Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCOLOGIE, DU DÉVELOPPEMENT DURABLE
ET DE L'ÉNERGIE

Direction Générale de la Prévention des Risques

Service des Risques Technologiques

Sous-direction des risques accidentels

Bureau des risques technologiques et des industries chimiques et pétrolières

02 OCT. 2013

Paris, le

La directrice générale de la prévention des risques

à

Mmes et MM les Directeurs régionaux de l'environnement, de l'aménagement et du logement

Monsieur le directeur régional et interdépartemental de l'environnement et de l'énergie d'Ile de France

MM les Directeurs de l'environnement, de l'aménagement et du logement

Nos réf. : BRTICP/2013-295/PB/XS

Affaire suivie par : Pierre BOURDETTE / Xavier STREBELLE
Tél : 01 40 81 89 76 / 01 40 81 89 78 - Fax : 01 40 81 90 39
pierre.bourdette@ developpement-durable.gouv.fr
xavier.strebelle@developpement-durable.gouv.fr

Objet : Note de doctrine sur les mesures de maîtrise des risques instrumentées (MMRI).
Annexe : Guide relatif aux mesures de maîtrise des risques instrumentées (MMRI).

La loi du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages et ses textes d'application ont introduit une nouvelle méthodologie d'évaluation des risques dans les études de dangers, qui a notamment permis de mettre en évidence la notion de mesure de maîtrise des risques (MMR).

Depuis, dans le cadre des travaux ayant conduit à l'élaboration et la reconnaissance en juillet 2011 du guide DT93 pour la maîtrise du vieillissement sur les MMR instrumentées (MMRI), il est apparu nécessaire de créer, sur demande de la profession, un groupe de travail spécifique pour conduire une réflexion générale sur la doctrine future à adopter pour les MMRI, en prenant mieux en compte leurs spécificités (ex : critères à respecter pour considérer une chaîne instrumentée comme MMRI indépendante, niveau de confiance maximum à considérer pour certains types de MMRI, examen de la possibilité pour une MMRI d'intégrer certains éléments d'une chaîne de conduite de procédé, etc.).

Les éléments de doctrine émanant de ce groupe de travail font l'objet d'un consensus avec les représentants de la profession. Ces éléments sont donnés dans le guide en annexe de la présente note, qui sera mis en ligne sur le site internet http://www.ineris.fr/aida/.

Copie : destinataires in fine.

Ce guide concerne uniquement les MMRI présentes dans les installations soumises à autorisation et est à mettre en œuvre dans les conditions précisées dans son préambule.

Ce guide ne remet pas en cause les dispositions éventuellement différentes déjà acceptées lors de l'instruction des études de dangers par l'inspection des installations classées, notamment pour les établissements Seveso seuil haut faisant l'objet d'un PPRT.

Pour toute nouvelle instruction d'une étude de dangers mettant en œuvre des MMRI, je vous invite à veiller à la bonne application de ce guide.

La directrice générale
de la prévention des risques,

Signé

Patricia BLANC

Destinataires en copie :

- Monsieur le directeur technique de l'Union française des industries pétrolières
- Monsieur le directeur du département technique de l'Union des industries chimiques
- Monsieur le délégué général du Groupe d'étude de sécurité des industries pétrolières et chimiques

Guide relatif aux Mesures de Maîtrise des Risques instrumentées (MMRI)

1 - Préambule

L'objet de ce guide est de définir des règles générales pour la prise en compte, dans les études de dangers, des mesures de maîtrise des risques instrumentées (MMRI) telles que définies au paragraphe 2 ci-dessous.

Lorsque l'instruction d'une étude de dangers a conduit l'inspection des installations classées à accepter des dispositions différentes de celles du présent guide avant sa publication, celles-ci ne sont pas à remettre en cause mais pourront faire l'objet d'une nouvelle analyse dans les cas suivants :

- 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) ;
- si une modification significative d'une ou plusieurs MMRI est réalisée ;
- si un retour d'expérience défavorable (par exemple, la défaillance récurrente et/ou majeure d'un élément d'une MMRI similaire) a été constaté.

Lorsqu'une instruction d'une étude de dangers est menée après la publication du présent guide, seules des conditions particulières peuvent justifier d'accepter, exceptionnellement, des dispositions différentes de celles prévues ci-dessous, après un examen très attentif de celles-ci, et moyennant une tierce-expertise.

2 - Définition et typologie des MMRI

2.1 Rappel sur les MMR

Les MMR sont définies dans le cadre des études de dangers dans un objectif de prévention et de réduction des accidents majeurs. Elles doivent répondre aux exigences fixées à l'article 4 de l'arrêté du 29 septembre 2005. En particulier, une barrière de sécurité doit, pour être retenue comme MMR pour un scénario d'accident, être indépendante des événements initiateurs conduisant à sa sollicitation, c'est-à-dire :

- un événement initiateur à l'origine du scénario d'accident ne doit pas lui-même entraîner une défaillance ou une dégradation de la performance de la MMR ;
- le scénario d'accident ne doit pas avoir pour origine une défaillance d'un élément de la MMR.

Des croquis en annexe 1 illustrent ces principes pour le cas de chaînes instrumentées.

2.2 Définition d'une MMRI

Une MMRI est une MMR 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 opérateur).

La MMR ne peut être considérée comme MMRI que si l'intervention humaine, lorsqu'elle existe, est limitée à une action déclenchée suite à une alarme elle-même déclenchée sans intervention humaine (le §2.4 définit des conditions de prise en compte de l'action humaine).

Cette définition de MMRI est retenue pour l'application de l'arrêté du 4 octobre 2010, section 1, art.7. Elle vient préciser le guide DT 93 pour la gestion et la maîtrise du vieillissement des MMRI.

En termes de doctrine, la notion de MMRI est distincte de la notion de MMR technique utilisée dans l'application des filtres (PPRT et MMR) pour l'exclusion de certains accidents ou phénomènes dangereux.
En particulier, les MMRI avec action humaine ne sont pas des « MMR techniques » au sens de la circulaire du 10 mai 2010. A l'inverse, une MMRI peut être considérée comme une MMR technique si elle ne comporte pas d'intervention humaine et être utilisée dans l'application des filtres PPRT et MMR.

Les deux croquis suivants illustrent, de manière générale, les cas où une chaîne instrumentée peut être reconnue comme MMRI :

Acquisition du signal (capteur, détecteur) — *Traitement du signal (automate, relais)* — *Action automatique (ex : vanne automatique)*

Acquisition du signal (capteur, détecteur) — *Traitement du signal (automate, relais)* — *Alarme et action opérateur*

A titre d'exemples, plusieurs cas de chaînes instrumentées avec intervention humaine pouvant être reconnues ou non comme MMRI sont placés en annexe 2 au présent guide.

2.3 Distinction MMRI de Sécurité (MMRIS) et MMRI de Conduite (MMRIC)

Les MMRI sont classées en deux catégories appelées MMRI de conduite (MMRIC) et MMRI de sécurité (MMRIS) et définies ci-après. Les MMRIC et MMRIS peuvent être distinguées comme sur le croquis suivant :

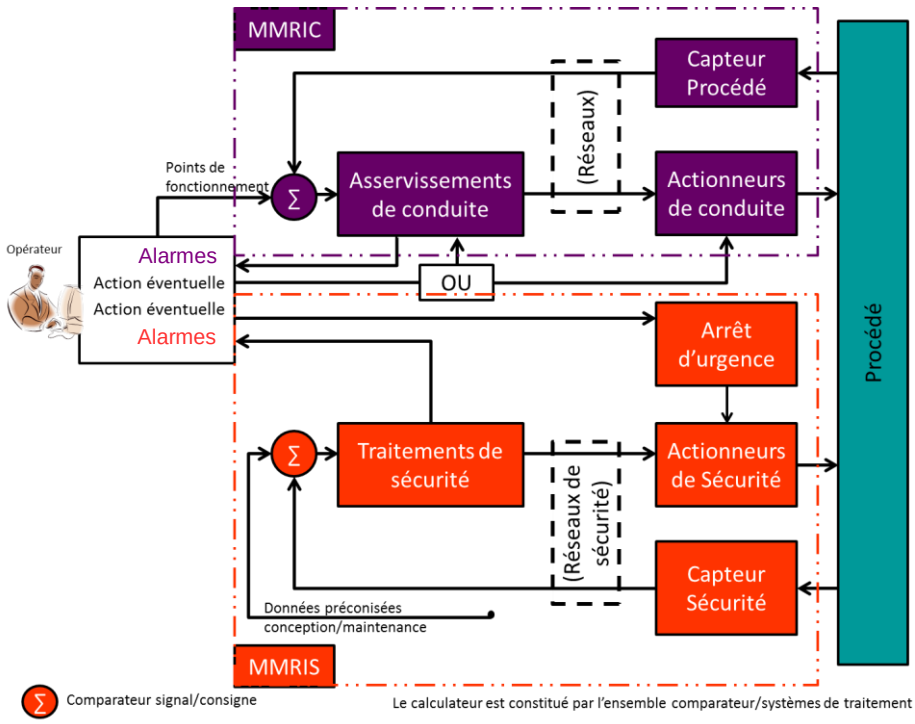


Illustration de la distinction fonctionnelle et matérielle entre une MMRIC et une MMRIS

Les deux paragraphes suivants (§ 2.3.1 et 2.3.2) permettent de distinguer plus précisément les MMRIS des MMRIC et de définir les conditions minimales à respecter pour les reconnaître en tant que telles. L'annexe 3 donne des exemples de MMRIS et MMRIC.

2.3.1 MMRI de Sécurité (MMRIS)

Une MMRIS repose sur un système instrumenté de sécurité, c'est-à-dire un système combinant capteur(s), unité de traitement et actionneur(s) ayant pour objectif de remplir exclusivement des fonctions de sécurité. Elle se matérialise par exemple par :

- une sécurité de pression haute avec ouverture automatique d'une vanne ;
- une alarme de sécurité avec intervention de l'opérateur sur un bouton-poussoir…

De manière générale, une chaîne instrumentée est considérée comme MMRIS lorsque ses éléments sont uniquement dédiés à la sécurité. Toutefois, les éléments d'une chaîne de sécurité peuvent aussi être utilisés pour la conduite de l'installation, sous réserve :

- qu'ils ne soient pas susceptibles de conduire à un événement initiateur à l'origine du scénario d'accident,
- que l'action de sécurité qu'ils assurent soit prioritaire sur toutes leurs autres actions,
- qu'ils ne soient pas déjà pris en compte dans une MMRIC pour ce scénario.

Dans le cas où un exploitant propose une MMRI basée sur un automate dédié également à des fonctions de conduite, l'exploitant doit a 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 opérateur 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 .

L'inspection se prononcera sur l'acceptabilité de la chaîne en tant que MMRIS en se basant en tant que de besoin sur une tierce expertise qui examinera le respect des critères ci-dessus.

Sous réserve d'un choix adapté pour les différents éléments de la chaîne (garanties sur la fiabilité, notamment via le retour d'expérience disponible ou un document justificatif), un niveau de confiance de 1 (NC1) d'une MMRIS peut être atteint lorsque le système de sécurité est conçu, exploité et maintenu dans des conditions standards et selon de bonnes pratiques (standards ou référentiels, recommandations fournisseurs, architecture éprouvée, concept éprouvé, procédures de sécurité…). Les règles de maintenance de l'exploitant font l'objet de procédures écrites telles que définies dans le guide DT 93 pour la gestion et la maîtrise du vieillissement des MMRI.

Si le NC affiché d'une MMRIS est supérieur à 1, il pourra être demandé à l'exploitant une justification particulière. Diverses méthodes peuvent être utilisées, notamment via :

- l'application des normes NF EN 61508 et NF EN 61511, ou ;
- l'application d'autres méthodes de calcul ou d'estimation de la fiabilité comme le référentiel Ineris Ω10.

La justification attendue devra comporter des éléments sur les critères de redondance retenus pour atteindre ce NC.

2.3.2 MMRI de Conduite (MMRIC)

Une MMRIC est une MMRI intégrée au système de conduite de l'installation. Elle se matérialise par exemple par :

- une alarme sur le système de conduite avec intervention de l'opérateur 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.

Pour que les chaînes implantées dans un système de conduite soient considérées comme des MMRIC, il faut que les conditions minimales suivantes soient vérifiées :

- les éléments de la chaîne ne sont pas susceptibles de conduire à un événement initiateur à l'origine du scénario d'accident ;
- l'action de sécurité assurée par les éléments de la chaîne est prioritaire sur toutes leurs autres actions ;
- les modifications des paramètres (les seuils d'alarme, par exemple) sont gérées au travers de procédures ou du système de gestion de la sécurité de l'établissement, quand il existe (cf. § 7.5 du guide DT 93) ;
- l'exploitant a mis en place une maintenance préventive au titre de la fonction de sécurité remplie (cf. guide DT 93, notamment son § 6.3.2) ;
- le système de conduite est conçu, exploité et maintenu dans des conditions standards et selon de bonnes pratiques (standards ou référentiels, architecture éprouvée, concept éprouvé, 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 à 1 (valeur retenue dans la norme NF EN 61511 « Sécurité fonctionnelle : Systèmes instrumentés de sécurité pour les industries de transformation »).

Sur un même scénario d'accident, deux MMRIC maximum peuvent être reconnues, sous réserve qu'elles soient indépendantes entre elles selon les critères précisés au § 3.1.

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'évaluation du niveau de confiance (définis notamment dans le référentiel Ineris Ω20).
Pour mémoire, 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 (cf. circulaire du 10 mai 2010).
S'agissant d'actions humaines intégrées à des MMRI, il convient particulièrement de s'assurer :

- que les alarmes associées aux MMRI sont facilement identifiables par l'opérateur sur le poste de conduite ;
- que les actions associées à ces alarmes sont clairement définies (notamment dans des procédures) ;
- de la disponibilité de l'opérateur (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) ;
- de 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

Un schéma en annexe 4 illustre les principes des paragraphes 3..1 et 3.2.

3.1 Indépendance des MMRIC

Sur un même scénario 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 accessoires[1] cités au paragraphe 3.3.3 du guide DT 93 (parafoudre, module d'isolement galvanique, module de conversion, etc.), les éléments de transmission du signal de type câblage, à l'exception des dispositifs à 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 porté par le câble) et qu'elles fassent appel à des opérateurs 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.

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

[1] Ne sont pas visés les accessoires non cités au § 3.3.3 du guide DT 93 tels que boîte de jonction, rack ou tranchée.

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) ;
- que 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) ;
- que la programmation de chaque fonction assurée par les MMRIS est rendue distincte (programme séparé, page de configuration séparée…) ;
- que 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) ;
- que la somme des NC retenus pour ces MMRIS est inférieure ou égale au NC de l'automate ;
- qu'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 ;
- que les choix techniques ont été faits par du personnel compétent, interne ou externe à l'entreprise, conformément au § 8 du guide DT 93 ;
- que le niveau de confiance global est évalué au regard de la probabilité d'occurrence d'éventuels modes communs de défaillance (sur le matériel et le logiciel) ;
- que l'évaluation et la vérification 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 ;
- de la justification de la maîtrise des modes communs de défaillance.

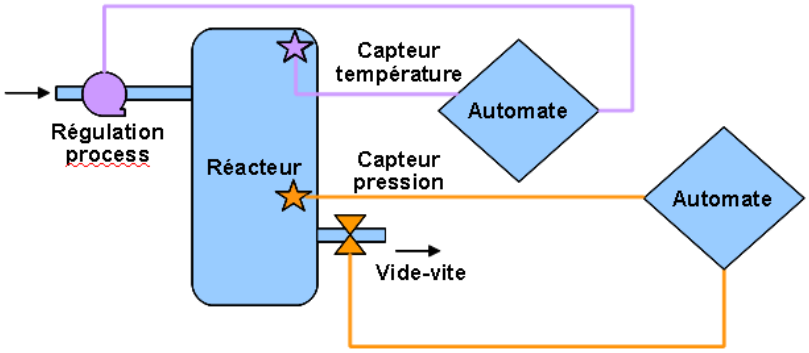
Une tierce-expertise peut compléter les éléments d'analyse de ce type de structure complexe avec un APS gérant plusieurs MMRIS pour un même scénario d'accident.

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 à la fois des MMRIS et des MMRIC pour le même scénario 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 dès la phase de conception de l'installation.

Annexe 1 – Illustration du § 2.1

Cas 1 : illustration du principe qu'un événement initiateur à l'origine du scénario d'accident ne doit pas lui-même entraîner une défaillance ou une dégradation de la performance de la MMR



Descriptif de l'installation

L'introduction en réactif est régulée par la chaîne de conduite *capteur t° - automate – vanne de régulation*.

Le réacteur est équipé d'une MMR *capteur de pression – automate – vide-vite*, en vue d'éviter la perte de confinement du réacteur en cas de montée anormale en pression (au delà de 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.

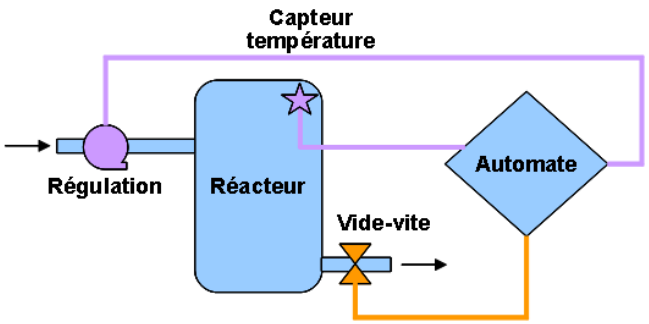
Scénario 2

Une erreur dans l'introduction du réactif entraîne 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.

<u>Cas 2</u> : illustration du principe que le scénario d'accident ne doit pas avoir pour origine une défaillance d'un élément de la MMR.



<u>Descriptif de l'installation</u>
L'introduction en réactif est régulée par la chaîne 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).

<u>Scénario 1</u>
Un défaut sur le *capteur t°* (dérive du capteur) 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 remonté 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.

<u>Scénario 2</u>
Une erreur dans l'introduction du réactif entraîne 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.

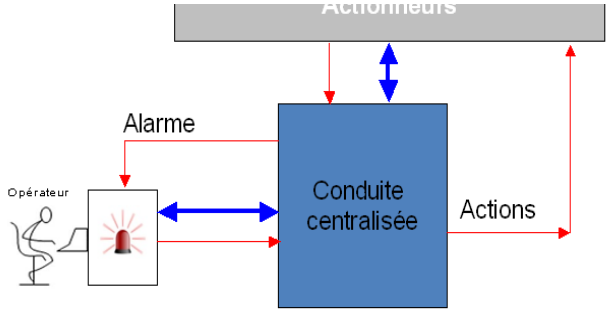
Annexe 2 - Illustrations de chaînes instrumentées avec intervention humaine à considérer ou non comme MMRI (§ 2.2)

Dans les exemples ci-dessous :

- par « conduite centralisée », il convient de comprendre « système de conduite de l'installation » ;
- ⟷ = contrôle du process ;
- → = fonction MMRI.

Exemple 1 : alarmes et actions passent par le système de conduite centralisé

Exemple 1 : alarmes et actions passent par le système de conduite centralisé

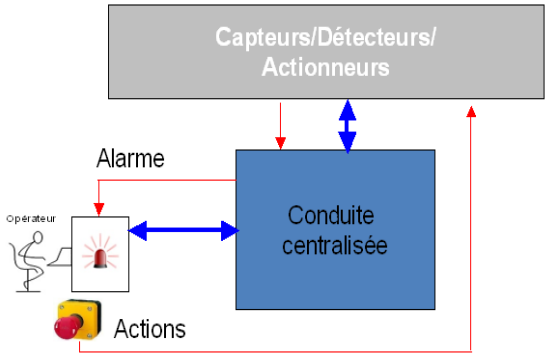


A : La prise d'information est technique (capteur/détecteur)

B : Le traitement de l'alarme (analyse et choix de l'action à mener) est humain (opérateur)

C : L'action est technique (actionneur commandé depuis la commande de la conduite centralisée)

Exemple 2 : alarmes passent par le système de conduite centralisé – actions indépendantes



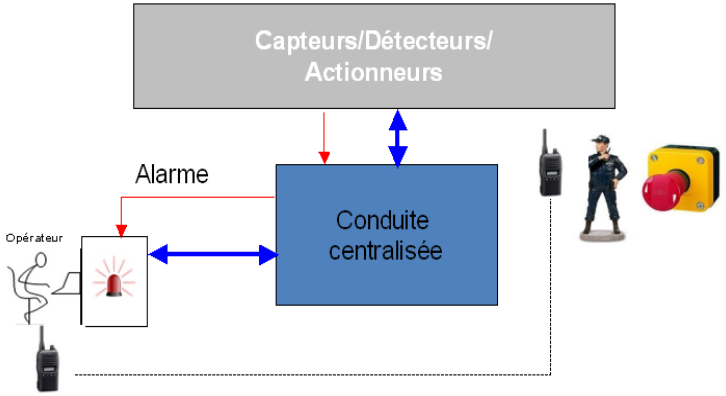
A : La prise d'information est technique (capteur/détecteur)

B : Le traitement de l'alarme (analyse et choix de l'action à mener) est humain (opérateur)

C : L'action est technique (actionneur commandé par un bouton poussoir)

NB : le traitement de l'alarme (humain ou automatique) est à différencier du traitement du signal (automatique pour une MMRI).

Exemple 3 : actions indépendantes du système de conduite centralisé

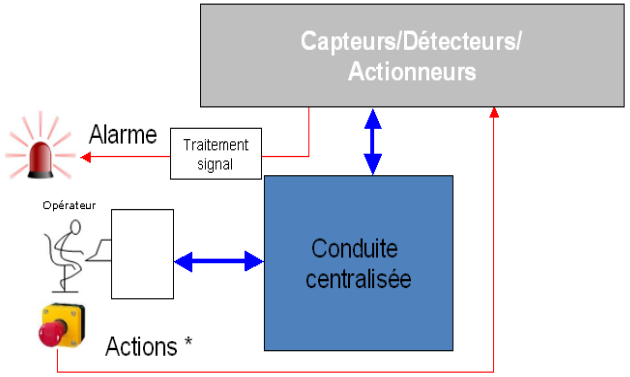


A : La prise d'information est technique (capteur/détecteur)

B : Le traitement de l'alarme (analyse et choix de l'action à mener) est humain (opérateur)

C : L'action est humaine (l'opérateur en salle de contrôle prévient un opérateur de terrain qui actionne la sécurité)

Exemple 4 : alarmes et actions indépendantes du système de conduite centralisée



** Les actions indépendantes peuvent transiter directement vers les actionneurs ou via automate/relayage de sécurité*

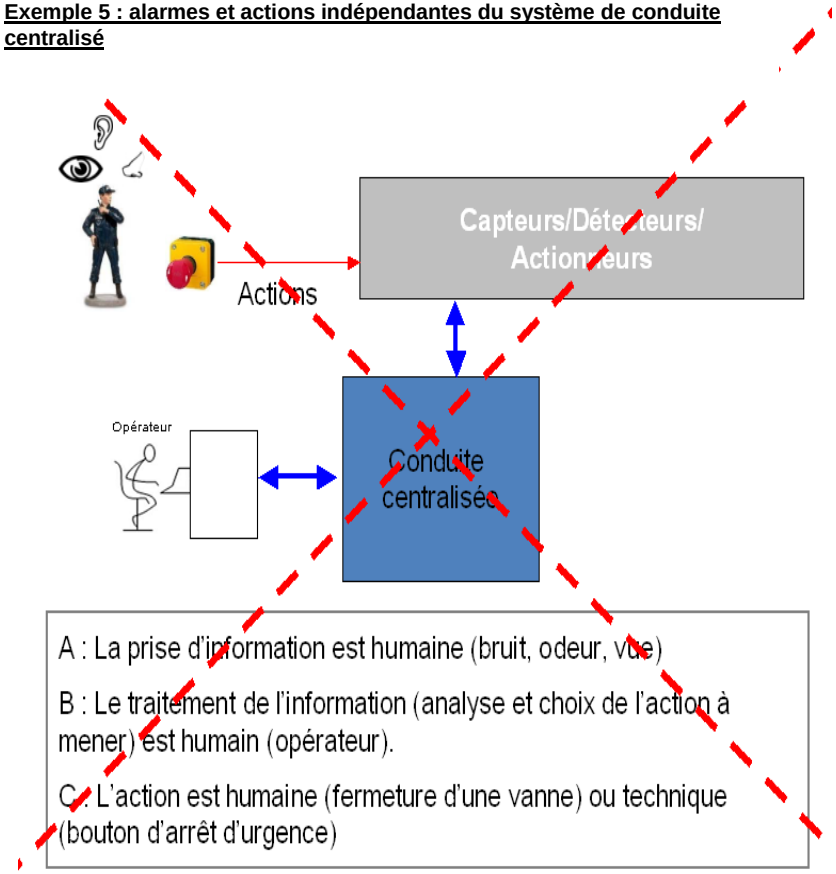
A : La prise d'information est technique (capteur/détecteur)

B : Le traitement de l'alarme (analyse et choix de l'action à mener) est humain (opérateur)

C : L'action est technique (actionneur commandé par un bouton poussoir)

NB : il convient de s'assurer du bon fonctionnement la transmission téléphonique.

Exemple 5 : alarmes et actions indépendantes du système de conduite centralisé

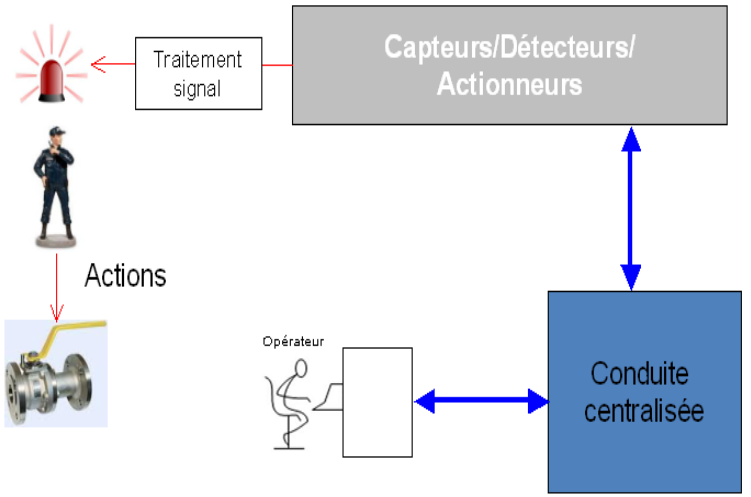


A : La prise d'information est humaine (bruit, odeur, vue)

B : Le traitement de l'information (analyse et choix de l'action à mener) est humain (opérateur).

C : L'action est humaine (fermeture d'une vanne) ou technique (bouton d'arrêt d'urgence)

Exemple 6 : alarmes, traitement et actions indépendantes du système de conduite centralisée



A : La prise d'information est technique (capteur/détecteur)

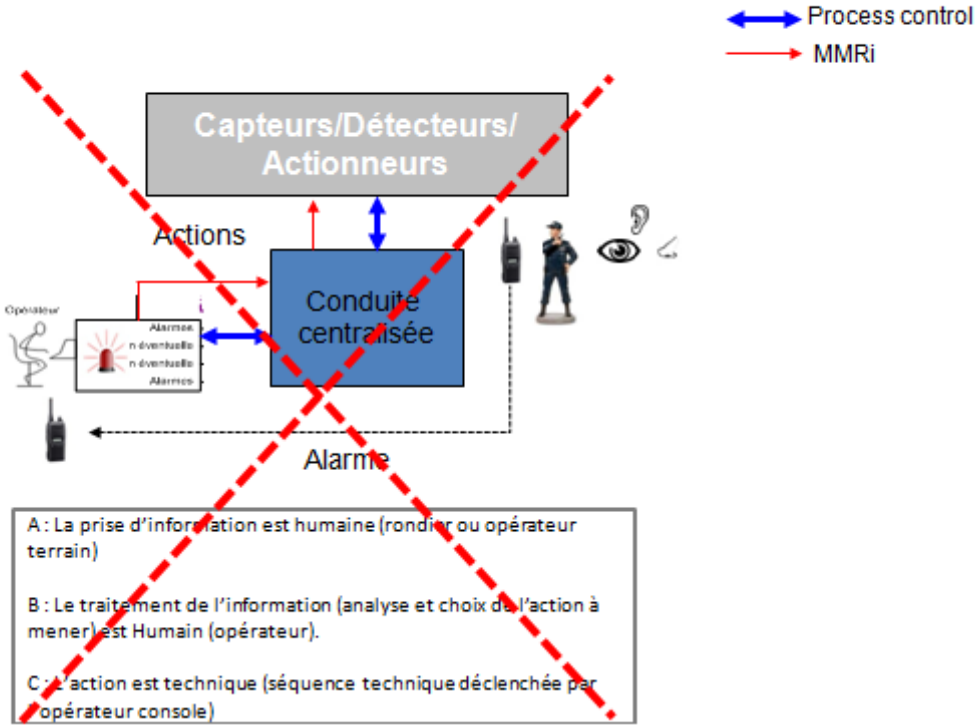
B : Le traitement de l'alarme (identification de la vanne à manipuler) est humain (opérateur)

C : L'action est humaine (manipulation de la vanne, clairement identifiée dans une procédure)

La configuration de l'exemple 5 n'est pas considérée comme une MMR pour chacune des raisons suivantes :

- la prise d'information est humaine
- le traitement de l'information est humain.

Exemple 7 : alarme indépendante du système de conduite centralisé



La configuration de l'exemple 7 n'est pas considérée comme une MMR pour chacune des raisons suivantes :

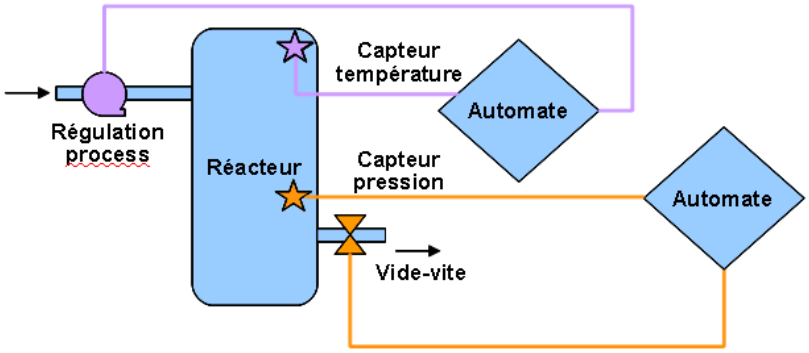
- la prise d'information est humaine
- le traitement de l'information est humain.

Annexe 3 - Exemples illustratifs des § 2.3.1 et 2.3.2 (distinction MMRIS/MMRIC)

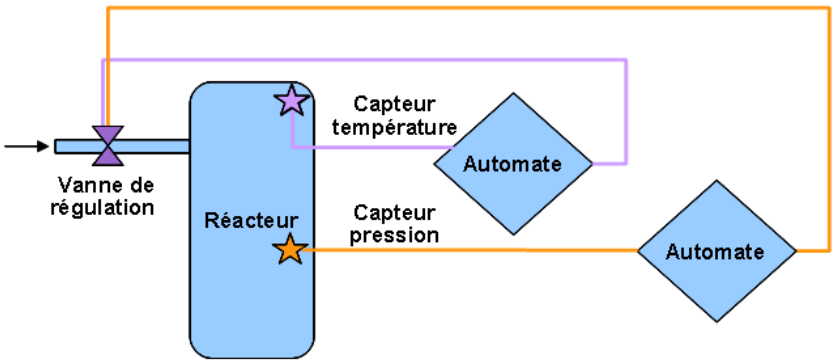
Illustrations du § 2.3.1 sur les MMRIS

Cas 1 : MMRIS constituées d'éléments exclusivement dédiés à la sécurité

Pour le cas 1 de annexe 1 (schéma repris ci-dessous), 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.



Cas 2 : MMRIS avec un actionneur utilisé également pour la conduite du procédé

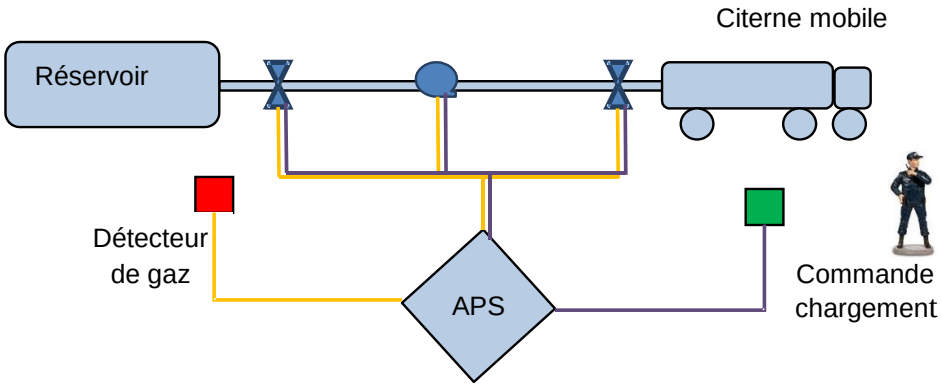


Par rapport au cas 1, la chaîne de sécurité *capteur de pression – automate – vanne* commande la fermeture de la vanne d'entrée en cas de montée en pression dans le réacteur au delà de Pmax. Cette chaîne peut être considérée comme une MMRIS pour le scénario 2 (montée en pression suite à une erreur de 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
- comme 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 : MMRIS avec un automate non dédié exclusivement à la sécurité



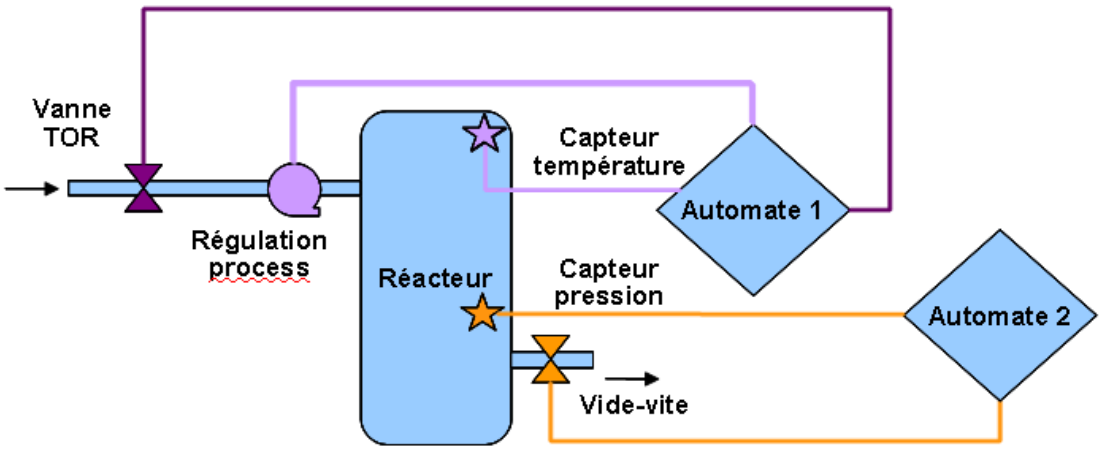
Exemple d'une installation de transfert de produit

Les vannes, ainsi que la pompe fonctionnent uniquement en TOR (Tout Ou Rien). Les vannes sont à sécurité positive (fermeture par manque d'énergie : air, électricité, eau).
La commande de chargement permet à un opérateur 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) .

Illustrations du § 2.3.2 sur les MMRIC

Reprise cas 1 de annexe 1 avec un même automate



Descriptif de l'installation
L'introduction en réactif est régulée par la chaîne 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 (au delà de Pmax).

Scénario

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

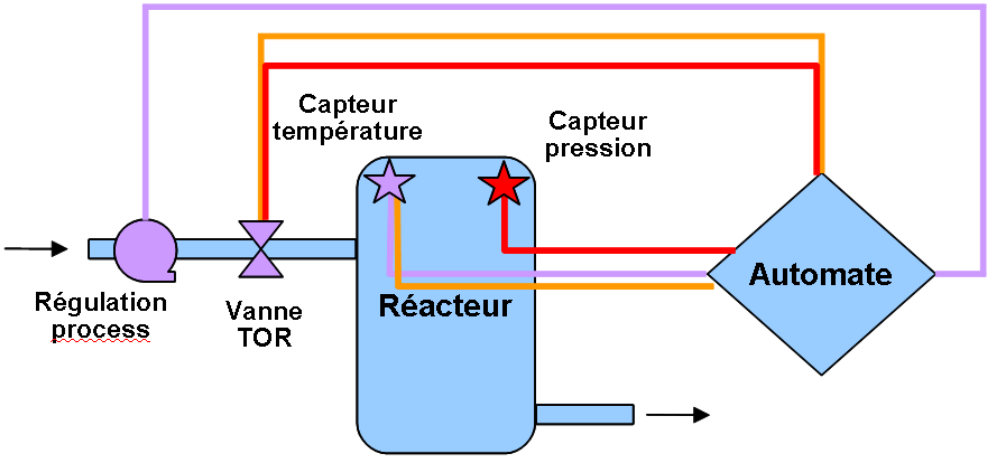
Pour ce scénario :

- 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.
- la chaîne *capteur de pression – automate 2 – vide-vite* peut être valorisée comme MMRIS

Annexe 4 - Exemple illustratif des § 3.1 et 3.2

Illustrations du § 3.1 sur l'indépendance des MMRIC

Chaînes avec un automate commun



Descriptif de l'installation
L'introduction en réactif est régulée par la chaîne 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.

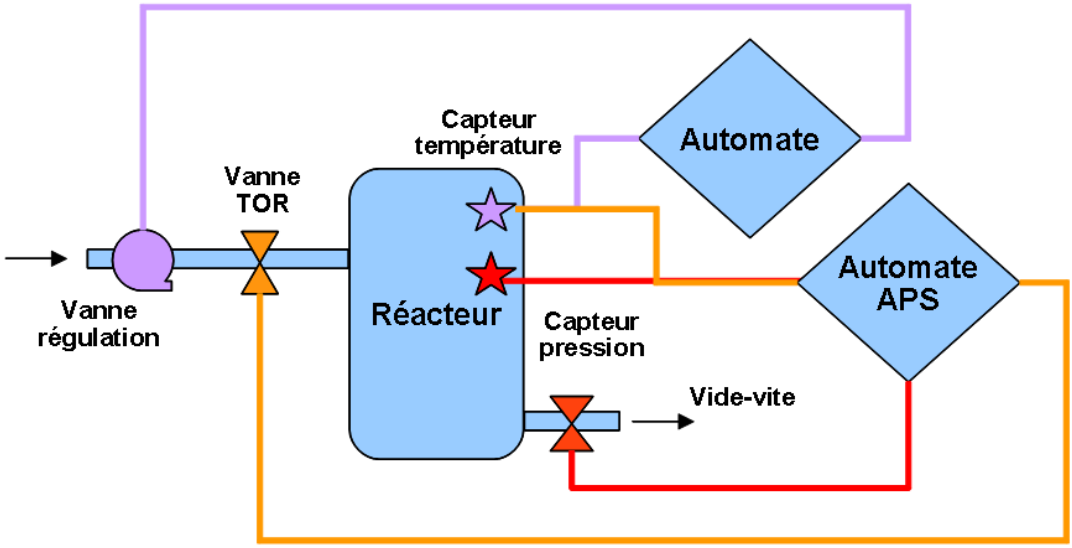
Scénario
Une erreur dans l'introduction du réactif entraîne un emballement thermique, avec montée en pression et en température et risque de perte de confinement.

Pour ce scénario, les chaînes *capteur température – automate – vanne TOR et capteur pression – automate – vanne TOR* ne peuvent pas :

- être considérées comme MMRIS car l'automate est associé à une fonction de conduite non binaire (régulation)
- être 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 scénario 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.

Illustrations du § 3.2 sur l'indépendance des MMRIS



Descriptif de l'installation

L'introduction en réactif est régulée par la chaîne 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 entraîne 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 (cf. § 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).