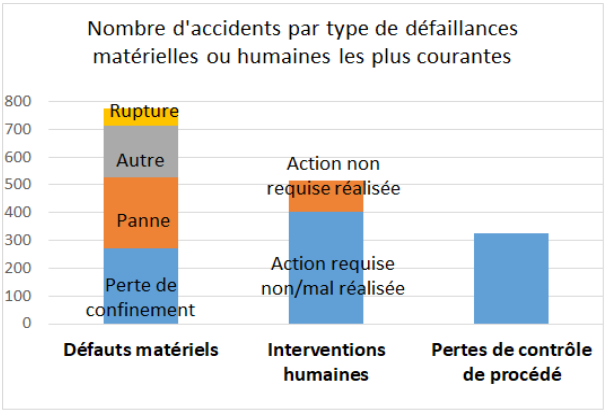
Éviter les défaillances multiples

Qu'elles soient matérielles ou humaines, 1/4 des accidents survenus dans des ICPE soumises à enregistrement ou autorisation depuis 2016 présente au moins 2 défaillances. Les premières vérifications post-accident portent le plus fréquemment sur le système en cause : a-t-il bien fonctionné comme prévu ? Est-ce que les actions humaines nécessaires ont été effectuées ? La présence d'une défaillance n'est déjà pas en soi un événement anodin ; la confrontation à des défaillances multiples l'est encore moins. Aussi est-il important de savoir analyser à son juste niveau et avec tout le recul nécessaire cette multiplicité, car elle vise à orienter les investigations sur la nature des causes profondes des défaillances : existence de modes communs, présence de défaillances génériques, défaillances attachées à un système isolé insuffisamment analysé, défaillances plus profondes liées aux modes d'organisation… Autant de pistes qui expliqueraient l'origine des défaillances multiples et permettraient d'y remédier.

1. Quelles sont les défaillances les plus courantes, dans les cas où elles sont multiples ?

Dans les accidents survenus dans des ICPE soumises à enregistrement ou autorisation depuis 2016 et présentant des défaillances multiples, les défaillances matérielles sont les plus courantes : perte de confinement, panne et rupture. On retrouve ensuite des erreurs humaines, des actions requises non ou mal réalisées : erreur de perception, de décision, d'interprétation ou d'exécution. Les pertes de contrôles de procédé (mélange incompatible, emballement de réaction ou réaction parasite) arrivent en 3ème position.



Les défaillances multiples peuvent agir comme des facteurs aggravants de l'événement initial, comme, dans le cas de défaillances des barrières de protection visant à limiter la gravité d'un phénomène dangereux (rideaux d'eau qui ne se déclenchent pas, détecteur défaillant retardant la détection de l'événement…). Certaines défaillances de mesures de maîtrise des risques (MMRs) pouvant conduire à des accidents majeurs, entraînent des atteintes à l'extérieur du site : e*xemples : odeurs, impacts visuels ou sonores (alerte gaz par exemple) jusqu'au déclenchement du PPI (ARIA 51372 et 52842).*

2. Des actions à différents niveaux pour maîtriser les défaillances multiples

2.1. Post accident, à courte échéance, des modifications matérielles, mais est-ce suffisant ?

Suite à un événement ayant mis en évidence des défaillances matérielles multiples, le système dans lequel l'élément ou les éléments sont mis en cause, doit être analysé en profondeur, ce qui peut aboutir à diverses évolutions :

- la modification de l'élément défaillant : ex : changement de technologie de vanne, de détecteur, mise en place de matériel ATEX ;
- des changements sur la conduite du procédé : ex : maintien de certaines fonctions pendant les phases d'arrêt/redémarrage, amélioration des synoptiques de conduite ;
- l'ajout d'équipements de sécurité : ex : redondance d'un capteur, ou d'une chaîne de détection/action ;
- au renforcement des moyens de surveillance : ex : vidéosurveillance, webcam, augmentation de la fréquence des rondes ;
- l'amélioration du contrôle et de la maintenance du système : ex : modification des fréquences de contrôle, de tests du système, des plans de maintenance… (*ARIA 47654, 49388, 49575, 50121, 50150).*

Pour mener ces changements, l'exploitant doit pouvoir mobiliser les personnes compétentes pour effectuer des choix pertinents des équipements et procédés. Une **étude de l'ergonomie des systèmes** ou des postes de conduites peut venir consolider les choix effectués : *exemples : accès à une vanne, disponibilité des informations sur les synoptiques.* L'exploitant doit être amené à prendre du recul sur l'événement, à redoubler de vigilance lors de son analyse et à rechercher les éventuels modes communs des défaillances. Les modifications matérielles n'étant pas suffisantes, il est nécessaire de mener une réflexion approfondie sur le système lui-même et globale sur les autres systèmes qui peuvent avoir des similitudes ou interactions avec celui en cause. Il s'avère primordial de revoir les **analyses de risques,** identifier les causes communes et généraliser les mesures préventives décidées à l'issue de celles-ci. Les méthodes d'analyse et l'organisation pour les mener peuvent aussi être remises en cause (*ARIA 50254, 52784, 51220).*

2.2. Quels sont les moyens essentiels pour faciliter la prise de décision ?

Certains événements mettent en cause des erreurs de perception, d'appréciation ou d'exécution de la part d'opérateurs, d'équipes en poste, malgré, parfois, l'appui de chefs d'exploitation et des équipes de maintenance. La multiplicité des erreurs renvoie inévitablement vers des facteurs organisationnels. Un défaut de communication peut aussi être à l'origine de l'absence de sollicitation de la personne compétente et d'erreurs dans l'action ou les actions à mener.

ARIA 51220 – 19/09/2017– Aramon (Gard) – France
A 9h20, une augmentation de la pression se produit dans un réacteur de fabrication d'un organomagnésien jusqu'à l'éclatement du disque de rupture. À l'origine, un mélange non conforme a été formé dans le réacteur : un 1er opérateur a mis une quantité d'amorce insuffisante, la consigne pouvant porter à confusion. Un 2ème opérateur, en l'absence de démarrage de la réaction, a introduit une quantité de réactifs excédentaire.
La fiche de fabrication prévoyait la possibilité d'ajouter du réactif, mais avec l'accord de la hiérarchie.
L'opération s'est déroulée un samedi, le chimiste a prévenu tardivement le cadre d'astreinte. Le manque de communication entre les deux postes et d'expérience des opérateurs ont conduit à cet événement. Suite à cet incident, l'exploitant reprend le suivi des habilitations des opérateurs à réaliser les synthèses. Il modifie la fiche de fabrication, afin de clarifier les quantités de réactifs à charger et de prévoir des points d'arrêt pour le démarrage de la réaction. Il interdit le lancement de cette réaction le week-end et planifie le démarrage en début de poste afin d'assurer un suivi du déroulement complet de la synthèse. Il mène une revue détaillée des synthèses d'organo-magnésiens afin d'établir des standards de fabrication et de réaction aux anomalies applicables à l'ensemble des usines concernées.

Les difficultés qui se cumulent pour prendre la bonne décision lors de la gestion d'un événement, peuvent être atténuées en agissant sur les différents leviers organisationnels :

- **mettre à disposition des procédures et consignes claires pour faciliter la prise de décisions :**

Les modifications matérielles exposées plus haut s'accompagnent le plus souvent d'une mise à jour des procédures et modes opératoires associés aux équipements modifiés. Il s'agit :

- des procédures d'exploitation : ex : fiche de fabrication avec des points d'arrêt sur les opérations délicates, fiche réflexe en cas d'anomalies, procédures d'arrêt/redémarrage, de tests, de contrôles, d'élaboration des plans de maintenance…

- des procédures de gestion de crise : ex : impliquer un nouveau scénario dans le POI, modifier la procédure d'appels de l'astreinte, mettre à jour les coordonnées téléphoniques des acteurs externes…

L'analyse des événements permet de savoir ce qu'il manquait aux opérateurs en salle de contrôle pour prendre la bonne décision. Les procédures et fiches doivent être lisibles, facilement accessibles et utilisables par tous. Les acteurs doivent être impliqués dans leur rédaction afin de faciliter leur prise en main par la suite. Certains accidents mettent en évidence l'importance de confronter corps de métier et points de vue pour l'élaboration de ces documents. Une fois ces procédures rédigées, leurs mises en place et en application doivent être appuyées par une organisation interne efficace à tous les niveaux hiérarchiques et fonctionnels (*ARIA 50339, 49109, 52021, 52324, 52384).*

L'ergonomie des salles de contrôle doit également faire l'objet d'une attention particulière pour vérifier, du point de vue des opérateurs, la pertinence et la bonne articulation des modifications matérielles.

- **remettre au centre des préoccupations la formation et la qualification des personnels :**

La mise à jour des consignes et procédures ne peut être envisagée sans accompagnement des opérateurs : il est nécessaire d'organiser des actions de sensibilisation, formation, habilitation dans certains cas, des tests de connaissance ou de mise en situation afin d'accompagner les équipes dans le changement. Il est à noter l'importance d'impliquer les sous-traitants dans ces sessions de sensibilisation/formation et de manière générale dans l'organisation (*ARIA 49970, 50686, 52553).*

Le recyclage des opérateurs, et surtout ceux désignés comme « experts », doit leur permettre de garder le contact avec la réalité des risques présentés par les installations qu'ils sont en charge de piloter.

- **mettre en place une organisation du travail, un encadrement et une communication efficaces :**

Il peut être intéressant d'envisager un brainstorming avec des sites du même groupe, ou dans la même branche d'activités pour trouver des moyens de communication efficace : *exemples : flash sécurité, réunions/causeries sécurité…* Des actions de communication sur le long terme doivent être mises en place.

Tous les changements doivent être appuyés par un solide système de gestion des modifications et de gestion des modes dégradés. L'encadrement dans sa globalité doit être le premier à adhérer aux démarches (*ARIA 51172).*

3. Des changements en profondeur et dans la durée

Les événements, avec des défaillances multiples, rappellent l'importance de pousser la réflexion sur les **causes profondes**, la **défense en profondeur** (barrières de sécurité, MMRs) et de manière globale sur les **analyses de risques**. Les enseignements tirés permettent de construire et généraliser des moyens de prévention et protection sur le long terme, de diminuer la récurrence des accidents, de limiter leurs conséquences et de vérifier la pertinence des scénarios d'accidents.

Malgré cela, une baisse de vigilance peut être parfois observée quand le nombre d'incidents/accidents diminue au sein d'une organisation. Il faut savoir rester en veille, analyser les « **signaux faibles** » ou « **situations à haut potentiel de gravité** » afin d'améliorer la sécurité. Un événement, pris individuellement, peut avoir peu de conséquences, mais s'il devient associé à d'autres circonstances, peut conduire à des dommages importants.

Les messages à faire passer doivent pouvoir atteindre toutes les personnes concernées. La multiplication des façons de communiquer apparaît primordiale. Utiliser un arbre des réussites (vs arbre des causes), faire intervenir un docteur en neurosciences pour expliquer le facteur humain, ou encore mener des enquêtes pour voir la **perception des risques** à tous les niveaux d'une organisation en sont des exemples.