UNIVERSITE BADJI MOKHTAR ANNABA
FACULTE DE TECHNOLOGIE
DEPARTEMENT D'ELECTRONIQUE
MASTER 2 : AUTOMATIQUE ET INFORMATIQUE INDUSTRIELLE

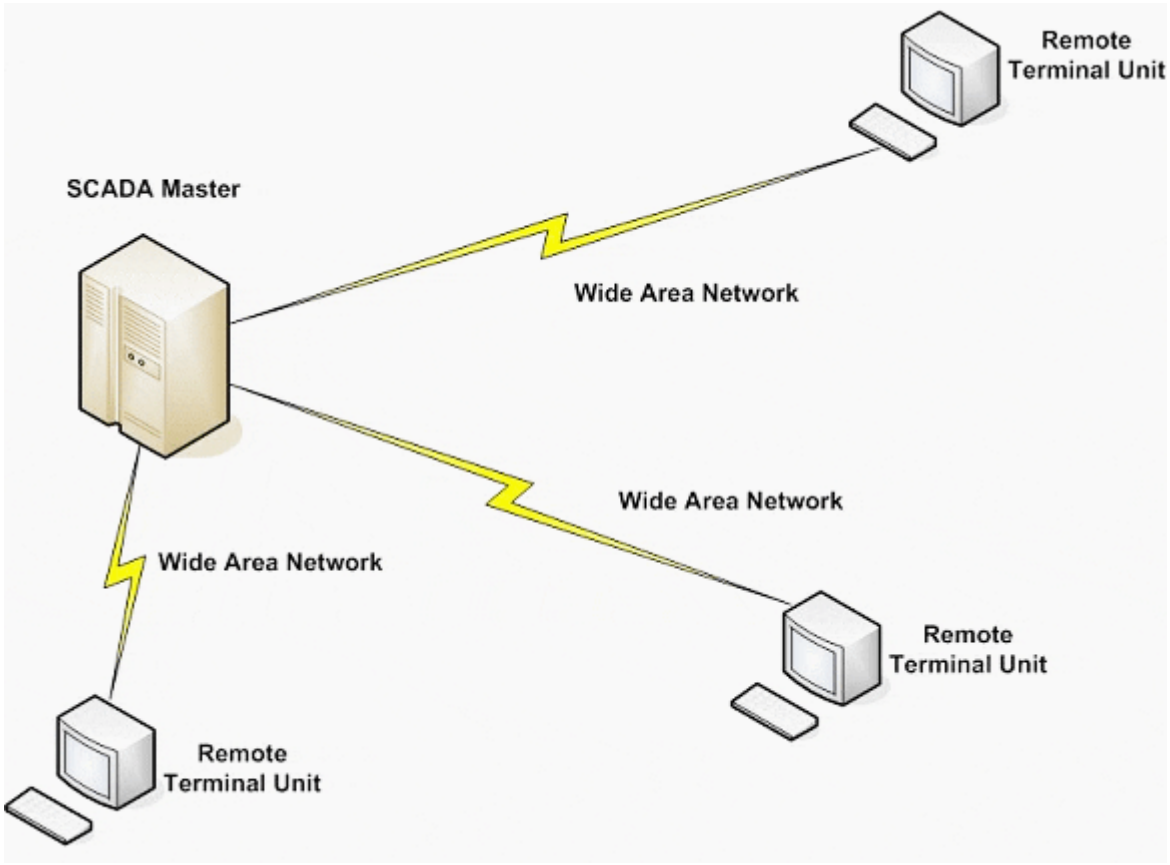
MATIERE : SUPERVISION INDUSTRIELLE

Chapitre 3. Architecture des systèmes SCADA

Architectures SCADA

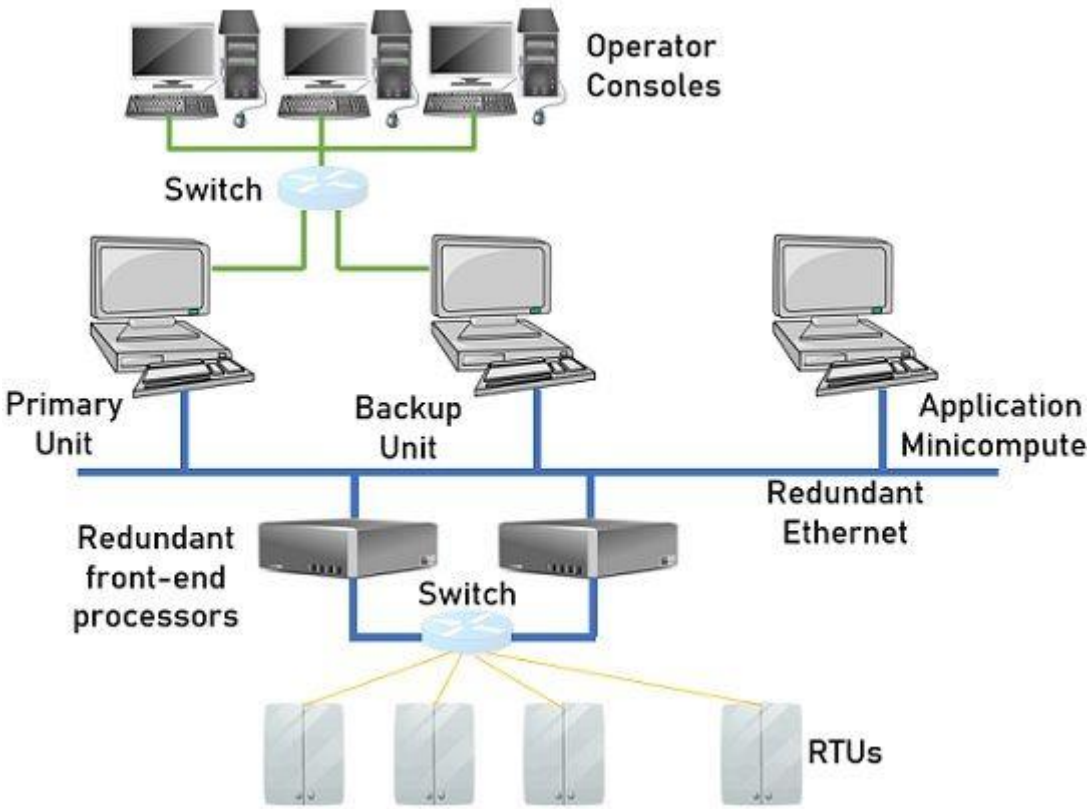
Les architectures des systèmes SCADA se sont développées au fil des ans pour répondre aux besoins croissants de fiabilité, de sécurité et de flexibilité. Les quatre architectures principales sont les suivantes :

- Architecture monolithique : Cette architecture est la plus simple et la plus ancienne. Elle consiste en un seul ordinateur central qui effectue toutes les fonctions du système SCADA, y compris l'acquisition de données, le contrôle et la surveillance.



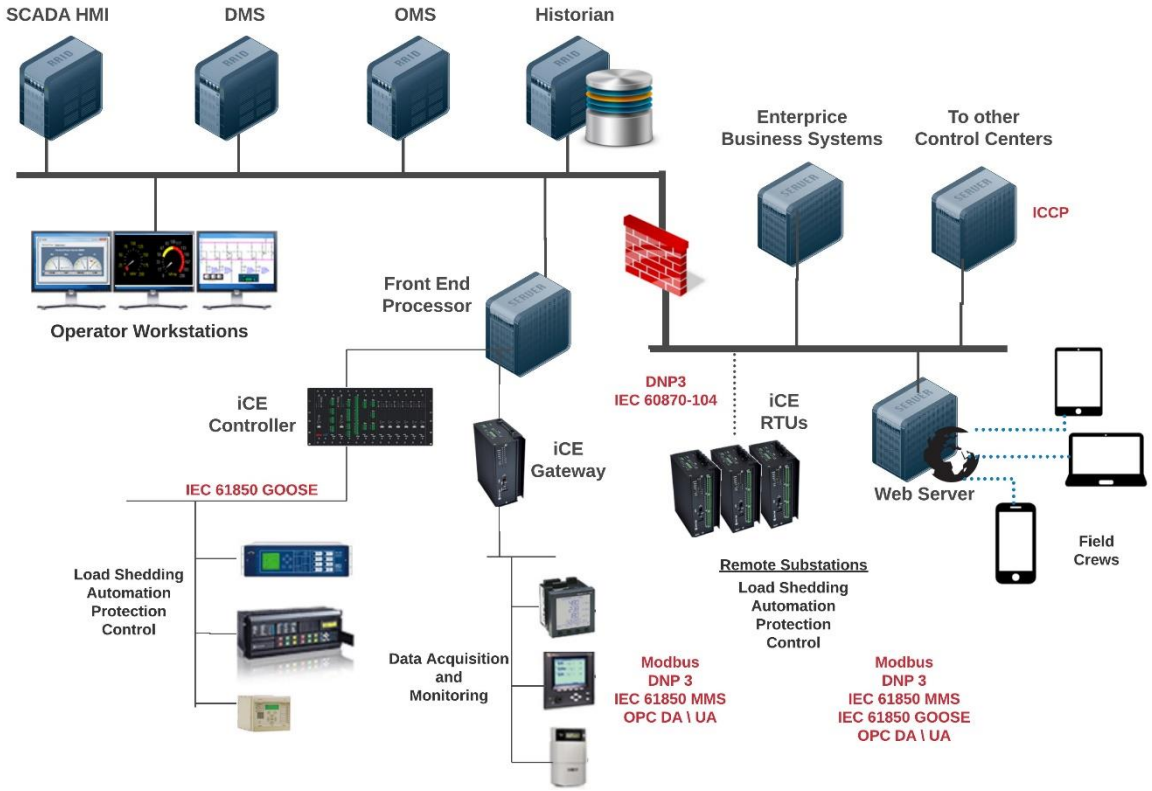
Architecture monolithique des systèmes SCADA

- Architecture distribuée : Cette architecture répartit les fonctions du système SCADA sur plusieurs ordinateurs. Les ordinateurs de terrain, appelés unités terminales à distance (RTU), sont responsables de l'acquisition de données et du contrôle local des équipements. Les ordinateurs centraux, appelés stations de contrôle (SC), sont responsables de la surveillance globale du système et de la prise de décisions.



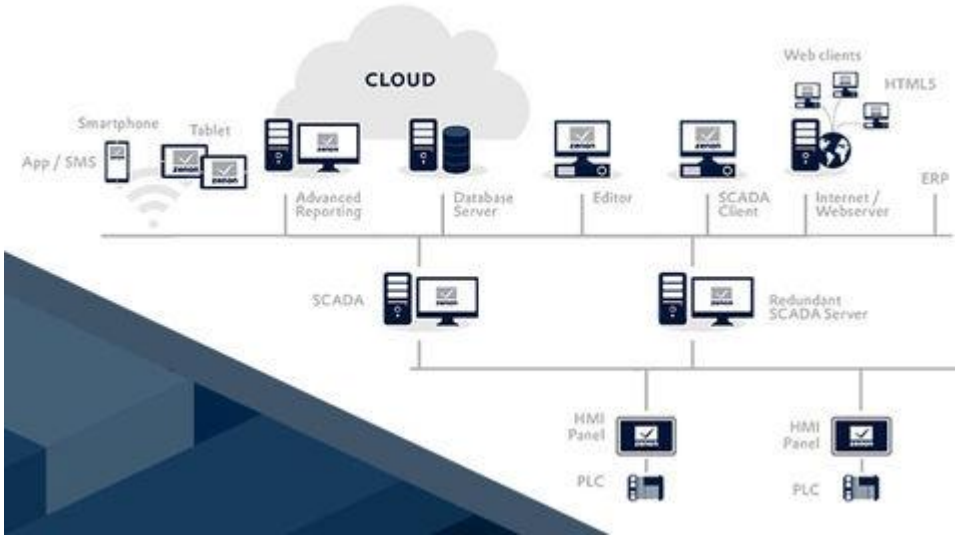
Architecture distribuée des systèmes SCADA

- Architecture en réseau : Cette architecture est une évolution de l'architecture distribuée. Elle utilise des réseaux informatiques pour connecter les ordinateurs de terrain et centraux. Cela permet une communication plus rapide et plus fiable entre les différents composants du système SCADA.



Architecture en réseau des systèmes SCADA

- Architecture IoT : Cette architecture est la plus récente. Elle utilise les technologies de l'Internet des objets (IoT) pour connecter les équipements de terrain au système SCADA. Cela permet une collecte et une analyse de données plus efficaces.



Architecture IoT des systèmes SCADA

Le choix de l'architecture SCADA appropriée dépend de plusieurs facteurs, notamment la taille et la complexité de l'installation, les besoins en sécurité et les contraintes budgétaires.

Les architectures monolithiques sont généralement utilisées pour les petites installations simples. Elles sont faciles à installer et à maintenir, mais elles peuvent être moins fiables et sécurisées que les architectures plus complexes.

Les architectures distribuées sont plus adaptées aux installations de taille moyenne à grande. Elles offrent une meilleure fiabilité et une plus grande flexibilité que les architectures monolithiques, mais elles peuvent être plus complexes à installer et à maintenir.

Les architectures en réseau sont idéales pour les installations de grande taille ou complexes. Elles offrent une excellente fiabilité et une grande flexibilité, mais elles peuvent être coûteuses à mettre en œuvre.

Les architectures IoT sont encore en développement, mais elles offrent un potentiel important pour les installations de toutes tailles. Elles permettent une collecte et une analyse de données plus efficaces, ce qui peut améliorer la performance et la sécurité des systèmes SCADA.

Protocoles SCADA :

Un protocole est un ensemble de règles qui permet à deux ou plusieurs entités d'un réseau de communiquer. L'émetteur et le destinataire de l'information doivent s'entendre sur le protocole utilisé.

Modbus et DNP3 (Distributed Network Protocol) sont deux des protocoles les plus courants utilisés dans les réseaux SCADA. Modbus est open source et 80 à 90 % des appareils d'usine (onduleurs, trackers, etc.) "parlent" le protocole Modbus. DNP3 est un protocole plus récent qui est principalement utilisé pour la communication entre différents appareils de sous-station dans le système SCADA.

MODBUS

Le Modbus est un protocole de type requête-réponse qui permet aux systèmes de supervision et d'acquisition de données (SCADA) d'interagir avec des matériels d'automatisation. Le matériel cible doit envoyer une réponse à chaque requête envoyée.

MODBUS : un protocole de communication maître-esclave

MODBUS est un protocole de communication maître-esclave où un maître peut communiquer avec un ou plusieurs esclaves. Le maître contrôle l'intégralité de la transmission et les appareils connectés sont des esclaves qui envoient des données à la demande du maître.

Fonctionnement de MODBUS :

1. Requête du maître:
   - Lorsque le maître souhaite obtenir des informations des esclaves, il envoie une requête (message) contenant :
   - L'ID de l'esclave : identifie l'esclave spécifique auquel la requête est adressée.
   - Le code de fonction : indique le type d'information demandé.
   - Les données (facultatif) : peuvent être envoyées avec la requête pour effectuer certaines opérations.
   - CRC16 : code de contrôle d'erreur pour garantir l'intégrité des données.
2. Réponse de l'esclave:
   - Les esclaves ne peuvent pas initier le transfert de données. Ils ne peuvent que répondre à la requête du maître.
   - Si la requête est reçue correctement, l'esclave analyse l'ID de l'esclave, le code de fonction et les données (le cas échéant).
   - L'esclave prépare ensuite une réponse contenant les informations demandées, le code de fonction correspondant et le CRC16.
   - L'esclave envoie la réponse au maître.
3. Validation de la réponse:
   - Le maître reçoit la réponse et vérifie le CRC16 pour s'assurer qu'il n'y a pas eu d'erreur de transmission.
   - Si le CRC16 est correct, le maître analyse la réponse et extrait les informations souhaitées.

Avantages de MODBUS :

- Simple et facile à mettre en œuvre: MODBUS utilise une structure de données simple et ne nécessite pas de configuration complexe.
- Ouvert et gratuit: MODBUS est un protocole ouvert et gratuit, ce qui signifie qu'il peut être utilisé par n'importe qui sans avoir à payer de frais de licence.
- Robuste et fiable: MODBUS est un protocole robuste et fiable qui a été utilisé avec succès dans de nombreuses applications industrielles.
- Large gamme de produits compatibles: Un grand nombre de produits industriels prennent en charge le protocole MODBUS, ce qui facilite la construction de systèmes SCADA et d'autres applications industrielles.

Inconvénients de MODBUS :

- Sécurité limitée: MODBUS ne dispose pas de mécanismes de sécurité intégrés, ce qui le rend vulnérable aux attaques.

- Performances limitées: MODBUS n'est pas aussi performant que d'autres protocoles de communication industrielle, tels que Ethernet/IP.
- Scalabilité limitée: MODBUS peut être difficile à mettre à l'échelle pour les grandes installations.

Exemples d'applications de MODBUS :

- Systèmes SCADA: MODBUS est couramment utilisé dans les systèmes SCADA pour surveiller et contrôler les processus industriels.
- Automatisation des bâtiments: MODBUS peut être utilisé pour automatiser divers systèmes dans les bâtiments, tels que l'éclairage, la ventilation et la climatisation.
- Gestion de l'énergie: MODBUS peut être utilisé pour surveiller et contrôler la consommation d'énergie dans les bâtiments et les installations industrielles.

Modbus RTU Frame Format

Start	Address	Function	Data	CRC	End
≥3.5 char	8 bit	8 bit	N * 8 bit	16 bits	≥3.5 char

Modbus ASCII Frame Format

Start	Address	Function	Data	LRC	End
;	2chars	2chars	N * 1 chars	2chars	CR, LF

DNP3 (Distributed Network Protocol)

DNP3, également connu sous le nom de IEEE Std 1815, est une norme complète qui définit les règles selon lesquelles les ordinateurs communiquent entre eux. Lancé en 1993, le protocole DNP3 a spécifiquement défini l'interaction entre les systèmes informatiques utilitaires en vue d'une communication à distance. À cette fin, l'objectif de DNP3 est de fournir un moyen léger de transporter des valeurs de données simples avec un haut degré d'intégrité.

DNP3 définit deux types de terminaux qui communiquent entre eux, à savoir un maître et une Outstation. Ceux-ci se définissent et s'expliquent comme suit :

- **Le maître**
  Le maître est un ordinateur ou un réseau utilisé dans un centre de contrôle. Cet ordinateur est puissant, il stocke toutes les données entrantes provenant de sources extérieures et les traite pour l'affichage.
- **Outstation**
  Également connue sous le nom d'esclave, l'Outstation est un ordinateur utilisé sur le terrain. Ces ordinateurs recueillent des informations provenant de nombreux dispositifs sur le terrain, tels que des capteurs de courant et des transducteurs de tension, et communiquent les données à la station maître. Un esclave DNP3 peut également être un dispositif à distance qui communique directement avec le maître, comme un RTU ou un IED, un débitmètre d'eau ou d'électricité, un onduleur PV ou tout autre type de station contrôlée.

En outre, DNP3 définit les variables de données par type et comportement et les hiérarchise en fonction de si elles représentent ou non un changement par rapport à l'état de référence. Toutes ces valeurs et règles sont définies par le maître au démarrage par le biais d'une requête appelée Integrity Poll, qui invite l'outstation à envoyer la valeur et l'état de tous les points configurés au maître. Après ce processus de configuration, l'outstation transmet de manière sélective des évènements suivant si la donnée a changé depuis la dernière lecture (polling). Ces transmissions se font souvent selon un calendrier cyclique, mais peuvent être spontanées si certains paramètres sont respectés.

Ces règles de communication permettent aux maîtres et esclaves de communiquer en utilisant une bande passante limitée pour transporter des données et des commandes. Cela permet d'envoyer des signaux sur des liaisons série, des liaisons série multipoints, des liaisons radio, des connexions par réseau commuté et sur des réseaux dédiés utilisant le TCP/IP ou UDP. Grâce à l'adaptabilité du système, DNP3 peut répondre à la majorité des cas d'interruption de connexion, créant ainsi un système de communication hautement résilient avec peu d'erreurs ou de défaillances. Cette flexibilité et cette fiabilité ont fait partie intégrante du développement de la norme DNP et de son adoption pour la communication à distance dans l'industrie.

En pratique, DNP3 est principalement utilisé dans l'automatisation des sous-stations électriques. Cependant, DNP3 a également été adopté au sein d'autres services et secteurs, par ex. ceux de la gestion de l'eau et des eaux usées. À mesure que la technologie et l'utilisation du protocole ont évolué, le groupe d'utilisateurs DNP a continué à développer la spécification pour en améliorer l'utilité et maintenir la compatibilité et l'interopérabilité entre les dispositifs mettant en œuvre la spécification originale ou toute fonctionnalité ajoutée.

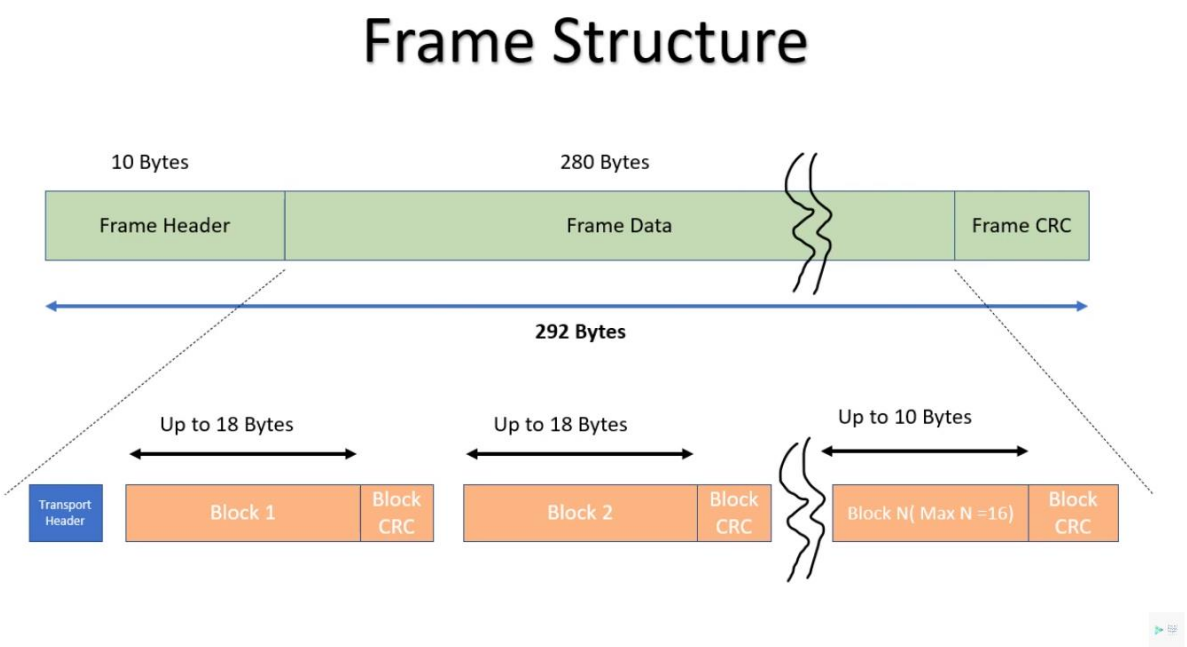
Sécurité et chiffrement DNP3

Si DNP3 est manifestement efficace pour transporter des données d'un bout à l'autre, la protection de ces données est une tout autre question. La cybersécurité présuppose un ensemble de mesures organisationnelles, architecturales et techniques. L'utilisation de DNP3 au sein d'un système rend spécifiquement plus stricte l'exigence de protection des données lors de leurs transmission. En outre, le système doit être protégé contre toute intervention non autorisée. À cette fin, les applications basées sur le DNP3 utilisent souvent une combinaison de cryptage TLS et de procédures d'authentification sécurisée, telles qu'elles sont définies ci-dessous :

- **Chiffrement TLS**
  Le chiffrement TLS protège les systèmes connectés sur TCP/IP en chiffrant les données de sorte que seul le système interne puisse les lire. Le chiffrement TLS est défini par la norme DNP3 et la norme connexe IEC 62351 partie 3, il est donc couramment utilisé comme mesure de sécurité de base pour se prémunir contre la divulgation indésirable d'informations, l'accès non autorisé et la manipulation des messages.

- **Authentification sécurisée**
  Ce mécanisme optionnel exige une authentification lorsque certaines requêtes proviennent du maître ou de l'oustation. Ces fonctions protégées par l'authentification sont souvent des fonctions critiques qui affectent le fonctionnement du système, telles que le réglage des télécommandes, la lecture des messages de confirmation, ou autres. L'authentification est bidirectionnelle et fonctionne selon le principe de question-réponse, de sorte que si une fonction est demandée, le maître doit fournir une réponse appropriée à un message provenant de l'outstation, sur base d'une clé pré-partagée. Cela permet de prévenir toute opération non autorisée ou involontaire. Si l'authentification ne permet pas de chiffrer les données ni de garantir la confidentialité, elle offre une couche de sécurité supplémentaire pour se protéger contre les fonctions potentiellement nuisibles ou les altérations du système.

  Idéalement, les systèmes DNP3 utilisent une combinaison de ces mesures pour garantir à la fois la confidentialité et la sécurité des équipements maîtres et esclaves.



Par rapport au Modbus, le DNP3 est un protocole plus sophistiqué, il a la capacité d'utiliser la fonctionnalité d'un rapport par exception (RBE). Avec la fonctionnalité RBE, seulement un changement de données est signalé au lieu de déclarer toutes les données à chaque fois qu'un dispositif est interrogé. Cette caractéristique du DNP3 permet à des données historiques et événementielles d'être transmises tout en assurant qu'aucune donnée critique ne soit perdue. (La possibilité de signaler l'événement historique et les données ne sont pas disponibles dans le protocole Modbus.)

PYRAMIDE CIM

Le secret des pyramides

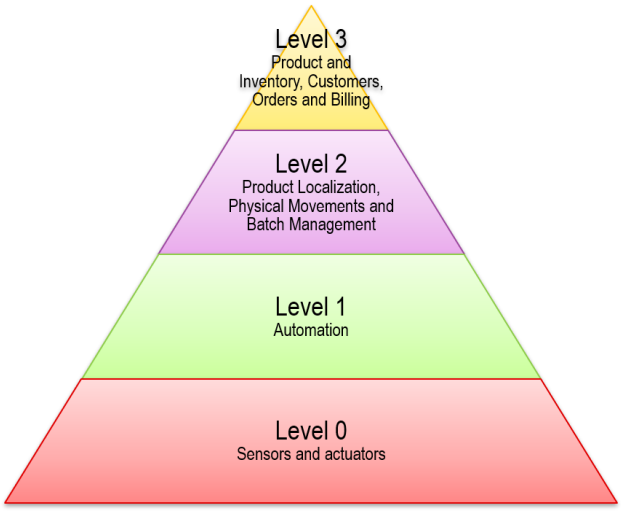
Le Computer Integrated Manufacturing (CIM) est un concept décrivant l'automatisation complète des processus de fabrication. C'est-à-dire que tous les équipements de l'usine fonctionnent sous le contrôle permanent des ordinateurs, automates

programmables et autres systèmes numériques. CIM signifie Computer Integrated Manufacturing fait pour:

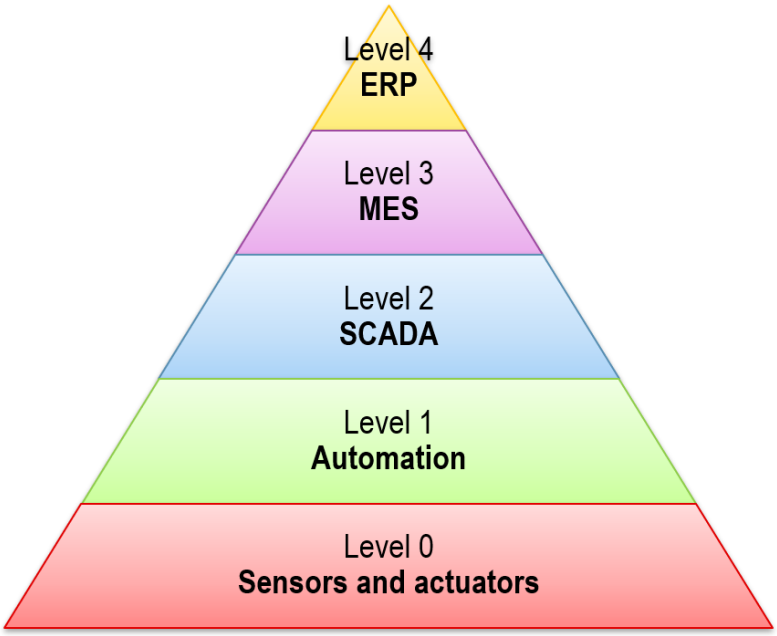
- Assurer une communication entre les mondes de l'informatique et t de l'automatisme

- Augmenter la productivité (fiabilité, pérennité...) des usines de fabrication

La pyramide du CIM est une représentation conceptuelle très en vogue dans le milieu industriel à partir des années 1980. Elle comporte une hiérarchie logique organisée en 4 niveaux correspondant à des niveaux de décision. Plus on s'élève dans cette pyramide, plus le niveau de décision/d'abstraction devient fort, car la visibilité gagne en globalité et les horizons et cycles opérationnels s'allongent. Le diagramme **CIM** d'origine ne mentionne pas le positionnement du **SCADA** (ces logiciels sont embryonnaires au moment où le CIM est mis en place). Il peut être tentant de l'ajouter sous forme d'une couche supplémentaire, et de caractériser plus précisément chacune des couches, ce qui donne la représentation suivante.



Cette représentation pyramidale repose implicitement sur plusieurs hypothèses, même si celles-ci ne sont jamais exprimées très clairement.

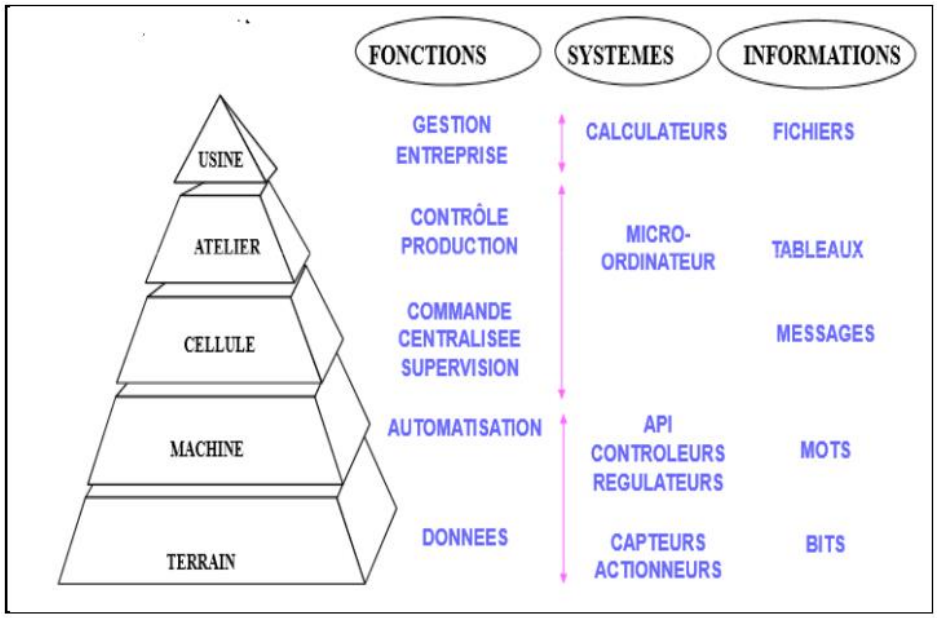


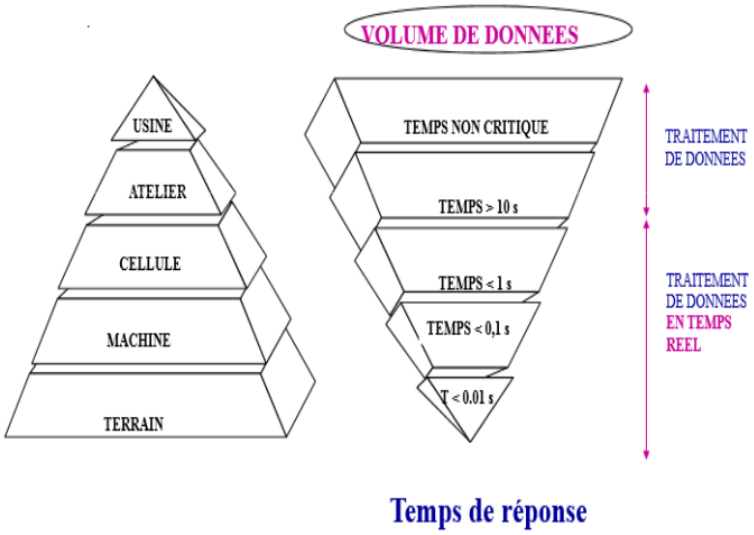
La première est une hiérarchie fonctionnelle, dont l'effet est renforcé par la représentation. Elle suppose que l'on va des fonctions les plus simples (au bas de la pyramide) aux fonctions les plus complexes (en haut de la pyramide). La seconde hypothèse - c'est sans doute la plus importante - est que *chaque bloc fonctionnel ne peut communiquer qu'avec celui qui est juste au dessus et celui qui est juste au dessous*. Cette dernière hypothèse est à la fois dictée historiquement par une analogie avec les structures managériales traditionnelles et l'existence de types de communication matérielle très différents àchaque niveau : dans les années quatre-vingt, les réseaux de capteurs, les réseaux automates, et les réseaux informatiques étaient de types très différents, incapables de cohabiter sur le même support physique.

MES (Manufacturing Execution System) est un système informatique qui connecte, surveille et contrôle des systèmes de fabrication et flux de données complexes au niveau des ateliers. L'objectif principal d'un MES consiste à garantir l'exécution effective des opérations de fabrication et à améliorer le rendement de la production.

Pour contribuer à cet objectif, un MES suit et collecte des données en temps réel précises tout au long du cycle de vie de production, de l'ordre de fabrication à la livraison du produit dans le cas de produits finis.

Pour chaque produit, le MES collecte des données relatives à la généalogie, aux performances, à la traçabilité, à la gestion des matériaux, à l'encours, ainsi qu'aux autres activités de l'usine au fur et à mesure de leur déroulement. A leur tour, ces données permettent aux décideurs d'appréhender les paramètres en vigueur dans les ateliers et d'optimiser le processus de production.
ERP L'**ERP** (**Enterprise Resource Planning**) est utilisé sur les sites de production pour gérer les ressources et apporte son soutien au responsable de production en l'aidant sur l'aspect organisationnel (type et quantité de matériau nécessaire à la production d'une commande, délais prévisionnels en fonction des stocks et de l'approvisionnement des fournisseurs...).





Temps de réponse

- **Niveau 0 ou "Niveau de TERRAIN"**

  Inclut les dispositifs physiques présents dans l'usine, comme les actionneurs et les capteurs. Ces dispositifs recueillent des données sur le processus de production et contrôlent les actions physiques en temps réel.

- **Niveau 1 ou "Niveau de CONTRÔLE"**

  Il comprend les dispositifs logiques comme les ordinateurs, les API, PID, etc. Comme son nom l'indique, il a pour rôle de contrôler et superviser les opérations réalisées au niveau du terrain, en traitant les données des capteurs et en prenant des décisions pour contrôler les actions.

- **Niveau 2 ou "Niveau de SUPERVISION"**

  Il correspond aux systèmes de supervision, contrôle et acquisition de données (SCADA). Il est en charge de superviser et contrôler différents processus et zones d'une installation industrielle. Des interfaces graphiques sont utilisées pour superviser l'état du processus, recevoir des alarmes et prendre des décisions importantes.

- **Niveau 3 ou "Niveau de PLANIFICATION"**

  Au niveau supérieur se trouvent les systèmes d'exécution de la production (MES). Il est centré sur la planification de toute l'installation industrielle. Les données recueillies dans les niveaux précédents sont utilisées pour la prise de décisions stratégiques, comme la programmation de la production ou la maintenance préventive.

- **Niveau 4 ou "Niveau de GESTION"**

  Au sommet de la pyramide, se trouvent les systèmes de gestion intégrale de l'entreprise (ERP). Il est centré sur la prise de décisions qui relèvent du niveau corporatif pour la gestion globale de l'entreprise.