Support de cours :
Sécurité industrielle

- Les Mesures de Maitrise de Risques Instrumentées -

NB : *Support du cours déjà fait avec les étudiants qui étaient présents (es), au début du S2.*

1. **La Sûreté de Fonctionnement (S.D.F)**
2. **Présentation de la méthode générale AMDEC**

- **Une démarche de prise des Mesures de Maitrise des Risques Instrumentées.**

…….. *Suite….*

C'est une méthode d'amélioration, avec un certain niveau de minimiser, lors de la conception d'un processus existant, pour diminuer son taux de défaillances et d'améliorer ses performances par un nombre de pannes moindre.

Les Objectifs sont :

Il faut définir des règles générales pour la prise en compte, dans les études de dangers, des mesures de maîtrise des risques instrumentées (MMRI) dans la prévention et la réduction des accidents majeurs. Elles doivent répondre aux exigences fixées à un article* (article 4 de l'arrêté du 29 septembre 2005).

Une barrière de sécurité (comme MMR), doit être indépendante des événements initiateurs à l'origine d'un scénario d'accident pour ne pas entraîner une défaillance ou une dégradation de la performance;

Lorsque l'instruction d'une étude de dangers a conduit l'inspection des installations classées a accepter des dispositions différentes, celles-ci ne sont pas à remettre en cause, mais pourront faire l'objet d'une nouvelle analyse, dans le cadre de la mise à jour d'une étude de dangers suite à un ré-examen périodique (révision quinquennale) ou particulier (demande anticipée ou modification des installations).

***** Article d'un décret imposé par une loi.

Cas 1 :

Illustration du principe d'événement initiateur à l'origine du scénario d'accident et ne pas entraîner une défaillance (ou dégradation) de la performance de la MMR (Figure 1). .

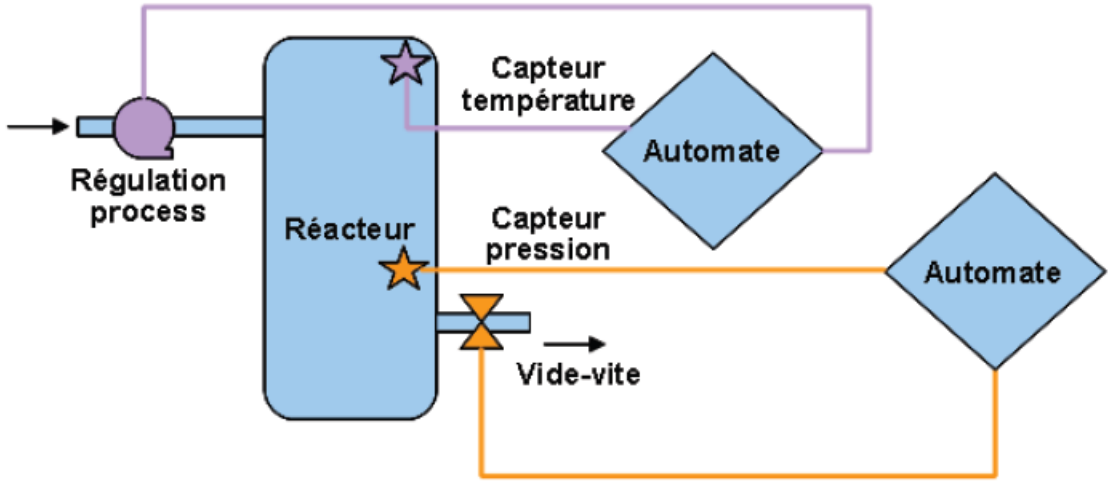

Figure 1. Principe de l'événement initiateur

Description de l'installation de la Figure 1:

L'introduction en réactif est régulée par la chaine de conduite *capteur t° - automate – vanne de régulation*. Le réacteur est équipé d'une MMR *capteur de pression – automate – vide-vite*, pour éviter la perte de confinement du réacteur en cas de montée anormale en pression (supérieur à Pmax).

Scénario 1 :

Un défaut sur la chaîne de conduite *capteur t° - automate – vanne de régulation* entraîne une trop grande introduction de réactif qui provoque un emballement de réaction. Cela entraîne une montée en pression et en température du réacteur. La température atteinte est supérieure à la plage de fonctionnement du capteur de pression, qui rend inopérant la chaîne de sécurité (mesure erronée du capteur de pression qui ne détecte pas le franchissement de Pmax).

La montée en pression du réacteur entraîne sa perte de confinement.

- Pour ce scénario, la MMR *capteur de pression – automate – vide-vite* ne peut pas être valorisée.

Scénario 2 :

Une erreur dans l'introduction du réactif entraine la production de gaz dans le réacteur. Cela entraîne une montée en pression du réacteur, sans augmentation anormale de la température dans le réacteur.
La montée en pression du réacteur est détectée par le capteur de pression et correctement traitée par l'automate déclenchant la vidange du réacteur, évitant ainsi la perte de confinement.

- Pour ce scénario, la MMR *capteur de pression – automate – vide-vite* peut être valorisée.

Cas 2 :

Illustration du principe du scénario d'accident ne doit pas avoir pour origine une défaillance d'un élément de la MMR (Figure 2).

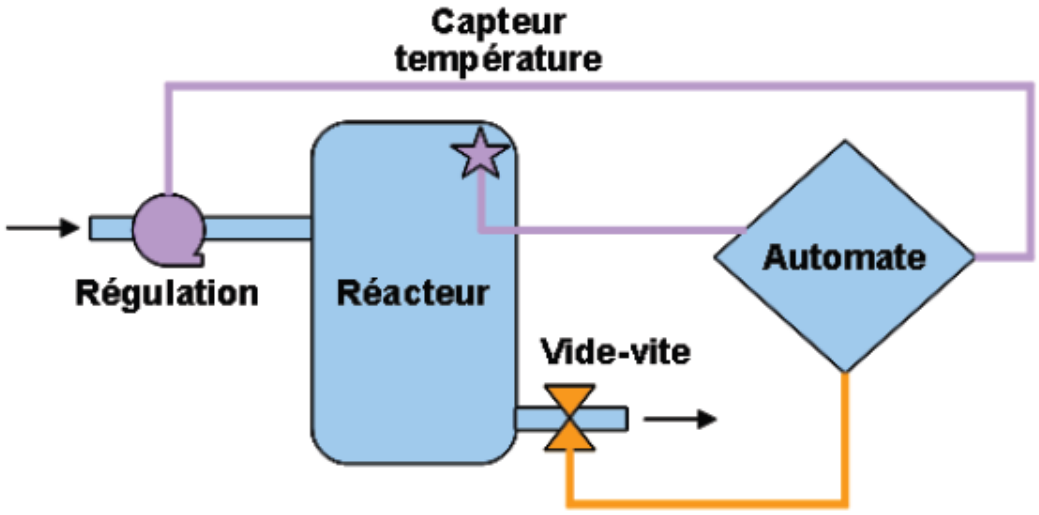

Figure 2. Principe d'accident non lié à une défaillance de la MMR

Descriptif de l'installation de la Figure 2.

L'introduction en réactif est régulée par la chaine de conduite *capteur t° - automate – vanne de régulation*. Le réacteur est équipé d'une MMR *capteur de température – automate – vide-vite*, en vue d'éviter la perte de confinement du réacteur en cas de montée anormale en température (au delà de Tmax).

Scénario 1 :

Un défaut sur le *capteur t°* entraîne une trop grande introduction de réactif qui provoque un emballement de réaction. Cela entraîne une montée en pression et en température du réacteur. La franchissement de Tmax n'est pas remonte au niveau de l'automate qui ne peut pas déclencher le vide-vite avant atteinte de la pression de rupture du réacteur.

- Pour ce scénario, la MMR *capteur de température – automate – vide-vite* ne peut pas être valorisée.

Scénario 2 :

Une erreur dans l'introduction du réactif entraine un emballement thermique. La franchissement de Tmax est bien détecté par le capteur de température et correctement traitée par l'automate qui déclenche le vide-vite avant atteinte de la pression de rupture du réacteur.

- Pour ce scénario, la MMR *capteur de température – automate – vide-vite* peut être valorisée.

Par ailleurs, si une modification significative d'une ou plusieurs MMRI est réalisée ou si un retour d'expérience défavorable (ex. la défaillance récurrente et/ou majeure d'un élément similaire) a été constaté. Lorsqu'une instruction d'une étude de dangers est menée, seules des conditions particulières peuvent justifier d'accepter, des dispositions différentes prévues, après un examen attentif (tierce-expertise).

2.2. Définition d'une MMRI

Une MMRI est constituée par une chaîne de traitement comprenant une prise d'information (capteur, détecteur…), un système de traitement (automate, calculateur, relais…) et une action (actionneur avec ou sans intervention d'un operateur). Elle ne peut être considérée comme telle, que si l'intervention humaine est limitée à une action déclenchée suite à une alarme, elle-même déclenchée sans intervention humaine.

En termes de conception, la notion de MMRI est contraire de la notion technique utilisée pour l'exclusion de certains accidents ou phénomènes dangereux. En particulier, ceux, avec action humaine ne sont pas des « MMR techniques » si elle ne comporte pas d'intervention humaine. Illustration, de manière générale, de cas où une chaîne instrumentée peut être reconnue comme MMRI (figure 3).

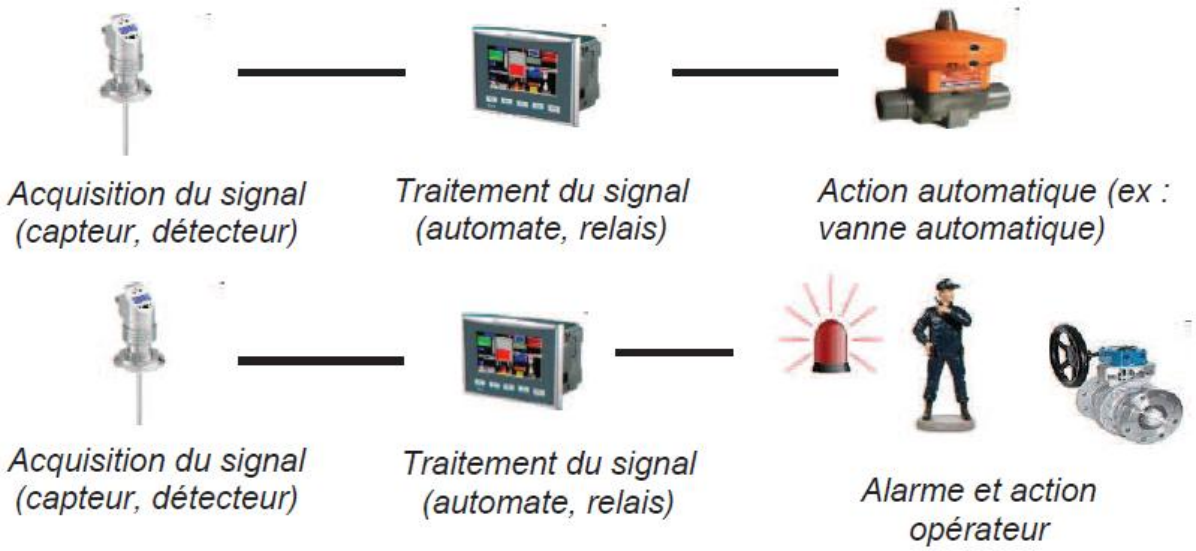

Figure 3. Chaîne instrumentée de MMRI

Nous avons les Illustrations de chaînes instrumentées avec intervention humaine à considérer ou non comme MMRI, données par les exemples ci-dessous :

- « conduite centralisée » ⇨ comprendre « système de conduite de l'installation » ;
  - ⇔ = contrôle du process ;
  - → = fonction MMRI.

Exemple 1 :

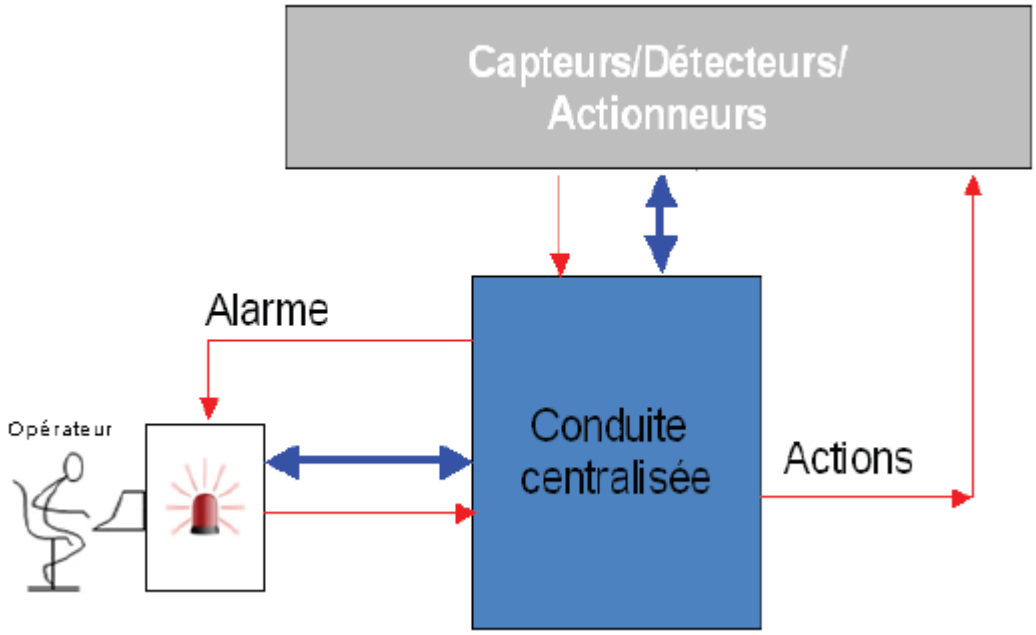

Figure 4. Alarmes et actions qui passent par le système de conduite centralisé.

Le **cas 4,** à la prise d'information technique (capteur / détecteur), le traitement de l'alarme (analyse et choix de l'action) est réalisé par opérateur et l'action est technique, par actionneur commandée par la conduite centralisée.

Exemple 2 :

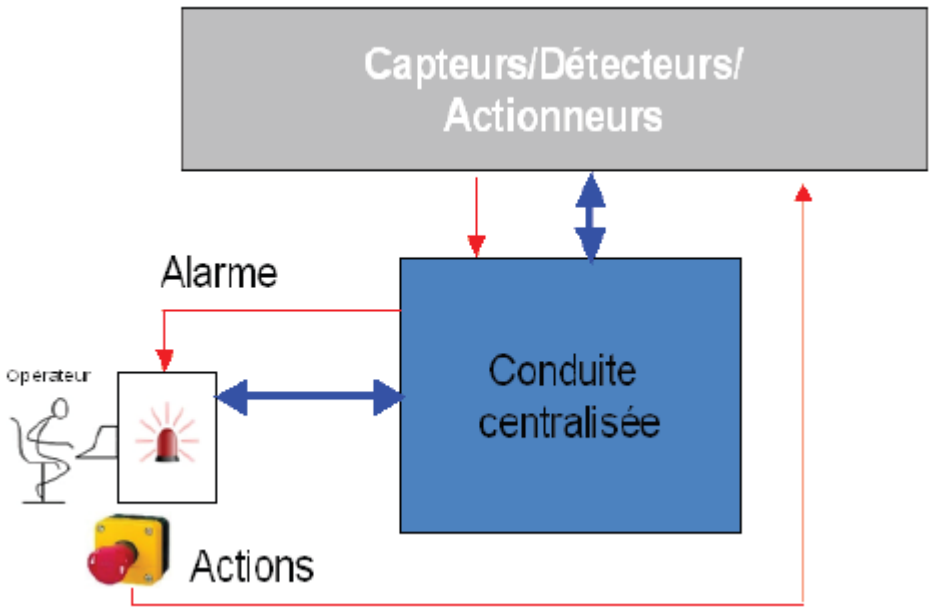

Figure 5. Alarmes qui passent par le système de conduite centralisé avec actions indépendantes.

Exemple 3 :

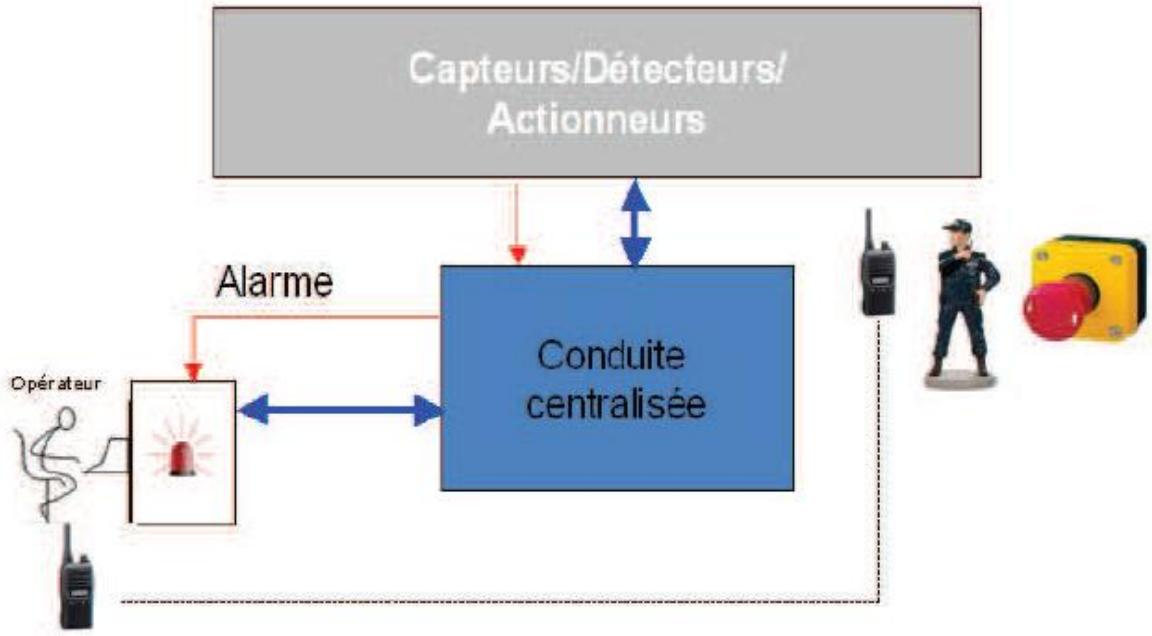

Figure 6. Actions indépendantes du système de conduite centralisé.

Le **cas 3,** à la prise d'information technique (capteur / détecteur), le traitement de l'alarme (analyse et choix de l'action) est réalisé par opérateur et l'action est technique, par un opérateur de terrain qui actionne la sécurité.

Exemple 4 :

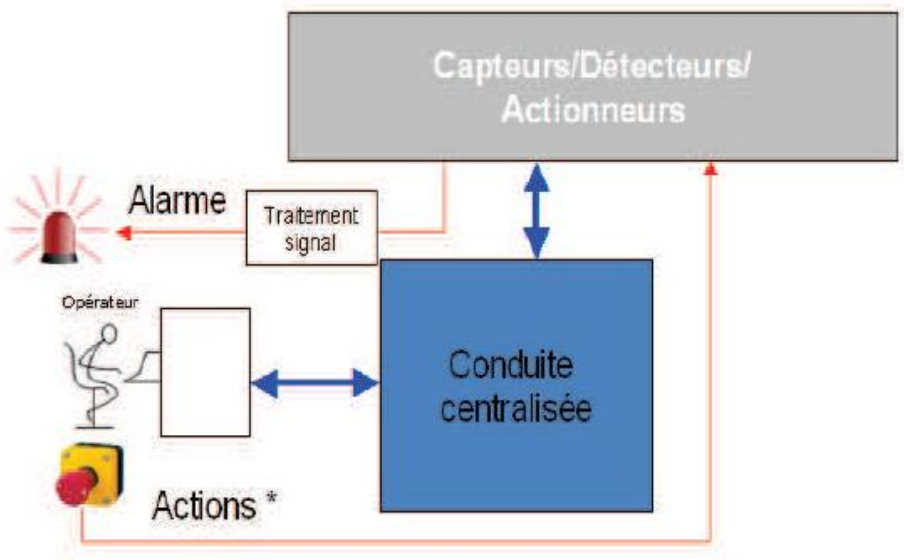

Figure 7. Alarmes et actions indépendantes du système de conduite centralisé.

Les **cas 2 et 4,** ont la prise d'information technique (capteur / détecteur), le traitement de l'alarme (analyse et choix de l'action) est réalisé par opérateur et l'action est technique, par actionneur commandée par un bouton poussoir.

Exemple 5 :

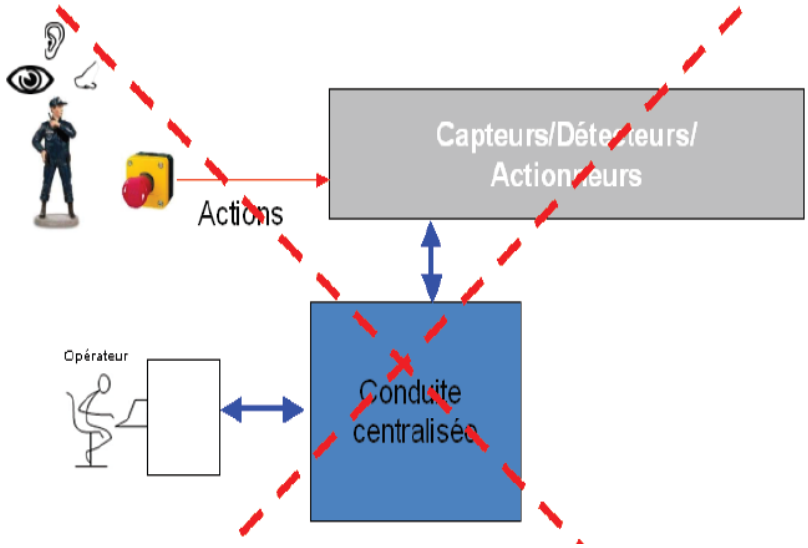

Figure 8. Alarmes et actions indépendantes du système de conduite centralisé.

Le **cas 5,** à la prise d'information humaine (bruit / odeur, vue), le traitement de l'information (analyse et choix de l'action) est réalisé par opérateur et l'action est humaine, par fermeture d'une vanne ou technique par bouton d'arrêt d'urgence.

Exemple 6 :

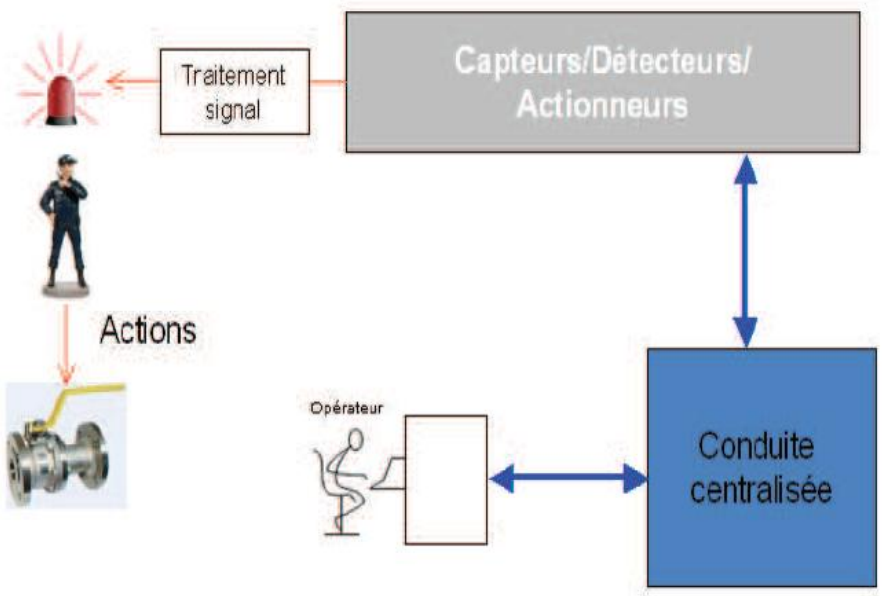

Figure 9. Alarmes, traitement et actions indépendantes du système de conduite centralisé.

Le **cas 6,** à la prise d'information est technique (capteur/détecteur), le traitement de l'alarme (identification de la vanne à manipuler est par opérateur et l'action est humaine par manipulation de la vanne, identifier dans une procédure.

Exemple 7 :

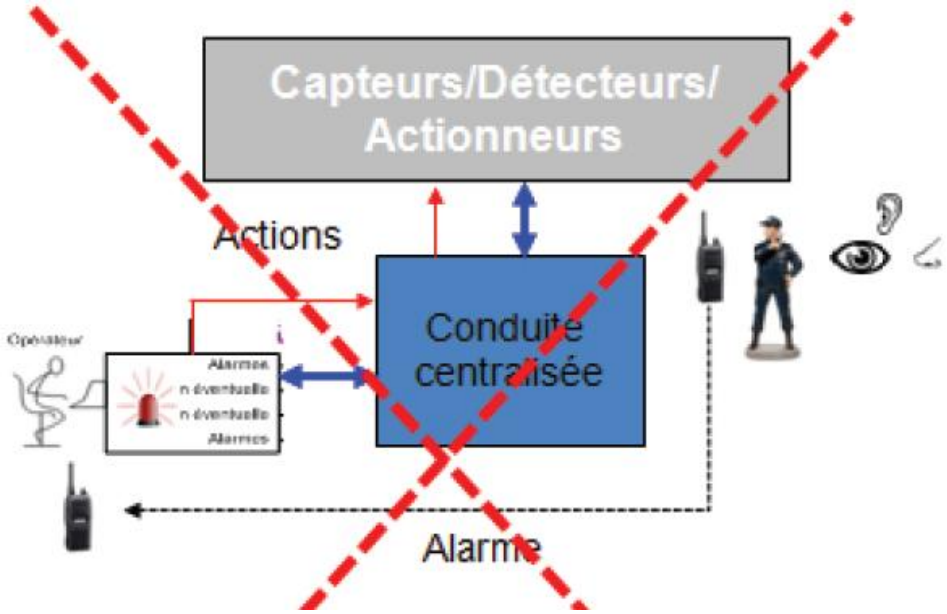

Figure 10. Alarmes indépendantes du système de conduite centralisé.

La configuration dans les **cas 5 et 7,** n'est pas considérée comme une MMR car :

- La prise d'information est humaine
- Le traitement de l'information est humain.

2.3- MMRI de Sécurité (MMRIS) et de Conduite (MMRIC) :

Les MMRI sont classées en deux catégories appelées MMRI de sécurité (MMRIS) et MMRI de conduite (MMRIC) (figure 11).

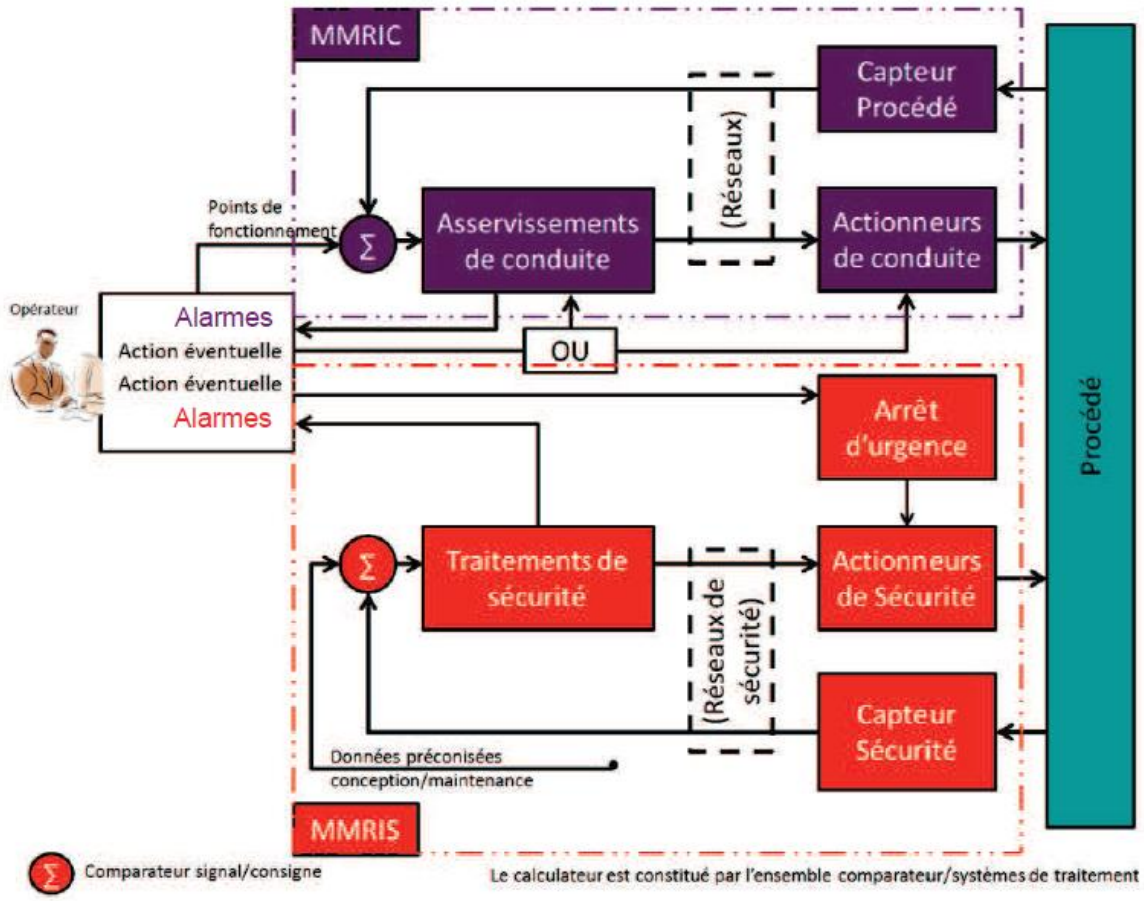

Figure 11. *Illustration de la distinction fonctionnelle et matérielle, entre une MMRIC et une MMRIS*

2.3.1. La MMRI de Sécurité (MMRIS)

Une MMRIS repose sur un système instrumenté de sécurité, combinant capteur(s), unité de traitement et actionneur(s) ayant pour objectif de remplir des fonctions de sécurité. Elle se matérialise par, une sécurité de haute pression avec ouverture automatique d'une vanne, une alarme de sécurité avec intervention humaine. Une chaîne instrumentée est considérée comme MMRIS, lorsque ses éléments sont dédies uniquement à la sécurité. Toutefois, les éléments d'une chaine de sécurité peuvent aussi être utilisés pour la conduite des installations, sous réserve, qu'ils ne soient pas susceptibles de conduire à un événement initiateur à l'origine du scenario d'accident, que l'action de sécurité qu'ils assurent soit prioritaire sur toutes leurs autres actions et qu'ils ne soient pas déjà pris en compte dans une MMRIC pour le même scénario.

Dans le cas où un exploitant propose une MMRI basée sur un automate dédié également à des fonctions de conduite, l'exploitant doit à minima justifier du respect des dispositions suivantes :

- L'automate est un APS (Automate Programmable de Sécurité) et ne gère que des opérations de conduite simples comme des actions binaires (ex : commandes de fermeture et d'ouverture de vannes par un operateur lors d'une opération de dépotage, commande de marche/ arrêt…) ;

- La défaillance (matériel ou logiciel) des fonctions de conduite n'a pas d'impact sur les fonctions de sécurité ;

- Toute modification des consignes relatives à une fonction de conduite est gérée avec la même exigence qu'une modification des consignes relatives aux fonctions de sécurité.

De plus, pour les nouvelles MMRIS, la chaîne de sécurité est conforme aux **normes NF EN 61508** et **NF EN 61511**.

Cas 1 :

La chaîne de sécurité *capteur de pression– automate – vide-vite* peut être considérée comme une MMRIS pour le scénario 2 (montée en pression suite à une erreur de réactif) car les éléments de la chaîne sont dédiés uniquement à la sécurité (Figure 12).

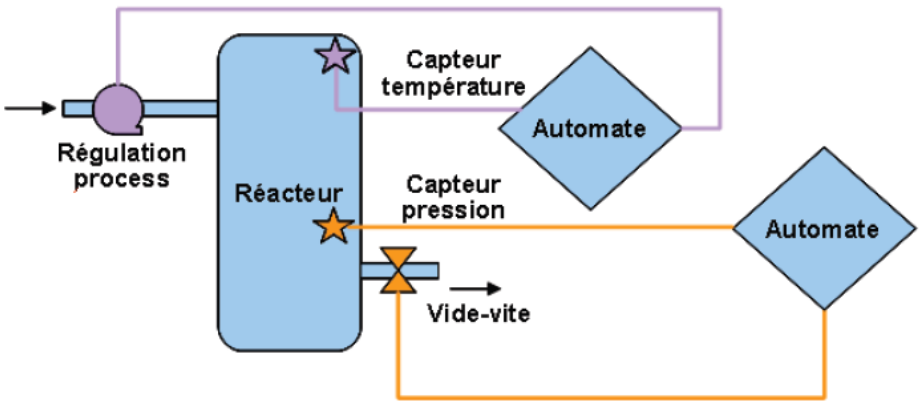

Figure 12. Les MMRIS constituées d'éléments dédiés à la sécurité.

Cas2:

La chaîne de sécurité *capteur de pression – automate – vanne* commande la fermeture de la vanne d'entrée en cas de montée en pression dans le réacteur au delà de Pmax **(**Figure 13).

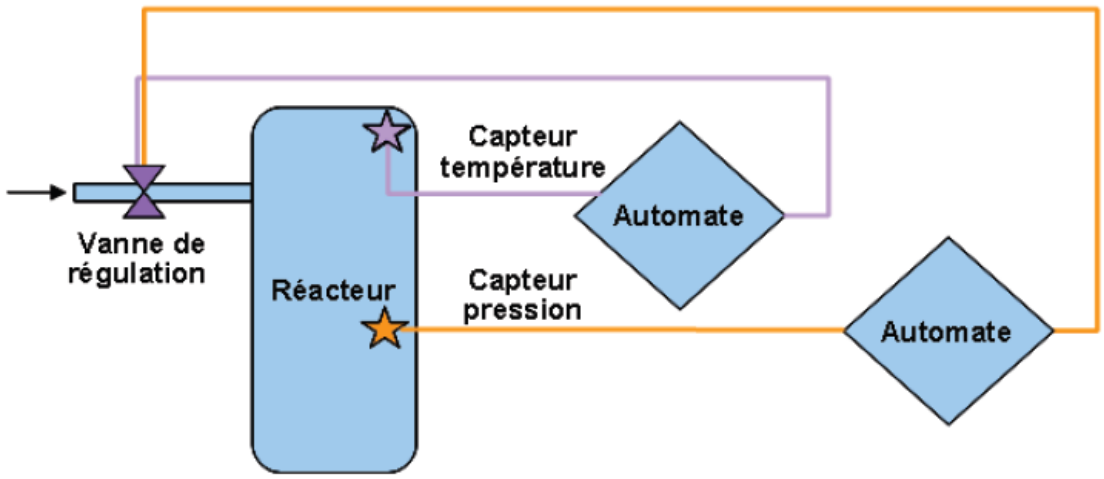

Figure 13. MMRIS, avec actionneur, utilisé pour la conduite du procédé.

Cette chaîne peut être considérée comme une MMRIS pour le scénario 2 (montée en pression suite à une erreur de réactif), sous réserve que l'action de fermeture en cas de montée en pression soit prioritaire sur la fonction de conduite. La chaîne capteur de *capteur t°* - *automate – vanne* ne peut pas être considérée pour ce scénario comme:

- une MMRIC car l'actionneur est déjà pris en compte pour la MMRIS
- une MMRIS car l'automate ne gère pas uniquement des opérations simples car la vanne a également des fonctions de régulation pilotée par cet automate.

Cas 3 :

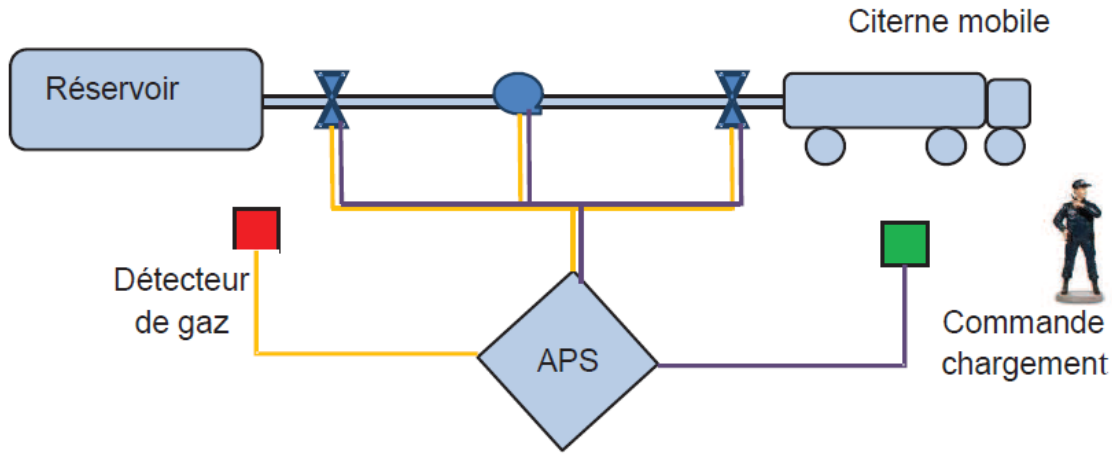

Figure 14. MMRIS avec automate non dédié exclusivement à la sécurité.

Exemple d'une installation de transfert de produit :

Les vannes, ainsi que la pompe fonctionnent uniquement en **TOR** (Tout Ou Rien). Les vannes sont a sécurité positive (fermeture par manque d'énergie : air, électricité, eau). La commande de chargement permet à un operateur d'ouvrir/fermer les 2 vannes et de démarrer/arrêter la pompe au début de l'opération de chargement. Si du gaz est détecté par le détecteur, automatiquement les 2 vannes sont fermées (si elles étaient ouvertes) et/ou la pompe est arrêtée (si elle était démarrée). Si les vannes étaient déjà en position fermée et si la pompe était déjà arrêtée, tout signal d'ouverture/démarrage venant de la commande manuelle de chargement est inhibé. La chaîne détection gaz – automate de sécurité – fermeture des vannes/arrêt pompe peut être considérée comme une MMRIS car les opérations d'exploitation gérées par l'APS sont des actions binaires. Cela est possible sous réserve des autres conditions précisées au **§ 2.3.1** (par exemple : priorité aux actions de sécurité).

2.3.2. MMRI de Conduite (MMRIC)

Une MMRIC intégrée au système de conduite de l'installation et se matérialise par:

- Une alarme sur le système de conduite avec intervention de l'operateur sur un organe terminal tel qu'une vanne manuelle, un arrêt d'urgence (AU) ;

- Une chaîne de détection ou de sécurité implantée dans le système de conduite. Il faut que les conditions minimales suivantes soient vérifiées :

- Les éléments de la chaîne ne sont pas susceptibles de conduire à un événement initiateur a l'origine du scenario d'accident ;

- L'action de sécurité assurée par les éléments de la chaîne est prioritaire sur toutes leurs autres actions ;

- Les modifications des paramètres (ex : les seuils d'alarme) sont gérées au travers de procédures ou du système de gestion de la sécurité de l'établissemen;

- L'exploitant a mis en place une maintenance préventive au titre de la fonction de sécurité remplie;

- Le système de conduite est conçu, exploité et maintenu dans des conditions standards et selon de bonnes pratiques (standards ou référentiels, architecture éprouvée, concept éprouve, procédures d'exploitation et de maintenance, détection des principales défaillances telles que défaut capteur ou perte d'alimentation actionneur…). Le niveau de confiance d'une MMRIC est au maximum égal a '**1'** (valeur retenue dans la norme **NF EN 61511** « Sécurité fonctionnelle : Systèmes instrumentés de sécurité pour les industries de transformation »).

Reprise cas 1, avec un même automate :

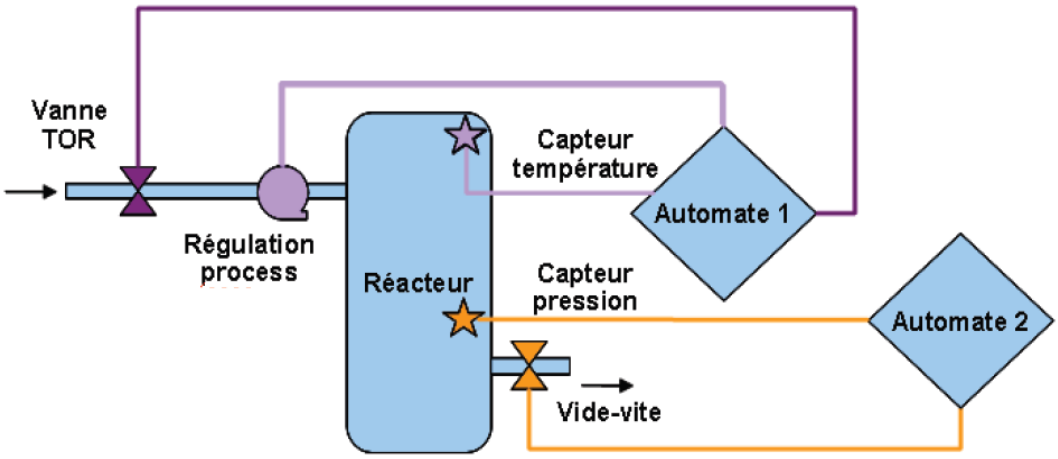

Figure 15. Principe de l'événement initiateur avec vanne TOR à l'amant.

Descriptif de l'installation Figure 15 :

L'introduction en réactif est régulée par la chaine de conduite *capteur t° - automate 1 – vanne de régulation*. En cas de montée en température au delà de Tmax, l'automate **1** commande la fermeture de la vanne TOR. Le réacteur est également équipé d'une MMR *capteur de pression – automate 2 – vide-vite*, en vue d'éviter la perte de confinement du réacteur en cas de montée anormale en pression (supérieur à Pmax).

Scénario

Une erreur dans l'introduction du réactif entraine un emballement thermique, avec montée en pression et en température et risque de perte de confinement.

Pour ce scénario :

- La chaîne *capteur t° - automate 1– vanne TOR* peut être valorisée comme MMRIC (elle ne peut pas être valorisée comme MMRIS car l'automate '**1'** gère également la régulation du process), sous réserve que l'action de fermeture de la vanne TOR soit prioritaire (passe en premier).
- La chaîne *capteur de pression – automate '2' – vide-vite* peut être valorisée comme MMRIS.

2.4. Prise en compte de l'action humaine :

La prise en compte de l'action humaine passe par la vérification de certains critères d'évaluations du niveau de confiance. Le niveau de confiance d'une MMR avec action humaine est dans le cas général au maximum égal à '**1'** et peut, pour les MMRIS, sous certaines conditions particulières, être supérieure sans toutefois dépasser '**2'**.

S'agissant d'actions humaines intégrées à des MMRI, il faut s'assurer que:

- Les alarmes associées aux MMRI sont facilement identifiables par l'operateur sur le poste de conduite ;
- Les actions associées à ces alarmes sont clairement définies (notamment dans des procédures) ;
- La disponibilité de l'operateur (présence permanente et temps d'action « compatible » avec le temps de réponse de la MMRI, nombre limité de procédures d'urgence attribuées à un même opérateur) ;
- La formation des opérateurs, notamment dans le cadre des actions susceptibles de conduire à des conséquences potentielles sur la sécurité de l'installation.

3 - Notions d'indépendance des MMRI entre elles :

3.1 Indépendance des MMRIC

Sur un même scenario d'accident, deux MMRIC maximum peuvent être reconnues, sous réserve qu'elles soient composées d'éléments distincts (y compris les interfaces opérateurs homme/machine, les éléments de transmission du signal de type câblage, a l'exception des dispositifs a sécurité positive ou '**fail safe**' entraînant la mise en repli de l'installation (position de sécurité) en cas de perte de l'alimentation ou du signal porte par le câble et qu'elles fassent appel a des operateurs différents (cas d'une action humaine). En particulier, les automates associés à chacune des MMRIC doivent être distincts (cas des automates de postes de conduite d'unités ou d'installations différentes).
Dans le cas d'un scénario avec MMRIS et MMRIC, les MMRIC doivent également être composés d'éléments distincts de ceux des MMRIS (Figure 16).

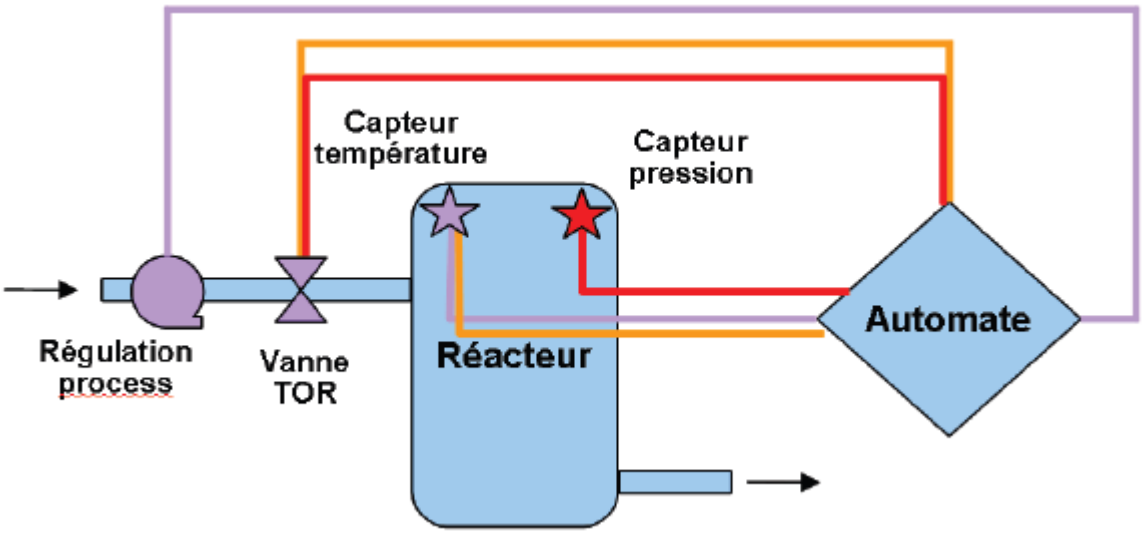

Figure 16. Chaînes avec un automate commun

Descriptif de l'installation Figure 16 :

L'introduction en réactif est régulée par la chaine de conduite '*capteur température - automate –vanne de régulation*.
En cas de montée en température au delà de Tmax ou de montée en pression au delà de Pmax, l'automate commande la fermeture de la vanne TOR.

Scénario :
Une erreur du réactif entraine un emballement thermique, avec montée en pression et en température et risque de perte de confinement.
Soit, les chaînes *capteur température – automate – vanne TOR et capteur pression – automate – vanne TOR* ne peuvent pas :

- Etre considérées comme MMRIS car l'automate est associe a une fonction de conduite non binaire (régulation),

- Etre considérées comme deux MMRIC indépendantes pour chacune des raisons suivantes :

L'actionneur (vanne TOR) et le traitement (automate) sont communs pour ces deux chaînes. En application des dispositions du **§ 2.3.2** qui précise que sur un même scenario d'accident deux MMRIC maximum peuvent être reconnues sous réserve qu'elles soient indépendantes, une seule des deux chaînes peut être ici valorisée pour le scénario étudié.

3.2. Indépendance des MMRIS

Plusieurs MMRIS valorisées pour un même scénario d'accident doivent répondre aux mêmes critères d'indépendance que pour les MMRIC, sauf pour le système de traitement qui peut être commun dans le cas d'un APS, sous réserve de s'assurer que:
- La défaillance d'un élément de la boucle de traitement d'une MMRIS (carte d'acquisition, module de traitement, carte de sortie, transmission, alimentation…) ne remet pas en cause le fonctionnement des autres MMRIS (APS disposant d'une carte d'acquisition et d'une carte de sortie spécifiques à chaque MMRIS et module de traitement redondant) ;
- Les défaillances d'un élément de la boucle de traitement d'une MMRIS (carte d'acquisition, module de traitement, carte de sortie, transmission, alimentation…) sont détectées ou conduisent automatiquement à une mise en repli (position de sécurité) et que les réparations peuvent être réalisées dans un délai défini sans remettre en cause la fonction de sécurité assurée par les autres MMRIS (soit parce que les réparations peuvent être réalisées sans remettre en cause le fonctionnement des autres MMRIS soit parce que le potentiel de danger est supprimé) ;

- La programmation de chaque fonction assurée par les MMRIS est rendue distincte (programme sépare, page de configuration séparée…) ;

- Sur défaut général de l'automate (pertes d'alimentations électriques, ruptures de câbles…), la mise en repli (position de sécurité) est assurée (sécurité positive / **fail safe**) ;

- La somme des NC retenus pour ces MMRIS est inférieure ou égale au NC de l'automate ;

- Il existe un facteur minimum de **10** entre le produit des probabilités de défaillance des MMRIS et la probabilité de défaillance dangereuse de l'APS commun ;

- Les choix techniques ont été faits par du personnel compétent, interne ou externe à l'entreprise ;

- Le niveau de confiance global est évalue au regard de la probabilité d'occurrence d'éventuels modes communs de défaillance (sur le matériel et le logiciel) ;

- L'évaluation et la verification de la performance de ces solutions techniques ont été faites par des personnes ou entité différentes de celles qui ont développé ces solutions ;

- Pour les nouvelles MMRIS, de la justification de l'inconvénient ou de l'impossibilité de disposer directement de chaînes totalement indépendantes, pour un même scénario d'accident ;

- La justification de la maîtrise des modes communs de défaillance.

Une tierce-expertise peut compléter les éléments d'analyse de ce type de structure complexe avec un APS gérant plusieurs MMRIS pour un même scenario d'accident (Figure 17).

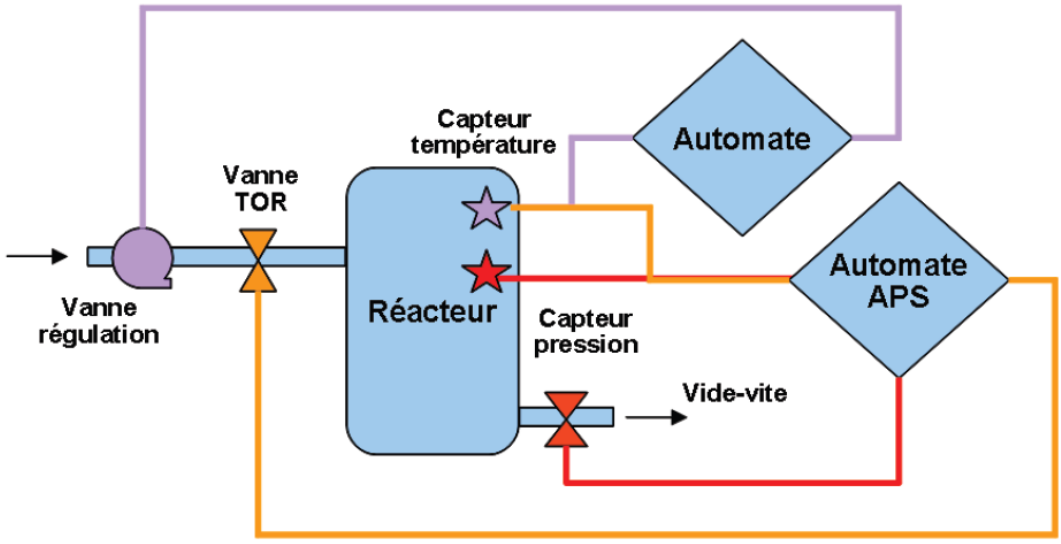

Figure 17. Principe de Chaînes avec Indépendance des MMRIS

Descriptif de l'installation Figure 17 :

L'introduction en réactif est régulée par la chaine de conduite *capteur température - automate – vanne de régulation*. En cas de montée en température au delà de Tmax, l'automate de sécurité commande la fermeture de la vanne TOR. En cas de montée en pression au delà de Pmax, l'automate de sécurité commande l'ouverture de la vanne vide-vite.

Scénario :

Une erreur dans l'introduction du réactif entraine un emballement thermique, avec montée en pression et en température et risque de perte de confinement.
Pour ce scénario, les chaînes *capteur température – automate de sécurité – vanne TOR et capteur pression – automate de sécurité – vide-vite* peuvent être considérées comme deux MMRIS indépendantes car seul le système de traitement est commun (automate APS). Cela est acceptable sous réserve du respect des critères du **§ 3.2**. La chaîne *capteur température – automate – vanne de régulation ne peut pas être valorisée comme MMRIC (ni comme MMRIS) car le capteur de température est commun avec la chaîne capteur température – automate de sécurité – vanne TOR* déjà valorisée en MMRIS (**§ 3.1** qui précise que dans le cas d'un scénario avec MMRIS et MMRIC, les MMRIC doivent être composés d'éléments distincts de ceux des MMRIS).

4 - Perspectives d'amélioration du niveau de sécurité à moyen ou long terme :

A ce jour, il est admis que la diversification des fonctions de sécurité via l'utilisation a la fois des MMRIS et des MMRIC pour le même scenario d'accident, est une bonne pratique pour limiter le nombre et le niveau des modes communs de défaillance.
Pour les installations nouvelles, la première couche instrumentée de sécurité peut reposer sur des MMRIC. Si une couche supplémentaire est nécessaire, la mise en place de MMRIS doit être envisagée des la phase de conception de l'installation.

Nota : Merci de préparer vos leçons.
La suite vous sera transmise ultérieurement.

Bonne santé à tous