Chapitre 1 Concepts et définitions sur supervision industrielle

1. Introduction

L'automatisation industrielle est l'ensemble des techniques permettant de réduire ou d'éliminer l'intervention directe et continue des travailleurs humains dans les processus de production et de traitement industriel. Ses principaux objectifs sont :

- augmenter la productivité et la qualité du produit fini ;

- réduire les coûts de production ;

- et réduire la charge des travailleurs et les soulager des tâches dangereuses.

Les systèmes d'automatisation actuels reposent principalement sur des appareils dotés de microprocesseurs, parmi lesquels les Automates Programmables Industriels (API) occupent une position centrale. Ils ont été spécialement conçus pour résister aux conditions de fonctionnements exigeantes de l'environnement industriel. Ils sont également capables de gérer de grandes quantités d'entrées et de sorties provenant des capteurs et des actionneurs, tout en coordonnant les interactions complexes entre les dispositifs de l'installation.

Figure 1.1 : Exemple d'automates programmables industrielles (de gauche à droite : S7-1200 et micro PLC ELC-6AC-R).

Cependant, ces systèmes ne fonctionnent pas de manière transparente pour les opérateurs humains. Autrement dit, ils ne sont pas intrinsèquement capables de communiquer des informations directement

exploitables par les opérateurs. Ils ne peuvent pas, par exemple, anticiper des situations anormales, réagir de manière proactive en temps opportun, ou contribuer à la prise de décisions pour optimiser le fonctionnement global de l'installation.

Le besoin de voir, en temps réel, ce qui se passe à l'intérieur du processus a poussé les fabricants d'automatismes à compléter les systèmes de commande par des solutions de supervision pour surveiller le fonctionnement des installations automatisées. Cela a ouvert la voie à de nouvelles approches en matière de gestion et d'optimisation des processus automatisés et une réduction des pannes et des risques potentiels.

Figure 1.2 : Supervision d'un processus industriel complexe depuis une salle de contrôle (les écrans affichent d'une manière graphique le flux des informations provenant des équipements de terrain).

2. Supervision industrielle

1.1 Définition

Définition : La supervision industrielle désigne un ensemble de fonctionnalités permettant à un opérateur humain de surveiller et de contrôler, localement ou à distance et en temps réel, le fonctionnement d'une installation automatisée ou d'une machine.

La surveillance se concentre sur l'observation des données pour détecter les conditions anormales et les situations critiques. Ce processus de surveillance s'appuie sur la collecte et l'analyse

constantes de données provenant de capteurs et de divers équipements. Les données collectées sont présentées aux opérateurs sous forme graphiques facilement interprétables pour faciliter la tâche de surveillance.

Dans le cadre de la supervision industrielle, le contrôle comprend les actions effectuées par les opérateurs pour gérer et ajuster le processus et les équipements de l'installation. Cette capacité est cruciale pour assurer une réactivité immédiate face aux variations imprévues et aux changements des besoins opérationnels. Parmi ces actions on retrouve la modification des consignes, l'ajustement des paramètres des équipements, l'annulation ou la modification des tâches associées aux automates, la mise en marche, l'arrêt, etc.

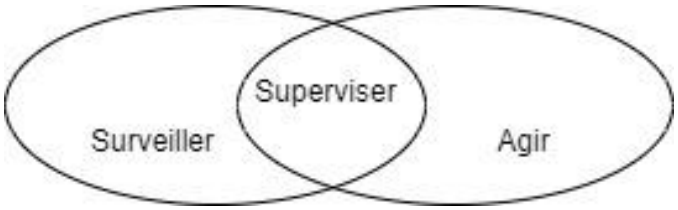


Figure 1.3 : Supervision=surveiller + agir.

1.2 Fonctionnalités d'un système de supervision

Les systèmes de supervision modernes offrent une gamme de fonctionnalités pour répondre aux besoins complexes de l'automatisation industrielle. Parmi leurs fonctionnalités clés, on site :

a. Surveillance en Temps Réel

Les systèmes de supervision collectent des données provenant de capteurs, d'équipements et de machines pour les afficher en temps réel sur un système informatique sous forme graphique claire. Cela aide grandement l'opérateur humain à surveiller aisément l'installation ou la machine et déceler rapidement les anomalies.

b. Contrôle

Ils offrent aux opérateurs la possibilité d'ajuster les paramètres, de définir des consignes et d'effectuer des actions à distance sur les équipements ou les machines. Cela inclut la modification des seuils, la mise en marche ou l'arrêt d'équipements spécifiques.

c. Archivage et Historique des Données

Ils enregistrent et archivent les données historiques pour permettre l'analyse rétrospective[1]. Cette fonctionnalité est essentielle pour tirer des leçons des incidents passées pour détecter les anomalies à temps et améliorer les performances du processus.

d. Gestion des Alarmes

Ils gèrent les alarmes en temps réel, pour signaler les événements anormaux ou critiques. Les systèmes de supervision hiérarchisent et affichent les alarmes pour permettre une réponse rapide aux situations d'urgence ou aux problèmes potentiels.

e. Intégration avec d'autres Systèmes

Ces systèmes sont conçus pour s'intégrer à d'autres systèmes tels que les ERP (Enterprise Resource Planning) ou les logiciels de gestion de maintenance, pour assurer une coordination optimale des opérations.

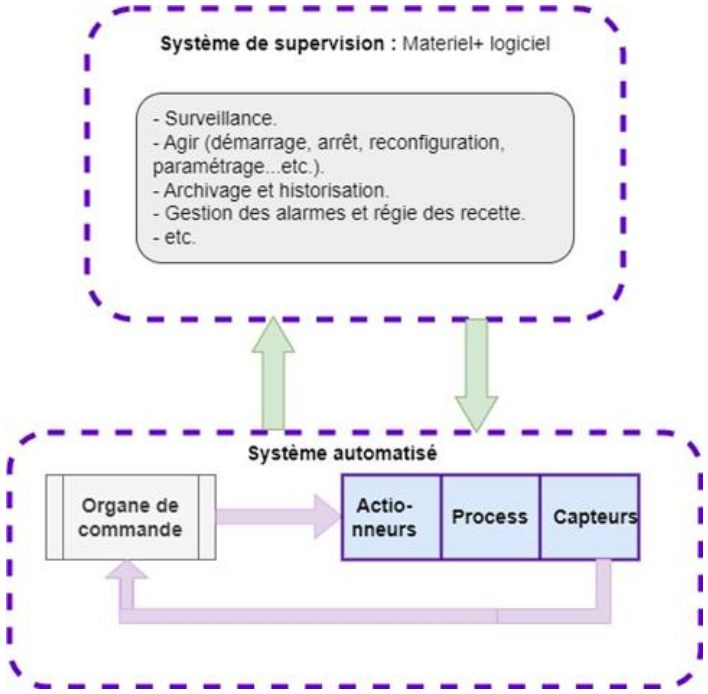


Figure 1.4 : Rôles de la supervision industrielle.

[1] Fait référence à l'examen et à l'interprétation des données collectées dans le passé afin de tirer des informations significatives.

3. Domaines d'application

Les applications de la supervision industrielle se déploient dans divers secteurs, parmi lesquels :

Installations industrielles automatisées : production manufacturière (usines des produits de consommation, automobiles…etc.), industrie pétrolière, industrie agroalimentaire…etc.

Production et distribution de l'énergie électrique : Des centrales de production aux réseaux de distribution, la supervision industrielle intervient pour assurer la fiabilité et l'efficacité énergétique.

Gestion des transports : On la trouve également dans la gestion des flux routiers et ferroviaires, ainsi que dans la surveillance et la maintenance des tunnels (ventilation, éclairage, etc.).

Gestion des ressources hydrauliques : Gestion des réseaux hydrauliques, barrages, alimentation en eau.

Gestion technique des bâtiments : La supervision industrielle contribue également à la gestion technique des bâtiments, notamment en contrôlant les systèmes de chauffage, d'éclairage, les ascenseurs, assurant ainsi des conditions optimales de fonctionnement et de sécurité.

4. Définitions

Pour mieux saisir les concepts et les notions abordés dans ce cours, on définit d'abord quelques termes clés lié à la supervision industrielle.

HMI (Human Machine Interface) : L'acronyme HMI[2] (ou panel HMI) signifie Interface Homme-Machine. Ce terme est employé pour désigner un écran qui propose une interface graphique conviviale qui permet de superviser une installation ou une machine.

[2] HMI est en fait un terme générique qui désigne n'importe quel dispositif permettant à un opérateur d'interagir avec une machine ou un appareil en milieu industriel. Un bouton ou un voyant peuvent être qualifiés d'HMI.

PC industriel (Industrial PC) : C’est un ordinateur spécialement conçu pour résister aux environnements industriels exigeants.

Panel PC : C’est un système informatique tout-en-un qui combine à la fois un écran tactile et un PC industriel dans un seul boîtier. Il est couramment utilisé dans la supervision des processus industriels là où l’on exige des fonctionnalités avancées qui ne sont pas remplies par de simple HMI.

Operateur Workstation (Poste opérateur) : C’est une combinaison de dispositifs matériels et logiciels spécifiquement conçus pour la supervision industrielle depuis une salle de contrôle. Elle comprend généralement un ordinateur avec des logiciels de supervision, des écrans, un clavier, une souris et d'autres périphériques nécessaires à l'interaction avec les systèmes industriels.

Salle de contrôle (control room) : C’est un espace centralisé dans lequel se fait les opérations de supervision des processus complexe.

Alarme : Notification généré par le système de supervision pour signaler des conditions anormales ou dangereuses.

Evènement : Notification généré par le système de supervision pour signaler un évènement qu'il soit important ou non.

Measurements Processing (traitement des mesures) : Ce processus fait référence à la manipulation et à l'analyse approfondie des données de mesure collectées à partir de capteurs ou d'autres dispositifs pour détecter des tendances, des schémas, des anomalies ou des situations inhabituelles.

Logging : Il fait référence à l'enregistrement ou à la journalisation (génération de fichier journal) des données liées aux opérations, aux performances et aux événements qui se produisent dans un système industriel.

Gestion des recettes (Recipe Management) : Elle fait référence à la capacité de stocker, gérer et exécuter des ensembles prédéfinis de paramètres, de configurations ou de procédures pour des opérations spécifiques. Les recettes sont des configurations préétablies qui définissent les paramètres nécessaires pour exécuter une tâche ou un processus donné.

5. Interfaces de Visualisation

La supervision industrielle repose sur des interfaces de visualisation qui permettent à l'opérateur humain de surveiller et de contrôler à distance le processus industriel. Ces systèmes présentent les données qui reflètent l'état du processus ainsi que les actions de l'opérateur.

Les premiers moyens de visualisation étaient composés de témoins lumineux de différentes couleurs, des compteurs et des jauges arrangés sur des tableaux de bord pour indiquer les différentes situations et modes de fonctionnement du processus. Des boutons de formes variées étaient utilisés pour le contrôle du processus.

Figure 1.5 : Exemples des premières interfaces de visualisation utilisés dans la supervision industrielle.

Actuellement, Ces moyens traditionnels ont été remplacés par des systèmes informatiques à écran souvent désignés par **HMI** qui affichent les informations sous forme de synoptiques animés, tableaux et tracés de courbes.

Figure 1.6 : Quelques HMI de Siemens.

Ces interfaces de visualisation modernes peuvent être de différentes formes et tailles selon les besoins des tâches de la supervision :

- Des consoles HMI basiques de quelques pouces, offrant des fonctionnalités limitées et dédiés à des applications spécifiques ;
- des HMI de gamme moyenne, tactiles ou avec clavier, proposant des fonctionnalités plus étendues ;
- des HMI de haute gamme offrant des fonctionnalités encore plus avancées, utilisés dans des applications complexes.

Les HMI de gamme moyenne à haut de gamme peuvent fonctionner avec des systèmes d'exploitation embarqués.

Pour les tâches de supervision complexes, on utilise des HMI à base d'ordinateurs, c-à-d, des PC, des panels PC, des PC industriels ou des stations de travail[3] avec un ou plusieurs écrans. Ces interfaces fonctionnent souvent avec des systèmes d'exploitation courants comme Windows.

Figure 1.7 : De gauche à droite : un poste opérateur basé sur une station de travail, un panel PC.

6. Supervision locale et supervision étendue à distance

Selon l'emplacement où les opérateurs surveillent le processus, deux approches complémentaires sont utilisées pour gérer les tâches de

[3] Une station de travail est un type d'ordinateur haute gamme qui se distingue d'un PC grand public par performances élevées et une capacité de traitement avancée.

supervision industrielle : la supervision locale, qui se déroule sur place, et la supervision étendue depuis une salle de contrôle centrale.

6.1 Supervision locale

La supervision locale se fait directement sur site pour superviser une machine ou un nombre limité d'équipements. Elle repose sur des HMI installés à proximité du processus à superviser. Ses principales caractéristiques sont :

- **Proximité physique :** Les systèmes de supervision locale sont installés près des machines ou des processus qu'ils supervisent.
- **Réactivité :** Ils assurent des réponses rapides aux événements et aux modifications des conditions locales.
- **Fiabilité :** Moins de dépendance aux réseaux de l'usine externes.
- **Gestion isolée :** Limites dans la coordination globale des processus.
- **Maintenance locale :** Maintenance et dépannage sur site.
- **Nombre d'équipements supervisés :** Le nombre d'équipement que l'on peut superviser dans ce cas est limité.

Figure 1.8 HMI utilisés dans la supervision sur cite.

Figure 1.9 HMI mobiles (portatifs).

6.2 Supervision étendue à distance

La supervision industrielle étendue implique la centralisation du contrôle et de la surveillance des processus industriels à partir d'une salle de contrôle centrale, souvent distante des équipements surveillés. Cette approche utilise des réseaux informatiques pour connecter les équipements sur site à un ordinateur centralisé. Ses principales caractéristiques sont :

- **Centralisation :** Contrôle et surveillance centralisés depuis une salle de contrôle.
- **Connectivité réseau :** Utilisation de réseaux pour relier les équipements sur site au système central.
- **Surveillance globale :** Capacité à surveiller plusieurs processus ou sites simultanément.
- **Coordination globale :** Possibilité de coordonner et d'optimiser l'ensemble des processus.
- **Maintenance à distance :** Possibilité de dépannage et de maintenance à distance.
- **Dépendance réseau :** Vulnérabilité aux pannes de réseau.
- **Temps de réponse :** Possibilité de délais dans les réactions aux événements locaux.

Figure 1.10 De gauche à droite, salles de contrôle des années 1950, 1970 et 2010.

7. Architecture matérielle typique de la supervision industrielle

La supervision requiert plusieurs composants interconnectés qui travaillent ensemble pour contrôler et surveiller les processus industriels.

La figure ci-dessous montre l'architecture fonctionnelle typique d'un système de supervision local constitué d'un seul HMI utilisé pour superviser un processus commandé par un seul PLC.

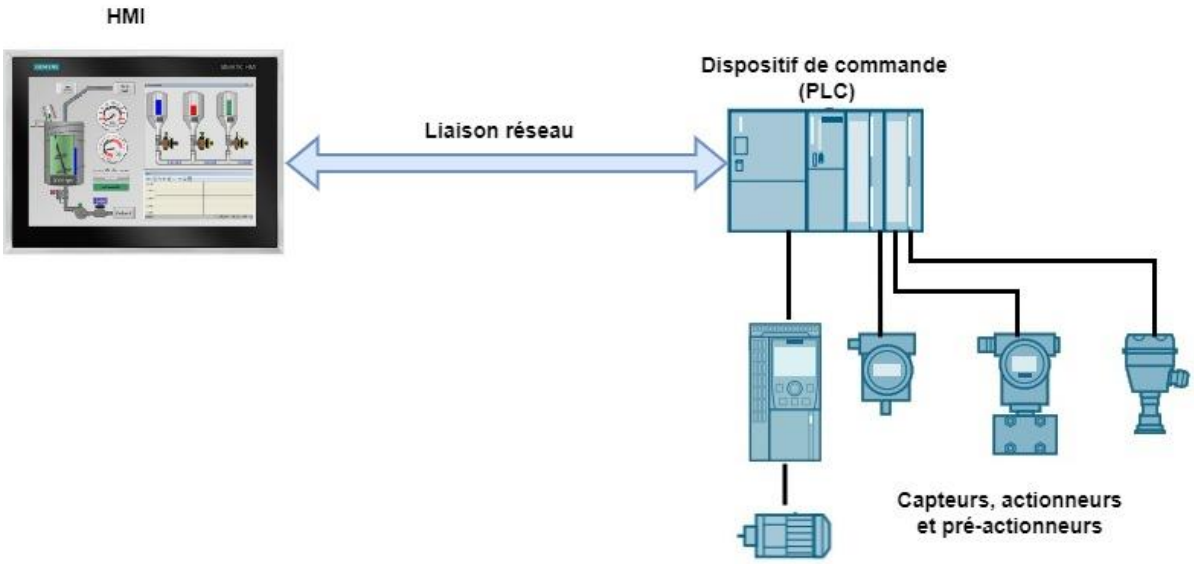


Figure 1.11 Architecture fonctionnelle typique d'un système de supervision local.

Durant son fonctionnement, le PLC exécute le cycle de fonctionnement appelé cycle automate qui dure typiquement de de 1 à 50 ms :

- Le PLC lit les signaux des capteurs (les entrées) et les mémorise.
- Il calcule les équations logiques de fonctionnement du système en fonction des entrées et d'autres variables internes puis il les mémorise.
- Les résultats (commandes) sont recopiés dans les sorties (envoyés aux actionneurs).

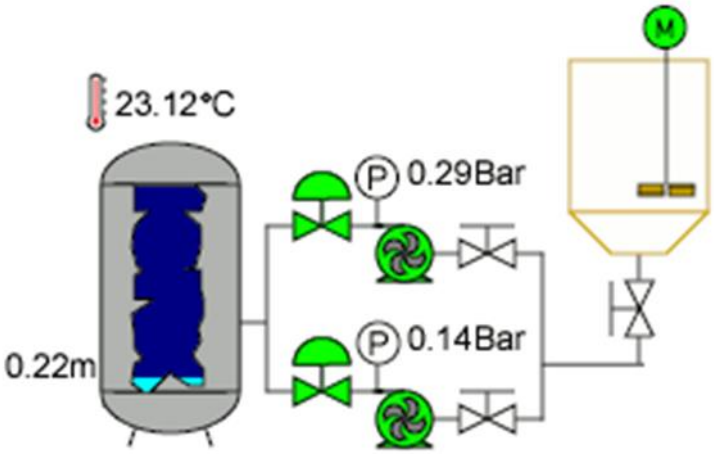
D'autre part, le PLC envoie les données des capteurs et les états des actionneurs à l'HMI via un réseau de communication. Il les interprète et les présente sous forme de graphiques ou d'autres représentations visuelles sur son interface utilisateur.

L'HMI actualise régulièrement les données reçues du PLC pour permettre à l'opérateur de surveiller en temps réel l'état du processus. Le cycle d'automate est généralement plus court que le cycle d'actualisation des données par l'HMI, car même si l'HMI peut actualiser les informations plus rapidement, la réaction de l'opérateur humain pour interpréter, analyser et réagir aux données prend un temps relativement lent.

L'opérateur peut interagir avec l'HMI en utilisant des interfaces tactiles ou des commandes pour effectuer des actions telles que l'activation ou la désactivation d'équipements le changement des paramètres et des consignes de l'algorithme de commande du PLC, etc.

8. Questions

1- Enumérez quatre fonctionnalités principales de la supervision industrielle.
2- Donnez quelques exemples où la supervision industrielle est utilisée en dehors le secteur industriel.
3- Quelle est la différence entre la commande du processus par le PLC et la commande par le système de supervision ?
4- Expliquer la raison pour laquelle les systèmes de supervision sont équipés d'un historien permettant d'archiver les variables et les événements survenus dans l'installation.
5- Qu'est-ce qu'une alarme ?
6- Qu'est-ce qu'un évènement ?
7- Décrivez brièvement comment la coopération entre le PLC et l'HMI permet de superviser un processus industriel.
8- Expliquez pourquoi la fréquence d'actualisation des données reçues par un HMI est faible par rapport au cycle d'automate.
9- Que se passe-t-il si le cycle d'actualisation des données d'un HMI est plus court que celui de l'automate ?
10- Que pourrait-il se produire en cas de non-respect des contraintes de temps réel : a- pour le PLC ? b- pour le système de supervision ?
11- L'interface HMI d'une petite installation industrielle présente le diagramme ci-dessous.
  a- Identifiez les capteurs de l'installation.
  b- Identifiez les actionneurs.
  c- Identifiez trois scénarios anormaux dans lesquels le système de supervision doit générer des alarmes.


23.12°C
P
0.29Bar
P
0.14Bar
0.22m
M

Chapitre 2 Système SCADA

1. Introduction

Les systèmes de supervision industrielle ont connu une évolution importante en lien avec le progrès de l'informatique. Aujourd'hui, leurs fonctionnalités s'étendent bien au-delà de la simple collecte des signaux des capteurs et des actionneurs pour les visualiser dans les tableaux de bord munis de voyants, de boutons, de compteurs, de jauges, etc. Ils sont désormais capables de superviser de loin les installations réparties et utilisent des systèmes informatiques pour traiter, archiver, générer et distribuer un flux d'informations vers toutes les parties prenantes de l'entreprise.

Ce concept de supervision industrielle avancée, interconnectée et qui intègre les nouvelles technologies de communication et de l'information est appelé SCADA (Supervisory Control And Data Acquisition, en français système d'acquisition et de contrôle de données).

2. Système de contrôle et d'acquisition de données (SCADA)

Un système SCADA désigne l'ensemble des composants matériels et logiciels qui permettent la supervision en temps réel des installations à partir d'emplacements distants.

Le terme SCADA est souvent employé pour désigner tout logiciel permettant l'accès à des données distantes d'un processus et permettant de le contrôler.

2.1 Exemple introductif

Un parc d'éolienne peut s'étendre sur plusieurs centaines voire des milliers d'hectares. Un élément crucial pour son fonctionnement est le système SCADA. Ce dernier contribue à maximiser la production d'énergie renouvelable tout en assurant la sécurité et la fiabilité des opérations.

Le système SCADA permet de connecter chaque éolienne, le poste électrique et les stations météorologiques à un ordinateur central. Ce dernier permet de superviser en temps réel le comportement de chaque éolienne ainsi que du parc éolien dans son ensemble depuis une salle de contrôle qui peut être localisée à des centaines de kilomètres du parc lui-même.

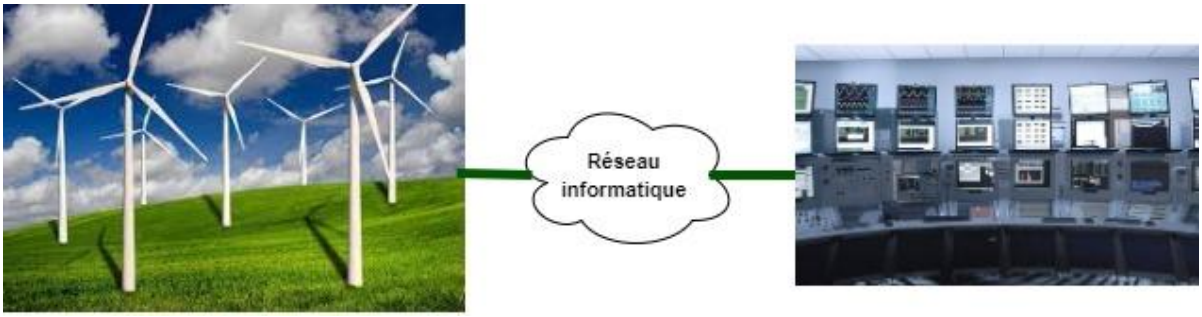


Figure 2.1 Supervision d'un parc d'éoliennes.

Le système SCADA collecte, traite et affiche les données provenant du terrain, telles que :

- l'état opérationnel des éoliennes individuelles (fonctionnelles, en maintenance, en arrêt d'urgence, etc.) ;
- la vitesse du vent et direction pour chaque éolienne ;
- la production d'énergie électrique générée par chaque éolienne et le parc dans son ensemble ;
- tensions, courants et autres paramètres électriques ;
- le statut des équipements de sécurité et de surveillance.

Il permet de modifier les paramètres de fonctionnement de chaque éolienne, de mettre hors service celles qui montrent des signes d'anomalies, de consulter l'état des sous-stations du parc, d'arrêter les éoliennes qui ne sont pas nécessaires, etc.

L'acquisition des données de chaque éolienne se fait par un dispositif électronique (que l'on désigne par le terme RTU). Ce dernier rassemble les signaux provenant des capteurs et les transmet via un réseau informatique à l'ordinateur central. L'existence d'un système de communication fiable est essentielle pour mener à bien cette tâche, qu'il s'agisse d'un réseau filaire ou sans fil.

2.2 Architecture matérielle typique d'un système SCADA

Le fonctionnement d'un système SCADA se fait de la manière suivante :

- Les capteurs et les autres équipements situés sur le terrain sont souvent connectés à des instruments ou modules d'acquisition de données que l'on désigne dans le contexte SCADA par **RTU** (**Remote Terminal Unit : unité terminale déportée**). Ces unités sont responsables de transmettre, via un réseau de communication, les données collectées vers un ordinateur central appelé **MTU (Master Terminal Unit : unité terminale maitresse)** et d'exécuter les commandes envoyées par ce dernier.

- L'MTU reçoit les données des RTU et les traite pour en extraire des informations utiles et générer des alarmes et des rapports. Elle communique avec **les postes opérateur** et leur transmet les données nécessaires pour leur permettre de surveiller le processus et d'envoyer les actions de contrôle aux RTU.

- Les postes opérateurs sont des interfaces utilisateurs qui peuvent être des PC des stations de travail des PC industriels muni d'un ou de plusieurs écrans ou des consoles selon les besoins de l'opération. Ils permettent aux opérateurs de surveiller et de contrôler le processus à distance.

- Un réseau de communication fiable et sécurisé est responsable de la transmission des données entre les RTU et l'MTU. Il utilise des protocoles de communication conçus spécialement pour les systèmes SCADA tel que DNP3 ou des protocoles industriels tel que Modbus.

- Les données importantes, les alarmes et les actions de contrôle effectuées par les opérateurs sont archivées dans une base de données interne dans l'MTU ou dans un serveur externe appelé **historien**. Ces données peuvent être utilisées ultérieurement pour améliorer et optimiser le fonctionnement du processus et pour analyser les causes des défauts et des anomalies qui peuvent survenir.

- Le logiciel SCADA est responsable de toutes les opérations effectuées par l'MTU et les postes opérateur. Il permet de configurer le système, de collecter et de traiter les données, de présenter les données aux opérateurs et de générer des alarmes, etc.

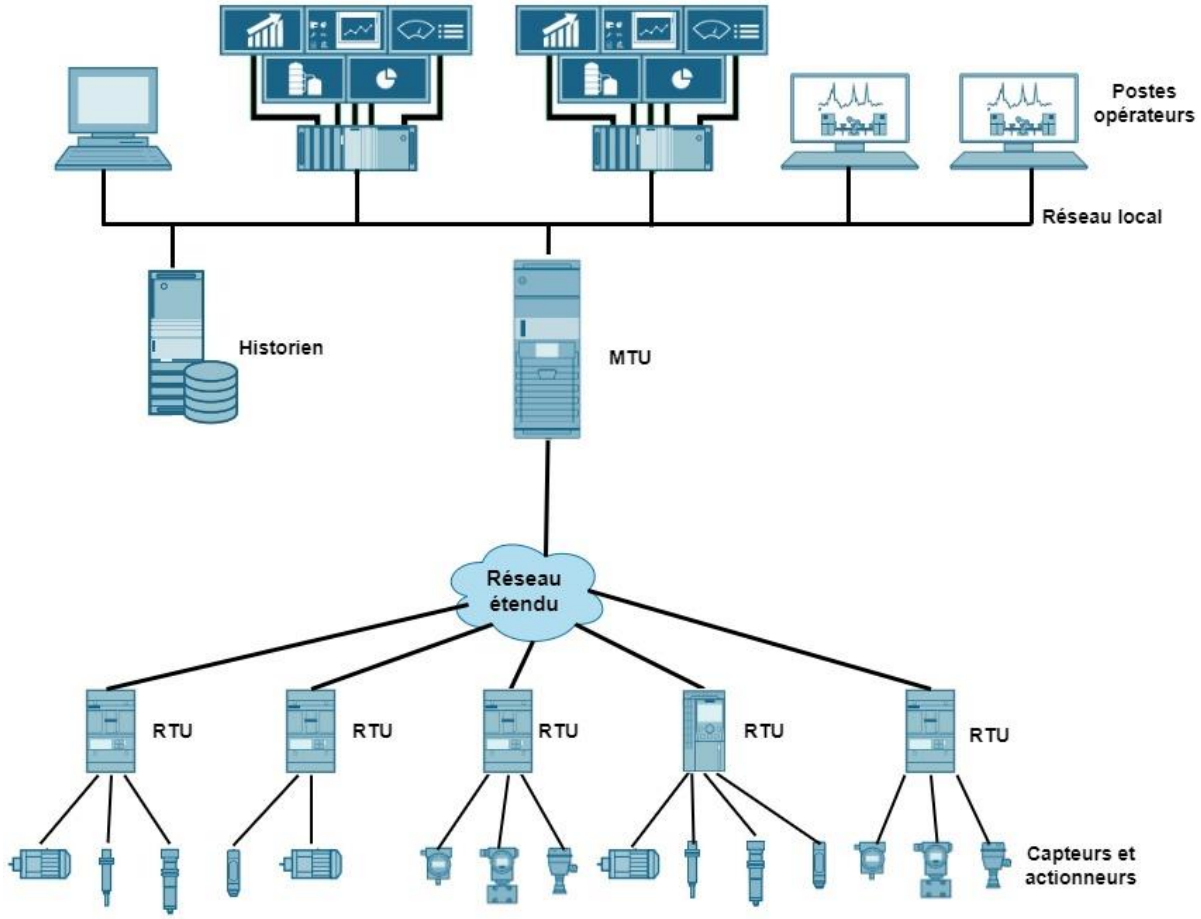


Figure 2.2 Architecture typique d'un système SCADA.

Exemple

La Figure 1 représente une installation industrielle simple où le système SCADA est constitué d'une station SCADA (MTU), de deux contrôleurs programmables (PLC1 et PLC2), d'un réseau de communication reliant ces composants et d'un autre ordinateur connecté à la station SCADA pour servir d'historien, c'est-à-dire une base de données destinée à archiver les données importantes. PLC1 et PLC2 transmettent les informations des capteurs et les états des actionneurs via un réseau informatique à la station SCADA. Cette dernière traite et affiche ces données en temps réel sur son écran sous forme graphique pour faciliter la supervision des équipements sur le terrain (une pompe, une vanne et des capteurs de niveau et de flux).

Le logiciel SCADA est responsable de l'ensemble des fonctions du système SCADA : il assure la gestion de la communication entre la station SCADA et les deux PLC, traite et visualise les données de manière graphique, facilite l'interaction entre les équipements de

terrain et l'opérateur (via les PLC), archive les données importantes dans la base de données, etc.

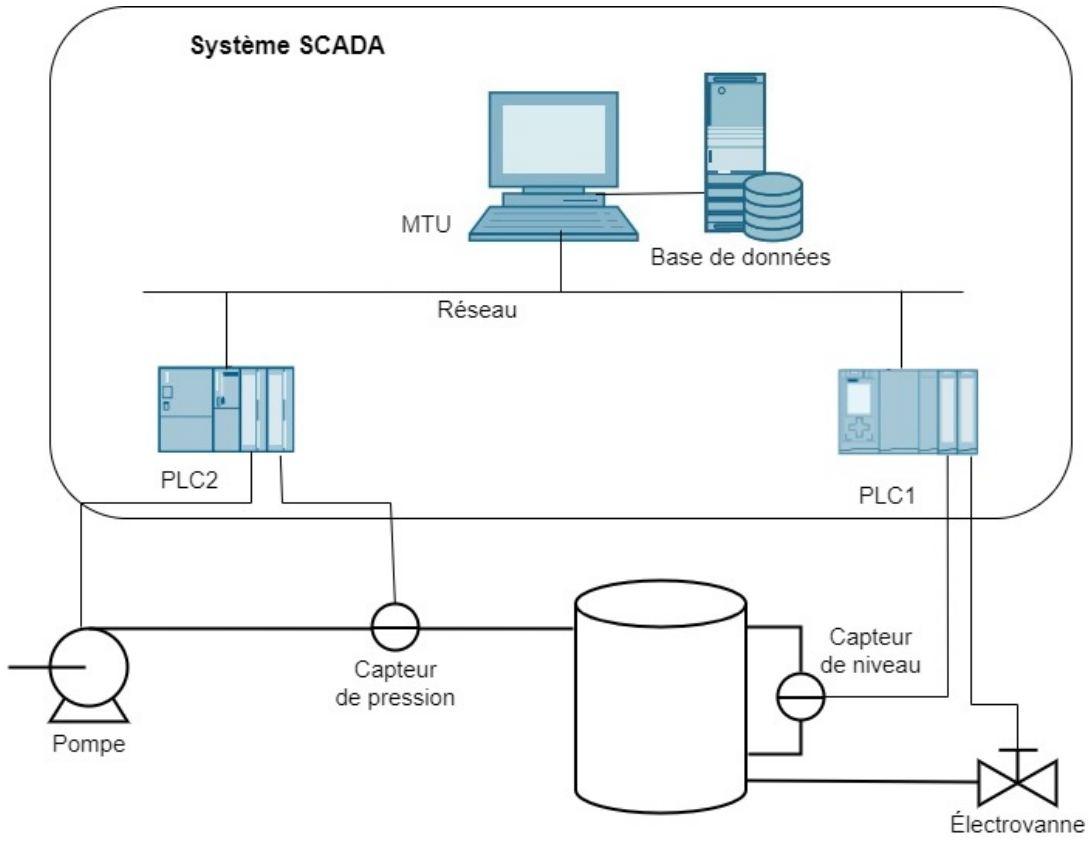


Figure 2.3 Exemple d'un système SCADA simple.

3. Système SCADA vs HMI

Une question cruciale se pose quant à la différence entre la supervision locale utilisant des HMI (sur site) et la supervision par un système SCADA. Avant d'aborder cette question, on souligne tout d'abord que ces deux techniques de supervision sont complémentaires. Pour mieux comprendre ces nuances, voici un résumé des principales différences entre ces deux techniques :

Échelle de supervision : Les systèmes SCADA sont conçus pour superviser des processus à grande échelle, souvent dispersés géographiquement, tandis que les panels HMI sont spécialement conçus pour superviser des opérations à une échelle plus restreinte, localement, directement sur site.

Analyse des données : Les systèmes SCADA offrent une analyse approfondie des données collectées, permettant des évaluations

détaillées, tandis que les panels HMI sont généralement moins dotés en fonctionnalités d'analyse avancée des données.

Archivage des données : Les systèmes SCADA utilisent des serveurs robustes, avec de vastes capacités de stockage ou font appel au cloud pour archiver des données cruciales. En revanche, les HMI, bien qu'offrant des fonctionnalités d'archivage, disposent souvent d'une capacité de stockage limitée et se concentrent sur des données spécifiques.

Connectivité au réseau d'entreprise : Les systèmes SCADA ont pour objectif premier de s'intégrer au niveau de gestion de l'entreprise, cherchant une connexion directe avec les systèmes de gestion globaux. À l'inverse, les panels HMI fonctionnent souvent en tant qu'équipements isolés, déconnectés du réseau d'entreprise.

4. Composants matériels du système SCADA

4.1 Master Terminal Unit (MTU)

L'MTU ou server SCADA est le cerveau du système SCADA. Elle peut être constituée par un ou plusieurs ordinateurs interconnectés. Elle est responsable de diverses fonctionnalités dont voici les plus importantes :

Surveillance et contrôle centralisé : L'MTU communique avec les RTU pour collecter les données des équipements de terrain, tels que des mesures de capteurs, pour les traiter et les envoyer aux postes opérateurs afin de les afficher sous forme graphique conviviale simple à interpréter. De plus, elle permet aux opérateurs d'envoyer des commandes, de configurer les paramètres du système et d'interagir avec les équipements de terrain pour des opérations de maintenance.

Traitement des données : l'UMT applique des algorithmes d'analyse et de traitement sur les données reçues des RTU pour détecter les tendances, les anomalies ou les schémas significatifs dans les opérations des processus surveillés. Elle peut également effectuer des fonctions analytiques avancées telles que le suivi, l'analyse statistique et peut générer des rapports et des graphiques pour aider à la prise de décision.

Gestion des Alarmes : Elle génère les alarmes pour informer les opérateurs des situations anormales et les inciter à prendre des actions correctives.

Sécurité et Authentification : Elle intègre des fonctionnalités de sécurité pour protéger les données sensibles et l'accès au système.

Communication : C'est l'UMT qui établit et gère des liens de communication avec les RTU. Elle intègre différents protocoles et technologies de communication pour assurer un échange efficace des données.

Stockage et Journalisation des Données : L'MTU comprend souvent une base de données pour stocker des données avec horodatage collectées à partir des dispositifs de terrain. Elle enregistre les données à des intervalles prédéfinis pour une analyse ultérieure. L'MTU gère également les politiques de d'accès aux données, garantissant la sécurité des données sensibles.

Génération de rapports : L'MTU génère des rapports sur les évènements, les alarmes et actions des opérateurs. Cela peut aider à améliorer les performances, la productivité et la prise de décision.

4.2 RTU (Remote Terminal Unit : Unité Terminale Déportée)

Une RTU est une unité autonome de contrôle et d'acquisition de données, généralement basée sur un microprocesseur, qui permet de surveiller et contrôler les équipements dans des sites distants depuis une station centrale. Pour collecter les données et en voyer les commandes une RTU typique dispose de modules pour :

- Entrées analogiques et numériques pour relier les capteurs ;
- Sorties analogiques et numériques pour relier les actionneurs ;
- Entrée réseau pour communiquer avec les PLC et d'autres périphériques ;
- Entrées pour compteurs.

Pour communiquer avec l'MTU, une RTU doit disposer d'un port de communication réseau avec et/ou sans fil.

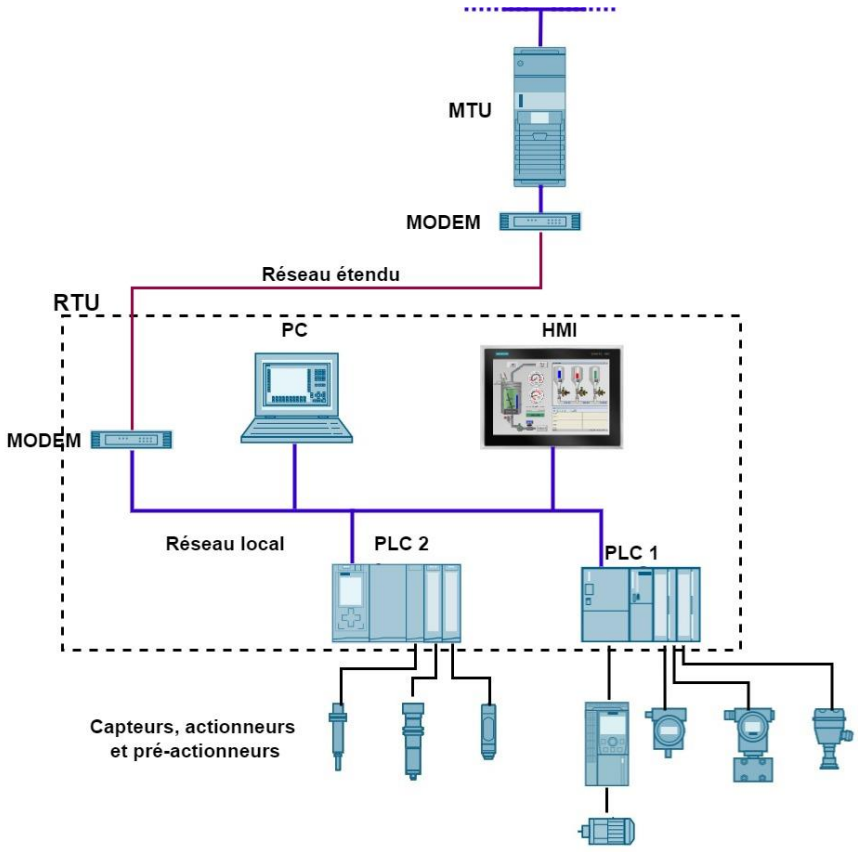


Figure 2.4 Exemple de RTU.

Les RTU modernes disposent généralement de la possibilité d'être configurer et programmer à distance depuis l'MTU. Ils peuvent également être configurer et programmer localement sur site.

Bien que les RTU ont été conçues pour communiquer avec l'MTU, ils ont également la faculté de communiquer entre elles. Une RTU peut également agir comme une station relais pour une autre RTU, qui n'est pas accessible depuis l'MTU.

Une unité qui peut être classifier de RTU peut être composer par plusieurs périphériques, comme montrer dans la Figure 2.4, ou par un seul équipement. Plusieurs dispositifs technologiques peuvent être identifier comme RTU :

Dispositif de télémesure et télécommande : Ce sont des dispositifs spécialisés dans la communication des données. Ils collectent les données directement à partir des capteurs, PLC ou d'autre équipements pour les envoyer l'MTU, et en envoient des commandes du MTU aux équipements de terrain.

IED (Intelligent Electronic Device : dispositif électronique intelligent) : Ce sont des dispositifs à microprocesseur conçu pour des tâches de commande spécifiques. On trouve dans cette catégorie les variateurs de vitesse, les dispositifs de régulation, les disjoncteurs, les relais de protection…etc. Certains des IED ont la capacité de communiquer directement avec l'MTU.

PLC : Certains PLC intègrent des fonctionnalités de communication avancées sous forme de modules d'extension, ce qui a fait disparaître la frontière entre les RTU et les PLC.

Figure 2.2 Quelques exemples d'IED (de gauche à droite : relais de protection, variateur de vitesse et régulateur PID de température).

4.3 Postes opérateur

Les postes opérateur (operator workstations) dans les systèmes SCADA sont les outils clés permettant aux opérateurs de surveiller les données collectées du terrain et de contrôler et interagir avec le processus industriel. Ces stations offrent différentes fonctionnalités dont les plus importantes sont :

Affichage des données en temps réel : Ils permettent de visualiser les données provenant des capteurs et des actionneurs en temps réel. Cela peut inclure des graphiques, des tableaux, des courbes, etc.

Contrôle et commande : Les opérateurs peuvent utiliser les postes opérateurs pour contrôler et commander les processus industriels à distance. Cela peut inclure l'activation/désactivation d'équipements, le réglage des valeurs des paramètres, l'exécution de séquences d'opérations, etc.

Gestion des alarmes et des événements : Les postes opérateurs donnent aux opérateurs une vue d'ensemble des événements et des alarmes en temps réel. Ils peuvent les acquitter, les trier par priorité et prendre les mesures appropriées en cas d'urgence ou de panne.

Les postes opérateurs sont constitués de systèmes informatiques, avec application SCADA, de différents types tels que les PC grand public, des stations de travail, des PC industriels et des interfaces HMI. Ces systèmes utilisent généralement Windows comme système d'exploitation.

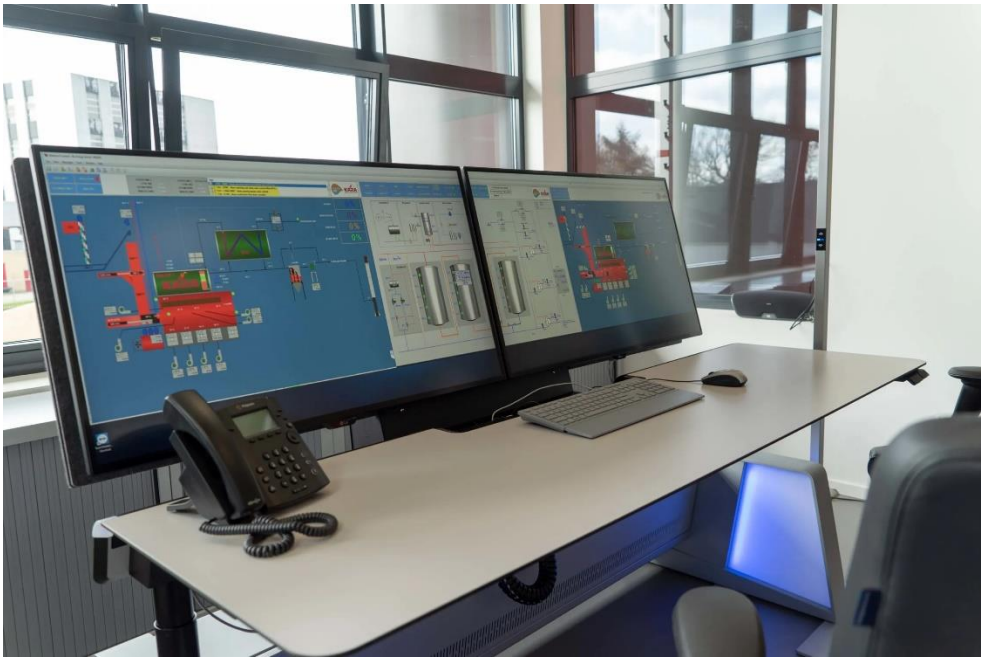


Figure 2.4 Exemple d'un poste opérateur.

4.4 Réseau de communication

Sans un réseau de communication correctement conçu, un système SCADA ne peut pas exister. Tous les aspects de supervision d'archivage externe des données et de visualisation de l'état du processus sur une multitude de postes opérateur reposent entièrement sur le système de communication.

Le but des réseaux de communication au sein d'un système SCADA est de connecter les RTU au MTU et connecter cette dernière aux postes opérateur, historien, imprimantes le réseau de gestion de l'entreprise…etc.

On peut trouver dans les systèmes SCADA tous types de réseaux : LAN (Local Area Network), WAN (Wide Area Network), avec et sans file, réseaux industriels, Ethernet…etc.

5. Générations des systèmes SCADA

Le contrôle des installations industrielles via des calculateurs électroniques est devenu une réalité dans les années 1950. Ensuite, dans les années 1960, la télémétrie est apparue pour offrir encore plus de capacités à la communication et la transmission des données des systèmes automatisés vers des sites de supervision distants. Le terme SCADA est apparue dans les années 1970 pour décrire des systèmes équipés de microprocesseurs utilisés pour la surveillance et le contrôle de processus automatisés. L'industrie pétrolière, production de l'énergie électrique et quelques services publics étaient les premiers principaux utilisateurs de ces nouvelles technologies.

Les systèmes SCADA sont classés en quatre génération selon les technologies employées.

5.1 Première génération (systèmes SCADA monolithiques)

Les anciens systèmes SCADA étaient basés sur un seul mini-ordinateur (ordinateur de grande taille) qui était une unité autonome isolé, car à l'époque les réseaux locaux étaient généralement inexistants. La communication avec les RTU se fait à l'aide de protocoles de communication développés par les fournisseurs d'équipements RTU, et étaient souvent propriétaires.

La fonction cruciale des systèmes de première génération se limite au signalement des processus et à la surveillance des capteurs.

5.2 Deuxième génération (Systèmes SCADA distribués)

Au cours des années 80 et le début des années 90, avec la miniaturisation des ordinateurs, l'avènement des réseaux locaux (LAN) et l'apparition des logiciels HMI, les systèmes SCADA sont devenu des systèmes distribués composés de plusieurs ordinateurs interconnectés. Cela a réduit le cout et la taille du système.

Malheureusement, les protocoles de communications étaient généralement propriétaires, ce qui signifie que les connexions en dehors du matériel du fournisseur du système SCADA n'étaient pas possibles.

5.3 Troisième génération (Systèmes SCADA en réseau)

Plus tard dans les années 90 et 2000, les fabricants des systèmes SCADA ont commencé à mettre en œuvre des architectures de systèmes ouverts avec des protocoles de communication normalisés. Cela a permis d'utiliser dans le même système SCADA des équipements interconnectés issus de différents fabricants, ce qui les a adaptés aux technologies modernes telles que SQL et les applications Web.

Aujourd'hui, ces systèmes SCADA permettent d'accéder aux informations sur les installations en temps réel de n'importe où dans le monde.

5.4 Quatrième génération (Systèmes SCADA internet des objets)

La quatrième génération des systèmes SCADA, qui est encore en phase de développement, utilise l'internet des objets et le cloud computing. Cela minimise énormément le coût d'infrastructure du système et simplifie sa maintenance.

6. Questions

1- C'est quoi un système SCADA ?
2- Pourquoi est-il avantageux d'intégrer le système SCADA avec le niveau de gestion de l'entreprise ?
3- Quelle est la différence entre un système SCADA et HMI ?
4- C'est quoi une RTU ?
5- Quels sont les dispositifs industriels que l'on peut, dans certain cas, qualifier de RTU ?
6- Citez les composants matériels du système SCADA et indiquez le rôle de chacun d'eux.
7- Quelle est l'importance de l'historien dans un système SCADA et comment est-il utilisé pour l'analyse rétrospective des données ?
8- Qu'est-ce que la télémétrie en relation avec les systèmes SCADA ?
9- Décrivez le rôle des postes opérateurs (operator workstation) dans un système SCADA.
10- Quelles sont les quatre générations des système SCADA ?
11- Quelle est la différence principale entre la deuxième génération et la troisième génération ?
12- Quels sont les avantages et les défis de l'intégration des systèmes SCADA avec l'Internet des objets (IoT) ?

Chapitre 3 Protocoles SCADA

1. Introduction

Les RTU sont souvent dispersées sur de vastes sites, parfois dans des environnements éloignés ou difficiles d'accès. Cela présente une série de défis majeurs en termes de communication avec le serveur SCADA (MTU), allant de la fiabilité des liaisons de communication à la sécurité des données lors de leur transmission. Les retards dans la transmission des données sont notamment très fréquents, entraînant une latence entre la collecte des informations par les RTU et leur traitement par la MTU, ce qui a un impact sur la réactivité du système.

Cependant, l'utilisation de protocoles de communication spécialement conçus pour les systèmes SCADA permet de surmonter en grande partie ces problèmes de communication de données. Ces protocoles offrent une collecte précise, sécurisée et en temps réel des données, garantissant ainsi un fonctionnement efficace du système. Ils sont conçus pour résister aux limitations liées à la distance, à l'environnement et aux conditions variables de réseau, assurant ainsi une communication fiable entre les RTU et la MTU. De plus, ces protocoles intègrent des mesures de sécurité avancées pour protéger les données contre les manipulations ou les interceptions non autorisées.

2. Deux grandes familles de Protocoles SCADA

Dans les systèmes SCADA, les protocoles de communication jouent un rôle essentiel dans l'échange de données entre les RTU et la MTU. Deux grandes familles de protocoles sont utilisées : les protocoles industriels et les protocoles développés spécialement pour des systèmes SCADA.

2.1 Protocoles industriels

Les protocoles industriels, tels que Modbus, Profibus, Profinet, BACnet, etc, ont été développés essentiellement pour l'automatisation des processus industriels. Ils permettent de commander et de contrôler des équipements tels que des PLC des capteurs, des actionneurs et d'autres dispositifs dans les lignes de production et de traitement

industriel. Certains de ces protocoles sont également utilisés dans des application SCADA.

Ces protocoles fonctionnent généralement de manière **cyclique**, c-à-d, dans une application SCADA, chaque station RTU **envoie périodiquement toutes ses données** collectées vers la MTU. Cela peut provoquer la congestion de certains réseau SCADA, c-à-d, le flux de données dépasse la capacité maximale du réseau à transporter ces données de manière efficace. Cela entraîne les conséquences suivantes :

- retard dans la réception des données par l'MTU, engendrant une actualisation tardive des données présentées par les interfaces HMI;

- retard dans la détection des évènements et le déclenchement des alarmes, ce qui engendre des prises de mesures correctives tardives par les opérateurs ;

- horodatages imprécis des données enregistrées ;

- horodatages imprécis des alarmes, ce qui compromet la précision temporelle des événements enregistrés, compliquant l'analyse des incidents et la compréhension des séquences d'événements ;

- retards de l'exécution des commandes des opérateurs.

Un autre facteur peut entraver l'application de ces protocoles dans des système SCADA : la plupart de ces protocoles n'intègrent pas des mesures de sécurité pour protéger les données lors de leur transmission et prévenir les attaques.

2.2 Protocoles développés pour SCADA

Des protocoles tels que DNP3 et IEC60870 ont été développés pour répondre aux exigences spécifiques des systèmes SCADA. Ils sont capables de gérer des communications sur des réseaux à large échelle, incluant parfois des connexions sans fil ou même des connexions via des liaisons satellitaires.

Ces protocoles intègrent souvent des fonctionnalités spécifiques, telles que :

- La capacité à intégrer des mesures de sécurité avancées, telles que le cryptage des données. Cela permet de protéger les

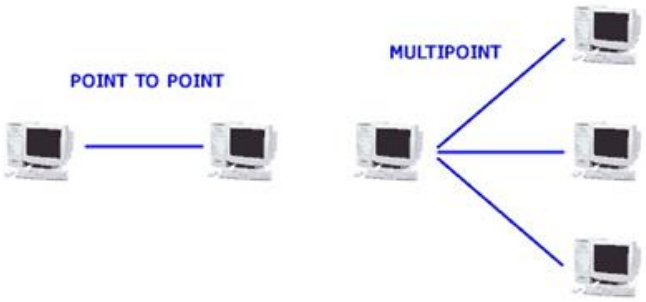
informations sensibles contre tout accès non autorisé, assurant ainsi la confidentialité des données lors de leur transmission.
- La synchronisation du temps[4], garantissant un horodatage précis des événements, ce qui facilite l'analyse rétrospective des données et aide à comprendre les séquences chronologiques des événements.
- La gestion des événements : Chaque RTU est capable de détecter les changements dans les valeurs des variables (signaux des capteurs et d'autres équipements). Il envoie ensuite uniquement les données des variables ayant subi des changements à l'MTU. Cela permet d'éviter la congestion des réseaux à faible débit en limitant le transfert de données aux seules informations pertinentes qui ont réellement subi des changements.
- Les mécanismes de redondance pour garantir la disponibilité des données et la continuité du fonctionnement, même en cas de défaillance d'une partie du réseau.

3. Modes de communication

Dans les systèmes SCADA, il existe différents modes de communication entre les MTU et les RTU, ainsi qu'entre les RTU eux-mêmes.

3.1 Approche interrogation (Maitre-esclave)

Cette approche peut être utilisée pour des systèmes de communication configurés en mode point à point ou multipoint.



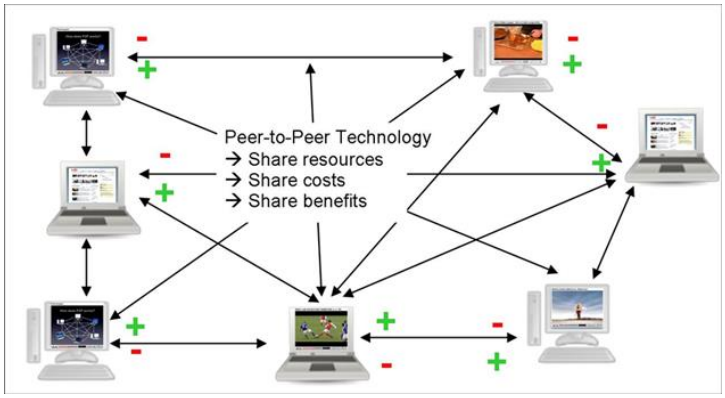
Le maitre contrôle totalement le système de communication puisqu'il gère périodiquement les demandes de transfert des données des

[4] Fait référence à la capacité de synchroniser l'horloge de différents dispositifs dans un système pour qu'ils affichent tous la même référence temporelle. Lorsque les dispositifs sont synchronisés, cela permet de de stocker les événements et les données collectées avec des horodatages précis et uniformes.

différents esclaves. Ces derniers ne peuvent pas prendre l'initiative mais répondent seulement à la demande du maitre.

3.2 Approche paire à pair (peer to peer)

Cette approche est appliquée pour la communication entre RTU et un autre RTU, elle repose sur l'aptitude de chaque nœud du réseau de communiquer avec un autre nœud directement seulement qu'il doit avoir un contrôle d'accès et collision du réseau autrement dit il faut écouter tout d'abord avant d'entamer la communication.



4. Exemples de protocoles SCADA

4.1 Protocole Modbus

Modbus est un protocole de communication ouvert et largement utilisé dans le domaine de l'automatisation industrielle. Il a été développé en 1979 par la société Modicon[5] pour interconnecter les automates programmables.

Le protocole Modbus est basé sur une architecture **maitre-esclave**, où un appareil maître (par exemple, l'MTU) communique avec un ou plusieurs appareils esclaves (par exemple, les RTU). Le maître envoie des requêtes aux esclaves pour lire ou écrire des données, et les esclaves répondent en conséquence.

[5] Modicon est l'entreprise à l'origine de la création de l'automate, désormais acquis par Schneider Electric.

a. Types de Protocole Modbus

Il existe trois principaux types de protocoles Modbus :

Modbus RTU : C'est le type de protocole Modbus le plus couramment utilisé. Il utilise une communication série asynchrone et transmet les données sous forme de trames binaires. Les standards physiques qu'il utilise sont RS-232, RS-422 et RS-485.

Modbus ASCII : Contrairement à Modbus RTU, Modbus ASCII transmet les données sous forme de caractères ASCII, ce qui rend la communication plus lisible pour les humains. Il utilise également une transmission série asynchrone et utilise les protocoles physiques RS-232, RS-422 et RS-485. Actuellement l'utilisation de Modbus ASCII est rare dans l'industrie, car il est plus lent que Modbus RTU en raison de la nécessité de convertir les données en ASCII.

Modbus TCP : C'est une version du protocole Modbus qui utilise le protocole de communication Internet (TCP/IP) pour la transmission de données via Ethernet. Cela permet une communication plus rapide et une intégration facile dans les réseaux Ethernet déjà existants. Modbus TCP est devenu de plus en plus populaire avec l'adoption croissante des réseaux Ethernet dans l'industrie.

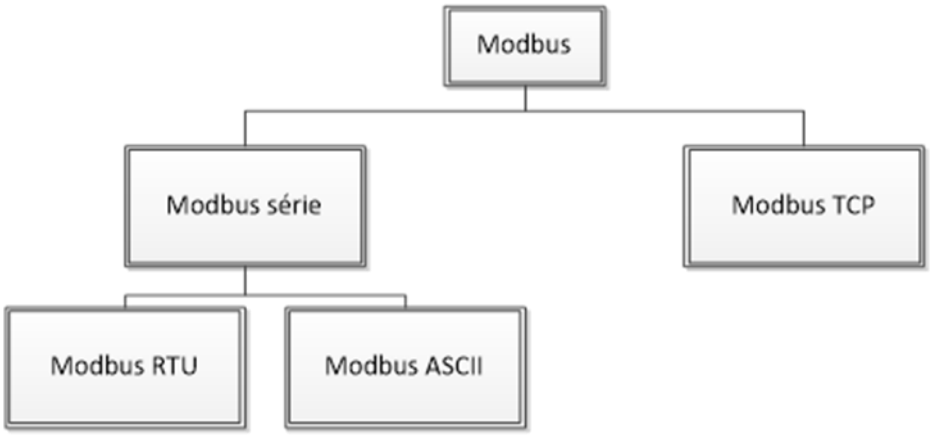


Figure 3.1 Types du protocole Modbus.

b. Principe de fonctionnement

Le réseau du protocole Modbus est organisé en une configuration maître-esclave. Le maître est le nœud principal qui initie les échanges de données avec les esclaves. Le maître a la capacité de communiquer individuellement avec chaque esclave ou d'envoyer des messages de diffusion générale qui sont destinés à tous les esclaves du réseau.

Lorsqu'une requête est adressée individuellement à un esclave, celui-ci renvoie une réponse correspondante à la requête. Cependant, les requêtes de diffusion générale ne nécessitent pas de réponses spécifiques. Il est important de souligner que la communication directe entre les esclaves n'est pas réalisable.

Sur la ligne de communication, un seul équipement est autorisé à émettre à la fois. C'est le rôle du maître de gérer les échanges et d'initier les communications. Il interroge les esclaves les uns après les autres, en envoyant des requêtes individuelles. Aucun esclave ne peut envoyer de message à moins d'être sollicité par le maître.

Dans le cas où un échange de données est incorrect ou ne donne pas de réponse dans un délai spécifié, le maître répète la question ou considère l'esclave interrogé comme absent. Lorsqu'un esclave ne comprend pas un message, il envoie une réponse d'exception au maître pour le notifier. Le maître peut alors décider de réitérer la requête ou de passer à une autre instruction.

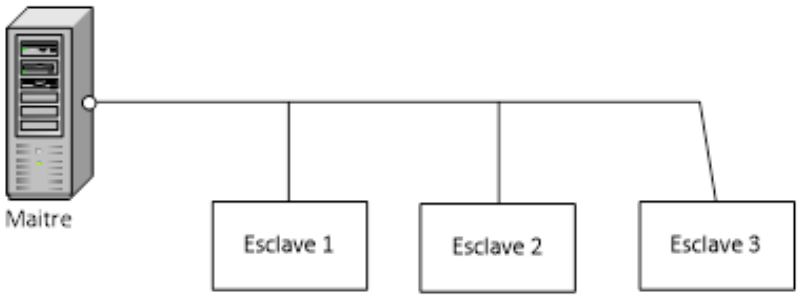


Figure 3.2 Topologie utilisée par le Modbus série.

Il est important de noter que le Modbus en mode série se limite à un seul maitre actif, contrairement au Modbus TCP qui peut prendre en charge plusieurs maîtres simultanément. Cela signifie que plusieurs clients peuvent communiquer avec plusieurs serveurs Modbus TCP.

c. Table Modbus

La table Modbus (appelée également mémoire Modbus et table des données) est une structure de données utilisée dans le protocole Modbus pour stocker et échanger les données entre le maitre et les esclaves.

Les esclaves dans le protocole MODBUS utilisent une mémoire de données qui est organisée en quatre zones de données accessibles en lecture et/ou en écriture par le maître. Ces zones de données correspondent aux différents types de connexions possible avec ces périphériques.

1- Les "Coils" (ou bobines) : Cette zone se trouve dans la plage d'adresses allant de 00001 à 09999 et utilise une structure organisée en bits. Les coils contiennent les valeurs actuelles des sorties discrètes, également appelées signaux de sorties TOR (tout ou rien). Ces valeurs sont utilisées pour commander des actionneurs TOR tels que des relais, des vannes ou des moteurs TOR.
2- Les "Entrées" (ou inputs) : Située dans la plage d'adresses allant de 10001 à 19999, cette zone est également organisée en bits. Les entrées représentent les valeurs actuelles des entrées discrètes provenant de capteurs TOR. Il est important de noter que le maître ne peut pas écrire directement dans cette zone, car elle est destinée à fournir des informations de lecture uniquement.
3- Les "Registres d'Entrée" (ou input registers) : Cette zone est localisée dans la plage d'adresses de 30001 à 39999 et utilise une structure organisée en mots de 16 bits. Les registres d'entrée contiennent les valeurs actuelles des entrées analogiques, telles que des mesures de température, de pression ou de niveau captées par des capteurs analogiques. Le maître peut lire ces valeurs pour surveiller l'état des processus.
4- Les "Holding Registers" (ou registres généraux) : Localisée dans la plage d'adresses de 40001 à 49999, cette zone utilise également une structure organisée en mots de 16 bits. Les holding registers stockent les valeurs actuelles des sorties analogiques du périphérique, telles que les signaux de commande pour des actionneurs analogiques (variateurs de vitesse, vannes proportionnelles, etc.). Le maître peut écrire dans cette zone pour réguler les sorties analogiques.

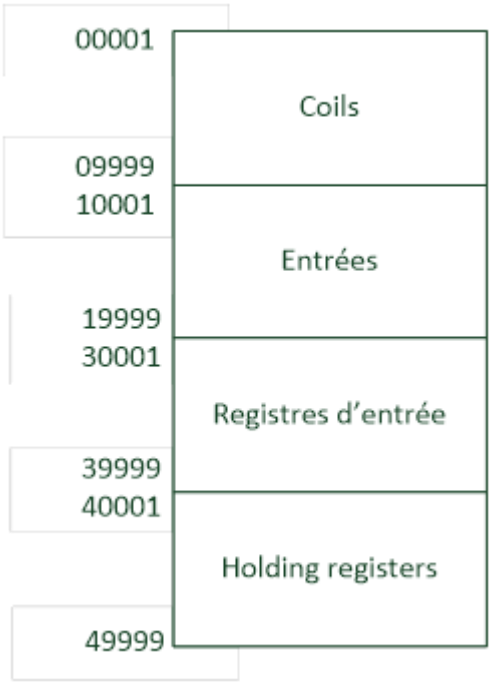


Figure 3.2 Organisation de la mémoire Modbus d'un périphérique esclave.

L'accès à ces bits/registres par le maitre, se fait par l'intermédiaire de fonctions MODBUS standardisées.

Type de variable	**Type**	**Accés**	**Exemple d'utilisation**
Entrée discrète	Bit	Lecture seule	Entrées TOR
Coils	Bit	Lecture/Ecriture	Sortie relais
Registres d'entrée	Mot de 16 bits	Lecture	Entrées analogique
Holding registers	Mot de 16 bits	Lecture/Ecriture	Données modifiables par l'application

Tableau 1 Types des variables Modbus.

d. Format général d'une trame Modbus

Une requête Modbus contient :

- l'adresse de l'esclave à interroger,

- un code fonction, qui indique le type d'action à exécuter (lecture bit, écriture registre,…),
- la plage de bits/registres concernés,
- les données à écrire dans le cas d'une écriture.
- La réponse de l'esclave contient :
- l'adresse de l'esclave qui répond,
- un code fonction, qui indique le type d'action exécutée,
- le nombre d'octets de données compris dans la réponse,
- les données lues dans le cas d'une lecture.

Une trame Modbus est définie de la manière suivante :

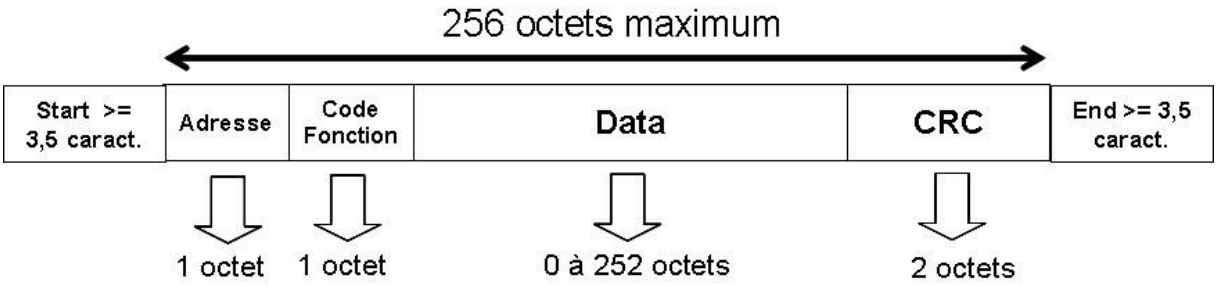


Figure 3.2 Trame Modbus.

- Adresse identifie le destinataire =0 à 247.
- Code fonction définie l'action à réaliser (lecture bit, écriture registre…) =1 à 127.
- Data défini les données qui dépendent du code fonction.
- CRC Contrôle par redondance cyclique pour détecter les erreurs de transmission.

Modbus offre 19 fonctions différentes. Elles se caractérisent par un code fonction sur un octet. Tous les équipements ne supportent pas tous les codes fonction.

Code	Nature de la fonction Modbus
01	Lecture de n bits de sortie consécutifs
02	Lecture de n bits d'entrée consécutifs
03	Lecture de n mots de sortie consécutifs
04	Lecture de n mots d'entrée consécutifs
05	Ecriture de 1 bit de sortie
06	Ecriture de 1 mot de sortie
07	Lecture du status d'exception
08	Accès aux compteurs de diagnostic
09	Téléchargt , télédéchargt et modes de marche
0A	Demande de compte-rendu de fonctionnement
0B	Lecture du compteur d'événements
0C	Lecture des événements de connexion
0D	Téléchargt , télédéchargt et modes de marche
0E	Demande de compte-rendu de fonctionnement
0F	Ecriture de n bits de sortie
10	Ecriture de n mots de sortie
11	Lecture identification
12	Téléchargt , télédéchargt et modes de marche
13	Reset de l'esclave après erreur non recouverte

Tableau 2 Code fonction Modbus.

4.2 Le protocole DNP3

Le protocole DNP3 (Distributed Network Protocol version 3) est un protocole de communication non propriétaire largement utilisé dans les systèmes SCADA, principalement pour la supervision des réseaux électriques et les systèmes de distribution d'eau. Il a été développé par **Westronic** dans les années 1990.

Le DNP3 a été optimisé pour une communication fiable et efficace pour éliminer les problèmes des réseaux SCADA à faible débit en utilisant des messages et des formats de données spéciales.

a. Types de données et messages DNP3

Dans le protocole DNP3, le terme "point" est utilisé pour faire référence à des entrées, des sorties ou des compteurs connectés au système. Les informations échangées via ce protocole peuvent être classées dans les catégories suivantes :

- **Entrée binaire (Binary Input) :** Ces points représentent des signaux TOR (Tout Ou Rien) issues des capteurs ou d’autres équipements de terrains.

- **Sortie binaire (Binary Output) :** Ces points représentent des sorties TOR, généralement utilisées pour commander des actionneurs TOR tels que des relais, des vannes, etc.
- **Entrée analogique (Analog Input) :** Ces points représentent des mesures continues de grandeurs physiques telles que la température, la pression, le niveau, etc. Les données sont généralement transmises sous forme numérique.
- **Sortie analogique (Analog Output) :** Ces points permettent de contrôler des actionneurs analogiques, comme la régulation de la vitesse des moteurs, l'ouverture de vanne proportionnelle, etc.
- **Compteur (Counter) :** Les compteurs sont utilisés pour suivre et enregistrer les événements, par exemple, le nombre de cycles, de pannes, d'opérations, etc. Ils peuvent être utilisés pour des fonctions de surveillance et de déclenchement d'alarmes.
- **Double entrée binaire (Double-bit Binary Input) :** Ces points sont utilisés pour représenter des états d'équipements qui peuvent avoir plus de deux états possibles, par exemple, hors service, en service, en attente, etc.

Pour collecter les données, le maître DNP3 utilise trois types de messages :

- **Interrogation (sans fonctionnalité spécifique) (moins fréquent) :** Ce type de message est utilisé pour demander des informations spécifiques à l'appareil distant, sans fonctionnalités particulières.
- **Interrogation avec rapport d'exception (RBE) (fréquent) :** Dans ce cas, le dispositif distant répond au maître en ne transmettant que les valeurs demandées qui ont subi des changements depuis la dernière interrogation. Cela permet une transmission plus efficace des données.
- **Message du dispositif distant sans scrutin avec rapport d'exception (par demande) :** Ce type de message est généralement utilisé dans le cas où un RTU est configuré pour envoyer au maître des données qui ont atteint des valeurs critiques ou pour déclencher des alarmes, sans attendre l’interrogation régulière du maître.

b. Formats des données

Dans le protocole DNP3, les données sont représentées sous forme d'objets. Par exemple, pour représenter les données d'un capteur TOR, il existe cinq structures de données appelées objets :

- Entrée binaire (Binary Input)

- Entrée binaire avec état (Binary Input with Status)
- Entrée binaire avec changement non temporel (Binary Input with Non-Time-Based Change)
- Entrée binaire avec changement temporel (Binary Input with Time-Based Change)
- Entrée binaire avec changement temporel relatif (Binary Input with Relative Time-Based Change)

Chaque objet est défini par deux valeurs : **le groupe** de l'objet et **la variation** de l'objet. Ces valeurs permettent de spécifier le type et les attributs spécifiques de l'objet dans le protocole DNP3.

En plus de cela, il y a des **objets statiques** et des **objets événementiels** ou **objets évènements**. Les objets statiques représentent des données qui ne changent pas fréquemment, tandis que les évènements sont utilisés pour transmettre des informations spécifiques sur des événements pertinents, tels que des alarmes, des défauts, des changements d'état, etc.

Il convient de noter que ces informations sont spécifiques à l'implémentation du protocole DNP3 et peuvent varier d'une application ou d'un système à l'autre.

Exemple : objets statiques et événementiel pour une entrée binaire.

Statiques :

- Grp#1 Var 01 : Entrée binaire
- Grp#1 Var 02 : Entrée binaire avec état

Évènements :

- Grp#2 Var 01 : Entrée binaire avec changement non temporel
- Grp#2 Var 02 : Entrée binaire avec changement temporel
- Grp#2 Var 02 : Entrée binaire avec changement temporel relatif

Le maître (MTU) indique à l'appareil distant (RTU) l'objet à envoyer en précisant le groupe et la variation dans sa requête. Si l'objet spécifié est de type statique, le RTU envoie la valeur instantanée demandée au maître. Cependant, si l'objet spécifié est de type événement, le RTU envoie au maître l'intégralité de sa file d'attente contenant tous les événements stockés.

Changement de la valeur de la donnée	Horodatage

➔Evènement

Un objet évènement ou évènement tout cours est composé du changement de la valeur de la donnée plus l'horodatage du changement.

Dans le message RBE sans scrutin, Le RTU prend l'initiative et envois les évènements critiques au MTU. Si le Grp# et la Var ne sont pas spécifiés par le MTU, le RTU envois les événements en Grp# et la Var programmés comme étant la forme par défaut de ce type de message.

c. Adressage des données

Dans le protocole DNP3, l'adressage des données à transmettre se fait à l'aide de pointeurs ou d'index, qui sont des valeurs numériques utilisées pour identifier les données.

Par exemple, pour spécifier 8 entrées binaires et 8 entrées analogiques, on peut utiliser les chiffres 0, 1, 2, 3, 4, 5, 6, 7 pour chaque type d'entrée. Chaque chiffre correspond à un pointeur spécifique pour adresser les données.

Le maître (MTU) envoie au dispositif distant (RTU) une combinaison de groupe (Grp#), de variation (Var#) et de pointeur pour spécifier les données à récupérer.

d. Les classes

Les classes des données permettent une utilisation efficace de la bande passante du canal de transmission pour les événements et les rapports par exception en leur attribuant des priorités.

Classe 0 : pour les objets statiques

Correspond à l'état courant d'un bit, valeur courante d'un compteur ou entrée/sortie analogique.

Classe 1,2 et 3 : pour les événements

Changement de l'état d'un bit, franchissement de la valeur seuil par un compteur ou une donnée analogique

Priorités : Classe1 > Classe2 > Classe0

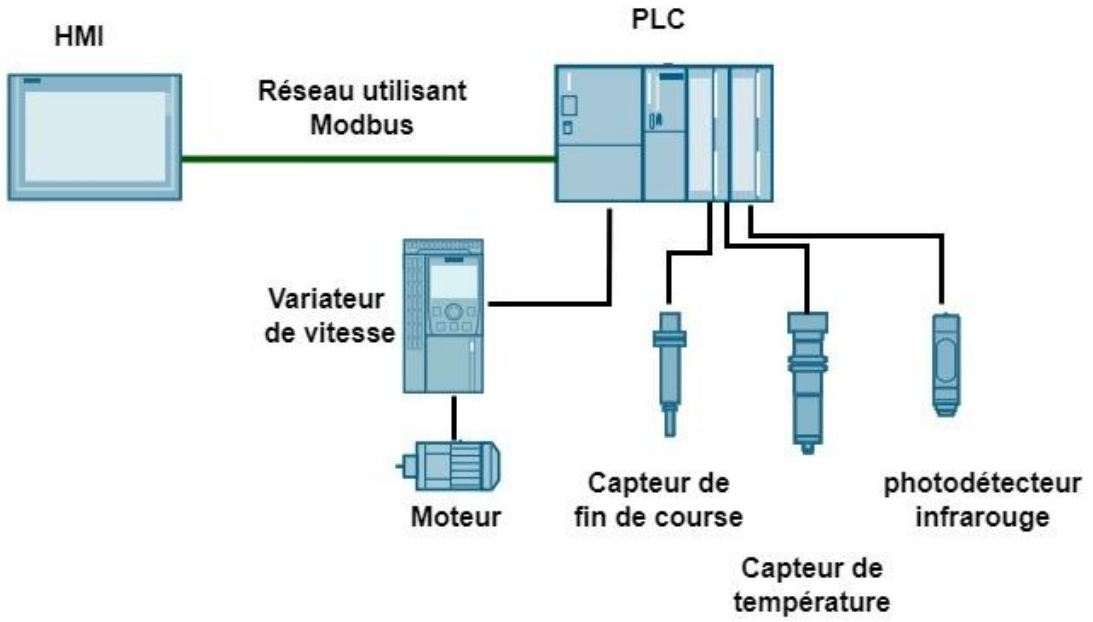
5. Questions

1- Quels sont les différents types du protocole Modbus ?
2- Le protocole Modbus intègre-t-il des mécanismes de cryptage pour sécuriser les données transmises ?
3- Quelle est la différence principale entre Modbus RTU et Modbus TCP ?
4- Dans une communication Modbus entre MTU et RTU, quel est le maitre et quel est l'esclave ?
5- Quels sont les types de données pris en charge par le protocole Modbus, et comment sont-elles représentées ?
6- Citer quelques limites de l'application du protocole Modbus dans dans les systèmes SCADA.
7- Quel est le type de message du protocole DNP3 qui permet de gérer plus efficacement la bande passante du canal de transmission ?
8- Illustrer les concepts d'objets statiques et d'objets événements dans le cadre du protocole DNP3, par des exemples.
9- Comment le DNP3 surmonte-t-il le problème d'horodatage non précis des évènements.
10- Comment l'MTU spécifie-t-elle au RTU les données à récupérer dans le protocole DNP3 ?
11- Comment le protocole DNP3 spécifie les données à transmettre ?
12- Donner un exemple d'adressage de données pour spécifier 5 entrées binaires et 5 entrées analogiques en utilisant des pointeurs dans le protocole DNP3 ?
13- Quelle est l'utilité des classes dans le DNP3 ?

Exercice

Le schéma présenté dans la figure ci-dessous illustre le diagramme d'un système automatisé spécifique.

1- Selon le principe de fonctionnement d'un système supervision, identifiez le maitre et l'esclave Modbus dans ce système.
2- Clarifiez la distinction entre les adresses incluses dans la trame Modbus (de 0 à 247) et les adresses allouées aux différentes zones mémoire Modbus.
3- Associez à chaque composant de l'installation l'adresse une adresse de la table Modbus.


HMI
PLC
Réseau utilisant
Modbus
Variateur
de vitesse
Moteur
Capteur de
fin de course
photodétecteur
infrarouge
Capteur de
température