Plate-forme pour la conduite interactive et sûre

Fabien Clanché, David Gouyon, Dragos Dobre, Jean-François Pétin, Gérard Morel

Plate-forme pour la conduite interactive et sûre

Fabien Clanché, David Gouyon, Dragoş Dobre, Jean-François Pétin, Gérard Morel

[1] Centre de Recherche en Automatique de Nancy (CRAN)
UMR 7039 CNRS Nancy Université
Faculté des Sciences et Technologies – BP 70239
54506 Vandœuvre-lès-Nancy Cedex
{fabien.clanche;david.gouyon;dragos.dobre;jean-françois.petin;gerard.morel}@cran.uhp-nancy.fr

***Résumé* – La plate-forme CISPI, représentative de la variété des modes opératoires d'une tranche de centrale de production d'électricité, est intégrée dans un ensemble de démonstrateurs dédiés à la sûreté de fonctionnement (SAFETECH). Afin de palier aux dégradations et défaillances du système, ainsi qu'aux erreurs humaines de conduite, cette plate-forme expérimentale a pour objectif d'illustrer de nouvelles formes d'organisation de la commande et de la conduite de procédés industriels exploitant au mieux les capacités de stockage, de traitement et de communication de nouvelles technologies ambiantes pour favoriser une sécurité active (interactions homme/système, opérateurs en salle de commande/opérateurs de terrain, produits/système) des procédés.**

***Mots clés* – plate-forme expérimentale, contrôle-commande, interaction homme-système, intelligence ambiante, sûreté de fonctionnement, ingénierie système**

1. Introduction

Dans le cadre du CPER MISN, le CRAN développe un centre d'innovation et de démonstration des technologies sûres de fonctionnement nommé SAFETECH. Celui-ci est composé de plusieurs plates-formes industrielles pilotes afin d'illustrer les résultats scientifiques. Dans cet article, nous nous intéressons au démonstrateur dédié à la conduite de grands systèmes industriels à risque CISPI.

La conduite de ces procédés met en jeu un ensemble de processus complexes couvrants des modes opératoires variés (en production, en arrêt, en démarrage, etc) adaptés à la criticité des modes d'exploitation rencontrés (conduite normale, conduite incidentelle et accidentelle) selon des constantes de temps différentes (conduite en temps réel, maintenance hors ligne, …). Aujourd'hui, ces processus reposent sur des interactions entre les différents métiers des opérateurs et des systèmes propriétaires, hétérogènes et généralement limités à la phase de production normale.

Le démonstrateur développé au sein du service plates-formes expérimentale du CRAN illustre les travaux de recherche en IAM (Intelligent Actuation Mesurement) [1] et couvre les besoins pour valider les travaux actuels portant sur la sûreté active et sur l'ingénierie système basée sur les modèles.

Dans cet article, après avoir donné le contexte, les enjeux industriels et les verrous scientifiques liés à la conduite de grands systèmes à risque dans la section suivante, nous détaillerons l'architecture de la plate-forme existante, puis présenterons les travaux de recherche actuellement en cours.

2. Contexte et objectifs

De nos jours, la prise en compte des défauts/défaillances dans les systèmes socio-techniques critiques et/ou complexes, constitue un enjeu important tant sur le plan économique que scientifique, puisqu'à titre indicatif plus de 65% des problèmes de production sont liés à la présence de défaillances.

En ce sens, les travaux scientifiques ayant leur application sur la plate-forme s'inscrivent dans le contexte national et international des recherches développées :

- d'une part dans le domaine de la sécurité et de la sûreté de fonctionnement, en particulier des Systèmes à Evénements Discrets et des Systèmes Contrôlés en Réseau,
- d'autre part dans le domaine de l'Ingénierie Système nécessaire pour maîtriser les interactions et interopérations entre composants d'un système complexe.

2.1 Enjeux industriels

Les grands systèmes industriels (en particulier les centrales de production d'énergie) comportent une majorité d'équipements non instrumentés qui sont pilotés par des opérateurs de terrain [2]. Cela implique que la conduite est dépendante de décisions d'exploitation prises au plus près du procédé, par les opérateurs présents sur le terrain (les rondiers).
Le premier enjeu industriel est de déployer de nouvelles technologies dites ambiantes sur les différents niveaux des systèmes de production (du pilotage d'atelier jusqu'au contrôle le plus fin à l'échelle du capteur ou de l'actionneur) afin de permettre d'une part une meilleure analyse de la situation, et d'autre part de suivre les procédures les plus appropriées.
Le second enjeu industriel est de répartir les rôles entre opérateurs en salle de commande centralisée et rondiers sur le terrain dans les différents modes de fonctionnement, et d'en tenir compte, au plus tôt, dans les différents processus d'ingénierie.

2.2 Verrous scientifiques

La mise en œuvre de ces nouvelles technologies dans les systèmes industriels conduit à des architectures distribuées de plus en plus complexes basées sur la coopération d'objets logiciels dans lesquelles la communication joue un rôle prépondérant. Cette complexité peut engendrer des phénomènes émergeants liés aux interactions entre les constituants du système qui peuvent être à l'origine de comportements souvent néfastes, difficiles à prévoir et à maîtriser.
Les principaux défis scientifiques à relever concernent :

- la définition de stratégies de reconfiguration dynamique des architectures de conduite et de commande dans un contexte de mobilité des applications induits par les technologies ambiantes,
- la modélisation multi points de vue (commande, supervision, réseau sans fil, …) et multi-formalismes (modèles comportementaux, modèles structurels, fonctionnels, système, …) de ces architectures incluant des technologies ambiantes et l'évaluation de leurs performances (sûreté de fonctionnement, performances temporelles, …), en d'autres termes, combiner les approches formelles issues du Génie Automatique et les approches moins formelles issues de l'Ingénierie Système pour modéliser, vérifier et implanter des architectures de commande et de conduite interactive et sûre basée sur la mise en œuvre de technologies ambiantes,
- la garantie de la qualité de service de systèmes interopérants en maîtrisant à la fois les propriétés intrinsèques à chacun des systèmes (pilotage, commande, communication, …), et les propriétés émergentes issues de ces interactions multiples afin d'en limiter les effets.

3. Présentation de la plate-forme

L'objectif du démonstrateur est d'expérimenter de nouvelles formes d'organisation de la commande et de la conduite de procédés industriels exploitant au mieux les capacités de stockage, de traitement et de communication de l'information de nouvelles technologies ambiantes pour favoriser une sécurité active (interactions homme/système, produits/système) des procédés.

Pour illustrer ces aspects, le procédé pilote à développer devait satisfaire à différentes contraintes :

- s’apparenter à un système réel, c’est-à-dire proposer un ensemble représentatif de processus complexes couvrants des modes opératoires variés (en production, en arrêt, en démarrage, etc), représentatifs de la criticité des modes d’exploitation réels (conduite normale, conduite incidentelle et accidentelle) selon des constantes de temps différentes (conduite en temps réel, maintenance hors ligne, …). En ce sens, il doit être composé d’un nombre suffisant d’équipements (vannes, robinets, cuves, …) et de lignages permettant la circulation des fluides ;
- mettre en œuvre des technologies ambiantes (PDA, réseau de capteurs sans-fil et tags RFID, …) afin d’assister les opérateurs de conduite locale dans leur mission ;
- mettre en œuvre des technologies dédiées à la sûreté (automates de sécurité, onduleur, etc) et proposer des mécanismes redondants (lignages, etc …) afin d’optimiser son fonctionnement ;
- être conforme aux directives européennes et aux règles, normes et conseils de l’Institut National de Recherche et Sécurité (INRS) afin de garantir l’intégrité physique des personnes ;
- pouvoir être installé dans une salle de manipulation de taille réduite (35 m² maximum).

Les différentes possibilités d’utilisation de la plate-forme en recherche et en enseignement ont amené sont installation au sein du service plates-formes expérimentales du CRAN. Ce service, transverse aux différents groupes thématiques de recherche, a pour vocation la conception, la réalisation et l’exploitation de différentes plates-formes expérimentales et de démonstrateurs. Il s’est donc chargé de la conception, du développement et du déploiement du dispositif CISPI dans les locaux du CRAN.

3.1 Partie opérative

Le démonstrateur retenu est un procédé inspiré à ceux que l’on rencontre dans les centrales nucléaires. Ces systèmes de production d’énergie utilisent la fission de noyaux atomiques pour produire de la chaleur, dont une partie est transformée en électricité (entre 30% et 40% en fonction de la différence de température entre la source froide et chaude). Le principe de fonctionnement de notre démonstrateur, appelé CISPI, consiste en la préparation d’un mélange constitué d’eau et d’adjuvant qui doit ensuite suivre différents lignages afin de simuler le refroidissement de la tranche d’une centrale nucléaire (Figure 1).

Le procédé pilote est constitué de 4 stations de travail (Figure 2). La « Station commande » est destinée à faire coopérer les autres stations de travail dans un objectif de conduite locale. Elle intègre un écran tactile pour la conduite locale, un automate de sécurité maître servant d’interface entre les entrées/sorties déportées dans les autres stations et les systèmes de supervision, et un pupitre rendant compte de l’état du système. La station « Régulation 1 » permet de faire circuler le mélange selon un débit paramétré afin de simuler le refroidissement de la tranche, elle comprend une vanne de régulation, des capteurs de niveau et de débit. La station « Régulation 2 » est redondante pour garantir le refroidissement en cas de défaillance ou de maintenance de la station « Régulation 1 ». La station « élaboration » est chargée de la fabrication du mélange et de son évacuation, et est constituée de trois cuves (adjuvant, élaboration et stockage). La Figure 3 présente la partie opérative de la plate-forme.

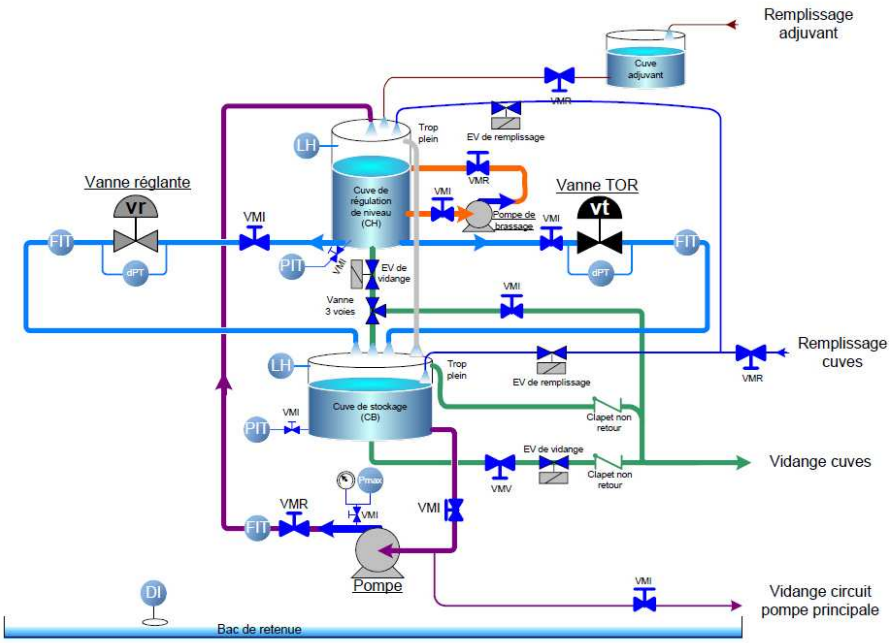

Figure 1 : Plan de circulation des fluides

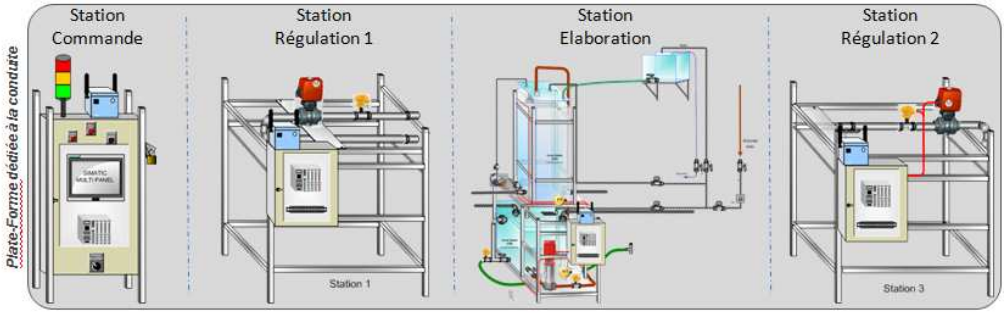

Figure 2 : Stations de travail

Figure 3 : Vue des stations

3.2 Architecture de conduite et de commande

La salle de commande permet aux opérateurs de surveiller et de réguler les différents indicateurs du procédé expérimental (débit de circulation du fluide, temps de brassage, …) de façon centralisée. La conduite centralisée est réalisée au travers de pupitres de supervision (représentant les équipements de conduite centralisés en salle de commande (Figure 4) ou les interfaces de pilotage locales) et d'équipements mobiles (PDA, …) permettant aux opérateurs de conduite d'interagir localement avec les actionneurs et/ou capteurs. Pour cela, plusieurs serveurs (conduite, système d'information et maintenance, OPC, simulation, …) ont été mis en place.

Figure 4 : Salle de commande

La plate-forme est commandée par un automate de sécurité S7 315 2PN/DP Siemens et 3 modules d'entrées/sorties déportées (dont un de sécurité) ET200S dans les différentes stations. Les différents programmes embarqués dans ces équipements de sécurité participent au respect des exigences de sûreté de fonctionnement d'un système industriel critique.

Les différentes commandes, initiées depuis cette salle sont transmises à l'opérateur de terrain (rondier) situé au pied de la machine. Le rondier peut intervenir sur les composants non instrumentés ou sur un écran tactile connecté à la partie automatisme afin de préparer le procédé au mode d'exploitation (remplissage de la cuve d'adjuvant, préparation du mélange, …) choisi par l'opérateur en salle de commande. Cette interaction est rendue possible grâce à un PDA industriel (Psion Teklogix) équipé d'un module wifi. Afin de favoriser l'interaction entre l'homme et le système industriel, les vannes sont équipées de tags RFID et de capteurs sans-fil pour permettre d'une part, l'identification de ces matériels et d'autre part le renvoi de son état (ouvert ou fermé) au système de supervision.

3.3 Architecture de communication

L'architecture de communication (Figure 5) est répartie sur 2 réseaux. D'une part, le réseau « industriel » met en interaction les équipements décentralisés de CISPI, et d'autre part le réseau « d'entreprise » où circulent des informations très diverses (enseignement/recherche, comptabilité, internet). Cette stratégie sécurise les échanges entre composants de la plate-forme face aux attaques potentielles (virus, malware). De plus, les communications ne sont pas dépendantes de la charge du réseau d'entreprise (téléchargements, visioconférences, …). Un serveur OPC (OLE for Process Control) sert de pont entre ces 2 réseaux afin que les applications distantes de la salle de commande puissent superviser notre procédé.

Le réseau « industriel » est constitué de solutions hétérogènes (RFID, Wifi IEEE 802.15.4, Profisafe, Wifi 802.11.g et Ethernet filaire) pour faire communiquer les différents composants « intelligents ». Afin d'assurer l'interopérabilité des composants plusieurs passerelles ont été développées et/ou utilisées. La passerelle Stargate Net Bridge de Crossbow assure la remontée des informations du réseau de capteurs sans-fil MICAz vers la supervision. La mise en œuvre de Nouvelles Technologies de l'Information et de la Communication (serveur OPC, VLAN industriel, VLAN CRAN, serveurs web dans les API, …) permet d'ouvrir l'automatisation de la plate-forme au réseau d'entreprise (salle de commande, ERP, etc) et à Internet (e-supervision).

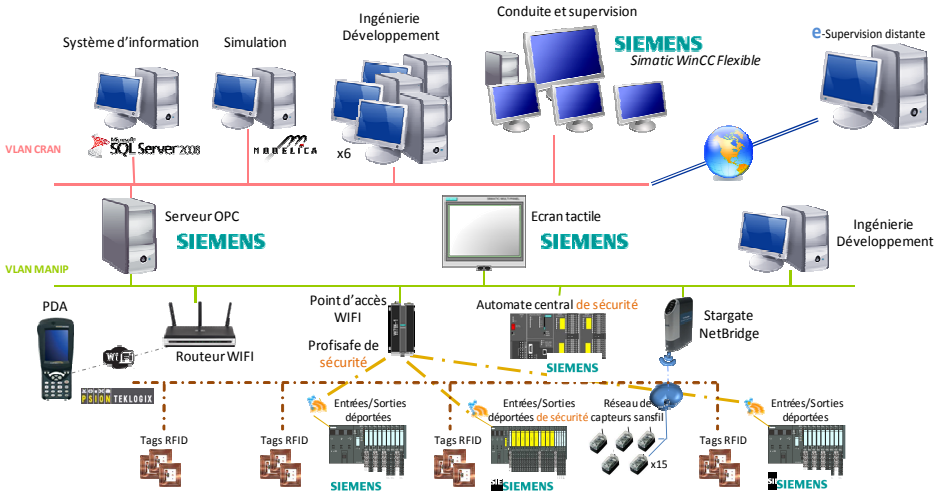

Figure 5 : Architecture de communication

4. Contributions scientifiques

Les différents travaux scientifiques validés sur cette plate-forme portent principalement sur l'amélioration de la sûreté de fonctionnement, et s'articulent autour de la proposition d'un système interactif d'aide à la conduite (Figure 6) [3] [4].

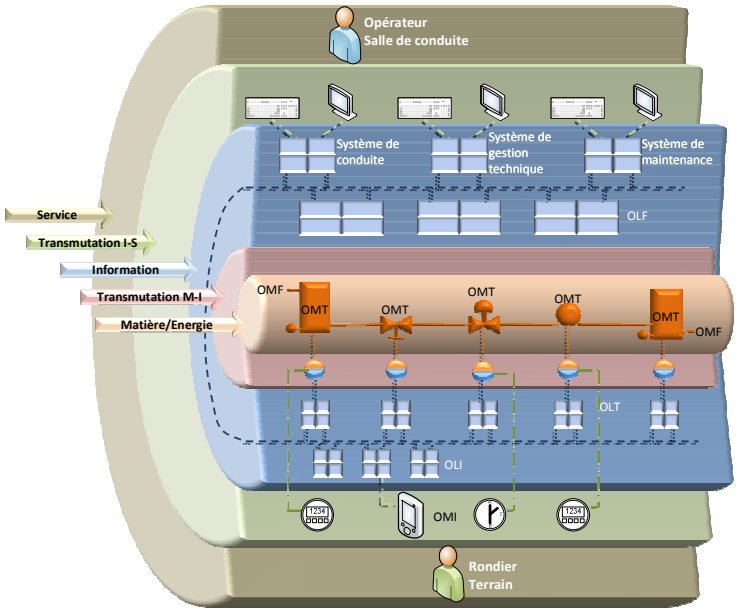

Figure 6 : Principe du Système Interactif d'Aide à la Conduite (SIAC)

Ce SIAC encapsule le canal physique par un canal d'informations qui articule différents types d'objets :

- techniques et physiques (flux matière/énergie), assurant la transmutation entre le canal physique et celui de l'information,
- interactifs, assurant la transmutation entre le canal d'informations et celui des services.

Ce continuum d'informations a pour objectif de permettre au rondier d'interopérer numériquement en tout lieu, à tout instant et pour toute action de conduite via les objets interactifs du SIAC.

Parmi les travaux validés sur la plateforme, nous pouvons notamment citer :

- le développement et la mise au point d'un environnement de simulation/émulation permettant d'évaluer à échelle industrielle les modèles de conduite développés : cet aspect a fait l'objet de développements de modèles élaborés avec MODELICA [5] (langage objet pour la modélisation des processus physiques) et des modèles de description des procédures de conduite dans le langage SysML [6] ;
- la spécification du SIAC permettant d'intégrer l'opérateur de conduite et le rondier dans la boucle de décision [4], avec pour objectif d'améliorer l'interopération numérique entre un système technique et des agents d'exploitation qui appliquent des procédures de conduite. La démarche poursuivie est de modéliser de manière abstraite les exigences relatives à la conduite d'une installation à risque, indépendamment de la répartition entre systèmes techniques et systèmes humains (opérateur), pour ensuite proposer une spécification des composants du SIAC. Pour cela, la définition d'une méthode de spécification / modélisation utilisant les bonnes pratiques de l'Ingénierie Système [7], et s'appuyant sur le langage SysML a été proposée [4] ;
- la modélisation conjointe de la commande et du réseau sans fil Wifi, afin d'évaluer des performances temporelles et de proposer un algorithme de gestion des priorités du protocole défini dans la norme IEEE 802.11e basé sur les états de commande [8] ;
- l'intégration de fonctionnalités de maintenance (bilan de santé) dans un composant [9]. Ces travaux ont également porté sur la définition de mécanismes de génération de code VHDL à partir de spécifications UML [10].

5. Application sur la plateforme

Le SIAC est en cours de mise en place, mais il est d'ors est déjà possible pour le rondier d'utiliser une interface interactive sur un PDA industriel (OLI sur la Figure 6) lui permettant d'une part de recevoir les actions à exécuter relatives au mode opératoire en cours, et d'autre part de communiquer avec les vannes manuelles, ces dernières ayant été instrumentées à l'aide de nœuds de réseaux de capteurs sans fil et de puces RFID (OLT sur la Figure 6). Le système de conduite surveille les actions faites en local par les rondiers et avertit, par le biais d'alarmes, que des actions non-conformes aux modes opératoires ont été exécutées.

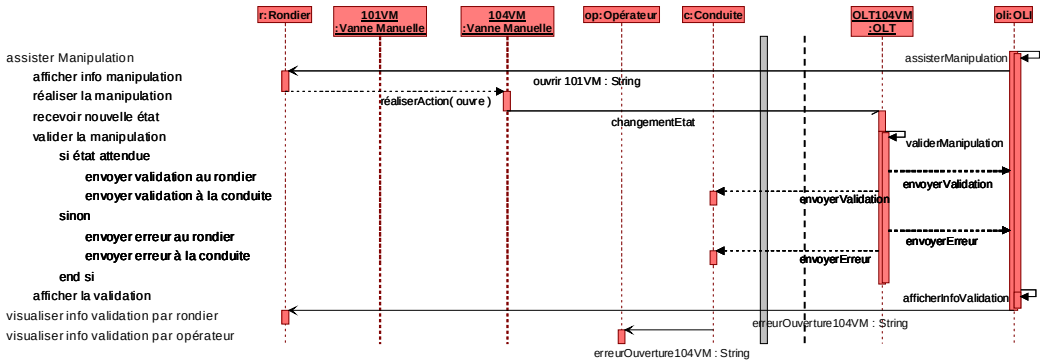

Figure 7 : Exemple de scénario d'exécution d'une action non-conforme par le rondier

A titre d'illustration, la Figure 7 présente un exemple de scénario d'exécution dans lequel le rondier réalise une action non-conforme par rapport aux modes opératoires en cours. Ainsi, lors de l'exécution d'un mode opératoire, le rondier reçoit, par l'intermédiaire de son PDA une requête d'ouverture de la vanne 101VM (Figure 8).

Figure 8 : Vue de la requête d'ouverture de la vanne 101VM sur le PDA du rondier

Le rondier procède, par erreur, à l'ouverture d'une vanne voisine physiquement similaire, la vanne 104VM. Par le biais de l'instrumentation ambiante mise en place sur les vannes manuelles (réseaux de capteurs sans fil avec cartes d'entrées/sorties), le SIAC, et plus précisément l'OLT associé à la vanne, reçoit une notification concernant l'ouverture réalisée par le rondier, procède à sa validation en comparant cette notification avec les informations qu'il a reçues concernant le mode opératoire en cours d'exécution, détecte l'erreur et la signale, d'une part au rondier par le biais de son PDA, et d'autre part à l'opérateur en salle de commande par le biais de l'écran de conduite (Figure 9).

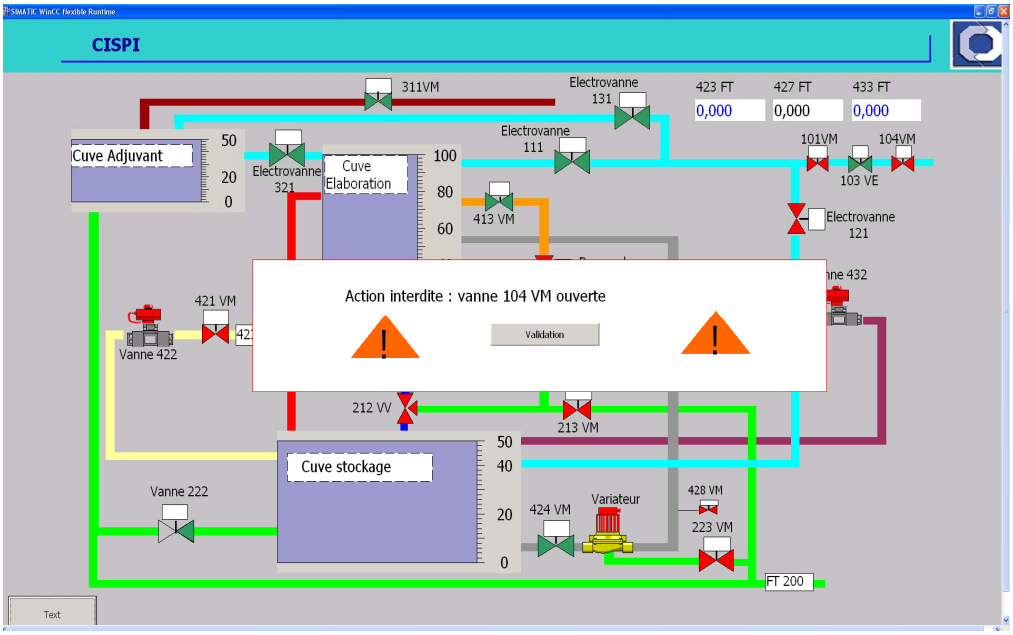

Figure 9 : Vue de l'écran de conduite indiquant qu'une action non conforme a été effectuée

6. Conclusion

La plate-forme CISPI, financée dans le cadre du CPER MISN et d'un projet Nancy-Université / région Lorraine, est aujourd'hui opérationnelle au sein du service plate-forme du CRAN. Elle permet de tester le comportement et la réactivité du système de conduite en fonction des stratégies adoptées (conduite décentralisée ou centralisée) et du mode d'exploitation (conduite normale, incidentelle ou accidentelle), et capitalise le savoir-faire acquis par le CRAN en matière d'IAM. Elle est mise à la disposition des formations de Nancy Université, notamment dans le cadre de l'Unité d'Enseignement intégration système du Master Ingénierie de Systèmes Complexes, et sert de support à des projets d'étudiants de diverses formations (IUT, Licence Sciences Pour l'Ingénieur, ESIAL, …).
Un système multi agent est en cours de développement ; son objectif est de gérer l'exécution des différents modes opératoires en parallèle, en assurant les synchronisations entre opérateurs et rondiers, et les exclusions nécessaires.

7. Bibliographie

[1] Pétin, J.-F., Iung, B., Morel, G. (1998). *Distributed intelligent actuation and measurement (IAM) system within an integrated shop-floor organisation*. Computers in Industry, 37 (3), 197-211.

[2] Galara, D., & Pirus, D. (2007). *Finding the way up to the standardization of Human Machine Interface*. IEEE 8th Human Factors and Power Plants and HPRCT 13th Annual Meeting, (pp. 133-139). Monterey, CA, USA.

[3] Dobre, D., Morel, G., Petin, J.-P., Bajic, E. (2008). *Improving digital interaction for operator-driven process-plant operation*. 9th IFAC Workshop on Intelligent Manufacturing Systems (IMS'08). Szczecin, Pologne.

[4] Dobre, D., Morel, G., Gouyon, D. (2010). *Improving Human-System Digital Interaction for Industrial System Control: Some Systems Engineering Issues*. 10th IFAC Workshop on Intelligent Manufacturing Systems (IMS'10). Lisbonne, Portugal.

[5] The Modelica Association (2010). *Modelica – A unified object-oriented language for physical systems modeling Version 3.2*.

[6] Object Management Group (2008). *Systems Modeling Language Version 1.1*.

[7] Association Française d'Ingénierie Système (AFIS) (2009). *Découvrir et Comprendre l'Ingénierie Système* (éd. 3).

[8] Habib G., Marangé P., Pétin J.-F., Divoux T. (2009). *Évaluation de l'influence d'un réseau de communication sans fil sur la commande d'un SED*, Journal Européen des Systèmes Automatisés, Volume 43/7-9 (2009), pages 855-870, Modélisation des Systèmes Réactifs, O. Roux & D. Lime Editeurs, Actes du congrès MSR 2009, 16-18/11/2009, Nantes.

[9] Moreira T., Wehrmeister M., Pereira C., Pétin J-F., Levrat E., (2010) *Generating VHDL Source Code from UML Models of Embedded Systems*, IFIP Advances in Information and Communication Technology, Volume 329/2010, pp. 125-136.

[10] Object Management Group (2010). *Unified Modeling Language Version 2.3*.