



GUIDE METHODOLOGIQUE POUR LA GESTION ET LA MAITRISE DU VIEILLISSEMENT DES MESURES DE MAITRISE DES RISQUES INSTRUMENTEES (MMRI)

**Application de l'arrêté ministériel du
4 octobre 2010**



**Guide méthodologique pour la
gestion et la maîtrise du
vieillessement des Mesures de
Maîtrise des Risques
Instrumentées (MMRI)**

**DT 93
Juillet 2011**

Avertissement

Ce document technique ne doit pas être considéré comme exhaustif. Établi de bonne foi, il doit être utilisé comme un guide qui devra dans chaque cas particulier être complété ou adapté et vérifié.

L'Union des Industries Chimiques, l'Union Française des Industries Pétrolières n'acceptent pas de responsabilité dans l'usage qui sera fait de ce document.

Il reflète l'état des connaissances scientifiques et techniques au moment où il a été écrit.

SOMMAIRE

1. Préambule

2. Objet du guide et problématique du vieillissement

2.1. Objet du guide

2.2. Problématique du vieillissement et aspects réglementaires

3. Typologie des MMRI

3.1. Définition et sélection d'une MMRI objet du plan de modernisation

3.2. Architecture de base des MMRI

3.3. Composants-types d'une MMRI

4. Conception des MMRI

4.1. Prise en compte des facteurs de vieillissement des MMRI

4.2. Paramètres à prendre en compte

5. Mécanismes de vieillissement des composants d'une MMRI

5.1. Généralités

5.2. Processus de vieillissement des composants Electriques, Electroniques et Electroniques Programmables

5.3. Processus de vieillissement des matériaux organiques, polymères et composites des composants et matériels électriques

5.4. Capteurs

5.5. Transmission de l'information

5.6. Systèmes de traitement de l'information

5.7. Eléments terminaux

5.8. Sources d'énergie

6. Bonnes pratiques en matière de maintenance et de tests des MMRI

6.1. Programme et plans de surveillance

6.2. By-pass, inhibition des MMRI

6.3. Maintenance

6.4. Tests de fonctionnement

6.5. Gestion des pièces de rechange et de l'obsolescence

7. Exploitation des MMRI

7.1. Objectif

7.2. Organisation de l'exploitation des MMRI

7.3. Procédures et documents d'exploitation des MMRI

7.4. Analyse des événements

7.5. Modification des MMRI

8. Gestion des compétences

8.1. Objectif

8.2. Activités liées à la sécurité des installations et définition des compétences requises

8.3. Évaluation des compétences

8.4. Acquisition et maintien des compétences requises

8.5. Le contrôle des compétences des prestataires extérieurs à l'entreprise

9. Etat zéro et fiche de vie d'une MMRI

10. Annexes

10.1 Logigramme de sélection

10.2 Exemple illustratif

10.3 Méthode alternative à la norme de détermination de la période de test des MMRI

11. Glossaire des termes techniques

12. Terminologie

13. Référence de normes citée

14. Autres documents de référence

1. Préambule

Ce guide a été réalisé par un collège d'experts, de fournisseurs/fabricants de matériel et de représentants de l'administration et de l'industrie. Il présente des techniques et méthodes de gestion et de maîtrise du risque technologique lié au vieillissement des mesures de maîtrise des risques instrumentées¹ (MMRI) exploitées dans les installations industrielles à risques au sens de l'arrêté du 10 mai 2000 modifié² susceptibles de porter atteinte aux intérêts visés par l'article L. 511-1 du code de l'environnement.

Il s'agit d'un document évolutif et révisable dans les mêmes conditions que celles qui ont prévalu à son élaboration. Il est le reflet de l'état de l'art, en l'état actuel des connaissances des experts ayant participé à son élaboration.

Ce document est un guide de type 1 selon la note de doctrine du 19 juin 2008 du directeur général de la prévention des risques. D'autres techniques ou méthodes peuvent être utilisées, sous réserve qu'elles fassent l'objet d'une tierce-expertise conformément aux dispositions de l'arrêté du 4 octobre 2010.

Ce guide s'inscrit dans le cadre de la mise en application du plan de modernisation (cf. articles 7 et 8 de l'arrêté ministériel du 4 octobre 2010).

Un logigramme joint en annexe 10.1 illustre l'application de différents chapitres du guide (sélection des MMRI visées par le guide, détermination pour ces MMRI de fréquences de test...).

2. Objet du guide et problématique du vieillissement

2.1. Objet du guide

Le présent guide a été réalisé suite aux travaux débutés en 2009 dans le cadre de la mise en œuvre d'un plan d'actions pour la maîtrise du vieillissement des installations industrielles à risques technologiques (dit « plan de modernisation ») lancé par le ministère du développement durable en fin d'année 2008.

Il est le fruit des travaux menés de 2009 à 2011 au sein du groupe de travail national dédié à la problématique du vieillissement des mesures de maîtrise des risques instrumentées. Ces travaux ont été pilotés par le ministère du développement durable.

Depuis plusieurs années, le ministère du développement durable diffuse des guides sectoriels dans le cadre de la politique de prévention des risques technologiques. Ces guides sont le plus souvent issus de la réflexion et des échanges au sein d'un groupe de travail mis en place par le ministère, comme dans le cas du groupe évoqué ci-dessus.

Ce guide est considéré par l'administration comme constituant un recueil de bonnes pratiques d'utilité reconnue. Il a été élaboré et mis en consultation auprès des différentes fédérations professionnelles concernées à l'issue des travaux du groupe de travail.

¹ Les MMRI sont englobées dans les « MMR » au sens de la circulaire du 29 septembre 2005.

² Arrêté du 10 mai 2000 modifié relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation.

Le présent guide constitue principalement :

- un panorama des techniques existantes (françaises et étrangères) pour le suivi des MMRI et de leur matériel connexe (utilités),
- un document pratique donnant des règles pour la gestion et la maîtrise globales du vieillissement de ces équipements dans le temps.

Ce guide se concentre sur les équipements existants à sa date de validation et sur de nouvelles pistes d'améliorations à prendre en compte par les industriels et à décliner concrètement dans l'ensemble des sites SEVESO.

2.2. Problématique du vieillissement et aspects réglementaires

2.2.1 Contexte global

Plusieurs incidents et accidents survenus ces dernières années dans les installations industrielles françaises ont pointé du doigt la problématique du vieillissement des installations, de leur maintenance et de leur surveillance en exploitation.

Ce constat a conduit la DGPR à lancer fin 2008 (cf. note de méthode du 12 décembre 2008) une démarche visant à élaborer un plan d'actions pour la maîtrise et la gestion du vieillissement des installations industrielles à risques technologiques. L'objectif de cette démarche est d'établir des guides qui permettront la mise en œuvre de ces plans d'actions.

2.2.2 Problématique du vieillissement

2.2.2.1 Cas général des MMR

La principale problématique du vieillissement des MMR est l'indisponibilité des fonctions de sécurité associées qui peut conduire à la dégradation du niveau de sécurité des installations. Cette dégradation peut conduire à la perte de confinement, et plus généralement à toute défaillance pouvant conduire à l'émanation de substances dangereuses à l'extérieur du site. Ces événements peuvent présenter des risques par :

- l'énergie emmagasinée si l'équipement est sous pression,
- le caractère dangereux de la substance, vis-à-vis des personnes ou de l'environnement.

Les risques encourus sont alors principalement liés à un impact sur la population environnante et/ou sur l'environnement (pollution).

Le vieillissement doit être pris en compte à la conception et être maîtrisé par des opérations de suivi qui peuvent s'effectuer lors du fonctionnement de l'installation ou en phase d'arrêt. En phase d'arrêt, ces opérations peuvent entraîner la modification ou le remplacement de tout ou partie de l'équipement dont le suivi aurait révélé des anomalies.

Les MMR doivent donc faire l'objet d'un suivi adapté.

2.2.2.2 Spécificité des MMRI

Au même titre que les MMR, les MMRI doivent faire l'objet d'un suivi adapté dont les principes font l'objet de ce guide. Ce suivi doit également prendre en compte la gestion de l'obsolescence et le maintien des compétences tout au long de la durée de vie de la MMRI.

2.2.3 Aspects réglementaires du vieillissement

2.2.3.1 Cas général

De façon générale, les MMRI doivent répondre aux exigences fixées dans l'article 4 de l'arrêté ministériel du 29 septembre 2005³, dans les articles 7 et 8 de l'arrêté du 4 octobre 2010⁴ spécifique au suivi et à la gestion du vieillissement des MMRI et à l'article 7.1 de l'arrêté du 10 mai 2000 modifié.

2.2.3.2 Cas particulier des accessoires de sécurité montés sur les Equipements Sous Pression (ESP)

L'examen et la vérification des accessoires de sécurité intégrés dans une MMRI et couverts par la réglementation des ESP, font l'objet des exigences définies dans le présent guide, sans préjudice des prescriptions prévues au titre de la réglementation ESP (notamment en ce qui concerne les inspections et requalifications périodiques aux intervalles fixés pour les équipements qu'ils protègent). S'agissant de la réglementation ESP, la nature des contrôles à réaliser est déterminée de manière plus précise dans la circulaire BSEI n°06-080 du 6 mars 2006⁵.

Il existe une norme européenne harmonisée (NF EN 764-7) qui donne des éléments sur la conception et le suivi des accessoires de sécurité montés sur les ESP.

2.2.4 Aspects normatifs

Des normes de sécurité fonctionnelle d'application volontaire (notamment la norme NF EN 61511) donnent de bonnes pratiques pour la conception, la gestion et la maîtrise des SIS dont certaines pourraient être utilisées pour traiter la problématique liée au vieillissement.

3. Typologie des MMRI

3.1. Définition et sélection d'une MMRI objet du plan de modernisation

Une MMRI est une MMR faisant appel à de l'instrumentation de sécurité et constituée d'un ensemble d'éléments techniques et/ou organisationnels nécessaires et suffisants pour assurer une fonction de sécurité. Elle est visée par l'article 4 de l'arrêté du 29 septembre 2005.

Les MMRI sont identifiées dans les études de dangers.

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 opérateur).

³ Arrêté modifiant l'arrêté du 10 mai 2000.

⁴ Arrêté relatif à la prévention des risques accidentels au sein des installations classées pour la protection de l'environnement soumises à autorisation.

⁵ Circulaire relative aux conditions d'application de l'arrêté du 15 mars 2000 relatif à l'exploitation des équipements sous pression, modifié en dernier lieu par l'arrêté du 30 mars 2005.

Pour un accident potentiel placé sur la grille d'appréciation de la maîtrise des risques de la circulaire du 10 mai 2010⁶, une mesure de sécurité instrumentée présente au sein d'un établissement visé par l'arrêté du 10 mai 2000 modifié est identifiée comme MMRI devant faire l'objet d'un suivi particulier, en application des dispositions de l'article 7 de l'arrêté du 4 octobre 2010, lorsque l'application d'une probabilité de défaillance égale à 1 ferait passer l'accident potentiel correspondant dans une case MMR rang 2 ou NON de la grille de la circulaire du 10 mai 2010 avec un niveau de gravité au moins "important" selon l'arrêté du 29 septembre 2005. Toutes les MMRI agissant dans les scénarios d'accidents relevant de la ligne « désastreux » sont retenues dans le cadre du présent guide.

Dans le cas où cette méthode conduirait à exclure du plan de modernisation plusieurs MMRI pour un même scénario d'accident, l'exploitant ne pourra exclure qu'une de ces MMRI et exclura la moins fiable (cf. exemple en annexe 10.2).

Les MMRI visées par le plan de modernisation doivent être définies parmi les MMR prises en compte pour déterminer la probabilité des phénomènes dangereux. Toutefois, pour les établissements soumis à autorisation avec servitudes (AS), il est possible que, dans leur étude de dangers actuelle, la probabilité des phénomènes dangereux ait été déterminée à partir d'une cotation de l'Événement Redouté Central (ERC). Dans ces conditions, les dispositions du guide seront également appliquées, de manière transitoire dans l'attente de la révision quinquennale de leur étude de dangers, aux EIPS instrumentés en complément des MMRI déjà identifiées. L'exploitant devra préalablement s'assurer que les EIPS intègrent les différents éléments qui conduisent à l'action de sécurité.

En ce qui concerne les établissements Seveso seuil bas, les études de dangers remises à l'échéance du 7 octobre 2010 identifient clairement les MMRI en amont et en aval de l'Événement Redouté Central. Dans le cas où ces études auraient déterminé la probabilité des phénomènes dangereux à partir d'une cotation de l'ERC, l'étude est complétée en vue d'identifier les MMRI en amont de l'Événement Redouté Central pour la remise de l'état initial au 31 décembre 2013.

3.2. Architecture de base des MMRI

Les MMRI sont constituées de l'ensemble d'éléments comprenant :

- les capteurs, leurs connexions et leurs liaisons (y compris les éléments de traitement du signal (parafoudre, barrière d'isolement galvanique, barrière de sécurité intrinsèque, etc.)),
- l'interface opérateur dans le cas où l'action humaine fait partie de la MMRI,
- les logiques (numérique ou câblée) avec ou sans logiciel,
- les actionneurs et leurs liaisons :
 - relais de découplage, électrovannes et vannes,
 - organes de coupure et de commande des actionneurs électriques,
 - avertisseurs sonores et lumineux,
- les supports de transmission.

Ces éléments peuvent également être soumis aux exigences d'autres réglementations (ATEX, champs électromagnétiques...).

⁶ Circulaire récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risque à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003.

3.3. Composants-types d'une MMRI

3.3.1 Capteurs

Les capteurs mesurent en général des grandeurs physiques sur le procédé telles que pression, débit, niveau, température, vibrations, etc. et plus rarement des concentrations (analyseurs, etc.).

Les capteurs peuvent être « externes » au procédé (détecteurs de gaz et détecteurs incendie...).

Les équipements rencontrés sont généralement les suivants :

- Capteurs-Transmetteurs 4-20 mA,
- Capteurs « tout ou rien »,
- Capteurs-Transmetteurs dits « intelligents » ayant une capacité de traitement embarquée et de nouvelles fonctionnalités (auto-diagnostic, auto-ajustage, communication, etc.),
- Dispositifs pneumatiques,
- Arrêts d'urgence.

3.3.2 Systèmes de traitement

Pour la partie procédé, les systèmes de traitement gèrent en général l'ensemble des fonctions de sécurité de l'installation (ou d'une sous partie). Les systèmes de protection (systèmes feu et gaz) peuvent disposer de systèmes de traitement spécifiques.

3.3.2.1 Les systèmes de traitement à logique programmable ou paramétrable

En technologie numérique, ce sont généralement des calculateurs (Systèmes Numérique de Contrôle Commande (SNCC ou BPCS (Basic Process Control System)), des Automates Programmables Industriels standard (API ou PLC (Programmable Logic Controller)) avec fonction de supervision...) ou des Automates Programmables de Sécurité (APS).

En technologie conventionnelle, ce sont des régulateurs individuels ou du relayage.

Suivant la taille, la complexité de l'unité et la modularité de l'unité, la fonction d'automatismes est remplie par un ou plusieurs modules (API, contrôleurs de SNCC, APS, équipements de technologie conventionnelle) ou toute association de ces modules.

Dans le cadre de l'application du présent guide, l'utilisation d'un APS certifié selon la norme NF EN 61508 (ou autres standards tels que les normes EN ISO 13849 et EN 954-1) doit être retenue afin de s'assurer du maintien du niveau de sécurité requis lorsqu'un niveau de confiance (NC) strictement supérieur à 1 est recherché.

Leurs processeurs, leur mémoire et leur alimentation peuvent être redondants et disposent de fonctions d'autodiagnostic. Leur positionnement de repli de sécurité est connu en cas de défaut.

3.3.2.2 Les systèmes à base de logique statique de sécurité

Ces systèmes sont utilisés pour des applications spécifiques impliquant un très haut niveau de confiance des fonctions de sécurité. Ils sont réalisés avec des composants non programmables : aucun microprocesseur ou aucune puce programmée n'est utilisé pour les fonctions de sécurité. La logique de sécurité est basée sur des éléments matériels électriques et électroniques (de type résistance, transistors...). Ils peuvent être également appelés Solid State Logic Solver.

3.3.2.3 Les systèmes à base de logique à relais

Il s'agit de technologie à base de modules/relais de sécurité électromécaniques. Dans ce cas, pour les capteurs analogiques, le signal doit être converti en signal logique via des modules de relais à seuil de sécurité.

Dans le cadre de l'application du présent guide, l'utilisation de modules/relais éprouvés par l'usage ou certifiés selon la norme NF EN 61508 (ou autres standards tels que les normes NF EN 61511, EN ISO 13849 et EN 954-1) doit être retenue afin de s'assurer du maintien du niveau de sécurité requis lorsqu'un niveau de confiance (NC) strictement supérieur à 1 est recherché.

3.3.3 Les accessoires

Certains accessoires peuvent être nécessaires pour limiter les interactions entre l'équipement et son environnement (parafoudre, enveloppe de protection (quand la réglementation ATEX n'est pas applicable à l'installation), isolement galvanique, etc).

Des accessoires électroniques de traitement de signal sont parfois nécessaires :

- module d'isolement pour le cas de signaux en sécurité intrinsèque,
- module de conversion pour les températures, vibrations, etc.

3.3.4 Les interfaces opérateurs

Ce sont en général :

- des informations visuelles ou sonores sur les écrans de conduite ou verrines d'alarme,
- des avertisseurs (feux lumineux, klaxon, sirènes...) pour les systèmes d'avertissement feu et gaz et alarmes spécifiques.

3.3.5 Les éléments terminaux

Les organes utilisés pour les MMRI peuvent être par exemple :

- des vannes Tout Ou Rien (TOR) équipées d'un servomoteur électrique, hydraulique, pneumatique, ou de toute combinaison de ces énergies. Ces vannes peuvent être équipées :
 - ✓ d'une électrovanne,
 - ✓ d'un électro-positionneur,
 - ✓ de contacts de fin de course / indicateur de position,
 - ✓ de réserve d'énergie,
 - ✓ de protection feu.

Le servomoteur est piloté par le système de sécurité,

- des éléments électriques ou instrumentés intégrés aux machines tournantes s'ils font partie de la MMRI. Deux familles peuvent être identifiées :
 - ✓ Les machines tournantes intégrées au procédé dont l'arrêt est requis par les fonctions de sécurité ou dont le fonctionnement est une des sources potentielles de survenance du scénario redouté (pompes, compresseurs, aéro-réfrigérants, pompes à vide...). Dans ce cas, la fonction de sécurité consiste à couper l'énergie. Dans le cas où la machine tournante est à l'origine du scénario, l'instrumentation peut alors consister en un ensemble de capteurs (survitesse, vibrations, pression, détection de fuite, etc.), éventuellement reliés à un automatisme de sécurité, des alertes ou un arrêt d'urgence.
 - ✓ Les machines tournantes dont la fonction de sécurité associée dépend de leur bon fonctionnement (groupe motopompe à incendie, ventilateur d'extraction, pompes d'abattage/lavage...).

Dans le cas des pompes à incendie, la commande de sécurité de démarrage est en général issue d'une chute de pression détectée par un ou plusieurs capteurs. Le démarrage des pompes entraînées par moteur électrique est assuré par un boîtier de commande électromécanique (avec contacteur de puissance). Généralement, pour les pompes entraînées par moteur thermique, la technologie est de type électronique (cartes électroniques et signaux analogiques ou système programmable) puis électromécanique par relaiage pour la commande de démarreur du moteur diesel.

Remarque : en complément des éléments cités ci-dessus, dans certains cas particuliers et sous certaines conditions, les éléments terminaux des MMRI pourraient être des vannes de régulation ou des variateurs de vitesse.

3.3.6 Les sources d'énergie

Il existe plusieurs sources d'énergie :

- Electrique,
- Pneumatique,
- Hydraulique (liquide ou vapeur).

Ces sources d'énergie peuvent être combinées et éventuellement secourues.

3.3.7 Les supports de transmission

Les informations utiles au fonctionnement des MMRI peuvent être de plusieurs types :

- elles sont logiques ou binaires quand leur valeur (ou la condition qu'elles représentent) est vraie ou fausse,
- elles sont analogiques quand elles représentent des grandeurs physiques associées à des échelles de mesure.

Ces informations peuvent être échangées sous plusieurs formes :

- électrique,
- pneumatique,
- hydraulique,
- numérique.

Exemples	Valeur logique	Valeur analogique
Electrique	Contact fermé ou ouvert Présence ou absence tension	4-20 mA 1-5 V
Pneumatique	Présence ou absence pression	0,2-1 bar ; 3-15 PSI
Numérique	bit	Mot de n bits

Dans l'industrie les modes d'échange les plus répandus sont le mode électrique, et depuis quelques décennies déjà, le mode numérique (réseau de communication, électrique ou optique).

Soit la transmission de ces signaux est filaire (ou câblée), soit elle se fait par réseau communicant (sur support électrique, optique ou électromagnétique).

La transmission de signaux logiques de manière filaire est simple, fiable et facile à tester ; elle doit être privilégiée quand les conditions le permettent (petites distances et nombre limité d'information à transmettre).

La transmission de signaux analogiques par boucle de courant 4-20 mA, proportionnelle à la grandeur mesurée, est la plus répandue. Cette plage de valeur est parfois étendue à 0-22 mA pour permettre des fonctions de diagnostic (rupture de boucle ou défaut capteur). Des protocoles spécifiques ont été développés pour permettre le transfert d'informations numériques de diagnostic superposés aux signaux analogiques résultant de la mesure à l'aide d'un codage en fréquence (exemple : protocole HART non certifié comme étant de sécurité).

Au niveau de la transmission de signaux numériques, les réseaux locaux industriels ou réseaux de terrain (ou encore bus de terrain), sont de plus en plus utilisés. Ce sont des dispositifs assurant la transmission d'informations entre des capteurs, des actionneurs et des systèmes de contrôle/commande par l'intermédiaire d'un support unique (câble, fibre optique, radio, etc.). Ces réseaux « standard » non certifiés pour la sécurité n'ont pas été spécifiés et conçus pour la transmission d'informations relatives à la sécurité et des risques potentiels liés à l'implication de ces réseaux dans le maintien d'une fonction de sécurité peuvent avoir pour cause :

- soit une altération du traitement des informations,
- soit un retard dans le traitement des informations.

Ces réseaux peuvent dans certains cas être utilisés comme élément d'une MMRI dont le niveau de confiance doit tenir compte de ces spécificités.

Les réseaux dédiés à la sécurité sont des « composants » capables de répondre à des spécifications de niveau SIL (1, 2 ou 3). Ils permettent parfois la transmission de données du fonctionnel de l'installation (standard) qui ne sont pas gérées par le protocole de sécurité. Ils ne peuvent prétendre être de sécurité que si le concept général (protocole, architecture) a été validé par un organisme qualifié (par exemple, un organisme accrédité), et si tous les composants qui les constituent sont compatibles avec le profil de communication recherché.

4. Conception des MMRI

4.1. Prise en compte des facteurs de vieillissement des MMRI

Il est indispensable de prendre en compte les facteurs de vieillissement dès la phase de conception des MMRI. En effet, les exigences concernant l'aptitude à l'exploitation, à la maintenance et aux tests, intégrées dans cette phase peuvent être remises en cause par un vieillissement prévisible mais surtout prématuré des MMRI.

La conception des MMRI doit tenir compte des mécanismes de dégradation connus et prévisibles et du retour d'expérience issu du matériel installé et exploité dans des conditions similaires (y compris les conditions environnementales).

4.2. Paramètres à prendre en compte

Il est indispensable de prendre en compte les facteurs de vieillissement dès la phase de conception des MMRI. En effet, les exigences concernant l'aptitude à l'exploitation, à la maintenance et aux tests, intégrées dans cette phase peuvent être remises en cause par un vieillissement prévisible mais surtout prématuré des MMRI.

La conception des MMRI doit tenir compte des mécanismes de dégradation connus et prévisibles et du retour d'expérience issu du matériel installé et exploité dans des conditions similaires (y compris les conditions environnementales).

4.2.1. Niveau de confiance (NC)

Le niveau de confiance d'une MMRI est défini dans l'étude de dangers et est lié à une probabilité de non-fonctionnement de la MMRI.

4.2.2. Efficacité

Dès la conception, il devra être prévu les mécanismes permettant de mesurer l'efficacité des MMRI.

L'efficacité s'évalue par un test de bon fonctionnement réalisé suivant un protocole défini, pour vérifier si la MMRI est bien apte à remplir, dans son contexte d'utilisation, la fonction de sécurité qui lui est attribuée (exemple : fin de course de fermeture permettant de s'assurer de la position de sécurité de l'actionneur (lorsque la fonction de sécurité est la fermeture de la vanne), l'interprétation de mesures sur le procédé par l'opérateur confirmant que l'action de mise en sécurité a bien été effectuée, etc.).

Comme précédemment, il est important de prendre en compte les facteurs de vieillissement dans la conception de ces diverses mesures d'efficacité.

4.2.3 Temps de réponse

En complément des mesures à mettre en œuvre pour vérifier l'efficacité et le niveau de confiance de la MMRI, il faut également vérifier que sa technologie est adaptée avec la cinétique du phénomène dangereux qu'elle doit maîtriser et vérifier son temps de réponse à une sollicitation. Le vieillissement, des éléments d'une MMRI, peut être à l'origine d'une dérive du temps de réponse et celui-ci peut ne plus être en adéquation avec la cinétique du phénomène dangereux.

Le temps de réponse correspond à l'intervalle de temps entre le moment où la MMRI, dans un contexte d'utilisation, est sollicitée et le moment où la fonction de sécurité assurée par cette MMRI est réalisée dans son intégralité. Selon cette définition, le temps de réponse intègre :

- le temps nécessaire à la détection d'un ou des événements initiateurs,
- le temps nécessaire au traitement et à la transmission de l'information aux éléments devant remplir la fonction de sécurité,
- le temps nécessaire à la réalisation de l'action de sécurité.

Le temps de réponse peut être vérifié en réalisant des mesures sur site. La conception de la MMRI devra donc prévoir les moyens permettant de le mesurer, soit en opération, soit lors de phases de tests (exemple : mesure du temps de manœuvre sur la base de l'information transmise par le fin de course ou par des repères visuels).

Dans le cas d'une MMRI dont le fonctionnement implique l'action d'un opérateur, l'exploitant doit s'assurer que le temps de réflexion et d'action de l'opérateur est compatible avec le délai de mise en sécurité requis.

4.2.4 Testabilité

Les essais périodiques ont pour objet de vérifier que les MMRI continuent de respecter dans le temps leurs exigences fonctionnelles et de performances.

La conception doit ainsi aussi prendre en compte le critère de testabilité, puisque les tests font partie intégrante du cycle de vie de toute MMRI, en phase d'installation, d'opération ou de maintenance. Les tests peuvent être effectués à l'occasion d'un arrêt d'installation ou en fonctionnement lorsque les tests à l'arrêt ne permettent pas de vérifier à eux seuls le niveau de confiance de la MMRI. Dans le cas de nécessité de tests en fonctionnement, la conception doit prévoir la possibilité de les réaliser (inhibition, by-pass).

La fonction de test peut être dégradée par le vieillissement de composants nécessaires au test (ex : robinet d'isolement bloqué ou non étanche).

Les autodiagnostic peuvent être une alternative à certaines fonctions de tests manuels s'ils sont suffisamment exhaustifs (ex : un système de comparaison avec alarme, permanent, entre deux mesures de la même grandeur du procédé, fonction de contrôle utilisée en régulation permanente,...). Si l'exploitant a recours à ce type de test impliquant une comparaison avec un autre capteur, il doit mener au préalable une analyse probabiliste (semi-quantitative ou quantitative) des éventuels modes communs de défaillance et s'assurer que leur probabilité d'occurrence est compatible avec le niveau de confiance attribué à la MMRI. Lorsque les éléments de la MMRI sont actionnés régulièrement par le procédé, l'autodiagnostic réalisé par le système de traitement installé peut être suffisant.

4.2.5 Maintenabilité

Les temps moyens de réparation doivent être définis. Ils doivent tenir compte du temps du déplacement, du stock de pièces de rechange, des contrats d'entretien et doivent être compatibles avec le maintien dans le temps du niveau de confiance requis pour la MMRI.

A chaque MMRI doit correspondre une stratégie retenue par l'exploitant pour identifier et traiter les problèmes de vieillissement (augmentation significative des taux de défaillance des constituants) et d'obsolescence (perte des supports en pièces de rechange et compétences).

Il convient de s'assurer des moyens nécessaires permettant la maintenance des MMRI (ex : accès, by-pass, isolement, etc.) si la maintenance doit s'effectuer unité en service. La conception doit prendre en compte autant que possible la pérennité des équipements composant la MMRI (ex : privilégier les équipements à long cycle de vie ou équipements banalisés/standardisés).

Dés la conception, l'exploitant doit s'assurer de l'existence de procédures de gestion des inhibitions/by-pass prenant en compte les MMRI. Dans le cas où le by-pass inhibe complètement la MMRI, l'exploitant doit s'assurer de la possibilité de la mise en place de mesures compensatoires.

4.2.6 Exigences techniques

4.2.6.1 Les exigences fonctionnelles

Le cahier des charges relatif aux MMRI doit prendre en compte :

- la définition de la fonction, y compris le temps de réponse le cas échéant,
- les équipements la composant (capteurs, système logique et actionneurs),
- les seuils d'alarme ou de déclenchement et les valeurs régulées.

Pour les MMRI, le cahier des charges doit préciser les exigences de performance (classe d'étanchéité le cas échéant, le niveau de confiance, le domaine de validité et l'incertitude de la mesure dans le cas des capteurs...).

4.2.6.2 Les conditions de service

Pour se prémunir contre une apparition prématurée de phénomènes de vieillissement, il est primordial que l'adéquation entre le type d'équipement et les conditions de service soit prise en compte :

- Compatibilité avec le fluide véhiculé dans les circuits (abrasion, acidité...),
- Compatibilité avec les caractéristiques hydrauliques (pression, température...).

4.2.6.3 Les conditions environnementales

Le cahier des charges relatif aux MMRI doit prendre en compte les conditions environnementales d'utilisation à savoir température, humidité, contaminants, mise à la terre, interférences électromagnétiques/interférences radiofréquence (IEM/IRF), chocs/vibrations, décharges électrostatiques, classification ATEX, foudre...

4.2.6.4 Notion d'indépendance

Une MMRI ne peut pas être à l'origine de l'événement redouté ou du phénomène dangereux sur lequel elle est censée agir ; de même, elle ne peut pas être affectée par les événements du scénario d'accident sur lequel elle intervient avant d'avoir rempli sa fonction.

Dans un nœud papillon, pour un même scénario d'accident, différentes mesures peuvent être retenues en tant que MMRI si elles sont reconnues comme indépendantes les unes des autres.

5. Mécanismes de vieillissement des composants d'une MMRI

5.1. Généralités

Le processus de vieillissement des composants d'une MMRI est différent suivant qu'ils sont statiques ou actifs et est influencé par leurs conditions d'exploitation et modes opératoires (fixes, variables, évolution du point de fonctionnement, des modes d'exploitation au cours de la vie du processus). Les composants électromécaniques, électriques, électroniques analogiques sont susceptibles de présenter des signes précurseurs de vieillissement (apparition de biais et de dérives), contrairement aux composants numériques où la défaillance est plutôt d'apparence spontanée.

Au-delà du vieillissement, les modifications subies par l'installation de production au cours de sa vie opérationnelle lors d'opérations de maintenance ou de rénovation, peuvent avoir une influence prépondérante sur les performances d'une MMRI.

5.2. Processus de vieillissement des composants Electriques, Electroniques et Electroniques Programmables

Le processus de vieillissement des composants dépend de l'intensité et de la fréquence des stress auxquels ceux-ci sont soumis, lors de leur utilisation, voire lors de leur stockage si celui-ci n'est pas réalisé correctement. Ceux qui sont indiqués en gras sont les phénomènes significatifs les plus fréquemment identifiés dans l'industrie. Les phénomènes d'accélération du processus de vieillissement peuvent résulter de la présence d'un stress particulier, de plusieurs stress agissant de manière indépendante ou couplée. Le séquençage des stress, voire leur ordre d'apparition, peut avoir une importance (certaines lésions peuvent être propices à de nouvelles pathologies). Si certains stress sont permanents, ou récurrents (présence de cycles), d'autres peuvent apparaître de manière plus ou moins exceptionnelle (orages, inondations, ensoleillement exceptionnel, radiations, défaillance d'autres équipements ou composants induisant des surchauffes par exemple). Ces stress peuvent être regroupés, suivant leur nature, en 6 catégories (liste non exhaustive) :

- Les stress climatiques :
 - Zone tropicale,
 - Zone désertique,
 - Zone grand froid,
 - Zone fortement kéraunique...

- Les stress physico-chimiques :
 - **Température d'usage**, amplitude et dynamique des cycles thermiques, amplitude et fréquence des dépassements de seuils préconisés (surchauffes...),
 - Pression (vide et altitude), amplitude et dynamique des cycles, etc.,
 - **Ambiance aqueuse/corrosive** (liquide et gaz), condensation, chocs hydriques,
 - Ambiance dessiccative,
 - **Ambiance corrosive** (brouillards salins, fumées...),
 - Présence de polluants (gazeux, liquides et particules),
 - Rayonnements (naturels et artificiels)...
- Les stress mécaniques :
 - Sollicitations mécaniques permanentes (déformations, risque de ruptures...),
 - **Sollicitations mécaniques cycliques ou vibrations** (phénomènes de fatigue avec risque de fissuration, de possible desserrage de connexions...),
 - Propagation de contraintes,
 - **Usure à l'usage fréquent** (embrochage/débrochage des cartes ou des composants) ou mauvaises manipulations,
 - Accélération/décélération, chocs et secousses,
 - **Encrassement** (contacts, circuits de convection...)...
- Les stress électriques :
 - **Tensions d'alimentation** des composants, présence d'harmoniques,
 - Dynamiques des variations de tensions et courants,
 - **Décharges électrostatiques**, décharges ionisantes,
 - Champs magnétiques (respect de la CEM, perturbations radiofréquences...),
 - Chocs (microcoupures ; fréquence, amplitude et dynamique des pics de courant...),
 - Interruptions de service (fréquence et durées),
 - Cycles de charges/décharges (nombre, complétude, dynamique) dans le cas des batteries...
- Autres stress :
 - Faunes,
 - Flores,
 - Micro-organismes,
 - Poussières.
- La qualité des matériaux :
 - Faiblesses structurelles aggravantes (métaux et alliages présentant des défauts internes telles des dislocations ou occlusions),
 - Protection et d'isolement des circuits imprimés (Résines et enrobages silicones), des composants électriques,
 - Protection les composants et de leur servitudes (circuits de convection...),
 - Adéquation des matériaux avec leur environnement et leurs conditions d'exploitation...

S'y ajoutent les possibles combinaisons de stress : électrochimique (réduction anodique ou cathodique en présence d'hydrogène par exemple) en présence de potentiels électriques ou électrostatique, phénomènes thermomécaniques (fluage, rupture par perte de plasticité), thermohydriques (formation de glace)...

5.2.1 Composants électroniques et électroniques programmables

Parmi les stress définis précédemment (détermination le plus souvent empirique), influents sur le processus de vieillissement des composants électroniques numériques, l'exploitant retiendra prioritairement la température et ses variations les plus importantes, l'humidité (liquide et gazeuse), les phénomènes de condensation, les atmosphères corrosives (brouillard salin,

ambiance marine, fumées...), les décharges électrostatiques, la présence de poussières, les traces de corrosion (des composants, des contacts)...

5.2.2 Composants électriques

Parmi les stress définis précédemment influant sur le processus de vieillissement des composants électriques et électroniques analogiques, on retiendra prioritairement la température et ses variations les plus importantes, l'humidité, les poussières...

5.2.3 Partie électromécanique des matériels électriques

Parmi les stress définis précédemment et influant le processus de vieillissement des composants électromécaniques, on ajoutera aux contraintes mécaniques et physico-chimiques : les problèmes de corrosion, d'érosion, de fluage, de fatigue, de fissuration, de présence de dislocations (défaut interne aux métaux et alliages), de possibilité de propagation de contraintes, d'environnement électrochimique (par exemple, réduction anodique ou cathodique en présence d'hydrogène), encrassement...

En effet, en plus des mécanismes de vieillissement concernant les équipements statiques tels que câbles, transformateurs, batteries de condensateurs ; les appareillages électriques (interrupteurs, contacteurs, disjoncteurs, les systèmes à relais...) subissent un vieillissement dépendant des sollicitations mécaniques ou de l'absence prolongée de celles-ci. Les interrupteurs, contacteurs et disjoncteurs sont conçus pour effectuer un certain nombre de manœuvres. Pour exemple, d'un point de vue mécanique :

- En basse tension : un contacteur a une durabilité mécanique comprise entre 10 et 20 millions de cycles de manœuvres⁷.
- En haute tension :
 - un contacteur a une durabilité mécanique de l'ordre de 300 000 cycles de manoeuvres⁷,
 - un disjoncteur a une durabilité mécanique de l'ordre de 10 000 manœuvres⁷.

5.3. Processus de vieillissement des matériaux organiques, polymères et composites des composants et matériels électriques

Compte tenu de la variété des environnements et des matériaux associés aux composants et matériels électriques, une description même sommaire de l'ensemble des mécanismes de vieillissement envisageables est difficile. Néanmoins, les différents types de vieillissement suivants peuvent être appréhendés :

- Le vieillissement physique :
 - Migration de molécules (absorption, évaporation, extraction, biodégradation). La perte des adjuvants entraîne bien entendu la perte des propriétés qu'ils apportaient (stabilité pour les stabilisants, souplesse pour les plastifiants...). Ces phénomènes d'échange matériau-milieu dépendent eux aussi des paramètres thermodynamiques et de la composition du milieu (pression partielle ou activité de l'espèce migrante).
 - Relaxation structurale (déformation, puis fissuration par association d'une contrainte mécanique et d'un liquide tensioactif : cas du polyéthylène par exemple). La cinétique ne dépend que des paramètres thermodynamiques (température T , contrainte σ).
- Le vieillissement mécanique :
 - Fluage/Relaxation,
 - Fatigue,

⁷ Un cycle de manœuvre correspondant à une fermeture et une ouverture de l'appareil hors opération sur défaut.

- Usure.
- Le vieillissement chimique
 - la chaleur (dégradation thermique),
 - la lumière (photo-dégradation),
 - l'oxygène (création d'hydroperoxydes instables se décomposant sous l'effet des UV ou de la chaleur).
- Le vieillissement par interactions avec l'environnement :
 - par thermo-oxydation,
 - par photochimie/photo-oxydation. Les contraintes climatiques (radiations solaires, humidité, chaleur) vont altérer les propriétés mécaniques des matériaux polymères et leur aspect de surface :
 - diminution de la contrainte à la rupture,
 - changement du comportement mécanique,
 - évolution de la rigidité,
 - coloration ou décoloration de la matière,
 - craquelures en surface, farinage.
 - par radiochimie,
 - par milieu réactif,
 - par biochimie/biodégradation : la digestion par microorganismes de fragments de polymère biodégradable produit, en présence d'oxygène, du dioxyde de carbone et de l'eau et en milieu sans oxygène du méthane. Parmi les matériaux biodégradables disponibles sur le marché, on distingue :
 - les polymères issus de ressources renouvelables : amidon, mélanges d'amidon avec d'autres biodégradables, polyacides lactiques (PLA), les polymères bactériens (PHA, PHB, PHBV),
 - les polymères issus du pétrole : polycaprolactone (PCL), copolymères aliphatiques-aromatiques, polyester-amides (BAK...).
- Couplage de vieillissement chimique sous contrainte :
 - physico-chimie,
 - physico-mécano-chimie : stress-cracking en milieu solvant, chocs hygro-thermiques, fissuration/oxydation, fissuration/vieillissement chimique, vieillissement sous contraintes.

Différentes conséquences peuvent être observées sur les propriétés des matériaux. L'oxydation se traduit par la détérioration des propriétés diélectriques dans une certaine gamme de fréquences. Certains processus chimiques se traduisent par la formation d'espèces ayant des bandes d'absorption totalement ou partiellement situées dans le spectre visible (400 à 800 nm). Dans ce cas, les matériaux vont apparaître plus ou moins colorés, comme c'est le cas du PVC. Tous les polymères comportant des groupes aromatiques sont susceptibles de jaunir pendant le vieillissement. On sait que certains produits d'oxydation des amines sont très colorés, notamment en rouge-brun (réactions dans les chaînes azotées).

Les remèdes au vieillissement chimique des matériaux polymères :

- Absorbants UV : benzophénone, benzotriazole, triazine, benzoxazinone,
- Ni-Quenchers : action de désactiver les états excités,
- Antioxydants primaires : phénoliques,
- Antioxydants secondaires : phosphites, phosphonites, thio-compounds,
- Capteurs de radicaux : HALS (Hindered Amine Light Stabilizers) - action chimique et curative.

5.4. Capteurs

Les capteurs peuvent disposer ou non de connectivités réseaux de terrain, voire être intelligents (disposant en plus d'une interface électronique numérique, facilitant l'accès à des fonctionnalités de calibrage et de diagnostic...).

De par leur conception, les dispositifs de mesure sont généralement constitués de 4 parties :

- le piquage (ligne connectée au procédé transmettant le produit à la sonde mesurant la valeur process requise),
- le ou les éléments sensibles à ou aux grandeurs physiques mesurées,
- le transmetteur, conditionneur (conversion de l'information physique en signal électrique),
- le raccordement électrique et éventuellement les réseaux.

1. Le piquage :

Les phénomènes de vieillissement sont liés :

- aux phénomènes de corrosion, de piqûration aux différents chlorures et sulfures, phénomènes souvent amplifiés par la notion de bras mort où les produits stagnent dans la tuyauterie,
- aux phénomènes d'endommagement par fatigue :
 - o contraintes mécaniques et ou thermomécaniques,
 - o vibrations,
 - o cycles de procédé (pression / température).

2. L'élément sensible (sonde, élément primaire...) :

L'élément sensible peut être soumis aux conditions du procédé (pression, température, type de produit,...) et/ou aux conditions environnementales, conditions pouvant entraîner des vieillissements accélérés que la conception ne peut pas toujours éviter. Les causes sont :

- l'usure du composant par les fluides du procédé (abrasifs, corrosifs...),
- la perte de qualité des composants de l'élément :
 - o dégradation ou pollution des huiles dans le temps (transmetteur de pression avec service H₂),
 - o perte d'étanchéité des circuits (exemple : circuit sous vide de séparateurs à membrane),
 - o usure ou détérioration de la membrane jusqu'à la destruction par réaction chimique, chocs répétés en pression ou température, migration des gaz dans les matériaux, fragilisation par H₂S...
- les phénomènes d'endommagement par fatigue :
 - o contraintes mécaniques et ou thermomécaniques,
 - o vibrations,
 - o cycles de procédé (pression / température).

Les phénomènes d'encrassement, de bouchage sont souvent liés à la durée de fonctionnement mais ne sont pas, à proprement parler, des phénomènes liés au vieillissement.

On peut noter que, par nature, certains de ces paramètres sont souvent rendus négligeables par l'isolement ou l'éloignement de l'élément sensible par rapport au procédé (pouvant nécessiter des traitements supplémentaires de l'information) :

- sondes de mesure dans un puits thermométrique,
- membrane de mesure déportée.

L'élément sensible peut être une pièce d'usure qui doit obéir à des règles de remplacement liées à de l'inspection ou des périodes préconisées par le fabricant (exemple : turbine).

L'élément sensible peut être dégradé par des poisons qui réduisent sa durée de vie (exemple : cellule de détecteurs feux et gaz).

3. Le transmetteur (partie traitant la mesure de l'élément sensible et la transmettant) :

De par sa conception, cette partie est souvent dans une enveloppe mécanique qui la protège de nombreux phénomènes.

La partie mécanique de l'enveloppe ne présente pas de phénomène particulier de vieillissement hormis la corrosion ou la perte de propriétés physico-chimiques (cas des matériaux organiques).

La partie traitement de la mesure et transmission, à base d'électronique, subit les mêmes phénomènes de vieillissement que ceux définis en § 5.1.2 du présent guide.

La durée de vie d'une pile étant naturellement limitée, il convient d'y être attentif sur les équipements qui en sont pourvus.

5.5. Transmission de l'information

L'information entre les capteurs et le système de traitement transite par :

- une liaison physique (câble, fibre optique),
- une liaison immatérielle (radio électrique),
- de la connectique.

Concernant le raccordement électrique/optique (liaison avec l'automate de sécurité ou équivalent), les câbles utilisés en instrumentation sont soit posés sur des chemins de câbles en aérien, soit enterrés.

Les phénomènes de vieillissement des câbles d'instrumentation dépendent rarement de leur charge contrairement aux câbles dits de puissance mais surtout :

- de la température ambiante (forte chaleur et grand froid),
- du rayonnement solaire (UV) et des intempéries,
- de leur exposition aux produits chimiques ou pétroliers,
- de la qualité de leur protection mécanique,
- de la corrosion/oxydation pour certains câbles de mesure (température type thermocouple avec câbles acier, ambiance H₂S...).

Le phénomène redouté est la détérioration du câble pouvant provoquer la perturbation ou la perte de la mesure.

En ce qui concerne la connectique :

- de nombreux standards coexistent, leurs qualités et robustesses mécaniques et électriques sont très variables, de même que la qualité de liaison électrique des masses. Les matériaux utilisés pour supporter les contacts peuvent être de tout type et sont donc susceptibles de sensibilités à une grande diversité de stress.
- les liaisons câbles/connecteurs peuvent être définitives (soudure), par piquage (souvent sur câbles spécifiques auto-cicatrisants), par serrage (par vis, ou dispositifs à ressort). Les liaisons très rigides peuvent être mal adaptées pour des composants soumis à des vibrations importantes.

5.6. Systèmes de traitement de l'information

Quand la fonction de traitement de l'information n'est pas assurée par l'homme, les systèmes de traitement de l'information peuvent être électromécaniques, pneumatiques, électriques, électroniques, électroniques programmables (microprocesseur, microcontrôleur, carte/module, ordinateur, automate programmable).

Le traitement des données peut être centralisé, réparti ou distribué. Une même fonction peut ainsi être décomposée en sous-fonctions supportées par des ensembles déportés comportant, à

l'image de l'unité de traitement principale, une unité de traitement de l'information, des modules d'entrées/sorties, des coupleurs réseaux.

Il existe des différences de processus de vieillissement en fonction du type de redondance pouvant être utilisé :

- Chaudes : les composants sont soumis au même historique de stress,
- Tièdes : la partie alimentation des composants est soumise aux mêmes contraintes,
- Froides : les conditions de stockage peuvent influencer sur le vieillissement du composant.

En général, si les conditions d'usage préconisées par le constructeur sont respectées, les composants électroniques numériques défont sans processus de vieillissement apparent. La qualité du processus de maintenance (chapitre 6) ou l'évolution de l'installation de production ainsi que du système de contrôle-commande associé (chapitre 7) peuvent avoir une influence sur le processus de vieillissement.

La qualité des masses (état des contacts et des connexions), de même que les circuits de ventilation (risque d'obstruction ou orifice de pénétration de polluants) sont sujets au vieillissement.

5.7. Eléments terminaux

5.7.1 *Vannes*

Comme tout mécanisme, les vannes peuvent subir une dégradation de leurs performances liée à leur sollicitation ou à une absence prolongée de mouvement.

Les effets du vieillissement peuvent être :

- Le collage, lié à un frottement trop important entre surfaces en contact, qui engendre un effort important pour les manœuvres.
- Le blocage, qui intervient lorsque le collage crée un couple résistant supérieur à celui que peut fournir l'actionneur ou dû à un corps étranger ou à un changement d'état du fluide (polymérisation, gommage, dépôt, colmatage...).
- La détérioration des matériaux (corrosion, fatigue, cavitation, érosion, abrasion, inclusion dans le matériau...) qui peut amener à une diminution des étanchéités.
- La dérive des couples de serrage de la boulonnerie des différents assemblages.

5.7.2 *Avertisseurs feu et gaz et alarmes*

Pour les avertisseurs lumineux ou sonores généralement constitués de composants électroniques, les phénomènes décrits au paragraphe 5.1 s'appliquent.

Pour les technologies non électroniques les éléments les plus sensibles sont les lampes à filament.

5.7.3 *Eléments électriques ou instrumentés intégrés aux machines tournantes (faisant partie de la MMRI)*

Les machines tournantes équipées de capteurs permettant de détecter une anomalie de fonctionnement pouvant mener à l'événement redouté sont visées au § 5.4 du présent guide.

Pour les machines tournantes dont la fonction de sécurité est d'assurer leur service, les composants à considérer sont généralement de type électronique ou électromécanique (relais). Les phénomènes décrits en § 5.2 et 5.3 s'appliquent.

5.8. Sources d'énergie

5.8.1 Généralités

On ne s'attachera dans ce paragraphe qu'au vieillissement des circuits des sécurités à émission. Le vieillissement des équipements électriques utilisés dans la distribution des sources d'énergie électrique est décrit en § 5.2 du présent guide. Le vieillissement des équipements particuliers est développé dans les paragraphes suivants.

5.8.2 Alimentation sans interruption (ASI)

Leur fonction première est de permettre de maintenir le fonctionnement des sécurités à émission dans le cadre des MMRI.

Les mécanismes de vieillissement sont généralement liés aux domaines :

- électronique (cf. § 5.2),
- électrique (cf. § 5.3),
- encrassements potentiels liés à la ventilation importante de l'équipement.

5.8.3 Batteries d'accumulateurs

Des batteries assurent le stockage de l'énergie électrique pour le maintien des fonctions à émission.

La température ambiante et le cyclage (nombre et amplitude des cycles de charge et de décharge) peuvent être des facteurs importants d'accélération du vieillissement.

Ces équipements, de par leur conception, ont une durée de vie qui dépend de leur type :

- Plomb ouvert : entre 3 à 5 ans
- Plomb étanche : 5 à 10 ans. La température ambiante est un facteur de vieillissement (25°C recommandés en général),
- Cadmium-Nickel : 20 à 25 ans,
- Lithium : 1200 cycles complets de charge/décharge.

5.8.4 Groupes électrogènes

Lorsque les groupes électrogènes sont considérés, au même titre que les ASI, comme des sources d'Alimentation Electriques de Sécurité (cas des sécurités nécessitant de l'énergie électrique pour fonctionner), les références ci-dessous s'appliquent.

Les phénomènes de vieillissement des groupes électrogènes sont liés aux domaines suivants :

- Electroniques pour les composants entrant dans les chaines de régulation de vitesse et de tension,
- Electrique pour tous les composants entrant dans les chaines d'automatismes de démarrage, d'arrêt et de sécurité, ainsi que pour ce qui concerne l'alternateur,
- Mécanique pour le moteur à combustion interne et ses accessoires ainsi que pour l'alternateur (paliers),
- Système de réfrigération.

Le respect des prescriptions des textes réglementaires ci-avant permet de s'affranchir au mieux d'une défaillance du groupe électrogène de secours.

Le respect également des cycles de maintenance (la révision du moteur alternatif à combustion interne ne peut qu'avoir un impact positif sur la durée de vie du moteur).

5.8.5 Sources d'énergie par fluides (hydrauliques ou pneumatiques)

Dans le cas de sécurité à émission, l'énergie hydraulique ou pneumatique est stockée dans les capacités dont le vieillissement est maîtrisé au travers du plan d'inspection, ces capacités rentrant dans le cadre des dispositions fixées dans l'arrêté du 15 mars 2000. Dans le cas des capacités non visées par l'arrêté du 15 mars 2000, les dispositions du présent guide leur sont applicables.

6. Bonnes pratiques en matière de maintenance et de tests des MMRI

6.1. Programme et plans de surveillance

L'exploitant doit définir et formaliser sa méthodologie de gestion et de maîtrise du vieillissement des MMRI au travers d'un programme de surveillance⁸ mis en place sur l'ensemble du site (échéances des campagnes de visite, répartition des tâches, etc.). En complément, un plan de surveillance⁸ est défini pour chaque MMRI du site (avec une déclinaison sur chacun des composants de la MMRI (détecteur, logique et actionneur)). Ce plan revêt une grande importance car la majorité de ces équipements ne sont pas amenés à fonctionner en situation normale d'exploitation de l'installation. Il définit la nature et la périodicité des contrôles à effectuer pour s'assurer de leur intégrité et de leur disponibilité dans le temps.

L'exploitant doit également mettre en œuvre les dispositions nécessaires pour vérifier la suffisance et l'efficacité dans le temps du programme de surveillance du site et des plans de surveillance de chaque MMRI.

Le plan surveillance est défini à partir des critères suivants :

- De calculs de fiabilité et/ou du retour d'expérience (utilisateurs, fournisseurs) et/ou des règles et standards de construction pour des niveaux de confiance supérieurs ou égaux à 1,
- D'éventuelles prescriptions réglementaires ou règles assurantielles applicables,
- Des prescriptions et recommandations de maintenance des fournisseurs, a minima celles qui concernent la sécurité,
- Des arrêts périodiques des unités (arrêts programmés ou réglementaires).

Ce plan se décompose sous forme d'opérations de maintenance corrective et préventive et d'opérations de surveillance (contrôles, inspections...). Le plan de maintenance pour la partie maintenance corrective intègre la gestion des pièces de rechange et des procédures de réparation. Le plan de maintenance préventive intègre la gestion de l'obsolescence des matériels.

Les opérations de maintenance et de tests sont encadrées par des procédures. Elles peuvent avoir une portée générale (plan de maintenance et objectifs) ou restreinte à un équipement ou à une situation donnée.

Les procédures générales qualifient le plan de maintenance et prévoient sa déclinaison par dispositif, équipement ou famille d'équipements.

Les procédures doivent décrire les modes opératoires de maintenance, les protections nécessaires, ainsi que les enregistrements à réaliser et les niveaux d'acceptation. La périodicité des différentes actions à mener doit être définie et tracée pour l'ensemble du cycle de vie de la MMRI.

⁸ Tel que défini dans l'arrêté ministériel du 4 octobre 2010.

6.2. By-pass, inhibition des MMRI

Toute inhibition d'alarme ou passage en manuel ou hors service d'une boucle de régulation ou d'un automatisme doit au minimum être tracée et avoir fait l'objet d'une analyse de risques préalable. Cette traçabilité peut être assurée par un support papier (permis de travail, cahier de consignes...) ou par le système quand celui-ci le permet.

Des by-pass peuvent être utilisés afin d'inhiber tout ou partie de la MMRI pendant les opérations de tests, de maintenance ou de défaillance. Ils doivent alors satisfaire les exigences suivantes :

- Une procédure d'utilisation des by-pass doit être définie et doit intégrer les modalités de remise en service des MMRI.
- La procédure précise les modes opératoires, la fonction des personnes, la coordination et la communication de l'information des différents acteurs (qui active, qui garde la liste des matériels by-passés), la pose, la dépose, la remise en fonctionnement, les mesures compensatoires si nécessaires, les éventuelles restrictions sur les activités alentours, la procédure ou le dispositif prévu qui informe de l'état du système. La vérification du bon enlèvement de l'inhibition fait également partie des procédures de vérifications des opérations de maintenance (procédure de réception, procédure de remise en service).
- En plus des procédures, il est recommandé que les exploitants utilisent les moyens suivants pour éviter que l'inhibition reste en place :
 - l'établissement d'une liste des by-pass en possession de l'exploitant stipulant leur état,
 - l'utilisation d'un moyen de signalisation visuelle qui indique qu'une MMRI est inhibée.

6.3. Maintenance

6.3.1 *Maintenance corrective*

Les actions de maintenance corrective sont déclenchées suite à :

- Une panne de l'équipement,
- Un défaut détecté par des tests périodiques,
- Un défaut détecté par des tests automatiques ou des autodiagnostic,
- Une anomalie détectée par suivi visuel (rondes et vérifications périodiques...).

Les interventions de maintenance corrective sur les MMRI sont prioritaires sur celles des équipements de moindre impact sur la mise en sécurité de l'installation.

Pour chaque constituant des MMRI, un temps moyen de rétablissement (ou MTTR) doit être défini et clairement spécifié dans le plan de maintenance pour déterminer les moyens nécessaires à la réparation (stocks de pièces de rechanges, outillages, personnel, contrat de maintenance spécifique, etc.).

Ce temps est un des paramètres permettant de maintenir dans le temps le niveau de confiance ou le niveau SIL d'une MMRI.

Les temps moyens de réparation doivent faire l'objet d'un suivi régulier dans le temps, afin de s'assurer qu'il ne s'écarte pas significativement des temps prévus lors de la conception, notamment lorsque les pièces de rechange ou les compétences se raréfient.

L'objectif est de procéder à la réparation immédiate. Si elle n'est pas possible immédiatement (par exemple dans l'attente de pièces détachées pour des équipements particuliers, dans l'attente de la réparation de la pièce en atelier, dans l'attente des moyens d'accès et/ou de manipulation,...), si nécessaire des mesures compensatoires adaptées sont mises en œuvre.

Dans l'hypothèse où deux MMRI seraient en défaut simultanément, la priorité d'intervention s'établirait selon les critères suivants :

- dans un premier temps, au regard de la criticité des MMRI en fonction de leur contribution à la réduction du niveau de risque,

- dans un second temps, au regard de la difficulté pour mettre en place des mesures compensatoires.

Pour les phases temporaires d'attente, en cas de panne ou de maintenance, les situations dégradées font l'objet de procédures spécifiques. Elles indiquent notamment les processus de validation, les responsabilités et les durées de phases temporaires, les mesures compensatoires si nécessaires et la gestion de la communication interne entre les équipes.

Pour les situations ne faisant pas l'objet d'une procédure formalisée, l'analyse de risque est réalisée au cas par cas.

La redondance sur certains dispositifs critiques permet de faciliter les opérations de maintenance et de tests (by-pass...). Par exemple, pour la maintenance de capteurs redondants, un seul est en service pour remplir la fonction de sécurité, pendant que l'autre fait l'objet des opérations de maintenance dans le délai prédéfini.

6.3.2 Maintenance préventive

La maintenance préventive peut se subdiviser en différents types de maintenance :

- la maintenance systématique à :
 - Périodicité temporelle fixe (intervalle de temps prédéfini),
 - Périodicité d'usage : heures de fonctionnement, nombre d'unités produites, nombre de mouvements effectués...),
- la maintenance conditionnelle réalisée suite à diagnostic sur l'état de dégradation réel de l'équipement,
- la maintenance prévisionnelle réalisée suite à analyse sur l'évolution supposée de l'état de dégradation de l'équipement. Les données peuvent provenir de banques de données (OREDA, EIREDA, base de données interne quand elle existe...) exploitées en fonction des stress présents ou du retour d'expérience sur le type d'équipement concerné.

La maintenance préventive se compose d'opérations de maintenance et de tests, dont il faut déterminer le contenu et la fréquence. Pour définir ces fréquences, les critères ci-après sont utilisés dans la majorité des cas :

- Les cycles d'arrêt périodiques/réglementaires des installations (cas des vannes automatiques...),
- Des exigences techniques (cas des détecteurs de gaz...),
- Durée de vie de l'élément (remplacement de batteries d'accumulateurs, condensateurs chimiques, piles, etc.)...),
- Le retour d'expérience (mise à jour des versions de logiciel d'exploitation corrigeant des défauts majeurs,...), lequel pourra être abordé avec les fournisseurs.
- L'impact de l'environnement (dépoussiérage des équipements, remplacement des filtres...),
- L'historique de fonctionnement (retours de tests non satisfaisants pouvant entraîner soit une augmentation de la fréquence de maintenance préventive, soit une modification de la conception).

Si des fréquences sont imposées par la réglementation, elles constituent en général un minimum requis.

Dans le cas des procédés continus, certaines opérations de maintenance et de tests ne peuvent être réalisées que lorsque l'installation est à l'arrêt. La fréquence de ces opérations est alors fixée par la fréquence des arrêts de production, sous réserve que l'architecture pour répondre au niveau de confiance requis soit déterminée en conséquence.

Cas particulier des groupes électrogènes :

La périodicité des vérifications à réaliser sur les groupes électrogènes est définie à l'article 9 de l'arrêté du 26 février 2003 relatif aux circuits et installations de sécurité, lequel est repris ci-après :

- L'ensemble des installations de sécurité doit faire l'objet d'une maintenance régulière par des agents qualifiés.
- Le bon fonctionnement des installations de sécurité doit être vérifié dans le cadre de la surveillance prescrite à l'article 47 du décret du 14 novembre 1988⁹ et lors des visites périodiques prévues à l'article 53 du même décret.
- Les groupes électrogènes de sécurité doivent faire l'objet d'un entretien régulier et d'essais selon la périodicité minimale suivante :
 - tous les quinze jours, vérification du niveau d'huile, d'eau, de combustible, du dispositif de réchauffage du moteur et de l'état de la source utilisée pour le démarrage (batterie ou air comprimé),
 - tous les mois, en plus des vérifications ci-dessus, essai de démarrage automatique avec une charge nominale de 50% de la puissance du groupe et fonctionnement avec cette charge pendant une durée minimale de 30 minutes.

Les interventions ci-dessus et leurs résultats doivent être consignés dans un document annexé au registre prévu au 3 de l'article 55 du décret du 14 novembre 1988.

Par ailleurs, conformément aux prescriptions de la norme NF E 37312 portant sur les prescriptions particulières concernant les performances et les essais des groupes électrogènes utilisables en tant que source de sécurité pour l'alimentation des installations de sécurité, les dits groupes doivent être pourvus de moyens de surveillance tels que définis à l'article 10 de cette norme.

6.4. Tests de fonctionnement

6.4.1 Périodicité

Les essais périodiques ont pour objet de vérifier que les MMRI continuent de respecter dans le temps leurs exigences fonctionnelles et de performances.

La périodicité de ces tests est un optimum déterminé à partir des critères suivants (si justifié(s) selon le type de MMRI) :

- du retour d'expérience de l'exploitant,
- de l'architecture : en fonction des contraintes de disponibilité et de sécurité, les boucles de sécurité peuvent présenter des structures plus ou moins redondantes,
- des fonctions de diagnostic disponibles (autodiagnostic, comparaison de mesures...),
- de la périodicité des arrêts d'exploitation (notamment lorsque les MMRI sont directement associées aux équipements « process »),
- du calcul de fiabilité (exemple : NF EN 61508 et 61511 ou autres méthodes de calcul / estimation de fiabilité comme le rapport Oméga 10),
- des risques générés par une fréquence de test trop importante. Le risque d'erreur qui pourrait conduire à une situation critique peut être augmenté (par exemple, la possibilité de laisser en place le shunt est augmentée). Par ailleurs, la sollicitation trop fréquente de certains systèmes de sécurité peut être un facteur d'usure (exemple, pour les vannes, l'usure des tiges).

⁹ Décret pris pour l'exécution des dispositions du livre II du code du travail (titre III : Hygiène, sécurité et conditions du travail) en ce qui concerne la protection des travailleurs dans les établissements qui mettent en oeuvre des courants électriques.

Une méthode simplifiée décrite en annexe 10.3 permet de déterminer la période maximale de test des équipements instrumentés utilisés dans les mesures de maîtrise des risques instrumentés (MMRI). Elle peut constituer une méthode alternative aux méthodes fiabilistes issues des normes NF EN 61508 et NF EN 61511 si celles-ci ne sont pas appliquées sur le site.

Le résultat tracé de tests issus d'arrêts non programmés ré initialise l'échéancier des tests.

Nota : dans les chaînes de sécurité comprenant des automates de sécurité, la périodicité est le plus souvent déterminée en fonction de la partie « capteurs » ou de la partie « actionneurs ».

6.4.2 Nature des tests de fonctionnement périodiques

Une procédure doit encadrer les conditions de réalisation des tests et les résultats doivent être enregistrés. Cette procédure doit indiquer la méthode à suivre pour vérifier si la boucle fonctionne correctement. Il est souhaitable que la boucle complète soit testée dans les conditions les plus proches des conditions réelles de fonctionnement sans toutefois générer de risque « process ». Dans ce cas, un test par parties est envisageable (test de la chaîne de détection et test de la chaîne d'action) pour autant que l'on s'assure du recouvrement des parties testées afin de vérifier l'ensemble de la boucle constituant la MMRI.

Les tests périodiques peuvent comprendre :

- Des vérifications fonctionnelles : chaîne complète ou par parties
 - fonctionnement de l'équipement.
 - plages de mesure,
 - seuils de déclenchement,
 - signalisation,
 - des temps de manœuvre...
- Des vérifications visuelles :
 - absence de dégradation (ex : câblage, presse étoupe, calorifuge...),
 - repérage...
- Des vérifications des conditions environnementales (suivant celles retenues à la conception) :
 - Humidité,
 - Vibrations,
 - Température...

Le contenu des tests doit permettre de démontrer le bon fonctionnement de chaque élément de la chaîne instrumentée.

Les tests peuvent être effectués à l'occasion d'un arrêt d'installation ou en fonctionnement lorsque les tests à l'arrêt ne permettent pas de vérifier à eux seuls le niveau de confiance de la MMRI. Dans le cas de nécessité de tests en fonctionnement, la conception de l'installation doit prévoir la possibilité de les réaliser (inhibition, by-pass).

Les autodiagnostic peuvent être une alternative à certaines fonctions de tests manuels s'ils sont suffisamment exhaustifs (exemple : un système de comparaison avec alarme, permanent, entre deux mesures de la même grandeur du procédé, fonction de contrôle utilisée en régulation permanente...). Si l'exploitant a recours à ce type de test, il doit mener au préalable une analyse des éventuels modes communs de défaillance et s'assurer que leur probabilité d'occurrence est compatible avec le niveau de confiance attribué à la MMRI. Pour les MMRI actionnées régulièrement par le procédé, l'autodiagnostic installé est suffisant. Dans le cas de systèmes dormants, en présence de certains types de fluides, la fonction d'autodiagnostic peut générer une défaillance (par exemple, la création d'un amalgame de produit bloquant le mouvement complet d'une vanne).

Une bonne pratique consiste à vérifier, lors d'un déclenchement d'unité, le bon fonctionnement des éléments des MMRI et à tracer les vérifications effectuées, celles-ci pouvant être assimilées à un test dont l'exhaustivité doit être évaluée.

6.4.3 Critères d'acceptabilité des tests périodiques

De manière générale, les critères d'acceptabilité du test doivent être précisés dans la procédure visée au § 6.4.2 du présent guide.

Lorsque le test utilise une mesure physique, le critère d'acceptabilité du test doit tenir compte de l'incertitude de mesure et, le cas échéant, de la dérive envisageable de la grandeur entre deux tests.

6.5. Gestion des pièces de rechange et de l'obsolescence

6.5.1 Gestion des pièces de rechange

La gestion des pièces de rechange doit permettre les opérations de maintenance préventive et corrective dans les temps compatibles avec ceux définis dans le plan de surveillance.

Pour faciliter la gestion et le remplacement des composants des MMRI, les exploitants choisissent d'utiliser, quand c'est possible, des produits standardisés et compatibles (interchangeables même lorsqu'ils proviennent de constructeurs différents).

La gestion des pièces de rechange peut se décliner suivant plusieurs formes, en fonction de la nature des équipements et de la disponibilité des compétences dans l'environnement industriel du site.

Pratiquement :

- Pour le matériel d'instrumentation de terrain banalisé (ex : transmetteur de pression, de température, électrovanne...) : stock chez l'industriel (ou chez son prestataire de maintenance instrumentation attitré) des pièces ou équipements, ceux-ci sont également utilisés pour les fonctions de conduite de procédé, ce qui assure un renouvellement permanent des stocks,
- Pour les systèmes de traitement, la politique est élaborée en commun avec le fournisseur :
 - Pièces de première urgence disponibles sur site,
 - Pièces de seconde urgence disponibles chez le fournisseur ou mutualisées avec d'autres exploitants selon convention.

6.5.2 Durée de vie des composants d'une MMRI

La plupart des équipements d'instrumentation n'ont pas de durée de vie intrinsèque. Néanmoins, en fonction de leurs conditions d'utilisation, les composants d'une MMRI sont soumis au vieillissement à des degrés divers (exemple : corrosion plus forte sur les sites proches de la mer, produits agressifs...).

A noter qu'en instrumentation, il n'est pas rare de trouver de « vieux » équipements qui remplissent parfaitement leur fonction (exemples : transmetteurs, cartes électroniques), quand ils sont installés dans des conditions n'accéléralant pas le vieillissement.

La fréquence des remplacements dépend donc du contexte, notamment de l'environnement. Les principales sources qui déterminent la fin de vie d'un dispositif ou équipement, et donc son remplacement, sont les informations issues du retour d'expérience. Les informations des constructeurs sont également prises en compte.

Les motifs de changements indiquant qu'il entre peut-être dans sa période de vieillissement ou de fin de vie, sont principalement liés à l'augmentation inhabituelle du nombre des défaillances d'un dispositif ou équipement :

- taux de panne plus important que le taux de défaillances aléatoires classique, détecté lors de la maintenance préventive ou corrective,
- dérive du temps de réponse.

6.5.3 Obsolescence des composants des MMRI

L'obsolescence peut concerner un composant de la chaîne de sécurité (un capteur, un convertisseur, etc.) mais n'est généralement pas problématique pour les composants courants (interchangeables ou banalisés).

Pour les systèmes de traitement l'obsolescence doit être anticipée car ils constituent un mode commun et un changement majeur qui ne peut être effectué que lors des arrêts programmés des installations.

Face à ces contraintes l'exploitant a les alternatives suivantes :

- Renouveler ses équipements, de façon à avoir du matériel supporté par le fournisseur.
- S'équiper (en interne ou via une sous-traitance adéquate) pour prolonger le bon fonctionnement du système. Il doit être en mesure de :
 - Réparer / remplacer les cartes,
 - Prévoir la consommation de composants / cartes et les stocks correspondants,
 - Anticiper les arrêts de production de composants,
 - S'assurer de la disponibilité des compétences sur ces anciennes technologies.

La gestion de l'obsolescence est de la responsabilité de l'exploitant qui doit s'organiser en conséquence.

Lorsque l'obsolescence d'un élément de la chaîne de sécurité (capteur, convertisseur, etc.) conduit à son remplacement non à l'identique, cette modification sera gérée dans le cadre du SGS (système de gestion de la sécurité, volet « gestion du changement ») pour les exploitants d'établissements Seveso seuil haut ou dans le cadre d'un système équivalent pour les exploitants d'établissements Seveso seuil bas.

7. Exploitation des MMRI

7.1. Objectif

Les objectifs des recommandations de ce chapitre sont :

- d'exploiter les MMRI de sorte que les fonctions de sécurité prévues à la conception soient maintenues,
- d'assurer que le niveau de confiance requis de chaque MMRI soit maintenu pendant l'exploitation.

7.2. Organisation de l'exploitation des MMRI

L'exploitation des MMRI s'inscrit pleinement dans le Système de Gestion de la Sécurité (SGS) ou dans le cadre d'un système équivalent. La description de l'organisation doit couvrir les points suivants quel que soit le régime d'exploitation, normal ou transitoire :

- les responsabilités (personnes, les services et les organisations responsables de ces activités),

- les moyens (procédures, les mesures et les techniques à utiliser pour l'exploitation),
- la planification.

7.3. Procédures et documents d'exploitation des MMRI

Les procédures et documents d'exploitation des MMRI comprennent :

- Le plan de maintenance incluant les critères à contrôler et à satisfaire ainsi que les analyses préalables avant intervention sur une MMRI justifiant l'indisponibilité et les mesures compensatoires mises en œuvre (cf. chapitre 6),
- Les audits (suivant SGS ou système équivalent),
- La fiche de vie et les enregistrements associés (cf. chapitre 9).

7.4. Analyse des événements

Ceci doit inclure la surveillance des points suivants :

- les analyses suite à la sollicitation d'une MMRI ;
- les défaillances des équipements faisant partie des MMRI, établies pendant les essais périodiques ou la sollicitation réelle ;
- la cause des déclenchements intempestifs.

Les divergences entre le comportement attendu et le comportement réel des MMRI doivent être analysées et, en cas de besoin, des modifications doivent être faites, de telle manière que la sécurité prescrite soit maintenue.

L'analyse de ces événements peut conduire soit à des changements de fréquence de maintenance préventive ou de test soit à des modifications de conception de l'architecture de la MMRI et des MMRI équivalentes installées dans l'établissement.

La traçabilité sera assurée à partir des supports disponibles chez l'industriel (papier, base de données...).

7.5. Modification des MMRI

Les modifications des installations (modification des modes de fonctionnement, modernisation des installations ou équipements qui ne s'installent plus de la même manière ou aux mêmes endroits) peuvent modifier sensiblement les performances d'une MMRI.

La procédure de modification d'une MMRI suit celle décrite dans le système de gestion de la sécurité (SGS) pour les exploitants d'établissements Seveso seuil haut ou dans le cadre d'un système équivalent pour les exploitants d'établissements Seveso seuil bas.

La gestion des modifications des MMRI et de leurs environnements doit permettre d'assurer que les niveaux de confiance des MMRI prescrites sont maintenus en dépit de toutes les modifications faites à ces dernières. De manière générale, toute modification d'une MMRI ou susceptible d'affecter une MMRI doit faire l'objet d'une analyse d'impact dont l'objectif est de vérifier que cette modification ne provoque pas de régression du point de vue de la maîtrise des risques.

Cette analyse d'impact est tracée dans un document de modification, qui comprend également :

- une description de la modification ou du changement,
- la raison du changement,
- les essais utilisés pour vérifier que la modification a été correctement mise en œuvre et que la MMRI fonctionne comme cela est prescrit.

La fiche de vie et, le cas échéant, la documentation d'exploitation et de maintenance doivent être mises à jour en fonction des modifications apportées.

8. Gestion des compétences

8.1. Objectif

De manière générale, l'exploitant d'un établissement Seveso doit identifier les besoins en matière de formation des personnels associés à la prévention des accidents majeurs. L'organisation de la formation ainsi que la définition et l'adéquation du contenu de cette formation doivent aussi être explicitées.

Dans le cadre de la problématique liée au vieillissement des MMRI, ceci implique que soient identifiées des actions de formation, qualification et de recyclage pertinentes et adaptées aux matériels utilisés, afin de maintenir le niveau de compétence des intervenants. Il apparaît également nécessaire de s'assurer que ces principes soient intégrés par les entreprises sous-traitantes dont les activités (maintenance, contrôles périodiques...) sont en lien direct avec la sécurité des procédés industriels.

Concrètement, ceci se traduit par la mise en place d'un système de gestion des compétences impliquant des procédures et des contrôles pour identifier les compétences nécessaires, les obtenir et assurer leur pérennité.

Ceci a pour corollaire de s'assurer que seules les personnes possédant la compétence requise pour une activité de conduite, de test ou de maintenance d'une MMRI peuvent être affectées à cette activité ; l'appréciation de la compétence de ces personnes étant notamment fondée sur leur formation et leur expérience.

Pour obtenir la garantie que les intervenants ont une compétence adaptée aux exigences des activités qu'ils réalisent, l'exploitant est conduit à mettre en œuvre différents processus afin :

- 1) D'identifier les activités critiques liées à la sécurité des installations et définir les compétences requises pour leur réalisation,
- 2) D'évaluer les compétences existantes et manquantes dans la population des intervenants,
- 3) De faire acquérir les compétences nouvelles requises par le biais d'un dispositif de formation par compagnonnage ou/et de formation interne ou externe (pouvant se traduire par des habilitations),
- 4) De maintenir les compétences par le biais d'une pratique régulière ou, si nécessaire, de formation (prise en compte du retour d'expérience et des évolutions technologiques des matériels),
- 5) De s'assurer de l'adéquation entre compétences disponibles et requises (fiches de postes), notamment par des dispositions visant à anticiper les mouvements de personnel.

En outre, si l'exploitant a recours à la sous-traitance, il doit aussi s'assurer de la qualité des prestations réalisées par ces entreprises.

Pour les établissements Seveso seuil haut, l'existence d'un SGS implique déjà la mise en œuvre de ces recommandations. Pour les exploitants d'établissements Seveso seuil bas, ces recommandations doivent être formalisées au travers d'un système équivalent.

La mise en place d'un carnet individuel de formation constitue une bonne pratique pour suivre et contrôler l'adéquation des compétences mise en œuvre.

8.2. Activités liées à la sécurité des installations et définition des compétences requises

Les exigences liées à la sécurité (maintenance des matériels des MMRI et leurs tests périodiques, conduite des MMRI...) doivent être identifiées et des exigences relatives à leur exécution définies par l'exploitant. Le domaine des compétences requises doit couvrir les exigences liées à la sécurité définies ci-dessus. La définition des compétences requises couvre les connaissances

théoriques, l'expérience mais aussi les savoir-faire, pour l'exploitation normale comme pour les situations dégradées.

L'ensemble de ces éléments pourra alimenter le référentiel métier de l'intervenant ou fiche de poste.

8.3. Évaluation des compétences

L'évaluation des compétences peut se faire au travers :

- D'entretiens périodiques orientés vers la formation,
- De contrôles des activités,
- D'observations in situ effectuées par le responsable,
- De demandes de l'agent lui-même.

Les encadrants doivent participer au processus d'habilitation des agents dont ils sont responsables. Ces moyens permettent d'analyser les besoins de compétences et d'établir les plans de formation (stage, compagnonnage, immersion...).

Il convient d'avoir une politique de gestion des compétences simple, qui anticipe les besoins, qui est régulièrement actualisée et qui est opérationnelle.

Le personnel employé temporairement doit également être pris en compte afin de s'assurer qu'il dispose des compétences requises.

8.4. Acquisition et maintien des compétences requises

8.4.1 Formation

8.4.1.1 Des opérateurs

Les opérateurs doivent être formés à la fonction et à l'exploitation des MMRI dans leur domaine de responsabilité. Cette formation doit assurer *a minima* :

- la compréhension du fonctionnement des MMRI (les points déclenchement et l'action résultante qui est prise par la MMRI) ;
- la sensibilisation au risque sur lequel doit agir la MMRI et aux dangers susceptibles d'être engendrés par le phénomène dangereux résiduel ;
- l'explication du fonctionnement de tous les « shunts » (ou by-pass) et dans quelles circonstances ces shunts sont à utiliser ;
- l'explication du fonctionnement de tous les shunts manuel, des activités de démarrage manuel et dans quelles circonstances ces shunts manuels sont à activer ;
- l'explication de la conduite à tenir lors de l'activation d'une alarme de diagnostic quelconque (par exemple, quelle mesure doit être prise lorsqu'une alarme d'une MMRI est activée, indiquant qu'il y a un problème avec ce dernier).

8.4.1.2 Des agents de maintenance

La formation doit comprendre la connaissance des sources d'information utiles pour réaliser les diagnostics et la maintenance (accès à l'historique des pannes, accès à la fiche de vie, plans et schémas...).

D'un point de vue pratique :

- en interne, les objectifs et les moyens nécessaires sont déterminés par l'exploitant,
- en cas de sous-traitance, conformément aux exigences du code du travail, un cahier des charges fixe les objectifs à atteindre et les modalités de contrôle (cf. § 8.5).

8.4.2 L'évaluation des modules de formation

Des moyens doivent être prévus par l'exploitant pour évaluer le contenu de chaque module de formation et pour l'améliorer si nécessaire.

Ceci peut se traduire par :

- L'existence de fiches d'appréciation de stage ;
- L'existence de sessions-tests périodiques pour les modules existants et utilisés, ou préliminaires pour les nouveaux modules ;
- L'existence d'un processus d'évolution, de modification ou de remise en cause des modules de formation avec indication des motifs associés.

8.4.3 L'organisation de la formation par compagnonnage

Le compagnonnage est un mode d'apprentissage d'un métier basé sur une intégration d'une personne arrivant dans une équipe constituée dont il prend part progressivement à l'activité sous le contrôle d'un membre expérimenté. Il permet une appropriation progressive de l'activité. Il permet également l'acquisition d'éléments de compétences fortement liés au contexte professionnel et à l'expérience.

Ce mode de formation peut s'avérer particulièrement judicieux :

- dans le cas où les matériels utilisés sont vieillissants et, de fait, dans le cas où les nouveaux arrivants n'ont pu se familiariser avec le matériel pendant leur cursus de formation ou d'études (y compris les expériences antérieures),
- pour favoriser la transmission du savoir lors du remplacement d'un agent.

Il est nécessaire de formaliser l'organisation et la traçabilité de cette formation.

De façon plus générale, des notes d'organisation relatives à la formation peuvent être formalisées. Ces notes peuvent également prendre en compte la notion d'habilitation afin de correctement définir les programmes de formation en fonction des attendus.

La définition d'un plan de formation annuel est une obligation réglementaire pour chaque entreprise et doit être discutée avec les représentants du personnel.

8.4.4 Les formations de remise à niveau

Dans le cas où la pratique régulière ne permet pas à elle seule le maintien de la compétence, alors, l'un des buts de la formation est d'assurer un minimum de pratique.

Il peut s'avérer nécessaire de procéder à une remise à niveau périodique des personnels afin de rappeler les éléments de connaissance qui ont pu être oubliés du fait de leur non-utilisation, de compléter la formation initiale sur des points particuliers dont le retour d'expérience (incidents/accidents) a montré l'importance, de tenir compte de l'impact des évolutions d'installations sur les consignes et modes opératoires et de tenir compte de l'évolution des techniques employées.

Il pourra être mis en œuvre des techniques de formation utilisant, par exemple, des chantiers école permettant de simuler les pratiques de terrain.

8.5. Le contrôle des compétences des prestataires extérieurs à l'entreprise

Le recours à la sous-traitance pour des tâches impactant directement la sécurité des installations nécessite d'évaluer les moyens mis en œuvre ainsi que leur exécution.

Ceci peut se traduire notamment par la mise en place de notes d'organisation régissant l'intervention de prestataires extérieurs, de clauses spécifiques dans les cahiers des charges et les contrats, d'actions de surveillance exercées sur les prestataires et de vérification de leurs habilitations avant intervention.

9. Etat zéro et fiche de vie d'une MMRI

Un recensement précis des MMRI visées par le plan de modernisation doit être réalisé au plus tard le 31 décembre 2013 et une fiche de vie doit être établie pour chacune d'entre elles¹⁰ afin de synthétiser les données nécessaires à leur suivi.

Suivant les outils à disposition, la fiche de vie peut :

- être complètement traitée dans une seule base de données (éventuellement papier...)
- faire référence à des informations réparties dans différents systèmes (ex : GMAO, gestion électronique de documents, outils de gestion...)

Doivent être ainsi capitalisées les principales informations concernant les caractéristiques des MMRI :

- le lien avec le(s) scénario(s) justifiant la MMRI,
- le niveau de confiance associé,
- les standards de conception et/ou de construction utilisés (exemple : référence à des réglementations, des normes ou des standards internes à l'entreprise),
- les conditions environnementales, telles quelles sont visées au § 4.2.6.3 du présent guide,
- les fonctions de sécurité qu'elles assurent (exemple : description succincte de la fonction de sécurité assurée ou référence au logigramme de sécurité ou matrice causes/effets),
- le temps de réponse maximum si requis,
- la position de repli en cas de défaillance détectée (alarme signifiant la défaillance ou déclenchement automatique),
- la fréquence, la nature (unité en marche ou à l'arrêt) et les procédures de tests,
- le suivi réalisé (diagnostics, essais périodiques, inspections, mesures et résultats enregistrés, maintenances préventive et corrective) durant la vie de l'équipement,
- les réparations ou modifications éventuelles durant la vie de l'équipement et leur justification,
- les analyses des résultats de test, quand ceux-ci révèlent un comportement potentiel non sûr, durant la vie de l'équipement.

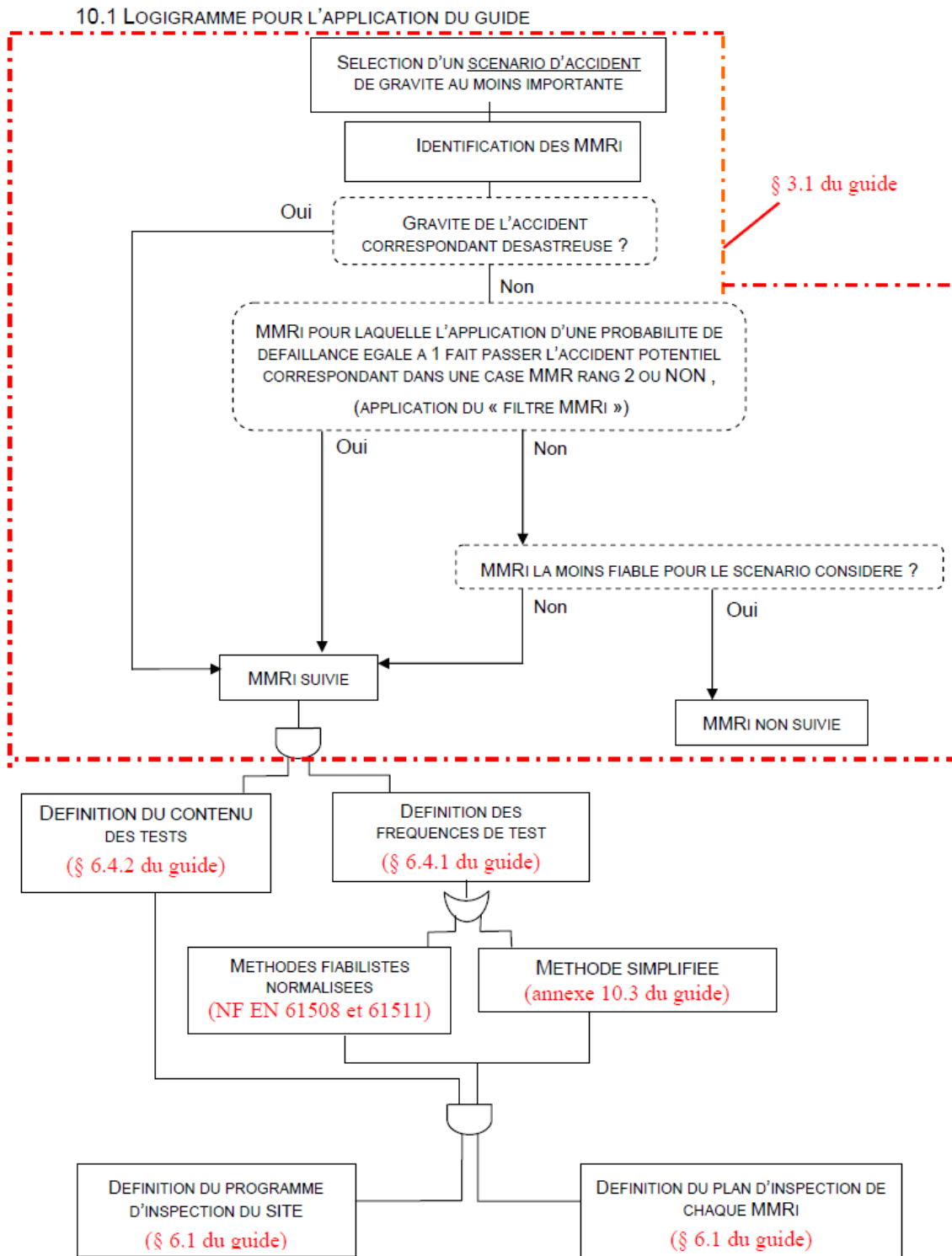
Pour ces trois derniers points, les informations annexées à la fiche de vie comprennent autant que faire se peut les données antérieures à la création de cette fiche (état initial).

La fiche de vie a ensuite vocation à être mise à jour au fil du temps, notamment après chaque réparation ou modification, et à perdurer tant que la MMRI est en service dans l'installation. La date de mise au rebut et la justification devront être formalisées.

Nota : les MMRI pour lesquelles il apparaît qu'aucun contrôle de bon fonctionnement n'a été réalisé depuis leur mise en service doivent faire l'objet d'un contrôle détaillé dans l'année qui suit l'état initial. En cas de dysfonctionnement avéré, elles doivent être réparées ou remplacées dans le délai tel que défini dans le plan de maintenance. Dans cette attente, des mesures compensatoires doivent être mises en œuvre pour garantir le niveau de sécurité requis de l'installation.

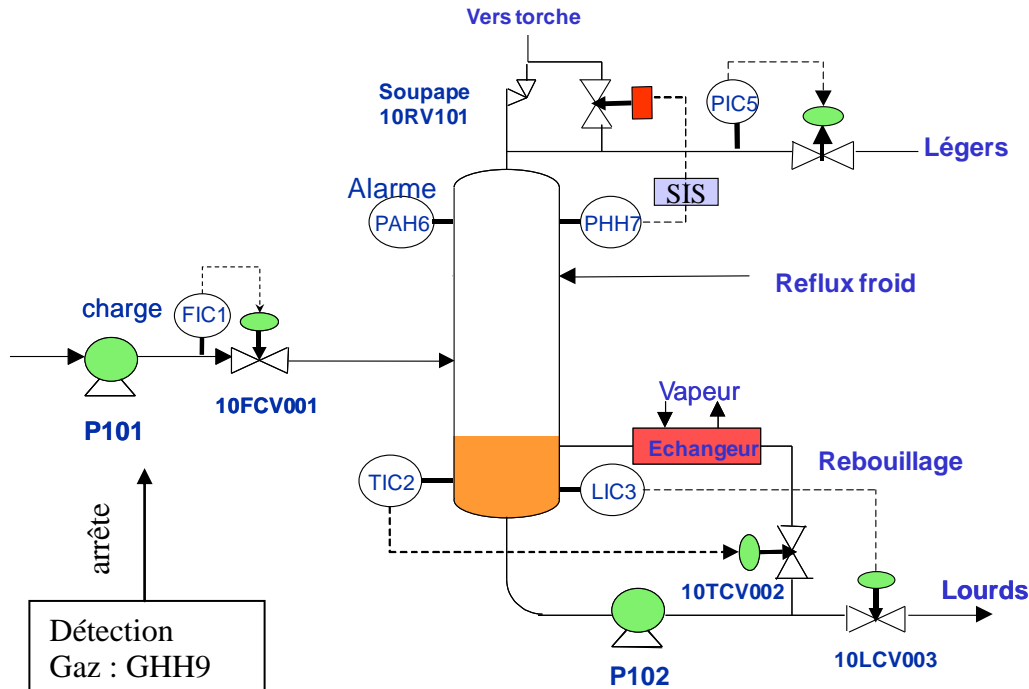
¹⁰ La fiche de vie d'une MMRI peut se matérialiser par un document composé de fiches spécifiques à chaque élément de la chaîne instrumentée, si nécessaire.

10. Annexes



10.2 Exemple illustratif

Schéma simplifié de l'installation

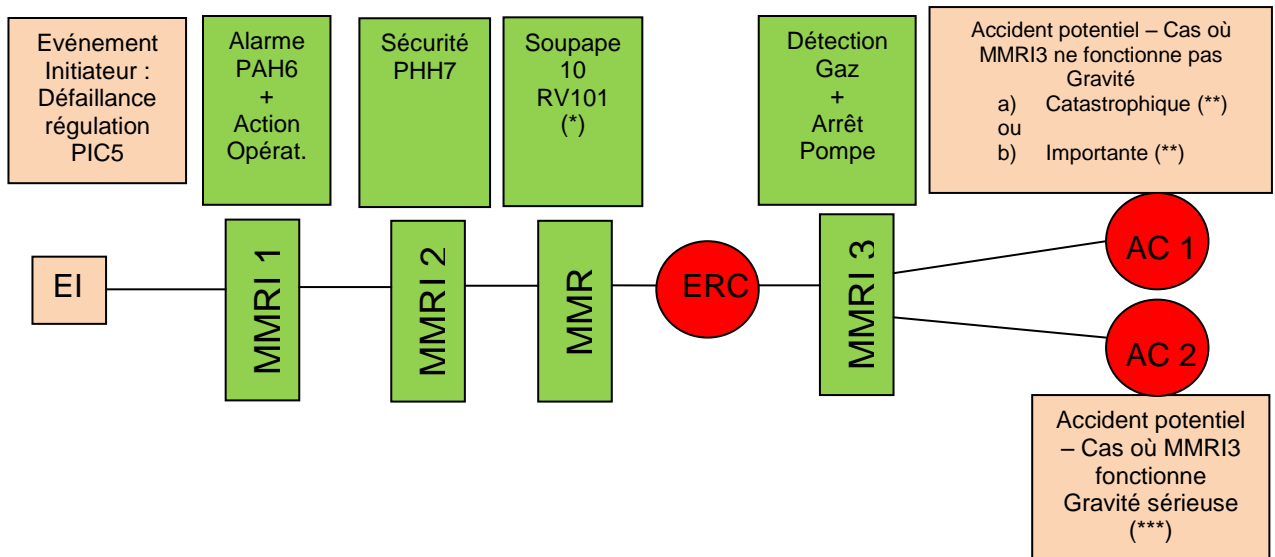


Dans cet exemple, il s'agit d'une colonne de séparation de GPL (propane/butane) avec hypothèse de défaillance de la régulation d'évacuation des légers (PIC5) et montée en pression dans la colonne jusqu'à une perte de confinement.

Remarque importante : cette estimation ne peut être appliquée de manière systématique / générique à des scénarios semblables.

MMR disponibles :

- Pression haute : Alarme PAH6 avec action opérateur consistant en un certain nombre de mesures en tant que de besoin :
 - Prise en manuel de la PIC5 (pour augmenter l'ouverture).
 - Prise en contrôle manuel du débit de rebouillage de fond de tour (par la 10TCV002) pour réduire les apports thermiques dans la tour, donc baisser les volumes vaporisés, puis du débit d'alimentation liquide (par la 10FCV 0001).
- Pression très haute : Fonction de sécurité Instrumentée PHH7,
- Pression très très haute : Soupape 10RV101,
- Arrêt automatique de la pompe P101 sur détection gaz.

Scénarios d'accident identifiés :

(*) La soupape est mentionnée pour illustrer le fait qu'il existe d'autres MMR qui interviennent dans les calculs, même si elles ne sont pas des MMRI

(**) Cas de deux sites similaires, ne se distinguant que par leur environnement plus ou moins dense, en termes de population potentiellement impactée par l'accident considéré. Dans le premier cas, la densité de population est importante et, de ce fait, la gravité est considérée comme étant catastrophique [a) ci-après]. Dans l'autre cas, la densité de population est faible, la gravité étant alors considérée comme importante [b) ci-après].

(***) Pour la suite du traitement de l'exemple, l'accident potentiel AC2 n'est pas examiné : sa gravité étant « sérieuse », il ne répond pas au critère de sélection mentionné au §3.1

On suppose dans le schéma ci-dessus que les capteurs, les actionneurs et le système de traitement étant différents, ces MMR sont indépendantes de l'événement initiateur et sont indépendantes entre elles, sous réserve que les systèmes de traitement PIC5 et PAH6 soient indépendants et que l'action opérateur soit indépendante des autres actions.

Si la fréquence de l'événement initiateur est d'une fois tous les ans et en considérant les probabilités de défaillance à la sollicitation (PFD) des MMR données à titre d'exemple :

- PFD alarme PAH6 et action opérateur : 10^{-1}
- PFD SIF (Fonction Instrumentée de sécurité) PHH07 : 5.10^{-2}
- PFD soupape 10RV101 : 10^{-2}
- PFD détection gaz et arrêt pompe : 5.10^{-2}

La fréquence du phénomène dangereux correspondant à l'accident potentiel le plus grave (AC1 : non fonctionnement de la protection par détection Gaz) serait égale à :

Fréquence événement initiateur x PFD des MMR :
soit $(1 \text{ fois tous les ans}) \times (10^{-1}) \times (5.10^{-2}) \times (10^{-2}) \times (5.10^{-2}) = 2,5.10^{-6}$ par an (Probabilité E car $\leq 10^{-5}$ /an) soit 1 fois par 400 000 ans.

a) Exemple dans le cas où la gravité est catastrophique :

Gravité des conséquences sur les personnes exposées au risque (note 1)	PROBABILITÉ (sens croissant de E vers A) [note 1]				
	E	D	C	B	A
Désastreux	NON partiel (sites nouveaux : note 2) / MMR rang 2 (sites existants : note 3)	NON rang 1	NON rang 2	NON rang 3	NON rang 4
Catastrophique	MMR rang 1	MMR rang 2 (note 3)	NON rang 1	NON rang 2	NON rang 3
Important	MMR rang 1	MMR rang 1	MMR rang 2 (note 3)	NON rang 1	NON rang 2
Sérieux			MMR rang 1	MMR rang 2	NON rang 1
Modéré					MMR rang 1

Avec toutes les MMR	Sans Soupape	Sans PAH6	Sans GHH9	Sans PHH7
---------------------	--------------	-----------	-----------	-----------

Pour chaque MMRI prise seule :

- Si on enlève uniquement le PAH6, on passe en MMR Rang 2 donc le PAH 6 est une MMRI qui doit être suivie dans le cadre du plan de modernisation.
- Si on enlève uniquement le PHH7, on passe en MMR Rang 2 donc le PHH 7 est une MMRI qui doit être suivie dans le cadre du plan de modernisation.
- Si on enlève uniquement le GHH9, on passe en MMR Rang 2 donc le GHH9 est une MMRI qui doit être suivie dans le cadre du plan de modernisation.

b) Exemple dans le cas où la gravité est importante :

Gravité des conséquences sur les personnes exposées au risque (note 1)	PROBABILITÉ (sens croissant de E vers A) [note 1]				
	E	D	C	B	A
Désastreux	NON partiel (sites nouveaux : note 2) / MMR rang 2 (sites existants : note 3)	NON rang 1	NON rang 2	NON rang 3	NON rang 4
Catastrophique	MMR rang 1	MMR rang 2 (note 3)	NON rang 1	NON rang 2	NON rang 3
Important	MMR rang 1	MMR rang 1	MMR rang 2 (note 3)	NON rang 1	NON rang 2
Sérieux			MMR rang 1	MMR rang 2	NON rang 1
Modéré					MMR rang 1

Avec toutes les MMR	Sans Soupape	Sans PAH6	Sans GHH9	Sans PHH7
---------------------	--------------	-----------	-----------	-----------

Pour chaque MMRI prise seule :

- Si on enlève uniquement le PAH6, on passe en MMR Rang 1 donc le PAH 6 n'est pas une MMRI qui devrait être suivie dans le cadre du plan de modernisation
- Si on enlève uniquement le PHH7, on passe en MMR Rang 1 donc le PSHH 7 n'est pas une MMRI qui devrait être suivie dans le cadre du plan de modernisation
- Si on enlève uniquement le GHH9, on passe en MMR Rang 1 donc le GHH9 n'est pas une MMRI qui devrait être suivie dans le cadre du plan de modernisation

En revanche, d'après la règle du § 3.1.1 du présent guide " Dans le cas où cette méthode conduirait à l'exclusion du plan de modernisation plusieurs MMRI pour un même scénario d'accident, l'exploitant ne pourra exclure qu'une de ces MMRI et exclura la moins fiable" : le PHH7 (SIS) et le GHH9 sont donc retenues comme MMRI à suivre dans le cadre du plan de modernisation et le PAH 6 n'est pas une MMRI à suivre dans le cadre du plan de modernisation.

10.3 Méthode alternative à la norme de détermination de la période de test des MMRI

10.3.1 Documentation de la feuille de calcul objet du 10.3.2

10.3.1.1 Introduction

Cette méthode semi quantitative permet de déterminer la période maximale de test des équipements instrumentés utilisés dans les mesures de maîtrise des risques instrumentés (MMRI). Elle est basée sur des critères simples, facilement identifiables, éprouvés par l'expérience et par la pratique. Elle peut constituer une méthode alternative aux méthodes fiabilistes issues des normes NF EN 61511 et 61508 si celles-ci ne sont pas appliquées sur le site. Elle s'adresse à des architectures simples (une détection, une action).

10.3.1.2 Vocabulaire

Le vocabulaire employé est défini dans le guide MMRI, cependant, en rappel :

- NC : niveau de confiance tel que défini dans la circulaire du 10 mai 2010.
- SIL : Safety Integrity Level au sens des normes NF EN 61508 et NF EN 61511.
- TOR : équipement à fonctionnement Tout ou rien. Pour une vanne, cela correspond à une vanne au fonctionnement ouvert ou fermé. Pour un capteur, cela correspond à un appareil donnant une information logique 1 ou 0.
- Vote 1oo2, 2oo3 : cela correspond à une fonction réalisant un vote de 1 parmi 2 pour le 1oo2 ou de 2 parmi 3 pour le 2oo3.
- DB&B : dispositif d'isolement de 3 vannes réalisant un double vannage et un évent au milieu, souvent utilisé pour les circuits de gaz des fours pour garantir l'étanchéité.

10.3.1.3 Explication sur la méthode développée dans le fichier Excel

Eléments d'une MMRI et découpage des fréquences de test

La méthode permet de différencier les périodes de test de chacun des éléments d'une MMRI (capteur, système de traitement et actionneur) en prenant en compte leurs spécificités. Cette pratique n'est acceptable bien sûr que si la somme des tests partiels permet de couvrir l'ensemble de la fonction de sécurité.

Il est convenu que, pour permettre cette différenciation des périodes de tests, le test d'un élément est global et intègre :

- le test de fonctionnement de l'équipement,
- le test de sa liaison et sa connexion dans le système de traitement.

Le test du système de traitement peut alors être réalisé de façon indépendante et permettre de garantir ainsi l'intégrité de la fonction réalisée.

Si le test est réalisé globalement sur la chaîne instrumentée, la période à retenir entre deux tests est la plus courte.

Le niveau de confiance à atteindre sera déterminé par le niveau de confiance cible à atteindre par la MMRI tel que déclaré dans l'étude de dangers (choix exclusif parmi NC1 - NC2 - NC3).

Cas des capteurs et actionneurs

Pour les capteurs et actionneurs, l'observation d'un critère se traduit par un coefficient positif ou négatif. Ce coefficient est exprimé en années. La somme de ces coefficients donne la période de test exprimée en années. Les coefficients sont fixés par l'aspect positif ou négatif sur la fréquence de test en comparaison avec une pratique de base éprouvée ou bien maîtrisée.

En conséquence :

- Coefficient = 0 : pratique de base
- Coefficient < 0 : condition défavorable pour la période de test
- Coefficient > 0 : condition favorable pour la période de test

Les critères ne prennent pas en compte la technologie employée celle-ci étant considérée comme adéquat et en accord avec le service et la fonction requis.

Les critères sont uniquement définis sur la base de leur caractère d'influence sur la période de test et sont donc génériques.

a. Test des capteurs

On entend par ce test, le test du capteur jusqu'au système de traitement, ce qui inclut tout le câblage jusqu'au système de traitement et les éventuels modules intermédiaires.

Les critères suivants doivent être analysés :

	Coefficients
TOR à émission	-5
TOR à émission avec surveillance de ligne	-4
TOR à manque	-3
Mesure continue retransmise (analogique)	0
Analogique avec comparaison	4
Configuration verrouillée et (Capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié (REX))	5
Redondance en mode sécurité positive	4
Redondance en mode à émission	1
Non redondance en NC3	-20
Traçage indispensable ou flushing	-2
Bouchage / Produit colmatant	-3

Service sans difficulté	1
Autres cas difficiles	-1
Exigence NC1	-1
Exigence NC2	-3
Exigence NC3	-6
Inspection visuelle 1 à 2 fois par an ou nettoyage des lignes	2
Inspection des tendances dans le cas des comparaisons	1

Type d'équipement :

Choix exclusif parmi :

- *TOR à émission* : capteur à 2 états, l'état de danger est signalé par un signal haut, l'état normal est le signal 0. Par exemple pressostat, thermostat câblés à émission.
- *TOR à émission avec surveillance de ligne* : idem ci-dessus avec un dispositif permettant de signaler une défaillance (perte de continuité électrique) du câblage entre capteur et système de traitement.
- *TOR à manque* : capteur à 2 états, l'état de danger est signalé par le signal 0, l'état normal est le signal haut (par exemple, pressostat, thermostat câblés à manque).
- *Mesure continue retransmise* : capteur continu dont le signal varie proportionnellement à la mesure et dont le signal est retransmis à l'opérateur (mesure dite vivante par opposition à la technologie TOR).

Diagnostic :

Choix multiples possibles parmi :

- *Analogique avec comparaison* : capteur analogique dont la mesure est comparée en continu avec un autre capteur (ou une estimation de la mesure à partir d'autres capteurs), en cas d'écart une alarme est automatiquement générée vers l'opérateur et une procédure de maintenance et d'opération permet d'analyser et de corriger le problème le plus rapidement possible.
- *Configuration verrouillée et (Capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié (REX))* :
 - *Configuration verrouillée* : pour les capteurs dits intelligents, la possibilité de modification du réglage est verrouillée par switch, mot de passe, etc.
 - *Capabilité SIL de l'appareil en SIL2* : appareil conçu pour l'utilisation en sécurité et pouvant faire partie tout seul d'une chaîne de sécurité SIL 2. Cet appareil est donc, de fait, doté d'autodiagnostic. Cette capabilité est garantie par le fabricant de l'appareil.

Ou éprouvé par l'usage sur le procédé spécifié (REX) : cet appareil est utilisé sur des procédés similaires avec un retour d'expérience positif (*cumul de 100 000 heures d'utilisation équivalent à 10 équipements sur un an ou 1 équipement pendant 10 ans*) géré par la société.

Architecture :

La redondance ici signifie qu'en cas d'un capteur défaillant, la fonction est assurée (par exemple vote 1oo2, 2oo3) par un ou plusieurs autres capteurs.

La redondance peut être homogène (2 capteurs de pression) ou hétérogène (par exemple un capteur de pression et un capteur de température, si l'un et l'autre représentent bien le même phénomène).

Choix multiples possibles parmi (A et B exclusifs) :

- *A : Redondance en mode sécurité positive*: redondance pour capteur à TOR à manque ou analogique,
- *B : Redondance en mode à émission* : pour capteurs TOR à émission,
- *C : Non redondance en NC3* : un coefficient négatif très élevé affecté à cette ligne permet d'interdire une architecture non redondante pour les NC3.

Conditions d'utilisation / Service :

Choix exclusif parmi :

- *A : Traçage indispensable ou injection dans les lignes d'impulsion* : cela concerne des mesures qui ont besoin d'autres dispositions actives pour fonctionner (air, vapeur, électricité, produits sous pression...) :
 - *Traçage indispensable* : par exemple, mesure de débit ou de pression sur eau/vapeur pour laquelle le traçage évite le gel des prises d'impulsion.
 - *Injection dans les lignes d'impulsion* : par exemple, pour les produits très visqueux colmatant, un solvant est injecté en permanence dans les lignes d'impulsion pour éviter le figeage.
- *B : Bouchage / Produit colmatant*
- *C : Service sans difficulté* : par exemple, produit pur, propre, qui ne gèle pas et ne fige pas
- *D : Autres cas difficiles*, différents des cas A et B et estimés moins difficiles que le cas colmatant

Suivi spécifique :

Choix multiples possibles parmi :

- *Inspection visuelle 1 à 2 fois par an ou nettoyage des lignes* : par exemple, l'inspection visuelle des traçages compense partiellement la faiblesse apportée par les traçages, dans le cas de produits colmatants le nettoyage de ligne est une mesure de maintenance préventive qui compense partiellement les conditions d'utilisation. Cette inspection visuelle consiste à vérifier l'état apparent de l'appareil et de son raccordement au procédé (ex : état du calorifuge, fonctionnement du traçage, présence de fuites, état des raccordements électriques, circuit process non isolé / non by-passé...) sans démontage ni manœuvre. Ces inspections doivent s'appuyer sur une procédure et leur traçabilité doit être assurée. Elles sont intégrées dans le plan d'inspection de la MMRI.
- *Inspection des tendances dans le cas des comparaisons* : dans le cas de mesures analogiques avec comparaison, le suivi des courbes de tendance des 2 mesures permet un suivi complémentaire à la simple alarme d'écart entre les deux mesures.

Niveau de confiance :

Choix exclusif parmi :

- Niveau de confiance 1 : niveau requis par l'analyse de danger pour la MMRI
- Niveau de confiance 2 : niveau requis par l'analyse de danger pour la MMRI
- Niveau de confiance 3 : niveau requis par l'analyse de danger pour la MMRI

Résultat :

La période de test est donnée en années. Elle est égale au maximum à la somme de tous les coefficients. Des butées sont fixées :

- Si < -5 , revoir architecture car la conception ne permet pas, sur ces critères et avec une période de test raisonnable, de garantir le niveau de confiance requis.
- Entre -5 et 0 , période à prendre $0,5$ an maximale soit une période test de 6 mois.

- Si > 6 , prendre 6 ans maximum ce qui semble être une période de test maximale raisonnable avec des technologies éprouvées.

Effectuer des tests à une fréquence trop rapide n'est pas souhaitable compte tenu des risques intrinsèques à leur mise en œuvre.

Bien entendu cette méthode ne s'affranchit pas des périodes préconisées par les fournisseurs, en particulier dans les cas de dégradation naturelle progressive/consommable (ex : détecteurs de gaz catalytique, etc.).

b. Test des actionneurs

On entend par ce test, le test de l'actionneur jusqu'au système de traitement, ce qui inclut tout le câblage jusqu'au système de traitement et les éventuels modules intermédiaires.

Les critères suivants doivent être analysés :

	Coefficients
Actionneur à émission	-5
Actionneur à émission avec surveillance de ligne de la télécommande et réserve d'énergie...	-2
Actionneur à manque	0
Capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié	5
Test électrovanne intermédiaire	1
Test de course partielle sur la vanne	1
Etanchéité forte	-3
Etanchéité normale	0
Redondance en mode sécurité positive en vannes TOR	5
Redondance en mode sécurité positive en vanne TOR et vanne de régulation	3
Redondance en mode à émission	1
Non redondance en NC3	-20
Double isolement avec évent (DB&B)	1
Service corrosif, colmatant, abrasif...	-3
Service facile	1

Exigence NC1	-1
Exigence NC2	-3
Exigence NC3	-6

Inspection visuelle 1 à 2 fois par an 1

Type d'équipement :

Choix exclusif parmi :

- Actionneur à émission : par exemple, la fonction de sécurité demande à fermer et la vanne reste ouverte en cas de perte de continuité de la commande électrique ou par manque de puissance.
- Actionneur à émission avec surveillance de ligne de la télécommande et réserve d'énergie : méthodes pour compenser certaines défaillances du fonctionnement à émission.
- Actionneur à manque : par exemple, la fonction de sécurité demande à fermer et la vanne reste se ferme en cas de perte de continuité de la commande électrique ou par manque de puissance.

Diagnostic :

Choix multiples possibles parmi :

- *Configuration verrouillée et (capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié (REX)) :*
 - *Configuration verrouillée* : pour les actionneurs dits intelligents, la possibilité de modification du réglage est verrouillée par switch, mot de passe, etc.
 - *Capabilité SIL de l'appareil en SIL2* : appareil conçu pour l'utilisation en sécurité et pouvant faire partie tout seul d'une chaîne de sécurité SIL 2. Cet appareil est donc de fait doté d'autodiagnostic. Cette capabilité est garantie par le fabricant de l'appareil.

Ou éprouvé par l'usage sur le procédé spécifié (REX) : cet appareil est utilisé sur des procédés similaires avec un retour d'expérience positif (*100 000 heures d'utilisation équivalent à 10 équipements sur un an ou 1 équipement pendant 10 ans*) géré par la société.

- *Test électrovanne intermédiaire* : un dispositif de bipasse permet de tester le fonctionnement de l'électrovanne sans arrêter le procédé au moins une fois entre deux tests complets.
- *Test de course partielle sur la vanne* : système électronique automatique ou manuel permettant de vérifier en marche le début fermeture de la vanne.

Exigences techniques de sécurité propres aux actionneurs :

Choix exclusif parmi :

- *Etanchéité forte* : par exemple, cas de toxique, fuel gaz vers brûleurs.
- *Etanchéité normale* : une fuite peut être tolérée. Exemple, coupure de chauffe sur pression haute de colonne à distiller.

Architecture :

La redondance ici signifie qu'en cas de 1 vanne défaillante, la fonction est assurée (par exemple vote 1oo2, 2oo3) par une ou plusieurs autres vannes en série s'il faut couper un fluide.

La redondance peut être homogène (2 vannes) ou hétérogène (par exemple fermeture d'une vanne et arrêt d'un compresseur si l'une ou l'autre des actions arrête le scénario considéré).

Choix multiples possibles parmi (A et B et C exclusifs) :

- *A : Redondance en mode sécurité positive en vannes TOR* : vanne et électrovanne à manque
- *B : Redondance en mode sécurité positive en vanne TOR et vanne de régulation* : ne peut être pris en compte que si un défaut de la vanne de régulation n'est pas à l'origine du scénario.
- *C : Redondance en mode à émission* : par exemple la fonction de sécurité demande à fermer et les vannes ne se ferment pas par défaut de la commande électrique ou par manque de puissance.
- *D : Non redondance en NC3* : un coefficient négatif très élevé affecté à cette ligne permet d'interdire une architecture non redondante pour NC3.
- *E : Double isolement avec évent (DB&B)* : pour le cas d'étanchéité forte requise.

Conditions d'utilisation / Service :

Choix exclusif parmi :

- *Service corrosif, colmatant, abrasif, destructeur...*
- *Service facile* : produit pur, propre, qui ne fige pas...

Suivi spécifique :

Choix multiples possibles parmi :

- *Inspection visuelle 1 à 2 fois par an ou nettoyage des lignes* : par exemple, l'inspection visuelle des vannes, de l'actionneur et des électrovannes peut permettre de détecter des dérives ou problèmes potentiels (graissage, fuite, vibration, défaillance traçage, réseau d'air défaillant, état des raccordements électriques...) et est une mesure de maintenance préventive qui compense partiellement les conditions d'utilisation. Ces inspections doivent s'appuyer sur une procédure et leur traçabilité doit être assurée. Elles sont intégrées dans le plan d'inspection de la MMRI.

Niveau de confiance :

Choix exclusif parmi :

- Niveau de confiance 1 : niveau requis par l'analyse de danger pour la MMRI
- Niveau de confiance 2 : niveau requis par l'analyse de danger pour la MMRI
- Niveau de confiance 3 : niveau requis par l'analyse de danger pour la MMRI

Résultat :

La période de test est donnée en années. Elle est égale au maximum à la somme de tous les coefficients. Des butées sont fixées :

- Si < -5 , revoir architecture car la conception ne permet pas, sur ces critères et avec une période de test raisonnable, de garantir le niveau de confiance requis.
- Entre -5 et 0 , période à prendre $0,5$ an maximum soit une période test de 6 mois.
- Si > 6 , prendre 6 ans maximum ce qui semble être une période maximale de test raisonnable avec des technologies éprouvées.

Effectuer des tests à une fréquence trop rapide n'est pas souhaitable compte tenu des risques intrinsèques à leur mise en œuvre.

Bien entendu cette méthode ne s'affranchit pas des périodes préconisées par les fournisseurs, en particulier dans les cas de dégradation naturelle progressive/consommable (ex : graissage sur certaines vannes...).

c. Système de traitement

c.1 Cas des Automates de sécurité

Un document du fournisseur associé à la certification SIL précise la notion de proof test qui est destiné à révéler les pannes dangereuses non détectées par l'autodiagnostic de l'automate en fonctionnement.

Les périodes de test sont fixées selon les préconisations du constructeur. Le logiciel d'application est testé lors de la mise en service et à chaque modification. La qualité de diagnostic des automates programmables de sécurité (APS) permet de s'assurer que le programme d'application ne peut pas se corrompre. En revanche, il revient à l'exploitant de s'assurer que le programme en service n'est pas modifié indument : verrouillage des codes, suivi des versions, ségrégation des responsabilités/hiérarchie, gestion du changement, compétences...

c.2 Cas des relais et des automates programmables standard

	NC1	NC2	NC3
Relais à Emission éprouvé par l'usage	1 an	N/A	N/A
Relais à manque éprouvé par l'usage	2 ans	1 an	N/A
Relais certifié de sécurité (à manque)	6 ans	3 ans	1 an
Automate éprouvé par l'usage	6 ans	N/A	N/A

Notes :

Période applicable pour des chaînes avec 1 à 10 relais, au-delà diviser par le nombre de dizaine

Pour les relais, les périodes de tests sont fixées suivant 2 critères :

- le niveau de confiance requis,
- la technologie utilisée : relais câblés à émission, relais câblés à manque et éprouvés par l'usage, relais de sécurités certifiés câblés à manque.

La période sera réduite si la fonction réalisée a plus de 10 relais.

Concernant les automates programmables standard, l'application est réduite à un niveau de confiance de 1 qui doit néanmoins être justifié par l'exploitant.

Cette évaluation ne s'affranchit pas des périodes préconisées par les fournisseurs.

10.3.2 Feuilles de calcul

10.3.2.1 Test des capteurs

Critères	Exemples		NC 1 service facile TOR à Manque	NC 1 service facile Analogique avec comparaison	NC1 Service difficile Analogique avec comparaison	NC2 Service facile Analogique avec comparaison	NC2 Service difficile Analogique avec comparaison	NC2 Service facile TOR redondant à manque avec comparaison	NC3 Service facile Analogique avec comparaison + redondance	NC3 Service difficile Analogique avec comparaison + redondance	NC1 TOR à manque service difficile avec inspection tous les ans	NC1 TOR à émission service facile
	Coefficient											
TOR à émission	-5											
TOR à émission avec surveillance de ligne	-4											
TOR à manque	-3		-3	0	0	0	0	-3	0	0	-3	-5
Mesure continue retransmise (analogique)	0											
Analogique avec comparaison	4		0	4	4	4	4	0	4	4	0	0
Configuration verrouillée (accès restreint) et (Capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié (REX))	5		5	5	5	5	5	5	5	5	0	0
Redondance en mode sécurité positive	4		0	0	0	0	0	4	4	4	0	0
Redondance en mode à émission	1		0	0	0	0	0	0	0	0	0	0
Non redondance en NC3	-20		0	0	0	0	0	0	0	0	0	0
Traçage indispensable ou flushing	-2											
Bouchage / Produit colmatant	-3											
Service facile	1		1	1	-3	1	-3	1	1	-3	-3	1
Autres cas difficiles	-1											
Exigence NC1	-1											
Exigence NC2	-3											
Exigence NC3	-6		-1	-1	-1	-3	-3	-3	-6	-6	-1	-1
Inspection visuelle 1 à 2 fois par an ou nettoyage des lignes	2		0	0	0	0	0	0	0	0	2	0
Inspection des tendances dans le cas des comparaisons	1		0	0	0	0	0	0	0	0	0	0
Somme des Coefficients			2	9	5	7	3	4	8	4	-5	-5
Résultat : Période de test en années			2	6	5	6	3	4	6	4	0,5	0,5
Calcul période de test: Si "Somme des coefficients" < -5, revoir architecture, si entre -5 et 0, période à prendre 0,5 an maximum, si > 6, prendre 6 ans maximum												
Note 1: Si le fournisseur donne une période de test liée à la technologie elle doit être respectée (détection gaz catalytique)												
Note 2: Non applicable aux équations compliquées (ex: 2oo2, conditions sur 2 capteurs,...)												
Note3: Redondance = architecture 1oo2, 2oo3												

10.3.2.2 Test du système de traitement

Technologie \ NC Requis de la MMRI	<u>NC1</u>	<u>NC2</u>	<u>NC3</u>
Relais à Emission éprouvé par l'usage (1)	1 an	N/A	N/A
Relais à manque éprouvé par l'usage (1)	2 ans	1 an	N/A
Relais certifié de sécurité (à manque) (1)	6 ans	3 ans	1 an
Automate éprouvé par l'usage	6 ans	N/A	N/A
Automate de sécurité	Suivant données du constructeur (2)		
Notes :			
(1) Période applicable pour des chaînes avec 1 à 10 relais , au-delà diviser par le nombre de dizaine			
(2) logiciel d'application testé lors de la mise en service et à chaque modification			

10.3.2.3 Test de l'actionneur

Critères	Exemples Coefficient	NC 1 service facile vanne TOR à Manque éprouvée par l'usage	NC 1 service facile vanne TOR à émission éprouvée par l'usage	NC 1 service facile vanne TOR à émission surveillée éprouvée par l'usage	NC 1 service difficile vanne TOR à Manque éprouvée par l'usage	NC3 Service facile 2 Vannes TOR à manque	NC3 exigence étanchéité forte - service facile double isolement avec événement	NC2 exigence étanchéité forte - service facile double isolement avec événement	NC3 Service difficile 2 Vannes TOR à manque	NC2 Service facile 1 Vanne TOR à manque éprouvée par l'usage	NC2 Service facile 2 Vannes TOR à manque éprouvée par l'usage	NC2 Service difficile 1 Vanne TOR à manque éprouvée par l'usage
		à Emission	-5									
à Emission avec surveillance de ligne de la télécommande et réserve d'énergie,....	-2	0	-5	-2	0	0	0	0	0	0	0	0
à Manque	0											
Capabilité SIL de l'appareil en SIL2 ou éprouvé par l'usage sur le procédé spécifié	5	5	5	5	5	5	5	5	5	5	5	5
Test électrovanne intermédiaire	1	0	0	0	0	0	0	0	0	0	0	0
Test de course partielle sur la vanne	1	0	0	0	0	0	0	0	0	0	0	0
Exigence étanchéité forte	-3											
Exigence étanchéité normale	0	0	0	0	0	0	-3	-3	0	0	0	0
Redondance en mode sécurité positive en vannes TOR	5											
Redondance en mode sécurité positive en vanne TOR et vanne de régulation	3	0	0	0	0	5	5	5	5	0	5	0
Redondance en mode à émission	1											
Non redondance en NC3	-20	0	0	0	0	0	0	0	0	0	0	0
Double isolement avec event (DB&B)	1	0	0	0	0	0	1	1	0	0	0	0
Service corrosif, colmatant, abrasif	-3											
Service sans difficulté	1	1	1	1	-3	1	1	1	-3	1	1	-3
Exigence NC1	-1											
Exigence NC2	-3	-1	-1	-1	-1	-6	-6	-3	-6	-3	-3	-3
Exigence NC3	-6											
Inspection visuelle 1 à 2 fois par an	1	0	0	0	0	0	0	0	0	0	0	0
Somme des Coefficients		5	0	3	1	5	3	6	1	3	8	-1
Résultat :Période de test en années		5	0,5	3	1	5	3	6	1	3	6	0,5
Calcul période de test: Si "Somme des coefficients" <-5, revoir architecture, si entre -5 et 0, période à prendre 0,5 an maximum, si > 6 , prendre 6 ans maximum												
Note 1: Non applicable aux vannes FL (Reste en l'état)												
Note 2: Non applicable aux architectures multi branches												
Note3 : Redondance = architecture 1oo2, 2oo3												

11 - Glossaire des termes techniques

11.1. TERMES RELATIFS A LA SECURITE FONCTIONNELLE

Terme	Définition	Source(s)
Sécurité fonctionnelle	Ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent : fiabilité, maintenabilité et logistique de maintenance.	NF EN 61511
Disponibilité	Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée. <i>Cette définition est conforme à celle de la norme NF EN 61069</i>	NF EN 61511
Fiabilité	Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné. <i>Elle se mesure par une probabilité.</i>	NF EN 61511
Maintenabilité	Dans des conditions données d'utilisation, aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits. <i>Elle se mesure par une probabilité</i>	NF EN 61511
Crédibilité	Mesure dans laquelle un système est capable de reconnaître et signaler son état et de résister à des entrées incorrectes ou des accès non autorisés. <i>Selon cette norme, la sûreté de fonctionnement se décompose en disponibilité et crédibilité, la première comprenant fiabilité et maintenabilité et la seconde intégrité et sûreté.</i>	NF EN 61069
Intégrité	Assurance fournie par un système que les tâches seront correctement accomplies à moins que le système ne prévienne que l'un quelconque de ses états pourrait conduire à une situation contraire.	NF EN 61069

11.2. TERMES RELATIFS A LA SECURITE

Terme	Définition	Source(s)
Domage	Blessure physique ou atteinte à la santé des personnes ou atteinte aux biens ou à l'environnement.	NF EN 61508
Danger	Source potentielle de dommage.	NF EN 61508
Situation dangereuse	Situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs dangers.	NF EN 61508
Événement dangereux	Événement susceptible de conduire à un dommage.	NF EN 61508
Risque	Combinaison de la probabilité d'un dommage et de sa gravité.	NF EN 61508

Terme	Définition	Source(s)
Risque tolérable	Risque accepté dans un certain contexte et fondé sur les valeurs admises par la société.	NF EN 61508
Risque résiduel	Risque subsistant après que des mesures de prévention ont été prises.	NF EN 61508
Sécurité	Absence de risque inacceptable.	NF EN 61508

11.3. MATERIELS ET DISPOSITIFS

Terme	Définition	Source(s)
Logiciel	Création intellectuelle comprenant les programmes, les procédures, les données et les règles, ainsi que toute documentation associée se référant au fonctionnement d'un système de traitement de données.	NF EN 61508
Actionneur	Mécanisme de "puissance" utilisé pour animer une machine.	EN 1070

11.4. SYSTEME : ASPECTS GENERAUX

Terme	Définition	Source(s)
Système Instrumenté de Sécurité (SIS)	Système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal(aux).	NF EN 61511-1
Architecture	Configuration spécifique des éléments matériels et logiciels dans un système.	NF EN 61508
Module logiciel	Construction consistant en des procédures et/ou déclarations de données pouvant aussi être en interaction avec d'autres constructions de même nature.	NF EN 61508
Redondance	Existence de plusieurs moyens pour accomplir une fonction requise ou pour représenter des informations.	NF EN 61508

11.5. FONCTIONS DE SECURITE ET INTEGRITE DE SECURITE

Terme	Définition	Source(s)
Fonction de sécurité	Fonction à réaliser par un système SIS, par un système relatif à la sécurité basé sur une autre technologie, ou par des dispositifs externes de réduction de risque, prévue pour assurer ou maintenir un état de sécurité au processus, par rapport à un événement dangereux spécifique.	NF EN 61511
Intégrité de sécurité	Probabilité moyenne pour qu'un système instrumenté de sécurité exécute de manière satisfaisante les fonctions instrumentées de sécurité requises, dans toutes les conditions spécifiées et dans une période de temps spécifiée.	NF EN 61511
Niveau d'intégrité de sécurité (SIL)	Niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions instrumentées de sécurité, à allouer aux systèmes instrumentés de sécurité. Le niveau d'intégrité de sécurité 4 possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.	NF EN 61511

11.6. ANOMALIE, DEFAILLANCE ET ERREUR

Terme	Définition	Source(s)
Anomalie	Condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise.	NF EN 61508
Evitement des anomalies	Utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du système instrumenté de sécurité.	NF EN 61511
Tolérance aux anomalies	Aptitude d'une unité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs.	NF EN 61508
Défaillance	Cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise ou à fonctionner comme prévu.	NF EN 61508
Défaillance aléatoire du matériel	Défaillance survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel.	NF EN 61508
Défaillance systématique	Défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés.	NF EN 61508
Défaillance dangereuse	Défaillance qui a la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.	NF EN 61511
Défaillance en sécurité	Défaillance qui n'a pas la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.	NF EN 61511
Défaillance de cause commune	Défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multi- canal, conduit à la défaillance du système.	NF EN 61508
Erreur	Ecart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte.	NF EN 61508
Erreur humaine	Action humaine ou absence d'intervention, qui peut produire un résultat non recherché.	NF EN 61508

Terme	Définition	Source(s)
Défaut	Etat d'une entité caractérisée par son inaptitude à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens extérieurs. Note : Un défaut est souvent le résultat d'une défaillance de l'entité elle-même, mais il peut exister sans défaillance préalable.	NF EN 61511 et NF EN ISO 13849-1

11.7. ACTIVITES LIEES AU CYCLE DE VIE

Terme	Définition	Source(s)
Analyse d'impact	Activité de détermination de l'effet qu'une modification à une fonction ou à un composant d'un système a sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes.	NF EN 61508

11.8. CONFIRMATION DES MESURES DE SECURITE

Terme	Définition	Source(s)
Vérification	Confirmation, par examen et apport de preuves tangibles, que les exigences spécifiées ont été satisfaites.	NF EN 61508
Validation	Confirmation, par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu sont satisfaites.	NF EN 61508
Test périodique	Essai effectué pour révéler des défauts non détectés dans un système instrumenté de sécurité, de telle sorte que, au besoin, le système puisse être restauré dans sa fonctionnalité de conception.	NF EN 61511
Détecté	Révéler. Déclaré. Se rapporte au matériel et signifie détecté par les tests de diagnostic, les tests périodiques, une intervention de l'opérateur (par exemple une inspection et des tests manuels), ou lors de l'exploitation normale.	NF EN 61508
Non détecté	Non révéler. Non déclaré. Se rapporte au matériel et signifie non détecté par les tests de diagnostic, les tests périodiques, une intervention de l'opérateur (par exemple une inspection physique et des tests manuels), ou lors de l'exploitation normale.	NF EN 61508

12 - Terminologie

Terme	Définition	Source(s)
Biais	Ecart ou décalage permanent entre valeur réelle et valeur mesurée.	
Dérive	Variation lente et continue d'une grandeur.	
Capteur	Dispositif transformant l'état d'une grandeur physique observée (température, pression, niveau) en une grandeur utilisable (intensité électrique, position d'un flotteur). Par extension, capteur est utilisé pour désigner l'ensemble constitué de capteurs, conditionneurs, transmetteurs de signaux, alimentation.	
Conditionneur	Dispositif mettant en forme le signal mesuré pour le traduire en une grandeur permettant le traitement (par exemple : tension, courant, fréquence) (multiplexeurs, amplificateurs, filtres, convertisseurs analogique-numérique).	
Kéraunique	Exprime la valeur annuelle moyenne du nombre de jours d'orages (jours où l'on entend le tonnerre en un lieu donné).	
Obsolescence	L'obsolescence peut avoir plusieurs causes liées notamment : <ul style="list-style-type: none"> • aux évolutions technologiques, • à la perte de compétence sur le matériel, • aux évolutions réglementaires, • à l'arrêt du support technique (après l'arrêt de production), • à l'indisponibilité des pièces de rechange. 	
Sécurité positive ou à manque	Fonction de sécurité qui se met en position de sécurité stable par perte d'énergie motrice ou de commande (électricité, air, huile, vapeur...).	
Sécurité à émission	Fonction de sécurité qui se met en position de sécurité stable par l'émission de l'énergie pour la commande et, dans certains cas, par la présence d'énergie motrice.	
Type de redondance	- Chaudes : les composants sont tous en fonctionnement mais un seul est désigné comme actif. Le basculement se fait automatiquement et immédiatement (millisecondes). - Tièdes : les composants de secours sont en veille. Le basculement se fait automatiquement mais avec un temps de latence faible (secondes). - Froides : les composants de secours sont inactifs et ne sont rendus actifs qu'en cas de défaillance des composants principaux. Le basculement peut être effectué manuellement avec un temps de latence plus important (minutes).	
Alimentation sans interruption (ASI)	Equipement principalement destiné à assurer la permanence d'une source d'alimentation en courant alternatif. L'ASI peut également servir à améliorer la qualité de la source d'alimentation en la maintenant dans les limites des caractéristiques spécifiées.	NF EN 62040-1

Terme	Définition	Source(s)
Mean Time To Restoration (MTTR)	Temps moyen de rétablissement. Ce temps est le cumul du : <ul style="list-style-type: none"> - temps de la détection de la défaillance, - temps écoulé avant de commencer la réparation, - temps de réparation effectif, - temps écoulé avant la remise en fonctionnement du composant. 	NF EN 61511
Highway Addressable Remote Transducer (HART)	Protocole de communication numérique conçu pour les applications de mesures des procédés industriels.	

13 - Références de normes citées

Titre	Référence
Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables, relatifs à la sécurité	NF EN 61508
Sécurité fonctionnelle : Systèmes instrumentés de sécurité pour les industries de transformation	NF EN 61511
Vocabulaire Electrotechnique International, Chapitre 191 Sûreté de fonctionnement et qualité de service	NF EN 61511
Mesure et commande dans les processus industriels - Appréciation des propriétés d'un système en vue de son évaluation - Partie 5 : Evaluation de la sûreté de fonctionnement d'un système	NF EN 61508
Sécurité des machines : terminologie.	EN 1070

14 - Autres documents de référence

Titre	Référence
Rapport Q10 - Version 2 de septembre 2008 (INERIS)	DRA-08-95403-01561B
Les automates de sécurité (INERIS)	DRA-08-85350-09702A
Panorama des pratiques de maintenance et de test-Dispositifs et systèmes de sécurité	DRA-08-95404-07287C
Evaluation de sûreté des logiciels - Partie 1 : Principes, Normes, Cycle de vie, Méthodes (INERIS)	DCE-07-85338-17675A
Les Réseaux de terrain (INERIS)	DCE-07-83530-09891A
Note de doctrine générale du 19 juin 2008 relative aux guides sectoriels en matière de risques industriels (DGPR)	
Note de méthode du 12 décembre 2008 relative au plan d'actions pour la maîtrise du vieillissement dans la prévention du risque technologique (DGPR)	BRTICP/2008-601/CBO
Arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation	
Arrêté du 29 septembre 2005 modifiant l'arrêté du 10 mai 2000 modifié relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation	
Arrêté du 4 octobre 2010 modifié relatif à la prévention des risques accidentels au sein des installations classées pour la protection de l'environnement soumises à autorisation	
Arrêté du 10 mai 2000 modifié relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation	
Circulaire du 6 mars 2006 relative à la réglementation des équipements sous pression	BSEI n°06-080
Circulaire du 10 mai 2010 récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risque à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003	