L'opérateur : le maillon faible ?

La composante « humaine » devient un facteur clef de l'exploitation, avec ce paradoxe que l'homme apparaît en première analyse « comme le maillon le plus faible » du processus d'exploitation, alors que la conduite des évènements complexes montre le potentiel de « l'intelligence humaine » dans la résolution de ces crises. Ne dites pas à celui qui a prononcé cette phrase qu'il n'a pas l'expérience nécessaire pour affirmer de telles choses, Pierre Virleux est chargé de mission à la direction de la Division Production Nucléaire de l'EDF.
Cette volonté de rendre l'homme au cœur de la réflexion, de lui rendre la conduite des installations automatisées, c'était le sujet du dernier rendez-vous des automaticiens au sein du Club Automation. Plusieurs entreprises sont venues donner leur vision sur la place de l'homme.

Maquettage et prototypage dans la cimenterie

Travailler sur un projet neuf est une chose, mais partir dans le revamping d'une installation existante est une autre paire de manches. C'est ce que vient de réaliser, en partenariat avec l'Université de Valenciennes, la plus importante cimenterie Belge. Profiter de l'acquis des opérateurs sur le terrain est un atout qui peut parfois se transformer en inconvénient, chacun souhaitant plutôt conserver ses habitudes anciennes que véritablement migrer vers de nouvelles solutions.

La première étape, menée par l'équipe de Mouldi Sagar, maître de conférence à l'Université de Valenciennes, et qui a piloté le projet, a été d'établir un diagnostic ergonomique. Il a permis d'analyser la situation de référence afin de modéliser la tâche et l'activité. Une sorte d'état des lieux duquel sont tirées les tâches et activités des opérateurs. Dans le cas présent la situation était complexe, la salle de contrôle occupant une superficie de 440 mètres carrés avec un travail posté en 3x8.

Le personnel concerné regroupe, par équipe, deux opérateurs de conduite, un contremaître, un chef de poste, un laborantin et plusieurs rondiers et agents de maintenance. Tous doivent avoir accès aux informations en provenance des 109 automates programmables sur les divers écrans. Un contexte limitant les modifications générales *« la politique ne consistait pas à tout refaire, mais plutôt à rajouter petit bout par petit bout »* confirme Mouldi Sagar.

Le compte-rendu de situation mettait en exergue un manque de cohérence total de l'installation constituée au fil des évolutions. Les opérateurs se retrouvaient à la tête de plusieurs PC gérant l'électricité pour l'un ou les alarmes pour l'autre. Sans compte un nombre de claviers assez impressionnant, chacun d'eux relié à son propre PC.

De cette situation de référence, il fallait atteindre une situation dite « tremplin » avec pour but de dessiner la situation future qui devait se résumer à un PC de gestion avec un écran géant et quelques écrans d'alarmes. Avant d'arriver à la situation finale, plus d'une année de travail aura été nécessaire.

Trois maquettes ont été nécessaires pour valider la nouvelle application, chaque étape devait être dûment explicitée. Que fait-on en cas de démarrage à chaud ? En mode dégradé, quelle est l'action à mener ? *« Il a fallu repasser le film aux opérateurs pour voir comment ils géraient tel ou tel incident »*.

Dans un premier temps les données indirectes, comme les entretiens avec les opérateurs ou les supports de travail, ont été rajoutées aux données directes en provenance des actions et enregistrements verbalisés. En a découlée une caractérisation des situations critiques à partir de commentaires, une identification des structures significatives de l'activité ainsi qu'une analyse quantitative comprenant actions, déplacements et communications.

La première maquette prototype a mis en avant un nombre de courbes beaucoup trop important et qui insistait trop sur la chimie spécifique aux cimentiers plutôt que sur le process des installations. *« Cette maquette a été sévèrement critiquée par les opérateurs. Le point de vue des opérateurs de conduite et des ergonomes n'avait pas été intégré dans cette version »*.

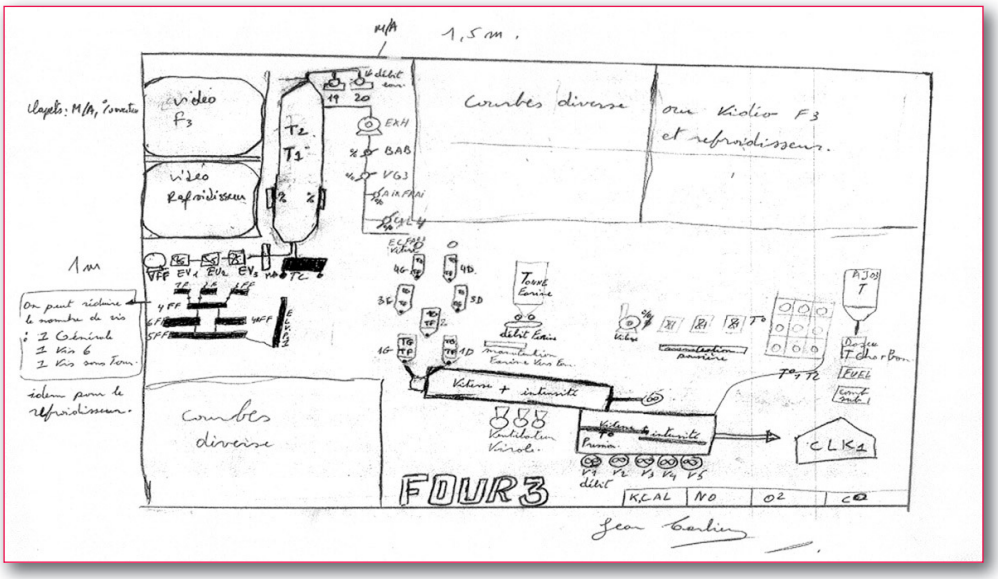
De la première maquette, une deuxième a été établie en prenant en compte le point de vue de chaque opérateur, après rem-

plissage de tableaux identifiant les paramètres utiles. Certains affichages étaient totalement inutiles et les opérateurs avouaient ne jamais s'en servir. Chacun y est allé de son croquis à main levée. Tous les dessins représentaient beaucoup plus le cycle du process de fabrication, certains intégraient même une vidéo du four, plus représentative à leurs yeux que des chiffres.

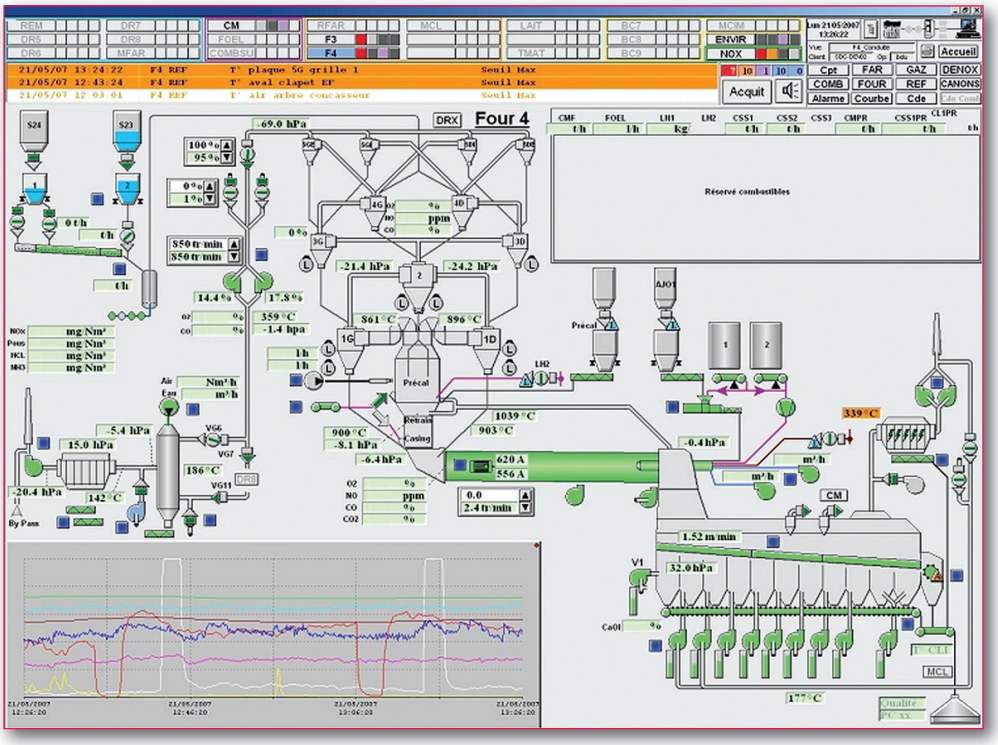
Cette seconde maquette montrait les besoins des opérateurs exprimés dans la première phase d'analyse du travail qui s'opposent au constat, assez théorique, des ingénieurs exprimés dans la première maquette. *« Les opérateurs avaient besoin de plus d'indications sur le niveau des paramètres, leur trajet dans l'installation, leur niveau dans les cuves, l'évolution de la température dans le four en fonction de la couleur de cuisson »*.

La maquette finale fut la synthèse des deux premières, avec une logique de fonctionnement correspondant aux ingénieurs mais également une logique d'utilisation voulue par les opérateurs, ces derniers préférant des chiffres aux courbes. Sont représentées sur les vues, les flux de matières d'une source vers une destination, des états de trémies, des valeurs d'état des dispositifs fonctionnels, des valeurs de mesure soit sous forme de courbe de tendance et/ou directement sous divers formats (graphes, chiffres…).

Avant de se lancer dans la réalisation, une expérimentation ergonomique a été faite, la simulation de la situation future comprenait un écran géant pour la vue de veille, un écran de conduite et un écran d'alarmes, des scénarios de conduite bien précis ont été testés comme le démarrage du four, la conduite normale et en mode dégradé, l'arrêt du four… *« nous avons pu brancher le prototype directement aux automates de processus de production et réaliser une expérimentation ergonomique en présence des opérateurs avec les moyens destinés à la situation future »*.



Maquette V2, vue par les opérateurs.



Vue de la conduite générale actuelle.

Une implication des opérateurs dans le processus de conception qui les positionne comme co-concepteurs du projet global.

Les défis de l'EDF

Pour Pierre Virleux, chargé de mission à la Direction de la Division Production Nucléaire, à l'EDF, le problème à résoudre pouvait se résumer à cette question *« comment économiser les ressources cognitives des opérateurs pour les mettre en situation de pouvoir apporter toute leur intelligence à la résolution de problèmes complexes ? »*.

En France ce sont 58 tranches (réacteurs) jumelées ou séparées qui ont été implantées par lots de 2,4 ou 6 tranches, chacun d'entre elles ayant une production maximum de 900 à 1500 MW. Pour chaque tran-

Contrôle-commande dans la salle de contrôle des tranches 1.300 MW.

che, une salle de commande centralisée et quelques installations décentralisées permettent de remonter les informations en provenance de plusieurs milliers d'actionneurs. Ce sont environ 10.000 informations tout ou rien ou analogiques qui arrivent en salle de commande.

Inutile de dire que les niveaux de sécurité sont très élevés, le risque de fusion du cœur, accident moins grave que Tchernobyl, ayant une probabilité de l'ordre de 10^{-6}. Et l'opérateur fait partie du calcul, Three Mile Island fut le résultat d'une mauvaise interprétation de la part du personnel sur place.

Dans le nucléaire trois types de situations sont à gérer : l'accidentel, la tranche en fonctionnement et l'arrêt de tranche. Le plus courant reste la tranche en fonctionnement qui implique du « doigté » comme le souligne Pierre Virleux *« le travail s'apparente à de la maintenance sur un avion, en vol »*.

Contrôle-commande dans la salle de contrôle des tranches 1.400 MW.

Le personnel de conduite est composé de sept équipes qui fonctionnent en 3x8, avec en permanence une dizaine de personnes (chef d'exploitation, un superviseur, deux opérateurs et un opérateur de configurations locales). Sur le sol français, les contraintes sont à prendre en compte sur trois générations de systèmes de contrôle/commande.

La première équipe les centrales 900 MW qui sont les premières à avoir été installées, la technologie étant plus proche de la commande à relais avec une salle de commande conventionnelle câblée et des écrans d'aide à la conduite rajoutés. La deuxième équipe les centrales de 1300 MW, et intègre les premiers microprocesseurs (MicroZ et Controlbloc Alstom). Dans ces tranches, les écrans ont été prévus lors de la conception avec une gestion des alarmes, mais l'ensemble des expériences acquises avec la première génération n'a pas été intégré lors du développement.

La troisième génération pour les centrales de 1400 MW n'utilise plus la licence d'exploitation Westinghouse et fait appel à une technologie de contrôle/commande numérique. Comme le rappelle Pierre Virleux *« les centrales 1.400 MW étaient les premières dans le monde à afficher de telles ambitions technologiques, ce qui ne s'est pas fait sans douleur, avec plusieurs années de retard »*.

Dans cette dernière génération, la salle de commande est informatisée, avec l'introduction de panneaux auxiliaires en technologie conventionnelle, des alarmes et des fiches d'alarmes informatisées. Egalement informatisées, les consignes de conduite normales et accidentelles.

De ces trois systèmes différents, il est possible de tirer des conclusions, même si les modifications ne peuvent se faire qu'à la marge.

Parmi les bénéfices de la technologie informatique, l'utilisateur note une augmentation du nombre d'informations disponibles au poste de commande ce qui implique une diminution du stress en conduite. A l'inverse, la vision d'ensemble est moins bonne en raison d'un effet tunnel des écrans. Il est également noté un processus de mise à jour des documents informatisés plus complexe. Mais le plus important c'est que le gain en fiabilité n'a pas véritablement bougé *« les progrès entre les premières et les dernières tranches sont insignifiants »*.

Contrairement à la commande à relais, la technologie numérique peut amener à un éloignement du process et donc à une potentielle perte de sens dans les activités d'exploitation, et notamment une perte de compréhension et de suivi des phénomènes physiques.

A l'inverse, cette même technologie permet de disposer de simulateurs de formation réalistes. Dans le cas du nucléaire, chaque centrale dispose de son propre simulateur. De même, seul un contrôle/commande avancé de type numérique autorise les échanges d'informations entre différentes fonctions/métiers de l'exploitation qu'il s'agisse de la conduite, maintenance, gestion technique ou optimisation. Le lien entre la salle de contrôle pouvant se faire via un PDA.

L'ensemble de ces années d'expériences a servi à valider les choix technologiques pour

l'EPR de Flamanville qui devrait entamer sa production en 2012. Pour ce quatrième type de centrale, installé par EDF, le système de contrôle/commande a été choisi sur « étagère », finis les développements internes, ce sera du Siemens qui pilotera.

Un principe de séparation entre les procédures de conduite (méthodes, modes opératoires, fiches d'alarmes) et les images du procédé (permettant de la commander) a été mis en place afin de clarifier le rôle des hommes et celui du contrôle/commande.

Les séquences d'actions, sans plus-value humaine, ont été automatisées. Un pré-câblage a aussi été prévu pour anticiper l'arrivée des technologies sans fil (aide à la conduite, gestion des arrêts de tranche, maintenance…).

Mais l'EPR lancé, l'EDF n'a fini son travail pour autant. Parmi les challenges en cours, on trouve la re-spécification des principales activités d'exploitation afin de définir l'articulation entre une salle de commande « sanctuarisée » et les autres métiers.

De même, les termes utilisés sont souvent trop « administratifs », il faut toujours rechercher à ce que les termes employés aient du sens pour les opérateurs et ne puissent surtout porter à confusion. Le syndrome Three Mile Island plane toujours, quelques 20 ans plus tard. Pour surmonter le risque humain, un travail en commun dès la conception, entre les concepteurs, les exploitants et les spécialistes du facteur humain est la solution pour Pierre Virleux, même si atteindre cet objectif n'est pas toujours évident.

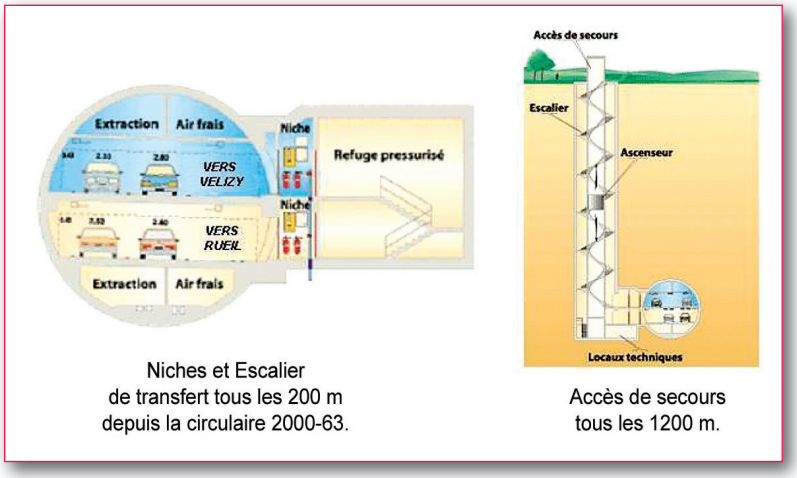
Le nez dans le tunnel

Autre situation à risque, c'est la gestion des tunnels routiers. Dans ce cas, l'événement qui ne doit pas se reproduire est celui de l'incendie du tunnel du Mont-Blanc qui, en Mars 1999, dura 53 heures et provoqua la mort de 39 personnes. Le futur tunnel de l'A86 en région parisienne fait partie de ceux qui ont été conçus après cet accident. La première tranche devrait ouvrir en octobre 2007.

Cette tranche dispose d'une grande densité d'équipements gérés par un système centralisé, le Système de Supervision et de Contrôle Commande (SSCC). *« L'objectif, en sus des fonctionnalités classiques d'une GTC, est de donner à l'exploitant un ensemble d'indicateurs et de moyens lui permettant une gestion facilitée de la crise »* précise Philippe Marsaud, chef de projet du SSCC.

Ce futur tunnel à péage, qui se situera dans l'Ouest de la Région Parisienne, permettra de boucler l'A86 considéré comme le deuxième périphérique autour de la capitale. La partie Est du tunnel aura une longueur d'une dizaine de kilomètres avec une profondeur moyenne de 70 mètres. Pour la première fois, les voies ne seront plus côte à côte, mais superposées. La voie inférieure mènera vers Rueil, la voie supérieure vers Vélizy.

Héritant de la circulaire 2000-63, née de l'accident du Mont-Blanc, des niches avec escalier de transfert sont installées tous les 200 mètres, avec un accès de secours tous les 1.200 mètres vers la surface. La GTC d'une telle installation comprend tout aussi bien la gestion climatique dont la ventilation en cas d'évacuation ; la gestion du trafic, les bouchons étant strictement interdits sous le tunnel ; la gestion des utilités comme l'éclairage ou la vidéo ; la gestion de la communication avec la radio et la téléphonie ; la gestion de la sécurité avec les appels d'urgence et les détections automatiques à partir de systèmes de vision… Le tout étant piloté en permanence par deux opérateurs.



Vue du tunnel Est.

Le premier constat qu'a tiré Philippe Marsaud est simple *« l'opérateur dispose d'un grand nombre de systèmes pour détecter les incidents et mettre en œuvre les actions appropriées, mais ces systèmes peuvent générer un volume important d'informations difficiles à gérer, nous avons 72.000 points de contrôles, plus de 23.000 équipements pour 37.000 alarmes »*.

D'où les choix d'architecture modulaire qui laisse toutes les portes ouvertes pour une intégration future de nouvelles technologies. La durée de vie de l'installation étant largement supérieure à celles des matériels mis en place, la grande difficulté reste d'intégrer toutes ces informations en provenance de matériels hétérogènes, sur un seul superviseur.

La solution qui va être mise en place démarre avec un système de prévision du trafic qui analyse les données en temps réel du trafic Ile-de-France, et effectue la régulation des entrées

Vert RVB (42;241;12)	Tous les moyens qui participent à la réalisation de la fonction sont dans leur état nominal.	Etat nominal du moyen
Orange RVB (255;130;0)	Au moins 1 des moyens qui participent à la réalisation de la fonction est dans en état secouru.	Etat secouru du moyen
Rouge 1 RVB (224;111;95)	Au moins 1 des moyens qui participent à la réalisation de la fonction est défaillant. Les 3 niveaux de défaillance (rouge) sont retenus, indiquant l'importance de la défaillance et son impact possible sur l'exploitation de l'ouvrage.	Seuil de dégradation ayant très peu d'impact sur l'exploitation et ne nécessitant pas forcément la mise en oeuvre d'action compensatoire de la part du superviseur, autre qu'une action de maintenance.
Rouge 2 RVB (221;0;0)		Seuil de dégradation pour lequel des mesures compensatoires pourront être mises en œuvre au travers de FMC CME dans la MCI. Lorsque l'action compensatoire définie ne peut pas être réalisée, il faut alors passer au niveau de défaillance supérieur, voire à l'arrêt
Rouge 3 RVB (113;0;0)		
Noir RVB (0;0;0)	Au moins 1 des moyens qui participent à la réalisation de la fonction présente une défaillance qui implique la fermeture de l'ouvrage.	Seuil de dégradation des performances du moyen (éventuellement couplé à celui d'un ou plusieurs autres moyens) à partir duquel il est jugé que, malgré les mesures compensatoires proposées pour pallier les dégradations de performances définies aux seuils précédents, l'exploitation ne peut plus s'effectuer dans des conditions satisfaisante (conditions d'arrêt).

Indicateurs par code couleurs.

dans le tunnel, le péage servant de barrière efficace. Ensuite, un système d'aide à l'exploitation (SAE) sera implanté pour centraliser la détection des incidents et la réaction à ces incidents. L'enchaînement, suite à l'apparition d'un événement, est qualifié dans une FMC (Fiche Main Courante) avec une proposition d'un plan d'action adapté en réaction à l'alarme d'exploitation avec une validation (ou modification) par l'exploitant.

Les actions proposées sont adaptées au contexte de l'événement et agissent sur les équipements. Elles peuvent être subordonnées à une confirmation de la part du superviseur, la mécanique de construction de plans d'actions reposant sur l'exécution de règles d'exploitations préprogrammées.

Ont également été prévues des Conditions Minimum d'Exploitation (CME) qui répondent au dysfonctionnement total ou partiel d'un équipement ou d'un moyen qui aura conduit à la dégradation, voire à la perte d'une fonction.

Une fois définies les CME permettent d'identifier une aire à l'intérieur de laquelle l'exploitation est possible, ainsi que les conditions associées à cette exploitation. Le rôle de chaque équipement est analysé en fonction de sa contribution à l'exploitation du tunnel. Chaque alarme technique ou d'exploitation est ainsi traitée de manière à animer en permanence un baromètre temps réel de l'exploitation représentant le niveau de disponibilité des fonctions.

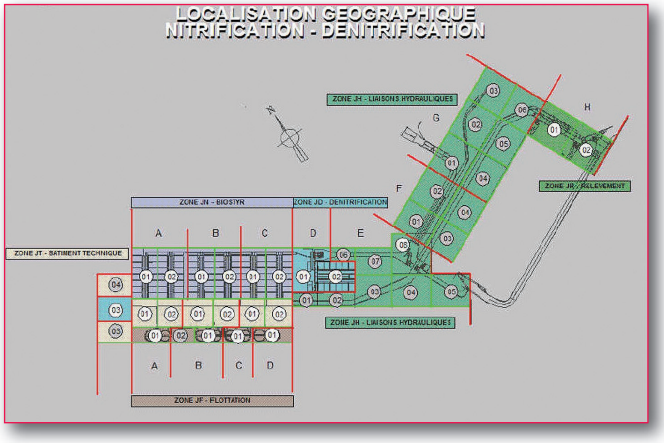
Les défaillances sont regroupées selon quatre niveaux représentés par des couleurs, le dernier correspondant à un dysfonctionnement conduisant à la fermeture de l'ouvrage. Sur ses indicateurs, l'opérateur voit la couleur augmenter d'intensité (de vert à rouge foncé). Plus le pourcentage augmente, plus on se rapproche d'un arrêt.

Standardiser le traitement des eaux

Au total, le SIAAP dépollue, chaque jour, les eaux usées de plus de 8 millions de Franciliens. L'usine d'épuration Seine Aval d'une capacité nominale de 2.100.000 mètres cubes par jour s'est dotée d'une nouvelle entité de nitrification/dénitrification permettant de restituer à la Seine une eau sans nitrate. Sachant que la Seine a un débit d'environ 100 mètres cubes par seconde, l'usine d'Achères est dimensionnée pour en traiter de 24 à 52.

C'est tout début 2007 que les travaux se sont achevés, la période d'étude aura duré 9 mois et la réalisation avec période d'observation une quarantaine de mois. Une période durant laquelle la continuité de service des parties en exploitation devait être assurée.

Après un découpage géographique des fonctions, une étude fonctionnelle proprement dite a été faite. *« Quant on s'attaque à un monstre, on part du haut vers le bas avec la mise en place de strates. L'ensemble de l'étude a été fait conjointement avec le personnel du site »* précise Didier Tavel, ingénieur en automatismes et sûreté de fonctionnement.



Découpage géographico-fonctionnel.

Actionneur	Type de Défaillance	Mode	Etat	Alarme et actions associées		Conseil
Groupes Motopompe 1 et 2	Défaut protection	Mode AUTO	Pompe en marche et Séquence de démarrage	Arrêt du pilotage de la pompe par l'automate Mise en marche de la 2ème pompe si disponible	2	
				Arrêt du pilotage de la pompe par l'automate (2ème pompe non disponible)	1	
			Pompe en marche et en production	Arrêt du pilotage de la pompe par l'automate Mise en marche de la 2ème pompe si disponible	2	
				Arrêt du pilotage de la pompe par l'automate (2ème pompe non disponible)	1	
			Pompe en marche et augmentation de capacité	Arrêt du pilotage de la pompe par l'automate	1	
			Autres Etats (Arrêt et Séquence d'arrêt)	Arrêt du pilotage de la pompe par l'automate	2	
		Mode ESSAI	Tous	Arrêt du pilotage de la pompe par l'automate	3	

Etat des défaillances de la partie Opérative.

Les fonctions définies, le découpage suivant a été technique avec l'élaboration de solutions techniques et, pour chacune d'entre elles, des schémas de procédé et d'instrumentation, des schémas de l'architecture de la distribution électrique et du système de contrôle/commande.

Une analyse des modes de défaillance et de leurs effets sur l'exploitation et la maintenance a été ensuite menée, avec comme première phase l'identification des fonctions critiques avec une analyse des effets d'un fonctionnement dégradé ou de la perte d'une fonction sur chaque file de traitement.

A partir des ateliers critiques, le travail a permis d'identifier les équipements critiques avec la description de leurs effets potentiels avant le traitement de la défaillance.

Suite à la méthode d'Analyse des modes de défaillances, est venue la mise en place de la méthode Gemma (Guide d'étude des modes de marche et d'arrêt) avec 25 SNCC qui dialoguent ensemble. Une conception détaillée des méthodologies *« qui a été un moyen de faire travailler ensemble des personnes qui connaissent le process depuis plus de 20 ans avec de jeunes recrues »* précise Didier Tavel.

Jusqu'à cette étape seule l'architecture a été définie, mais pas encore les interfaces homme-opérateurs. C'est la méthode EERGOS (Etudes ERGonomiques centrées sur les Opérateurs en Situation) qui a été déployée et a permis de concevoir une maquette dynamique soumise ensuite à des « candides ».

L'objectif était de valider que le résultat était cohérent avec les deux termes Utilité et Utilisabilité (« Utilité » permet de vérifier que la fonction mise en place sur l'IHM va servir à quelque chose de réel, « Utilisabilité » correspond à l'étape suivante qui valide que la fonction proposée est assez pédagogique), ces deux

termes étant toujours menés en cohérence et en partenariat avec les utilisateurs sur le terrain.

Au total, 71 réunions GEMMA et 17 réunions SCC ont été nécessaires pour que le système puisse fonctionner sans perte de temps avec, par exemple, l'harmonisation des codes couleur.

Rationaliser les Aéroports

Les ADP (Aéroports de Paris) regroupent un territoire de 6.680 ha, pratiquement la même surface que Paris intra-muros. Ils représentent le deuxième groupe aéroportuaire européen avec un chiffre d'affaires de deux milliards d'euros et 11.000 employés.

Les grands projets d'hier sont complétés par de nouveaux grands projets comme le tri bagages de la partie Est qui traitera 15.000 bagages par heure, on trouve aussi le CDGVAL tout juste mis en service ou le terminal 2G.

Au fil des ans, tous ces grands projets se sont rajoutés les uns aux autres, sans forcément rechercher une homogénéité entre des systèmes de nature aussi différents que ceux destinés à la gestion des parkings ou aux systèmes de balisage.

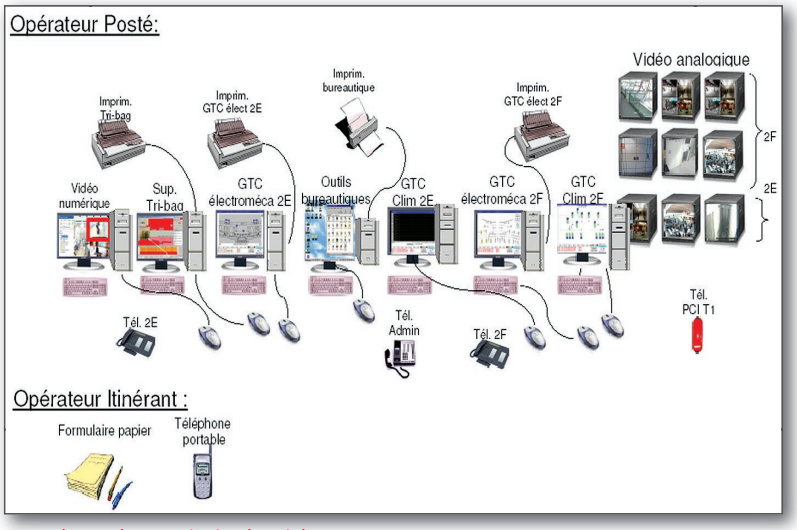
Face à cet état des lieux, une démarche d'optimisation a été menée pour permettre une meilleure visibilité des missions et des outils existants, mais aussi pour définir une solution cible.

Un pilote a été mis en place avec un doublement du matériel existant afin de travailler à partir des informations réelles. Rapidement le projet a mis en exergue le nombre invraisemblable d'imprimantes ou de binômes claviers/souris sur un seul et même poste de travail. La GTC électromécanique avait son imprimante, le tri-bagage aussi, sans parler de la GTC climatisation ou de celle dédiée à la vidéo. A l'inverse, pour l'opérateur itinérant le matériel était dérisoire, un formulaire papier étant le plus souvent son seul outil.

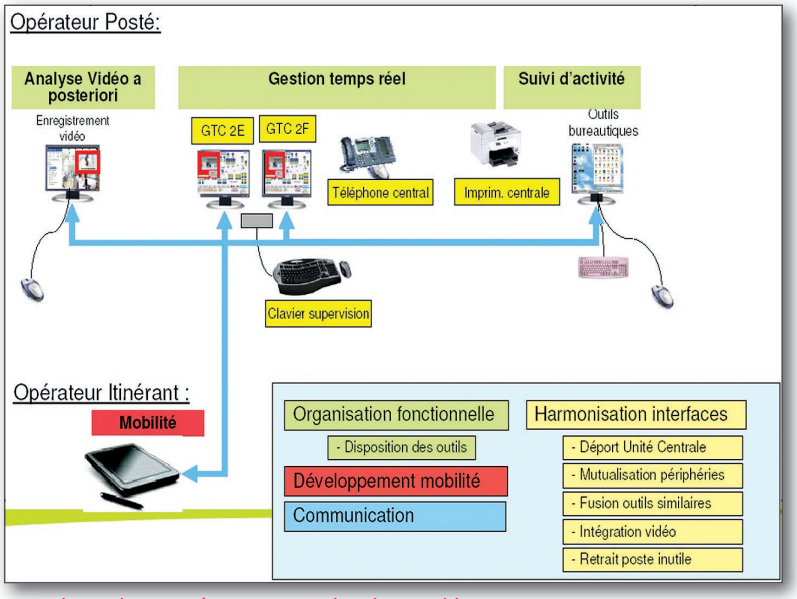
En dehors du poste d'analyse vidéo, l'ensemble des informations a pu être réuni sur une interface unique pour l'opérateur posté. Changement radical également pour l'opérateur itinérant qui se déplace maintenant avec une tablette mobile pouvant accéder, en tout lieu, à l'ensemble des informations aussi bien de supervision que de vidéos. Il peut même récupérer des formulaires ou recevoir des alarmes directement sur le terrain, l'ensemble de la surface étant couvert par deux réseaux, un GPRS et un Wifi.

Pour le poste principal, un travail important fut l'élimination des fausses alarmes, avec hiérarchisation de celles retenues. Certains objets, présents sur l'interface, sont dynamiques et en lien direct avec Autocad, tout changement dans le logiciel de conception est passé dans la moulinette et vient enrichir l'interface opérateur.

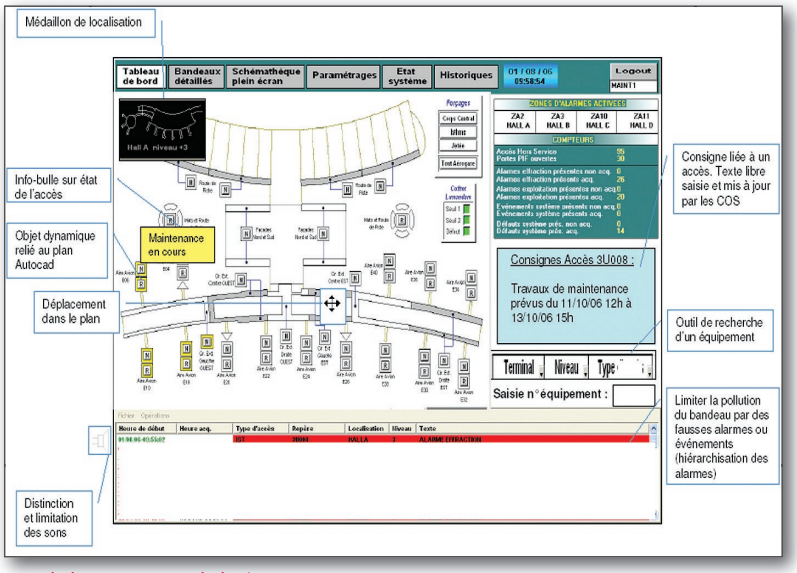
Lors de la consultation, les opérateurs ont même demandé qu'en cas d'alarme critique une fenêtre contenant les informations viennent au-dessus de l'ensemble des autres affichages et ne puisse disparaître qu'une fois acquittée. C'est aujourd'hui le cas lors d'intrusion dans une zone protégée. Bien entendu, le nombre de cas est restreint, il n'était pas question de transformer le poste de l'opérateur en une vaste « boîte de nuit ».



Poste de conduite intégré, tel qu'à l'origine.



Poste de conduite une fois revue pour la solution cible.



Vue de la supervision de l'aérogare CDG.