

Caisse Nationale de l'Assurance Maladie

des Travailleurs Salariés

Sécurité Sociale

Circulaire CNAMTS

Date :
08/12/87

Origine :
PAT

MM les Directeurs
des Caisses Régionales d'Assurance Maladie

MM les Directeurs
des Caisses Générales de Sécurité Sociale

Réf. :

PAT n° 1203/87

Plan de classement :

26102					
-------	--	--	--	--	--

Objet :

DIFFUSION DE LA NOTE TECHNIQUE RELATIVE A L'INTRODUCTION DE L'INFORMATIQUE
DANS LES PROCEDES DE FABRICATION

Les Directeurs des CRAM et CGSS sont invités à diffuser auprès des entreprises concernées de leur circonscription la note technique susvisée, approuvée par le Comité Technique National des Industries Chimiques le 1er décembre 1987.

Pièces jointes :

0	1
---	---

Liens :

Date d'effet :

Date de Réponse :

Dossier suivi par :

Téléphone :

@

08/12/87

Origine :
PAT

MM les Directeurs
des Caisses Régionales d'Assurance Maladie

MM les Directeurs
des Caisses Générales de Sécurité Sociale

N/Réf. : PAT N° 1203/87

Objet : Diffusion d'une Note Technique

Lors de sa réunion du 1er décembre 1987, le Comité Technique National des Industries Chimiques a adopté la Note Technique ci-jointe, relative à l'introduction de l'informatique dans les procédés de fabrication.

Conformément à la demande du Comité, j'ai l'honneur de vous prier de bien vouloir diffuser cette Note auprès des entreprises concernées de vos circonscriptions.

D'autre part, j'ai demandé à l'Institut National de Recherche et de Sécurité de publier cette Note dans la revue "Travail et Sécurité".

Vous voudrez bien faire connaître à cet organisme le nombre de tirés à part qui vous seront nécessaires pour assurer la diffusion de ce document.

Pour le Directeur
Le responsable de la Division
Prévention des AT et des MP

P. ZIMBERLIN

INTRODUCTION DE L'INFORMATIQUE DANS

LES PROCEDES DE FABRICATION

**NOTE TECHNIQUE APPROUVEE PAR LE COMITE TECHNIQUE NATIONAL
DES INDUSTRIES CHIMIQUES LE 1er DECEMBRE 1987**

I - AVANT-PROPOS

1.1. Mode de conduite des installations

La conduite des installations de l'Industrie Chimique subit une mutation très rapide.

L'époque n'est pas si lointaine où les opérateurs agissaient directement et manuellement sur les organes de manoeuvre et de commande des différents matériels en fonction des paramètres physico-chimiques qui étaient, eux aussi, quelquefois directement mesurés sur les lieux des opérations ou sur des échantillons prélevés dans les produits de réactions.

Puis, peu à peu, les commandes à distance se sont généralisées, au moins dans les unités continues, dès lors que l'on a su reporter en salle de contrôle les informations nécessaires à la conduite et que l'on a pu agir sur les dispositifs de commande par l'emploi de la pneumatique ou des servomoteurs.

On a assisté alors à la généralisation de la conduite des unités à partir des salles de contrôle, où les opérateurs avaient devant les yeux des synoptiques plus ou moins vastes avec les valeurs des paramètres sur indicateurs ou enregistreurs. On a pu alors installer des niveaux d'intervention ou d'alarme sur les paramètres les plus sensibles.

Ces opérations nécessitaient toujours l'intervention d'un ou plusieurs opérateurs sur un mécanisme de commande.

Ces systèmes ont été plus ou moins développés suivant l'importance des unités et le type de travail en continu ou discontinu.

Souvent des interventions sur certains organes au sein même de l'unité, restaient indispensables, ceci étant assez fréquent dans les opérations discontinues.

Une autre étape a été franchie lorsque l'on a su utiliser des régulations qui ont permis la réalisation d'opérations automatiques dans les limites des paramètres définis, sans l'intervention d'opérateurs.

Pour ces opérations, seuls des dépassements de paramètres entraînaient l'intervention des opérateurs.

Enfin, le développement de l'informatique a permis de faire prendre en charge par l'ordinateur le contrôle des procédés de fabrication. On pourrait imaginer que ce contrôle soit total et qu'il ne soit alors plus nécessaire de reporter en salle de contrôle des informations sur le déroulement des opérations dans les unités. Dans la quasi-totalité des cas connus, ce stade n'est pas encore franchi, ne serait-ce que pour des raisons de sécurité des biens et des personnes, dans l'état actuel des techniques, les systèmes d'exploitation en service n'étant pas encore à même de prévoir tous les incidents dans toutes les circonstances, et surtout, de savoir y porter remède.

Aussi, aujourd'hui, voit-on se développer des salles de contrôle où les opérateurs disposent d'écrans et de claviers qui leur fournissent un certain nombre d'informations et leur permettent d'interroger le système sur l'état de déroulement du procédé et, également, d'intervenir sur certaines phases par l'intermédiaire d'organes de commandes.

1.2. Perception du processus par les opérateurs

Avant l'informatique, les opérateurs en salle de contrôle, d'un seul regard sur les tableaux synoptiques, disposaient en général de l'ensemble des données du procédé et réagissaient en fonction des variations qu'ils constataient ainsi qu'aux alarmes déclenchées par les automatismes. Ils avaient donc une perception globale du processus. Ils pouvaient de plus recevoir des informations complémentaires ponctuelles provenant des rondiers éventuellement à leur demande.

Avec le développement de l'informatique, les grands synoptiques ont disparu pour être remplacés par des écrans sur lesquels les opérateurs peuvent faire apparaître soit un synoptique général avec un nombre d'informations réduites, soit, comme par effet de "zoom", des synoptiques de détails où les informations sont évidemment plus complètes. Plus le procédé est automatisé et plus il est piloté par l'ordinateur, moins il est a priori nécessaire de faire figurer des informations sur les écrans. Par contre, les procédés informatiques permettent de rendre accessibles à la demande, de multiples informations complémentaires. Malgré cela, et comme on le verra, puisqu'il n'est pas souhaitable de surcharger les écrans, les opérateurs ressentent un manque d'informations sur le déroulement du processus dont ils ont l'impression d'être dessaisis. Ceci est particulièrement sensible lors de la nécessité de leurs interventions sur alarme où il leur semble manquer d'une vue générale des réactions en cascade possibles, d'autant que les différents "écrans" ne peuvent être visibles simultanément.

Ces évolutions, et d'autres facteurs qui seront développés plus loin, font qu'il est nécessaire d'étudier à l'avance une introduction de l'informatique dans un processus de fabrication, de manière à ce qu'elle soit mieux ressentie par le personnel et que le procédé soit en même temps le plus performant, en respectant toutes les règles de sécurité.

2 - MISE EN PLACE DE PROCESSUS UTILISANT L'INFORMATIQUE

2.2. Etudes préalables

a) Analyse des risques

Un examen préalable du procédé est nécessaire avant toute mise en place de l'informatique. Cet examen doit comporter une analyse des risques, c'est-à-dire la recherche de tous les paramètres influant sur la nécessité du bon déroulement des opérations, ainsi que des remèdes ou dispositifs nécessaires à mettre en place, afin que la sécurité des biens et des personnes soit assurée quelles que soient les circonstances.

Cette analyse doit être faite avec autant de précisions qu'il s'agisse d'un procédé nouveau ou ancien, d'une nouvelle implantation ou de l'intégration de l'informatique dans une installation existante. Elle doit orienter vers les conditions les plus élevées de sécurité.

Il convient de définir les paramètres influant dès le début de l'analyse afin de pouvoir les intégrer dans les logiciels de conduite qui seront utilisés par l'ordinateur. Ce dernier ne peut improviser en cas d'incident ; tous les incidents que l'on peut imaginer et leurs remèdes doivent être prévus à l'avance.

Il existe différentes méthodes pour réaliser les analyses de risques. Certaines ont été développées par des grosses entreprises de l'industrie chimique ou par des organisations professionnelles.

Une telle analyse doit être menée en collaboration étroite avec les futurs responsables de l'unité, à tous les niveaux techniques, ainsi qu'avec le personnel qui conduira les installations.

D'une manière générale, les connaissances des responsables d'unité et des opérateurs doivent être utilisées, en particulier lorsqu'il s'agit d'installations existantes à modifier.

Pour un procédé nouveau, cette analyse de risque doit être engagée dès la phase pilote et semi-industrielle et être complétée au fur et à mesure du développement du procédé, en s'efforçant de rendre le procédé le plus simple possible.

L'analyse des risques doit donc prendre en compte les éventuelles défaillances du système informatique, dont les effets imprévisibles priveraient l'opérateur d'informations contrôlées ou l'unité de son pilotage. Dans ce dernier cas, il est indispensable de placer l'unité en position de sécurité ou de disposer d'une autre manière de pilotage pour au minimum pouvoir la mettre en sécurité dans un délai qui doit permettre d'éviter toute atteinte grave aux personnes et aux installations, ce qui conditionne le personnel nécessaire.

b) Etude du pilotage de l'unité

Parmi les points de l'unité ou les phases du processus qui peuvent être automatisées ou régulées, on déterminera ceux dont la défaillance (écart excessif par rapport à la

fourchette de régulation par exemple) entraînerait des conséquences suffisamment importantes sur le fonctionnement de l'unité pour être dangereuses. Ils seront hiérarchisés et c'est à partir de cette hiérarchie que l'on pourra déterminer les informations indispensables ou secondaires qui devront être prises en compte par l'ordinateur et éventuellement signalées aux opérateurs.

Il faudra également déterminer si les procédures de mise en route et d'arrêt pourront être intégrées dans les programmes informatiques ou si ces opérations resteront commandées manuellement.

Il devra être prévu les procédures qui, en cas d'incident, permettent le repli sur une position stable non dangereuse, voire l'arrêt en sécurité ou total ainsi que les remises en route.

Toutes les procédures qui ne seraient pas prises totalement en compte par l'ordinateur doivent être parfaitement claires et ne pas prêter à interprétation de la part de ceux qui auront à les employer.

c) Travail et poste de travail des opérateurs

Il importe de définir parfaitement ce que doit être la tâche des opérateurs et la part de leur participation effective au pilotage du procédé, autrement dit, de définir qui, de l'opérateur ou de l'ordinateur, déclenche les actions sur les organes de commande et à partir de quel critère.

A supposer que toutes ces actions soient prises en charge par l'ordinateur, il conviendra de fournir néanmoins aux opérateurs un certain nombre d'informations qui doivent leur permettre de surveiller le déroulement des opérations et le cas échéant, de reprendre en main le système dégradé.

On s'attachera à :

- fournir des informations sur le point de fonctionnement et sa position relative par rapport aux limites,
- fournir toutes les informations utiles : cette règle semble évidente mais elle est souvent oubliée,
- ne pas fournir trop d'informations, c'est-à-dire certaines informations inutiles parce qu'elles sont redondantes ou sans rapport avec le fonctionnement,
- fournir des informations faciles à interpréter pour mieux utiliser et alléger le travail de réflexion de l'opérateur,
- ne pas exiger un trop grand nombre d'actions sur les commandes et faire en sorte que ces actions soient sans ambiguïté, faciles à concevoir et à exécuter, dans un court délai compatible avec le temps de réaction de l'installation,

- laisser à l'opérateur la possibilité de fonctionner manuellement, c'est-à-dire de corriger ses actions en suivant l'évolution des paramètres à corriger. C'est ce que l'on fait lorsqu'une régulation est en panne et que l'on intervient en commande manuelle.

Au cours de l'exploitation du procédé, il pourra s'avérer indispensable de réintroduire de nouvelles informations nécessaires à la conduite de l'unité. Ceci suppose que le matériel informatique ait une capacité de réserve suffisante ou qu'il soit extensible.

Il va de soi que toute modification doit alors être portée à la connaissance du personnel de conduite.

L'objectif de ces règles de pilotabilité est essentiellement de réduire la charge de travail de l'opérateur lorsqu'il doit reprendre en main un système dégradé que l'ordinateur ne peut maîtriser car il s'agit d'incidents non prévus ou imprévisibles.

Si l'un des buts de l'informatique est de décharger l'opérateur du plus grand nombre possible d'opérations physiques et intellectuelles, il ne faut pas pour autant lui supprimer toute matière à réflexion et action, car on risque d'émousser ses réflexes et de lui faire perdre ses facultés de prévision et d'extrapolation, ce qui peut avoir des conséquences fâcheuses : la première, l'insatisfaction à ne plus participer suffisamment au processus, la seconde, l'absence de réaction ou des réactions dans le mauvais sens lors d'incidents imprévisibles, par manque de vigilance ou d'habitude.

La définition des alarmes est extrêmement importante, leur fonction est d'être parfaitement perçues par l'opérateur et claires dans leur signification.

Le dysfonctionnement d'un paramètre ou d'un composant important pour la sécurité, entraîne souvent, par propagation dans le système, la mise en alarme d'un grand nombre de paramètres. Pour ne pas risquer d'étourdir l'opérateur, il convient d'en hiérarchiser les alarmes, c'est-à-dire, avoir des alarmes bien marquées, sonores et lumineuses, pour une défaillance primaire, les autres défaillances qui en résultent étant signalées par des alarmes plus discrètes (clignotants par exemple). Il est souhaitable de rendre immédiatement apparentes à l'opérateur au poste de conduite, les alarmes primordiales pour la sécurité.

Le pilotage "aux alarmes" est à proscrire. Il ne faut pas attendre l'alarme pour commencer à réagir. C'est pourquoi, il est très important de pouvoir avoir sous les yeux l'évolution de variables que l'opérateur pourra sélectionner. On a ainsi une pré-alerte, qui généralement laisse un temps suffisant pour préparer une éventuelle stratégie si la dérive s'accentue.

Le fait de ne disposer que d'informations ponctuelles ne permet pas de détecter et de suivre une dégradation lente.

L'ensemble des informations ainsi collectées doit permettre d'établir un diagnostic.

Suivant les processus et la marge de manoeuvre existant entre le point de consigne et l'alarme à ne pas franchir, le traitement à effectuer pourrait être pris en charge par les

opérateurs (temps suffisant de réaction) ou par les automatismes. Quel que soit le système utilisé, les opérateurs devront avoir un retour d'information sur les actions effectivement réalisées sur l'unité.

On devra définir qui, des opérateurs ou des automatismes, devront conduire l'installation vers une situation stable en sécurité, en cas d'incident incontrôlable ou de panne du système de contrôle. La procédure devra être établie à l'avance et parfaitement connue. Là encore, la notion de marge de manoeuvre est à prendre en considération quant aux temps de réaction des opérateurs et des résultats des actions sur l'unité.

d) L'ergonomie des systèmes

- L'information

On l'a vu, toutes les informations fournies doivent être claires et facilement compréhensibles, les actions sans ambiguïté, voire réflexes.

Il faut éviter la trop grande abondance d'informations, sans pour autant la réduire à néant.

Les opérateurs doivent pouvoir, lorsqu'ils le souhaitent, obtenir temporairement des informations complémentaires à celles qui apparaissent en permanence. Le temps nécessaire à l'acquisition de ces informations complémentaires doit être compatible avec les actions demandées aux opérateurs.

- Représentation de l'information

On rencontre souvent la présentation d'un paramètre de fonctionnement sous forme digitale : l'opérateur doit lire un nombre et le situer par rapport à des limites. Un index se déplaçant entre ces limites donne une information équivalente en exigeant un travail mental bien plus faible et limite les erreurs d'interprétation.

La présentation digitale ne présente que des inconvénients pour le pilotage d'un paramètre, car il est très difficile d'en déduire la grandeur de l'écart par rapport à la valeur nominale, le sens de l'écart et la vitesse de variation de l'écart, alors que tous ces éléments sont évidents en présentation analogique où l'on peut voir effectivement l'évolution du système.

L'élaboration des tactiques et des stratégies passe par une parfaite compréhension de l'état du système et de son évolution. Les informations fournies par le système informatique doivent être présentées de manière à permettre et faciliter cette compréhension.

- Charge de travail

Les opérateurs de pilotage peuvent en général être automatisés parce qu'elles dépendent de règles opératoires conduisant à une décision très simple. Dans un contrôle de

processus, il y a toujours intérêt à soulager l'opérateur des opérations de pilotage, en l'assistant par des automatismes, tout en lui laissant le travail de conduite pour lequel les prises de décision sont beaucoup plus délicates. En effet, il n'est généralement pas facile de prévoir toutes les situations possibles, donc de prévoir toutes les réponses nécessaires.

Le système doit être conçu pour que la charge de travail de chaque opérateur prévu pour son fonctionnement, lui permette de conduire les unités, surtout en situation dégradée.

Avec l'introduction massive de l'informatique dans les contrôles de processus, on a vu apparaître des présentations d'informations sous forme de tableaux de chiffres, ces tableaux permettent, a posteriori, de suivre de façon très précise, l'état instantané du système, mais ils ne permettent en aucun cas, de suivre son évolution ni d'avoir une idée globale et rapide de la situation.

L'imprimante périphérique classique, destinée à enregistrer les informations qui seront dépouillées ultérieurement, doit être éloignée de la zone de contrôle. Elle est non seulement souvent bruyante, mais n'est pas destinée à la conduite de l'unité, elle peut être même gênante dans la mesure où les opérateurs se fient à ses réponses plutôt qu'aux écrans.

Elle peut être remplacée dans la mesure du possible par d'autres systèmes de mémorisation.

Si pour une raison quelconque elle ne pouvait être éloignée, elle devrait être, si nécessaire, insonorisée.

Les salles de contrôle et les matériels devront être disposés et aménagés de façon ergonomique en tenant compte, entre autres choses, de l'éclairage et de l'ensoleillement. On pourra se reporter à la brochure de l'INRS n° 513 "La conception des usines et la sécurité" épuisée en ce qui concerne le choix des couleurs.

2.3. Mise en place du système

Pour faciliter la mise en place du système, on aura fait participer le personnel de l'unité à sa définition et à sa réalisation, s'il est déjà désigné.

Tout le personnel devra avoir reçu une formation particulière pour le familiariser avec le nouveau système de conduite.

Il y a un intérêt tout particulier à ce que l'on puisse disposer de consoles servant de simulateurs reproduisant le déroulement du procédé avec la possibilité de simuler des pannes.

Ces simulateurs pourront être utilisés ultérieurement pour la formation de nouveaux embauchés ou le recyclage du personnel.

2.4. Suivi du système

Compte tenu des capacités de stockage d'informations que permet l'informatique, il y a tout intérêt à conserver l'historique de marche des installations, ce qui peut permettre à terme d'étudier les divers incidents et d'en rechercher les causes. Ceci peut conduire à une amélioration du processus ainsi que son mode de conduite.

Sachant que, même si le système est bien conçu, il peut y avoir une perte de vigilance des opérateurs par routine, il est bon de veiller à leur entraînement périodique en simulant des incidents, ceux-ci étant peu fréquents en conduite normale, la conduite d'exception ne peut s'apprendre que sur simulation indépendante de l'installation.

Il va de soi que le plus grand soin doit être apporté à assurer la permanence des liaisons contrôle-unité et unité-contrôle ainsi que des capteurs.

Par ailleurs, l'informatique n'étant pas un garant du bon fonctionnement mécanique ou électrique des installations, celles-ci nécessitent au moins autant que celles qui ne sont pas informatisées, un entretien rigoureux du fait du manque partiel de contrôle visuel permanent.

Cependant, pour le suivi des dérives progressives, l'informatique peut être une aide au diagnostic des prévisions de pannes.