Guide pour la protection des Systèmes de contrôle industriels (ICS)

❖ Définitions :

- **Système Industriel** : Un système industriel est composé de deux parties :

- Une partie opérative, qui exécute les tâches (travail, action) en produisant un phénomène physique à partir des ordres de la partie commande.

- Une partie de commande, qui assure le pilotage et le contrôle du système.

- **Systèmes de contrôle industriels (ICS):**

- est une expression générale utilisée pour décrire différents types de systèmes de contrôle et d'instrumentation associée qui comprennent les dispositifs, systèmes, réseaux et contrôles utilisés pour faire fonctionner et ou automatiser les processus industriels.

❖ Les enjeux de la cybersécurité des systèmes industriels

Les cyberattaques sont de plus en plus diversifiées et complexes, et le besoin d'améliorer les pratiques de cybersécurité devient une priorité. Les réseaux industriels sont mal protégés contre les attaques des systèmes informatiques d'entreprise en raison du niveau élevé d'interaction entre eux (voir figure 1).

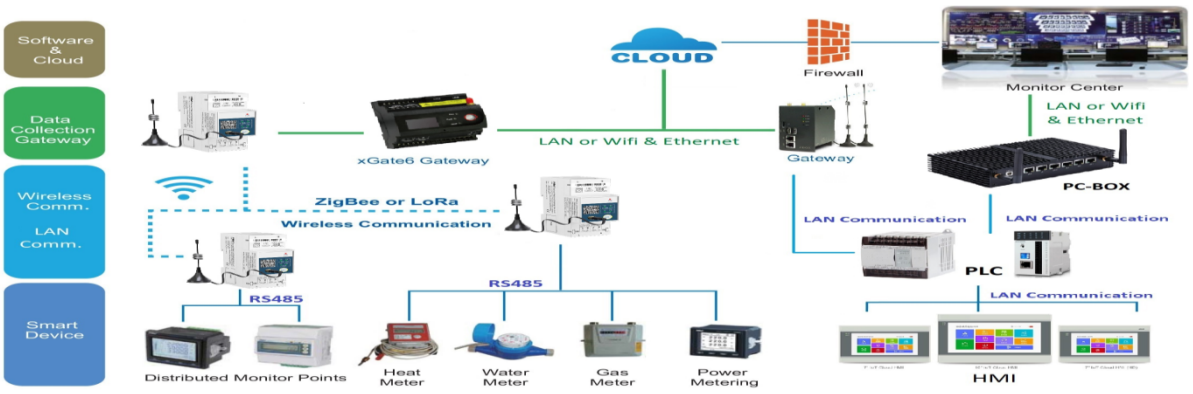

Figure1

- **Menaces courantes sur les ICS**

Parmi ces risques, citons :

-Menaces externes et attaques ciblées (terrorisme, hacktivistme…), menaces internes (comportements malveillants des personnels) et l'erreur humaine.

- L'élargissement de la surface de cyberattaque de l'ICS qui peut entraîner une augmentation des incidents de sécurité.

- L'idée de l'élimination de la segmentation du réseau de l'ISC pour permettre un meilleur accès aux systèmes critiques.

- Blocage ou retard de la circulation de l'information dans les réseaux ICS, ce qui pourrait perturber leurs fonctionnement.

-Modifications non autorisées des instructions, des commandes ou des seuils d'alarme, susceptibles d'endommager ou d'arrêter des équipements, d'avoir des répercussions sur l'environnement et/ou de mettre en danger des vies humaines.

-Envoi d'informations inexactes aux opérateurs du système, soit pour masquer des modifications non autorisées, soit pour inciter les opérateurs à entreprendre des actions inappropriées, ce qui pourrait avoir divers effets négatifs.

-Modification des paramètres de configuration de l'ISC ou infection par un logiciel malveillant, ce qui pourrait avoir divers effets négatifs.

-Interférence avec le fonctionnement des systèmes de sécurité, ce qui pourrait mettre en danger la vie humaine.

- **Vulnérabilités fréquemment rencontrées:**

Des principales vulnérabilités rencontrées dans les systèmes d'informations industriels, on peut citer :

- Absence de politique de sauvegarde des données et des configurations des équipements.
- Absence de politique de gestion des médias amovibles.
- Absence de méthodes d'investigation et d'audit.
- Absence de veille sur les vulnérabilités (mise à jour des systèmes d'exploitation et des applications).
- Absence de mécanisme de signature des firmwares.
- Absence d'inventaire du parc de système d'information industriel.
- Défaut de la politique de gestion des mots de passe et des accès.
- Utilisation de protocoles vulnérables.
- Absence de plan de continuité d'activité.
- Mal définition des responsabilités.

- Manque de sensibilisation.
- L'utilisation d'appareils mobiles, WiFi et d'appareils RFID.
- Absence de défense multicouche.
- Accès à distance sans contrôle.
- Absence de journaux d'accès.
- Logiciels de jeux et autres sur les ordinateurs de contrôle.
- Manque d'outils de détection.
- Logiciels de contrôle non examinés.
- Menace persistante avancée.

Quelques vecteurs d'attaques

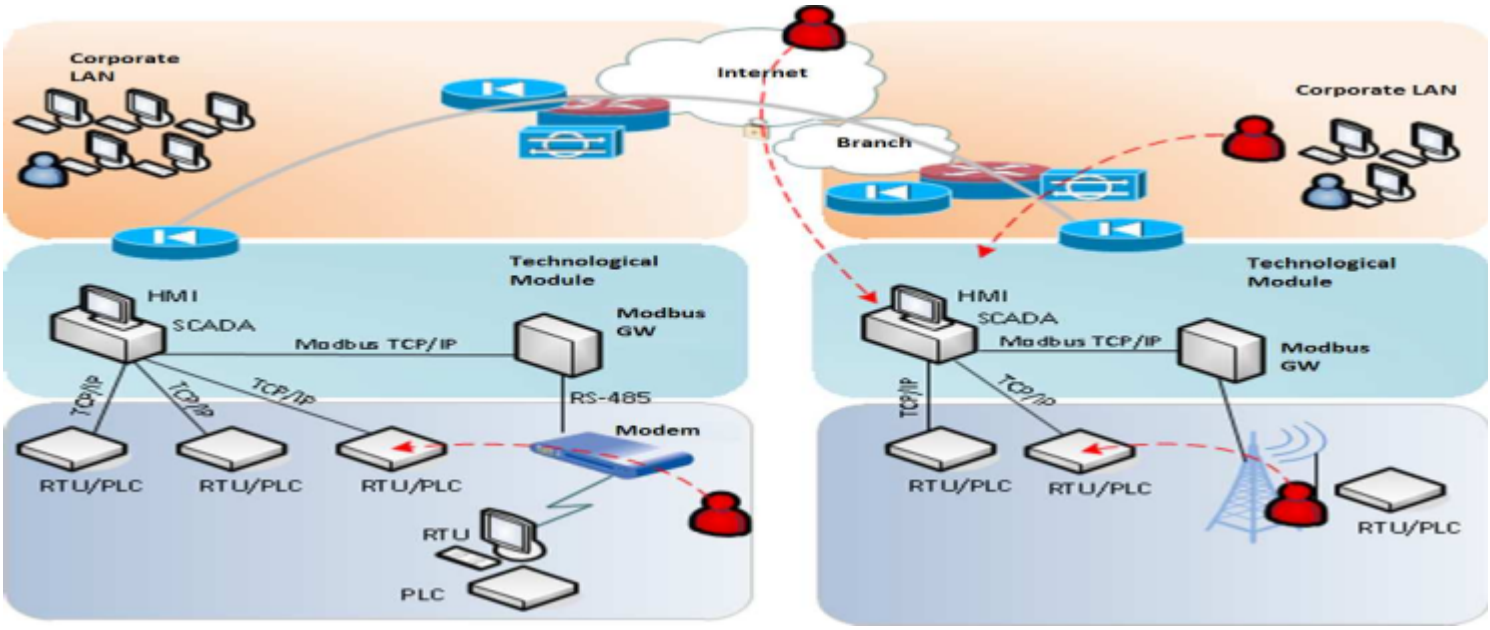

Figure 2

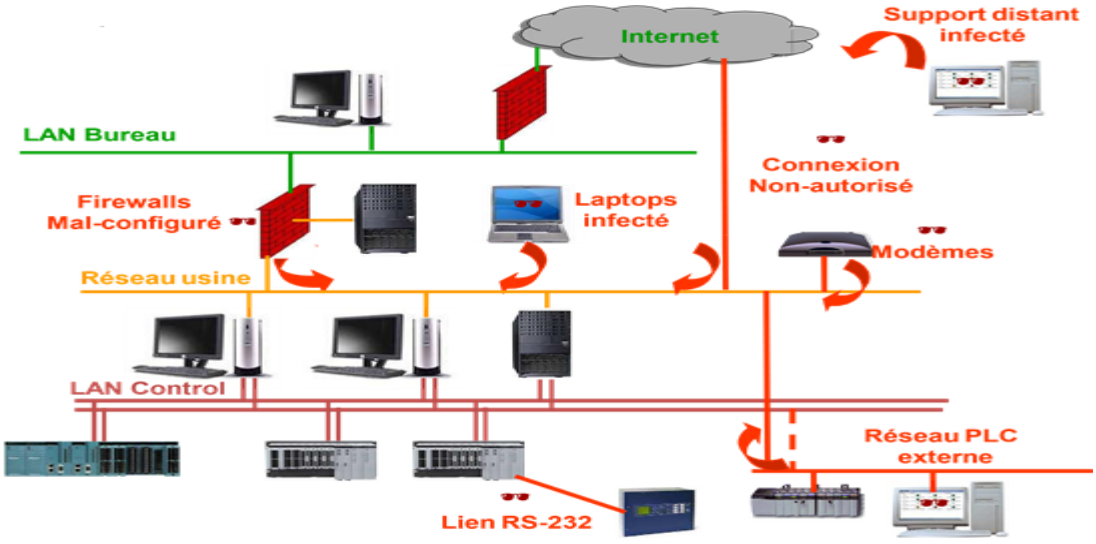

Figure 3

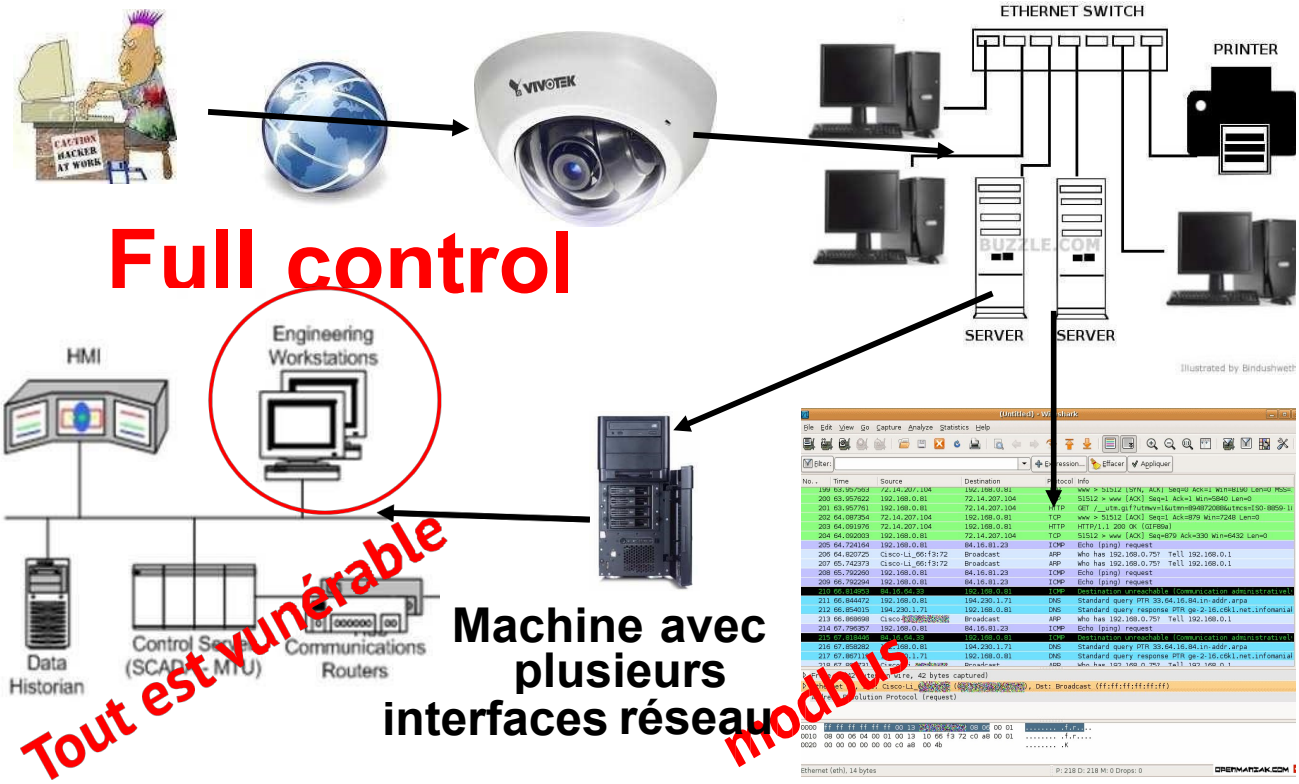

Figure 4

- **Les bonnes pratiques pour la protection des Systèmes de contrôle industriels (ICS):**

Pour protéger vos Systèmes ICS, cela passe par l'adoption de plusieurs bonnes pratiques :

- Définir et inventorier les actifs de l'ICS.
- Effectuer une analyse de risques et des vulnérabilités.
- Fournir une formation et sensibiliser le personnel de l'ICS à la sécurité.
- Utiliser un processus de cycle de vie de la sécurité

- Évaluation des menaces

- Mise en œuvre de contre-mesures et vérification

- Surveillance et maintenance

- Segmentation du réseau

- Décomposer le réseau en zones physiques ou logiques ayant des exigences de sécurité similaires (voir figures 5,6 et 7).

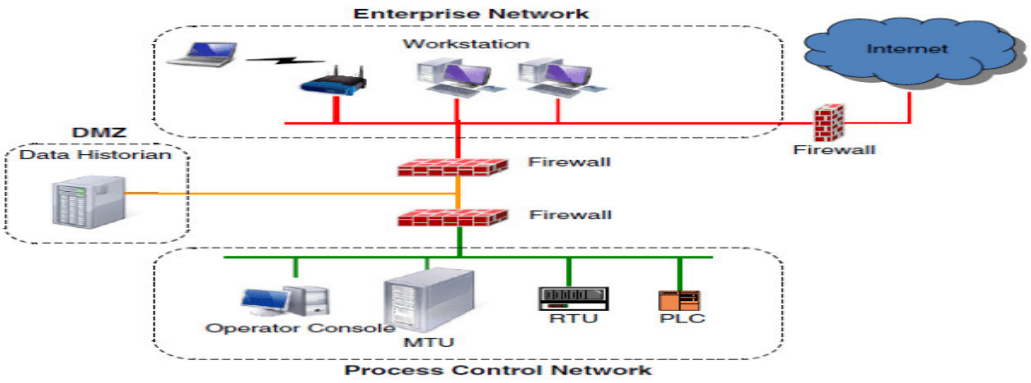

Figure 5

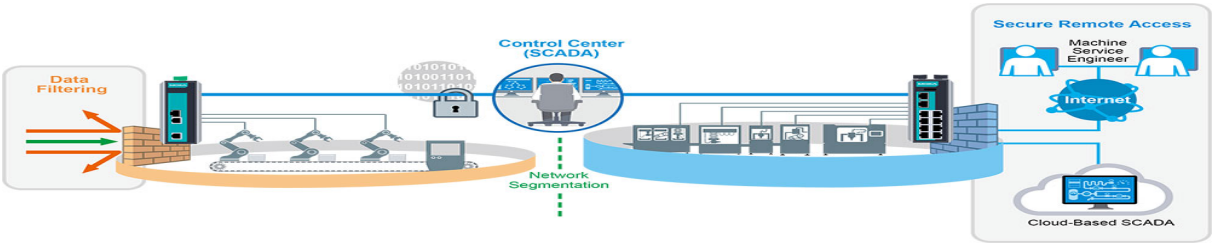

Figure 6

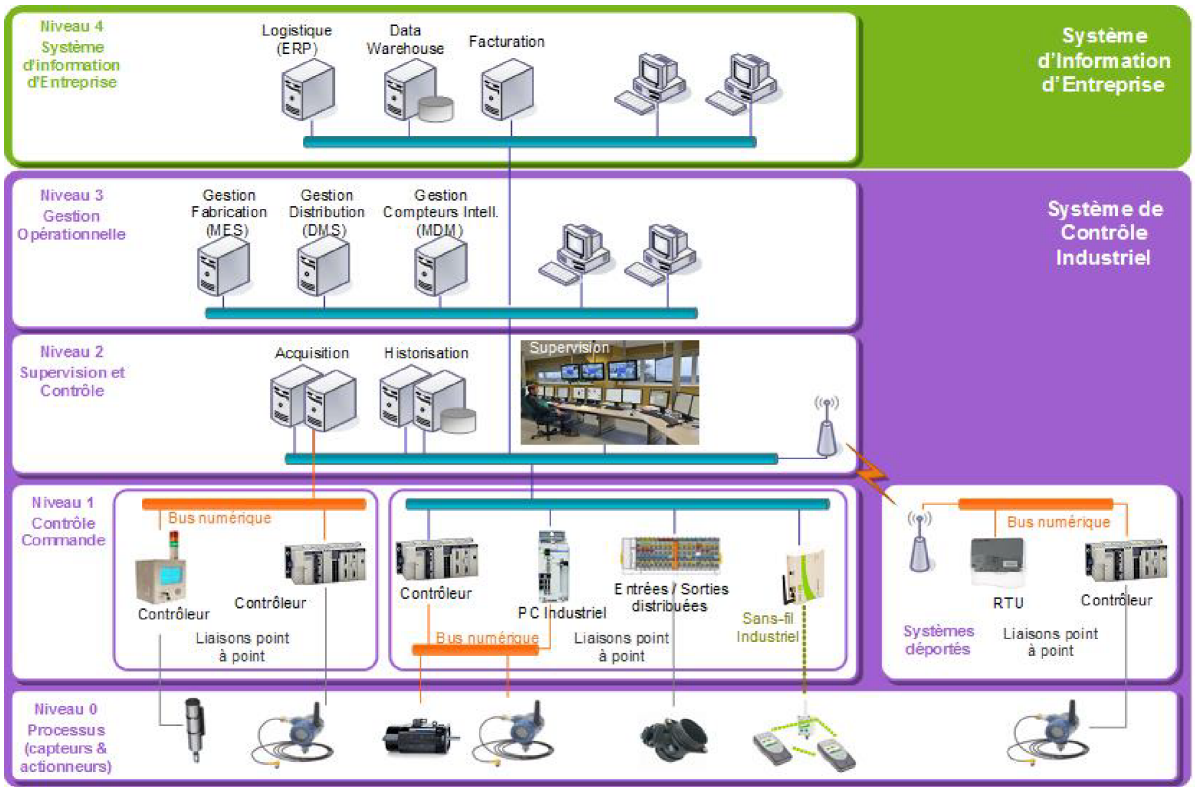

Figure 7

- Définir l'interaction entre les zones

- Exigences relatives aux dispositifs.

- Identification du trafic autorisé sur les conduits.

- Exigences en matière de communication sécurisée.

- Politique d'Authentification

- Utilisez une gestion centralisée des utilisateurs.

- utiliser les protocoles Radius et TACACS+.

- Politique d'Autorisation

- Seuls les dispositifs autorisés peuvent être connectés.

- Désactivez tous les ports inutilisés.

- Contrôle de l'adresse MAC au niveau du port.

- Intégrité et cryptage des données

- Utiliser HTTPS, désactiver http.

- Utiliser SSH, désactiver TELNET.

- Utiliser SNMPv3, désactiver SNMPv1/v2.

- Utiliser des Pare-feu et VPN sécurisé pour garantir que le système de contrôle industriel répond aux exigences de sécurité des zones.
- Surveillez les connexions VPN pour détecter tout accès suspect.
- Restreindre et sécuriser l'utilisation des outils d'administration à distance.
- Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau.
- Mettre en place des solutions de journalisation nécessaires pour contrôler les évènements survenus sur vos serveurs critiques et vos équipements réseaux.
- Utilisez des services chiffrés pour protéger les communications réseau.
- Changez les mots de passe par défaut.
- Protéger les accès aux locaux et aux équipements.
- Mettre en place une politique de sauvegarde, backup et cryptage des données et configurations.
- Mettre en place une politique de veille sur les vulnérabilités, gestion des correctifs, Sauvegardes/restaurations et de documentation.

- Mettre en place une politique de réponse aux incidents.
- Remplacer tous les logiciels et matériels en fin de vie.
- Utiliser l'authentification à deux facteurs (2FA) ou multifactorielle.
- Adopter les standards (Exemple : **NIST SP800 82 rev3 , NIST SP800 53 rev5**).
- Réaliser des Audits techniques sur les systèmes industriels pour vérifier l'efficacité des mesures techniques mises en place et prioriser au mieux les actions à réaliser pour diminuer le niveau de menace sur ceux-ci.
- Élaboration d'un programme de sécurité complet:

  -Obtenir l'adhésion de la haute direction.

  -Constituer et former une équipe multifonctionnelle.

  -Définir la charte et le champ d'application.

  -Définir les politiques et procédures spécifiques du ICS.

Exemple : Cas de Stuxnet

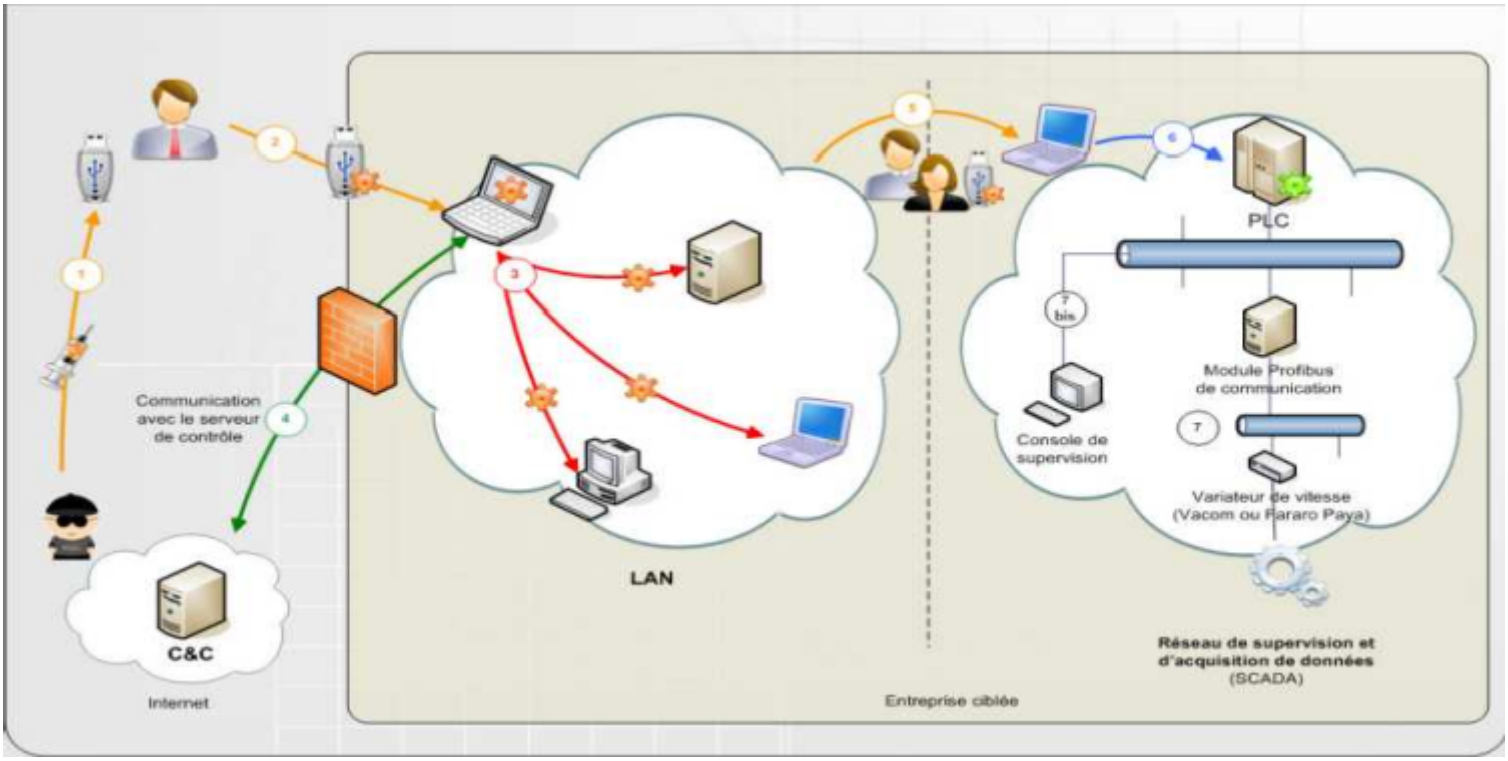

Figure 8