sur la performance et la sécurité du système.
TÂCHE M-3 : RÉPONSE AUX RISQUES CONTINUE	Les résultats des activités de surveillance continue sont analysés et des réponses appropriées sont apportées. [Cybersecurity Framework : RS.AN]	Corrélez les informations sur les événements détectés avec les résultats de l'évaluation des risques pour obtenir une perspective sur l'impact des incidents sur le système OT.
TÂCHE M-4 : MISE À JOUR DES PACKAGES D'AUTORISATION	Les documents de gestion des risques sont mis à jour en fonction des activités de surveillance continue. [Cybersecurity Framework : RS.IM	]
TÂCHE M-5 : RAPPORTS DE SÉCURITÉ ET DE CONFIDENTIALITÉ	Un processus est en place pour rapporter l'état de la sécurité et de la confidentialité à l'autorité d'autorisation ainsi qu'à d'autres dirigeants et cadres supérieurs.	

Tâches	Résultats	Conseils spécifiques à l'OT
TÂCHE M-6 : AUTORISATION CONTINUE	Les responsables de l'autorisation effectuent des autorisations continues en utilisant les résultats des activités de surveillance continue et communiquent les changements dans la détermination des risques et les décisions d'acceptation.	
TÂCHE M-7 : ÉLIMINATION DU SYSTÈME	Une stratégie d'élimination des systèmes est développée et mise en œuvre, si nécessaire.	La durée de vie planifiée des composants IT peut ne pas s'appliquer aux composants OT. Tenez compte de l'entretien et de la réparation des composants OT qui doivent être maintenus au-delà de la disponibilité des composants IT.

CHAPITRE 5
THE PROTECTOR : APPLICATION DE SURVEILLANCE, DETECTION ET PREVENTION DES INTRUSIONS

CHAPITRE 5 THE PROTECTOR : APPLICATION DE SURVEILLANCE, DETECTION ET PREVENTION DES INTRUSIONS

Notre Projet Innovant spécialisé dans la cybersécurité des **Systèmes de Contrôle Industriels (ICS)** et des environnements **OT « ICS Cyber Protector** » dans le cadre de l'Arrêté Ministériel 1275. Notre objectif est de développer des solutions de protection avancées pour les infrastructures critiques, répondant aux défis croissants des cybermenaces dans le domaine industriel. En tant que première réalisation, **ICS Cyber Protector** a conçu **THE PROTECTOR v1**, un prototype, ce premier produit témoigne de l'engagement de la start-up à fournir des solutions évolutives et performantes pour sécuriser les réseaux industriels.

5.1 INTRODUCTION

THE PROTECTOR est une solution de pointe en cybersécurité, spécifiquement conçue pour la protection des Systèmes de Contrôle Industriels (ICS) et des Infrastructures Critiques. Grâce à son architecture innovante, **cette plateforme assure une surveillance continue** du réseau, **détecte et analyse en temps réel les menaces** potentielles à travers un tableau de bord intuitif.

THE PROTECTOR combine des technologies de détection avancées IDS/IPS, une visualisation claire des alertes et une personnalisation adaptée aux besoins industriels, garantissant une sécurité optimale face aux cyberattaques ciblées sur les environnements opérationnels les plus sensibles. Il s'agit d'un bouclier indispensable pour anticiper, identifier et neutraliser les menaces dans un monde où la cybersécurité des systèmes critiques est devenue un enjeu majeur.

5.2 OBJECTIFS DU PROJET

- **Développer une interface utilisateur conviviale** permettant la visualisation en temps réel des alertes et des données de sécurité réseau.
- **Fournir des outils avancés de visualisation et de gestion** des configurations, des règles et des services Suricata.
- **Assurer la compatibilité multiplateforme**, notamment avec les systèmes d'exploitation Ubuntu et Raspbian.
- **Intégrer des fonctionnalités de sécurité avancées**, telles qu'un scanner de vulnérabilités intégré et l'intégration de flux de renseignements sur les menaces

5.3 PERIMETRE FONCTIONNEL

5.3.1 Surveillance des Alertes

- **Affichage en temps réel des alertes** générées par Suricata.
- **Détails des alertes** : affichage des informations telles que l'horodatage, l'ID de la signature, la classification, la priorité, les adresses IP et ports impliqués, le protocole et le message d'alerte.
- **Filtrage et recherche des alertes** par différents critères (date, priorité, IP, etc.).

5.3.2 Interface Utilisateur

- **Tableau de bord personnalisable** avec des widgets pour la surveillance du réseau, les alertes actives et les performances du système.
- **Navigation intuitive** avec accès rapide aux principales fonctionnalités via des boutons sur la page d'accueil.

5.3.3 Outils de Visualisation

- **Graphiques et diagrammes interactifs** utilisant Chart.js et Plotly pour la visualisation des données en temps réel et historiques.
- **Analyse des tendances et des données historiques** pour identifier les motifs récurrents et les problèmes à long terme.

5.3.4 Gestion des Configurations

- **Accès et modification des fichiers de configuration Suricata** directement depuis le tableau de bord.
- **Gestion des règles Suricata** : possibilité de visualiser, ajouter, éditer et supprimer des règles.

5.3.5 État et Contrôle du Système

- **Surveillance de l'état du service NIDS** en temps réel avec des indicateurs de santé et de performance.
- **Fonctions de contrôle** : démarrer, arrêter et redémarrer le service NIDS depuis le tableau de bord.

5.3.6 Sécurité et Gestion des Vulnérabilités

- **Scanner de vulnérabilités intégrées** pour analyser le réseau et fournir des rapports exploitables.
- **Intégration de flux de renseignements sur les menaces** pour rester informé des dernières menaces et vulnérabilités.

5.3.7 Journalisation et Rapports

- **Collecte centralisée des journaux** utilisant Logstash et Fluentd.
- **Génération de rapports détaillés** sur l'activité du réseau, les alertes et les performances du système.

5.4 EXIGENCES TECHNIQUES ET TECHNOLOGIES UTILISEES

"THE PROTECTOR" est construit sur une pile technologique moderne qui garantit la scalabilité, les performances et la convivialité. Chaque composant de cette pile a été sélectionné pour répondre aux exigences de la surveillance en temps réel, de l'analyse des données et de la visualisation du trafic réseau.

5.4.1 Technologies Backend

- **Django REST Framework (DRF) :** L'API principale du backend est construite avec le Django REST Framework, responsable de la gestion des requêtes, des réponses, de l'authentification des utilisateurs et de l'acheminement des données de Suricata vers le frontend. DRF fournit une structure robuste et évolutive pour gérer un grand volume d'alertes et de journaux générés par les événements IDS/IPS.
- **Base de données PostgreSQL :** PostgreSQL est utilisée comme base de données principale pour stocker les journaux, les alertes et les données de trafic réseau. Sa conformité ACID et son support des requêtes complexes en font un choix idéal pour gérer et analyser de grands volumes de données structurées. PostgreSQL permet également l'indexation de champs spécifiques, comme les adresses IP et les horodatages, optimisant ainsi les recherches et les requêtes d'alerte.

5.4.2 Technologies Frontend

- **ReactJS :** Le frontend de "THE PROTECTOR" est développé avec ReactJS, permettant un rendu dynamique des données et une interface utilisateur hautement réactive. ReactJS garantit que le tableau de bord offre des mises à jour en temps réel du trafic réseau, des alertes et des journaux, offrant aux utilisateurs une expérience fluide lors de l'analyse des données.
- **Bibliothèques de visualisation :** La visualisation des données est mise en œuvre à l'aide de bibliothèques telles que MUI et D3.js pour générer des graphiques, des tableaux et des diagrammes qui permettent aux utilisateurs de comprendre facilement l'activité réseau et les alertes. Ces graphiques sont personnalisables, offrant aux utilisateurs différentes manières de visualiser les données réseau, telles que par période, protocole ou gravité des alertes.

5.4.3 Intégration IDS/IPS

- **Suricata IDS/IPS :** Suricata, un moteur IDS/IPS de nouvelle génération, est intégré à "THE PROTECTOR" pour effectuer une inspection approfondie des paquets (DPI) et analyser le trafic réseau en temps réel. La capacité de Suricata à traiter le trafic réseau à grande vitesse, combinée à ses méthodes de détection basées sur les signatures et les anomalies, lui permet de détecter à la fois les menaces connues et les comportements suspects.

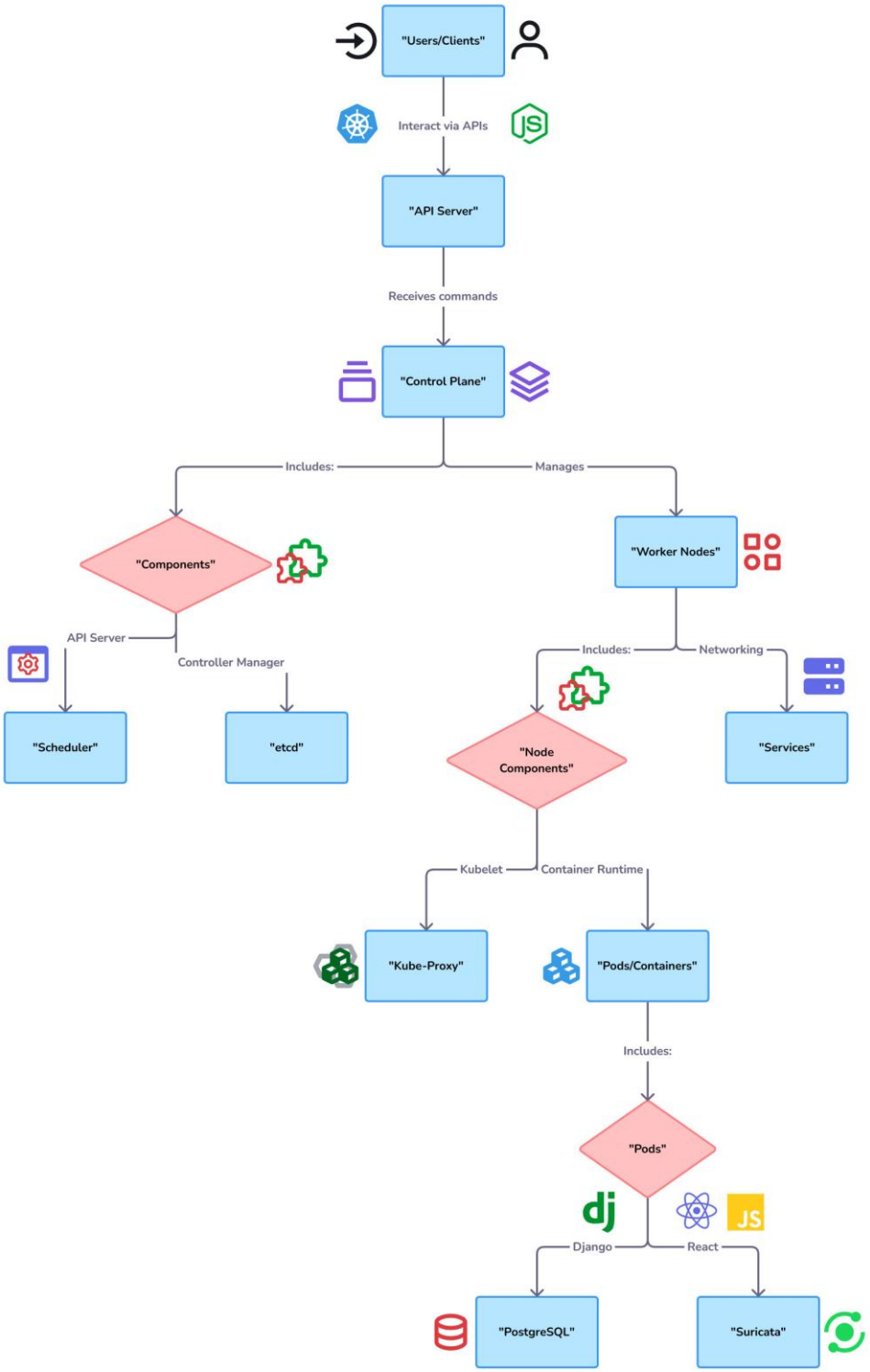


FIGURE 5. 1 : Architecture de l'application "THE PROTECTOR"

Les journaux de Suricata sont analysés et envoyés à l'API backend au format JSON, permettant à **"THE PROTECTOR"** de filtrer, catégoriser et afficher les alertes de manière efficace.

5.4.4 Pile de déploiement

- **Docker :** Des conteneurs Docker sont utilisés pour encapsuler les différents composants de "THE PROTECTOR", y compris l'API, le frontend et la base de données. Docker garantit que la plateforme est facilement déployable et évolutive sur plusieurs environnements, que ce soit sur site ou dans le cloud.
- **Pipelines CI/CD :** Les pipelines d'intégration continue et de déploiement continu (CI/CD) sont utilisés pour automatiser le processus de test et de déploiement. Cela garantit que les mises à jour de "THE PROTECTOR" sont systématiquement publiées avec un temps d'arrêt minimal, permettant aux utilisateurs d'accéder aux dernières fonctionnalités et améliorations.

5.4.5 Compatibilité

- **Systèmes d'exploitation** : Tous les systèmes.

5.5 AVANTAGES DE L'INTERFACE WEB "THE PROTECTOR V.1" :

5.5.1 Une Accessibilité Totale et Compatibilité avec "THE PROTECTOR"

Avec l'interface web "THE PROTECTOR v.1", les entreprises industrielles bénéficient d'une accessibilité inégalée pour la gestion de la sécurité de leurs systèmes.

L'opérateur ou l'administrateur de sécurité réseaux peut accéder à son tableau de bord IDS/IPS et SIEM à tout moment et en toute simplicité via un navigateur web. Compatible avec une multitude d'appareils (ordinateurs, tablettes, smartphones) et de systèmes d'exploitation, "THE PROTECTOR v.1" s'assure que les équipes de sécurité restent connectées à leurs infrastructures critiques, quelle que soit leur localisation.

Sur le plan technique, cela est rendu possible grâce à la combinaison d'un backend Django robuste et un frontend React réactif, garantissant une expérience utilisateur fluide et sécurisée.

5.5.2 Visualisation des Données de Sécurité Simplifiée et Personnalisée pour une Analyse Efficace

L'interface intuitive de "THE PROTECTOR v.1" transforme des volumes massifs de données réseau en visualisations interactives et faciles à interpréter. Graphes, diagrammes et cartes de chaleur aident les équipes de sécurité à identifier rapidement les tendances et les anomalies dans les réseaux industriels.

Grâce à l'intégration de bibliothèques graphiques avancées dans le frontend React, cette solution assure une analyse en temps réel, offrant une réactivité maximale face aux cybermenaces. Les utilisateurs peuvent, de plus, personnaliser leurs tableaux de bord pour adapter les métriques et les alertes aux besoins spécifiques de leurs environnements industriels.

Avec un backend basé sur Django et une base de données PostgreSQL, cette personnalisation est à la fois puissante et flexible, répondant aux exigences les plus complexes.

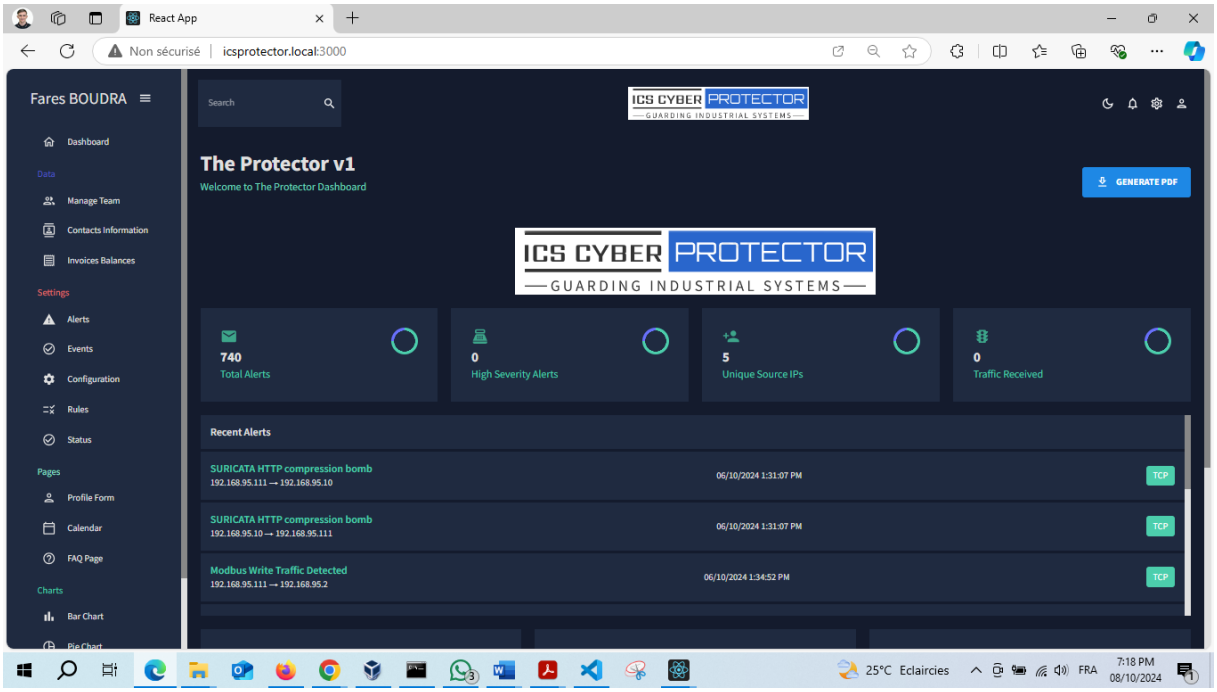


FIGURE 5. 2 : Tableau de bord (dashboard) en mode sombre

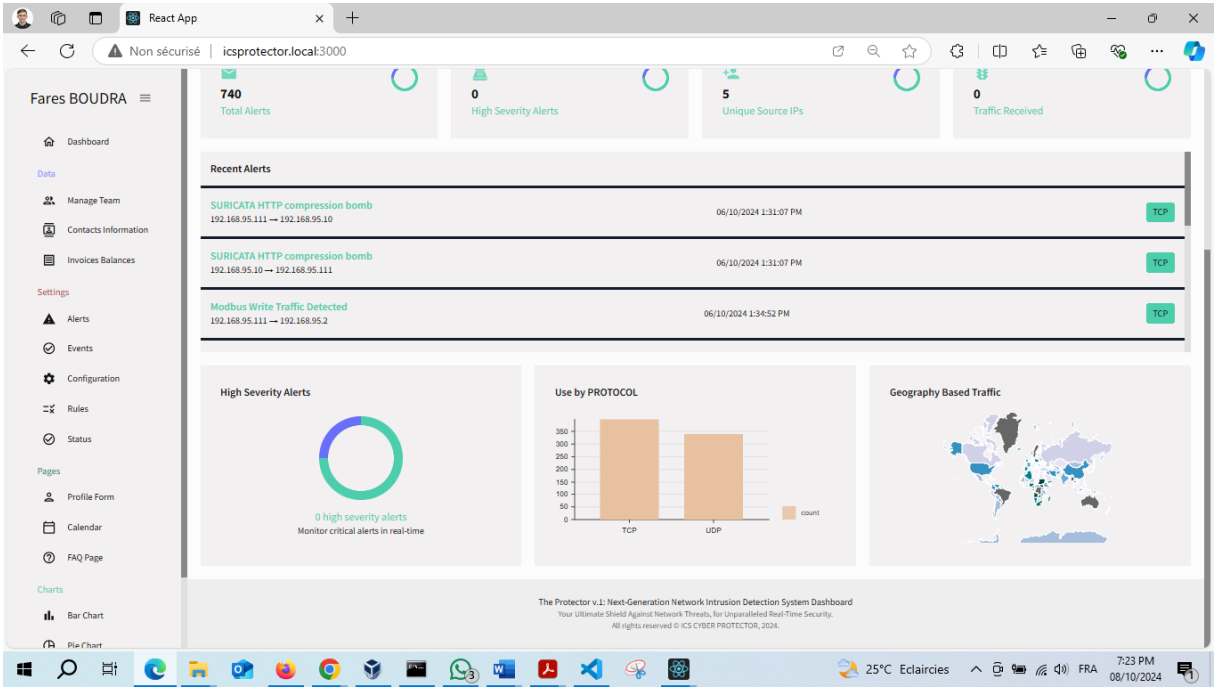


FIGURE 5. 3 : En mode claire

5.5.3 Intégration Transparente et Collaboration Renforcée pour une Synergie Sécuritaire Totale

"The Protector v.1" se distingue par sa capacité à s'intégrer facilement à d'autres solutions de sécurité via des API robustes, permettant une consolidation fluide des données et une vue d'ensemble de l'infrastructure. Que vous souhaitiez combiner vos données avec des outils SIEM ou étendre les fonctionnalités avec d'autres IDS, cette interface facilite l'interconnexion des systèmes. Sur le plan commercial, cela permet d'offrir une solution évolutive et adaptable, en ligne avec les besoins croissants des entreprises. De plus, le partage simplifié des informations de sécurité entre les membres des équipes renforce la collaboration et accélère la prise de décisions critiques.

Ce processus est soutenu par une architecture backend optimisée sur Django et des mécanismes d'authentification sécurisés, garantissant un partage d'informations sans compromis sur la sécurité.

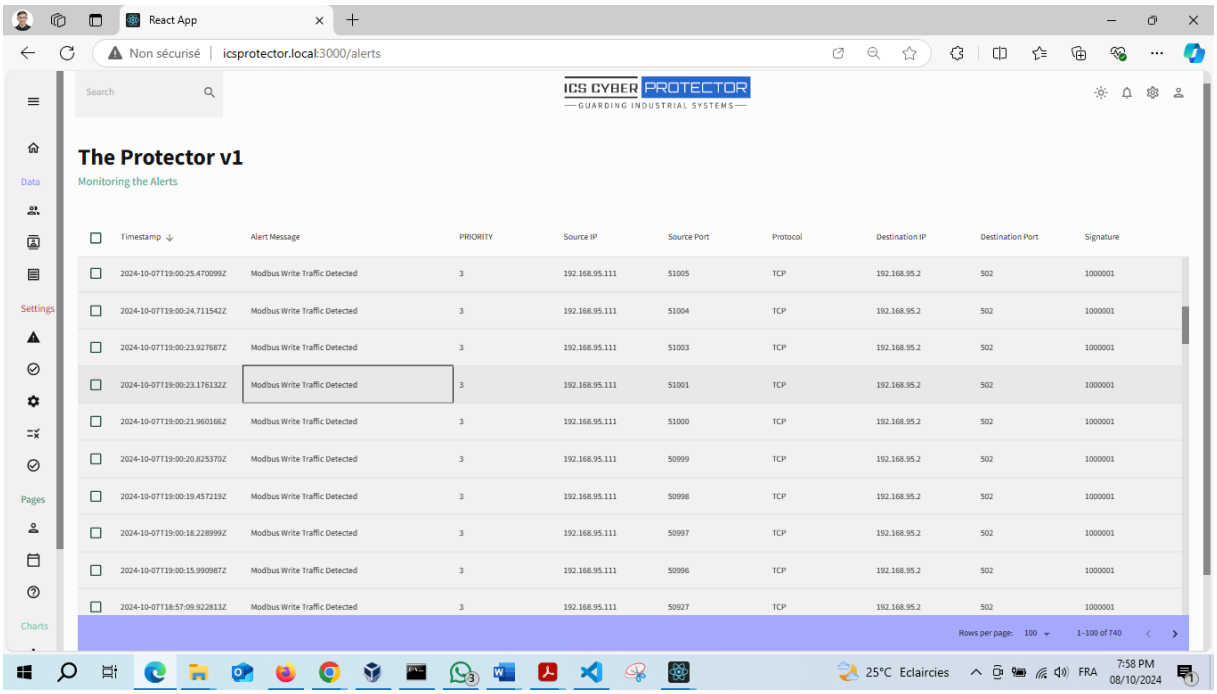


FIGURE 5. 4 : Tableau des alertes

5.5.4 Gestion Centralisée et Évolutivité Illimitée pour les Entreprises de Toutes Tailles

"La gestion des systèmes IDS/IPS est simplifiée grâce à la centralisation de toutes les opérations via "THE PROTECTOR v.1".

Depuis une seule interface web, les administrateurs peuvent surveiller et gérer plusieurs instances de systèmes de sécurité, réduisant ainsi les coûts opérationnels et améliorant l'efficacité globale de l'administration des réseaux industriels.

Grâce à son architecture modulaire, cette solution peut facilement évoluer pour répondre à l'augmentation des volumes de données, garantissant une performance optimale même dans les environnements les plus exigeants. Ce niveau d'évolutivité est rendu possible par l'utilisation

de technologies comme Docker et Suricata, qui permettent une configuration rapide et adaptée à chaque client, tout en assurant une maintenance centralisée et une gestion des ressources réseau sur mesure."

En définitive, "THE PROTECTOR v.1" se positionne comme bien plus qu'un simple outil de détection d'intrusions. Avec son interface web innovante, ses puissantes fonctionnalités techniques et son architecture évolutive, il incarne une solution de cybersécurité complète pour les entreprises industrielles. Capable d'adapter ses fonctionnalités aux besoins spécifiques des environnements ICS, THE PROTECTOR v.1 offre une solution clé en main pour garantir la protection des infrastructures critiques face aux cybermenaces croissantes.

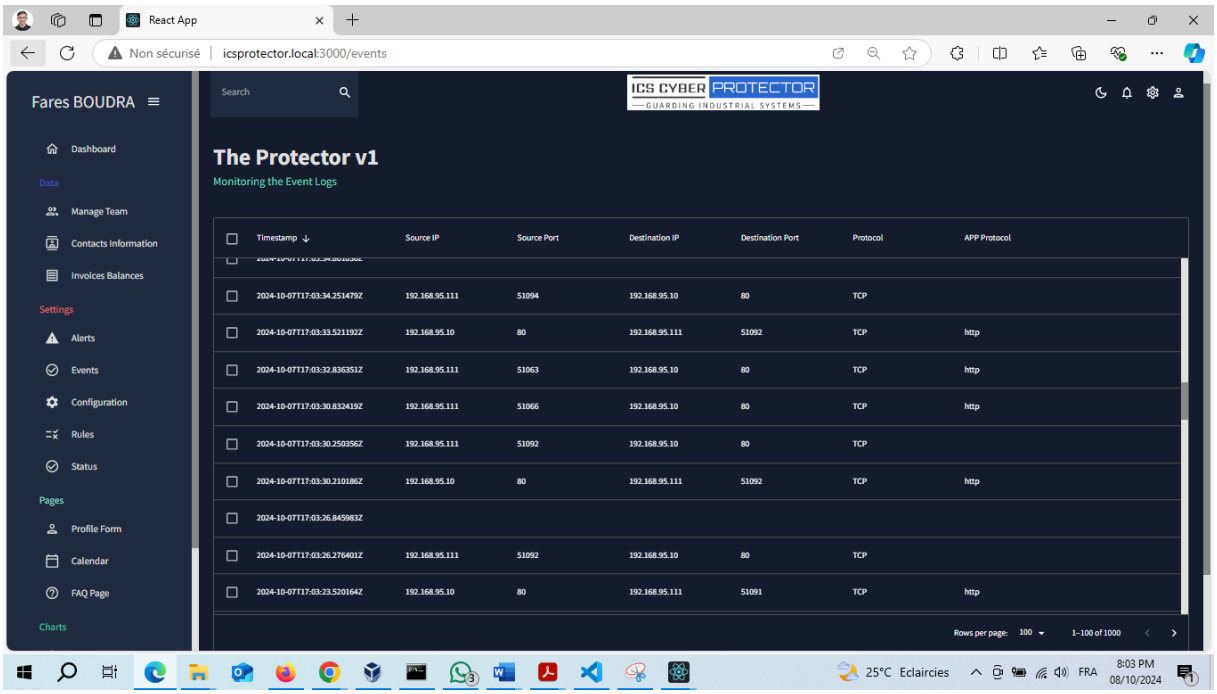
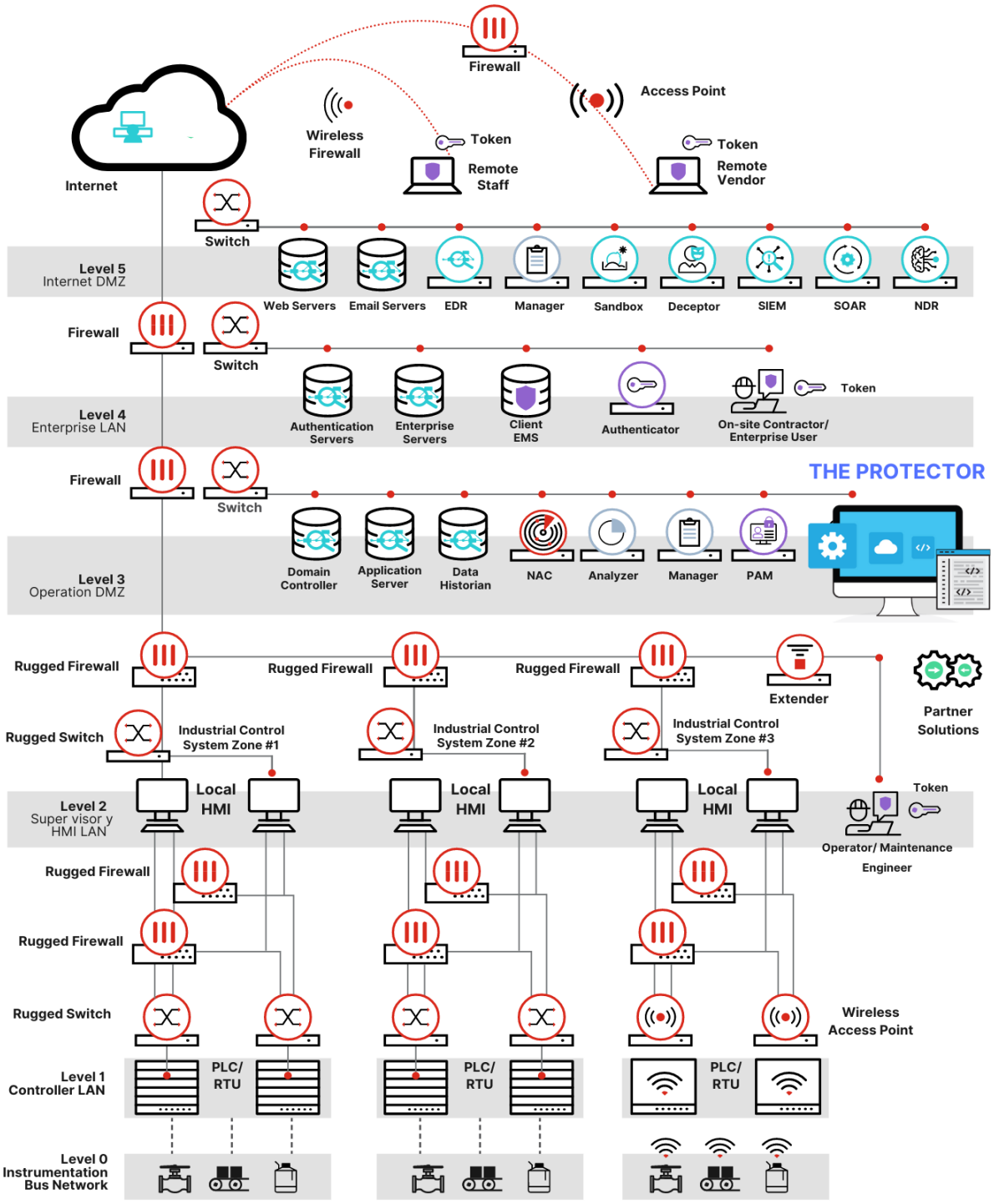


FIGURE 5. 5 : Tableau des évènements

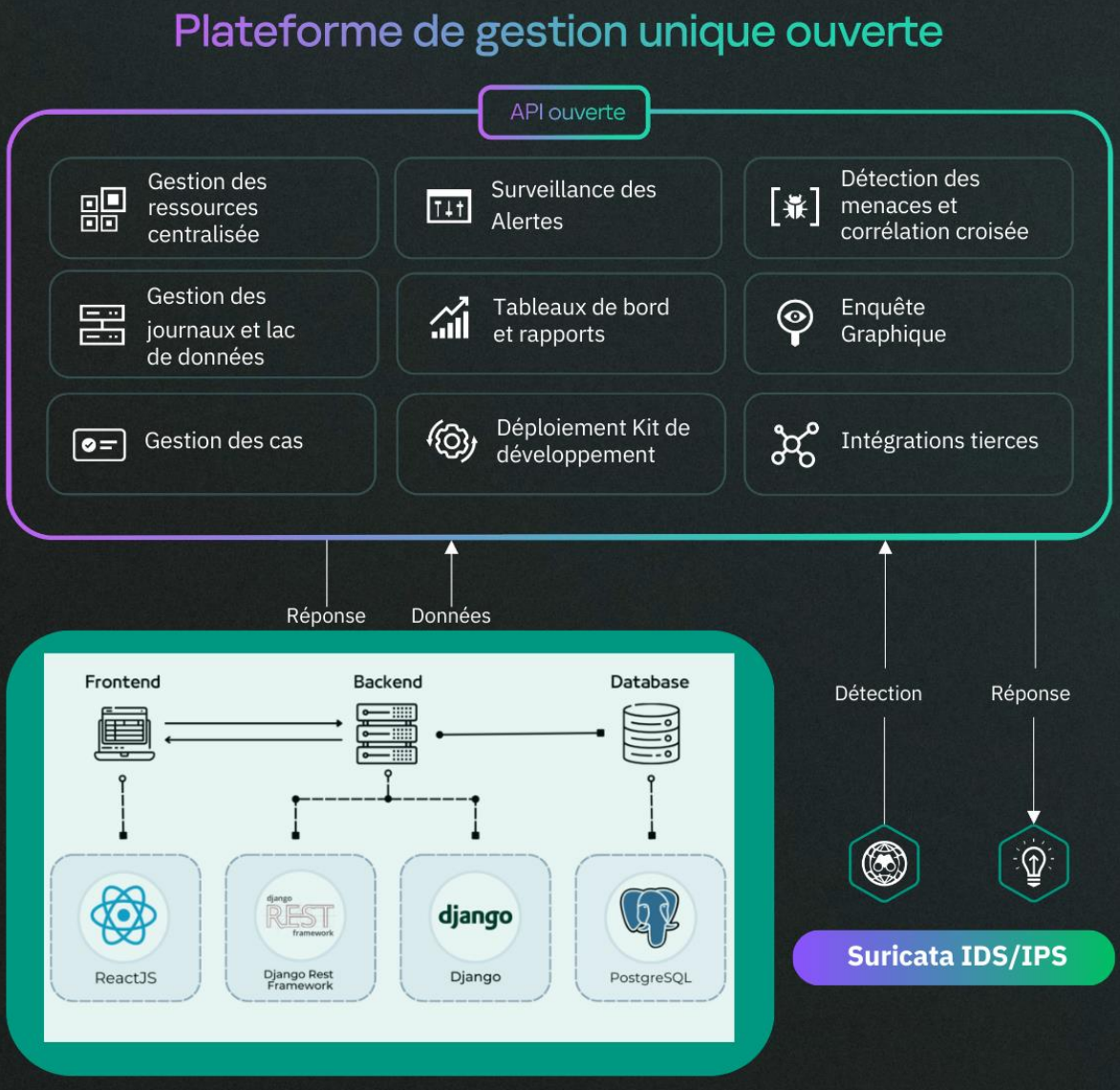


Securing layers 0,1,2 and 3 of the Purdue Model using THE PROTECTOR solution across a connected IT and OT infrastructure.

FIGURE 5. 6 : Installation de la solution THE PROTECTOR au niveau 3

THE PROTECTOR

Tableau de bord de nouvelle génération pour les systèmes de détection d'intrusion réseau, un moteur de corrélation ainsi que des réponses automatisées. Il est possible d'ajouter des connecteurs tiers pour rassembler toutes les données.



Avec ***THE PROTECTOR***, offrez à votre entreprise industrielle une solution de cybersécurité ultra-performante, capable de détecter, analyser et neutraliser les menaces en temps réel, tout en garantissant une protection proactive et évolutive pour vos systèmes de contrôle critiques. Découvrez l'avenir de la sécurité industrielle avec une interface intuitive et des technologies avancées, conçues pour assurer la continuité de vos opérations et la protection de vos infrastructures les plus sensibles.

5.6 TEST ET SCENARIOS D'APPLICATION

Cette partie détaille l'expérimentation de la solution de cybersécurité "THE PROTECTOR" dans le cadre du Lab **GRFICS** [Graphical Realism Framework for Industrial Control Simulations].

GRFICS a été développé pour surmonter les obstacles à l'entrée en matière de sécurité des systèmes de contrôle industriels (ICS), en offrant une simulation complète des réseaux ICS dans un environnement virtuel réaliste.

L'objectif est d'évaluer la capacité de "THE PROTECTOR" à détecter les anomalies réseau dans cet environnement.

5.6.1 Présentation du Lab GRFICS

Le Lab GRFICS simule un réseau ICS, intégrant des composants critiques comme l'interface homme-machine (HMI), les contrôleurs logiques programmables (PLC) et les modules d'entrées/sorties (I/O). Il permet de visualiser des processus physiques en 3D, offrant ainsi une meilleure compréhension des impacts potentiels des attaques cybernétiques sur les infrastructures industrielles.

Le réseau inclut une simulation de processus chimiques complexes, basés sur le modèle simplifié de l'usine chimique Tennessee Eastman, où des valves et capteurs contrôlent des paramètres critiques tels que la pression et le débit des réacteurs chimiques.

Version 2 du Framework de réalisme graphique pour la simulation de contrôle industriel (GRFICS)

Cette version de GRFICS est organisée en 5 machines virtuelles VirtualBox (une simulation 3D, un PLC logiciel, une IHM, un pare-feu pfsense et une station de travail) communiquant entre elles sur des réseaux virtuels réservés à l'hôte. Pour une explication plus détaillée de l'ensemble du framework et des informations générales sur les réseaux ICS, référez au document de l'atelier situé à l'adresse :

https://www.usenix.org/sites/default/files/conference/protected-files/ase18_slides_formby.pdf

https://www.usenix.org/system/files/conference/ase18/ase18-paper_formby.pdf

Une série de vidéos expliquant la configuration de la machine virtuelle et des exemples d'attaques est disponible sur la chaîne YouTube de Fortiphyd à l'adresse

https://www.youtube.com/playlist?list=PL2RSrzaDx0R670yPlYPqM51guk3bQjFG5

Simulation

La machine virtuelle de simulation (appelée ChemicalPlant) exécute une simulation réaliste d'une réaction de processus chimique contrôlée et surveillée par des périphériques d'E/S distants simulés via une API JSON simple. Ces périphériques d'E/S distants sont ensuite surveillés et contrôlés par la machine virtuelle PLC à l'aide du protocole Modbus. Cette machine virtuelle est située dans le sous-réseau du réseau ICS (192.168.95.0/24) avec les adresses IP 192.168.95.10-192.168.95.15

FIGURE 5. 7 : Simulation

PLC

La machine virtuelle PLC (nommée plc_2) est une version modifiée d'OpenPLC (https://github.com/thiagoralves/OpenPLC_v2) qui utilise une ancienne version de la bibliothèque libmodbus avec des vulnérabilités connues de dépassement de mémoire tampon. Cette machine virtuelle est située dans le sous-réseau du réseau ICS (192.168.95.0/24) à 192.168.95.2

Interface homme-machine

La machine virtuelle HMI (nommée ScadaBR) contient principalement une IHM opérateur créée à l'aide du logiciel gratuit ScadaBR. Cette IHM est utilisée pour surveiller les mesures de processus collectées par l'automate et envoyer des commandes à l'automate. Cette machine virtuelle est située dans le sous-réseau du réseau DMZ (192.168.90.0/24) à 192.168.90.5

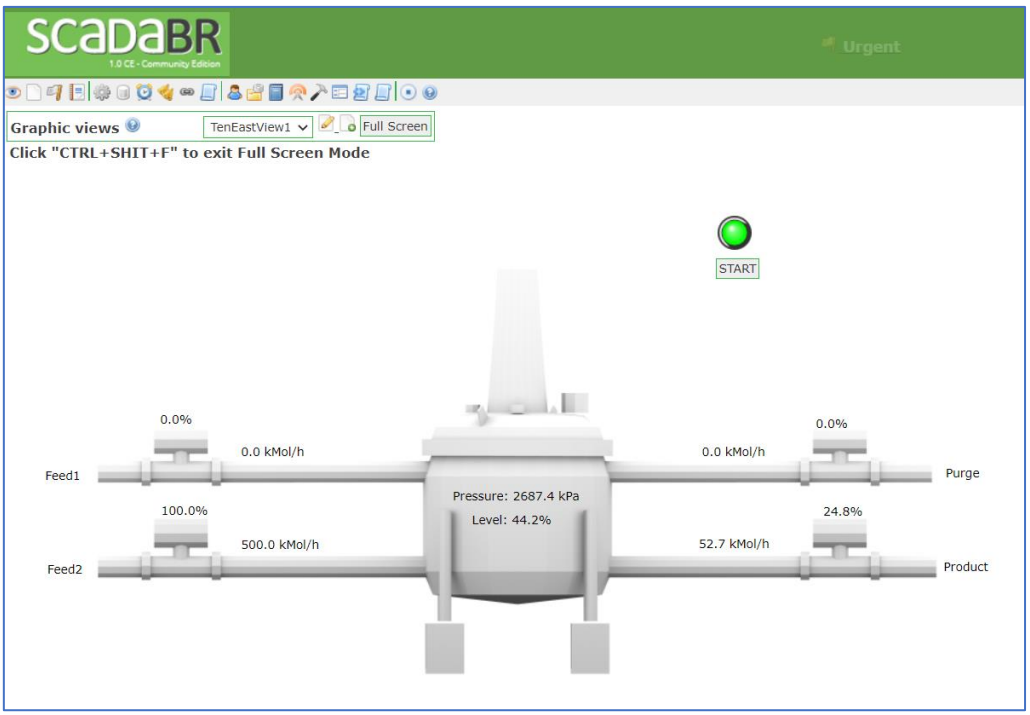


FIGURE 5. 8 : SCADABR (HMI)

PfSense Firewall/Router

The firewall VM (named pfSense) provides routing and firewall features between the DMZ and ICS network. The WAN interface is on the DMZ subnet (192.168.90.0/24) at 192.168.90.100 and the LAN interface is on the ICS subnet (192.168.95.0/24) at 192.168.95.1

Engineering Workstation

The workstation VM is an Ubuntu 16.04 machine with software used for programming the OpenPLC. The workstation is located in the ICS network (192.168.95.0/24) at 192.168.95.5.

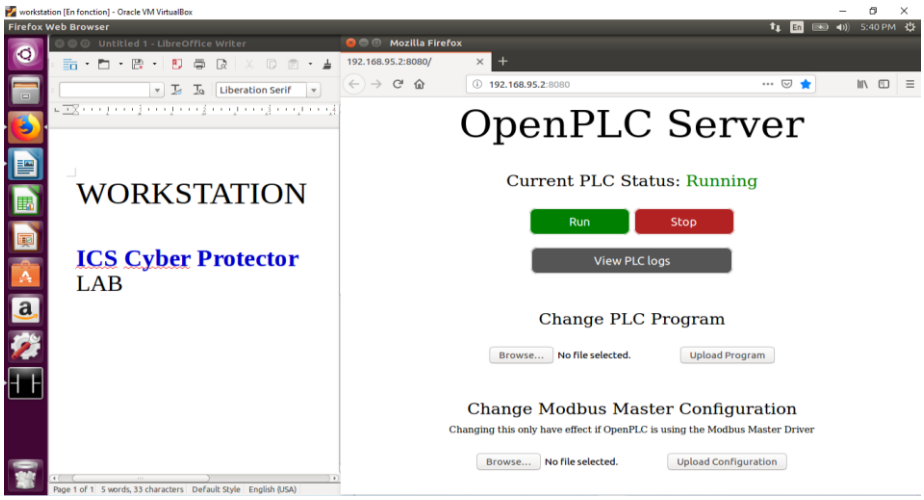


FIGURE 5. 9 : Workstation

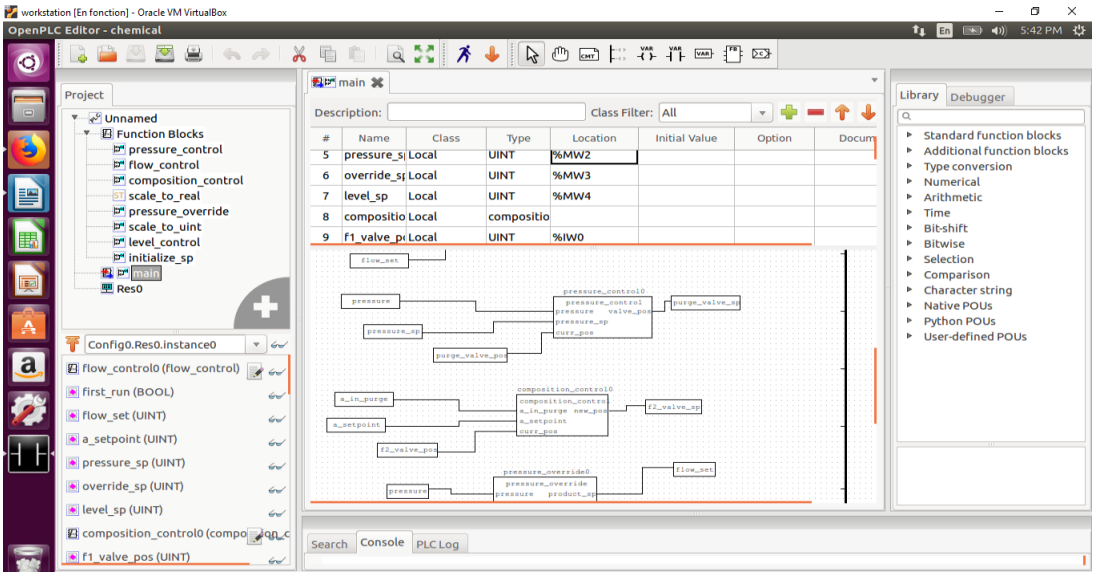


FIGURE 5. 10 : Logiciel OPENPLC dans la machine Workstation

5.6.2 Objectifs du Test

Le test vise à déterminer si "THE PROTECTOR" peut efficacement détecter des anomalies dans le trafic réseau du Lab GRFICS, notamment des attaques courantes dans les environnements ICS, telles que :

- **Injection de commandes Modbus** : En raison de l'absence d'authentification native dans le protocole Modbus, il est fréquent que des commandes malveillantes soient injectées pour manipuler le comportement du processus physique.

5.6.3 Méthodologie

Le test est conduit dans un réseau virtuel, où "THE PROTECTOR" sera configuré pour analyser et surveiller le trafic réseau. Les principales étapes sont les suivantes :

1. **Déploiement de THE PROTECTOR** : Connecter la solution au réseau ICS simulé dans GRFICS afin de surveiller les communications entre les composants (HMI, PLC, modules I/O).
2. **Injection d'anomalies** : Des attaques simulées seront effectuées, telles que l'injection de commandes Modbus non autorisées, des attaques MITM, et la modification des programmes PLC.
3. **Surveillance et détection** : "THE PROTECTOR" surveille en temps réel les flux de données pour identifier les comportements suspects ou les violations de sécurité.
4. **Réaction et alerte** : L'outil doit générer des alertes et des notifications pour toute activité anormale détectée, permettant ainsi aux opérateurs de réagir rapidement.

5.6.4 Arrêt du processus

Nous avons trouvé la vidéo de *Fortiphyd* pour injecter des commandes Modbus malveillantes, en utilisant *Metasploit*, pour arrêter le processus très claire et concise. Étant donné que nous avons mis un lien vers la chaîne YouTube et la vidéo pertinente, et qu'ils font

un si bon travail d'enseignement sur la façon d'utiliser *Metasploit* pour attaquer le réseau, même dans les réseaux traditionnellement non sécurisés comme ceux que l'on trouve dans la technologie opérationnelle (OT), quelqu'un qui lance des commandes *Metasploit* peut courir le risque de déclencher des sonnettes d'alarme. Comme nous l'avons évoqué plus tôt, nous avons décidé d'utiliser une méthode différente pour apporter les modifications malveillantes au processus chimique : *mbtget*.

Utilisation d'arp-scan :

```
┌──(root㉿kali)-[~]
└─# arp-scan --interface=eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:07:33:9f, IPv4: 192.168.95.116
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.95.1    08:00:27:d4:e1:1a       PCS Systemtechnik GmbH
192.168.95.2    08:00:27:39:62:d8       PCS Systemtechnik GmbH
192.168.95.10   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.11   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.12   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.13   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.14   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.15   08:00:27:49:b7:03       PCS Systemtechnik GmbH
192.168.95.111  0a:00:27:00:00:18       (Unknown: locally administered)
192.168.95.112  08:00:27:48:f9:0d       PCS Systemtechnik GmbH
192.168.95.113  08:00:27:be:9f:19       PCS Systemtechnik GmbH

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.970 seconds (129.95 hosts/sec). 1
1 responded

┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:38:a9, IPv4: 192.168.90.116
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.90.5    08:00:27:41:ff:18       PCS Systemtechnik GmbH
192.168.90.100  08:00:27:6b:9f:74       PCS Systemtechnik GmbH
192.168.90.111  0a:00:27:00:00:15       (Unknown: locally administered)
192.168.90.112  08:00:27:e1:bd:11       PCS Systemtechnik GmbH
192.168.90.117  08:00:27:b1:68:56       PCS Systemtechnik GmbH
```

FIGURE 5. 11 : Utilisation d'arp-scan

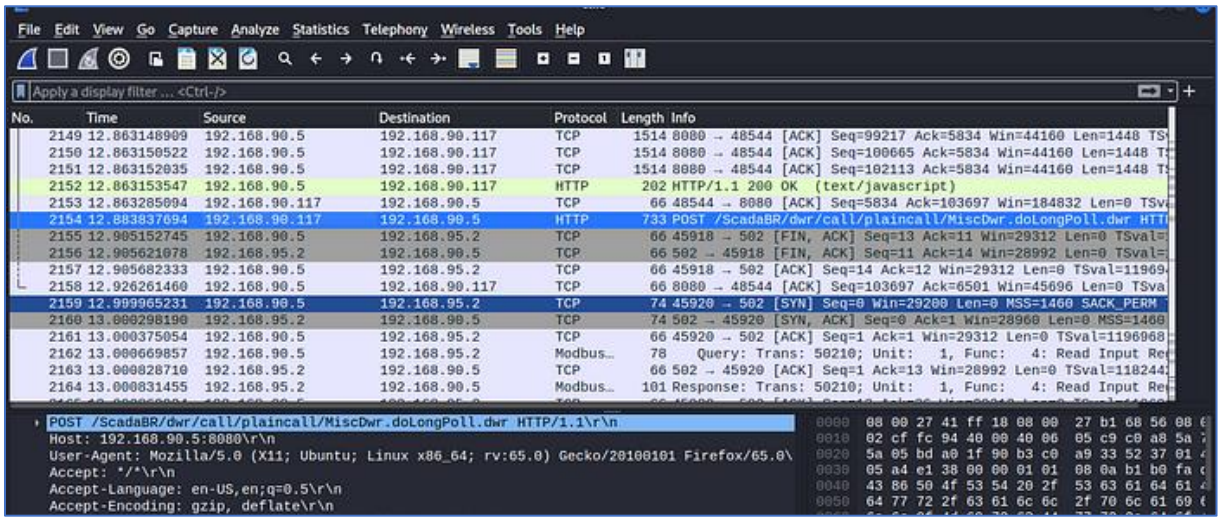


FIGURE 5. 12 : Première analyse avec Wireshark

Nous sommes donc déjà sur le réseau OT et l'avons cartographié. Alors, tout d'abord, ouvrez Wireshark et examinons les appareils qui communiquent entre eux. Nous voyons d'abord 192.168.90.117 et 192.168.90.5 envoyer des paquets HTTP via le port TCP 8080, donc en creusant un peu plus.

La visite de la page nous amène à ce qui ressemble à une HMI ScadaBR. Certains attaquants habitués au piratage des systèmes informatiques pourraient immédiatement rechercher le logiciel et essayer de trouver des exploits publics pour les vulnérabilités, mais rien de tout cela n'est nécessaire ici.

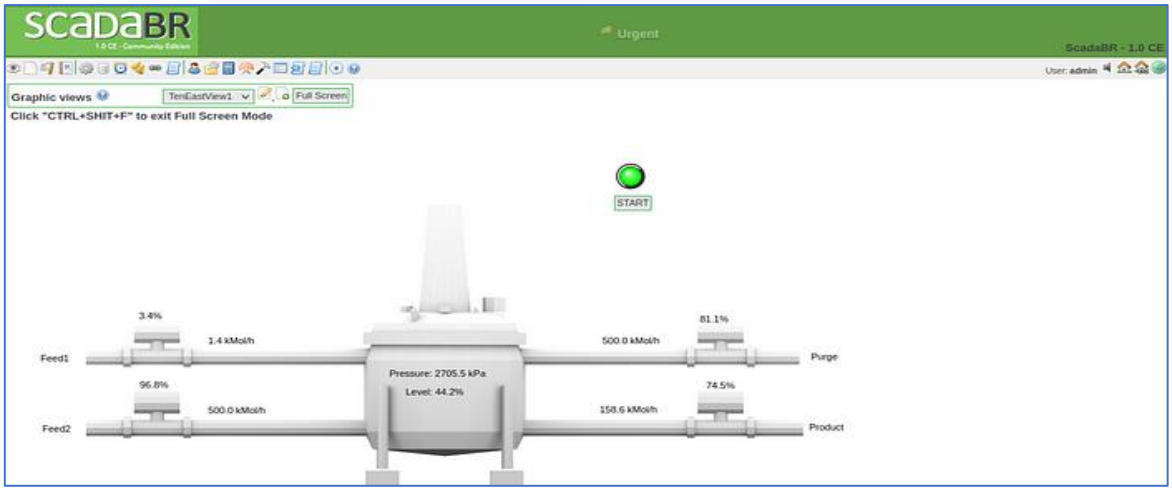


FIGURE 5. 13 : Vue de SCADABR (HMI)

Nous pouvons donc maintenant voir en temps réel comment les changements de valeurs affectent le processus chimique. D'après les résultats de cette interface utilisateur, il semble que le réservoir principal soit conçu pour rester entre 2 650 et 2 750 kPa. Nous surveillons le processus, alors essayons maintenant de trouver des moyens d'y apporter des modifications. Pour cela, revenons à Wireshark. Démarrez une nouvelle capture et définissez le filtre sur modbus en saisissant ce qui suit dans le filtre d'affichage et en appuyant sur ENTRÉE.

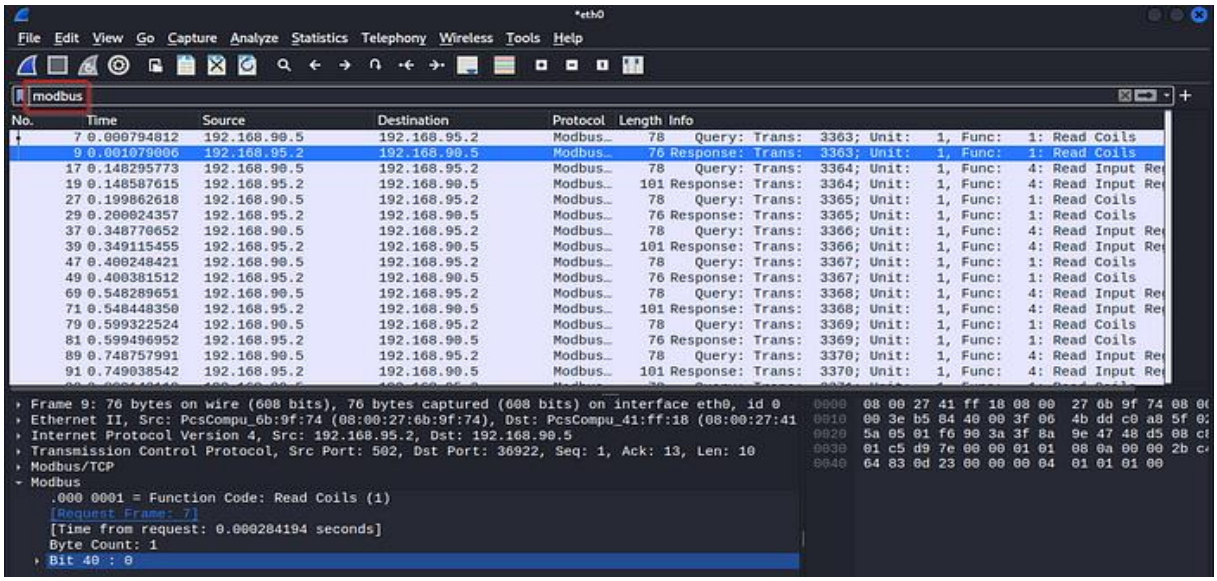


FIGURE 5. 14 : Le filtrage des résultats de scan Wireshark

Vous remarquerez donc assez rapidement que le périphérique 192.168.95.2, probablement un automate, continue d'envoyer des communications à 192.168.90.5 à raison d'un octet. Il s'agit d'un seul octet à l'adresse 40.

Le fait qu'ils continuent à envoyer cela encore et encore suggère que cela pourrait être important ! Voyons ce qui se passe lorsque nous définissons cette valeur sur 1.

Encore une fois, je ne vais pas revenir sur ce que Fortiphyd a démontré dans sa vidéo, je vais donc me concentrer ailleurs. Nous avons téléchargé mbtget, alors mettons-le en pratique.

Les bits sont l'endroit sur lequel nous devons nous concentrer ici, alors lisons d'abord la valeur. Nous choisissons donc -r1. Nous utilisons l'indicateur -a pour l'adresse modbus, qui est 40, le port est le port modbus par défaut de 502, puis enfin l'IP cible :

```
┌──(root㉿kali)-[~]
└─# mbtget -r1 -a 40 -p 502 192.168.95.2
values:
  1 (ad 00040):     0
```

FIGURE 5. 15 : La lecture de la valeur d'adresse 40

Voyons ce qui se passe si nous le mettons à 1. Tout ce que nous avons à faire est de changer le drapeau initial de -r1 à w5, puis de lui donner la valeur 1

```
┌──(root㉿kali)-[~]
└─# mbtget -w5 1 -a 40 -p 502 192.168.95.2
bit write ok
```

FIGURE 5. 16 : L'écriture de la valeur "1" dans l'adresse 40

Vérifions à nouveau notre HMI :

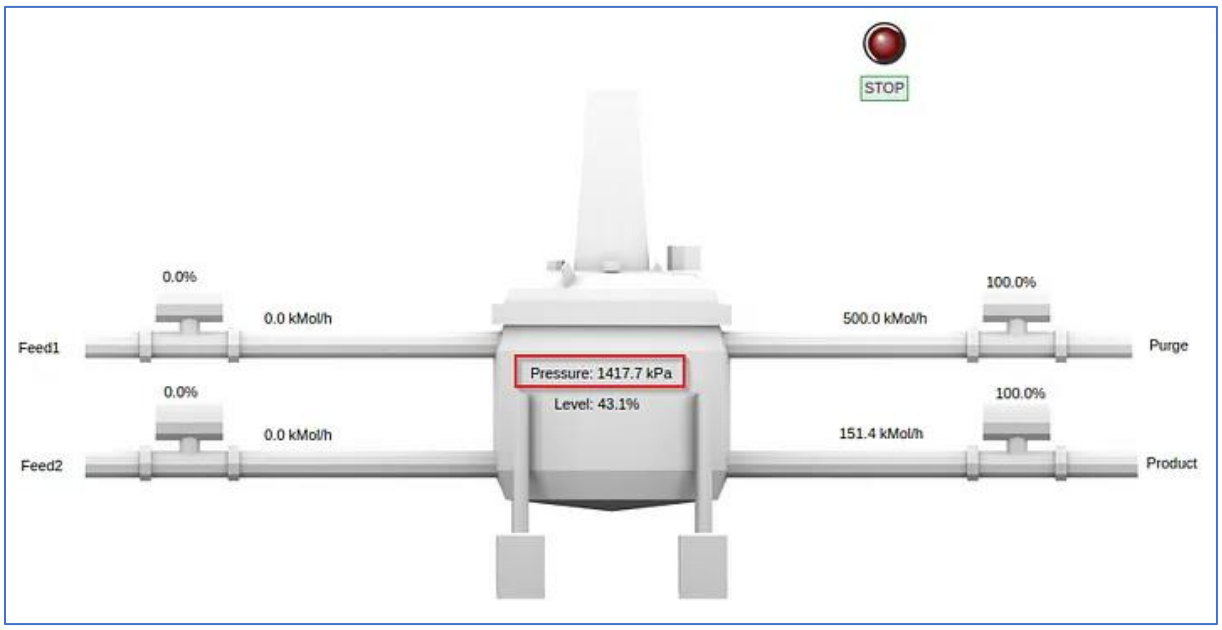


FIGURE 5. 17 : La chute de plus de 1000 KPA EN moins d'une minute

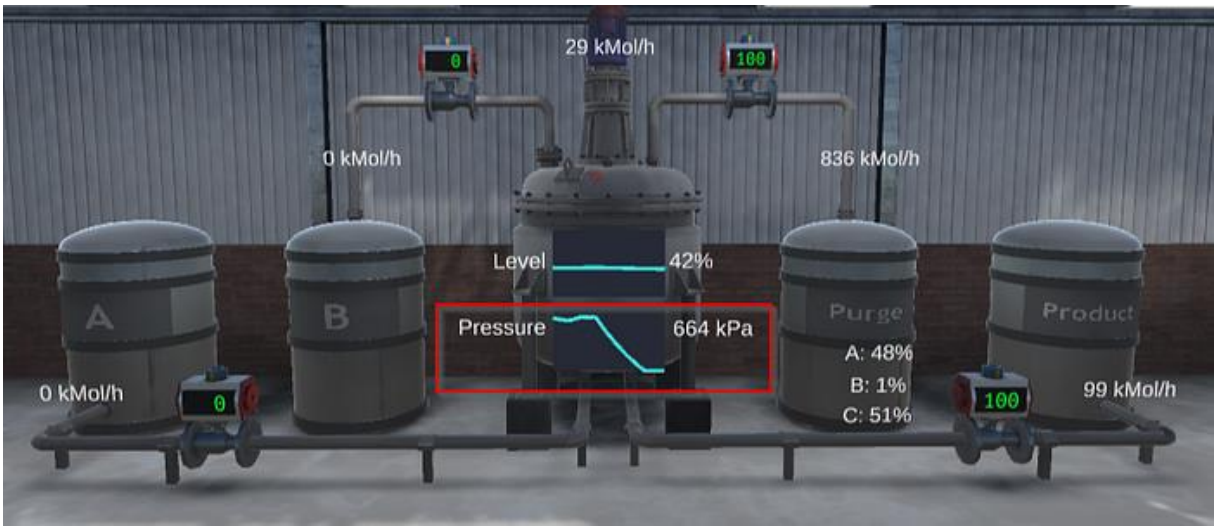


FIGURE 5. 18 : Réussite de l'attaque

5.6.5 Résultats Attendus

Les résultats de ce test évalueront la capacité de "THE PROTECTOR" à :

- Détecter les tentatives d'injection de commandes malveillantes via le protocole Modbus.
- Fournir des recommandations pour renforcer la sécurité des réseaux ICS grâce à la segmentation réseau et la mise en place de règles de pare-feu et d'intrusion (IDS/IPS).

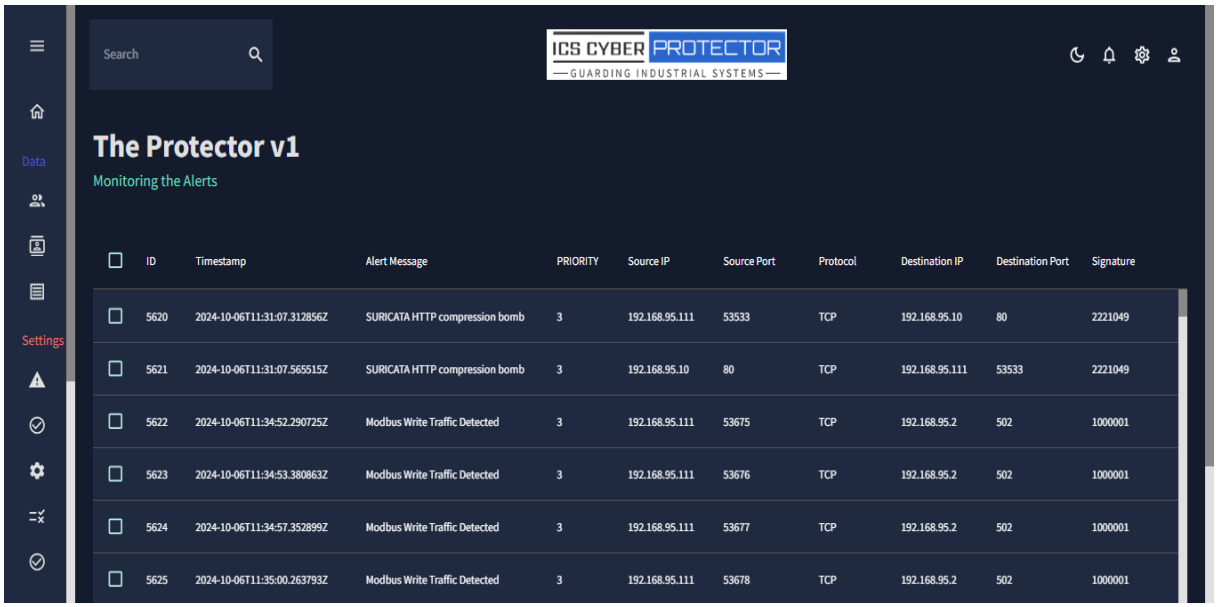


FIGURE 5. 19 : Affichage de l'alerte

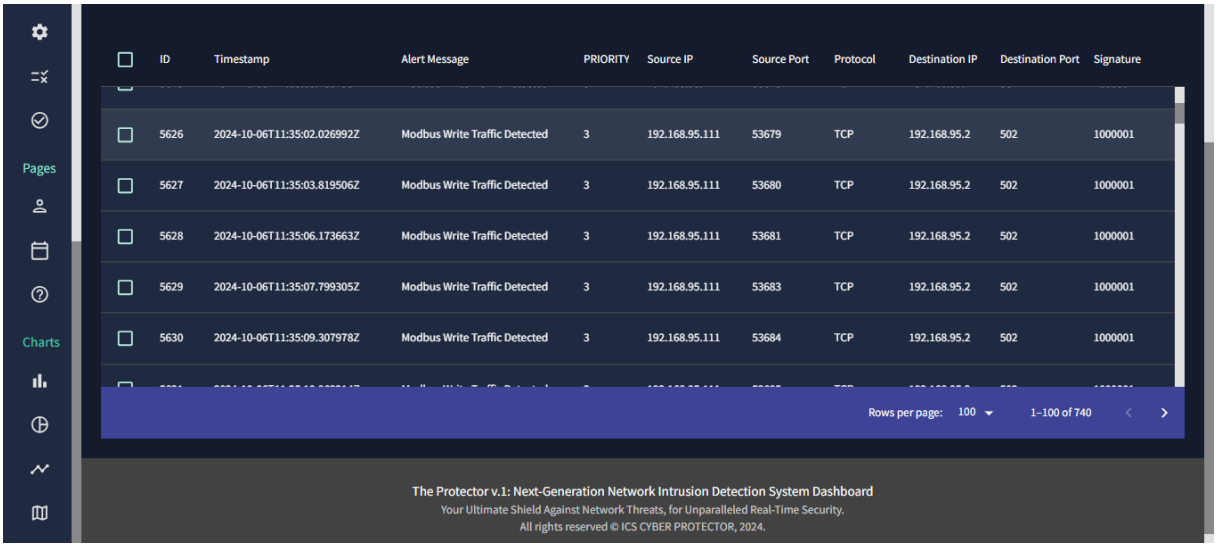


FIGURE 5. 20 : Affichage de l'alerte

5.6.6 Conclusion

Le Lab. GRFICS fournit un environnement contrôlé mais réaliste pour tester des solutions de cybersécurité comme "THE PROTECTOR". Ce test permettra de valider l'efficacité de la solution dans un cadre ICS virtuel avant son déploiement dans des environnements industriels réels. Si "THE PROTECTOR" réussit à détecter les anomalies du réseau GRFICS, cela prouvera son utilité pour protéger les infrastructures critiques en Algérie et dans d'autres secteurs industriels.

CONCLUSION GENERALE

CONCLUSION GENERALE

Ce mémoire s'est concentré sur la cybersécurité des systèmes de contrôle industriels (ICS) dans les infrastructures critiques, en particulier à travers l'implémentation et l'évaluation de solutions de détection et de prévention d'intrusion (IDS/IPS). L'objectif principal était d'analyser les risques liés à l'intégration de nouvelles technologies dans ces systèmes critiques, de proposer des approches adaptées pour renforcer la sécurité des environnements OT, et de fournir des solutions spécifiques telles que "**THE PROTECTOR**", un tableau de bord pour la supervision de la sécurité réseau.

Dans un contexte où les ICS sont de plus en plus interconnectés et exposés aux cybermenaces, il est primordial d'adopter des mesures de protection avancées. Nos recherches ont démontré l'efficacité des technologies IDS/IPS de nouvelle génération pour renforcer la sécurité des réseaux ICS/OT, en détectant les anomalies et en prévenant les attaques ciblées. La segmentation du réseau, combinée à l'implémentation de solutions de monitoring et d'analyse en temps réel, permet de réduire considérablement les risques de compromission des systèmes critiques.

Le développement de **"THE PROTECTOR"**, une plateforme de visualisation dédiée, a permis d'améliorer la gestion des alertes et la supervision du trafic réseau, en offrant aux opérateurs un outil efficace pour surveiller en continu les événements de sécurité. Cette solution, personnalisée pour les environnements industriels, représente une avancée significative dans la gestion des menaces pour les infrastructures critiques.

Malgré ces avancées, il est évident que la cybersécurité des ICS/OT reste un défi en constante évolution. Les menaces se complexifient, et les systèmes industriels continuent de s'adapter aux nouvelles technologies, ce qui implique une surveillance continue et l'amélioration régulière des outils de protection. Il est impératif que les futures recherches continuent à explorer des solutions innovantes pour garantir une meilleure résilience face aux cyberattaques, tout en tenant compte des contraintes spécifiques des systèmes OT, comme la disponibilité en temps réel et la sécurité des opérations.

En conclusion, ce travail a non seulement contribué à l'amélioration des pratiques actuelles de cybersécurité des systèmes industriels, mais il a aussi ouvert des perspectives pour le développement de nouvelles approches, alliant technologie et gouvernance, pour répondre aux besoins croissants de sécurisation des infrastructures critiques.

BIBLIOGRAPHIE

Algeria - Safety and Security. (s.d.). (U.S. Embassies abroad.) Consulté le Septembre 04, 2024, sur Privacy Shield: https://www.privacyshield.gov/ps/article?id=Algeria-Safety-and-Security

Algeria Country Report. (2023, Juin 13). Consulté le Mai 4, 2024, sur crisis24: https://crisis24.garda.com/insights-intelligence/intelligence/country-reports/algeria

Anderson, M. (2019, 05 13). *What is DCS? (Distributed Control System)*. Consulté le Septembre 05, 2024, sur REALPARS: https://www.realpars.com/blog/dcs

Anderson, N. (2012, Janvier 6). *Confirmed: US and Israel created Stuxnet, lost control of it*. Consulté le Septembre 05, 2024, sur arstechnica: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Bai, J., & Liu, Y. (2023, Octobre). Survey on Application of Trusted Computing in Industrial Control Systems. *Researchgate*. Consulté le Septembre 08, 2024, sur https://www.researchgate.net/figure/The-typical-architecture-of-industrial-control-systems_fig1_374565596

Balbix, Inc. (2024). *OT and ICS Security: The Next Big Challenge*. Consulté le Septembre 15, 2024, sur BALBIX: https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge/

Booz Allen Hamilton Inc. (2020). *Establishing an ICS/OT threat detection and response program.* Consulté le Septembre 07, 2024, sur https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/establishing-an-ot-threat-detection-program.pdf

Brooks SW, G. M. (2017). *An Introduction to Privacy Engineering and Risk Management in Federal Systems.* NIST Internal or Interagency Report (IR) 8062, National Institute of Standards and Technology, Gaithersburg, MD. Consulté le Septembre 21, 2024, sur https://doi.org/10.6028/NIST.IR.8062

CESI Centre de l'Expertise en Sécurité de l'Information. (2024-03-27). *Segmentation réseau.* Consulté le Septembre 05, 2024, sur https://reseau.uquebec.ca/system/files/documents/segmentation-reseau-v1-2-20240501.pdf

Check Point Software Technologies Ltd. (2024, Septembre 07). *Purdue Model for ICS Security*. Récupéré sur CHECK POINT: https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

Check Point Software Technologies Ltd. (s.d.). *Qu'est-ce que la segmentation du réseau ?* Consulté le 09 07, 2024, sur https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-network-segmentation/

Check Point Software Technologies Ltd. (s.d.). *Qu'est-ce que la segmentation du réseau ?* Consulté le Septembre 15, 2024, sur CHECK POINT: https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-network-segmentation/

CISA. (s.d.). Consulté le Septembre 01, 2024, sur CISA (Critical Infrastructure Security and resilience Agency): https://www.cisa.gov/

Cloudflare, Inc. (2024). *Qu'est-ce que la segmentation du réseau ?* Consulté le Septembre 07, 2024, sur CLOUDFLARE: https://www.cloudflare.com/fr-fr/learning/access-management/what-is-network-segmentation/

Critical infrastructure. (2023, June). Consulté le Avril 20, 2024, sur Wikipedia: https://en.wikipedia.org/wiki/Critical_infrastructure#References

Dumouza, A. (2018, Janvier 9). *INFRASTRUCTURE IN ALGERIA UNDER SIGNIFICANT IMPROVEMENT*. Consulté le Septembre 04, 2024, sur The borgen project: https://borgenproject.org/infrastructure-in-algeria/

Ersan Kabalci, Y. K. (2019). *Smart Grids and Their Communication Systems.* Springer. doi:10.1007/978-981-13-1768-2

Fabro, M. R. (2009). Using Operational Security (OpSec) to Support a Cyber Security Culture in Control Systems Environments.

Flaus, J.-M. (2018). *Cybersécurité des systèmes industriels* (éd. Iste éditions). Récupéré sur https://www.mollat.com/livres/2320340/jean-marie-flaus-cybersecurite-des-systemes-industriels

FORTINET Rapport 2023. (s.d.). *Guide de segmentation du réseau OT*. Consulté le Septembre 07, 2024, sur FORTINET: https://www.fortinet.com/fr/resources/cyberglossary/ot-network-segmentation-and-microsegmentation

Fortinet, Inc. (s.d.). *Segmentation réseau*. Consulté le Septembre 07, 2024, sur FORTINET: https://www.fortinet.com/fr/resources/cyberglossary/network-segmentation

Fouladirad, M. a. (2005). *Optimal statistical fault detection with nuisance parameters.* (Vol. 41). Automatica. doi:10.1016/j.automatica.2005.02.004

Fovino, I. (2013). *Secure Smart Embedded Devices, Platforms and Applications* (éd. 1e). (K. M. Markantonakis, Éd.) Springer, New York. doi:10.1007/978-1-4614-7915-4_20

General Industrial Automation. (2021, 01 23). *What is Modbus TCP Protocol? Introduction to ModbusTCP*. Consulté le Septembre 05, 2024, sur PLCynergy: https://plcynergy.com/modbus-tcp-protocol/

HARTING Technology Group. (2024). *Que sont les systèmes de contrôle industriels ?* Consulté le Septembre 15, 2024, sur Harting: https://www.harting.com/CA/fr-ca/node/20126

Homeland Security. (2016). *Critical infrastructure threat information sharing framework.* Homeland Security. Consulté le Août 17, 2024, sur https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

INETDOC (par Philippe Latu). (s.d.). *Segmentation des réseaux locaux.* Consulté le Septembre 07, 2024, sur inetdoc: https://www.inetdoc.net/pdf/lan-segmentation.pdf

Keith, S., Michael, P., & CheeYee, T. (2023). *NIST Special Publication (SP) NIST SP 800-82r3 : Guide to Operational Technology (OT) Security.* National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.SP.800-82r3

Kriaa, S. (2016). *Joint safety and security modeling for risk assessment in cyber physical systems.* PhD thesis.

LadderLW. (s.d.). *PLC Architecture and Types: With Comparison Table*. Consulté le Septembre 10, 2024, sur ladderlogicworld: https://ladderlogicworld.com/plc-architecture/

Mehta, U. (2024, 04 14). *Blog 117 # Enhancing Organizational Resilience through Comprehensive Risk Management*. Consulté le 09 15, 2024, sur Linkedin: https://www.linkedin.com/pulse/blog-117-enhancing-organizational-resilience-through-risk-umang-mehta-kjckf/

Mondi Anderson. (2018, 09 03). *SCADA Systems, What is RTU?* Consulté le Septembre 10, 2024, sur REALPARS: https://www.realpars.com/blog/rtu

Mondi, A. (2019, 06 03). *What is SCADA? (Supervisory Control and Data Acquisition)*. Consulté le 09 10, 2024, sur REALPARS: https://www.realpars.com/blog/scada

Moteff, J. D. (2015, June 10). *Critical Infrastructures: Background, Policy, and Implementation.* Congressional Research Service. Consulté le 04 20, 2024, sur https://sgp.fas.org/crs/homesec/RL30153.pdf

Nakashima, E. a. (2012). Stuxnet was work of us and israeli experts, officials say. Washington Post.

Naraine, R. P. (2010). Stuxnet attackers used 4 windows zero-day exploits. *ZDnet Blog*.

Nazir, S., & Shushma Patel, D. P. (2017). *Assessing and augmenting SCADA cyber security: A survey of techniques* (Vol. 70). (C. &. Security, Éd.) Sciencedirect. doi:10.1016/j.cose.2017.06.010

Nile Global, Inc. (s.d.). *Anomaly & Behavior Detection - Tools & Techniques.* Consulté le Septembre 08, 2024, sur Nile secure: https://nilesecure.com/network-security/network-anomaly-detection

NIST (SP) 800-30r1. (2012, September). *Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments.* NIST Special Publication (SP) 800-30, Rev. 1,

National Institute of Standards and Technology. Consulté le Septembre 21, 2024, sur https://doi.org/10.6028/NIST.SP.800-30r1

NIST (SP) 800-37r2. (2018). *Joint Task Force Risk, Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Special Publication (SP) 800-37, Rev. 2. Consulté le Septembre 21, 2024, sur https://doi.org/10.6028/NIST.SP.800-37r2

NIST (SP) 800-39. (2011). *Joint Task Force Transformation Initiative. Managing Information Security Risk: Organization, Mission, and Information System View.* Special Publication (SP) 800-39, National Institute of Standards and Technology. Consulté le Septembre 21, 2024, sur https://doi.org/10.6028/NIST.SP.800-39

NIST (SP) 800-82. (2011). *Guide to Industrial Control Systems (ICS) Security.* NIST Special Publication 800-82, National Institute of Standards and Technology. Consulté le Septembre 08, 2024, sur https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf

NIST Privacy Risk Assessment Methodology. (s.d.). Consulté le Septembre 21, 2024, sur https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

NIST Risk Management Framework. (s.d.). Consulté le Septembre 21, 2024, sur https://csrc.nist.gov/projects/risk-management

Nozomi Networks. (2023, 10 12). *ICS Cybersecurity Guide: Managing Risk in Industrial Operations*. Consulté le Septembre 15, 2024, sur Nozomi Networks: https://www.nozominetworks.com/blog/ics-cybersecurity-guide

Okta. (2024, 08 28). *IDS vs IPS : quelles sont les différences ?* Consulté le Septembre 08, 2024, sur Okta: https://www.okta.com/fr/identity-101/ids-vs-ips/

Ortega, A. a. (2013). Performance analysis of smart grid communication protocol DNP3 over TCP/IP in a heterogeneous traffic environment. *Colombian Conference on Communications and Computing (COLCOM 2013)* (pp. 4-5). Colombia: IEEE. doi:10.1109/ColComCon.2013.6564828

OTO Technology (par Mounia BOUHRIZ). (2024, 02 20). *Comment identifier et bloquer toutes menaces avec l'analyse comportementale de votre réseau informatique ?* Consulté le Septembre 08, 2024, sur OTO Cyberdefense: https://www.oto-cyberdefense.fr/fr/blog/cybersecurite/analyse-comportementale-reseau-info

Palo Alto Networks. (2024). *Network Security, What is an Intrusion Prevention System?* Consulté le Septembre 08, 2024, sur Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Palo Alto Networks. (2024, Septembre 07). *Qu'est-ce que la segmentation réseau ?* Récupéré sur Palo Alto: https://www.paloaltonetworks.fr/cyberpedia/what-is-network-segmentation

Raghvendra, N. (s.d.). *SCADA System – Components, Hardware & Software Architecture, Types*. Consulté le 09 2024, sur Electricalfundablog: https://electricalfundablog.com/scada-system-components-architecture/

Reaves, B. e. (2009). *Discovery, infiltration, and denial of service in a process control system wireless network.* IEEE. doi:10.1109/ECRIME.2009.5342612

Red Hat, Inc. (2023, 09 27). *Un système de prévention et de détection des intrusions, qu'est-ce que c'est ?* Consulté le Septembre 08, 2024, sur Red Hat: https://www.redhat.com/fr/topics/security/what-is-an-IDPS

Riad, C. (2021, Juillet). *Méthodologie orientée sûreté de fonctionnement pour la cybersécurité des systèmes de contrôle-commande.* Thèse de doctorat, Université de Lille.

Ruchi Bisht in InfoSecTrain. (2024, 01 12). *Top Challenges Faced in OT Security in 2024*. Consulté le Septembre 15, 2024, sur InfoSecTrain: https://www.infosectrain.com/blog/top-challenges-faced-in-ot-security/

Schwab, W. a. (2018). *The state of industrial cybersecurity 2018.* Trend Study Kaspersky Reports.

Schweber, B. (2019, 01 07). *Programmable Logic Controllers, Part 2: Evolution and history*. Consulté le 09 10, 2024, sur Microcontrollertips: https://www.microcontrollertips.com/programmable-logic-controllers-evolution-history/

Securing Critical Infrastructure: Concerns for Businesses. (2024, Janvier 18). Consulté le Septembre 4, 2024, sur Exiger: https://www.exiger.com/perspectives/securing-critical-infrastructure-concerns-for-businesses/

SolarWinds Worldwide, LLC. (s.d.). *9 meilleurs outils de surveillance de la bande passante et de l'utilisation du réseau*. Consulté le Septembre 08, 2024, sur DNSstuff: https://www.dnsstuff.com/fr/surveillance-bande-passante

SOPHOS Ltd. (2024, 09 08). *What is intrusion detection system (IDS)?* Consulté le Septembre 21, 2024, sur Sophos: https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids

TechTarget. (2016, 08). *Système de contrôle industriel (ICS)*. Consulté le Septembre 07, 2024, sur LeMagIT: https://www.lemagit.fr/definition/Systeme-de-controle-industriel-ICS

TitanHQ. (s.d.). *Bonnes pratiques de segmentation réseau pour améliorer la sécurité informatique*. Consulté le Septembre 07, 2024, sur TitanHQ: https://www.titanhq.fr/segmentation-reseau/

Tolo, S. a. (2019). Nuclear Facilities and Cyber Threats. *29th European Safety and Reliability Conference.* (pp. 1-8). Singapore: Research Publishing. doi:10.3850/978-981-11-2724-3_0966-cd

VARONIS inc (Michael Buckbee). (2023, 06 23). *IDS et IPS : en quoi sont-ils différents ?* Consulté le Septembre 07, 2024, sur VARONIS: https://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents

Versa Networks, Inc. (s.d.). *IDS contre IPS : Différences entre IDS et IPS.* Consulté le Septembre 08, 2024, sur Versa Networks: https://versa-networks.com/fr/sd-wan/ids-ips/

VERVE. (2024, 03 29). *OT Security Chalenges and how to solve them*. Consulté le Septembre 15, 2024, sur VERVE industrial: https://verveindustrial.com/resources/blog/ot-security-challenges/

Wainstein, S. B. (2024, 04 08). *Defender pour IoT et votre architecture réseau*. Consulté le 09 20, 2024, sur Microsoft Learn: https://learn.microsoft.com/fr-fr/azure/defender-for-iot/organizations/best-practices/understand-network-architecture

Wei Gao et Morris, T. e. (2010). *On SCADA control system command and response injection and intrusion detection.* IEEE. doi:10.1109/ecrime.2010.5706699

Wikipédia. (2022, 04 16). Contrôle industriel. *Dans Wikipédia, l'encyclopédie libre*. Récupéré sur https://fr.wikipedia.org/wiki/Contr%C3%B4le_industriel

Wright, G. (Éd.). (2023, Aout). *Critical infrastructure*. Consulté le Avril 20, 2024, sur techtarget.com: https://www.techtarget.com/whatis/definition/critical-infrastructure

Y. Yuan, Z. L. (2011). *Modeling load redistribution attacks in power systems.* (Vol. 2). IEEE. doi:10.1109/TSG.2011.2123925

Zhu, B. e. (2011). *A Taxonomy of Cyber Attacks on SCADA Systems.* IEEE. doi:10.1109/iThings/CPSCom.2011.34

Zoho Corporation Pvt. Ltd. (s.d.). *Surveillance du trafic réseau*. Consulté le Septembre 08, 2024, sur Site24x7 ManageEngine: https://www.site24x7.com/fr/network-traffic-monitoring.html

ANNEXE

ANNEXE A
SEGMENTATION RESEAU ET ROLE DES IDS/IPS

ANNEXE A SEGMENTATION RESEAU ET ROLE DES IDS/IPS DANS LA CYBERSECURITE DES ICS

A.1 INTRODUCTION

A.1.1 Aperçu sur la Segmentation Réseau

La segmentation réseau constitue un pilier essentiel en cybersécurité, en particulier dans les Systèmes de Contrôle Industriels (ICS), où la sécurité et la fiabilité des opérations sont des priorités absolues. Ce concept consiste à subdiviser un réseau en plusieurs sous-réseaux distincts, permettant de contrôler plus efficacement le flux de données et de renforcer la sécurité. Dans un environnement ICS, où les infrastructures critiques doivent être protégées contre les cyberattaques, la segmentation limite les déplacements latéraux des attaquants au sein du réseau. Cela réduit considérablement les risques de propagation des menaces à travers le système.

La mise en œuvre de la segmentation peut être réalisée de plusieurs manières. D'une part, elle peut être physique, en utilisant des dispositifs matériels comme des pare-feu ou des routeurs pour isoler des segments du réseau. D'autre part, elle peut être logique, à travers des solutions telles que les réseaux locaux virtuels (VLAN), qui permettent de créer des zones de sécurité indépendantes au sein d'un même réseau physique. Cette séparation logique permet d'isoler différentes parties du système, tout en appliquant des politiques de sécurité adaptées à chaque segment, afin de mieux protéger les systèmes critiques.

En plus d'améliorer la sécurité, la segmentation optimise également les performances du réseau en limitant le trafic inutile entre les segments, et en facilitant l'application de contrôles plus stricts là où cela est nécessaire. Cela contribue à renforcer la résilience globale du système contre les menaces extérieures tout en facilitant une gestion plus fine des flux de données et des accès. Grâce à ces mesures, la segmentation devient un outil stratégique pour assurer une défense en profondeur des réseaux industriels.

A.1.2 Importance de la Segmentation Réseau dans les ICS

La segmentation réseau est une mesure de sécurité primordiale pour les Systèmes de Contrôle Industriels (ICS), avec plusieurs avantages essentiels qui contribuent à la protection des infrastructures critiques :

- **Réduction des risques :** En divisant le réseau en segments distincts, on limite l'accès aux parties les plus sensibles uniquement aux utilisateurs et dispositifs autorisés. Cela réduit considérablement les risques de cyberattaques, car les intrus ou acteurs malveillants ne peuvent pas facilement se déplacer d'une partie du réseau à une autre. Chaque segment devient une barrière contre les attaques potentielles (TitanHQ, s.d.) (FORTINET Rapport 2023, s.d.).
- **Meilleure visibilité du réseau :** La segmentation offre une visibilité accrue sur le trafic réseau. Les équipes de cybersécurité peuvent ainsi surveiller plus précisément ce qui se passe dans chaque segment, facilitant la détection des comportements anormaux ou suspects. Cela permet une détection plus rapide des tentatives d'intrusion ou d'activités

malveillantes, avant qu'elles n'affectent l'ensemble du système (TitanHQ, s.d.) (Check Point Software Technologies Ltd, s.d.).

- **Contrôle d'accès renforcé :** En appliquant des politiques de contrôle d'accès spécifiques à chaque segment du réseau, il devient possible de restreindre l'accès aux systèmes et aux ressources critiques uniquement à ceux qui en ont besoin. Cette approche diminue la possibilité d'intrusions ou de déplacements latéraux, où un attaquant compromettrait un système pour accéder à un autre (CESI Centre de l'Expertise en Sécurité de l'Information, 2024-03-27) (Cloudflare, Inc, 2024).

- **Protection des systèmes critiques :** Les systèmes ICS sont souvent essentiels au bon fonctionnement des infrastructures et exigent une disponibilité continue. La segmentation permet d'isoler ces systèmes critiques du reste du réseau, minimisant ainsi leur exposition aux cybermenaces tout en assurant leur résilience. Cela est particulièrement important pour les systèmes qui ne peuvent pas être régulièrement mis à jour (FORTINET Rapport 2023, s.d.) (CESI Centre de l'Expertise en Sécurité de l'Information, 2024-03-27).

- **Gestion des menaces internes :** La segmentation contribue également à la détection des menaces internes. En limitant les privilèges et en surveillant l'activité dans chaque segment, il devient plus facile d'identifier les utilisateurs ou les dispositifs qui agissent de manière malveillante ou irrégulière, offrant ainsi une protection renforcée contre les attaques initiées de l'intérieur (Check Point Software Technologies Ltd, s.d.) (Cloudflare, Inc, 2024).

En conclusion, la segmentation réseau représente une défense stratégique et efficace pour renforcer la cybersécurité des systèmes de contrôle industriels. Elle aide à limiter les risques d'intrusion, à offrir une meilleure visibilité et un contrôle d'accès optimisé, tout en protégeant les systèmes critiques contre les menaces potentielles. En adoptant cette approche, les organisations peuvent mieux sécuriser leurs infrastructures industrielles face aux cyberattaques croissantes et complexes.

A.2 ROLE DES IDS/IPS DANS LES ICS

A.2.1 Présentation de l'IDS (Système de Détection d'Intrusion)

Un Système de Détection d'Intrusion (IDS) est un outil crucial dans la protection des réseaux industriels. Il est conçu pour surveiller en continu le trafic réseau afin d'identifier toute activité suspecte ou malveillante. Dans le contexte des Systèmes de Contrôle Industriels (ICS), l'IDS permet de détecter des anomalies susceptibles d'indiquer des intrusions. Grâce à des alertes envoyées aux administrateurs de sécurité, ces derniers peuvent intervenir rapidement pour empêcher une attaque de progresser.

Les IDS se déclinent en deux types principaux :

- **IDS basé sur le réseau (NIDS) :** Celui-ci surveille le trafic réseau global, analysant les paquets qui transitent dans le réseau pour détecter des comportements inhabituels.

- **IDS basé sur l'hôte (HIDS) :** Il surveille les activités locales d'un appareil ou d'un serveur spécifique pour détecter des actions suspectes.

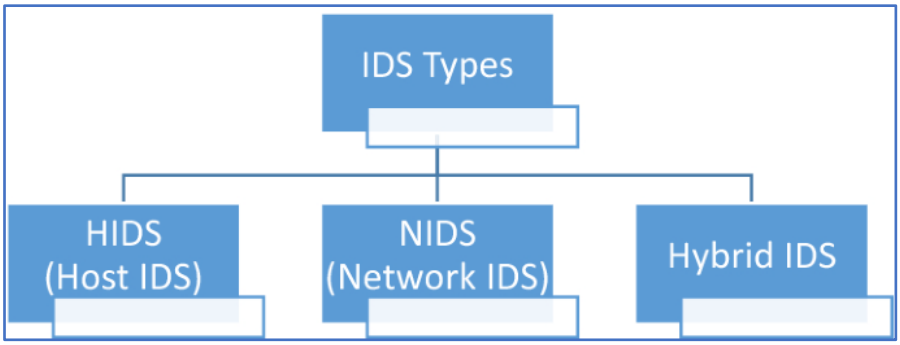


FIGURE A 1 : Types des IDS

En ICS, un IDS est indispensable pour obtenir une détection rapide et proactive des menaces qui pourraient perturber le fonctionnement des systèmes critiques.

A.2.2 Présentation de l'IPS (Système de Prévention d'Intrusion)

L'IPS (Système de Prévention d'Intrusion) va plus loin que l'IDS. En plus de détecter les menaces, il prend des mesures immédiates pour prévenir leur exploitation.

Contrairement à l'IDS, qui se contente d'alerter, l'IPS est intégré directement dans le flux réseau et peut bloquer activement les menaces en temps réel.

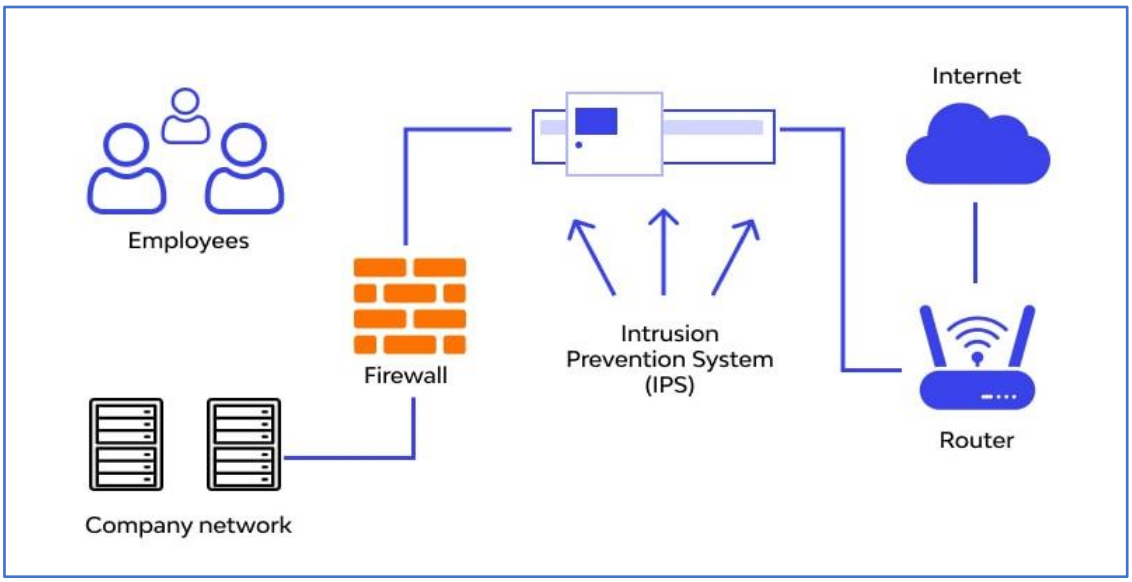


FIGURE A 2 : Installation de l'IPS en série

Les fonctions clés de l'IPS incluent

- **Analyse proactive du trafic :** Il scrute chaque paquet traversant le réseau pour détecter des signatures d'attaques ou des anomalies dans les comportements.
- **Intervention en temps réel :** Dès qu'une menace est détectée, l'IPS peut bloquer le trafic concerné, réinitialiser des connexions ou adapter les règles du pare-feu pour empêcher des intrusions ultérieures.

Grâce à ces capacités, l'IPS assure un environnement ICS plus sécurisé, en agissant directement sur les attaques avant qu'elles n'affectent les systèmes.

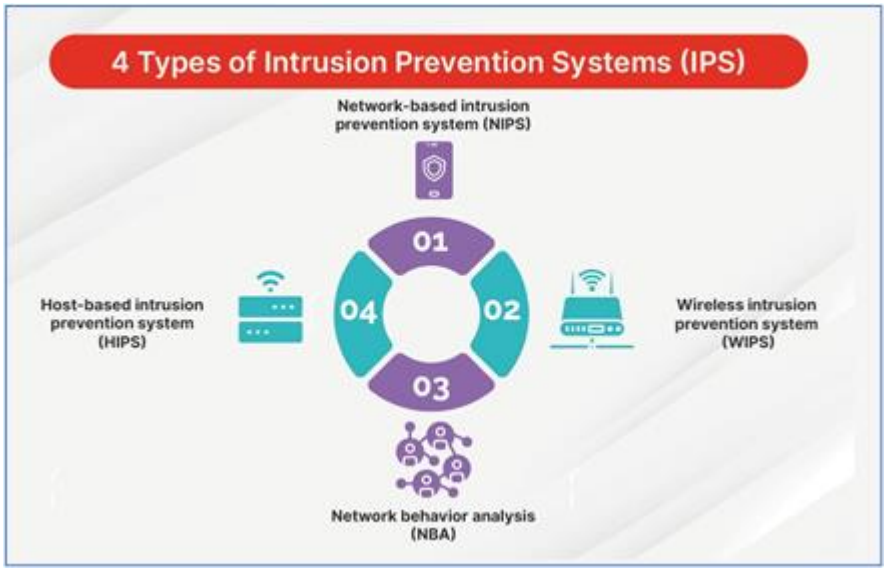


FIGURE A 3 : Types des IPS

A.2.3 Différences entre IDS et IPS

Bien que les deux systèmes aient des fonctions similaires en termes de détection des menaces, leurs modes d'action diffèrent :

Les systèmes de détection d'intrusion (IDS) surveillent le trafic réseau pour identifier des signatures correspondant à des cyberattaques connues. En revanche, les systèmes de prévention d'intrusion (IPS) non seulement analysent les paquets réseau, mais ils peuvent également bloquer ceux associés à des attaques identifiées, aidant ainsi à stopper ces menaces en temps réel (VARONIS inc (Michael Buckbee), 2023).

TABLEAU A 1 : Différence entre IDS et IPS

Caractéristique	IDS	IPS
Type de sécurité	Passif	Actif
Fonction principale	Détection et alerte	Détection et prévention
Action après détection	Envoi d'alertes aux administrateurs	Blocage automatique des menaces
Impact sur le trafic	Ne modifie pas le flux de données	Peut introduire une légère latence
Positionnement	Après le pare-feu ou en mode écoute	Directement intégré dans le flux réseau

En ICS, ces deux systèmes peuvent se compléter efficacement : l'IDS permet une détection continue et approfondie, tandis que l'IPS intervient pour bloquer les menaces en temps réel.

A.2.4 Défis de l'Utilisation des IDS/IPS dans les ICS

Le déploiement des systèmes IDS et IPS dans les environnements industriels, en particulier les ICS, présente des défis spécifiques :

1. **Compatibilité avec les systèmes anciens** : De nombreux ICS reposent sur des infrastructures vieillissantes, souvent incompatibles avec les technologies modernes de cybersécurité. L'intégration des IDS/IPS peut donc nécessiter des ajustements importants.
2. **Impact potentiel sur la latence** : Les ICS nécessitent souvent une réactivité très élevée. L'IPS, en interceptant et analysant chaque paquet, peut introduire une légère latence qui, dans certains cas, peut affecter la performance des systèmes critiques.
3. **Gestion des faux positifs** : Les IDS et IPS, s'ils ne sont pas correctement configurés, peuvent générer un nombre élevé de faux positifs. Cela entraîne une surcharge de travail pour les équipes de sécurité, qui doivent constamment analyser et trier ces alertes.
4. **Complexité de l'architecture ICS** : Les réseaux ICS sont souvent très complexes, avec une diversité d'équipements et de protocoles. Déployer des solutions IDS/IPS dans de tels environnements exige une planification minutieuse et une connaissance approfondie des infrastructures spécifiques.

L'intégration des systèmes de détection (IDS) et de prévention d'intrusion (IPS) dans les Systèmes de Contrôle Industriels est essentielle pour renforcer la sécurité de ces infrastructures critiques. Toutefois, leur déploiement doit être soigneusement étudié pour éviter des problèmes de compatibilité, de performance et de gestion des alertes. Une combinaison des deux technologies, associée à une segmentation réseau adéquate, permet de maximiser la protection contre les menaces cybernétiques.

A.3 STRATEGIES DE SEGMENTATION RESEAU DANS LES SYSTEMES DE CONTROLE INDUSTRIELS (ICS)

A.3.1 Modèles de Segmentation

La segmentation réseau est une stratégie essentielle pour renforcer la sécurité des Systèmes de Contrôle Industriels (ICS). Elle consiste à diviser un réseau en segments plus petits pour limiter la propagation des attaques et contrôler l’accès aux ressources critiques. Voici les principaux modèles de segmentation utilisés dans les ICS :

- **Segmentation physique** : Cette approche crée des sous-réseaux distincts à l’aide de matériel physique, comme des routeurs et des commutateurs. Chaque segment est isolé des autres, ce qui permet un contrôle strict du trafic. Bien que cette méthode réduise considérablement le risque de mouvements latéraux des attaquants, elle est souvent coûteuse à déployer et complexe à gérer en raison du matériel nécessaire.
- **Segmentation logique (VLANs)** : Ce modèle utilise des **réseaux locaux virtuels (VLANs)** pour segmenter logiquement le réseau sans modifier la topologie physique. Les VLANs permettent de créer des sous-réseaux au sein du même réseau physique, ce

qui réduit les coûts tout en offrant une gestion flexible du trafic. Cela est particulièrement utile dans les ICS où les ressources sont souvent limitées et où une solution de segmentation physique peut être difficile à mettre en œuvre.

- **Micro-segmentation** : Ce modèle va plus loin que la segmentation logique en isolant chaque charge de travail, appareil ou application au sein d'un réseau. La **micro-segmentation** permet d'appliquer des politiques de sécurité granulaires, réduisant ainsi la surface d'attaque et limitant les déplacements latéraux des menaces. Elle est souvent mise en œuvre à l'aide de solutions logicielles telles que les réseaux définis par logiciel (**SDN**). Cette méthode est particulièrement efficace dans les environnements ICS modernes qui nécessitent une isolation stricte des ressources critiques (Check Point Software Technologies Ltd, 2024) (Palo Alto Networks, 2024) (Fortinet, Inc, s.d.).

A.3.2 Segmentation et Zones de Sécurité dans les ICS

La segmentation réseau dans les ICS est souvent utilisée pour créer des **zones de sécurité** distinctes qui séparent les systèmes critiques du reste du réseau. Cela permet d'établir des périmètres de sécurité autour des zones opérationnelles sensibles et de restreindre l'accès.

- **Création de zones :** La segmentation permet de créer des zones où les automates programmables industriels (API) et autres équipements critiques sont isolés. Ces zones sont protégées par des règles d'accès strictes pour réduire le risque d'intrusions et protéger les systèmes essentiels contre les cybermenaces.
- **Limitation de l'accès** : En isolant les systèmes critiques et en mettant en place des contrôles d'accès, les organisations peuvent restreindre l'accès aux utilisateurs et dispositifs autorisés. Cela réduit le risque de mouvements latéraux en cas d'intrusion, empêchant les attaquants de pénétrer plus profondément dans le réseau.
- **Surveillance accrue** : Grâce à la segmentation, il devient plus facile de surveiller le trafic réseau entre les zones. Cela permet aux équipes de sécurité de détecter plus rapidement des comportements suspects ou des anomalies dans chaque segment du réseau (Fortinet, Inc, s.d.) (Check Point Software Technologies Ltd, s.d.).

A.3.3 La segmentation du réseau ICS/OT, pourquoi est-ce important ?

La convergence des environnements IT et ICS/OT complique l'établissement et le maintien d'une visibilité complète sur le réseau. Lorsque les assaillants ont la possibilité de franchir les défenses, il est essentiel de mettre en place une autre méthode de sécurité pour empêcher les intrus de se déplacer librement à travers le réseau ICS/OT. Cela souligne l'importance de la segmentation du réseau ICS/OT.

La segmentation du réseau ICS/OT offre plus de contrôle et de visibilité

La segmentation d'un réseau ICS/OT en sections ou zones plus petites donne aux professionnels de la sécurité beaucoup plus de contrôle et de visibilité, ainsi que la possibilité de mieux fortifier les réseaux de l'organisation contre les cyberattaques. Les experts du secteur de la cybersécurité affirment que la segmentation réseau est l'une des méthodes les plus efficaces pour protéger les technologies opérationnelles contre les menaces internes et externes. Il n'y a donc aucun doute à ce sujet : pour les RSSI, les

DSI et la direction informatique, la segmentation du réseau ICS/OT est un incontournable.

Les réseaux ICS/OT existants n'ont pas été conçus en tenant compte des restrictions, en particulier ceux qui fonctionnaient dans un environnement isolé et isolé, sans aucune connexion aux réseaux externes. De nombreux environnements ICS/ OT ont une approche de « confiance implicite » envers les utilisateurs et les appareils, permettant de contrôler et d'administrer n'importe quel actif numérique du réseau de n'importe où, quelle que soit l'importance de l'actif pour le fonctionnement ou la réussite de l'organisation. Ces réseaux OT traditionnels sont très attrayants pour les cybercriminels très motivés.

La segmentation du réseau ICS/OT est une bonne pratique reconnue CISA

Les meilleurs experts en cybersécurité du CISA (***Cybersecurity & Infrastructure Security Agency***) du gouvernement américain s'accordent à dire que l'un des meilleurs moyens de renforcer la posture de sécurité ICS/OT d'une organisation est d'utiliser la segmentation réseau. Il est essentiel de réduire la probabilité que des adversaires accèdent au réseau ICS/OT après avoir infiltré le réseau IT.

Principales différences entre la segmentation réseau IT et ICS/OT

Si vous vous demandez, la segmentation du réseau ICS/OT est un peu différente de la segmentation du réseau IT. Bien que la segmentation du réseau IT et ICS/OT souhaite améliorer leur sécurité et leurs performances, elle tente de le faire dans différents environnements qui ont leurs propres exigences distinctes.

Contrairement à l'informatique, la segmentation du réseau ICS/OT doit donner la priorité à la sécurité, à la fiabilité et à la nature en temps réel des systèmes de contrôle industriel (ICS) tout en répondant aux préoccupations de cybersécurité spécifiques aux infrastructures critiques. De plus, les réseaux ICS/OT ont besoin d'équipements renforcés pour fonctionner dans des environnements difficiles.

A.3.4 Comment les réseaux ICS/OT doivent-ils être segmentés ?

Les équipes informatiques doivent segmenter leurs réseaux en plusieurs zones fonctionnelles, qui peuvent inclure des sous-zones ou des micro-segments. Chaque zone doit être accessible uniquement par des dispositifs, applications et utilisateurs autorisés et authentifiés. Un conduit, généralement un pare-feu, est essentiel pour définir et appliquer les limites de chaque zone. Ces conduits agissent comme des canaux sécurisés permettant aux données et applications critiques de circuler d'une zone à l'autre.

En résumé, la meilleure approche pour la segmentation du réseau ICS/OT consiste à diviser le réseau en zones fonctionnelles distinctes, accessibles uniquement aux appareils, applications et utilisateurs autorisés.

Il est crucial d'appliquer les limites de chaque zone à l'aide d'un pare-feu, qui joue le rôle de contrôleur d'accès et de protection, tout en permettant un transfert sécurisé des données et applications essentielles à travers le réseau ICS/OT.

Définition des Zones et des Conduits de Sécurité dans les Réseaux ICS/OT

1) Zones de Sécurité

Dans les réseaux de Systèmes de Contrôle Industriels (ICS) et d'Operational Technology (OT), une zone de sécurité est un environnement réseau délimité regroupant des actifs ayant des exigences de sécurité communes. Ces zones contrôlent l'accès et gèrent les flux de données pour restreindre les communications aux dispositifs et utilisateurs autorisés. Les types courants incluent :

- **Zone publique :** Environnement ouvert, renforcé contre les attaques.
- **Zone d'accès restreint :** Environnement contrôlé avec accès limité.
- **Zone de gestion :** Zone dédiée à la gestion des systèmes avec des contrôles d'accès stricts.

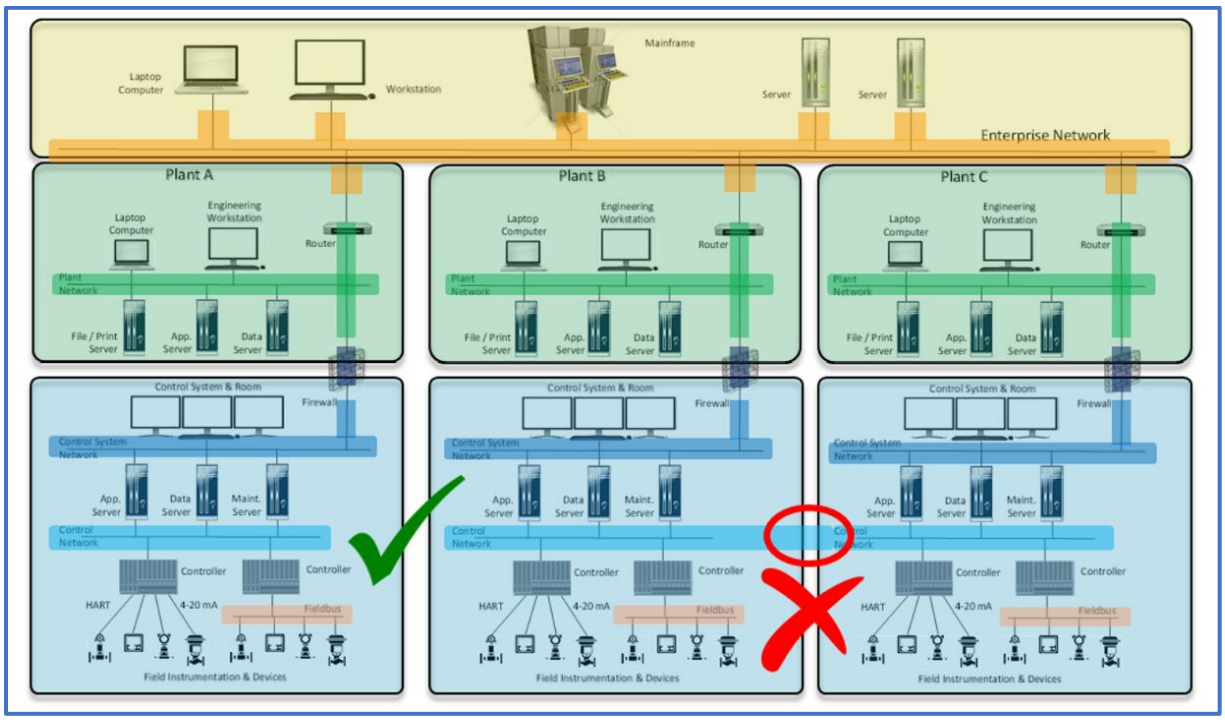


FIGURE A 4 : Configurations correctes et incorrectes, ainsi que des exemples de conduits

Chaque zone doit avoir des limites de sécurité définies pour tous les flux entrants et sortants.

2) Conduits de Sécurité

Les conduits de sécurité, souvent matérialisés par des pare-feu, établissent et appliquent les limites entre différentes zones. Ils régulent le trafic entre zones, empêchant les mouvements latéraux non autorisés, et assurent la sécurité en inspectant le trafic qui traverse ces conduits.

3) Importance dans les ICS/OT

La définition claire des zones et conduits dans les réseaux ICS est cruciale pour :

- **Isolation des systèmes critiques :** Limite l'impact d'une intrusion sur l'ensemble du système.
- **Contrôle d'accès renforcé :** Applique des politiques d'accès strictes réduisant le risque d'accès non autorisé.
- **Visibilité accrue :** Facilite la surveillance du trafic réseau pour identifier rapidement toute activité suspecte.

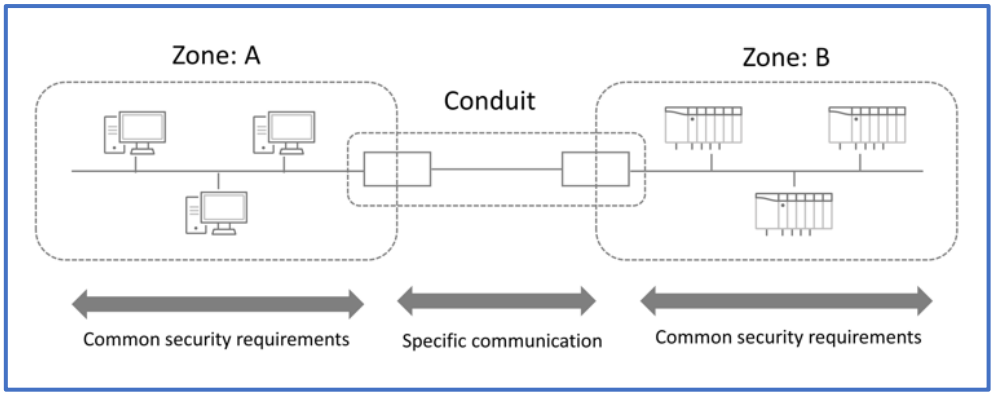


FIGURE A 5 : Conduits (basé sur IEC documentation)

Segmentation réseau OT vs micro-segmentation

Si la segmentation du réseau OT complique l'accès des intrus, la microsegmentation apporte une couche de protection supplémentaire. En associant des actifs physiques critiques à l'innovation numérique, divers avantages peuvent être obtenus, mais cela peut aussi entraîner des défis en matière de visibilité et de contrôle. En déployant la microsegmentation, les équipes informatiques peuvent retrouver la visibilité et le contrôle sur leur technologie opérationnelle. Voici un tableau comparatif des similitudes et des différences entre la segmentation réseau OT et la microsegmentation :

TABLEAU A 2 : Les points clés entre la segmentation et la micro-segmentation

Critère	Segmentation du Réseau OT	Micro-segmentation du Réseau OT
Portée	Segments ou zones fonctionnelles	Isolation jusqu'à l'échelle des appareils ou applications
Protection	Limite l'accès entre les zones	Limite les interactions entre chaque composant individuel
Complexité	Moins complexe, mais avec des segments plus larges	Plus complexe, mais protection plus granulaire
Visibilité	Réduite à chaque segment	Accroît la visibilité sur chaque appareil ou application
Contrôle	Contrôle des accès entre zones :	Contrôle détaillé au niveau de chaque interaction :

	• Une offre de base d'un pare-feu nouvelle génération (NGFW). • Mise en place de zones et de conduits de sécurité • Sécurité pour la communication inter-VLAN • Surveillance du trafic réseau nord et sud et prévention des menaces • Les signatures IPS aident à mettre en œuvre des correctifs virtuels et empêchent l'exploitation des vulnérabilités du système contre les menaces internes ou externes	• Un pare-feu NGFW intégré à un commutateur réseau pour garantir que le trafic est rapide, fiable et sécurisé. • Une segmentation plus approfondie des zones de sécurité en fonction des différentes exigences de sécurité • Surveillance du trafic réseau est et ouest et inspection approfondie des paquets • Sécurité des communications intra-VLAN • Les signatures de contrôle applicatif aident à mettre en œuvre des protocoles et des politiques applicatives granulaires et à arrêter le mouvement latéral des menaces

Stratégies Optimales de Segmentation du Réseau OT avec des Pare-feux de Nouvelle Génération (NGFW)

Comment une organisation peut mettre en œuvre la micro-segmentation !? en toute confiance sans perturber son ou ses réseau(x) !!

Pour mettre en œuvre la micro-segmentation sans perturber ses réseaux, une organisation doit procéder de manière progressive et méthodique, en adoptant une approche par étapes qui commence par une analyse approfondie des flux de données critiques et des points d'interconnexion au sein des réseaux OT, tout en minimisant les interruptions potentielles en testant et validant chaque segment avant de le déployer à grande échelle. Il est crucial de suivre les meilleures pratiques telles que l'élaboration d'un plan détaillé, l'établissement de priorités pour les zones sensibles, et d'éviter les erreurs comme la mise en œuvre simultanée de toutes les modifications ou l'absence de collaboration avec les parties prenantes.

TABLEAU A 3 : Bonnes pratiques pour mettre en œuvre la micro-segmentation

Bonnes pratiques	Pires pratiques
Mettre en place un processus détaillé définissant les responsabilités de chacun.	Négliger d'identifier les besoins et risques spécifiques de l'organisation.
Élaborer un plan avec une vision à long terme et un calendrier réaliste.	Ne pas fixer d'objectifs clairs ou s'aligner sur les intérêts des parties prenantes.
Minimiser les perturbations en adoptant les mesures les plus sûres.	Ignorer l'importance de compléter l'identification et la priorisation des zones.
Collecter des données à chaque étape et réévaluer avant de passer à l'action suivante.	Essayer de tout déployer simultanément, augmentant le risque de perturbations.

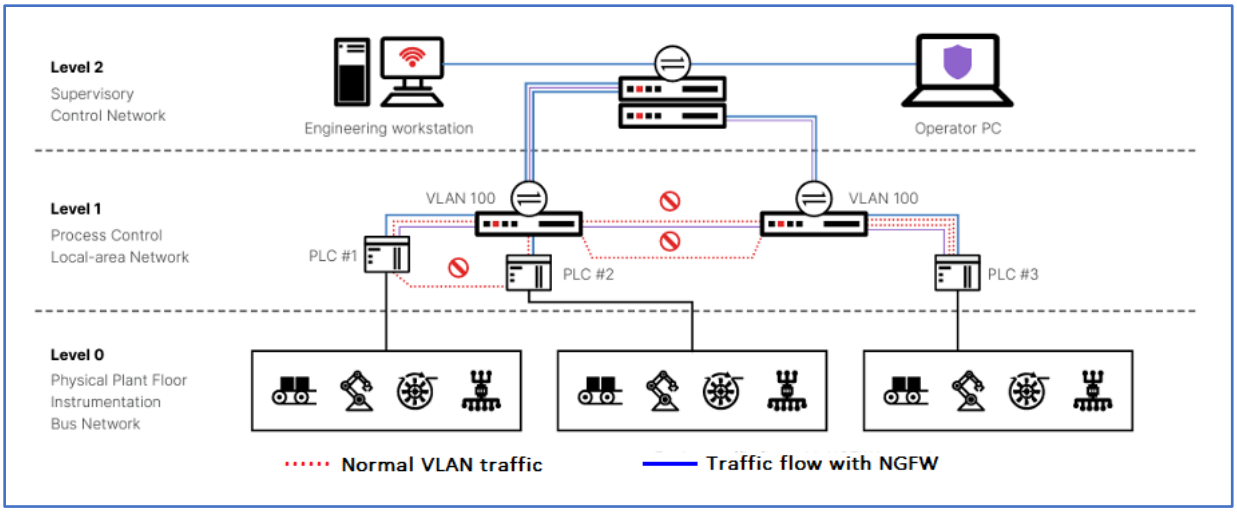


FIGURE A 6 : Traffics normal et trafics avec NGFW

A.4 ARCHITECTURE ZERO-TRUST DANS LES ICS

Le **modèle Zero Trust** est une approche de sécurité qui gagne en popularité dans les environnements de systèmes de contrôle industriels (ICS), où la protection des infrastructures critiques est primordiale.

Contrairement aux modèles de sécurité traditionnels qui partent du principe que les utilisateurs et les appareils internes sont fiables une fois qu'ils accèdent au réseau, le modèle Zero Trust adopte une approche plus stricte et prudente. Il repose sur l'idée que **toute entité**, qu'elle soit à l'intérieur ou à l'extérieur du réseau, doit être considérée comme une menace potentielle.

Cela signifie que les accès ne sont accordés qu'après authentification et validation de l'identité, et que chaque interaction ou demande d'accès doit être vérifiée en temps réel. Ce modèle est particulièrement utile dans les environnements ICS, où un compromis sur la sécurité peut avoir des répercussions graves, notamment sur la continuité des opérations.

L'un des principes clés du Zero Trust est le concept de **"ne jamais faire confiance par défaut"**. Même si un utilisateur ou un appareil a été autorisé précédemment à accéder à une partie du réseau, cela ne garantit pas un accès permanent. Chaque demande d'accès est analysée indépendamment, en fonction de plusieurs facteurs, notamment l'identité de l'utilisateur, l'appareil utilisé, l'emplacement géographique et le comportement attendu.

Cette approche permet de limiter la possibilité d'attaques internes ou de mouvements latéraux des cyberattaquants à l'intérieur du réseau ICS. Par exemple, un employé ayant accès à un automate programmable industriel (API) dans une zone spécifique du réseau ne pourra pas se déplacer librement vers d'autres parties sensibles du réseau sans une nouvelle authentification. De cette manière, la sécurité du réseau est renforcée à chaque point de contrôle.

Enfin, le modèle Zero Trust s'appuie sur une combinaison de technologies pour assurer une surveillance et un contrôle continus, tels que la **micro-segmentation**, l'authentification multi-facteurs (MFA), et les outils de détection et de réponse aux menaces.

La micro-segmentation permet de diviser le réseau en zones plus petites et plus sécurisées, rendant ainsi plus difficile pour les attaquants de se déplacer d'un segment à l'autre. Chaque segment peut être doté de ses propres règles d'accès et d'authentification, offrant ainsi une couche supplémentaire de protection (INETDOC (par Philippe Latu)) (TitanHQ, s.d.).

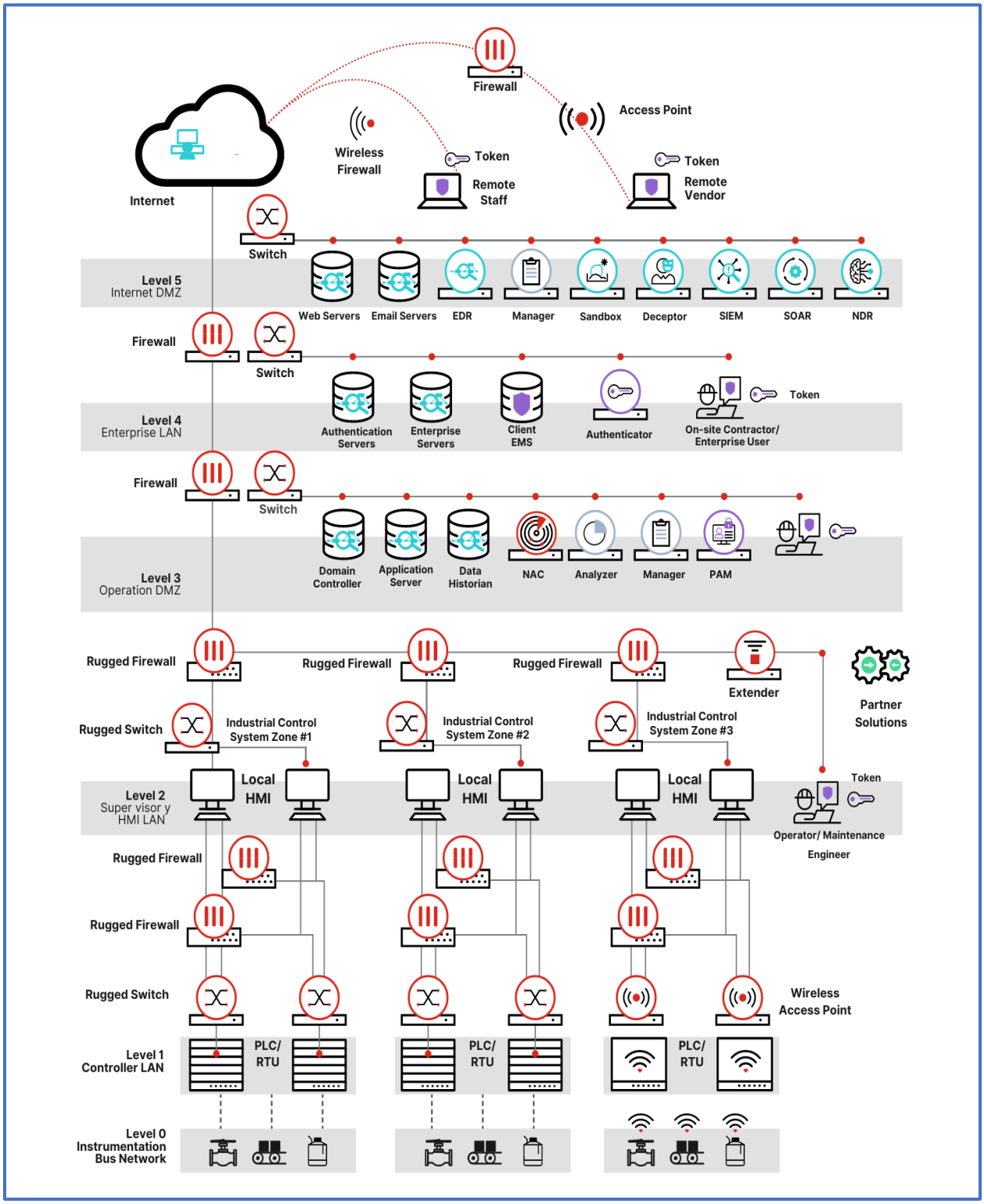


FIGURE A 7 : Architecture Zero-Trust Securite dans les ICS/OT

- **Application du Zero Trust dans les ICS** : Dans une architecture Zero Trust, chaque demande d'accès à une ressource est vérifiée et authentifiée indépendamment de son origine. Cela signifie que même les utilisateurs ayant un accès légitime au réseau doivent continuellement prouver leur identité et l'autorisation d'accès aux systèmes critiques.
- **Micro-segmentation et Zero Trust** : La micro-segmentation s'intègre naturellement dans une approche Zero Trust. En créant des périmètres de sécurité autour de chaque ressource critique, les organisations peuvent appliquer des contrôles d'accès très granulaires. Cela limite les déplacements latéraux et permet de restreindre précisément les permissions, renforçant ainsi la sécurité globale du réseau.
- **Renforcement de la sécurité** : En combinant la segmentation réseau avec une architecture Zero Trust, les organisations peuvent créer une défense en profondeur contre les menaces. Cela permet de protéger les infrastructures ICS contre des attaques sophistiquées en s'assurant que chaque accès à une ressource sensible est dûment autorisé et surveillé (Check Point Software Technologies Ltd, 2024) (Fortinet, Inc, s.d.).

La mise en œuvre de la segmentation réseau dans les Systèmes de Contrôle Industriels (ICS) est cruciale pour améliorer la sécurité et protéger les infrastructures critiques contre les cyberattaques. Grâce à des modèles de segmentation variés (physique, logique, micro-segmentation), et à l'intégration d'une architecture Zero Trust, les organisations peuvent créer des défenses robustes tout en garantissant la continuité des opérations industrielles.

Ces stratégies permettent de réduire la surface d'attaque, de limiter les déplacements latéraux des attaquants et d'améliorer la surveillance du trafic réseau.

ANNEXE B
CONCEPTION ET CONFIGURATION D'IDS/IPS DANS LES SYSTEMES DE CONTROLE INDUSTRIEL

ANNEXE B CONCEPTION ET CONFIGURATION D'IDS/IPS DANS LES SYSTEMES DE CONTROLE INDUSTRIEL

Les sections suivantes décrivent en détail les différents types de déploiements utilisant les technologies présentées dans ce chapitre, à savoir les systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS). Ces déploiements seront basés sur une architecture initiale, qui évoluera progressivement pour former une architecture complète. Cette architecture finale inclura tous les composants nécessaires pour mettre en place à la fois un système efficace de détection et de prévention des intrusions, ainsi qu'un système intégré de collecte et de gestion des événements.

B.1 ARCHITECTURE DE BASE DU SYSTEME DE CONTROLE

L'architecture de base adoptée repose sur les recommandations énoncées dans la norme IEC 62443 (Figure B 1) qui établit un cadre pour la sécurisation des systèmes de contrôle industriel. Ce modèle divise l'environnement industriel en différentes zones, chacune correspondant à un niveau de sécurité spécifique.

Dans cette architecture, la segmentation est un principe fondamental, réalisée notamment par l'utilisation de pare-feu pour isoler la zone de contrôle des processus industriels de la zone métier. Deux zones démilitarisées (DMZ) sont mises en place pour gérer de manière sécurisée l'échange de données entre ces deux zones distinctes.

Les solutions architecturales proposées intègrent des mécanismes de sécurité robustes afin d'assurer la protection des communications et des dispositifs situés dans la zone de contrôle du réseau. Cependant, il est important de noter que la sécurité de la zone métier n'a pas été traitée dans le cadre de cette étude, car cela sort du périmètre de l'analyse. L'objectif principal ici est de garantir la sûreté et l'intégrité des systèmes critiques de contrôle au sein des infrastructures industrielles.

B.2 ARCHITECTURES DE SECURITE POUR LES SYSTEMES DE CONTROLE

La première architecture, illustrée dans la Figure B 2, montre l'intégration de dispositifs IDS pour surveiller le trafic au sein du réseau de contrôle. Le trafic transitant par le routeur ou les commutateurs est redirigé vers le capteur IDS à l'aide de ports miroirs (mirror/SPAN). En complément, une sonde est installée pour recevoir les informations des pare-feu et ainsi surveiller les échanges de données avec le réseau de la zone d'activité.

L'IDS doit être configuré avec les règles appropriées pour générer des alertes pertinentes, lesquelles seront affichées à l'opérateur ou à l'administrateur de sécurité via une console dédiée. L'évolution de cette architecture de sécurité implique la capacité de bloquer le trafic malveillant. Pour cela, il est nécessaire de positionner les capteurs directement dans le flux de trafic, au lieu de simplement le dupliquer via des ports miroirs, comme le montre la Figure B 3.

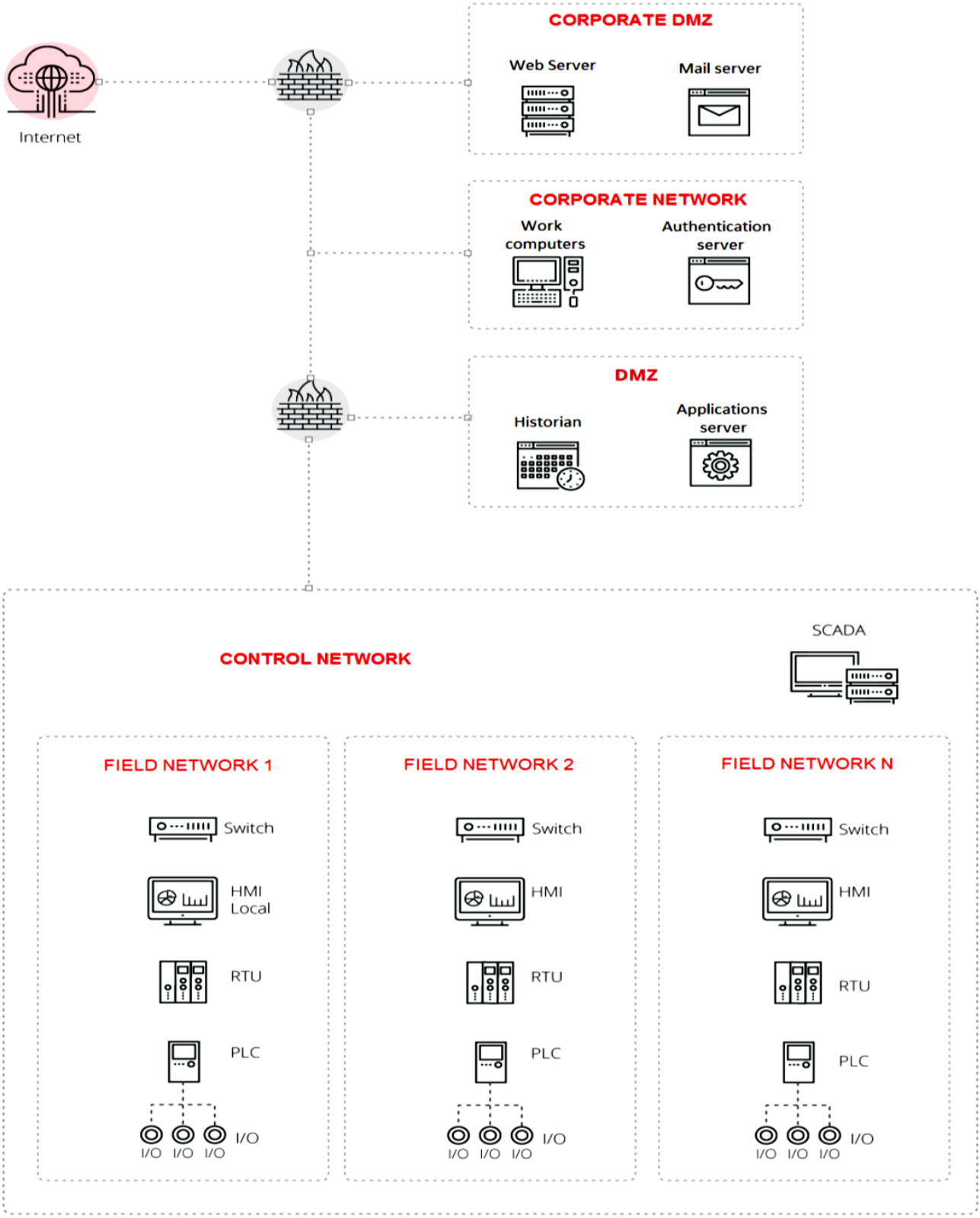


FIGURE B 1 : Architecture de base du systèmes de contrôle

Les règles de configuration doivent être soigneusement définies afin de garantir que le flux de trafic et les opérations normales ne soient pas perturbés, et que seules les intrusions et les menaces à la sécurité soient stoppées. L'emplacement des capteurs IPS est similaire à celui des capteurs IDS, et leur fonctionnement est identique, générant une alerte qui sera affichée dans la console IDS.

La Figure B 4 illustre l'intégration d'un SIEM au sein des systèmes de contrôle. Le rôle du SIEM est principalement de collecter et de gérer les journaux d'événements provenant de diverses sources de données, c'est-à-dire de tous les dispositifs du réseau. Il est important de prêter attention aux communications, car tous ces appareils doivent pouvoir envoyer leurs logs vers le SIEM, ce qui peut potentiellement entraîner une surcharge du réseau. Une solution efficace pour éviter cette surcharge est de dédier un réseau spécifique exclusivement pour l'envoi de ces messages.

La représentation finale, visible dans la Figure B 5, montre l'intégration des trois technologies – IDS, IPS, et SIEM – dans l'architecture d'un système de contrôle réseau. L'IPS est positionné aux niveaux supérieurs pour surveiller le trafic entre la zone de contrôle et la zone métier, tandis que l'IDS est placé pour gérer le trafic entre le réseau de contrôle et les systèmes sur le terrain, détectant toute anomalie potentielle. Le SIEM, quant à lui, collecte des informations de tous les appareils du réseau, y compris des dispositifs de traitement, des éléments de réseau, ainsi que des alertes générées par l'IDS et l'IPS.

Les lignes rouges sur les schémas représentent les points de connexion des capteurs IDS et IPS, là où ils se branchent pour capturer le trafic réseau. Ce réseau de surveillance fait le lien entre les capteurs IDS/IPS et le centre de gestion centralisé, et, par conséquent, il n'est pas nécessaire de permettre l'accès à ce réseau depuis d'autres parties de l'architecture.

Les lignes vertes menant au SIEM indiquent les sources d'information, mais ne représentent pas des connexions réseau physiques. Les données sont envoyées via les connexions déjà existantes, avec des règles spécifiques mises en place dans les pare-feu (et dans certains cas au niveau des IDS/IPS) pour garantir la bonne gestion de ces flux.

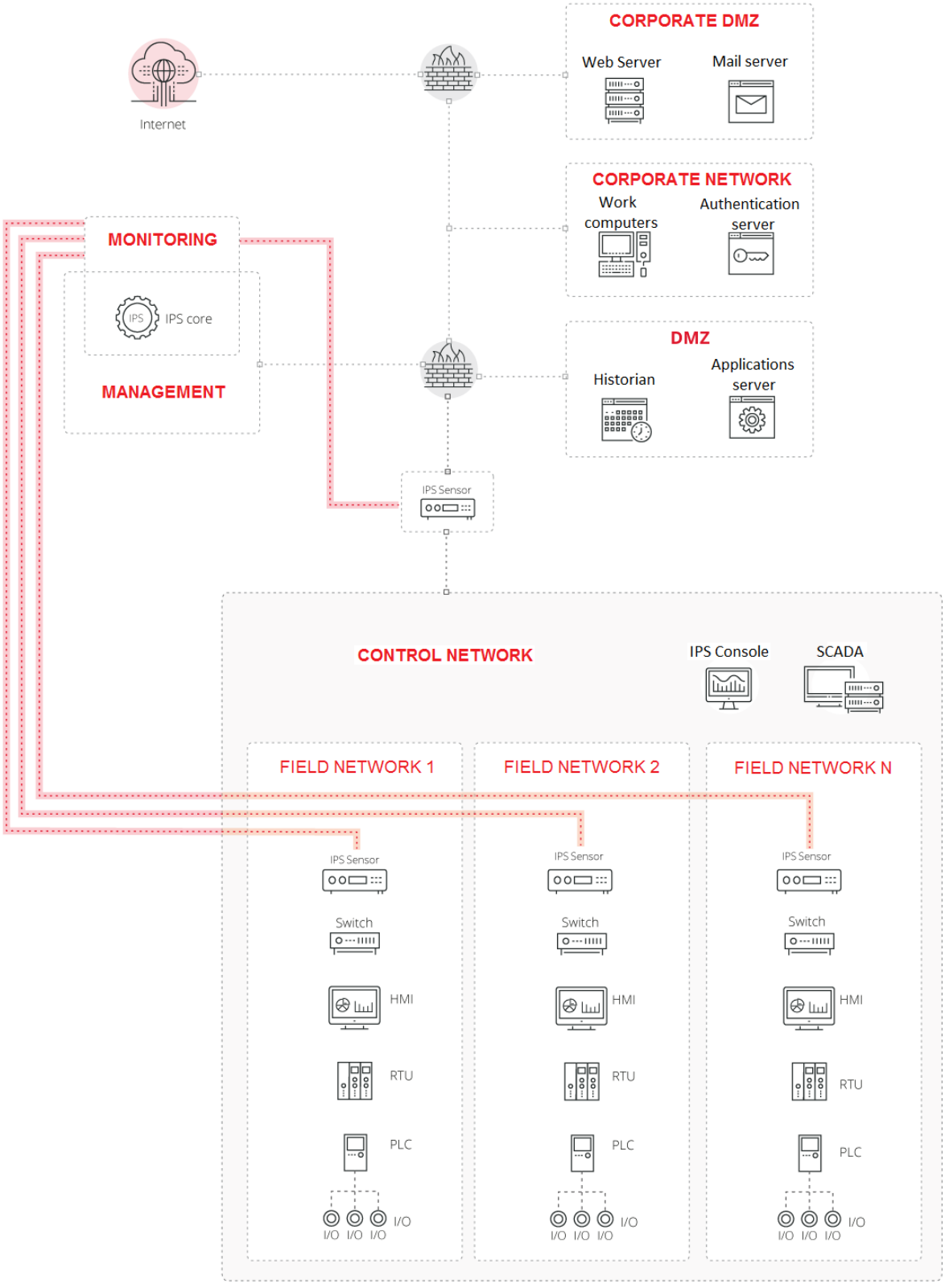


FIGURE B 2 : Architecture de sécurité avec IDS

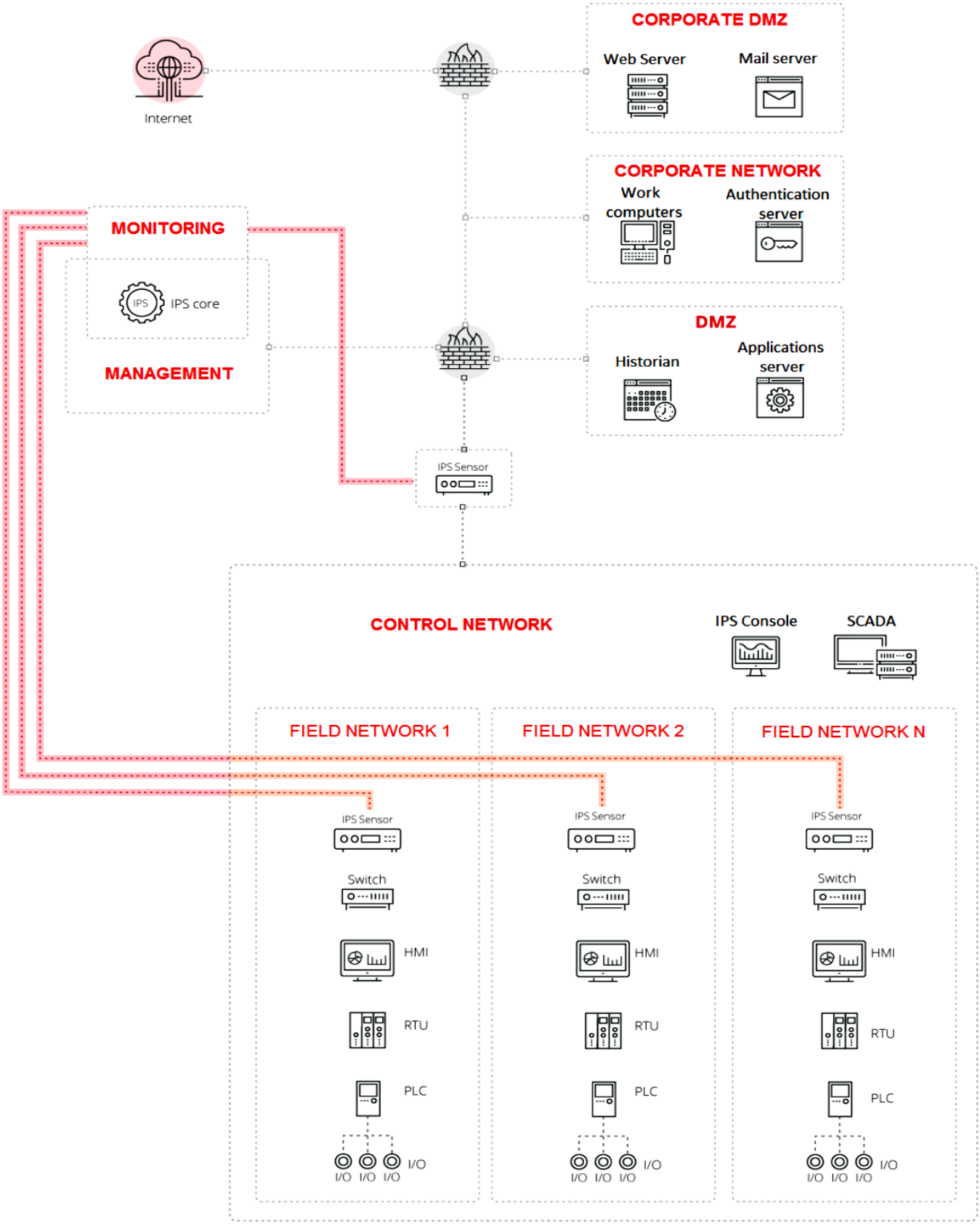


FIGURE B 3 : Architecture de sécurité avec IPS

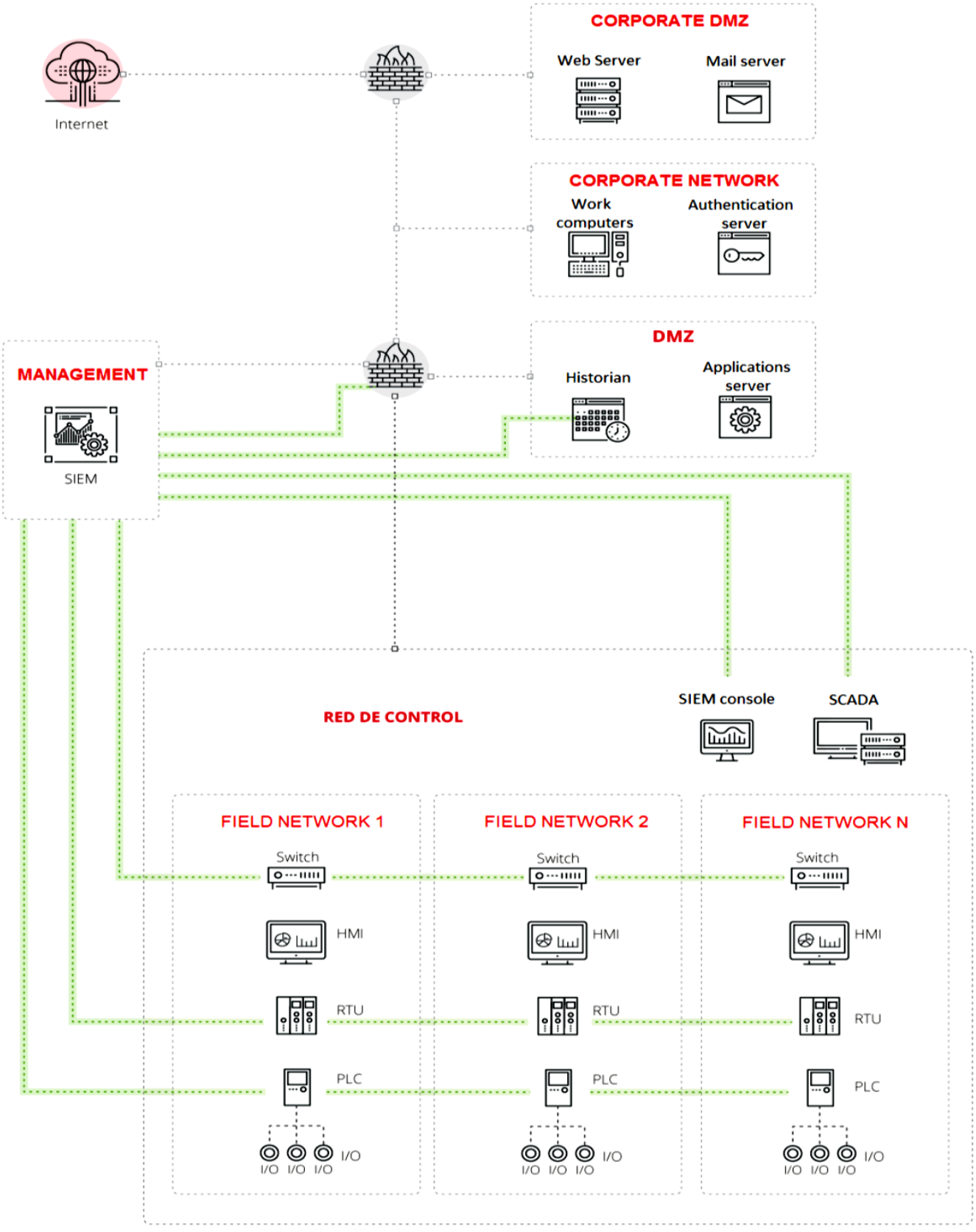


FIGURE B 4 : Architecture de sécurité avec SIEM

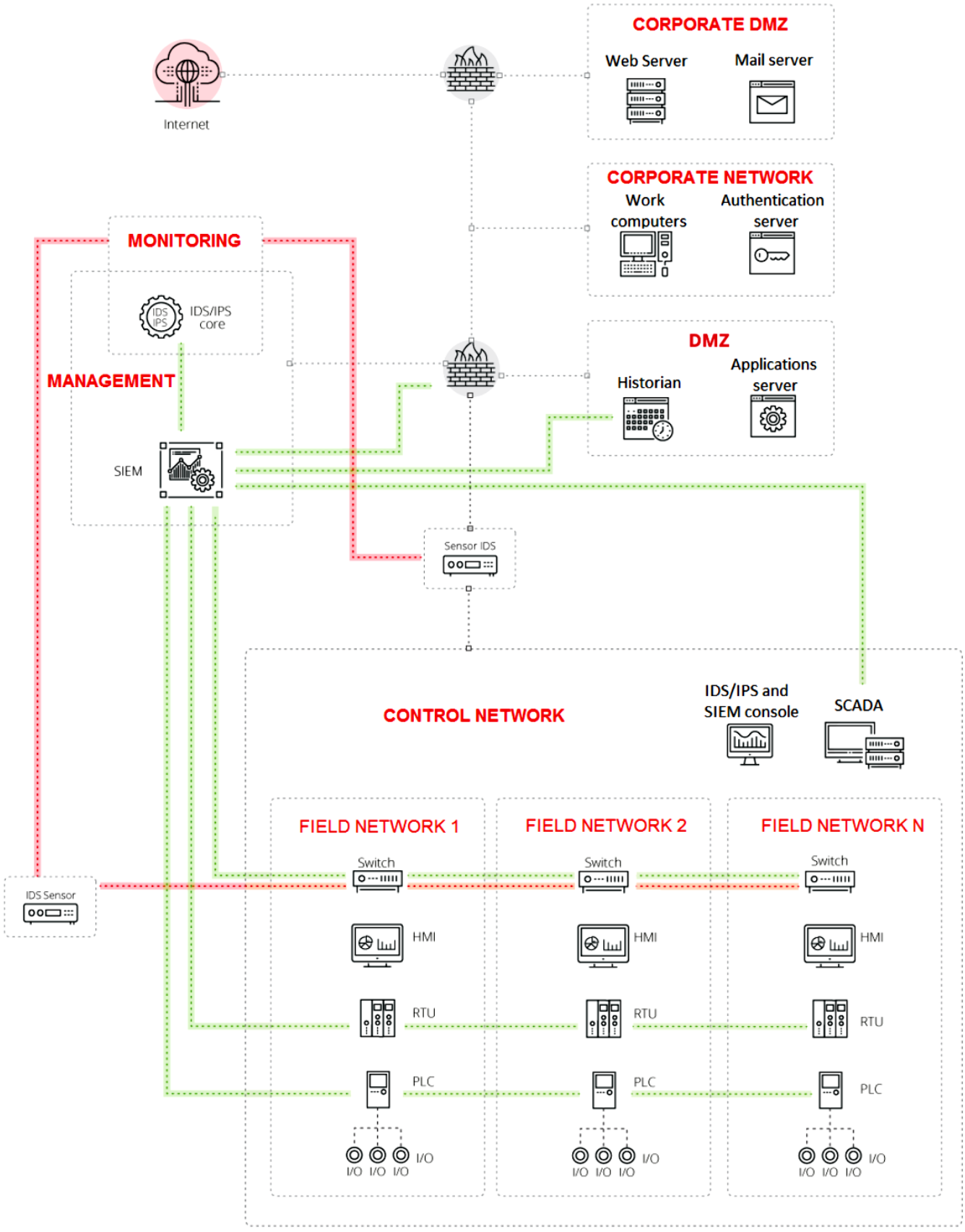


FIGURE B 5 : Architecture de sécurité avec IDS/IPS, SIEM

B.3 OUTILS DE DETECTION D'INTRUSIONS EFFICACES POUR LES SYSTEMES ICS

La sécurité des systèmes de contrôle industriels (ICS) repose sur des outils de détection d'intrusions (IDS) adaptés à leur environnement spécifique. Voici une sélection des outils les plus efficaces :

B.3.1 Snort :

Snort est un IDS basé sur des signatures largement reconnu, capable d'analyser le trafic réseau en temps réel. Il permet de détecter des attaques connues en comparant le trafic réseau à une base de données de signatures d'attaques. Sa flexibilité et sa capacité à être configuré pour différents environnements en font un choix populaire pour la protection des réseaux ICS.

B.3.2 Suricata :

Suricata est un autre outil performant qui combine la détection par signature avec une analyse approfondie des paquets (DPI). Conçu pour gérer des volumes élevés de trafic, il offre une détection efficace des anomalies. Sa capacité à surveiller le trafic dans des environnements critiques tels que ceux des ICS, en fait une option robuste pour la détection d'intrusions dans ces systèmes.

B.3.3 OSSEC

OSSEC est un IDS basé sur l'hôte (HIDS) qui surveille les journaux d'événements du système pour identifier les activités suspectes. Il est particulièrement utile pour détecter les menaces internes et peut analyser les données provenant de dispositifs connectés au réseau ICS, offrant ainsi une couche de sécurité supplémentaire en se concentrant sur la surveillance des hôtes individuels.

B.3.4 Zeek (anciennement Bro)

Zeek est un IDS qui adopte une approche différente en se concentrant davantage sur l'analyse comportementale du réseau que sur la simple détection basée sur des signatures. Zeek offre une surveillance approfondie du trafic réseau et peut être intégré à d'autres systèmes de réponse aux incidents, améliorant ainsi la capacité globale à gérer les menaces dans les réseaux ICS.

B.3.5 Systèmes de Détection d'Intrusions Basés sur l'Apprentissage Automatique

Les systèmes modernes de détection d'intrusions utilisent des techniques d'apprentissage automatique pour identifier les comportements anormaux dans le réseau. Ces outils basés sur des modèles statistiques sont capables de détecter des menaces inconnues et émergentes. Par exemple, des algorithmes tels que les réseaux neuronaux convolutifs (CNN) et récurrents (RNN) sont utilisés pour modéliser le comportement normal du réseau et détecter toute activité

anormale ou déviante, ce qui est particulièrement pertinent pour les réseaux ICS souvent ciblés par des attaques sophistiquées.

En définitive, le choix de l'outil de détection d'intrusions doit tenir compte des spécificités des systèmes ICS, notamment leur architecture, les contraintes de latence, et les types de menaces auxquelles ils sont exposés. L'intégration de plusieurs outils complémentaires peut également renforcer la sécurité globale en fournissant une couverture plus étendue contre divers vecteurs d'attaque.

B.4 SNORT VS SURICATA

B.4.1 Snort

Snort est un logiciel libre "sniffer" construit sur libpcap et tcpdump, qui permet de capturer tout le trafic qui atteint l'équipement sur lequel il est installé. Snort est conçu pour être précis dans la journalisation des activités sur le réseau et recherche en permanence d'éventuelles coïncidences entre le flux de données et les attaques qui sont enregistrées en fonction de différentes règles.

Snort dispose d'une base de données d'attaques qui est constamment mise à jour, ce qui permet en outre l'ajout ou la mise à jour via Internet. Les utilisateurs peuvent créer des "signatures" basées sur les caractéristiques des nouvelles attaques réseau et les envoyer à la liste de diffusion Snort sigs. Cette communauté a fait de Snort l'un des IDS les plus populaires, les plus récents et les plus robustes. Une autre des caractéristiques les plus importantes de Snort est que les principaux fabricants d'IDS/IPS l'utilisent et sont capables d'utiliser ses signatures sur presque tous les appareils.

B.4.2 Suricata

Suricata est le nom d'un projet de logiciel libre développé par la communauté Open Information Security Foundation (OISF). Il s'agit d'un moteur basé sur un ensemble de règles IDS/IPS pour surveiller le trafic sur le réseau et fournir des alertes à l'administrateur système lorsqu'un événement est considéré comme suspect. Il est conçu pour être compatible avec d'autres composants de sécurité existants et, de plus, accepte les appels d'autres applications.

Description :

Suricata peut fonctionner comme un IDS, un IPS, un moniteur de sécurité réseau (NSM) en temps réel ou comme un analyseur final pcap (fichiers avec captures de trafic). La fonction d'analyse réseau est basée sur des règles et des signatures, bien qu'elle puisse également offrir des supports pour de nouveaux scripts via le langage LUA. Il dispose d'entrées et de sorties standardisées dans des formats comme YAML qui lui permettent d'être facilement intégré à d'autres outils comme SIEM ou bases de données. En impliquant la communauté open source et l'ensemble le plus important de ressources de règles IDS/IPS disponibles, l'OISF a construit le moteur Suricata pour simplifier le processus de maintien du niveau de sécurité optimal. Grâce à des associations stratégiques, l'OISF profite de l'expérience d'Emerging Threats et d'autres

ressources importantes pour l'industrie afin de fournir les règles les plus récentes et les plus complètes disponibles.

Voici un tableau comparatif entre **Snort** et **Suricata** dans le contexte des systèmes de contrôle industriels (ICS) :

TABLEAU B 1 : Différence entre SNORT et SURICATA dans les ICS

Caractéristiques	Snort	Suricata
Type de Détection	Basé sur les signatures	Signatures et anomalies (DPI)
Conception	IDS basé uniquement sur les signatures	IDS/IPS combinant signatures et DPI
Performance	Bonne pour des réseaux de taille modérée	Optimisé pour les environnements à fort volume de trafic
Support Multithread	Non, fonctionne sur un seul thread	Oui, supporte le multithread natif
Analyse des Protocoles	Support limité pour les protocoles ICS	Analyse approfondie, y compris pour les protocoles industriels (Modbus, DNP3, etc.)
Détection des Anomalies	Détection basée uniquement sur des signatures prédéfinies	Détection d'anomalies par inspection approfondie des paquets et surveillance du comportement réseau
Scalabilité	Moins évolutif dans des environnements ICS à grande échelle	Conçu pour des environnements à trafic élevé, adapté aux grandes infrastructures ICS
Configuration et Personnalisation	Flexible mais nécessite plus de configuration manuelle	Flexible avec une meilleure gestion automatique des signatures et des règles
Performance de Débit	Performances limitées avec un grand nombre de règles	Meilleure gestion de gros volumes de trafic et de règles multiples
Logs et Reporting	Journaux de base avec analyse manuelle	Journaux détaillés avec possibilités d'intégration pour visualisation et monitoring (EveBox, Kibana)
IPS (Prévention d'Intrusion)	Fonctionnalités IPS limitées	Fonctionnalités IPS avancées avec blocage en temps réel des attaques

Communauté et Support	Large communauté, mais moins active	Communauté active avec des mises à jour régulières
Cas d'Utilisation ICS	Convient pour des systèmes ICS plus petits ou des segments réseau spécifiques	Adapté aux grandes infrastructures ICS avec une surveillance continue et un traitement rapide des attaques complexes

Résultat :

Dans le contexte des systèmes ICS, Suricata est généralement plus performant pour les environnements critiques, grâce à son support du multithread, ses capacités d'inspection approfondie des paquets, et sa détection d'anomalies. Snort reste un bon choix pour des environnements plus petits ou avec des ressources limitées, bien qu'il nécessite souvent plus de configuration manuelle et soit moins performant pour des réseaux complexes et à fort trafic.