PROJET MASTER 2

RAPPORT D'ACTIVITE

Contrôle Commande et Supervision

Son évolution, ses enjeux, les nouvelles tendances et nouveaux services.

Février 2007

Encadrant :

Frédéric KRATZ

frederic.kratz@ensi-bourges.fr

Professeur des Universités

Laboratoire Vision Robotique

Responsable de l'Equipe

Automatique du LVR

Responsable des Relations avec

les Entreprises / ENSIB

Co-Encadrant :

Manuel AVILA

manuel.avila@univ-orleans.fr

Maître de Conférence

Laboratoire Vision Robotique

Responsable de la Licence

Professionnelle Automatismes

Réseaux Internet

Réalisation :

Pascal VRIGNAT

pascal.vrignat@univ-orleans.fr

http://pascal.ajoux.free.fr

Enseignant

IUT de Châteauroux

2 AV. F. MITTERAND

36000 CHATEAUROUX

REMERCIEMENTS

Je tiens tout d'abord à remercier M' Frédéric KRATZ d'avoir accepté d'encadrer ce sujet et de m'avoir permis de présenter mon travail. Je remercie ensuite M' Manuel AVILA pour ses conseils de recherche et de rédaction. Je remercie également M' Florent DUCULTY et M' Stéphane BEGOT enseignants chercheurs du LVR pour leurs conseils. Je remercie M' Bernard ROBLES (ingénieur informatique IUT de Châteauroux) pour m'avoir ouvert des ports de communication. Je remercie M' Laurent MISMACQUE (Chef de la branche Education nationale, Enseignement Supérieur et Recherche) pour les informations qu'il a pu me fournir. J'aimerais aussi avoir, dans ces mots de remerciements, une pensée amicale pour M' Eddy BAJIC Professeur d'Université à Henri Poincaré, Nancy CRAN – UMR 7039 avec qui j'ai échangé des informations et points de vue dans ce domaine depuis plus de dix ans.

SOMMAIRE DU RAPPORT D'ACTIVITE

TABLE DES FIGURES

1 Le sujet

Le dernier salon international en automation (SCS Automation & Control - Paris- Nord Villepinte – 2006) a mis en évidence plusieurs orientations technologiques au service des besoins actuels des entreprises. Les API (Automate Programmable Industriel) connaissent des améliorations de tout ordre que ce soit les fonctionnalités, la capacité à communiquer, l'ergonomie, la facilité à étendre les systèmes, les logiciels, les outils pour l'implémentation. Une des tendances majeures est une intégration croissante de la technologie *«motion »* au sein des systèmes de contrôle. On peut l'assimiler à une convergence des technologies en général, puisque l'intégration fonctionnelle horizontale est devenue légion dans le domaine de l'automation. Les utilisateurs plébiscitent les solutions jouissant d'une telle architecture, acceptant de moins en moins les discontinuités entre les systèmes. L'utilisation d'Ethernet TCP/IP en est la nette illustration. Par ailleurs, la relation entre l'API et l'Interface Homme Machine (IHM) s'intensifie. En substance, l'IHM, le contrôle « motion » et l'API ont de plus en plus de fonctions en commun ; illustrant ainsi le concept de convergence.

Aujourd'hui, de plus en plus de systèmes complexes (nouvelles machines industrielles, logiciels, imprimantes et photocopieurs, matériel militaire ou de santé...) peuvent être connectés à internet. Ceci permet d'envisager de les maintenir à distance sans nécessairement avoir de personnel qualifié disponible sur le site à surveiller ou à réparer. Les interventions peuvent donc être plus rapides et les priorités sont gérées à un niveau plus global que dans le passé. Le personnel qualifié peut apporter une aide effective depuis pratiquement n'importe quel endroit. Les coûts globaux de déplacement de personnel qualifié sont donc diminués. La e-maintenance peut se montrer décisive en matière de coûts et de qualité.

D'autres avantages découlent directement des travaux effectués dans les domaines concernés par la e-maintenance. En effet, la maintenance au sein d'environnements dangereux est grandement simplifiée par l'utilisation de télé-surveillance, télé-diagnostic et même de télé-opération à l'aide de robots. Ces environnements dangereux concernent un grand nombre de domaines tels que la maintenance des réacteurs nucléaires, de satellites en orbite, ou de robots explorateurs de planètes ou de fonds marins.

Ce rapport d'activité essayera de faire le point sur ces nouveaux aspects techniques et humains.

<u>Ce sujet évoquera :</u>

- l'évolution des besoins, nouvelles tendances,
- les enjeux et challenges,
- le respect des réglementations.

- l'ouverture du SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) vers les MES (**M**anufacturing **E**xecution **S**ystem),
- Solutions innovantes de services :
    - IHM distribuées,
    - station locale avec accès centralisé,
    - échange d'informations entre IHM,
    - accès global aux données usine.
- Service & Diagnostic à travers le Web :
    - diagnostic à distance et Down-upload possible,
    - sécurisation des communications.

<u>Moyens matériels et logiciels de départ (application pratique) :</u>

Cette plate-forme décrite (Voir figures 1 et 2) permettra sur ce « cas d'école » d'évoquer l'ensemble de ces problématiques liées à ces nouvelles technologies.

L'architecture réseaux est présentée ci-après.

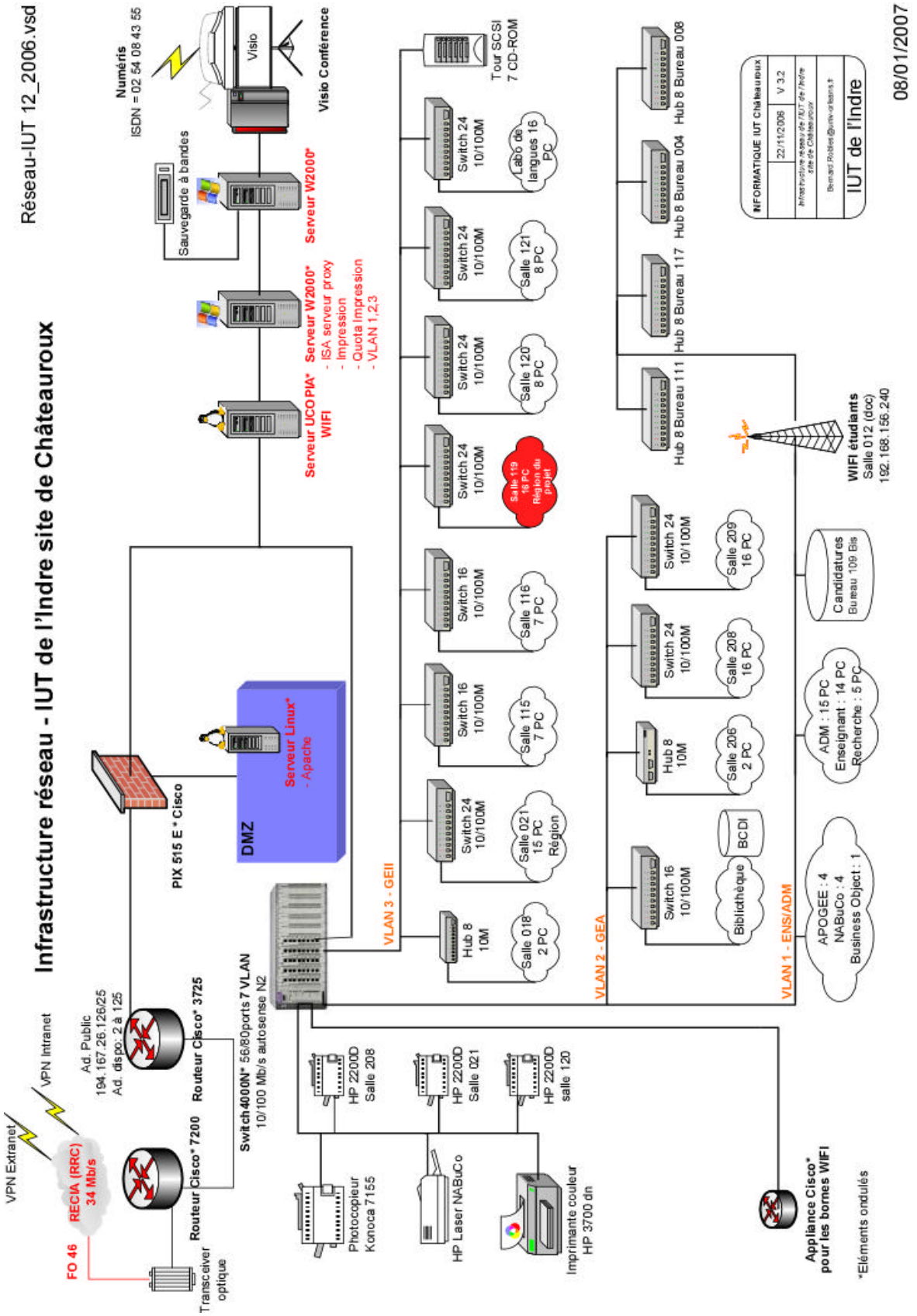


Figure 1 : Architecture du réseau informatique IUT de Châteauroux

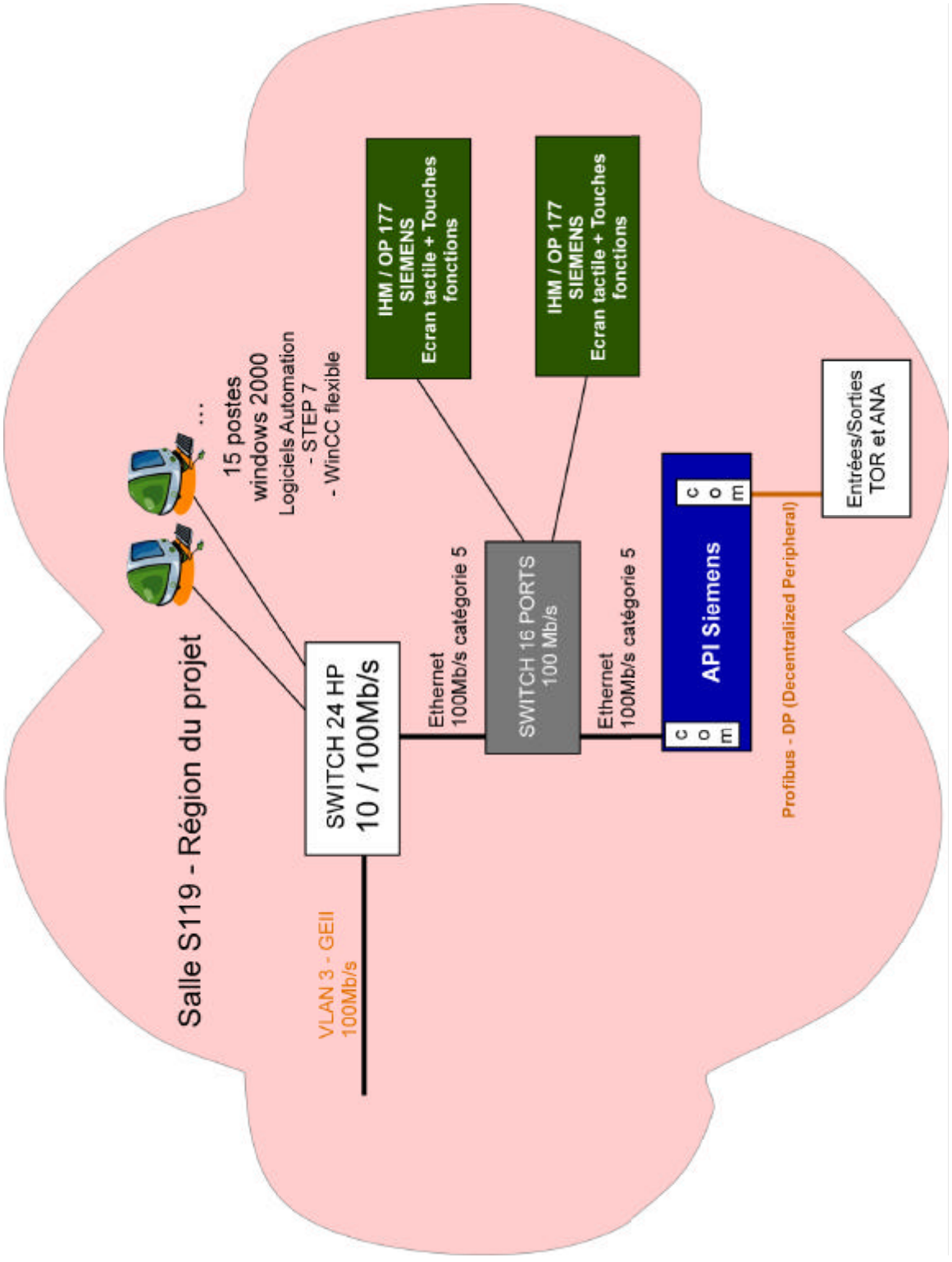


Figure 2 : Région du projet

2 Préambule

Dans le mot **IHM**, il y a **H**omme, et c'est pour ne pas y avoir pensé suffisamment tôt que certaines réalisations se sont soldées par des fiascos.

Le réseau ANACT ***pour l'amélioration des conditions de travail*** a pour vocation d'améliorer à la fois la situation des salariés et l'efficacité des entreprises, et de favoriser l'appropriation des méthodes correspondantes par tous les acteurs concernés. ***Il aide les entreprises et les autres organisations à développer des projets innovants touchant au travail***. Ce réseau encourage les entreprises à placer le travail au même niveau que les autres déterminants économiques (produits, marchés, technologies...) et privilégie la participation de tous les acteurs de l'entreprise (direction, encadrement, salariés) aux projets de développement. Les objectifs de l'ANACT sont, entre autres également, d'améliorer les conditions de travail et le niveau de vie, de promouvoir une série de principes relatifs au travail et d'encourager la coopération pour favoriser l'innovation et l'amélioration des niveaux de productivité et de qualité. L'Accord mise sur diverses formes de coopération, notamment l'échange d'informations, l'assistance technique et la consultation, pour atteindre ses objectifs.

Son programme d'activité est défini dans un Contrat de Progrès signé avec l'Etat (le 20 Janvier 2004 François FILLON, ministre des Affaires Sociales, du Travail et de la Solidarité et Alain LAMBERT, ministre du budget, ont cosigné avec Rémi DESCOSSE, président du conseil d'administration de l'ANACT, et Henri ROUILLEAULT, directeur général, le troisième contrat de progrès du réseau ANACT).

Certaines entreprises à hauts risques auxquelles incombent d'importantes responsabilités en matière de sûreté bien qu'elles accordent un rôle important à l'homme pour la sécurité «***l'opérateur en salle de commande est souvent considéré comme la « dernière barrière de sécurité »***), se méfient en général des interactions susceptibles d'intervenir entre l'Homme et le système technique, et attendent beaucoup de la technologie comme des procédures.

Le travail théorique des opérateurs est alors défini par rapport à des installations conçues avec un degré d'automatisation parfois élevé, et selon une vision des automatismes qui cherche à minimiser l'erreur dans une perspective de fiabilité et de sûreté.

L'activité est donc étroitement encadrée par un système de règles mis en place pour répondre aux exigences de sûreté. La conduite sur console ou sur tableau, les interventions locales, les rondes programmées, les phases transitoires, le recours à la maintenance, la transmission d'informations . . . Tout tend à être formalisé par des procédures précises.

Les équipes de conduite, y compris les agents de quart, ont ainsi pour mission de faire remonter les informations relatives aux défaillances, aux pannes et autres défauts afin de les traiter dans le cadre de retour d'expérience (REX). Cette *Fondation pour une Culture de Sécurité Industrielle* a lancé en 2005 un programme de recherche intitulé *Facteurs socio-culturels de réussite du retour d'expérience.* Les projets financés dans le cadre de ce programme ont pour vocation de mieux comprendre les activités de retour d'expérience et leurs apports en matière de sécurité industrielle.

Les exploitants l'admettent aujourd'hui volontiers : l'Homme conserve un rôle déterminant dans le bon fonctionnement et les performances effectives des systèmes automatisés.

En matière de performance, la stratégie de management industriel va donc dans le sens d'un élargissement de l'implication des Opérateurs dans le travail de conduite. Leur nécessaire participation à l'optimisation des résultats, en termes de productivité, de qualité et de coûts, est fréquemment évoquée.

Cette évolution du rôle des opérateurs, somme toute modérée, tend à renforcer la tension permanente au niveau du management entre deux orientations contradictoires :

- restreindre la marge de manœuvre des opérateurs aux tâches prescrites pour répondre aux impératifs de sûreté,
- l'étendre au contraire, pour mieux atteindre les objectifs de performance.

Les effets du travail routinier

L'un des principaux écueils qui peut menacer le travail de conduite concerne la routine. Inévitable, elle s'avère plus sensible lorsque l'atelier commence à vieillir, « s'encrasse ». Elle engendre souvent une démotivation des opérateurs. Elle pourrait laisser craindre une baisse de la capacité de vigilance face à l'inattendu, précisément engendrée par l'habitude et la répétition, dans un contexte totalement encadré et balisé.

Elle peut être induite par la conception même du système de conduite, avec la conduite par exception où l'opérateur attend quelquefois très longtemps en marche stable, un avertissement lui signalant le début d'une anomalie.

Pour les opérateurs, la notion de routine renvoie à la répétitivité des procédures, des dysfonctionnements, des tâches d'exécution, etc., dans un contexte où les marges d'action et d'initiative sont souvent réduites.

Dans des entreprises où les installations se caractérisent par une fréquence élevée d'aléas et de petits défauts, la surveillance dite de routine suppose une importante vigilance. Il s'agit avant tout des défauts ou des dysfonctionnements qui exigent un réel effort d'anticipation de la part de l'opérateur, compte tenu des enjeux particuliers de l'atelier: arrêt éventuel de l'installation qui remet en cause les efforts de productivité et de qualité, intervention en local (de l'équipe ou d'autres services) dans des conditions souvent difficiles, etc. Il s'agit d'anticiper en permanence des opérations à venir et des défauts connus qui risquent de les perturber.

Dans certaines entreprises, les opérateurs doivent effectuer des relevés écrits de différents paramètres sur le cahier d'unité et sur différentes fiches. Ces relevés peuvent prendre parfois jusqu'à 50% du temps passé en salle de commande. Le but du travail prescrit fondé sur des relevés écrits est d'une part de maintenir la vigilance des opérateurs, d'autre part de capitaliser l'information sur le procédé lorsque sa connaissance reste perfectible, ou pour répondre à des besoins de traçabilité. Les opérateurs reconnaissent l'importance de cette notion de traçabilité, y compris pour eux-mêmes, bien qu'ils expriment quelques réserves quant à l'utilité de certaines des valeurs relevées et le risque d'erreurs lors du "*recopiage des paramètres*" (selon leurs termes).

Ces relevés écrits peuvent contribuer à renforcer certaines formes de vigilance en lien avec l'évolution des paramètres du procédé, mais à certains moments, ils alourdissent la surveillance, ils affaiblissent d'autres formes de vigilance, plus complexes et moins évidentes, par exemple l'anticipation globale et intuitive de l'évolution du procédé, de l'état des installations, de ses défauts connus, du fait qu'ils interrompent et morcellent la surveillance.

Ces relevés écrits peuvent servir en partie à combler des lacunes de la **C**ommunication **H**ommes **S**ystème (**CHS**) , en donnant un aspect «passif » à la surveillance, alors que les outils dont disposent les opérateurs leur ouvrent théoriquement d'autres possibilités, permettant un enrichissement du travail (analyses de tendances, de corrélations, etc. pouvant faciliter une approche plus «intellectuelle » de la conduite). Le «recopiage » se substitue souvent en partie à l'examen des vues de la console, qui sont trop nombreuses pour être toutes consultées.

Eloignement et abstraction

L'activité de surveillance en salle de conduite se situe en quelque sorte dans un **univers virtuel**, qu'il faut raccorder d'une autre façon, par les rondes, l'intervention, etc., à la réalité des installations.

Compte tenu de l'état des techniques, les moyens de conduite ne donnent, en effet, qu'une représentation abstraite et parcellaire de cet univers. Ainsi, il peut exister un risque de "déréalisation" notamment chez de jeunes opérateurs n'ayant pas participé à la phase d'essais et n'ayant pas encore acquis les repères suffisants et une perception concrète du processus. Cette distance par rapport au réel, au tangible, suppose de la part de l'opérateur et plus largement de l'équipe, un travail permanent de reconstruction et de recomposition de l'état supposé de l'atelier, qui sous-tend toute l'activité de surveillance. Les « rondiers » participent à cette reconstruction et à cette recomposition, et sont parfois considérés comme les yeux et les oreilles des opérateurs de conduite. Les nouvelles salles de contrôle «blast proof » dans la pétrochimie éloignent encore plus les opérateurs de conduite des installations. L'implantation, l'aménagement de la salle de commande, la conception de la **C**ommunication **H**ommes **S**ystème (**CHS**), l'organisation du travail doivent faciliter l'activité de surveillance, la maîtrise des informations, la maîtrise des risques par les équipes de conduite, et c'est là un travail d'ergonomie à considérer comme essentiel.

La "flânerie" des automatismes

L'objet de la surveillance mise en oeuvre par l'opérateur dans ses pratiques de conduite concerne en grande partie des défauts et des dysfonctionnements. La notion de dysfonctionnement renvoie pour une bonne part aux aléas et aux défauts qui « perturbent » la conduite et empêchent son maintien sur un mode automatique. Ces perturbations qui affectent les installations (composants mécaniques, automatismes, matériels annexes) mais non le processus, n'ont en général pas d'incidence sur la sûreté, mais sur l'activité de conduite et de surveillance des opérateurs, en la rendant quelquefois bien

pénible. On distingue quelques cas types de dysfonctionnement qui semblent représentatifs des difficultés que rencontrent les opérateurs de conduite, parmi lesquels : les problèmes de codeurs qui obligent les opérateurs à des "remontées" manuelles ; les problèmes mécaniques qui se traduisent souvent par des petits blocages de certains éléments de l'installation ; les problèmes d'automates (dialogues qui ne se font pas, nécessités de forçage, etc...) ; les problèmes de capteurs, et plus largement d'instrumentation. L'origine de ces dysfonctionnements est généralement imputée aux caractéristiques du procédé (tenue des équipements et difficultés d'accès en milieu radioactif...) et des installations (importance des équipements et dispositifs spéciaux...). Lors de ces dysfonctionnements, «la reprise en manuel» qui consiste à mettre momentanément en « stand-by » l'automatisme s'avère souvent indispensable. Elle est plus ou moins bien vécue par les opérateurs. D'un certain point de vue, c'est une stratégie efficace pour éviter le surcroît de charge de travail collective résultant d'un arrêt ou d'un blocage possible (ce qu'on cherche à éviter), puis du dépannage et du redémarrage. C'est aussi pour les opérateurs un contexte privilégié où ils peuvent réguler et mettre en oeuvre leur savoir faire.

D'un autre côté, les multiples manœuvres (essais et vérifications, aller et retour entre les modes manuel et automatique) qui accompagnent l'anticipation des défauts éventuels, obligent à arbitrer entre des pertes de temps immédiates (en salle de contrôle) et des pertes de temps potentielles (sur le terrain, s'il faut débloquer un système).

Ce qui génère une forme de tension parfois proche du stress. L'opérateur a en effet toujours en tête le « coût » potentiel d'un dysfonctionnement non maîtrisé, tant pour les collègues de l'équipe de conduite que pour ceux des autres services concernés. Un dysfonctionnement non évité sur console (en salle de contrôle) accroît considérablement la probabilité d'avoir à intervenir en local (sur les installations réelles) pour réaliser des opérations de dépannage. Celles-ci sont souvent difficiles, pénibles, et dans certains cas ne sont pas exemptes de risques.

L'activité d'anticipation a donc aussi pour fonction de minimiser un risque, pour soi-même, pour le collectif de travail. Mais à un moment ou un autre cette forme de « gestion » des dysfonctionnements trouve ses limites.

Encore des questions

Cette analyse de l'ANACT ne laisse pas vierge le terrain des questions, que ce soit en matière de distance entre le pilotage virtuel de l'atelier et sa présence physique. Quelles conséquences impliquent l'éloignement sur la nature des tâches à effectuer sur les installations extérieures, compte tenu de l'éloignement du centre de conduite ? L'opérateur chargé des rondes sera-t-il davantage isolé ? Viendra-t-il souvent en salle rechercher des informations ? Quels cheminements prévoir ? Qu'en est-il des cas de marche dégradée, des phases de démarrage et des périodes incidentelles ? En ce qui concerne les salles de commande, comment les aménager compte tenu de la nécessité du travail collectif, caractéristique de certains modes de fonctionnement ? Comment limiter aussi les accès pour éviter que trop de monde vienne perturber l'activité ? Comment favoriser les échanges entre opérateurs extérieurs et opérateurs de conduite ? Faut-il déporter de l'information ? Quel type d'information ? Quel type d'éclairage, climatisation , etc... ? Où installer le pupitre ? Comment l'aménager ?

Les outils de conduite deviennent de plus en plus abstraits, impliquant des modes de raisonnement différents : combien de consoles faut-il installer ? Faut-il les regrouper ? Comment ? Quelle imagerie ? Comment donner aux opérateurs la connaissance synthétique de l'état de l'installation sous forme synoptique ? Comment l'aider à gérer les alarmes ? En marche stable ? En régime perturbé ? Et si l'activité d'anticipation a pour fonction de minimiser un risque, à un moment ou à un autre cette forme de «gestion» des dysfonctionnements trouve ses limites. Plusieurs questions se posent. Quelle méthode de traitement systématique peut-on mettre en place ? Les démarches curatives, préventives voir prédictives existantes sont-elles vraiment opérationnelles ? Et comment distinguer les causes dites techniques et d'autres causes, moins visibles qui relèvent de l'organisation ?

Après l'Homme, la Machine

A ces questions, la technique est censée apporter son lot de réponses. Difficile de voir le futur, tant la communication s'est focalisée pendant longtemps sur l'aspect graphique au détriment des autres composants.

Techniquement, on retrouve la panoplie des OS aussi bien standards que temps réel. Ces informations sont transmises selon plusieurs moyens, le plus important étant d'avoir quelque soit la donnée, à un instant « t » une information unique, cohérente et identifiée parfaitement. L'une des dernières évolutions reste le support de transmission, qui du câble série classique s'est vu rajouter le réseau Ethernet TCP/IP et internet.

Tout en haut de la panoplie des possibles, on trouve le casque 3D qui va permettre d'un seul coup d'oeil de voir aussi bien le lieu de production que celui de gestion et de supervision.
Plus pragmatique, les utilisateurs parlent de l'utilisation de quelques couleurs, avec notamment la forte tendance à éliminer toutes les couleurs de fond en gardant les couleurs de base, le rouge pour les incidents, le vert quant tout va bien. Du classique qui ne déroute pas l'opérateur. ***La course aux millions de couleurs semble révolue.***
De même pour l'intégration de l'écran de vidéo qui montre en permanence le site de production, l'opérateur ne le veut pas sur le même moniteur que l'IHM, chose aujourd'hui faisable techniquement, mais que devient un outil aussi perfectionné soit-il, lorsqu'une panne survient ?
Surtout que de plus en plus, on a tendance à éloigner l'opérateur de son centre de travail habituel, les distances le séparant de l'atelier augmentent, et il lui devient difficile de se rendre compte de visu ce qui se passe réellement.
A l'inverse, la prépondérance des PC et autres produits informatiques implique des espoirs pour le GSM (Norme actuelle des téléphones portables créée début 1990. Le GSM, concurrent du CDMA, est employé en Europe, Amérique latine, Moyen-Orient et Chine, par 1,2 milliards d'utilisateurs. La famille GSM inclut le GPRS (General Packet Radio Services), EDGE (Enhanced Data for GSM Evolution) et le 3GSM. Cet outil est intéressant notamment pour les opérateurs itinérants). Le GSM, c'est également la percée d'internet pour ceux que l'on appelle familièrement « les temporaires » , des opérateurs qui auront besoin d'intervenir sur un site pendant un temps court en fonction d'un problème particulier. Même constat pour la radio fréquence, avec une réduction du poids et de l'encombrement, elle vient remplacer les talkie-walkies d'une autre époque. Mais il faudra que l'opérateur garde ses réflexes notamment en cas de coupure radio. Dans le futur il restera à répondre à la question de savoir dans quelle mesure les clients légers, les butineurs Web remplaceront les IHM d'aujourd'hui ?

Interfacer l'Homme à la Machine

Bien souvent l'écran fait écran au procédé. Certains industriels ont eu tendance, sans s'en rendre compte, à oublier que l'opérateur doit conduire un procédé automatisé et non un système de conduite.

D'où la nécessité de mettre en oeuvre en amont un système d'Analyse Fonctionnelle de Conduite Opérateur ayant pour objectif d'élaborer une stratégie de conduite, en groupe inter-métiers, concepteur et futurs utilisateurs. Elle permet d'identifier des repères dans le procédé et précise l'ensemble des situations de conduite auxquelles l'opérateur va être confronté. Mais il reste des questions de fond, par exemple dans ce panachage intégrant des opérateurs, lesquels prendre ?
L'expérience tend à démontrer qu'il faut trouver le plus représentatif des opérateurs en se gardant bien de froisser les susceptibilités. Il faut que les réunions leur apportent quelque chose, c'est du donnant-donnant tout en valorisant leurs actions au maximum. Car le travail de l'opérateur n'est pas de spécifier des IHM, ce n'est ni son travail, ni sa formation. Comme le précisera l'un des responsables des sites de production de Schneider [10], il faut trouver les moyens d'éveiller la perspicacité de l'opérateur, afin de susciter sa réactivité. De même dans la composition des comités de discussion, les niveaux hiérarchiques doivent être mis à l'écart, aussi les spécialistes prônent d'éviter les hiérarchies établies dans la même réunion, sinon le risque d'avoir des discussions dans un seul sens est trop important.
Dans tous les cas il faut privilégier « les petits pas », avec la possibilité de revenir en arrière si nécessaire.

Sûreté de fonctionnement

La sûreté de fonctionnement est une des préoccupations essentielles des utilisateurs, d'autant que les superviseurs intègrent de plus en plus de fonctions de commande. Les méthodes de transmission de données employées dans l'internet ont été conçues pour transmettre principalement des messages de type texte avec des contraintes d'intégrité relativement basses. Les applications traditionnelles n'ont exigé aucune amélioration fondamentale. Cependant, de nouvelles applications d'internet emploient la transmission de données dans les tâches distribuées qui exigent une intégrité plus élevée. Les applications de sûreté incluent la télésurveillance, le diagnostic, la commande et l'entretien; pleine intégration des systèmes informatiques couvrant la production et l'administration (présentant de ce fait de nouvelles vulnérabilités); édition d'informations sécurisées. Ce problème de la sécurité des accès est actuellement un réel frein à l'implantation de ces architectures dans l'industrie.

- **sûreté de la recette et des télécommandes :** La production de recettes par le superviseur ne peut être faite sans prendre quelques précautions. La connaissance d'une clef d'accès, par exemple, réserve l'accès à l'envoi de recettes ou de télécommandes aux seules personnes habilitées. Par ailleurs il faut remarquer, qu'en général, il existe des

protections internes, les variables étant caractérisées par des attributs qui restreignent les manipulations autorisées (pas de visibilité, lecture seule, lecture et écriture). Dans le cas de processus configurables, il est intéressant de pouvoir vérifier que la configuration en cours correspond bien à la demande de changement de paramètres qui a été faite et, si ce n'est pas le cas, invalider la demande de modification.

- **sûreté de la communication :** le moyen de communication véhicule les informations nécessaires à la visualisation et aussi à la commande (éventuellement). C'est donc un élément déterminant dans la sûreté de fonctionnement. Les protocoles standards (plus ou moins), intègrent des moyens de détection (parité, somme de contrôle, codes correcteurs, codes détecteurs...) et éventuellement de recouvrement des fautes. L'occurrence de pannes sur le médium (coupure, court circuit, ...) est irrémédiable pour la transmission. La détection de ces pannes est donc nécessaire pour enclencher la procédure qui permettra la continuité du service (recouvrement) ou le repli sur un mode dégradé.
- **sûreté du matériel de traitement :** on peut se poser à ce sujet les mêmes questions que pour les automates programmables industriels à savoir : tenue aux grandeurs d'influence, indices de protection, types de contrôles intégrés et action sur défaut etc. Le comportement sur coupure d'alimentation permet de connaître les conditions de sauvegarde éventuelle de la base de données et de la reprise au retour d'alimentation, c'est donc aussi un point important.
- **sûreté du logiciel :** la certification du logiciel est un problème très difficile que l'on ne sait pas résoudre actuellement; en conséquence de quoi, à la certification du produit, on substitue la certification du procédé de fabrication; c'est la vocation des normes d'assurance de la qualité. Pour la méthodologie de conception et codage, il s'établit aujourd'hui un consensus pour reconnaître que l'automatisation du processus d'élaboration du programme (utilisation d'ateliers logiciel, génération automatique de code), va dans le sens d'une amélioration de la sûreté de fonctionnement du logiciel développé. Après l'écriture du programme, il convient de qualifier le logiciel. C'est une procédure qui consiste à tester le logiciel dans toutes les conditions possibles de son fonctionnement.

Performance / prix

Restent quelques critères à prendre en considération comme le rapport performance / prix qui sera à préférer au strict prix de vente. On distinguera le prix de l'équipement (logiciel + matériel) nécessaire au développement, de celui nécessaire à l'exploitation. L'utilisateur ayant des applications multiples peut ainsi optimiser l'investissement en n'achetant qu'une fois la partie développement. Pour évaluer le rapport performance / prix, il faudra tenir compte des possibilités de mise à jour, d'un service d'assistance, de la présence de documentation, du suivi du produit...

Dans ce contexte, ce qui est essentiellement visé, c'est l'amélioration de la disponibilité globale des installations pour des enjeux et challenges aujourd'hui incontournables :

Compétitivité = **P**roductivité + **M**ondialisation + **I**nnovation

3 Dans un monde coopératif

Les travaux multidisciplinaires (Voir figure 3) gravitant autour de l'activité de coopération montrent qu'un bon nombre de savoir-faire sont liés.
La figure ci-dessous résume bien la situation évoquée.

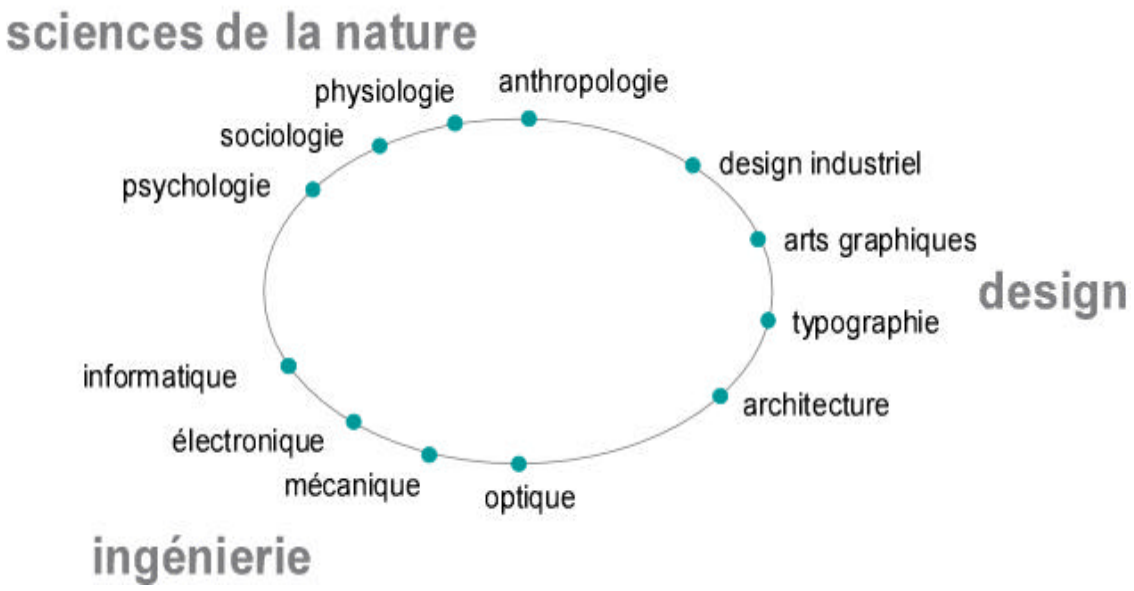


Figure 3 : Coopération et travaux multidisciplinaires

Dans le cas d'une coopération distante, au travers des systèmes distribués, les problèmes liés aux réseaux (disponibilité, sécurité...) et au développement de logiciels adaptés, viennent ajouter une difficulté supplémentaire. Des travaux réalisés dans le domaine de recherche du CSCW (Computer Supported Cooperative Work) tout comme les travaux, articles et ouvrages concernant la création de plates-formes coopératives sont nombreux.

3.1 Les concepts généraux et définitions

Le terme coopération revêt de nombreuses significations selon le contexte dans lequel il est utilisé. Il est fréquent de le voir relié avec d'autres termes proches tels que la *collaboration*, la *coordination* voir la *compétition*. La littérature propose comme définitions suivantes :
Au sens strict, coopérer signifie opérer ensemble (préfixe co-). Le dictionnaire Larousse édition de 1994 propose comme définitions suivantes concernant la coopération :

- Action de coopérer . Travailler en coopération avec quelqu'un,
- Organisation en coopérative d'une entreprise commerciale . Société de coopération,
- Politique d'aide économique, culturelle et technique aux pays en voie de développement ; cette aide. Ministère de la coopération. – Appelé qui part en coopération, comme coopérant.

Le dictionnaire http://www.lexilogos.com/ sur internet donne comme définition le 19 janvier 2007 :
COOPÉRER, verbe intrans.

- Agir, travailler conjointement avec quelqu'un en vue de quelque chose, participer, concourir à une œuvre ou à une action commune.
- [Le suj. est un animé ou un inanimé; le verbe est suivi d'un obj. secondaire introd. par à précisant l'œuvre ou l'action dont il s'agit] Le pouvoir exécutif, le pouvoir législatif, et le pouvoir judiciaire, sont trois ressorts qui doivent coopérer, chacun dans sa partie, au mouvement général (CONSTANT, Princ. pol., 1815, p. 19) : le Gouvernement britannique

était disposé à coopérer avec le Comité national à la création en France d'une organisation destinée à réaliser l'unité des Français dans la résistance à l'ennemi. DE GAULLE, Mémoires de guerre, 1954, p. 643.

- [Le suj. est un animé; le verbe n'est pas suivi d'un obj. secondaire introd. par à] Agir avec quelqu'un; agir ensemble. Penser à Dieu est une action; mais aussi nous n'agissons pas sans coopérer avec lui et sans le faire collaborer avec nous (BLONDEL, Action, 1893, p. 352). L'entrée des États-Unis dans la guerre leur imposait de coopérer avec la France libre (DE GAULLE, Mémoires de guerre, 1954 p. 187).

- Les machines (...) ont donné, à l'homme, parmi tant d'avantages, une malheureuse faculté, celle d'unir les forces sans avoir besoin d'unir les cœurs, de coopérer sans aimer, d'agir et vivre ensemble, sans se connaître...MICHELET, Le Peuple, 1846, p. 172.

- B. THÉOL. Coopérer à la grâce. Répondre à l'action de la grâce par un effort personnel : On coopère à la grâce, on correspond à ce que Dieu imprime intérieurement par l'amour qui est, dit Fénelon, le plus parfait exercice de la volonté. Se livrer à la grâce par un choix libre, c'est y coopérer de la manière la plus parfaite. MAINE DE BIRAN, Journal, 1821, p. 326.

Malgré ces définitions, les concepts d'***intérêts communs***, de ***droits*** (au sens légal du terme), de ***profit*** et d'***activité*** sont évoqués. Ces notions de ***confiance*** et de ***compréhension*** sont également évoquées. On fixe aujourd'hui à 1844, la naissance du mouvement coopératif moderne, avec la fondation, à Rochdale, en Angleterre, de la coopération de consommation établie par vingt-huit Rochdaliens dont le nom est passé à l'histoire avec celui qu'ils donnaient à leur association : « société des Equitables Pionniers de Rochdale ». Quelques années plu tard, Marx l'avait défini en 1867 comme plusieurs individus qui travaillent ensemble pour atteindre un objectif planifier. Entre ces individus, un mécanisme d'échange est mis en place dans le but d'accélérer l'accès à l'information ou à une nouvelle technologie. Aujourd'hui, les travaux effectués sur le workflow (déroulement d'opération) définissent la coopération ainsi : la tâche de coopération considère le processus de division du travail (en autres tâches) et des responsabilités (rôles) parmi les coauteurs. Elle considère aussi la définition des ressources et des périodes pour chaque tâche. La notion de planification qui ressort de cette définition est primordiale pour le déroulement de l'activité de coopération.
La figure 4 extraite [16] classe différentes actions selon le degré de communication de groupe.

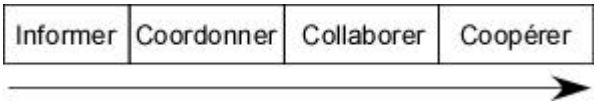


Figure 4 : Degré de communication de groupe

Cet exemple montre que la coopération se place sur un niveau plus complexe d'interaction que la collaboration.

3.2 L'organisation des membres coopérants

L'Homme est un être social qui s'organise en groupes afin de réaliser ses objectifs. C'est cette organisation qui structure la coopération et la rend ainsi efficace. Le groupe de membres coopérants est toujours organisé, même si l'organisation n'est pas systématiquement le fruit de règles préalablement établies. Cette organisation découle habituellement des relations hiérarchiques entre les différentes personnes. La politesse au sein du groupe permet d'éviter au maximum les interruptions, il s'agit par exemple d'une organisation implicite du groupe.
Un groupe est défini comme un ensemble d'entités réparties et distinctes qui sont reliées par un but commun. Un groupe peut être :

- *actif ou passif* : selon qu'il existe un échange de données entre les membres ou pas,
- *dynamique ou statique* : selon que les membres peuvent changer leurs rôles pendant la coopération ou non,
- *ouvert ou fermé* : selon qu'il accepte ou non les interactions des membres qui n'appartiennent pas au groupe,

- *déterministe, non déterministe ou anonyme* : selon que les membres du groupe se connaissent tous, ou seulement une partie d'entre eux, ou aucun,
- *permanent, à la longue durée ou à courte durée* : selon la tâche à réaliser et sa durée.

L'interaction est dite non contrôlée si le groupe est ouvert et contrôlée dans le cas d'un groupe fermé.
Il existe différents modes d'admission dans le groupe :

- *indépendance* : la personne qui rejoint le groupe n'a aucune information sur sa constitution,
- *spontanée* : la personne rejoint le groupe après avoir examiné la liste des participants,
- *par invitation* : la personne rejoint le groupe après avoir reçu un message, ou une requête qui nécessite sa participation (c'est typiquement le cas de l'intervention d'un expert),
- *par vote* : les membres du groupe existant votent dans le but de choisir un membre à intégrer au groupe.

Enfin, la structuration des groupes et du travail peut être décrite à deux niveaux différents : niveau statique ou niveau dynamique.

3.2.1 Organisation statique

L'organisation statique [3] reflète en général la structure relativement stable dans le temps d'une organisation. Elle comprend d'une manière générale :

- *des projets,*
- *des activités* au sein de ces projets,
- *des tâches* à accomplir et à coordonner au sein de ces projets,
- *des individus,* lesquels sont les membres d'un projet et participent à une ou plusieurs activités, à qui sont confiés un certain nombre de tâches et qui possèdent un rôle qui les caractérise au sein d'un projet ou d'une tâche,
- *des documents,* qui peuvent être publics ou appartenir à un projet spécifique ou à une activité particulière.

Les aspects spécifiques de cette organisation statique sont :

- *la création et la destruction* des projets, des activités et des tâches,
- *l'ajout ou la suppression* de membres (individus ou documents) à un projet, activité ou tâche,
- *le contrôle et la synchronisation* des tâches afin de respecter les délais spécifiés,
- *le contrôle de la sécurité* : en effet, l'appartenance d'un individu à un projet, une activité ou une tâche, et le rôle qu'il y joue, déterminent les droits qu'il possède sur les documents présents dans la coopération.

3.2.2 Organisation dynamique

L'organisation dynamique reflète en général la structure des utilisateurs connectés et des données manipulées à un instant précis. Elle est en quelque sorte une instance dynamique de la structure statique précédemment décrite. ***Le terme de session*** est souvent employé dans la littérature pour nommer les éléments de cette instance. La notion de groupe est prépondérante dans la description de l'organisation dynamique. Les utilisateurs des applications coopératives sont regroupés en fonction de différents critères qui peuvent être : la distance, l'affinité, les compétences, la partie du travail qu'ils réalisent…

L'organisation dynamique comprend les aspects spécifiques suivants :

- *l'identification, la connexion et la déconnexion*,
- *la création* d'une session, *l'entrée* d'un utilisateur dans une session, *la sortie* d'un utilisateur d'une session et la destruction d'une session. De tels mouvements peuvent être explicites (un utilisateur demande à entrer dans une session, ou sortir d'une session de travail coopératif correspondant à une activité dont il est membre), programmés (une réunion virtuelle, correspondant à un type particulier de session, a été prévue pour tel jour, à telle heure, pour telle durée et avec tels participants) ou implicites (un utilisateur ouvrant un document déjà édité par un autre membre d'une même activité se retrouve automatiquement dans la même session que lui),
- *la cohérence* des sessions.

Enfin, en ce qui concerne l'organisation dynamique d'un groupe de membres coopérants, les caractéristiques suivantes ont une importance capitale :

- *la charge de travail* est variable dans le temps : tous les membres coopérants peuvent réagir à un évènement simultanément, puis rester inactifs un long moment,
- *la charge de travail* est variable dans l'espace : deux membres peuvent effectuer une opération conjointement pendant que les autres en attendent le résultat pour réagir,
- *le rôle et les droits* des participants est variable dans le temps : un membre observateur (donc inactif) peut devenir un membre acteur,
- *la qualité de service* demandée peut être modifiée : par exemple si l'on introduit une connexion vidéo entre deux sites. Elle est donc variable dans le temps et dans l'espace.

Les paramètres organisationnels peuvent être gérés par :

- *des algorithmes dédiés,*
- *les membres coopérants eux-mêmes.*

3.3 Le travail coopératif et ses outils (problématique de la coopération à travers les systèmes distribués)

Le collecticiel est défini comme un système à base d'ordinateurs qui supporte des groupes de personnes réalisant en commun une tâche ou un but et qui fournit une interface pour accéder à un environnement commun. Le terme collecticiel (ou groupware en anglais) désigne tous les supports ou les produits logiciels qui supportent les applications du CSCW (Computer Supported Cooperative Work) [17]. Un collecticiel peut être défini [18] comme un système à base d'ordinateurs qui supporte des groupes de personnes réalisant en commun une tâche ou un but et qui fournit une interface pour accéder à un environnement commun. Les recherches menées dans le domaine du CSCW ainsi que dans le domaine des plate-formes coopératives, étudient donc cette problématique.

3.3.1 Coopération synchrone ou asynchrone

Etant donné qu'il existe des supports *synchrones* (visioconférence, instant messaging...) ou *asynchrones* (mail, forum...), deux types de coopération sont possibles [19] : la coopération synchrone et la coopération asynchrone. Lors d'une coopération asynchrone, les membres coopérants n'ont pas besoin d'être disponibles simultanément pour coopérer. Les données et les communications persistent dans le temps. La coopération synchrone nécessite la présence simultanée des membres impliqués.
Le plus souvent, les deux modes sont utilisés dans les applications multimédias. Les outils basés sur une combinaison des deux modes de communications (synchrone et asynchrone) sont bien adaptés à une expertise coopérative.

3.3.2 Coopération directe ou indirecte

Lorsque les individus coopèrent via un appareil technique, sans communiquer directement, il convient de parler de *coopération indirecte*. C'est le cas par exemple, d'un système dans lequel, en fonction de l'état de fonctionnement d'une machine, un membre coopérant A prend une décision qui modifie l'état de fonctionnement de cette machine. Découvrant ce nouvel état, le membre coopérant B prend une décision qui va entraîner une nouvelle modification. Dans ce cas, les membres ne communiquent pas, mais ils coopèrent tout de même. La gestion des tâches dans le système de maintenance PROTEUS [20] suit une logique de coopération indirecte. Dans le cas où le système permet une interaction directe entre les membres, le terme de *coopération directe* sera utilisé.

3.3.3 Coopération locale ou à distance

La coopération peut être définie par son aspect local ou distant. Il s'agira donc de *coopération locale* ou *distante*. Dans le cas de la *coopération locale*, les membres coopèrent dans un même lieu physique et sont donc en mesure d'interagir fréquemment.
La coopération à distance nécessite l'utilisation d'un média intermédiaire qui permet de relier les membres coopérants. Ceux-ci sont donc limités dans leurs interactions par la disponibilité, la largeur de la bande passante, le temps de réponse du système de coopération et du réseau sous-jacent.

3.3.4 Coopération collective ou distribuée

La coopération peut être *collective* ou *distribuée*. Dans le mode collectif du travail coopératif, les individus coopèrent ouvertement et consciemment : ils constituent un groupe qui a une responsabilité commune. Dans le mode distribué, au contraire, les individus sont semi-autonomes. Chacun peut modifier son comportement selon les circonstances et avoir sa propre stratégie : dans cette situation, chaque membre n'est pas nécessairement conscient des autres ni de leur activités ; ils coopèrent au travers de leur espace de travail. Cette deuxième situation de coopération s'approche de la collaboration, mais le système utilisé sert de lien, permettant la coopération.

3.3.5 Les différents types d'outils coopératifs

Beaucoup d'outils de travail coopératif s'adressent couramment à un groupe de 2 ou 10 personnes. Leur fonctionnement au-delà de 10 personnes devient la plupart du temps improductif. Ils utilisent un ou plusieurs réseaux de communications comme support. Il peut s'agir d'internet, d'un réseau intranet, de réseaux mobiles ou, plus simplement, du réseau téléphonique de type RTC (Réseau Téléphonique Commuté).

3.3.5.1 Les outils de communication

Ces outils facilitent les communications entre plusieurs personnes au travers des réseaux de communications. Les communications transportées peuvent être textuelles, vocales, audio, audiovisuelles ou graphiques. Il s'agit donc d'outils simples comme le téléphone, le chat, le mail ou d'outils plus évolués tels que les outils de visioconférences, les newsgroups, les forums, les wiki et les tableaux blancs.

3.3.5.2 Les outils de partage et de gestion de fichiers

Il s'agit d'outils permettant le partage de fichiers avec d'autres utilisateurs. Selon que le système permet ou non l'édition des fichiers partagés, un système de gestion de concurrences peut être nécessaire. Un système de partage de fichiers peut être basé sur un serveur ftp, ou base de données partagée.
Les systèmes de gestion de concurrences sont des outils permettant le partage de documents et la gestion des versions de documents. Ils détectent les éventuels conflits de versions en analysant les données stockées. Il existe actuellement deux outils assurant ces fonctions : SVN et CVS [3].

3.3.5.3 Les outils de worflow

Les outils de workflow sont utilisés afin d'organiser et d'automatiser l'enchaînement des tâches effectuées par différents intervenants dans le cadre du processus de travail intellectuel.

3.3.6 Classification des outils de travail coopératif

Les recherches menées dans le domaine du CSCW se sont attachées à définir des moyens de classifications des collecticiels.

3.3.6.1 Classification fonctionnelle

Le trèfle fonctionnel du collecticiel [21] repose sur la définition d'ensembles fonctionnels comme nous le montre la figure 5.

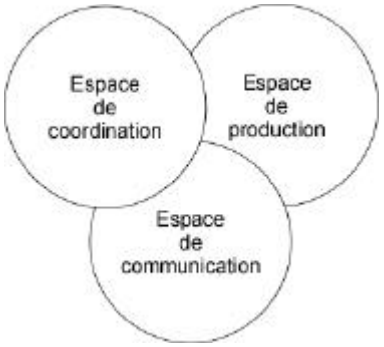


Figure 5 : Le trèfle fonctionnel du collecticiel

Nota : la couverture de ces ensembles fonctionnels n'est pas forcément identique.

- l'espace de production, désignant les résultats d'une activité de groupe,
- l'espace de coordination, qui définit les acteurs et leur structure sociale, ainsi que les différentes tâches à accomplir en vue de produire les objets de l'espace de production. Il s'agit de définir les acteurs (notamment les individus, les groupes, les rôles), d'identifier les activités et les tâches (notamment leurs relations temporelles) et de désigner enfin les acteurs responsables des tâches et des activités,
- l'espace de communication, qui offre aux acteurs de l'espace de coordination la possibilité d'échanger de l'information dont la sémantique concerne exclusivement les acteurs, le système n'étant q'un messager.

3.3.6.2 Classification conceptuelle

M. Diaz [22] propose de découper les collecticiels en trois mondes (Voir figure 6) :

- le monde des *données*,
- le monde des *utilisateurs* (qui accède et manipule les éléments du monde des données),
- le monde de l'*organisation* (qui structure les deux précédents).

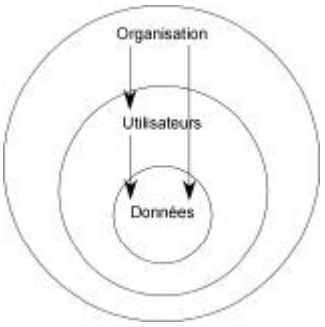


Figure 6 : Les trois univers conceptuels de la coopération [22]

3.3.6.3 Classification selon les modes de travail de groupe

Une classification topologique des outils de travail coopératif reposant sur l'espace (lieu identique ou distinct) et le temps (synchrone ou asynchrone) a été envisagée [23]. Selon les configurations géographiques et les contraintes temporelles du travail, une matrice des modes de travail de groupe (Voir figure 7) a été proposée. Cette classification présente l'avantage de définir simplement les outils, en fonction des deux critères. De plus, les besoins associés à chaque situation sont clairement exprimés.

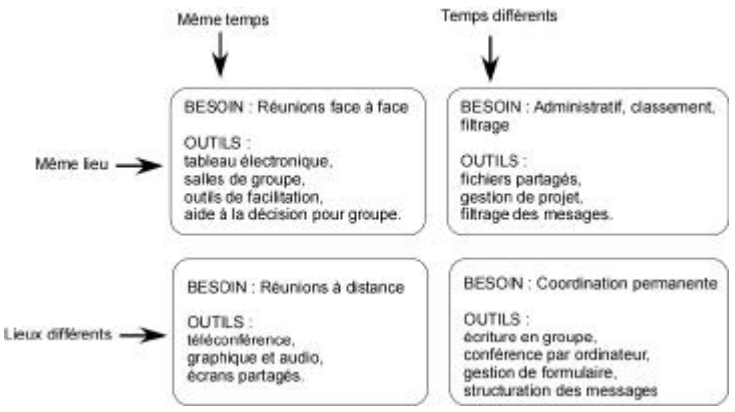


Figure 7 : Matrice des modes de travail de groupe

3.3.7 Gestion de la coopération

Il existe différents niveaux dans la gestion de la coopération : communication entre les membres du groupe, accès aux données partagées, etc... Différents domaines existent :

- gestion de la mémoire partagée,
- gestion de la communication,
- gestion du groupe,
- gestion de la qualité de service.

Ces différents domaines sont interconnectés. Souvent, la gestion des groupes sert de support pour la gestion de la communication et la gestion de la mémoire partagée. La gestion de la qualité de service se base sur les interactions effectives de la gestion de la communication et de la mémoire partagée.

3.3.7.1 Gestion de la mémoire partagée

Une des principales difficultés du travail coopératif est de gérer la cohérence des données partagées. Les accès concurrents aux objets peuvent être la cause de la perte de cohérence du système. C'est le cas si deux personnes veulent modifier simultanément un même objet ou une même variable. Il est possible d'utiliser des mécanismes de propriétés sur les données, mais il faut alors gérer la cohérence de ces propriétés afin que plusieurs sites ne soient pas en possession de même objet (propriété d'exclusion mutuelle), ou qu'un objet, n'appartenant plus à personne, devienne inaccessible (propriété de vivacité).

Dans les systèmes distribués utilisés pour supporter la coopération, il existe trois grands types d'architecture de gestion de la mémoire partagée répliquée [3] :

- *l'architecture centralisée* : dans ce type d'architecture, un seul processus conserve à la fois les données et la vue que peut avoir chaque utilisateur. Cette architecture a pour avantage la grande simplicité d'implémentation et la réduction au minimum de l'infrastructure nécessaire pour faire fonctionner l'application. L'inconvénient majeur est sa faible tolérance aux pannes.

- *l'architecture répliquée* : dans ce type d'architecture, les données sont répliquées sur chaque site utilisateur. Cette caractéristique, en plus de la possibilité de communication entre les différents sites, rend le système fortement tolérant aux fautes. Cependant, l'inconvénient majeur de cette structure est la difficulté de sa mise en oeuvre. La duplication des données et du contrôle rend les opérations (cohérence des données, ordonnancement des actions) très complexes et donc très coûteuses en ressources.
- *l'architecture hybride* : dans cette architecture, l'état est détenu par un processus central qui diffuse à autant d'autres processus que d'utilisateurs. Exemples : partage d'écrans et de fenêtres. Néanmoins, la dégradation du temps de réponse de l'interface utilisateur peut être sensible.

3.3.7.2 Gestion de la communication

Trois types de protocoles pour la gestion des communications sont utilisés [24] :

- *les protocoles asymétriques*, où les messages sont transmis à un coordinateur central qui les ordonne puis les diffuse. Ces protocoles ont pour conséquence une perte de temps due à la ré-émission des messages. De plus, le coordinateur central est un point sensible aux pannes,
- *les protocoles symétriques*, où tous les sites émettent et reçoivent à n'importe quel moment,
- *les protocoles à coordinateur tournant* où le droit d'émettre est donné temporairement à un site. La gestion des messages est alors simple et aucun site n'est un point plus sensible que les autres en cas de panne.

3.3.7.3 Gestion des groupes

Les protocoles de gestion de groupes visent à gérer les groupes et sous-groupes. Pour cela, ils effectuent des actions sur la création et la destruction de ces groupes ou sous-groupes selon des critères tels que la hiérarchie, les positions géographiques, la qualité de la connexion, les échanges de données en cours…

3.3.7.4 Gestion de la qualité de service

La gestion de la qualité de service consiste à fournir aux applications les ressources nécessaires à leur bon fonctionnement en respectant leurs besoins en bande passante ou taux de perte par exemple [24].
Il s'agit donc d'optimiser les points suivants :

- *la qualité de service réseau* : capacité d'un réseau à fournir le meilleur service possible à un trafic donné,
- *la qualité de service dans les équipements* : capacité des équipements à fournir le meilleur service possible,
- *la qualité de service de bout en bout* : correspondant à l'ensemble composé par la qualité de service du réseau traversé et la qualité de service des différents équipements locaux. Chaque couche traversée doit fournir les ressources nécessaires. Le destinataire bénéficie de la qualité de service du maillon le plus faible de la chaîne.

3.4 Les domaines d'application des systèmes coopératifs

L'ensemble des secteurs concernés par les innovations des systèmes coopératifs est très varié. Aujourd'hui, les activités de télé-médecine, e-learning, e-design, e-maintenance... se développent, en apportant elles-aussi leurs spécificités et leurs modes opératoires en matière de coopération. Pour exemple, la e-maintenance est devenue un domaine majeur d'application des systèmes coopératifs. Elle est basée sur le principe de perception de l'état d'un système complexe distant. Un ensemble de personnes peut ensuite accéder aux données, ainsi qu'à des moyens de communication ou d'intervention, au travers de différents systèmes et réseaux. Les outils transversaux (planification de tâches, gestion du personnel et des pièces détachées, aide à la détection de panne, aide à la décision…) sont la plupart du temps intégrés dans ces systèmes.
Aujourd'hui, de plus en plus de systèmes complexes (nouvelles machines industrielles, logiciels, imprimantes et photocopieurs, matériel militaire ou de santé…) peuvent être connectés à internet. Ceci permet d'envisager de les maintenir à distance sans

nécessairement avoir de personnel qualifié disponible sur le site à surveiller ou à réparer. Les interventions peuvent donc être plus rapides et les priorités sont gérées à un niveau plus global que dans le passé. Le personnel qualifié peut apporter une aide effective depuis pratiquement n'importe quel endroit. Les coûts globaux de déplacement de personnel qualifié sont donc diminués. La e-maintenance peut se montrer décisive en matière de coûts et de qualité.

D'autres avantages découlent directement des travaux effectués dans les domaines concernés par la e-maintenance. En effet, la maintenance au sein d'environnements dangereux est grandement simplifiée par l'utilisation de télé-surveillance, télé-diagnostic et même de télé-opération à l'aide de robots. Ces environnements dangereux concernent un grand nombre de domaines tels que la maintenance des réacteurs nucléaires, de satellites en orbite, ou de robots explorateurs de planètes ou de fonds marins.

Parmi les exemples existants, on pourra retenir :

- TEMIC (système automatique de surveillance et de diagnostic des pannes) [25],
- le projet LARs (armée américaine : chaque ordinateur ceinture est équipé d'un système de vidéo-conférence, de tableaux de bord électroniques et de systèmes dits « Logistics Assistance Representatives » ou « LAR »,
- le CIMS (Center of Intelligence Maintenance Systems) : Université Wilsconsin-Milwaukee développe une plate-forme appelée IMS (Intelligent Maintenance Systems). Cette plate-forme utilise un système multi-agent intelligent appelé Watch Dog analysant en permanence le comportement de l'état du système et prenant des décisions sur les procédures de maintenance à accomplir,
- PROTEUS (projet Européen) : L'entreprise CEGELEC en collaboration avec Schneider Electric et les laboratoires LAB, LIFC, LIP6 et LORIA, mènent en commun le projet Européen PROTEUS. Il s'agit de développer une plate-forme générique de e-maintenance. Celle-ci utilise les services du web afin d'interconnecter les différents outils existants dans les entreprises. La consultation de documentation technique, la commande de pièces, la gestion de la maintenance et la gestion du personnel, se font de manière transparente au sein d'un environnement distribué et hétérogène.

3.5 Ecrans et ordinateurs, il était une fois…

Ce paragraphe fera un point sur l'évolution technologique et spectaculaire de l'ordinateur et donc en terme d'IHM !

A l'origine de l'ordinateur, nous trouvons le boulier chinois qui date de l'an 700. Puis John Napier inventa les logarithmes en 1614 permettant ainsi dès 1620 l'utilisation de la règle à calcul. Ensuite, vint le règne des machines à calculer : en 1623, William Schikard, en 1642 Blaise Pascal invente la Pascaline, machine capable d'effectuer des additions et soustractions. En 1673, Von Leibniz ajoute à la Pascaline la multiplication et la division. Puis en 1834, Charles Babbage invente la machine à différence qui permet d'évaluer des fonctions idée reprise par Von Newman pour l'organisation logique d'une machine informatique. La suite est encore longue et je vous propose de passer directement en 1945. [5, 6, 7]

Vannevar Bush

As we may think, Atlantic monthly (1945) :

«publication has been extended far beyond our present ability to make real use of the record»

Memex : un instrument de mémoire externe

- un instrument utilisé pour conserver ses livres, notes, archives, etc ,
- un système de mots clés, de références croisées et des mécanismes d'indexation permettant d'accéder rapidement à l'information,
- la possibilité d'annoter les documents stockés et de sauvegarder un "chemin" (une chaîne de liens).

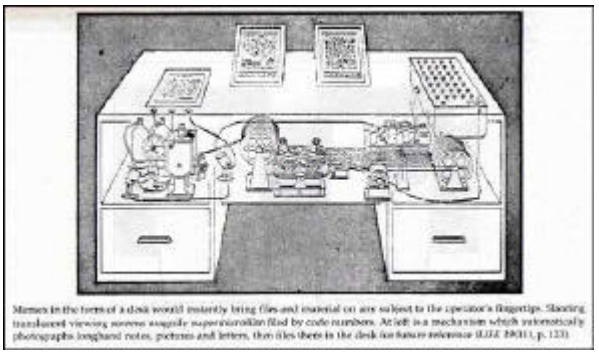
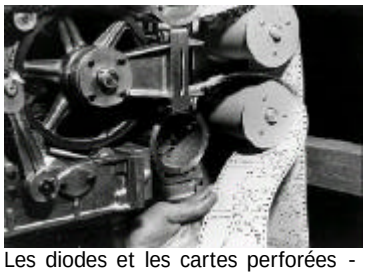


Figure 8 : Schématisation du concept « MEMEX »



Les diodes et les cartes perforées - sauvegardes des données - Mark-I, 1944

IBM SSEC, 1948

Console de maintenance - IBM 7030 (Stretch) - 169000 transistors - 16 Mo de stockage sur disque, 1961

J.R. Licklider

Chercheur au MIT[1] (psycho-acousticien)

Directeur de l'IPTO de l'ARPA (Information Processing Techniques Office)

1960 : propose l'idée de symbiose homme-machine

"The hope is that, in not too many years, human brains and computing machines will be coupled together very tightly and the resulting partnership will think as no human brain has ever thought » « essai-erreur » , découvrir les solutions...

Douglas Engelbart

Augmenting Human Intellect: A Conceptual Framework (1962)

« By augmenting man's intellect we mean increasing the capability of a man to approach a complex problem situation, gain comprehension to suit his particular needs, and to derive solutions to problems»

– traitement de texte structuré,

– hypermedia,

– la souris, le clavier à une main,

– écrans haute résolution,

– l'idée de fenêtrage,

– mobilier spécifique,

– partage de fichier et annotations,

– messagerie électronique,

– partage d'écran, télépointeurs,

– audio et video-conférences,

---

[1] Le Massachusetts Institute of Technology, abrégé MIT, est une institution de recherche et une université américaine, spécialisée dans les domaines de la science et de la technologie. Elle est située à Cambridge, dans le Massachusetts, à proximité immédiate de Boston.

Le MIT est un leader mondial pour l'enseignement et la recherche en science et en technologie, mais il est aussi réputé dans d'autres domaines comme le management, l'économie, la linguistique, les sciences politiques et la philosophie. En 2005, 61 membres ou anciens membres du MIT (corps enseignants et élèves) avaient reçu le prix Nobel. Parmi ses départements et écoles les plus célèbres, on compte :

Le Lincoln Laboratory (en français, Laboratoire Lincoln) ;
le Computer Science and Artificial Intelligence Laboratory (en français, Laboratoire d'Intelligence Artificielle et d'Informatique) ;
le Media Lab ;
le Nuclear Laboratory;
la Sloan School of Management.
le Center for Bits and Atoms (CBA) qui explore les liens entre l'information et sa représentation physique (voir fab lab)
Le MIT a été fondé en 1861 par William Barton Rogers. Au départ école d'architecture, l'institut devient rapidement pluridisciplinaire. Il compte près de 1000 enseignants pour 10000 élèves. Le cursus le plus suivi est celui d'ingénieur, 2000 étudiants, puis celui des sciences. Ce qui caractérise le MIT est sa proximité avec le monde industriel et sa très forte implication dans recherche scientifique et technologique, à laquelle les étudiants participent dès leur première année de cursus. En 2002, il fut la première université à mettre l'intégralité de ses cours en ligne sur Internet.

– l'intuition d'internet.

Ivan Sutherland

SketchPad (MIT, 1963) : un outil de dessin en avance sur son temps

– oscilloscope, stylo optique et boutons,

– désignation directe des objets à l'écran,

– feed-back sous forme de lignes élastiques,

– séparation entre l'écran et les coordonnées de dessin,

– zoom avant et arrière (facteur 2000 !),

– structure hiérarchique, opérations récursives,

– système de gestion de contraintes,

– icônes pour représenter des objets complexes.

Internet

Arpanet (1967) : un réseau pour relier des machines entre-elles. Mais : les gens utilisent toujours toutes les technologies à leur disposition pour communiquer avec d'autres personnes. Naissance d'un nouveau moyen de communication : le courrier électronique. Aujourd'hui, la communication entre individus domine les autres usages de l'informatique.

Ted Nelson

Inventeur des termes *hypertexte* et *hypermedia* (1968)

Reprend et étend les idées de V. Bush à travers Xanadu, un système de publication de documents à l'échelle mondiale.

-*Transclusion* : inclusion sans copie d'un fragment de document dans un autre document,

-*ZigZag* : structure pour données multidimensionnelles.

Beaucoup d'idées mal comprises. Malgré tout, une influence non négligeable.

Ethernet (1970)

Ethernet tire son nom de l'Ether, substance censée englober tout l'Univers (à rapprocher du vide aujourd'hui) tirant son **origine** dans la Grèce Antique.

Le premier réseau local Ethernet expérimental a été développé au centre de recherche Xerox de Palo Alto (XEROX P A R C) pour interconnecter des ordinateurs et des imprimantes laser à un débit de 2.94Mbps. En juillet 1976, les deux concepteurs de ce réseau *Bob Metcalfe* et *David Boggs* publièrent le document de référence.

Ethernet était à l'origine un standard développé par les laboratoires Xerox au tout début des années 1970. Ce standard a d'abord évolué jusqu'à la version Ethernet II aussi appelée DIX ou encore v2.0 avec l'association regroupant Digital Equipment Corporation, Intel et Xerox. Par la suite, Ethernet a été inclu dans les travaux sur la modélisation OSI au début des années 1980. Depuis cette époque, la technologie Ethernet est totalement indépendante des constructeurs ; c'est un des facteurs importants de sa popularité.

Les éléments de la couche physique (couche 1 OSI) sont définis par les normes IEEE des sous-comités 802.3 et la méthode d'accès CSMA/CD correspond à partie MAC de la couche liaison (couche 2 OSI).

Comme dans le cas des principes énoncés ci-avant, la généralisation de la commutation simplifie la méthode d'accès en éliminant toute la partie consacrée à la gestion des collisions. On attache aujourd'hui beaucoup plus d'importance aux méthodes de codage employées au niveau de la couche physique.

Les interfaces textuelles

VisiCalc sur un Apple II (1979)

Interfaces à ligne de commande :

– dialogue purement textuel, proche du dialogue oral,

– syntaxe précise, mais structure du dialogue figée et potentiellement complexe.

Menus et écrans de saisie :

– notion de statut courant de l'interaction : le menu regroupe les commandes disponibles à un instant donné, l'écran de saisie regroupe les paramètres requis pour une commande donnée.

Le MIT

Architecture Machine Group, Artificial Intelligence Laboratory, Media Lab...

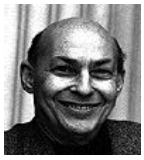
Quelques exemples de projets :

– le langage Logo,

– les débuts de la *multimodalité* : association du pointage et de la reconnaissance de la parole,

– langage naturel, synthèse de la parole et reconnaissance de l'écriture.

De gauche à droite :Marvin Minsky, Seymour Papert, Nicholas Negroponte.



SHRDLU

Un programme capable de dialoguer en langage naturel.

Créé par Terry Winograd, au MIT, entre 1967 et 1970

Buts :

– comprendre les mécanismes du langage humain,

– offrir un moyen simple pour dialoguer avec l'ordinateur,

4 idées simples :

– monde simple à décrire,

– mémoire de contexte,

– peut répondre sur ce qui est possible,

– peut se rappeler de noms.

GUS : the Genial Understander System

Développé chez Xerox par T. Winograd et quelques autres dans les années 70.

Exemple de dialogue :

GUS: Where would you like to go?

User: I want to go to San Diego on July 17th

GUS: Where will you be traveling to San Diego from?

User: San Jose

GUS: When do you want to return?

User: I prefer United Airlines

GUS: OK, I have United Airlines from San Jose to San Diego

departing July 17. When do you want to return?

Le Xerox PARC

Palo Alto Research Center

Centre de recherche fondé en 1970

Regroupement de talents qui s'intéressent à la photocopie mais aussi aux systèmes bureautiques.

Quelques inventions du PARC avant 1975 :

– l'Alto, une station de travail avec écran bitmap et souris,

– le couper/copier/coller,

– l'idée de système de fenêtrage,

– l'imprimante laser.

Alan Kay

L'un des fondateurs du Xerox PARC.

Le père de l'informatique individuelle, inventeur de l'ordinateur portable (Dynabook).

L'un des pères de l'interaction graphique et de la programmation objet (Smalltalk).

Le Xerox Star

Projet lancé en 1975, commercialisé en 1981.

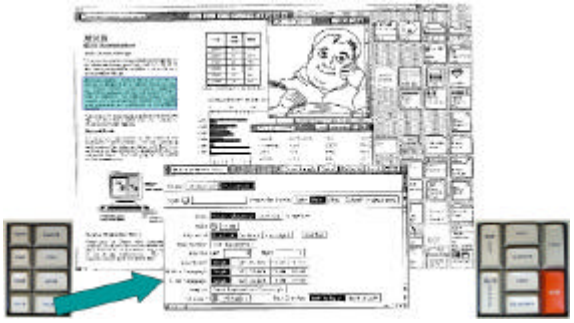
Pour un système destiné aux "business professionals".

Quelques caractéristiques importantes :

– conception matérielle guidée par les besoins logiciels,

– un système fonctionnant "naturellement" en réseau,

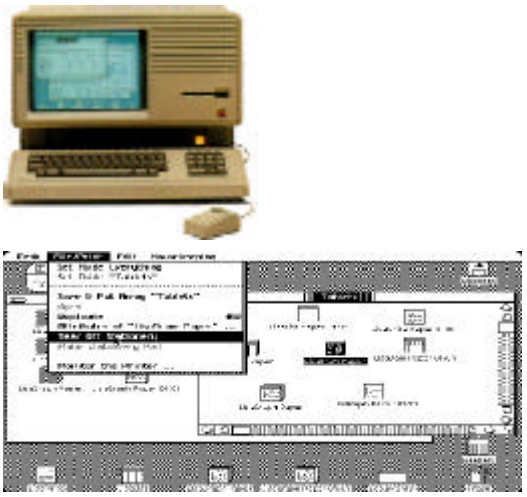
– une interface graphique basée sur la métaphore du bureau,
– l'utilisation d'icônes et de fenêtres et l'idée de WYSIWYG,
– un système centré sur les documents (l'utilisateur ne connaît pas les applications),
– ensemble restreint de commandes génériques accessibles par des touches spécifiques.
CPU microcodé d'une puissance inférieure à un MIPS :
– opérations rapides pour accéder à l'écran (BitBlt),
– 385Ko de mémoire.
Une connexion Ethernet
Périphériques de stockage :
– un disque dur de 10 à 40 Mo,
– un lecteur de disquettes 8 pouces.
Périphériques d'interaction :
– un écran noir et blanc de 17 pouces,
– une souris à deux boutons,
– un clavier spécial muni de deux pavés de touches de fonction.



Un échec commercial...
– un système trop nouveau, trop puissant, trop différent...,
– une cible marketing mal évaluée (ex : pas de tableur),
– un prix trop élevé ($16,500),
– une architecture fermée (impossible de développer des applications hors Xerox),
– un manque de volonté politique pour sortir du marché de la photocopie,
... mais une influence certaine sur les systèmes actuels.

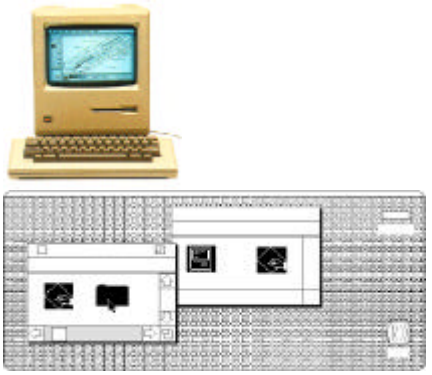
L'Apple Lisa (1983)

Inspiré du Star, un peu moins cher ($10,000).
Un nouvel échec commercial...



L'Apple Macintosh (1984)

Une barre de menu, des boîtes de dialogue modales et des applications "visibles" héritées de l'Apple II.



Le *Finder*,
MacPaint et *MacWrite*

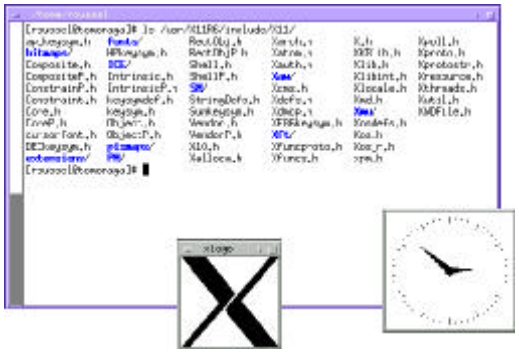
Les raisons du succès :
– des idées plus "mures", un marché prêt à les accepter,
– un prix agressif ($2,500) pour toucher le grand public,
– une boîte à outils pour faciliter les développements externes,
– des guides de style détaillés pour inciter à la consistance entre applications.

Le système X Window (1984)

Issu du projet Athena (MIT, 1983) : 4000 machines UNIX à connecter, fournies par les nombreux sponsors (DEC, IBM, Motorola, etc.)
Modèle client/serveur :
– séparation quoi/comment qui facilite la portabilité,

– utilisation transparente du réseau qui permet l'affichage déporté.

Séparation entre *mécanismes* et *politique d'utilisation.*



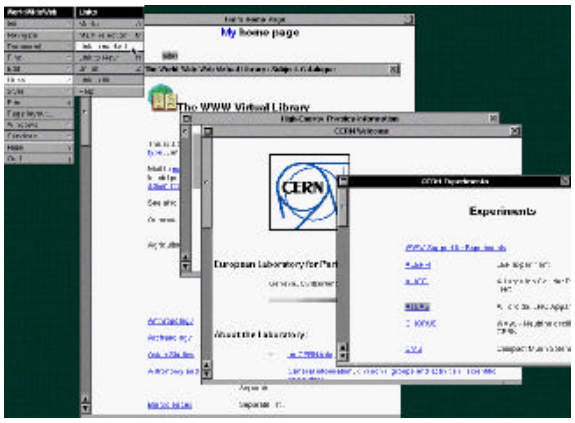
Le World-Wide Web
Croissance fulgurante...

Simplicité, esthétique mais :

– des protocoles figés très rapidement,

– des possibilités d'interaction extrêmement réduites.

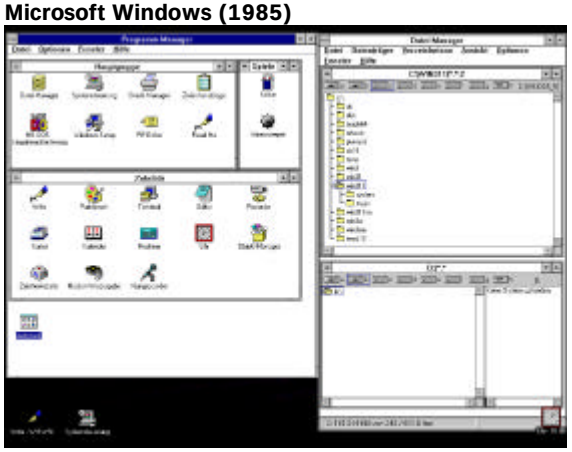
On est encore loin des idées de Nelson ou Engelbart...



Navigateur/éditeur de Tim Berners-Lee (CERN, 1990)

Sur nos écrans aujourd'hui !

Microsoft Windows (1985)



Apple Mac OS (1984)

Linux (1994)

3.6 Evolution des besoins et nouvelles tendances

Comme je viens de vous le présenter rapidement, depuis plus de 30 ans, nous vivons dans une perpétuelle évolution technologique dans le domaine des réseaux de communications industriels et donc puisque tout est lié, des IHM ! Les compétences rattachées à certains métiers comme le métier de l'automaticien ont complètement changé depuis ces dix dernières années au profit de compétences en informatique industrielle. L'objectif essentiel, est de faire circuler des informations de différentes origines :

- informations de gestion,
- informations de processus.

Les informations de gestion proviennent :

- du traitement des informations de description archivées,
- de la comptabilité analytique,
- de la gestion des ventes,
- de la gestion des clients,
- etc...

Les informations de processus (données temps réel) proviennent :

- du terrain,
- de l'atelier de fabrication,
- de la maintenance,
- des stocks en cours à l'instant "t",
- etc...

Pour exemples (Voir figure 9) :

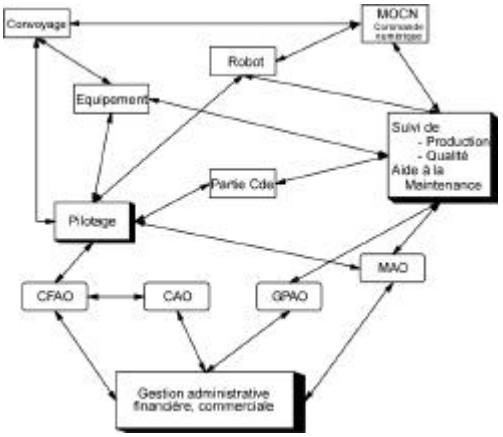
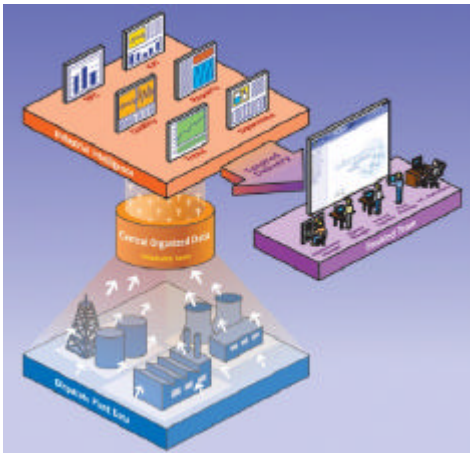


Figure 9 : Flux d'informations possible dans une entreprise



Le début des années 80 a vu l'apparition du concept CIM (Computer Integrated manufacturing) (Voir figure 10), modèle qui déjà essayait d'apporter une réponse à la quête de performance des entreprises en mettant en exergue les insuffisances de l'automatisation à outrance et la nécessaire communication entre les différents niveaux [26]. La représentation la plus courante faisait apparaître un découpage structurel de l'organisation de l'entreprise, et une communication spécifique entre les niveaux du modèle. Si ce modèle est encore largement répandu et présente une certaine légitimité, il a rapidement modification de la structure avec l'apparition des nouvelles technologies en matière de communication industrielle. Les mécanismes d'échanges sont construits autour d'un transfert vertical de l'information (niveau N vers N-1 ou N+1) nécessitant une remise en forme de l'information à chaque interface. Limitation technologique : l'évolution vers des architectures d'automatismes réparties et/ou distribuées associée à l'augmentation de la capacité de traitement des composants entraînent un accroissement des flux d'informations sur les médiums.

Paradoxalement durant les années 90, qui ont vu l'émergence puis la croissance des ERP (Entreprise Ressources Planification), le fossé s'est creusé entre les mondes de l'informatique et de la production. En 2000, les modules ERM (comptabilité/finance, ressources humaines et gestion commerciale) et GPAO ont représenté plus des deux tiers des ventes de licences sur le marché des ERP. Parallèlement à ce constat, la dernière décennie a vu l'apparition, au travers des technologies internet et des langages orientés objet, de nouveaux standards et mécanismes d'échange de données dans le monde de l'informatique.

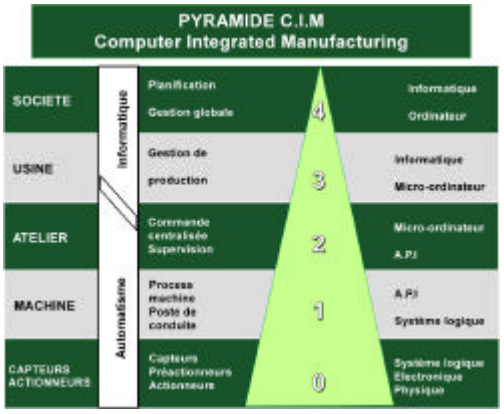


Figure 10 : Modèle pyramide CIM

La performance des entreprises est aujourd'hui indissociable de leur réactivité en terme de réponse aux demandes du marché (il faut passer d'une production de masse à une production personnalisée et flexible), de délai de conception et de mise sur le marché de nouveaux produits, de prise en compte des normes et réglementations (traçabilité des produits en agroalimentaire), de besoin de communication permanent et en temps réel (la bonne information pour la bonne personne en tout lieu et à tout moment). L'ensemble de ces exigences a contribué à l'avènement de l'offre MES (Manufacturing Execution System) et conduit à une modification sensible du modèle pyramidal du CIM (Voir figures 11 et 12).

Ethernet devient un réseau fédérateur dès le niveau 2 (on parle d'Ethernet atelier) et le MES par ses fonctionnalités, tant sur le plan du pilotage que de la supervision de l'atelier de production, se positionne en médiateur afin de réduire la fracture entre le monde de l'informatique de gestion et celui de la production.

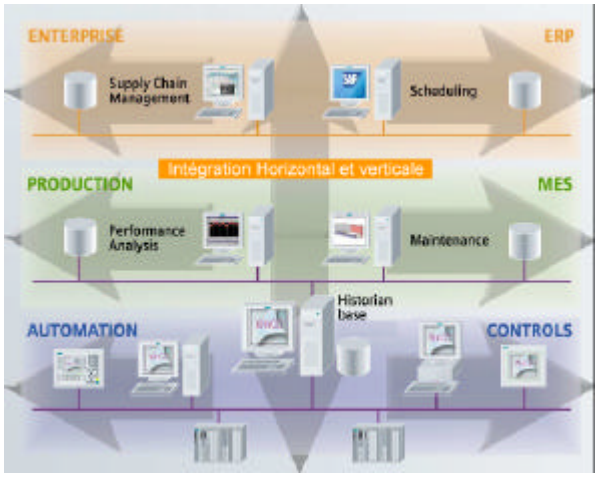


Figure 11 : Des données pour tous

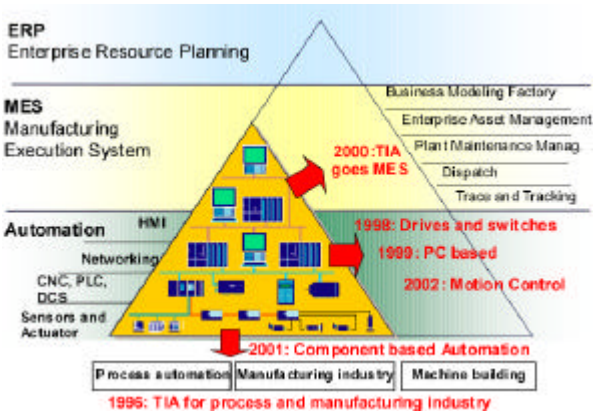


Figure 12 : Une évolution dans le temps

Dans un rapport de l'ambassade de France à Tokyo (Service pour la Science et la Technologie) [27] , il ressort les points suivants :

- les technologies de l'information et de la communication ont largement contribué à accélérer le développement de nouveaux produits et de nouvelles offres de services. Il appartient désormais au monde de la production industrielle

de suivre ce rythme nouveau, en adoptant lui aussi ces mêmes technologies. Toutes les activités sont concernées ; aussi assiste-t-on à la naissance de nouvelles disciplines : e-manufacturing, e-maintenance, e-logistique, e-business.

Les exemples concrets sont nombreux dans le domaine (Voir figure 13). On peut souligner par exemple cette expérience qui résume une situation actuelle [30].

Exemple d'une PME du sud de la France grande utilisatrice de e-maintenance :

- construction de ligne de fabrication, réparation et emplissage de bouteilles GPL,
- 95% du CA à l'export sur les 5 continents – 55 usines dans le monde,
- impossibilité de détachement de personnel pour la maintenance,
- maintenance à distance des automates reliés à un réseau accessible par téléphone et/ou IP,
- application e-maintenance développée en interne il y a 5 ans (2000),
- mise en place d'un extranet pour commande personnalisée des pièces de rechange.

Les résultats majeurs :

- gain sur chiffrage contrats de SAV / concurrence,
- réduction des délais : 3 semaines → 3 jours.

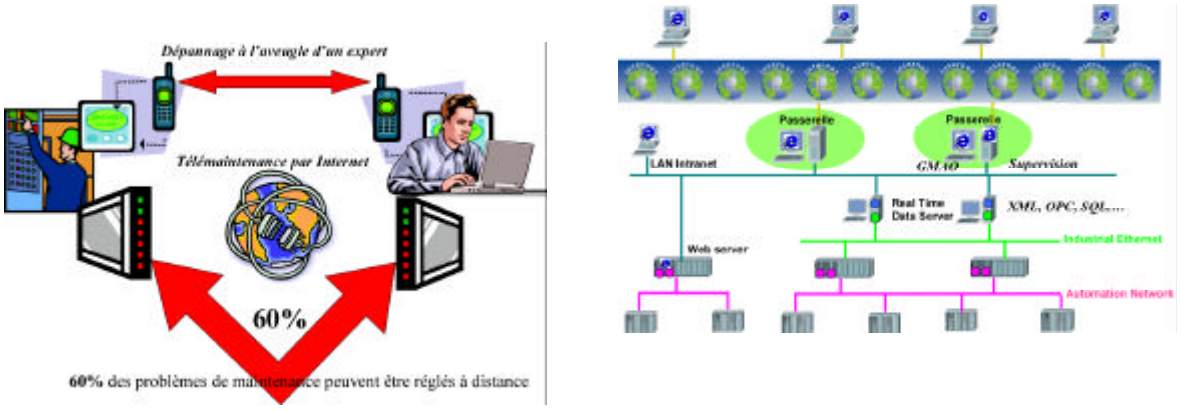


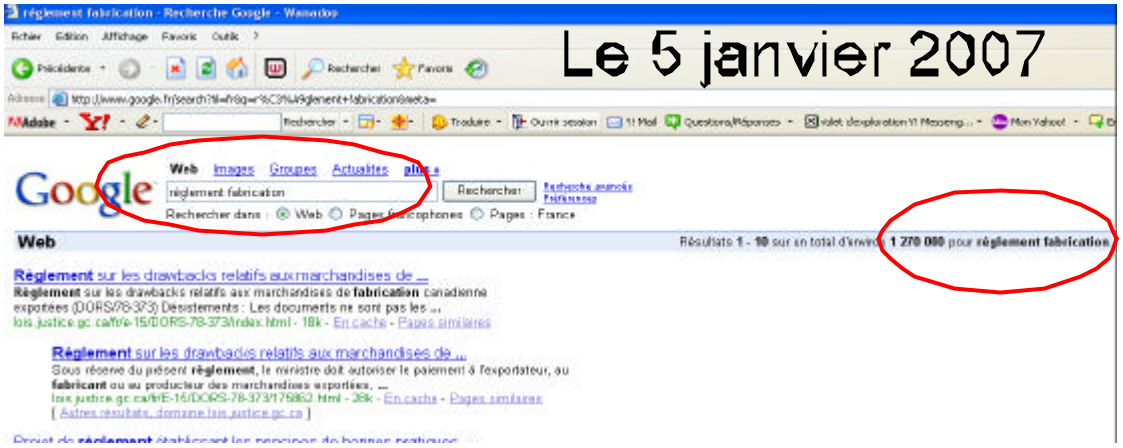
Figure 13 : Un monde ou les distances se réduisent à la vitesse de propagation des communications

3.7 Enjeux et Challenges

L'illustration présentée ci-dessous résume bien la situation actuelle [28].

Figure 14 : Enjeux et challenges

Dans cette mondialisation, de nombreux exemples nous le montre : commerce électronique en pleine évolution (le e-commerce continue son essor rapide en France avec une croissance encore supérieure à 40 % en 2005 et un volume d'affaires qui atteint les 7 milliards d'euros. Sur internet, la concurrence, particulièrement intense, impose aux distributeurs des efforts permanents d'ajustement et d'optimisation du site, de l'offre et des services. Car, pour profiter de la croissance des achats en ligne, il convient d'être à la hauteur des exigences des clients.), traçabilité globale, etc..., ***le respect des réglementations fait partie des incontournables ! Mais de quoi parle t -on ?***



Pour exemples :

- **EC178/2002** traçabilité agroalimentaire européenne,
- **Bio-Terrorism Act** américain Traçabilité F&B,
- **CFR21 part 11** réglementation sur les signatures électroniques,
- **HACCP** recommandation sur les contrôles en production,
- **Sarbanes Oxley** réglementation sur l'information,
- **2001/18/CE** loi sur les OGM,.....

3.8 Ouverture du SCADA vers le MES

Le terme SCADA vient d'une abréviation anglaise (Supervisory Control And Data Acquisition / Application de supervision des systèmes industriels). Elle permet de suivre et contrôler l'ensemble d'un processus industriel (fabrication, transformation, transport...). Ses principales fonctionnalités sont l'acquisition des données, l'analyse et le contrôle, le pilotage des processus, la gestion des automatismes, le suivi des états et des alarmes, la journalisation des événements... On trouve des SCADA dans la plupart des services d'utilité publique (transport de l'énergie – gaz, électricité, gestion de l'eau potable, traitement des eaux usées...). Le domaine d'application du MES (Manufacturing Execution System), se situe entre les niveaux Contrôle-Commande (niveaux 1 et 2 du CIM), occupés par les automatismes et la supervision, et le niveau Planification (niveau 4 du CIM), occupé par les Progiciels de Gestion Industrielle, comme la GPAO et plus généralement aujourd'hui les logiciels de type ERP (Entreprise Ressources Planification). Le MES, terme créé par le MESA au début des années 90, signifie Manufacturing Execution System, que l'on peut traduire en français par « Système d'exécution des fabrications ». Les différents domaines se distinguent non seulement par leurs fonctionnalités mais aussi par leurs échelles de temps : alors que la planification travaille au mieux à la journée ou à la demi-journée, le MES devra être capable de réagir dans des durées de quelques minutes. La figure 15 fait apparaître clairement que MES se situe au niveau de l'exécution. Il n'est pas un simple lien entre l'ERP et le contrôle commande, puisqu'il assure l'exécution des fabrications.

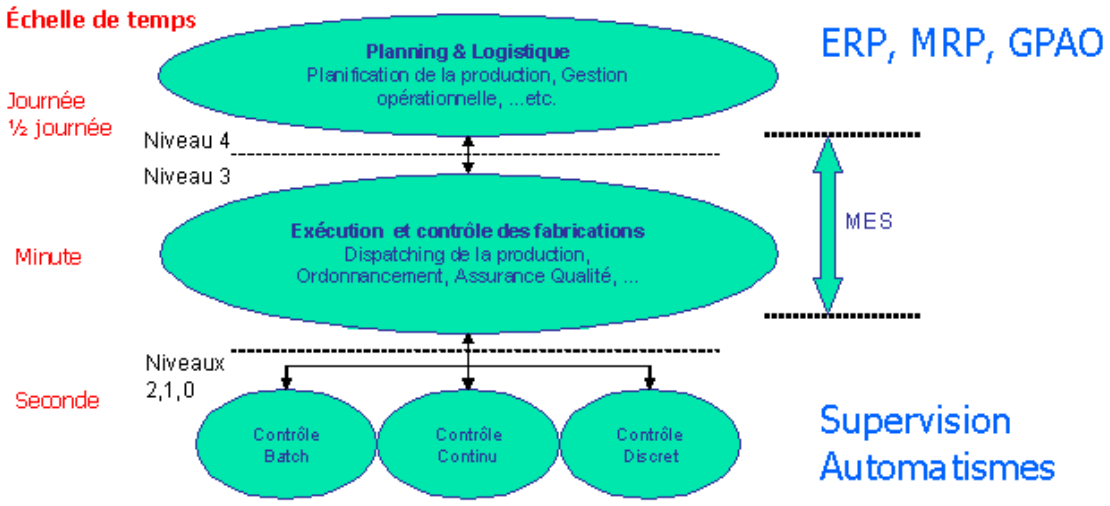


Figure 15 : Où se situe le MES ?

Dans cette perpétuelle évolution, nous pouvons décrire cet ensemble dans un plan vertical.

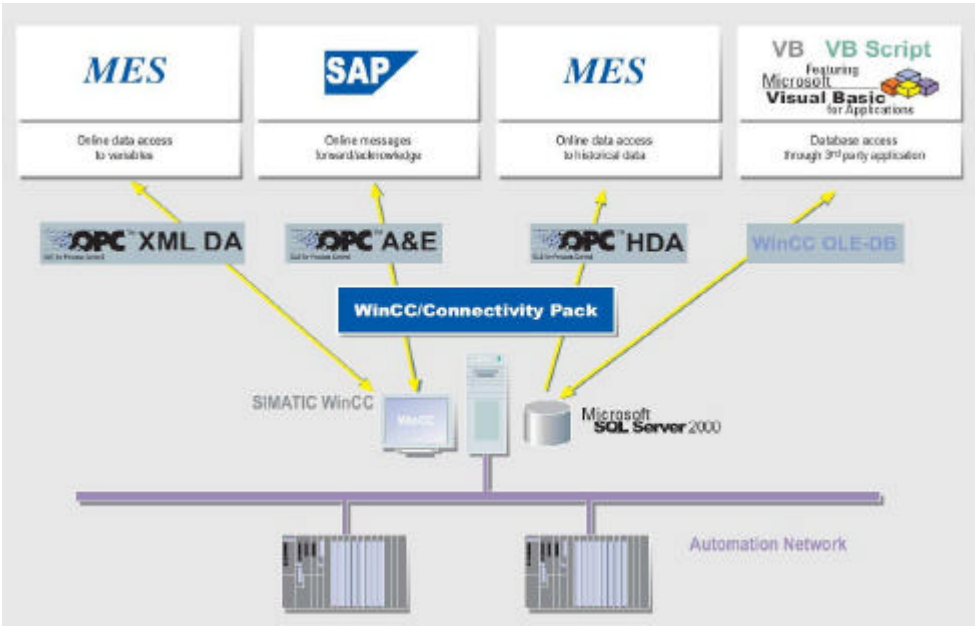


Figure 16 : Offre chez Siemens

3.9 Sécurisation des communications

La production manufacturée a augmenté au cours des années en se fondant sur une grande automatisation pour réduire les aléas de fonctionnement et augmenter la productivité. Il y a pression financière et commerciale pour l'adoption des technologies internet dans les automates. Une nouvelle génération de contrôleurs qui se connectent soit directement à internet soit communiquent en TCP/IP est disponible depuis quelques années. Il y a un réel besoin d'ouverture des systèmes de commande et de supervision de processus industriels sur internet. C'est pourquoi les constructeurs d'automatismes ont conçu de nouvelles plates-formes pour automatismes, ouvertes et basées sur les technologies de l'internet, telle que TCP/IP. Les méthodes de transmission de données employées dans l'internet ont été conçues pour transmettre principalement des messages de type texte avec des contraintes d'intégrité relativement basses. Les applications traditionnelles n'ont exigé aucune

amélioration fondamentale. Cependant, de nouvelles applications d'internet emploient la transmission de données dans les tâches distribuées qui exigent une intégrité plus élevée. Les applications de sûreté incluent :

- télésurveillance, diagnostic, commande et entretien.

Ces systèmes intégrés couvrent la production et l'administration (présentant de ce fait de nouvelles vulnérabilités); édition d'informations sécurisées.

Ce problème de la sécurité des accès est actuellement un réel frein à l'implantation de ces architectures dans l'industrie [14].

La gestion des cyber-risques demeure une question culturelle. Pendant que les normes et les standards se développent, que les technologies deviennent matures, c'est bien dans l'organisation et l'éducation que se fait «la différence » entre ceux qui parviennent à être efficaces et cohérents et les autres.

3.9.1 Cadre légal incontournable

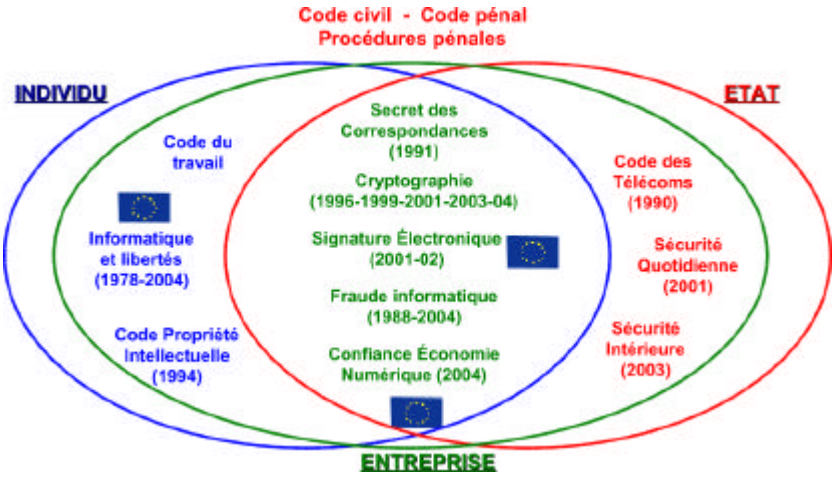


Figure 17 : Le cadre légal en terme de sécurité [13]

3.9.2 Des cyber-risques quotidiens

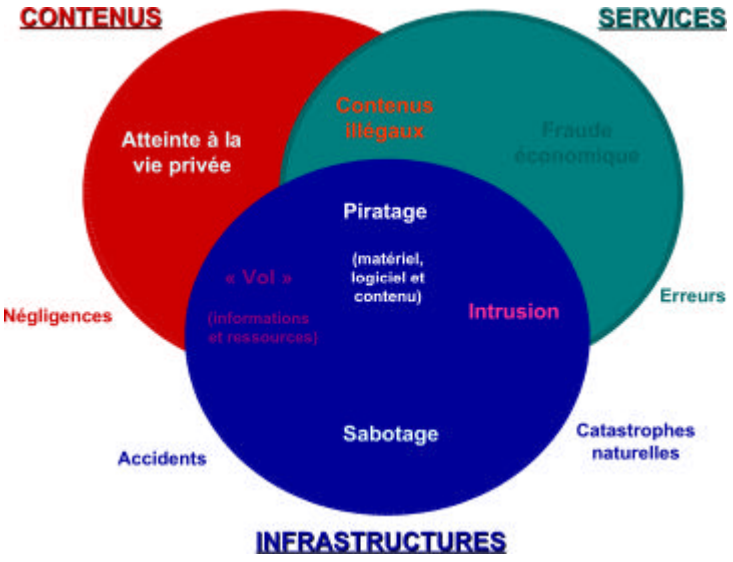


Figure 18 : Les cyber-risques [13]

3.9.3 Un management par des enjeux

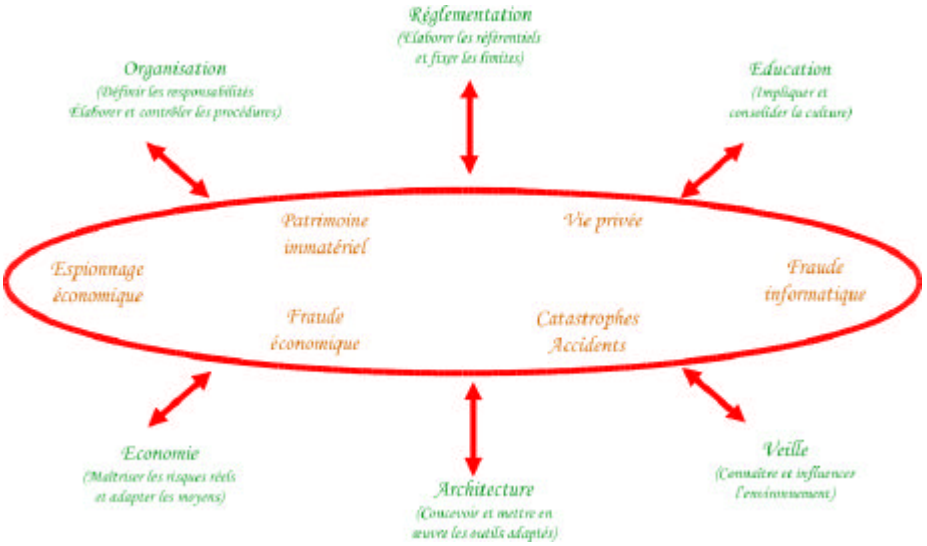


Figure 19 : Management par projet [13]

3.9.4 Des nouveaux acteurs de la sécurité

Le correspondant à la protection des données personnelles [29] **:**

- 40% des entreprises en disposent déjà,
- décret en attente depuis la loi du 6 août 2004,
- une fonction à risque (indépendance, délégation pénale,...).

Le superviseur-enquêteur des attaques logiques :

- indépendant des opérations « SSI »,
- focalisé sur les attaques intrusives, dénis de services, vers informatiques,...
- dûment formé sur les conditions d'intervention (en interne, en externe).

Le pilote de l'intelligence économique (défensive) :

- un relais entre les fonctions de veille et sécurité de l'information,
- un éducateur permanent sur les menaces réelles touchant tous les secteurs d'activité.

Le monsieur « crise » :

- effet post 11 septembre,
- un organisateur au cœur des métiers.

3.9.5 Principaux types d'attaques

Une organisation/entreprise est plus susceptible d'être attaquée si elle est connue et reconnue. Puisque ces nouveaux produits utilisent la technologie connue de l'internet, ils peuvent bénéficier de l'expérience que les développeurs web ont accumulé au fil des ans. Comme ces automates contrôleront et surveilleront des process industriels, ils devraient au moins résister à tous les types d'attaque recensés jusqu'ici. Le CERT (Computer Emergency Response Team) [52] a enregistré de nombreuses vulnérabilités des serveurs webs.

- ***Virus :*** un virus est un programme qui se réplique et se distribue sur votre ordinateur. Il n'est pas tout le temps agressif, mais il peut se répliquer jusqu'à ce que votre ordinateur soit tellement infecté qu'il soit inutilisable (par exemple disque dur plein). Quelquefois, un virus peut avoir un fort potentiel destructeur et par exemple détruire toutes les données de votre ordinateur. Une nouvelle variante de virus se sert des vulnérabilités dans les systèmes d'exploitation et les langages de script inclus dans les applications telles que des navigateurs internet, des outils de bureau, les clients de mail. Le virus « Lovebug » était un script malveillant qui a tiré profit d'un service appelé Active Scripting de Outlook. Ce type d'attaque est susceptible de devenir plus fréquent. Les systèmes d'exploitation Windows sont plus enclins à ces deux dernières attaques qu'Unix. Notez qu'Unix n'est pas nécessairement en soi plus sûr à cet égard, mais plutôt que Windows, plus répandu, est donc une cible plus attrayante et plus facile. Ceci pourrait changer bientôt avec la popularité croissante des systèmes Linux.

- ***Chevaux de Troyes :*** un cheval de Troyes est un programme qui ne se duplique pas, mais qui provoque des dommages ou menace la sécurité du système. Généralement, il est envoyé par courrier électronique par une personne, mais ne s'envoie pas automatiquement. Un cheval de Troyes peut arriver déguisé sous la forme d'un utilitaire. Certains chevaux de Troyes ont des effets malveillants sur l'ordinateur sur lequel ils sont exécutés, alors que d'autres, comme Back Orifice, fournissent des fonctionnalités de contrôle à distance aux pirates.

- ***Assauts par sniffage :*** de nombreux analyseurs de protocoles permettent d'utiliser une station "normale" du réseau afin de la transformer en véritable système d'analyse de LAN. En surveillant les paquets de données du réseau au niveau de la couche IP, il est possible de récupérer un grand nombre de mots de passe ou d'autres informations confidentielles en très peu de temps.

- ***Assauts par spoofing :*** l'IP spoofing est la technique la plus utilisée pour passer la protection des firewalls. Avec cette technique, la personne qui veut entrer illicitement sur le réseau remplace les adresses IP des paquets envoyés par des adresses d'utilisateurs autorisés. Cette forme d'attaque est particulièrement dangereuse lorsque le firewall identifie uniquement l'origine des paquets de données par leur adresse IP. Dans ce cas, le paquet de données est traité comme s'il venait d'un utilisateur autorisé et est transmis sur le réseau.

- ***Assauts ICMP :*** le protocole ICMP fait partie de la pile de protocoles TCP/IP et sert, entre autres, à indiquer les erreurs et messages de diagnostic à l'envoyeur d'un paquet. Il peut ainsi réagir à cette erreur. Dans la plupart des cas, la réaction de l'émetteur est immédiate et automatique. Une personne mal intentionnée peut donc être en position de manipuler des systèmes informatiques spécifiques sur le réseau.

- ***Attaques DoS :*** une attaque de DoS (Deny Of Service) (et une attaque DoS distribuée c'est à dire une attaque «many to one») n'entre pas nécessairement dans le réseau ou ordinateur accueillant un service, mais empêche ce service d'accomplir efficacement sa tâche. Une manière de faire ceci est d'inonder le système avec des demandes fausses, de ce fait encombrant le système pour des demandes légitimes. Un autre type de déni de service consiste à tirer profit de failles de sécurité connues du système. Par exemple, on a récemment découvert que si «Microsoft Information Server» reçoit une demande mal formée contenant beaucoup de suffixes (par exemple www.company.com/this.is.wrong.this.is), il dépense alors beaucoup d'efforts pour rechercher dans sa base de données les suffixes. Si de nombreuses demandes mal formées sont reçues, le serveur est ainsi monopolisé pour résoudre les demandes, ayant pour résultat un déni de service aux utilisateurs légitimes.

- ***Hopping :*** le hopping est une technique consistant à « sauter » d'un système informatique distant à un autre. De cette manière, les options disponibles sur le premier système sont employées pour gagner l'accès à l'autre système informatique. Dans beaucoup d'applications, telles que la maintenance à distance par exemple, il est possible d'accéder au système informatique à distance, ce qui constitue une véritable "porte d'entrée".

3.9.6 Solutions et parades

Les principales solutions ne diffèrent pas beaucoup des solutions mises en oeuvre pour la sécurisation de réseaux Ethernet « non industriels ». Ils reposent sur une combinaison de différents types de protections telles que les firewalls, la mise en place de mots de passe, etc ...

- ***Les firewalls :***

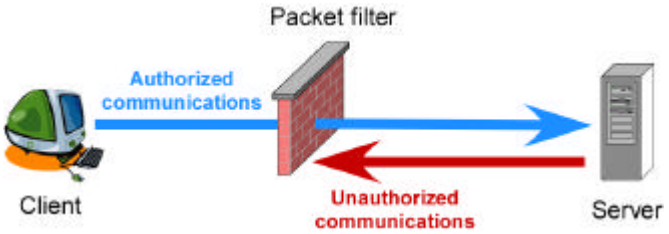


Figure 20 : Rôle du firewall

La fonction principale d'un firewall est de permettre aux personnes autorisées d'un réseau privé, l'accès au réseau internet. Il doit aussi empêcher toute personne non autorisée de s'introduire sur le réseau privé. Il est composé à la fois d'éléments logiciels et d'éléments matériels, qui doivent être configurés afin de bloquer les ports non utiles, et contrôler l'accès des ports utilisés. Si par exemple la supervision d'un processus automatisé n'est nécessaire qu'à l'intérieur du réseau privé, il est possible d'en fermer l'accès depuis internet. Si la supervision par internet est nécessaire, il est possible de n'ouvrir que les ports nécessaires à la supervision, et uniquement vers l'adresse IP de l'automate hébergeant cette application. Si nécessaire, il est également possible de vérifier l'adresse MAC du client cherchant à se connecter, afin de prévenir toute tentative de "spoofing" visant à se faire passer pour un utilisateur du réseau local alors que l'on est extérieur. Ainsi, l'efficacité de firewall repose sur l'application d'une politique de sécurité, qui consiste en un certain nombre de règles formelles. Elles déterminent quelles sont les actions autorisées, et de quel côté (du réseau intérieur ou extérieur) une connexion peut être établie. Ce mécanisme permet donc de vérifier tous les paquets de données, et donc de les laisser passer ou de les renvoyer. Avec ce principe, tout ce qui n'est pas expressément autorisé est donc refusé.

- ***La protection par mots de passe :*** Les firewalls sont efficaces uniquement lors d'attaques venant de l'extérieur de l'entreprise. Pour s'assurer que toute tentative d'intrusion sur un système depuis "l'intérieur" soit vouée à l'échec, il est nécessaire de mettre en place des mots de passe, avec un politique de gestion des droits d'accès aux différents composants du réseau. Il est en effet inutile de mettre en place un firewall si l'ensemble du réseau est accessible depuis n'importe quel poste informatique de l'entreprise. Les droits d'accès doivent êtres définis précisément pour chaque catégorie de personnel, et les mots de passe ne doivent pas êtres triviaux. Cela permet de se protéger notamment des tentatives d'attaques par sniffage, qui requièrent un accès direct au réseau. Un sniffer pourra permettre de mettre en évidence tous les paquets passant par le réseau. Il affichera les trames passant sur le réseau en vu de détecter d'éventuelles anomalies sur celui-ci.

- ***Attaques utilisant les virus et les failles de sécurité :*** ce type d'attaque est particulier, puisqu'il vise un type de matériel (ou logiciel) défini. Les virus et chevaux de Troyes sont, par exemple, spécifiques à un système d'exploitation. Il en est de même pour les attaques par les failles de sécurité. Les risques de voir un système automatisé attaqué par un virus est donc de ce fait assez faible. En effet, la proportion de systèmes de ce type sur internet est extrêmement faible par rapport à la proportion de systèmes Windows et Unix. De plus, le développement d'un virus demande une bonne connaissance de l'architecture du système attaqué. Or, les informations sur l'architecture interne des automates sont très peu répandues. Cependant, cette éventualité n'est pas nulle. En effet, un virus peut spécialement être développé dans le but de nuire à une entreprise en particulier dans le cadre, par exemple, de la concurrence entre deux grosses firmes. Il n'y a actuellement pas vraiment de protection spécifique à

ce type d'attaques, vu leur probabilité extrêmement faible. La seule solution est la mise à jour du microprogramme de l'automate programmable industriel, une fois une faille détectée.

- ***Autres protections :*** un **IDS** (Intrusion Detection System) est un dispositif de sécurité détectant les tentatives d'intrusion ou les événements suspects similaires sur un système informatique. Ce type de produit est principalement proposé par Cisco et ISS. Il peut s'agir d'un logiciel ou d'un boîtier externe (appliance). Un **HIDS** (Host based IDS) surveille les intrusions sur un serveur, un **NIDS** (Network based IDS) surveille l'activité des machines sur le réseau en capturant les trames échangées.

3.10 Solutions innovantes de services

Dans les applications RENAULT, le pupitre de Contrôle-Commande inclut un ensemble logiciel pour l'aide au diagnostic / redémarrage, et le suivi des moyens, un atelier de conception étant proposé aux OEM (Original Equipment Manufacturer, fabricant du matériel d'origine) pour le paramétrage de l'ensemble. Dans les applications PSA, le pupitre est proposé avec des prestations intégrées : simulation, contrôle du temps de cycle machine, paramétrage du suivi des moyens [31].
La réduction des temps de diagnostic fait partie des obligations actuelles. De nombreux exemples montrent l'intégration d'outils basé sur les technologies web. Pour exemples, pour accroître la productivité de son nouvel outil de production en réduisant les temps liés au diagnostic des dysfonctionnements, FBFC (Groupe AREVA) a doté ses équipes production d'un Système d'Aide au Diagnostic global (SAD) comprenant aussi bien la partie automatismes que la partie électricité. Pour un tel système, les critères prépondérants de choix sont : le coût, la sécurité et la facilité de mise à jour lors des évolutions des équipements. L'intégration d'outils d'aide au diagnostic basée sur des technologies Web répond à ces critères. Témoignage Olivier Allègre : AREVA-NP / FBFC / Direction technique Responsable Electricité, Automatismes, IHM.

« Le duo ThinPLC /SeeDiagramAnimator répond à tous ces critères :

- *le coût d'investissement est limité,*
- *les équipes de production ne peuvent pas modifier les automatismes,*
- *la mise à jour de la partie automatismes est rendue automatique à partir de la version sauvegardée par l'automaticien,*
- *la mise à jour de la partie électricité est très simple et tout écart entre deux mises à jour est signalé.*

La solution apporte également bien d'autres avantages :

- *la consultation des schémas électriques est grandement facilitée,*
- *la quantité de papier introduite en zone nucléaire contrôlée est réduite (gestion des déchets simplifiée pour les schémas électriques),*
- *grâce à la technologie client WEB, les postes de consultation du SAD sont banalisés et ne nécessitent aucune configuration particulière,*
- *grâce à la technologie client WEB, tous les acteurs du site ont accès au même référentiel technique (maintenance centrale, méthodes) que les équipes de production,*
- *grâce à la technologie client WEB, les écrans de diagnostic sont intégrés aux systèmes de supervision du site.*

Voici les principales raisons pour lesquelles FBFC a choisi de faire confiance aux solutions proposées par Anyware Technologies.»

Le marché du M2M (Machine to Machine) est en passe d'exploser d'ici 2010 ! pour un grand nombre d'acteurs [32]. Le secteur du Machine-to-Machine est promis à une croissance annuelle de 49%, selon le cabinet Idate. Les segments les plus prometteurs sont la gestion de la chaîne logistique ouverte, les systèmes de télé-médecine et les solutions de gestion de l'énergie. Ce marché du M2M regroupe les solutions permettant aux machines de communiquer avec un serveur central sans intervention humaine. Selon l'Idate, centre d'études et de conseil, il pourrait représenter au niveau mondial plus de 220 milliards d'euros en 2010, soit une croissance annuelle de 49%.

Pour l'Idate, il s'agit d'un marché en plein essor, poussé par des dynamiques favorables au niveau technologique et économique, voire réglementaire. Son développement variera en fonction du secteur d'activité. Les secteurs de la logistique, de la grande distribution, des « utilities » comme la gestion en distribution de l'eau, du gaz et de l'électricité. Les secteurs de la sécurité et de la santé figurent parmi les plus prometteurs.
Le marché potentiel du M2M se compte en milliards de machines et en centaines de milliards d'objets pouvant devenir communicants. En 2004, le nombre de modules M2M était de 92 millions d'unités, toutes technologies réseaux confondues. Ce nombre devrait, selon l'Idate, atteindre 500 millions d'ici 2010. Ils mettront en œuvre près de 2 milliards de machines et 100 milliards d'objets communicants, principalement des tags RFID (Radio Frequency Identification Device), avec les pilotes au niveau produit, dès 2009.

Les industries les plus avancées dans le domaine du M2M sont le transport pour la gestion de flotte et la télématique avancée (sécurité, secours, navigation dynamique…) et le secteur de la distribution de l'eau, du gaz et de l'électricité.

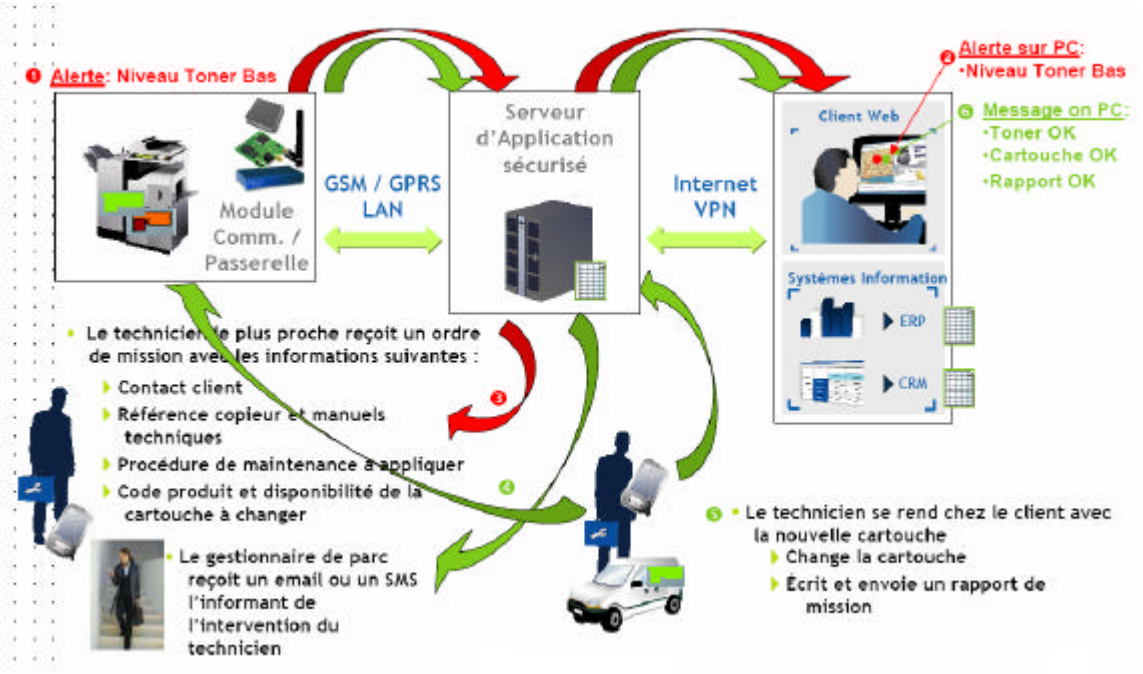


Figure 21 : Exemple d'une application M2M complète

4 APPLICATION : CAS D'ECOLE

Avant de rentrer dans le détail des travaux menés, je vous propose de faire un point sur les services innovants chez Siemens, base technologique hardware et software de travail pour la suite.

4.1 Solution innovante de services chez Siemens

4.1.1 Le service Sm@rtAccess

Principe : ce service permet l'accès aux données du processus depuis un endroit quelconque ainsi que la réalisation de solutions client-serveur peu coûteuses dans le domaine situé à proximité de la machine :

- concept Sm@rtClient,

- téléconduite ou télévisualisation d'un système IHM depuis un autre système IHM,
- communication entre systèmes IHM, accès en lecture et écriture aux variables d'autres systèmes IHM via le «protocole HTTP SIMATIC IHM»,
- intégration de pupitres à l'environnement MS Office. Accès en lecture et écriture de MS Excel aux variables d'autres systèmes IHM via «Simple Object Access Protocol» (SOAP) ,
- notion d'interface distribuée avec des vues identiques sur toutes les IHM,
- possibilité de gérer des discordances,
- par ce principe, une modification dans le serveur suffit à mettre à jour l'ensemble des clients.

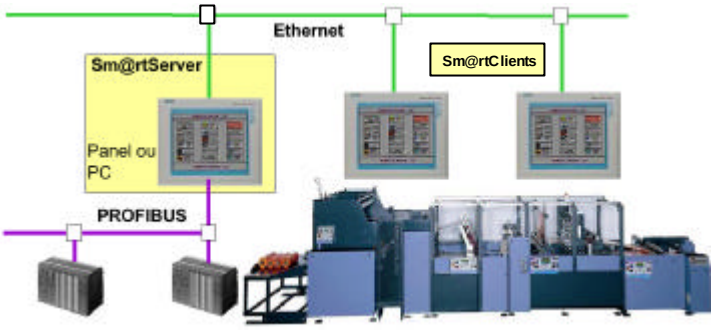


Figure 22 : Sm@rtServer et Sm@rtClients

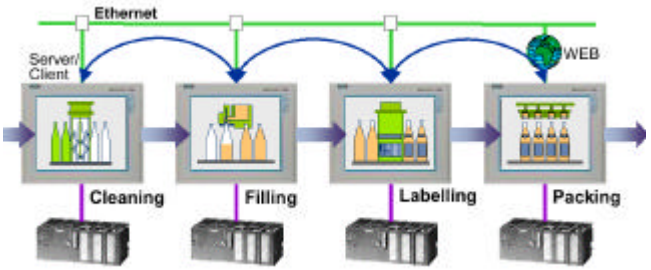


Figure 23 : L'accès aux variables process est possible en mode Client/Serveur

Cette solution permet l'accès à distance à toutes les variables d'un projet comme les variables d'un pupitre via leurs noms. Chaque pupitre est client et serveur d'un pupitre.

Dans cette orientation technologique, des stations d'opérateur(s) pourraient être Client d'un Serveur comme le montre la figure ci-dessous.

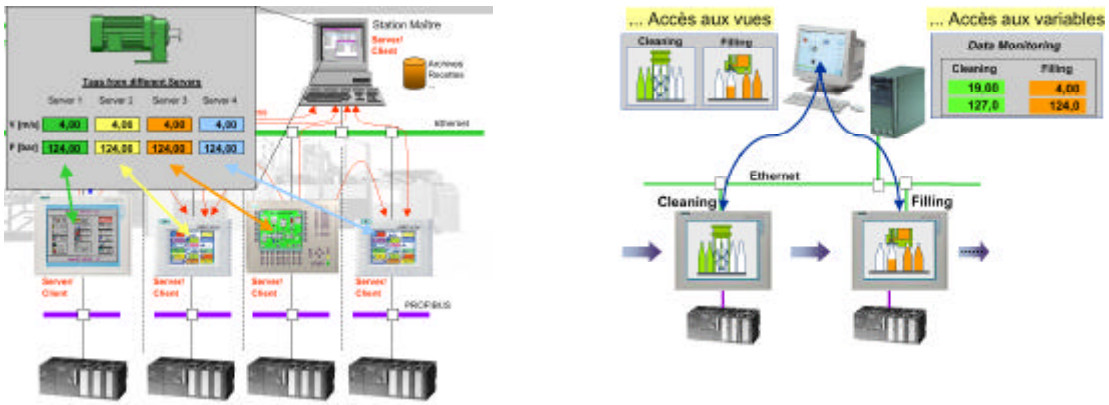


Figure 24 : Les vues, les variables sont accessibles à l'aide d'un PC connecté au réseau

Des liens sont possibles vers les applications de bureautiques par exemple Excel. Le Toolkit Microsoft SOAP [51] permet la visualisation et le contrôle de variables via Excel.

Dans ce concept, l'opérateur sur un poste local peut accéder aux variables à l'échelle de l'installation entière. Les postes opérateurs sont répartis. Il peut également s'inscrire dans une solution de type salle de commande locale avec possibilités d'archivage, d'analyse et de traitement de données du Process. L'intégration avec Office n'est pas nouvelle dans l'univers des solutions de développement pour les IHM. Le diagnostic et la maintenance via le WEB est plus originale.

4.1.2 Qu'est-ce que Sm@rtService ?

Sm@rtService permet de réaliser la télémaintenance de pupitres opérateurs pour une assistance via internet :

- téléconduite via internet/intranet,
- téléconduite d'un système IHM au moyen d'internet Explorer,
- accès aux informations d'assistance et de maintenance,
- mise à disposition de pages HTML standard sur le système IHM avec des informations d'assistance et de maintenance ainsi que des fonctions de diagnostic,
- assistance par e-mail,
- envoi d'e-mail sur la base d'alarmes et d'événements.

Ceci permet de réduire les temps d'inactivité imprévus et d'augmenter la productivité de l'installation.

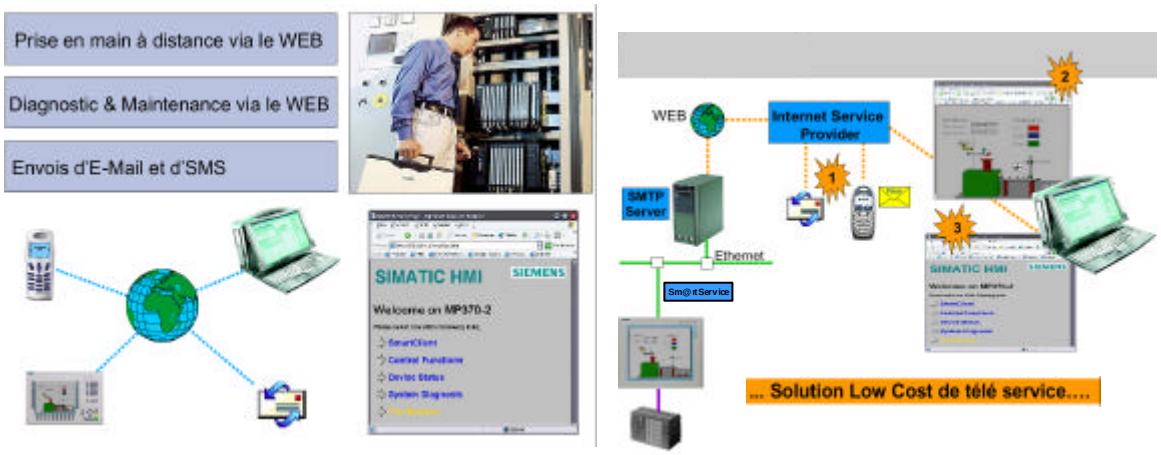


Figure 25 : Diagnostic et Maintenance via le Web

Dans ce concept de Diagnostic et de Maintenance via le WEB, l'agent en fonction des droits qui lui sont alloués peut gérer :

- des fonctions de pilotage pupitre distant,
- des fonctions bilan des états du process,
- des fonctions diagnostic système,
- des fonctions navigateur pour des dossiers,
- des pages HTML pour le développement personnalisé.

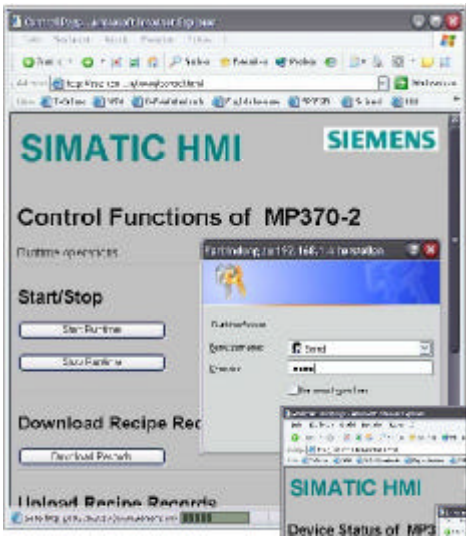


Figure 26 : Mots de passe pour le control à distance via le Web

Ce service est protégé par mot de passe avec une protection double :

- protection au niveau de l'accès via le Web,
- protection au niveau application,
- le « Download » du projet via internet est possible minimisant les coûts d'intervention,
- download / Upload Recettes (notion d'archives),
- paramétrage à distance de l'installation,
- consultation à distance de l'état du pupitre avec un pré-diagnostic efficace permettant d'agir rapidement,
- transfert en ligne des données de production (envoi de données archivées sans arrêt de production via le WEB).

Nous avons vu dans le paragraphe 3.3 que la compétitivité est le résultat de trois éléments indissociables aujourd'hui. Sm@rtService permet de gagner en productivité par élimination rapide d'incidents tout en minimisant les temps d'immobilisation d'une machine ou d'un ensemble de machines. Les interventions coûteuses sur place du personnel type SAV sont très fortement réduites.

4.2 Architecture de supervision du projet

L'architecture de supervision utilisée se décompose en quatre « niveaux » : le niveau internet, le niveau "entreprise" (réseau local), le niveau automatismes et enfin le niveau terrain.

4.2.1 Le niveau internet

Un poste client, n'importe où dans le monde, se connecte à l'adresse d'une IHM via le réseau mondial internet s'il y est autorisé.

4.2.2 Le niveau entreprise

Ce niveau est ici représenté par le réseau local de l'IUT de Châteauroux. L'accès à l'internet à partir de ce réseau est contrôlé par un routeur/pare-feu (le PIX515 produit CISCO page 3 du rapport) qui gère les accès externes (Renater[2] 34Mb/s sur fibre optique), interne à l'IUT, et donc vers l'automate programmable industriel (API) et les IHM. Le filtrage est effectué au niveau du pare-feu à l'aide de tables ACL (Access Control Lists). La table ACL se compose de lignes contenant les groupes d'utilisateurs et de colonnes faisant apparaître les droits de ceux-ci sous la forme d'en-têtes liés.

[2] Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche.

4.2.3 Le niveau automatismes

L'API Siemens comporte un coupleur Ethernet et un coupleur Profibus-DP. Il intègre également un serveur web et ftp, permettant la supervision à distance. Le CPU de l'automate implémente le programme de calcul permettant le pilotage du processus programmé. Un pupitre de commande et un bornier d'entrées/sorties est également présent sur le réseau Profibus-DP, pour la commande manuelle du processus (Voir figure 27).

4.2.4 Le niveau terrain

Le processus est piloté de façon distribuée entre l'API Siemens et le réseau Profibus-DP raccordé aux détecteurs, boutonnerie et aux actionneurs de la maquette.

Blocs de programme de l'API :

OB1 : Appel cyclique (Bloc d'organisation initial).

FC1 : Gestion des entrées et des sorties.

Entrées et Sorties :

Entrées TOR (carte 1 sur ET200S) :

I0.0 : Entrée recopiée dans la sortie A0.0

I0.1 : Incrémentation compteur MW50

I0.2 : RAZ compteur MW50

I0.3 : Validation rampe MW60 (rampe de 0 à 100 avec un pulse par seconde)

Sorties TOR (carte 2 sur ET200S (E/S sur Profibus-DP)) :

Q1.0 : Image entrée I0.0

Q1.1 : Clignotant 5 Hertz

Q1.2 : Clignotant 1 Hertz

Q1.3 : Clignotant 0,5 Hertz

Entrées analogiques +/- 10V (carte 3 sur ET200S (E/S sur Profibus-DP)) :

PEW256 : Entrée recopiée sur sortie ana PAW260 (variable MD70 dans l'IHM)

PEW258 : Entrée analogique sans traitement (variable MD74 dans l'IHM)

Sorties analogiques +/- 10V (carte 4 sur ET200S (E/S sur Profibus-DP)) :

PAW260 : Image entrée analogique PEW256

PAW262 : Image de la rampe MW60 (0 à 100% => 0 à 10 Volts)

Adresse réseau Ethernet :

Automate (API) : 10.0.2.60 (masque sous réseau 255.255.255.0)

IHM n°1 : 10.0.2.61 (masque sous réseau 255.255.255.0)

IHM n°2 : 10.0.2.62 (masque sous réseau 255.255.255.0)

Les éléments disposent d'adresses privées. Le routeur/pare-feu se charge de leur attribuer des adresses publiques et d'appliquer une « politique » de sécurité.

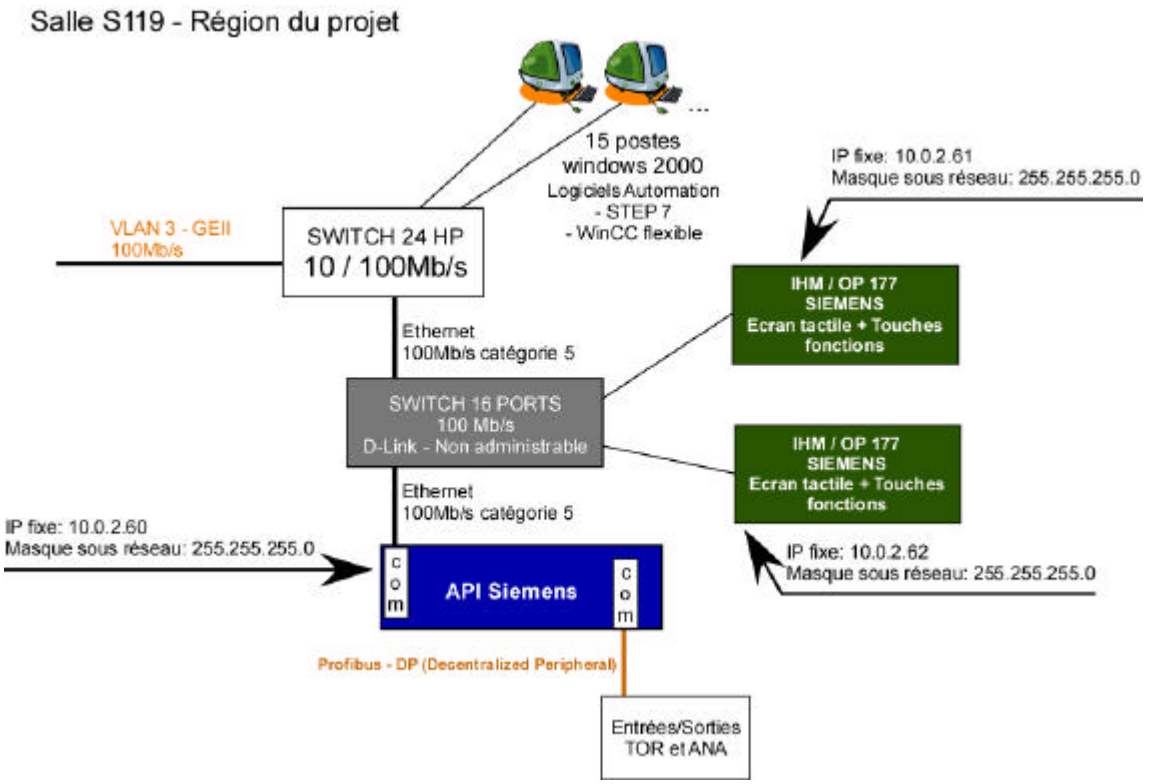


Figure 27 : Description détaillée de l'application matérielle

Photos des produits installés

4.2.5 Application de supervision pour IHM de type OP177 de chez Siemens

4.2.5.1 Présentation du matériel

Avant de détailler cette partie, voici en quelques lignes les caractéristiques de ce produit. Jusqu'à présent, la conduite et la supervision de petites applications étaient réalisées à l'aide d'afficheurs de texte simples.

Avec les SIMATIC TP 177B et OP 177B, nous pouvons disposer aujourd'hui de pupitres graphiques économiques d'entrée de gamme (350€ TTC logiciel compris pour les Universités). Les pupitres basés sur Windows CE avec 256 couleurs ou 4 niveaux de bleu se déclinent en différentes variantes et se prêtent à une multitude d'applications. Grâce notamment à l'outil de configuration innovant SIMATIC WinCC flexible et à l'interface Profinet.

Les points forts du produit :

- disponible avec 256 couleurs ou 4 niveaux de bleu,
- clavier à membrane et écran tactile (5,7" / 320 x 240),
- tampon de messages non volative (sans pile, donc sans entretien),
- touches de fonction configurables en tant que touches système et touches directes,

- processeur RISC et mémoire utilisateur 2 Mo plus mémoire de recettes intégrées,
- interface PROFIBUS embarquée, interface Profinet IO (12 Mbits/s), 1 x RS 232, 1 x RS 485 max,
- interface pour carte MMC standard pour la sauvegarde des données de recettes, de configuration et des données système,
- interface USB, par exemple : pour le raccordement d'une imprimante,
- certifications : CE, FM Class Div.2, UL, CSA, cULus, ATEX zone 2/22, Gost-R, C-TICK, autres en préparation.

4.2.5.2 Organisation des « pages écran » de l'IHM

L'objectif du travail accompli, n'est pas de développer un ensemble complexe mais de montrer les fonctionnalités de base sur des échanges respectant la notion de client/serveur (Voir figure 27). Ces pages ont été développées sous l'environnement Wincc Flexible 2005.

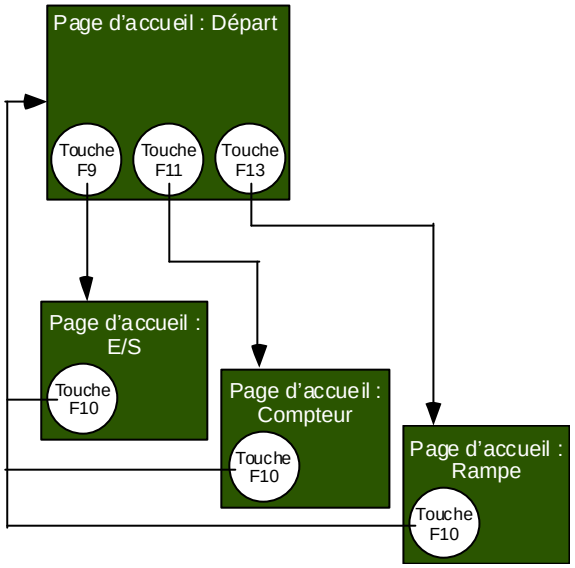
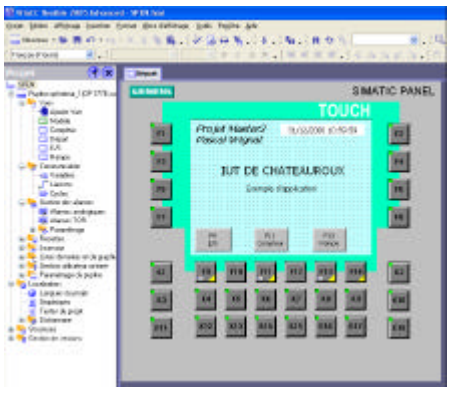
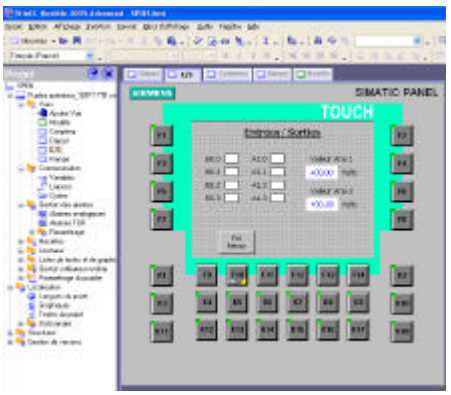


Figure 28 : Organisation des "pages écran" des IHM

Les clichés ci-dessous nous montrent le détail des pages réalisées. La page « E/S » permettra d'animer des objets graphiques en fonction de l'état logique des entrées/sorties tout-ou-rien (TOR) de l'API. Elle permettra également sur deux champs numériques d'indiquer les valeurs des entrées analogiques de l'API. L'IHM pourra incrémenter et remettre à zéro une valeur numérique dans l'API à l'aide des touches fonctions déclarées F1 et F2 dans la page «Compteur ». La page «RAMPE » permettra de gérer une rampe résultat d'un traitement numérique sur l'API. Les variables sont déclarées et détaillées figure 29.





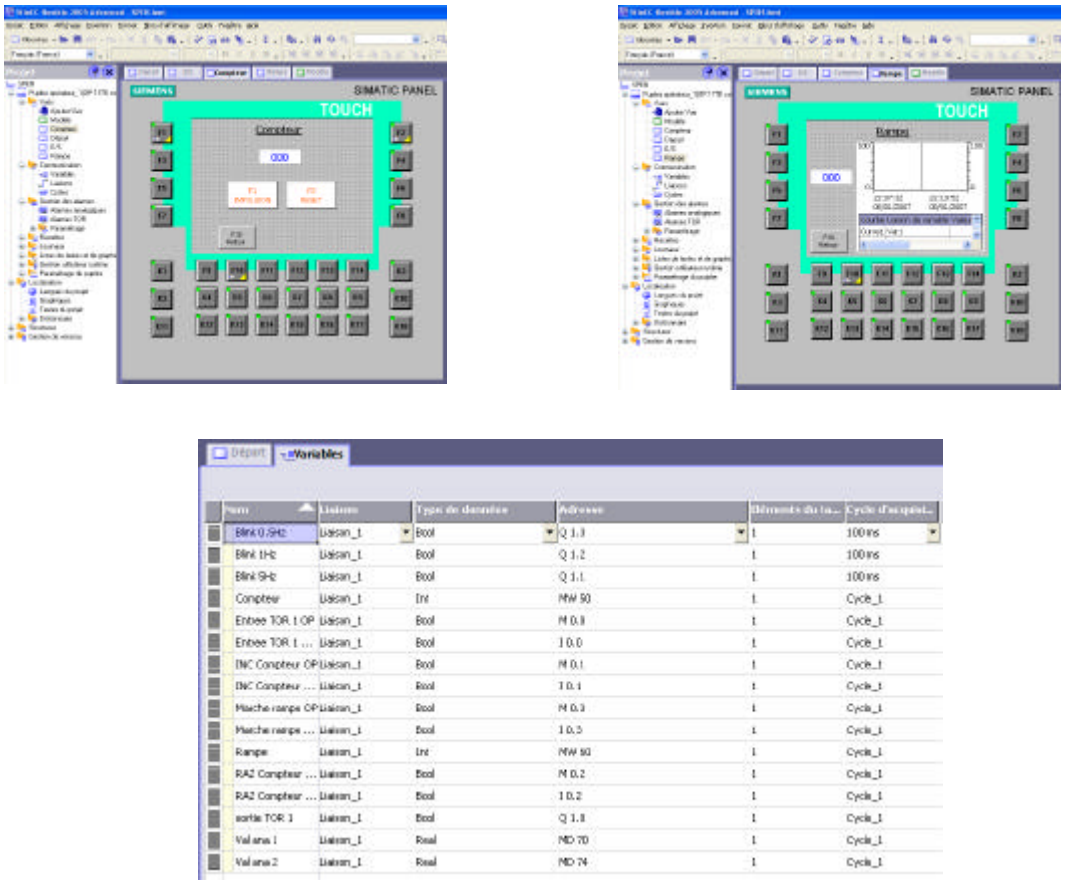


Figure 29 : Déclaration des variables

4.2.6 Organisation des réseaux de communications et respect des protocoles

L'arrivée d'Ethernet dans l'univers des automatismes ne date pas d'hier. Le consortium Profibus International, qui "gère" les évolutions du bus de terrain Profibus et sa bonne mise en oeuvre sur le terrain, s'est, dès la fin de 1999, posé la question des futurs rapports entre Profibus et Ethernet. Ainsi est né Profinet.

4.2.6.1 Installation du réseau et paramétrage des adresses IP

La normalisation internationale ISO/CEI 11801 et son équivalente européenne EN 50173, en tous points identiques, définissent un réseau informatique standardisé, indépendant de l'application et à usage bureautique, au sein d'un complexe immobilier. C'est dire qu'aucune ne tient compte des impératifs et spécificités du milieu industriel :

- cheminement des câbles subordonné à la topographie du site,
- niveau de mise en réseau spécifique à chaque machine ou installation,
- topologie bus,
- câblage et connectique robustes et pensés pour l'industrie :
    - respect des contraintes CEM (Compatibilité Electro-Magnétqiue),
    - de température et d'humidité,
    - protection contre la poussière et les vibrations.

C'est pourquoi Profinet définit dans son « Guide d'installation » un câblage industriel Fast Ethernet basé sur les spécifications de la CEI 11801 [33]. Comme le montre la figure 27, la couche 1 du modèle OSI est réalisée à l'aide d'un support cuivre blindé de catégorie 5.

Dans la plupart des cas, les ordinateurs personnels n'ont pas une adresse internet fixe car il n'y a pas toujours d'adresses disponibles pour l'ensemble des utilisateurs potentiels à un moment donné. Les adresses sont donc attribuées aux utilisateurs pour la période où ils se connectent et libérées dès la fin de la connexion. Schématiquement, lors de la première connexion de l'ordinateur « client », le fournisseur d'accès affecte une adresse internet (adresse IP) pour une certaine période de temps. Passée cette période l'utilisateur peut être déconnecté et cette adresse réaffectée à une autre machine. Lors d'une utilisation ultérieure, une nouvelle adresse internet lui sera allouée. Ceci explique qu'il est difficile d'avoir un serveur Web personnel, d'établir une communication audio-visuelle ou une relation directe entre membres d'une petite communauté, sans disposer d'une adresse fixe ou sans passer par un serveur relais disposant lui d'une adresse fixe (par exemple un fournisseur d'accès). Une solution possible est d'attribuer des adresses IP fixe via DHCP[3]. DHCP est avant tout conçu pour configurer dynamiquement les stations, en exploitant au mieux une réserve d'adresses IP, distribuées aux clients du réseau. Pourquoi alors, passer par DHCP plutôt que de configurer la machine directement ? Il y a au moins deux bonnes raisons :

- vous pouvez le faire de façon centralisée, sans avoir à vous déplacer de poste en poste,
- toutes les options : DNS, passerelle etc. restent configurées dynamiquement, ce qui vous évitera d'avoir à intervenir sur les machines si vous changez la topologie de votre réseau.

Le souci majeur est le suivant :

- si le serveur tombe en panne, l'ensemble des communications est interrompu ce qui pose un problème majeur pour la continuité de services obligatoires dans le cas d'applications industrielles.

La parade est l'organisation suivante proposée sur la figure 30.

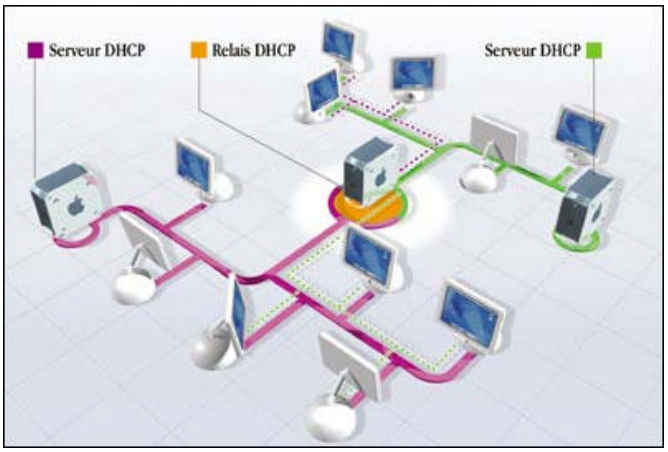


Figure 30 : Pour limiter « la casse » en cas de panne, on peut répartir les adresses affectées à des sous-réseaux distincts sur plusieurs machines, afin d'assurer au moins une partie du service sur chacun des sous-réseaux.

[3] Dynamic Host Control Protocol

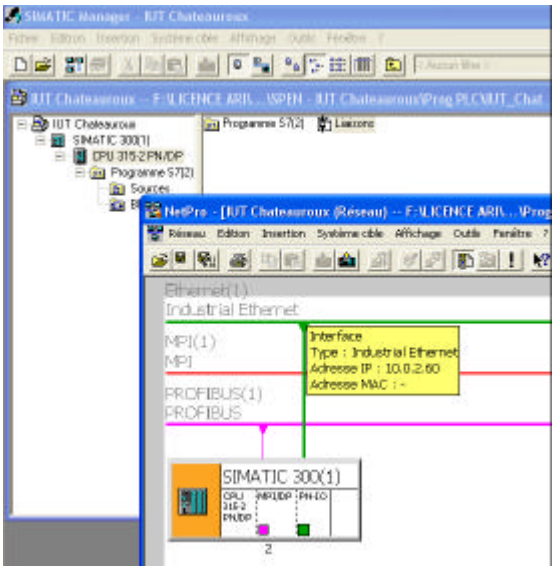


Figure 31 : Adressage IP de l'API sur le réseau Ethernet avec le logiciel Step7

L'adressage IP des IHM sera configuré individuellement dans le système d'exploitation Windows CE hébergé par chaque OP 177.

Pour rappel [34] :

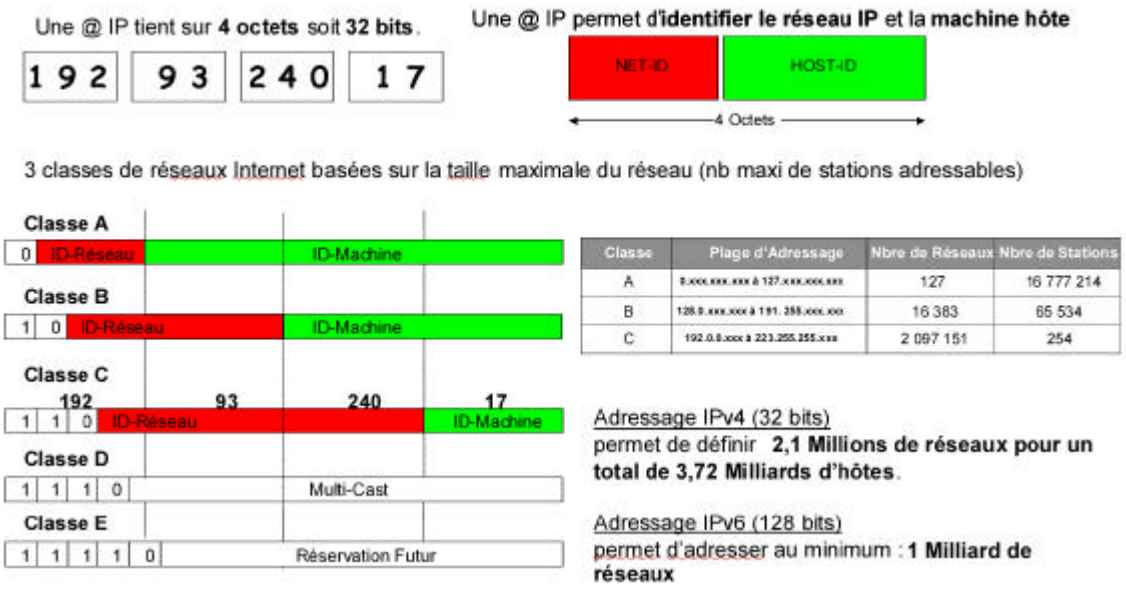


Figure 32 : Adressage IP et Classes de Réseau internet

4.2.6.2 Communication sur Ethernet Industriel : Profinet

Répondant à la norme CEI 61158, PROFINET se base sur le standard international Ethernet (IEEE 802.3) et mise de manière systématique sur Fast Ethernet à 100 Mbits/s et sur la technologie de commutation. Ethernet s'échelonne sur trois niveaux de performance :

- TCP/UDP et IP pour les échanges sans exigences temps réel (paramétrage et configuration),
- Le temps réel logiciel SRT (Soft Real Time) pour les données process à temps critique utilisées en automatisation industrielle,

- le temps réel isochrone IRT (Isochronous Real Time) pour des applications pointues comme la commande et la synchronisation d'entraînements (Motion Control).

Ces trois échelons couvrent toutes les applications d'automatismes. Parmi ses caractéristiques clés, citons [35] :

- la coexistence de transmissions temps réel et TCP/IP sur une seule ligne,
- un protocole temps réel standardisé pour toutes les applications et la communication aussi bien entre composants intelligents décentralisés qu'entre contrôleur et périphérie décentralisée,
- une communication temps réel évolutive, de performante à ultra-performante, avec synchronisation d'horloge.

La figure 33 positionne Profinet en fonction des exigences temps réel[4].

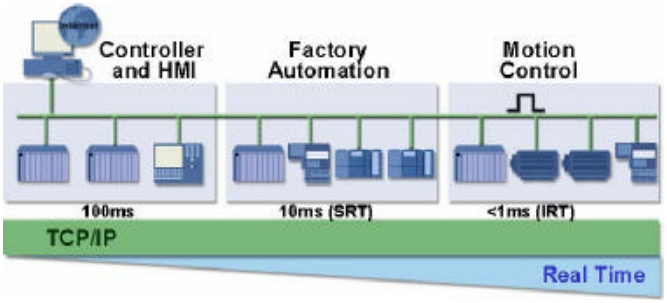


Figure 33 : Niveaux de performance de la communication Profinet en fonction des exigences temps réel

Ethernet et TCP[5]/IP sont les piliers de la communication Profinet. TCP/IP est en effet le protocole de communication du monde informatique. Néanmoins, en matière d'interopérabilité des applications, l'établissement d'un canal de transport TCP ou UDP commun (couche 4 du modèle OSI) sur les appareils de terrain ne suffit pas. En fait, TCP/IP ne fournit que le socle permettant aux équipements Ethernet d'échanger des données sur un canal de transport, dans des réseaux centralisés ou répartis. Il faut lui ajouter d'autres spécifications et protocoles au niveau applicatif, au dessus de TCP/UDP[6], tels que SMTP[7], FTP[8] et HTTP[9]. En effet, seule l'utilisation d'une même couche « Application » par l'ensemble des appareils est gage d'interopérabilité.

Pour satisfaire les contraintes temps réel de l'automatisation, Profinet net ne possède qu'un canal de transmission optimisé, dénommé Soft Real Time (Voir figure 34).

---

[4] En automatisation industrielle, les applications temps réel nécessitent des temps de réponse et de rafraîchissement compris entre 5 et 10 ms. On entend par « rafraîchissement» le temps nécessaire à la création d'une variable dans l'application d'un appareil, son envoi sur le réseau à un partenaire de communication, puis de nouveau sa mise à disposition de l'application, au niveau de ce même partenaire. Une communication temps réel doit ainsi gérer le traitement prioritaire du programme applicatif. L'expérience a pourtant montré que le temps de transmission d'une donnée sur une liaison Fast Ethernet à 100 Mbit/s (ou plus) est négligeable au regard du temps de traitement dans les appareils. Le temps nécessaire pour fournir cette donnée à l'application du producteur n'est pas affecté par la communication. Il en va de même du traitement des données reçues par le consommateur.

[5] Protocole de contrôle de la transmission émetteur-récepteur (absence d'erreur, séquence correcte et complète). TCP fournit un service sûr en mode connecté, une liaison devant être établie entre deux stations avant transmission, puis libérée au terme de l'échange. TCP intègre également des mécanismes de surveillance permanente de la liaison.

[6] Protocole de contrôle de la transmission émetteur-récepteur similaire à TCP, mais fonctionnant en mode non connecté et sans garantie de fiabilité (traitement de chaque paquet de données comme un seul message, sans accusé de réception). En l'absence de surveillance de temporisation ou d'établissement et de libération de la liaison, UDP est mieux adapté que TCP aux applications temps critique. Cette surveillance de la communication et du blocage des données, implicite dans TCP, peut s'effectuer sur UDP au niveau de la couche « applicative », par exemple avec RPC (Remote Procedure call).

[7] Simple Mail Transfer Protocol

[8] File Transfer Protocol

[9] HyperText Transmission Protocol

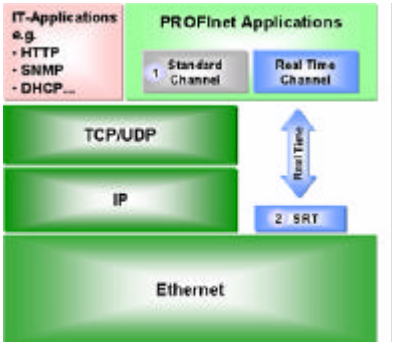


Figure 34 : Les différentes couches de la communication Profinet

Basé sur Ethernet (couche 2), il raccourcit considérablement le temps de traitement dans la pile de communication et accroît la vitesse Ethernet de rafraîchissement des données process. Tout d'abord, la suppression de plusieurs niveaux de protocole réduit la longueur du message; ensuite, la durée de préparation des données à la transmission et au traitement par l'application est écourtée. Parallèlement, la puissance de calcul réservée dans l'appareil à la communication est nettement allégée dans le cas de switchs[10] spécifiquement dédiés.

Profinet ne se contente pas de minimiser la pile de communication des automatismes programmables; il optimise aussi la transmission en attribuant à chaque paquet de données Profinet une priorité gérée conformément à la spécification IEEE 802.1Q. Les échanges entre appareils sont ensuite contrôlés par les constituants du réseau, en fonction de ces priorités : la priorité 6, accordée d'office aux données temps réel, l'emporte sur le traitement d'autres applications dont la téléphonie sur Internet, de priorité 5.

Hélas, cette solution ne suffit pas aux applications de positionnement et de synchronisme du Motion Control. Celles-ci exigent des temps de rafraîchissement de l'ordre de 1 ms avec une incertitude sur les tops de synchronisation (jitter) entre deux cycles consécutifs inférieurs à 1 µs, pour synchroniser un maximum de 100 noeuds. Pour satisfaire ces contraintes déterministes, Profinet a défini, au niveau de la couche 2 (Modèle OSI) de Fast Ethernet, une méthode de transmission contrôlée par tranche de temps. Grâce à la synchronisation d'horloge des participants du bus (constituants de réseau et appareils Profinet), avec la précision donnée plus haut, il est possible de réserver sur le réseau une tranche pour la transmission des données critiques de la tâche d'automatisation. Le cycle de transmission est donc segmenté en parties « déterministe » et « non déterministe » : les télégrammes cycliques temps réel sollicitent la tranche déterministe tandis que les télégrammes TCP/IP occupent la plage non déterministe. Tout comme si, par analogie avec la circulation autoroutière, on réservait la file de gauche au trafic express (temps réel) et confinait les autres usagers (transport TCP/IP) sur la file de droite, de sorte que les embouteillages sur ce côté de la chaussée ne ralentissent pas le trafic à temps critique (Voir figure 35).

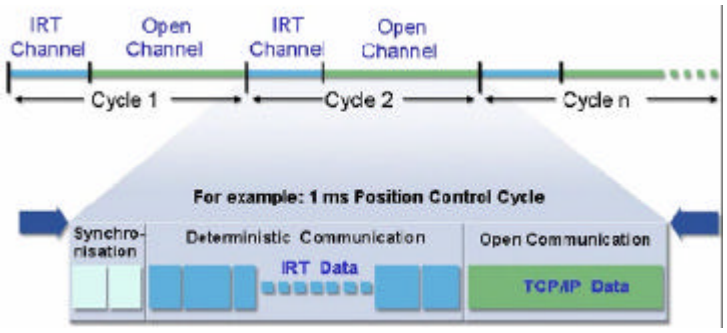


Figure 35 : Découpage temporel de la communication IRT en tranches déterministe et non déterministe

[10] Commutateur

La mise en oeuvre de cette transmission « isochrone » est matérielle : un circuit ASIC se charge de la synchronisation du cycle et de la réservation du canal temporel pour les données temps réel. Cette implémentation matérielle garantit la précision requise, dans l'ordre de grandeur souhaitée, et soulage le processeur de l'appareil Profinet des tâches de communication, libérant ainsi du temps de calcul pour l'automatisation elle-même.

4.3 Méthodologie de diagnostic des réseaux Ethernet industriels

L'activité d'un réseau est toujours occultée par le matériel qui nous fait face dans une application réseau : câble, connecteur, carte, interface, ordinateur, automate programmable, régulateur, variateur, et les nombreux logiciels enfouis ou développés par l'utilisateur pour ses besoins de contrôle/commande ou supervision, ...

Mais l'activité première d'un réseau est la gestion de la transmission de trames sur un médium d'accès souvent multiplexé et le codage physique binaire des trames souvent manipulées en hexadécimal. L'expert réseau industriel doit être capable de « parler le langage réseau » c'est à dire de comprendre ce qui circule sur le médium au plus bas des couches réseaux, la couche physique. Ce domaine s'appelle l'analyse de protocole et a pour objectif de fournir les moyens et méthodes de capture de l'activité réseau et d'analyse du trafic afin de voir « derrière le miroir » .... L'expert réseau doit connaître en détail le codage des trames supportées par le protocole analysé pour comprendre précisément la communication en cours. Néophytes s'abstenir sous peine de maux de tête violents !!!

Il est important pour un spécialiste réseau de pouvoir accéder directement aux contenus des trames échangés afin de connaître l'activité réelle du réseau à des fins :

- de diagnostic de fonctionnement du réseau,
- de mesure de performances,
- de calcul de temps de réponse,
- de compréhension des mécanismes de couche 2,
- surveillance et analyse du trafic réseau.

Les trames sont variées selon les caractéristiques du réseau, ces trames sont :

- de longueurs différentes de quelques bits (7 bits sur AS-i, de 256 octets sur Profibus à plus de 1514 octets sur Ethernet),
- de codage logique binaire différents allant de NRZ à Manchester différentiel,
- transmises dans des modes synchrones par blocs d'octets ou asynchrones par octet de formats,
- supportées par un médium de natures différentes : câble cuivre, Fibre optique, infrarouge, radiofréquence, courant porteur.

Pour exemple, la personne rattaché au service SSI[11] et qui est chargée d'intervenir sur site, avec ses connaissances et ses outils est un «Technicien Expert ». Lors de son intervention celui-ci est amené à étudier plusieurs éléments cités précédemment, et à rechercher les causes possibles de ce dysfonctionnement.

Celui-ci peut être, par exemple :

- la conception du schéma de principe de l'ensemble du réseau,
- la rupture ou le manque de qualité requise d'un câble,
- une charge trop importante à un nœud réseau,
- des paramètres applicatifs inappropriés, ex : une supervision avec des erreurs de paramétrage,
- ....

La figure 36 décrit l'enchaînement des différentes phases qu'un technicien est amené à suivre chez Schneider Electric [36] :

[11] Sécurité des Sytèmes d'Informations

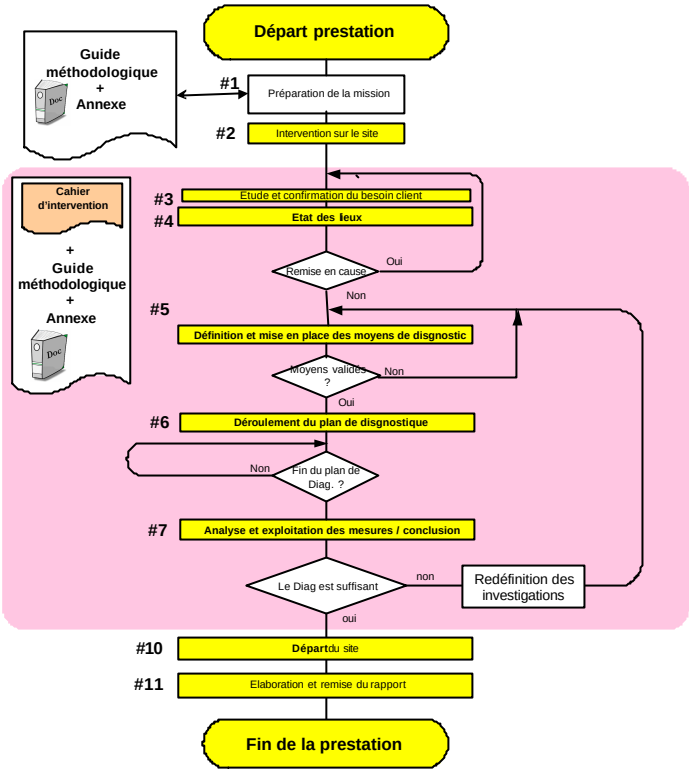


Figure 36 : Procédure de diagnostic réseau

Les différentes phases de l'intervention

#Phase 1 : Préparation

- Identification de l'intervention : fiche d'intervention
- Préparation et réservation des outils
- Préparation du cahier et des documents d'intervention

#Phase 2 : Intervention / aspect organisation sur le site client

- Prise en compte des contraintes client et des risques
- Organisation sur place

#Phase 3 : Etude et conf irmation du besoin client

- Vérification : analyser le problème et évaluer le besoin réel du client

#Phase 4 : Etat des lieux

- Analyse documentaire : étude de l'installation
- Analyse visuelle : vérification sur le terrain de l'existant

#Phase 5 : Définition et mise en place des moyens de diagnostic

- Définition du périmètre et des points de mesures
- Planification des travaux
- Elaboration du plan de diagnostic

#Phase 6 : Déroulement du plan de diagnostic au point de mesure

- Les travaux aux différents points de mesure prévus au plan de diagnostic

#Phase 7 : Analyse et exploitation

- Analyse et exploitation des mesures

#Phase 10 : Départ du site

- Donner au client la liste des travaux réalisés sur place
- Faire signer le procès verbal de fin d'intervention

#Phase 11 : Elaboration et remise du rapport

Les commentaires de l'expert ainsi que ses remarques sont relatés dans un rapport qui est remis par la suite au client. Dans ce rapport le technicien peut préconiser certaines interventions sur le réseau, ou des éléments du réseau.
Avant de présenter mes résultats sur cette partie de travaux, j'aimerais rappeler quelques définitions préalables.

4.3.1 Mécanisme d'encapsulation du modèle TCP-IP

L'empilement des protocoles selon les couches du modèle TCP-IP permet d'installer l'ensemble des services nécessaires à l'utilisateur d'un réseau [34] (Voir figure 37).

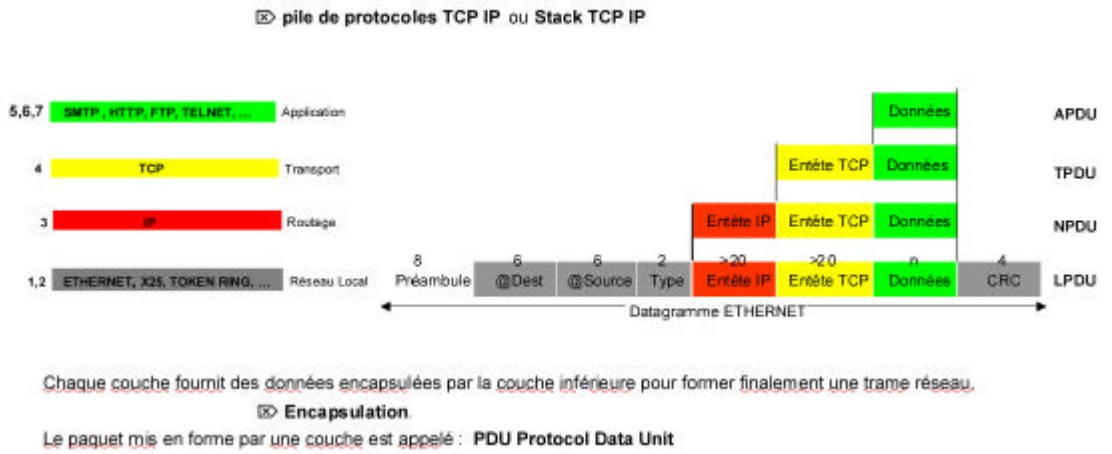


Figure 37 : Mécanisme d'encapsulation du modèle TCP-IP

4.3.2 Trame Ethernet-TCP-IP

La figure 38 résume les différents contenus d'une trame Ethernet-TCP-IP.

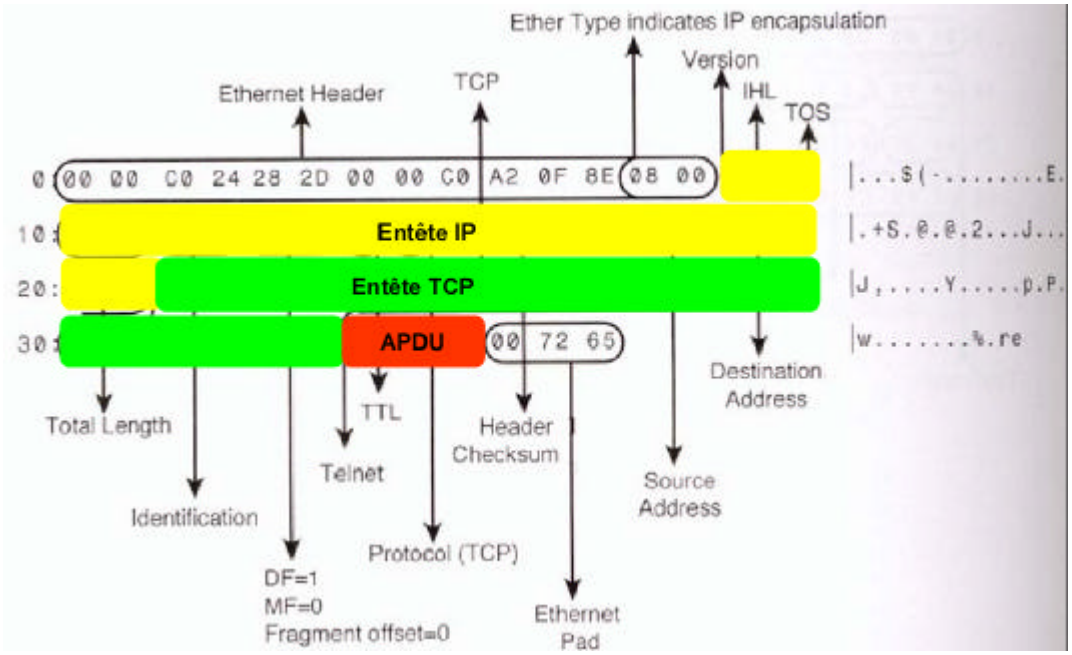


Figure 38 : Trame Ethernet-TCP-IP

4.3.3 Logiciels de diagnostic et d'analyse réseau appelé «Sniffer»

Au préalable et avant de se « lancer » dans l'utilisation de « sniffer », une simple commande Ping[12] peut permettre de savoir si un élément est connecté au réseau et si il répond. Cette commande envoie des paquets avec le protocole ICMP[13] vers l'adresse de la cible. Elle permet de vérifier les paquets reçus (32 octets de données ASCII[14] 'a' à 'z'...) et mesure le temps d'attente. Dans notre cas d'école, la figure 39 montre le résultat d'une commande ping sur les adresses 10.0.2.61 (une des IHM) et 10.0.2.64 (un élément non connecté au réseau).

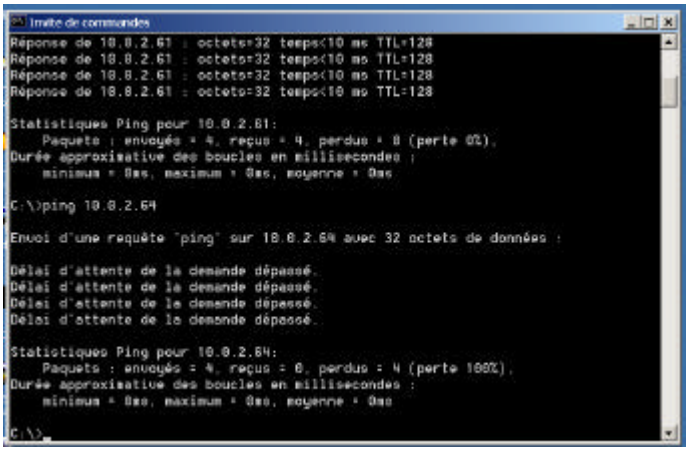


Figure 39 : Résultat d'une commande ping

Lors d'un diagnostic réseau, il est souvent utile d'observer les flux de communication et de les caractériser. Les outils d'analyse permettent d'observer les flux, de récupérer des trames particulières, au point de mesure. Ils permettent de réaliser des statistiques dynamiques sur les flux et les communications. Plusieurs outils logiciels existent sur le marché. J'ai souhaité en utiliser deux :

- Ethereal (Logiciel libre),
- NetAsyst (Version d'évaluation 12 jours).

Pourquoi ce choix ? Ethereal, outil d'analyse, est capable d'effectuer des captures de trames sur un réseau Ethernet. Il est très reconnu dans le monde de l'analyse réseau. Sa qualité première est sa mise a disposition sur internet gratuitement. Il est issu de la communauté des logiciels open sources LINUX. Il est composé de fonctions statistiques applicables sur l'ensemble d'une capture. Sa grande force est dans le traitement et la recherche de trames Ethernet. NetAsyst est un outil d'analyse également très utilisé mais payant. Il est capable :

- d'effectuer des captures de trames,
- de faire des statistiques en ligne,
- de générer des graphiques à partir de statistiques ou de flux de communication,
- de répertorier les protocoles et éléments présents sur le réseau.

L'analyse de trafic sur Ethernet est parmi les plus faciles. En effet n'importe quelle carte Ethernet peut fonctionner en mode dit «Promiscuitous[15] » et fournir ainsi toutes les trames circulant sur le segment auquel est raccordée cette carte. Une carte Ethernet standard se transforme en carte « espionne ». Dans le cas d'une configuration Ethernet en étoile sur hub[16], le poste analyseur de protocole peut être placé sur n'importe quel port du hub et capturer tout le trafic réseau. Dans le cas de configuration Ethernet commuté avec des switchs non admistrables, ceci n'est plus possible et il faut alors intégrer un segment de collision avec un hub pour y raccorder le poste sniffer. Ceci ne créant pas de

[12] Packet Internet Groper
[13] Internet Control Message Protocol
[14] American Standard Code for Information Interchange
[15] Une carte réseau fonctionne en « mode promiscuous » lorsqu'elle traite la totalité du trafic qui lui passe sous le nez.

perturbation majeure étant donné que l'analyse peut être totalement passive, ne générant aucun trafic supplémentaire sur le segment de réseau observé. Dans mon cas d'école, et compte tenu de l'organisation matériel implantée (Voir figure 27), j'ai intégré un segment de collision avec un hub (Référence : NUCOM NE 3116) car les switchs en place étaient non administrables.

Les paragraphes qui suivent décriront une plage de résultats obtenus avec deux logiciels « sniffer ».

4.3.3.1 Résultats obtenus avec NetAsyst

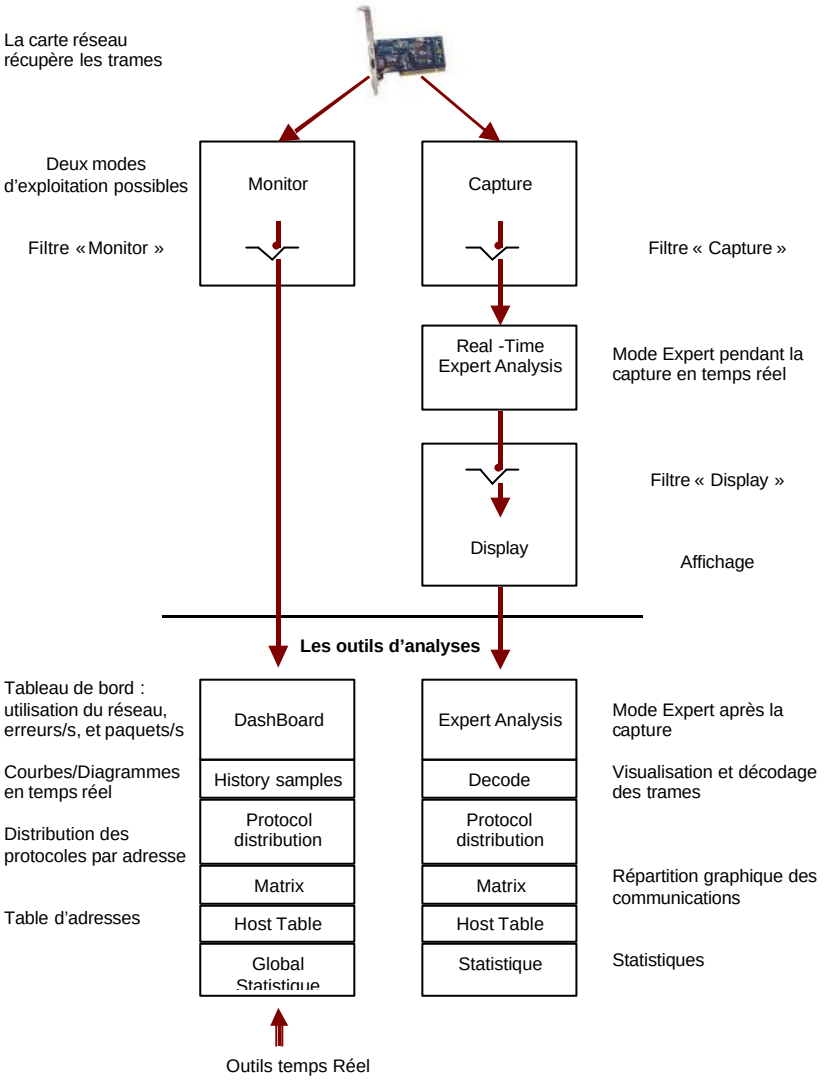


Figure 40 : Philosophie de fonctionnement

NetAsyst permet de pouvoir réaliser une étude du réseau sans avoir besoin de capturer des trames. Parmi les outils, la fonction « Matrix » permet de représenter graphiquement les interconnections entre les différents éléments connectés du réseau. Dans notre cas, l'API et des deux IHM sont bien interconnectés sur un protocole Ethernet (Voir figures 41 et 42).

[16] Concentrateur

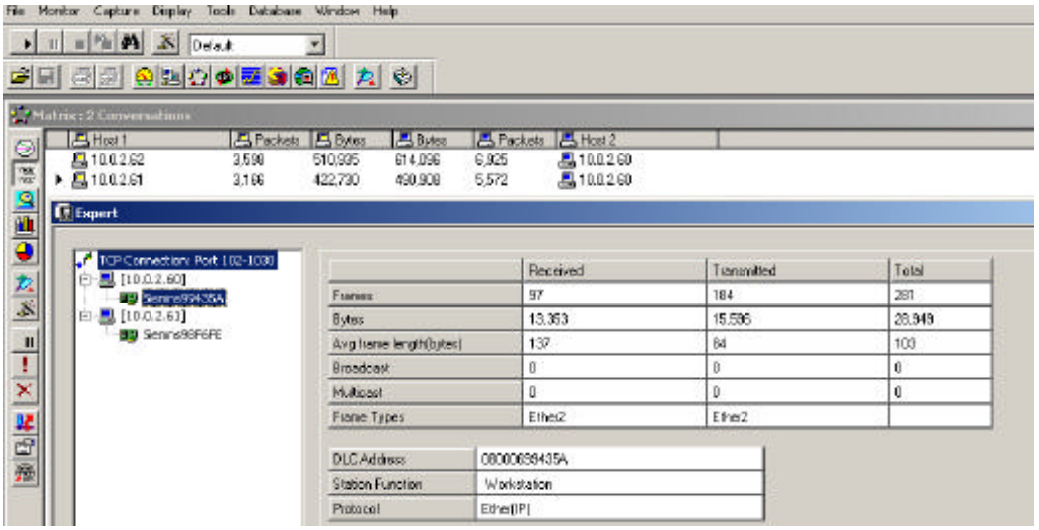


Figure 41 : « Sniffage » des interconnections

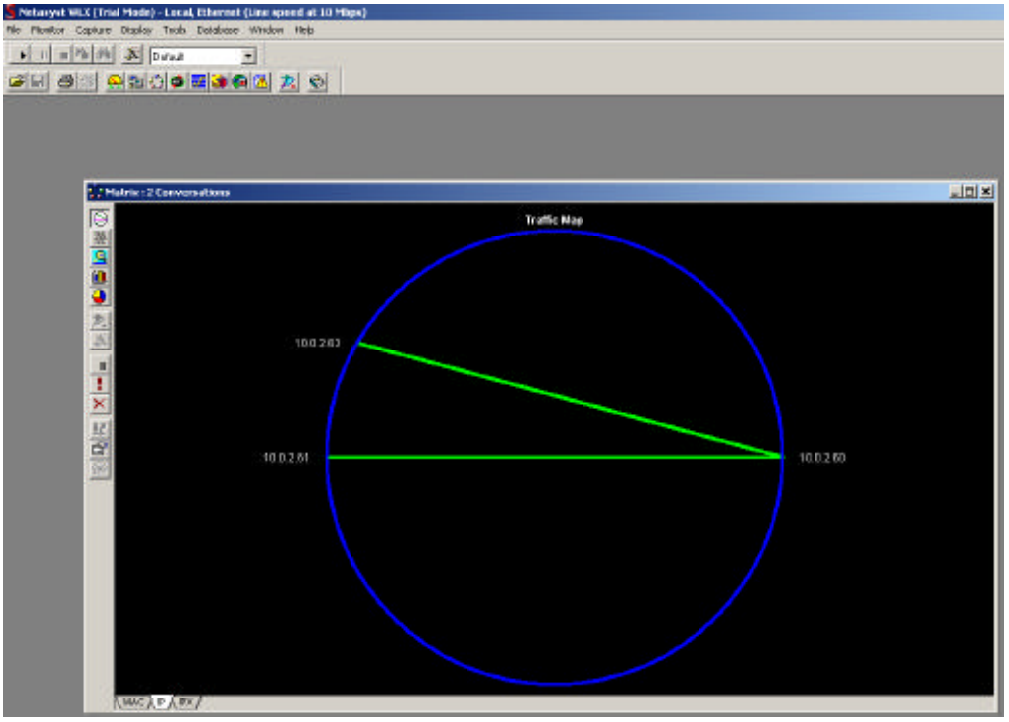


Figure 42 : Matrice des connections entre éléments connectés au réseau

Dans notre cas d'école, nous pouvons constater que les communications en cours ne sollicitent en aucune manière le réseaux. Le taux d'erreur est à zéro ici que le « bruit de font » (Braodcast[17] et multicast[18]) (Voir figure 43).

[17] Le broadcast est un terme anglais définissant une diffusion de données à un ensemble de machines connectées à un réseau. En français on utilise le terme diffusion.
[18] Emission d'un paquet IP à destination de plusieurs machines simultanément .à prime abord ressemblant au broadcast, le multicast se différencie par le fait que le paquet d'informations n'est envoyé qu'une seule fois en direction de plusieurs mac...

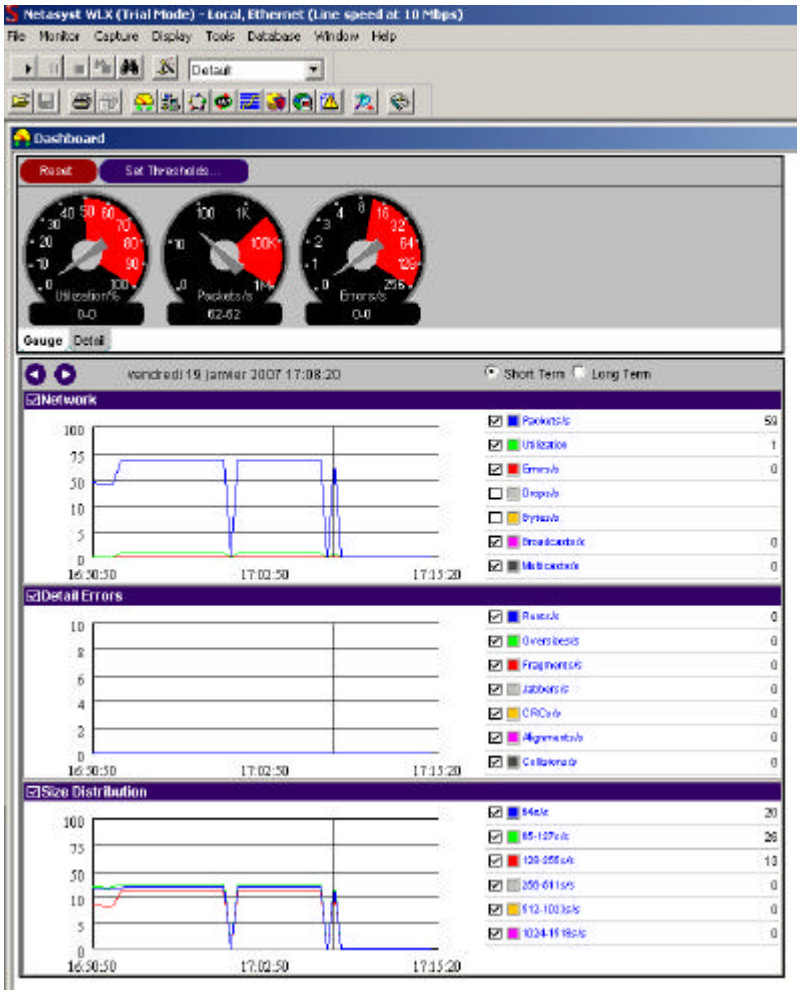


Figure 43 : Mode monitor, analyse en temps réel

4.3.3.2 Résultats obtenus avec Ethereal

Dans notre cas d'école, le logiciel Ethereal sera utilisé pour vérifier les contenus des paquets IP échangés et leur contenu entre les éléments interconnectés au réseau. Après activation de l'option « Capture packets in promiscuous mode », la carte réseau insérée sur notre « PC sniffer » pourra capturer les trames et nous pourrons intercepter et lire l'ensemble du trafic sur le réseau entre l'API et les deux IHM (Voir figure 44).

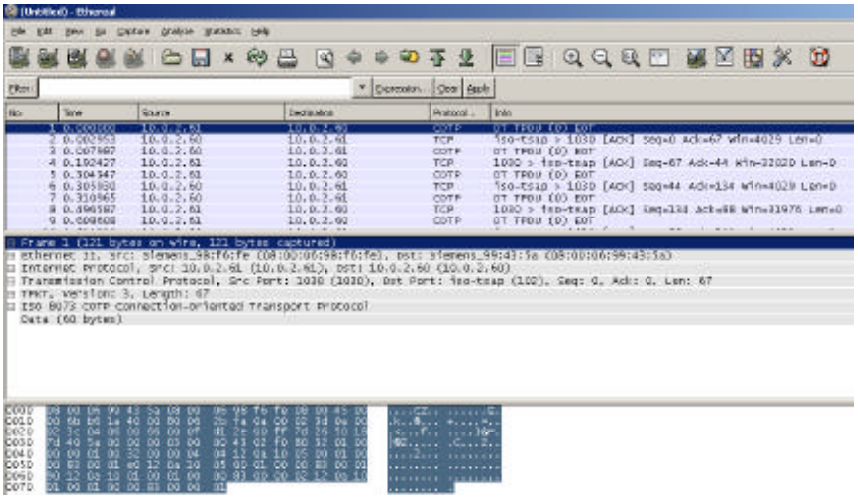


Figure 44 : Trame TCP IP conforme

La trame enregistrée confirme le respect des protocoles entre l'API et l'IHM. Le protocole COTP[19] est le protocole ISO 8073 sur TCP. Dans notre cas nous sommes sur un principe « SEND/RECEIVE » inter automate sur Ethernet [54].

4.3.3.3 Bilan de la fonction « Sniffer »

Cette prestation porte sur la mise en œuvre d'un réseau Ethernet installé et des services s'y rattachant dans sa vision globale où un dysfonctionnement a été signalé par le client.

Le diagnostic de ce dysfonctionnement présumé repose sur :

- la compréhension du besoin (expression du client),
- l'analyse du problème et son évaluation.

Et va nécessiter éventuellement :

- l'étude de la mise en œuvre des moyens (plan de diagnostic ou encore stratégie de diagnostic),
- l'analyse des paramètres existants,
- l'acquisition de mesures et leur analyse,
- la formulation d'hypothèse sur les causes éventuelles,
- la recherche de solutions et d'actions à mener pour améliorer le fonctionnement et (ou) accroître les objectifs de performance.

Les causes possibles de ce dysfonctionnement pourront être :

- la conception du schéma de principe ...,
- la rupture ou le manque de qualité requise d'un câble (ou support de communication couche 1 du modèle OSI),
- une charge trop importante à un nœud réseau...,
- des paramètres applicatifs inappropriés,
- etc...

Ces actions effectuées et résultats analysés seront de qualité et significatif si et seulement si les référentiels de base concernant la conception et l'installation des réseaux Ethernet seront respectés en amont ! (Voir tableau ci dessous).

Normes européennes CENELEC		
Symbole	**Descriptif**	**N°**
EN 50173-1	Technologie de l'information - **Systèmes génériques de câblage**	EN 50173-1 (~= ISO 11801)
EN 50174-1	Technologie de l'information - **Installation de Câblage / Planification de l'assurance qualité**	EN 50174-1
EN 50174-2	Technologie de l'information - **Installation de Câblage / Planification et pratiques d'installation à l'intérieur des bâtiments**	EN 50174-2
EN 50174-3	Technologie de l'information - **Installation de Câblage / Planification et pratiques d'installation à l'extérieur des bâtiments**	EN 50174-3
EN 50346,	Technologie de l'information -Installation de Câblage / **Essais des câblages installés**	EN 50346
EN 50310	Application de **liaison équipotentielle et de la mise à la terre** dans les locaux avec **équipement de technologie de l'information**	EN 50310

[19] Connection Oriented Transport Protocol

4.3.4 Sécurité des échanges

4.3.4.1 Mécanismes de sécurité de l'API spécifiques à Siemens

Le logiciel de configuration de l'automate, STEP 7, permet de créer des utilisateurs avec des mots de passe et de leur donner différents droits. Il est possible de définir pour chaque couple login/password des droits assez précis. On peut ainsi interdire à un utilisateur d'utiliser la table de variables symboliques. Plus simplement, on définit dans ce module les droits en lecture et en écriture des variables. Ces droits sont également valables pour les accès au serveur ftp embarqué de l'automate (Voir figure 45).

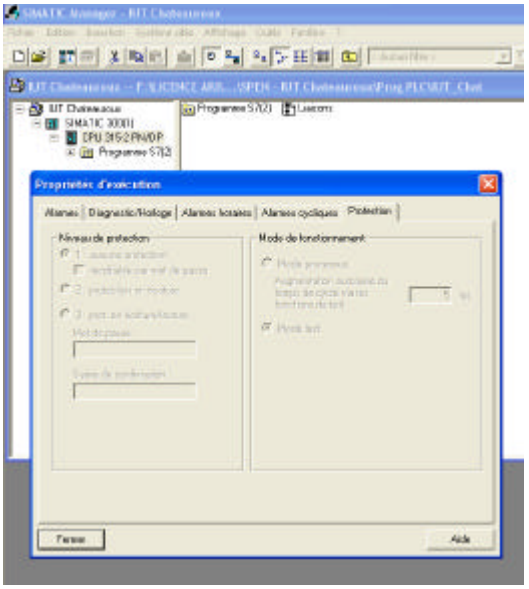


Figure 45 : Droits alloués aux utilisateurs de l'API

Il existe par défaut un utilisateur "everybody". On ne peut pas lui donner de mot de passe et on ne peut pas le supprimer. Il n'a par défaut aucun droit d'accès. Il est par contre à noter que l'on ne sait pas comment sont stockés ces logins et mots de passe à l'intérieur même de la mémoire de l'automate, s'ils sont cryptés, et éventuellement comment ils sont cryptés. A ce jour, je n'ai pu avoir aucune information sur ce point.

4.3.4.2 Mécanismes de sécurité de l'IHM spécifiques à Siemens

L'IHM dans notre cas d'école dispose (Voir paragraphe 4.2.5.1) d'un environnement Windows CE. Cet environnement, permettra comme le montre la figure 46 d'insérer un mot de passe interdisant d'accéder aux paramètres systèmes du produit.

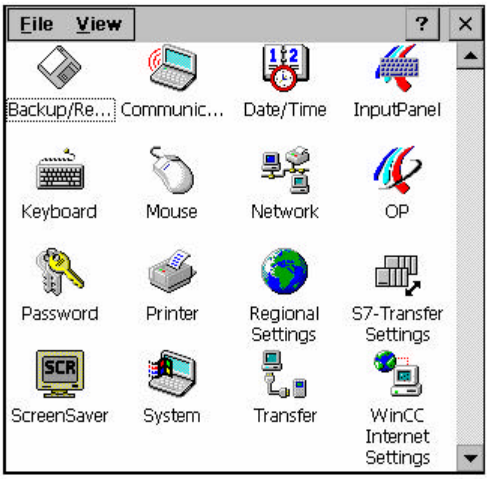


Figure 46 : Menu Windows CE du pupitre opérateur

Le développeur de l'application sous Wincc.Flexible pourra s'il le souhaite insérer des mots de passe dans son application hiérarchisant les accès à l'information.

4.3.4.3 Mécanismes de sécurité de l'application hébergée sur l'IHM

Le projet contient par défaut les groupes d'utilisateurs «Administrateurs» et «Opérateurs». Les figures 47 et 48 indiquent comment créer le groupe «Technologists» et définir les autorisations d'accès.

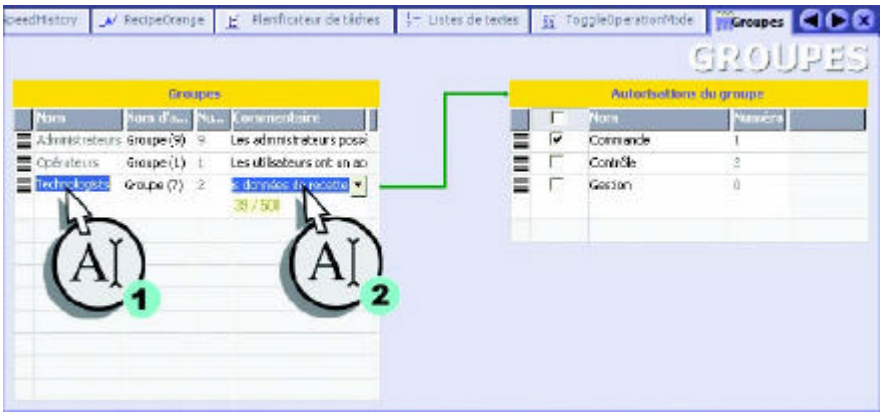


Figure 47 : Gestion des groupes utilisateurs (1) et des attributions associées (2)

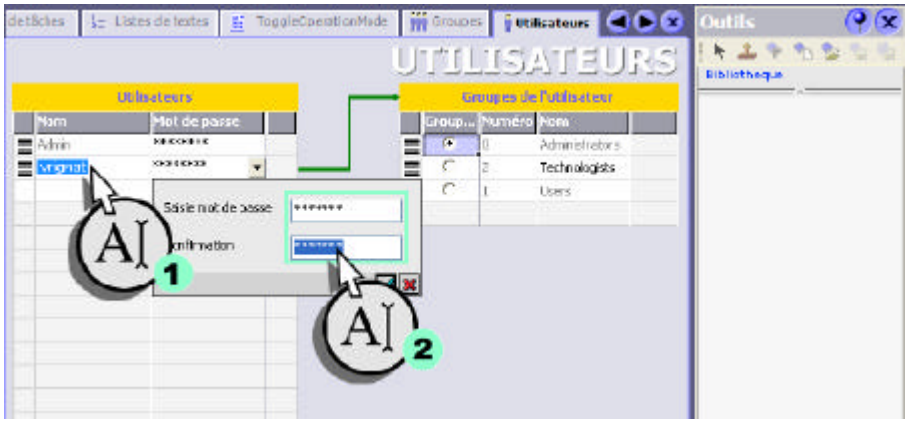


Figure 48 : Utilisateur (1) et autorisation d'accès (2)

4.3.4.4 Gestion des mots de passe

L'utilisation de mots de passe « forts » (password) est l'une des briques de base dans la sécurisation d'un système d'information. Malheureusement cette première étape est souvent absente dans la politique de sécurité. Il est par conséquent assez fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut [49].

4.3.4.4.1 Définition d'un mot de passe

Un mot de passe « fort » est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

4.3.4.4.2 Les différentes attaques sur les mots de passe

Afin d'éviter qu'un mot de passe ne soit facilement retrouvé par un outil conçu à cet effet, il peut être intéressant de connaître les différentes méthodes utilisées par les outils automatisés pour découvrir les mots de passe. Dans la plupart des cas, ce sont les empreintes (valeur de sortie d'une fonction de hachage) des mots de passe qui seront stockés sur le système. Les attaques sur les mots de passe consistent donc à calculer des empreintes et à les comparer à celles contenues dans les fichiers de mots de passe.

Attaques par force brute :

Cette attaque consiste à tester toutes les combinaisons possibles d'un mot de passe. Plus il existe de combinaisons possibles pour former un mot de passe, plus le temps moyen nécessaire pour retrouver ce mot de passe sera long. Un mot de passe fort, d'une longueur minimale de dix caractères et constitué d'au moins trois des quatre groupes de caractères énoncés ci-dessus (minuscules, majuscules, caractères spéciaux et chiffres), ne pourra être découvert par cette attaque dans un temps raisonnable, avec les moyens dont on dispose au le jour « J ».

Attaques par dictionnaires

Cette attaque consiste à tester une série de mots issus d'un dictionnaire. Il existe toutes sortes de dictionnaires disponibles sur l'internet pouvant être utilisés pour cette attaque (dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...). En utilisant un mot de passe n'ayant aucune signification cette attaque ne donnera aucun résultat. Cependant, plusieurs règles de transformation des mots du dictionnaire sont utilisées par les outils automatisés pour augmenter le nombre de combinaisons possibles. Citons par exemple :

le remplacement d'un ou de plusieurs caractères du mot du dictionnaire par une majuscule (bUreAU),

- le remplacement de certains caractères par des chiffres comme par exemple le S en 5 (mai5on),
- l'ajout d'un chiffre au début ou à la fin d'un mot (arbre9),
- l'ajout des mots de passe déjà découverts.

Il est possible d'utiliser les dictionnaires pré-calculés contenant une liste de mots de passe et leur empreinte associée. Même si cette possibilité accélère le temps nécessaire pour retrouver un mot de passe, elle nécessite une place plus importante en mémoire.

La solution idéale pour retrouver des mots de passe le plus rapidement possible serait d'avoir une liste exhaustive de tous les mots de passe possibles et de leur empreinte associée. Un tel dictionnaire n'est pas envisageable car il nécessiterait une place en mémoire bien trop importante. Cependant sur les algorithmes de chiffrement faibles (par exemple le chiffrement LM sur les systèmes Microsoft Windows), il est possible d'utiliser les attaques par compromis temps/mémoire.

Attaques par compromis temps/mémoire

Les attaques par compromis temps/mémoire sont des solutions intermédiaires permettant de retrouver un mot de passe plus rapidement qu'avec une attaque par force brute et avec moins de mémoire qu'en utilisant une attaque par dictionnaire. Ces compromis sont réalisés à partir de chaînes construites à l'aide de fonctions de hachage et de fonctions de réduction. Pour retrouver un mot de passe, il faudra d'abord retrouver à quelle chaîne appartient l'empreinte recherchée. Une fois que la chaîne aura été retrouvée il sera alors facile de retrouver le mot de passe, à partir du début de cette chaîne.

4.3.4.4.3 Créer un bon mot de passe

Un bon mot de passe est un mot de passe fort, qui sera donc difficile à retrouver même à l'aide d'outils automatisés mais facile à retenir. En effet, si un mot de passe est trop compliqué à retenir, l'utilisateur mettra en place des moyens mettant en danger la sécurité du système d'informations, comme par exemple l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier où l'utilisateur doit s'authentifier. Pour ce faire, il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.

Méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase «J'ai acheté huit cd pour cent euros cet après midi » deviendra ght8CD%E7am.

Méthode des premières lettres

Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

4.3.4.4.4 Gestion des mots de passe

Les mots de passe sont souvent la seule protection d'une station de travail. Il est donc indispensable de mettre en œuvre une politique de gestion des mots de passe intégrée à la politique de sécurité du système d'information.

Politique de gestion des mots de passe

La politique de gestion de mots de passe devra être à la fois technique et organisationnelle. Les éléments suivants pourront, entre autres, être inscrits dans cette politique :

Sensibilisation à l'utilisation de mots de passe forts

Les utilisateurs d'un système d'information doivent être sensibilisés à l'utilisation de mots de passe forts afin de comprendre pourquoi le risque d'utiliser des mots de passe faibles peut entraîner une vulnérabilité sur le système d'information dans son ensemble et non pas sur leur poste uniquement.

Renouvellement de mots de passe

Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps.

4.3.4.4.5 Les critères prédéfinis pour les mots de passe

Plusieurs critères peuvent être définis et mis en œuvre dans de nombreux systèmes pour s'assurer de la qualité des mots de passe. Ces critères sont, par exemple :

- une longueur minimum prédéfinie (au minimum 10 caractères),
- l'impossibilité de réutiliser les « n » derniers mots de passe,
- le nombre de tentatives possibles,

- la manière de déverrouiller un compte qui a été bloqué (pour éviter les dénis de service liés au blocage de tous les comptes sur un système d'information, il peut être intéressant que le déblocage des comptes se fasse de manière automatique après un certain délai),
- l'utilisation de la mise en veille automatique avec un déblocage par mot de passe.

4.3.4.4.6 Confidentialité du mot de passe

Un mot de passe sert à s'authentifier sur un système. Dans ce but il est important de veiller à ne pas divulguer son mot de passe. Un mot de passe ne doit jamais être partagé ni stocké dans un fichier ni sur papier. Cependant, il est possible que la politique de sécurité demande aux utilisateurs d'un système d'information de stocker les mots de passe sur papier dans un lieu sûr (enveloppe cachetée dans un coffre ignifugé) pour le cas ou un problème surviendrait.

4.3.4.4.7 Configuration des logiciels

Une large majorité de logiciels comme par exemple les logiciels de navigation internet proposent d'enregistrer les mots de passe, par le biais d'une petite case à cocher « retenir le mot de passe », pour éviter à l'utilisateur la peine d'avoir à les re-saisir. Ceci pose plusieurs problèmes de sécurité notamment lorsqu'une personne mal intentionnée prend le contrôle de l'ordinateur d'un utilisateur, il lui suffit de récupérer le fichier contenant la liste des mots de passe enregistrés pour pouvoir se connecter sur des sites à accès protégé.

4.3.4.4.8 Utilisation de mots de passe différents

Il est important de garder à l'esprit qu'un mot de passe n'est pas inviolable dans le temps. C'est pour cette raison qu'il est nécessaire de changer régulièrement son mot de passe et qu'il est important de ne pas utiliser le même mot de passe pour tous les services vers lesquels on se connecte. En effet, si le poste de travail de l'utilisateur est compromis et qu'un renifleur de clavier est installé, il sera possible pour un utilisateur mal intentionné de récupérer tous les mots de passe entrés au clavier (même si ces mots de passe sont des mots de passe forts). Si un des mots de passe est récupéré par cette attaque, l'utilisateur mal intentionné pourra seulement accéder aux services dont il connaîtra le ou les mots de passe révélés durant la période pendant laquelle le renifleur de clavier était installé.

4.3.4.4.9 Utilisation de mots de passe non re-jouables (One Time Password)

Il est possible d'utiliser des solutions permettant de s'authentifier à un système par le biais d'un mot de passe ne pouvant être utilisé qu'une seule fois. Cette solution présente l'avantage que lorsqu'un mot de passe est découvert, il ne pourra pas être réutilisé. Cette technique reste toutefois vulnérable aux attaques de l'intercepteur (man in the middle).

4.3.4.4.10 Utilisation de certificats clients et serveurs

L'utilisation de certificats de clés publiques sur les postes clients et serveurs permet de détecter l'intercepteur (man in the middle), mais reste vulnérable au vol de la clé privée ou du code porteur sur le poste de travail si elle n'est pas protégée dans un matériel adéquat.

4.3.4.4.11 Mettre en place un contrôle systématique des mots de passe

Pour s'assurer de l'absence de mots de passe faibles, il peut être intéressant pour un administrateur, s'il y est autorisé, de réaliser des tests sur la robustesse des mots de passe utilisés sur son système d'information. Des outils commerciaux ou gratuits sont disponibles sur l'internet. Le choix de l'outil le plus adapté dépend du type de mots de passe que l'on désire analyser.

4.3.5 Accès délocalisés à l'application avec le service Sm@rtAccess

Cette dernière partie fera un point sur la possibilité d'accéder à une IHM de mon ordinateur personnel par le biais d'une connexion internet (Voir figure 49).
Réaliser à distance le téléchargement d'une application de ce type n'est pas sans risque pour le process concerné. Dans ma démarche de travail, j'ai respecté les principales recommandations à adopter dans le cadre d'une télémaintenance avec téléchargement de l'application d'automation via une connexion internet [38] :

- minimiser les télémaintenances au strict nécessaire,
- toujours les contractualiser,
- créer un portail de contrôle d'accès,
- indépendamment des moyens de connexion,
- authentifier individuellement chaque « télémainteneur »,
- ouvrir le flux après l'authentification réussie,
- journaliser les connexions,
- recopier si possible la session complète des informations qui remontent à l'extérieur.

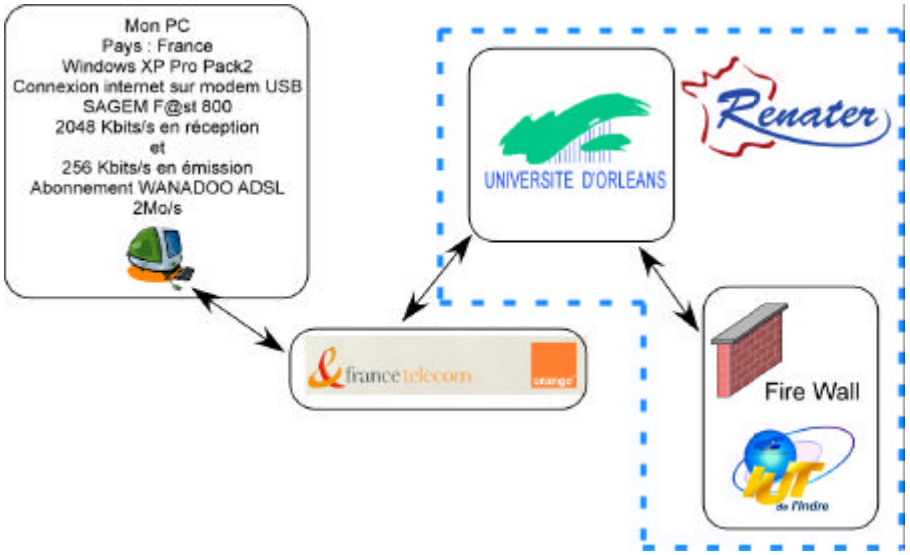


Figure 49 : Le parcours entre mon PC et une IHM en passant par Renater[20]

[20] Le réseau Renater est un réseau très haut débit qui relie en France toutes les facultés et les centres de recherche.

4.3.5.1 Configuration du routage

Figure 50 : Attribution de mon adresse IP à la connexion sur internet

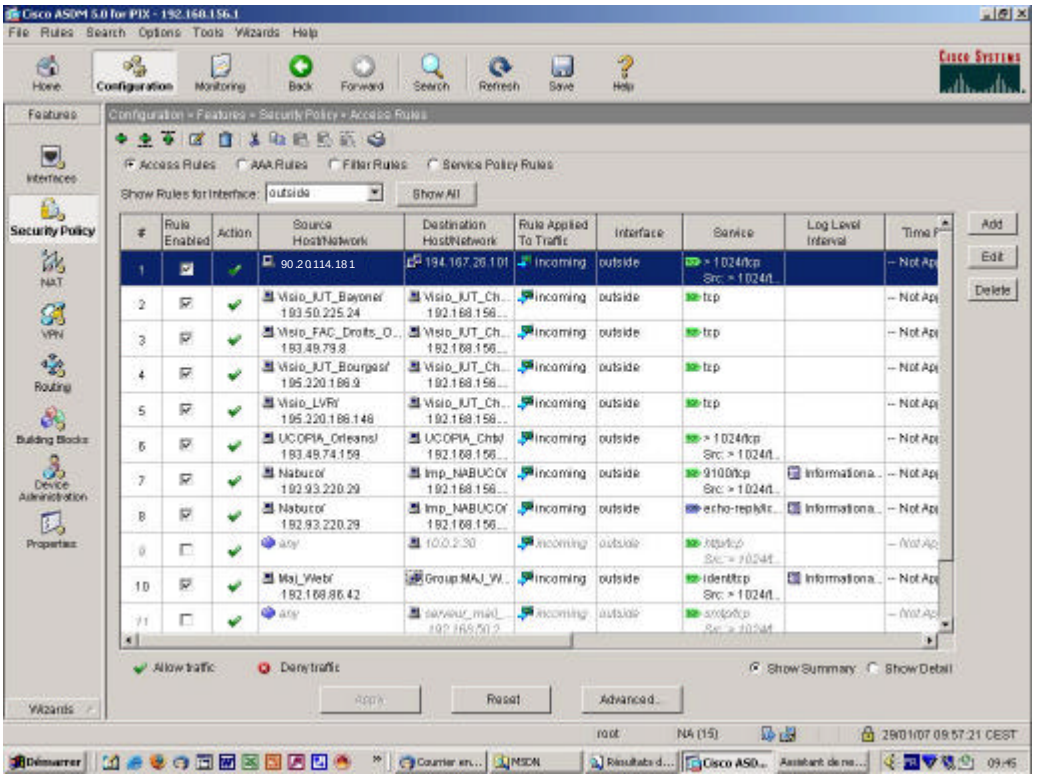


Figure 51 : Routage de mon adresse IP public vers une adresse public du firewall de l'IUT

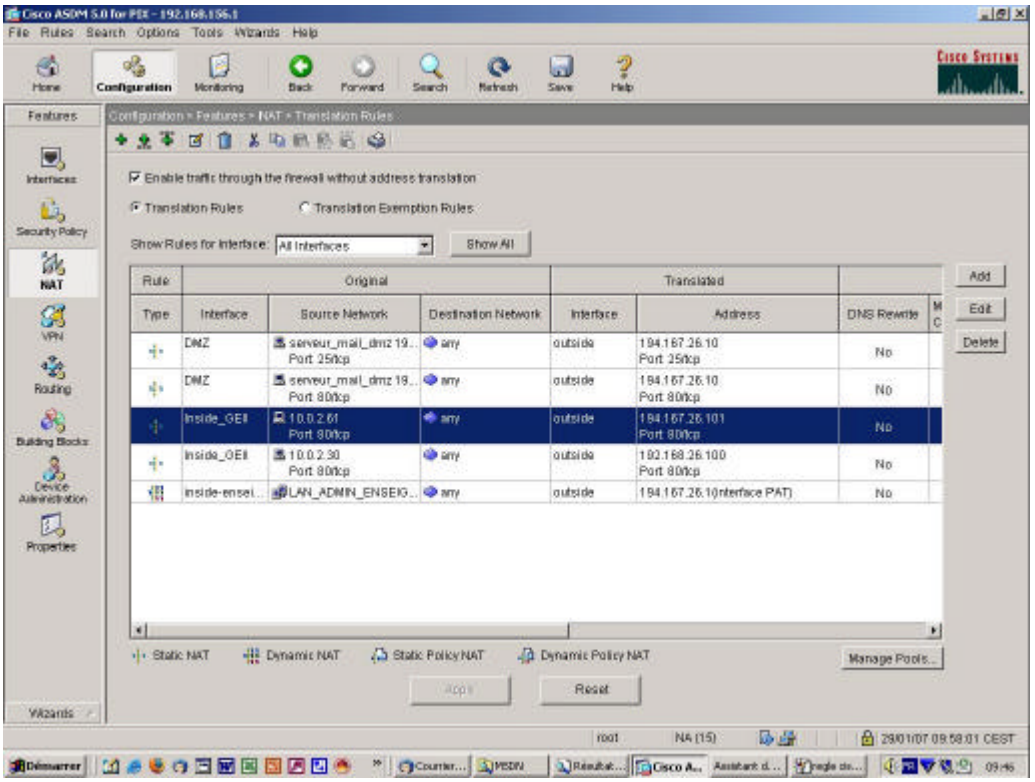


Figure 52 : Routage de l'adresse public attribué au firewall vers une adresse privée (une des deux IHM utilisées)

Il existe dans tous les systèmes TCP/IP une commande qui s'appelle "traceroute". Cette commande a pour but de repérer toutes les passerelles franchies pour aller de son poste à un hôte distant. En plus de déterminer les passerelles, elle indique, un peu à la manière d'un ping, le temps que met cette passerelle à répondre.
Cette commande, dans les systèmes Windows, s'appelle « tracert », sans doute à cause d'une vieille habitude de créer des noms de 8 caractères maximum. Sous Linux, elle s'appelle «traceroute ». Les deux commandes donnent les mêmes indications, celle de Linux étant un peu plus puissante dans la mesure où elle est plus paramétrable. L'emploi de la commande «tracert » montre le chemin emprunté pour aller de mon poste personnel au port ouvert pour cette application sur le firewall (Voir figure 53).

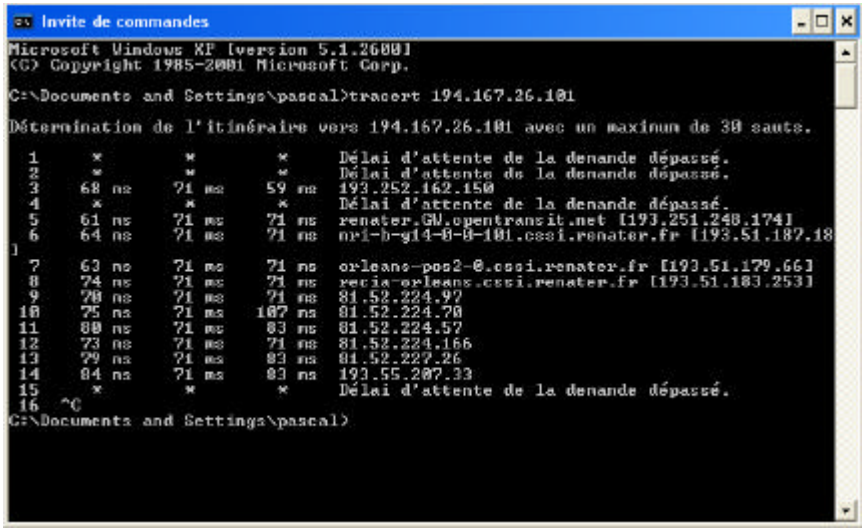


Figure 53 : Résultat de la commande « tracert »

Ce n'est pas bien loin, tout de même... 11 passerelles et il suffit de lire les noms pour constater que l'on passe par Orléans ! (Heureusement qu'on ne fait pas ça en voiture). Nous pouvons également constater qu'avec cette commande, nous arrivons « à la porte » du firewall soit juste à la sortie du routeur FranceTelecom (Voir figure 1). La commande s'appuie sur le "Time To Live" d'un paquet de données. Ce TTL dispose d'une valeur initiale, généralement entre 15 et 30 secondes, et est décrémenté à chaque passage de routeur. La décrémentation à chaque routeur est au moins d'une seconde, plus si le paquet reste en file d'attente dans le routeur plus d'une seconde. Dans un tel cas, le TTL est décrémenté à chaque seconde passée dans la file d'attente.

Si le TTL devient nul, le paquet est considéré comme mort et est détruit par le routeur. L'émetteur du paquet reçoit un message ICMP[21] « Time-to-live exceeded » pour le prévenir (une des raisons pour laquelle il ne faut pas filtrer tout le trafic ICMP sur un firewall).

C'est cette propriété qui va servir à définir la route. La cible envoie un premier paquet avec un TTL de 1s. Ce paquet, en arrivant sur le premier routeur, va voir son TTL tomber à 0, donc va être détruit, et le routeur va en informer l'émetteur au moyen d'un message ICMP « TTL expiré ». L'opération est effectuée par défaut trois fois (les trois indices de temps indiqués dans la réponse), puis, un nouvel essai sera fait, avec cette fois-ci un TTL de 2 secondes. Normalement, le paquet doit passer le premier routeur et être détruit par le second. Ainsi de suite jusqu'à arriver à destination.

Les paquets envoyés par la source peuvent être des paquets UDP ou ICMP. La commande "traceroute" de Linux envoie par défaut des paquets UDP[22], mais la directive « -I » force l'émission de paquets ICMP. Sous Windows, la commande « tracert » ne sait envoyer que des paquets ICMP. Dans notre cas, les paquets ne mettent qu'environ 70 ms pour faire l'aller-retour.

4.3.5.2 Configuration du service Sm@rtAccess

La partie la plus contraignante ayant été réalisée et contrôlée (le téléphone a beaucoup fonctionné avec notre ingénieur informaticien placé devant son poste d'administration du firewall), il ne reste plus qu'à paramétrer le service Sm@rtAccess dans le panneau de configuration de windows et de l'application WinccFlexible hébergée sur mon PC (Voir figures 54, 55 et 56).

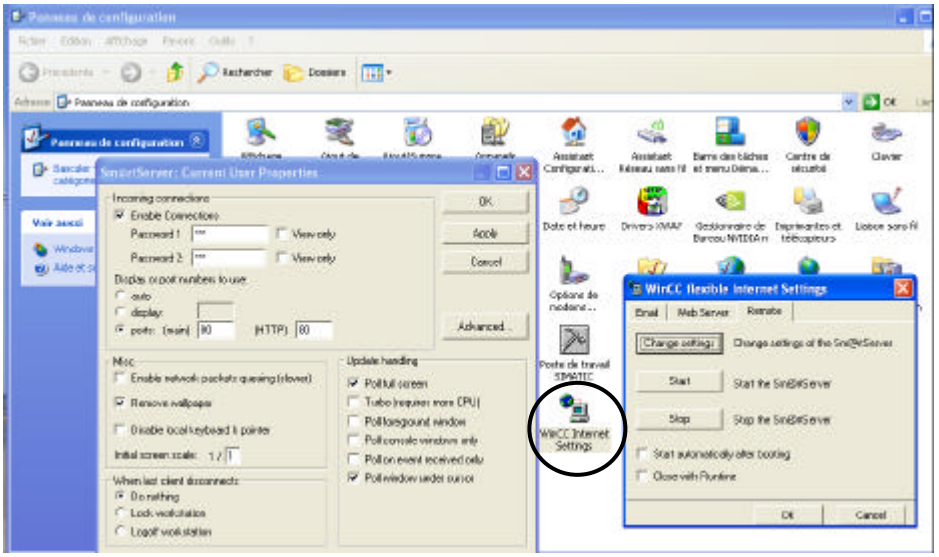


Figure 54 : Lancement du service Sm@rtAccess

[21] Internet Control Message Protocol
[22] User Datagram Protocol

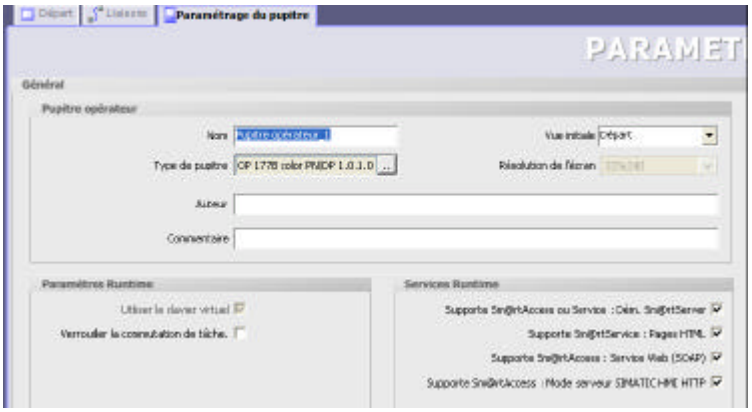


Figure 55 : Activation des services sur WinccFlexible

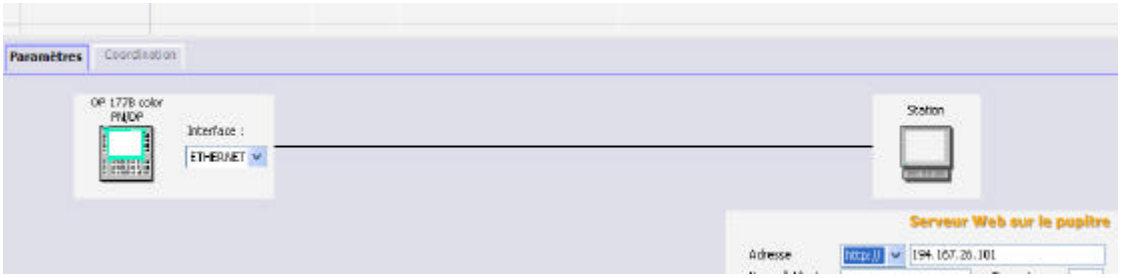


Figure 56 : Adressage de l'adresse IP avant téléchargement de l'application

Ce service particulièrement intéressant soulève un problème majeur :

- La sécurité du service de bout en bout contre le piratage (Voir figure 57).

Tous les systèmes sont vulnérables, nous avons vu qu'il y avait déjà un bon nombre de mots de passe à franchir pour accéder à l'ensemble de l'application. Néanmoins, au delà de l'utilisation du connexion de type VPN[23], le niveau de sécurité au même titre que les connexions actuelles proposées par exemple pour des paiements sur internet peut être posé pour ces services rattachés aux applications industrielles.

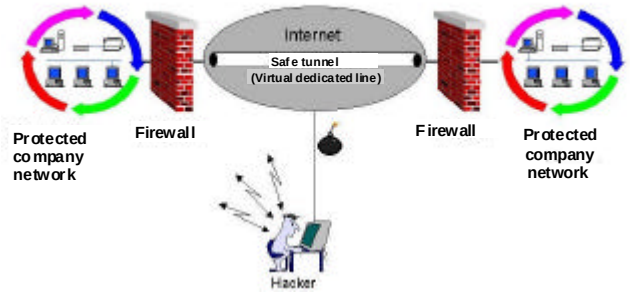


Figure 57 : Contrer les Hackers

[23] Un VPN ou Virtual Private Network, est un tunnel logique (par opposition au réseau privé) établi entre deux entités et dans lequel les données circulant ne sont pas « visibles » de l'extérieur. Cette « invisibilité » peut être due par exemple à un chiffrement des données ou à un protocole particulier des échanges de données.

Comme par exemples les utilisation de SSL: HTTPS[24], SSH, FTPS, POPS...

SSL peut être utilisé pour sécuriser pratiquement n'importe quel protocole utilisant TCP/IP. Certains protocoles ont été spécialement modifiés pour supporter SSL[25].

Il est possible de sécuriser des protocoles en créant des tunnels SSL. Une fois le tunnel créé, vous pouvez faire passer n'importe quel protocole dedans (SMTP, POP3, HTTP, NNTP...). Toutes les données échangées sont automatiquement chiffrées.

4.3.6 Accès délocalisés à l'application avec le service Sm@rtService

Sm@rtService permet de réaliser la télémaintenance de pupitres opérateur pour une assistance via Internet :

- téléconduite via internet/intranet,
- téléconduite d'un système HMI au moyen d'internet explorer,
- accès aux informations d'assistance et de maintenance,
- mise à disposition de pages HTML standard sur le système IHM avec des informations d'assistance et de maintenance ainsi que des fonctions de diagnostic,
- assistance par email (envoi d'email sur la base d'alarmes et d'événements).

Dans ce cadre, je vais vous présenter les résultats significatifs ainsi obtenus relatifs à des essais sur l'Intranet de l'IUT soit le VLAN3-GEII (Voir figure 1). Il est à souligner que ces résultats obtenus sur le réseau Intranet de l'IUT pourraient être identiques aux résultats obtenus sur un réseau d'entreprise en appliquant une « politique » identique ou similaire dans les droits d'accès et les passerelles. Il est à souligner également que ces services sont d'une manière identique disponibles via l'Internet. C'est d'ailleurs ce qui fait sa « force » !

Les configurations préalables ayant été déclarées (Voir figures 54 et 55), nous pouvons accéder aux services d'une IHM connectée au réseau via un navigateur internet par exemple, Internet Explorer (Voir figure 58).

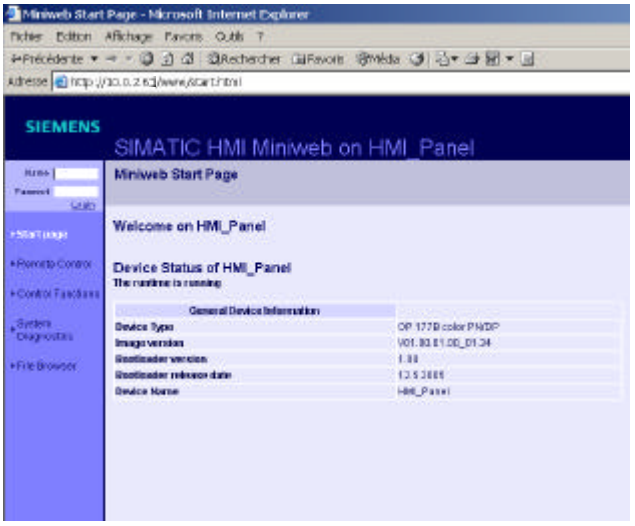


Figure 58 : Accès à l'IHM via Internet Explorer

[24] HTTPS: c'est HTTP+SSL. Ce protocole est inclus dans pratiquement tous les navigateurs, et vous permet (par exemple) de consulter vos comptes bancaires par le web de façon sécurisée. FTPS est une extension de FTP (File Transfer Protocol) utilisant SSL. SSH (Secure Shell): c'est une sorte de telnet (ou rlogin) sécurisé. Cela permet de se connecter à un ordinateur distant de façon sûre et d'avoir une ligne de commande. SSH possède des extensions pour sécuriser d'autres protocoles (FTP, POP3 ou même X Windows).

[25] Secure Sockets Layer est le protocole sur lequel repose la sécurisation en HTTPS. C'est avec le SSL que l'on crypte les données afin de les envoyer sur internet. La puissance de chiffrement du cryptage SSL se mesure en bits (en général 40, 56 ou 128 bits). Le nombre de bits définit le nombre de combinaisons nécessaires pour casser la clé de cryptage. Concrètement, le nombre de combinaisons est égale à 2 puissance le nombre de bits (pour 56 bits : 2 56 = 72.057.594.037.927.936 possibilités , imaginez avec un cryptage en 128 bits...)

Le service « System Diagnostics » permet d'historiser un certain nombre d'évènements effectués aux préalables sur l'IHM (Voir figure 59).

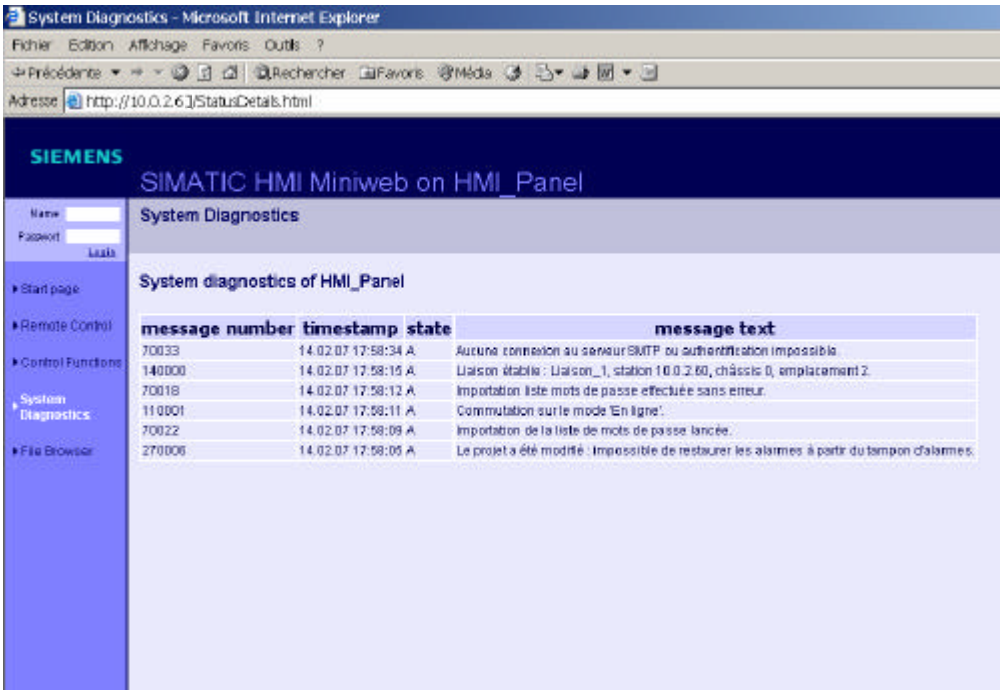


Figure 59 : Accès au service "System Diagnostics"

Compris dans les services de Sm@rtService, nous avons la possibilité de contrôler virtuellement sur un PC connecté au réseau l'application hébergée sur la console IHM via le navigateur si nous disposons des droits préalables (Voir figure 61). La console IHM sera accessible via l'activation du service Sm@rtClient (Voir figure 60).

Figure 60 : Accès à l'application de la console IHM via Internet Explorer

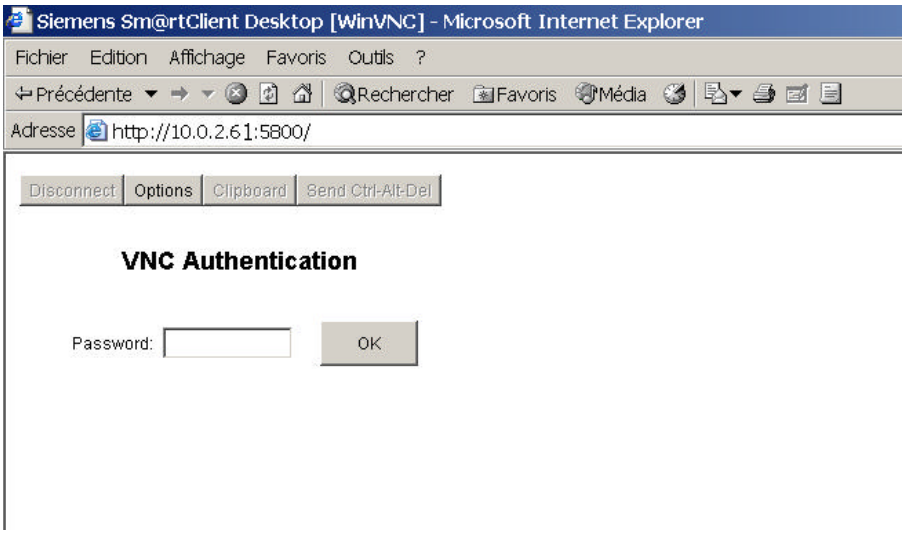


Figure 61 : Accès à l'application de l'IHM via Internet Explorer par validation préalable d'un mot de passe

Une fois la connexion effectuée l'application est accessible sur le navigateur web via des fonctions «applet JAVA[26] » (Voir figures 62 et 63). Par exemple dans notre cas, l'agent de maintenance « prend la main » sur l'IHM de l'opérateur. Mais réciproquement, l'agent de maintenance verra ce que l'opérateur fait sur son IHM.

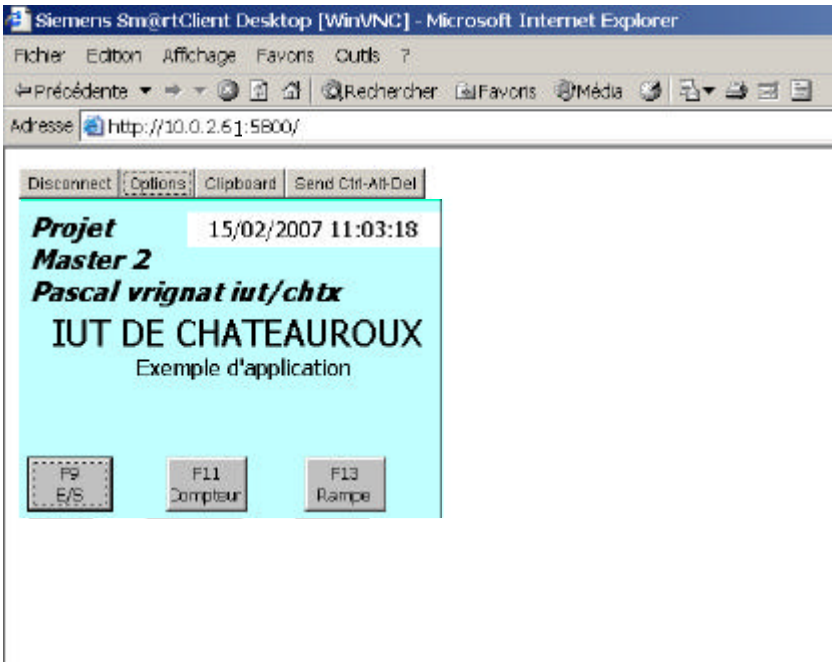


Figure 62 : Accès à l'application de IHM via un service Web

[26] Une applet est un programme Java qui s'exécute chez l'utilisateur après téléchargement par Internet. Dans le navigateur Web, la "machine virtuelle Java", se charge d'interpréter le code Java.

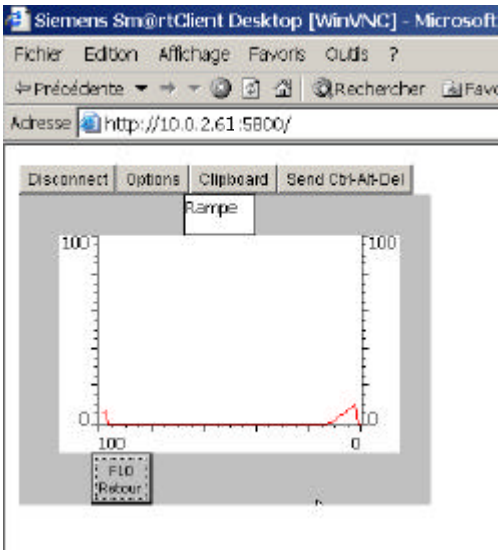


Figure 63 : Accès à la fonction contrôle de la rampe via le service Web

Le temps de réponse est un facteur très important dans une application de supervision. Or, si celui-ci est acceptable sur un réseau local, il peut doubler, tripler, voire plus, lorsque l'on consulte les «applets » depuis internet. De part la nature même des communications sur Internet, il peut beaucoup varier suivant le type de connexion du client et l'encombrement global du réseau. Il pourrait être intéressant de fournir une fonction « mesurant » d'une quelconque manière la qualité et la rapidité de la connexion, qui permettrait d'adapter les demandes de rafraîchissement des variables.

5 Conclusion

L'évolution des moyens de communications et la fiabilité de ceux-ci a modifié radicalement la conception des systèmes automatisés. La tendance actuelle est d'utiliser des supports de communication générique tel que Ethernet depuis la connexion d'un capteur jusqu'au réseau de bureautique. De nombreuses solutions commerciales existent pour permettre une interconnexion entre ces différents niveaux. La totalité des niveaux de la pyramide CIM peut s'interconnecter et permet d'offrir de nouveaux services comme nous l'avons vu dans ce sujet.

Les thèmes scientifiques de présentation du groupe de travail « MACOD » (GRD MACS) sont dans cette thématique [53] :

- T1 : Maintenance des systèmes distribués,
- T2 : Pronostic et aide au diagnostic,
- T3 : Processus d'agrégation et de déploiement des performances en maintenance,
- T4 : Maintenance coopérative,
- T5 : Optimisation des stratégies de maintenance (décision),
- T6 : Intégration de la maintenance en conception,
- T7 : Planification intégrée Production/Maintenance.

Nous avons vu que le « Sm@rtService » pour la maintenance et le diagnostic via le Web évite des interventions sur site coûteuses. Où que vous soyez dans le monde, un navigateur standard suffit pour accéder à une IHM depuis un PC connecté à internet, établir des diagnostics à l'aide de vues de diagnostic standard ou télécharger un projet à distance. Dans les situations critiques, la station sur site peut réagir à certains événements et envoyer des emails ou des SMS au personnel de maintenance.

Ces thèmes et plans d'actions sont majoritairement aux services des « décideurs financiers » lorsqu'ils analysent par exemple des tableaux synthétiques et cartésiens comme peut l'évoquer la figure 64.

Machines	Nb arrêts	Durée max par arrêt	Durée cumulé des arrêts	Disponibilté 1 an glissant	Disponibilté depuis le 1/1/2006	% Objectif	Pénalité
SP1						99,9% 2 arrêts/mois 4h	
SQ1						99,7%	
SD1						99,7	
SP2						99,9	

Figure 64 : Exemple de tableau de bord d'objectifs de fabrications

Les approches naïves, mais traditionnelles, de la sécurité des systèmes d'informations est une question technique. C'est bien connu. Et en tant que telle, elle doit être dirigée par un expert, ingénieur en sécurité, peut-être même ancien hacker lui-même. Il doit être hiérarchiquement rattaché au directeur des systèmes d'informations. Voilà un schéma classique de pensée qui permet de renvoyer la sécurité à un niveau subalterne. Schéma communément adopté par de nombreuses entreprises. L'expert sait. Il définit le besoin, élabore la solution. Puis, étant le seul à savoir, il l'exploite lui-même. D'ailleurs, comme la sécurité est son savoir-faire, l'expertise pointue que lui maîtrise, il n'a besoin de personne.

On pourra retenir comme principes de base que le management de la sécurité n'est pas plus compliqué que n'importe quelle question de direction. Il faut assigner à chacun une tâche précise, selon ses compétences, et faire travailler l'ensemble des équipes en harmonie. La définition des besoins relève de la maîtrise d'ouvrage. C'est une tâche peu technique pour laquelle les architectes ont avant tout une fonction d'écoute et un rôle de synthèse. Ils créent le lien entre les différentes composantes de l'entreprise. La maîtrise d'œuvre, pour sa part, va ensuite élaborer les solutions techniques pour réaliser les fonctions préalablement définies. Ces deux corps de métiers sont distincts. L'architecte qui dessine la maison, ou la cathédrale, n'est pas le bâtisseur : il n'y a rien de nouveau avec la sécurité. Une fois la solution créée, il apparaît deux nouvelles populations bien distinctes : d'une part l'utilisateur ou utilisatrice, Madame Dupond, secrétaire utilisant un PC connecté à un serveur lui-même en liaison avec le réseau de l'entreprise et l'internet, et d'autre part le service de maintenance et de hot-line qui doit faire en sorte que le poste de Madame Dupond fonctionne bien.

L'erreur serait de penser que le RSSI[27] doit être à la fois le maître d'ouvrage de la sécurité, son maître d'œuvre, l'assistant hot-line de Madame Dupond et le service de maintenance à lui tout seul. Et pourtant, combien d'organisations dans lesquelles le RSSI est un subalterne du DSI n'ont-elles pas peu ou prou cette vision du management de la sécurité ? Combien d'officines d'experts et de conseils techniques en sécurité ne font-elles pas plus ou moins consciemment référence à un tel modèle ? L'expert sait se protéger, il a même un tas de logiciels gratuits à sa disposition. Pourquoi Madame Dupond n'est-elle pas elle aussi experte ? Cela ne coûterait rien à personne. Une autre erreur classique est de faire reposer la sécurité sur quelques audits réguliers pour tester les défenses de l'entreprise. Cette approche est rassurante : les experts signent un rapport et l'entreprise est confortée dans ses choix. C'est oublier que la sécurité doit se préoccuper des menaces de demain, qui ne sont pas connues au moment de l'audit. Le management de la sécurité doit donc mettre en œuvre les outils d'exploitation et de supervision qui permettront à l'entreprise de disposer à tout moment des informations dont elle a besoin en cas d'attaques. Les outils sont bien connus des professionnels de l'exploitation. Il s'agit du « fault management », du « trouble ticketing », de toutes leurs composantes de reporting et de toutes les solutions de reconfiguration en temps réel et à distance. Ces outils doivent être alimentés par les informations des logs des firewalls, alertes des IDS, informations des proxy, et alertes des anti-virus, et spywares. Les outils de cartographie des équipements en constituent la pierre angulaire. Ils doivent scruter en permanence le système d'information et ses vulnérabilités pour piloter au quotidien les équipes opérationnelles afin de conserver un niveau maximum de prévention.

Dans une telle démarche, la direction, les experts et les équipes d'exploitation travaillent de concert pour un objectif bien défini et accepté par tous.

La transformation des systèmes d'information d'entreprises de production de biens et de service autour d'applications standards de type ERP[28], APS[29], CRM[30]... pose de nombreux défis tant dans leur mise en œuvre que dans leur usage. Aujourd'hui entre la Machine et l'Homme, mais demain encore plus, entre la Machine et la Machine, nous avons vu, que la coopération et les différents moyens de coopérations seront majeurs et primordiaux. Si l'on regarde le sens des mots, nous trouvons dans IHM : Interface Homme Machine. Siemens a récemment interverti ces lettres dans toutes ses documentations techniques pour l'Automation : HMI !. L'Homme sera t-il définitivement mis en avant ?

Dans son rapport sur l'entreprise communicante, Jacques Roure définit 5 processus principaux pour l'entreprise [37] :

- le processus de direction et de contrôle de l'entreprise ,
- le processus de gestion du cycle de vie du produit (PLM[31]),
- le processus de commande Production Livraison (SCM[32]),
- le processus de gestion de la relation client (CRM[33]),

[27] Responsable de la Sécurité des Systèmes d'Information
[28] Enterprise Resource Planning
[29] Advanced Planning Systems
[30] Client Management Relation
[31] Product Life Cycle Management
[32] Supply Chain Management
[33] Customer Relationship Management

- les processus de support (Ressources humaines, comptabilité, Informatique, Gestion des connaissances, Finance...).

Exprimées ainsi, les choses paraissent simples. Mais il ne vous a pas échappé que les entreprises, leurs produits, leurs procédés, leur historique, leur approche, leurs moyens, leurs compétences sont multiformes.

Cela déteint forcément sur la vision qu'elles ont eu du MES[34], sur leur façon de l'implanter, sur l'usage qu'elles prévoient, sur la rentabilité qu'elles en escomptent. Autrement dit, les frontières historiques du MES dans les entreprises sont celles que chaque entreprise aura bien voulu dessiner.

L'ensemble de ces nouvelles technologies pose le problème suivant : **Où situer aujourd'hui le MES dans l'organisation de la production ?**

[34] Manufacturing Execution System

Bibliographie

[1] P. Falson. Ergonomie cognitive du dialogue. Grenoble . Presses Universitaires, 1989.

[2] B. Pavard. Systèmes coopératifs : de la modélisation à la conception . Octarès Editions, Toulouse, 1994.

[3] David Saint-Voirin . Contribution à la modélisation et à l'analyse des systèmes coopératifs : application à la e-maintenance, Septembre 2006 numéro d'ordre 1164.

[4] P. Millot. Supervision des procédés automatisés et ergonomie. Hermes, 1988.

[5] J. Johnson al. (1989) «The Xerox Star: A Retrospective». IEEE Computer , September 1989.

[6] B. Myers. «A brief history of human-computer interaction technology». ACM interactions, 5(2):44-54, March/April 1998.

[7] J. Johnson al. (1989) «The Xerox Star: A Retrospective». IEEE Computer, September 1989.

[8] Information Security in Industrial Communications White Paper – 1999.

[9] Safety implications of industrial uses of internet technology - Prepared by Tessella Support Services plc for the Health and
Safety Executive.

[10] J'automatise n°16, Mai/Juin 2001.

[11] Cimax Edition Applicatif n°4, Décembre / Janvier 1998.

[12] Joël de Rosnay. « L'Homme Symbiotique, regards sur le 3ème millénaire » Editions du Seuil, 1995.

[13] P-L. Réfalo. « Sécuriser l'entreprise connectée ». Editions d'Organisation, 2002.

[14] Guillaume Desgeorge (2000) « La sécurité des réseaux » , article 2000.

[15] Bernd Lerp A&D AS FA HMI Product Management WinCC flexible Communications White Paper – 2006.

[16] U.Borghoff and J. Schlichter : Computer-suported cooperative work. Springer, 2000.

[17] M. Diaz and T. Villemur. Présentation et classification des applications coopératives. Technical report, LASS Contrat CNET FT n°92.1B.178 Lot 3, Avril 1993.

[18] H. Guyennet and J-C. Lapayre. The group appoch in distributed system. Journal of parallel and distributed computing practices PDCP, Nova science publisher, 2 (3) : 285-297, 1999.

[19] V. Baudouin, K. Drira, T. Villemur, and S. Tazi. Une approche sysnchrone pour une télé-expertise distribuée. In MFI 2001, Baden Baden, Germany 2001. IEEE.

[20] X. Rebeuf, N. Blanc, F. Charpillet, D. Cheve, A. Dutech, C. Lang, L. Pélissier, and J-P Thomesse. Proteus, des web services pour les systèmes de maintenance. In NOTERE 2004 – Nouvelles Technologies de la Répartion, pages 163-178, Saidia, Maroc, June 2004.

[21] Y. Laurillau and L. Nigay. Clover architecture for groupware. Inc CSCW '02 : Proceedings of the 2002 ACM conference on Computer supported cooperative work, pages 236-245, New York, NY, USA, 2002. ACM Press.

[22] M. Diaz, Z. Mammeri, and J-P. Thomesse. Communication de groupe dans les applications multimédias coopératives : une synthèse. In NOTERE '98 Colloque international sur les Nouvelles Technologies de la Répartition, Montréal, Québec, October 1998.

[23] R. Beuscart, F. Yousfi et D. Dufresne. Travail coopératif et groupware. Informatisation de l'unité de soins du futur, pages 195-210, 1994.

[24] E. Garcia. Une plate-forme de développement pour applications coopératives multimédia intégrant la gestion de la qualité de service. PhD thesis, LIFC Besançon, 2001.

[25] T. Ba, E. Garcia, H. Guyennet, J-C. Lapayre, N. Zerhouni, and R. Zemouri. Temic : Industrial cooperative telemaintenance. In ICCIE'01 International Conference on Computers and Industrial Engineering, Montreal, Canada, November 2001.

[26] Pascal Vrignat. « Réseaux locaux industriels ». Gaëtan morin édition, 1999.

[27] Rapport. Ambassade de France à Tokyo (Service pour la Science et la Technologie), SMM03_055, Septembre2003

[28] P. Chabert. La Supervision, Son évolution et ses enjeux, Colloque Pédagogique National IUT GEII, Montpellier 2006.

[29] P-L. P-L. Réfalo. La fonction SSI en entreprise, bilan et perspectives, Conférence , Paris, Juin 2005.

[30] C. Beltrami. e-maintenance :Possibilités actuelles et perspectives, Conférence A^{3}SI, Octobre 2005.

[31] f. Grzesiak . Maintenance et Automatismes, Article j3e, Mai 2006.

[32] Le marché du M2M en passe d'exploser d'ici 2010 !, Article Journal du Net, Juin 2005.

[33] Automatisation à l'échelle de l'entreprise, communication sans limites. PROFINET, le standard ouvert Industrial Ethernet. Revue Siemens, Avril 2006.

[34] E. Bajic : Protocoles TCP-IP et Modbus-TCP , Analyse de Trafic Ethernet-IP, Ecole de Printemps IUT Génie Electrique & Informatique Industrielle, Nancy, Mars 2006.

[35] Profinet Théorie et pratique, Siemens, Novembre 2003.

[36] G. Descamps : Méthodologie de diagnostic des réseaux Ethernet industriels sur la base des outils Schneider-Electric, Rapport d'activité, Juin 2006.

[37] J. Roure : La révolution dans la réduction des coûts de coordination et de transaction, Février 2002.

[38] H. Schauer : Infogérance/Télémaintenance et sécurité, Forum Gartner - EXP/BLG, 11 mai 2005.

[39] SIMATIC NET CP IT Instructions.

[40] SIMATIC NET CP IT Programming Tips.

[41] Support technique de Siemens Automation.

Internet

[42] http://www.scadanews.com

[43] http://www.tech-faq.com

[44] http://www.vpnc.org

[45] http://www.intranetjournal.com

[46] http://www.mag-securs.com

[47] http://www.dyndns.com

[48] http://www.club-mes.com

[49] http://www.proteus-iteaproject.com

[50] http://www.certa.ssi.gouv.fr

[51] http://www.m2m-ndt.fr/

[52]http://www.ethereal.com

[53] http://msdn.microsoft.com/webservices

[54] http://www.cert.org

[55] http://www.univ-valenciennes.fr/GDR-MACS/groupes_details.php?gt=MACOD

[56] http://www.wireshark.org

[57] http://www.hsc.fr

[58] http://www.renater.fr