

6.3. Seule une analyse de risque 100% correcte conduit à un environnement de travail plus sûr

La sécurité en production dépend de mesures de gestion exhaustives en la matière. Un des points prioritaires y relatif est l'analyse de risque des machines et des installations. Hélas, trop de fautes se présentent lors de l'exécution, créant des risques potentiels sous-jacents. La première question qui vient à l'esprit : quel type d'analyse faut-il utiliser? Par Sammy Soetaert.

Lors d'une analyse de risque, un inventaire est établi de tous les risques pouvant se présenter sur une machine ou une installation. Un inventaire des risques pour cette dernière est ensuite établi. L'analyse de chaque risque se fait sur la base des dégâts possibles et de la probabilité d'occurrence du défaut. Une fois cet exercice terminé, les risques sont véritablement décortiqués pour évaluer les mesures de prévention nécessaires afin de limiter les risques au minimum. Ces mesures sont diverses : des dispositifs physiques tels que les garde-corps et les arrêts d'urgence, les mesures non physiques telles les formations supplémentaires pour le personnel ou une refonte de certaines procédures. Lorsque toutes les mesures sont prises, l'analyse de risque est à nouveau exécutée pour évaluer la prévention mise en place. Si elle n'est pas suffisante, la procédure doit être renouvelée.

Procédé continu

Une analyse de risque n'est pas un événement ponctuel. À chaque changement dans l'entreprise, un renouvellement de l'analyse de risque s'impose. Mais... qu'entend-t-on par « changement » ? Certes, la zone est encore grise. Cependant, il est ici fortement recommandé d'être prudent et d'opter pour une nouvelle analyse de risque.

Types d'analyse

Une analyse de risque peut se faire suivant diverses méthodes. Le choix de ces dernières dépend principalement du type d'application. Elles diffèrent l'une de l'autre en termes de taille, de complexité, de systématique et en mode d'exécution. L'exécutant de l'analyse de risque peut vous assister dans le meilleur choix. Un aperçu de quelques méthodes populaires.

HAZOP

L'acronyme signifie « HAZard OPerability », analyse dangers et exploitabilité. L'essence d'un HAZOP est de générer des idées pour détecter les éventuelles défaillances et dérives par rapport au design du process normal. Afin d'être exhaustif, un système est mis en place de « mots-clés ». L'on travaille typiquement pour l'HAZOP avec une équipe forte, car connaissance et expérience vont de pair dans cette méthode. L'HAZOP est effectuée en utilisant un diagramme P&ID (schéma tuyauterie et instrumentation) et un PFD (schéma de procédé). Ils intègrent tous les renseignements relatifs aux matières, encombrements, capteurs, instruments, débits, pression... Sur la base de mots-clés standards (« PLUS BAS, PRESSION, MOINS DE, DÉBIT... par exemple) chaque sous process est examiné. S'il apparaît qu'un problème se présente dans l'une des combinaisons, le groupe détermine une mesure de prévention afin d'éliminer le risque. La méthode HAZOP stimule le groupe à sortir des sentiers battus. Simultanément, la méthode exige de la connaissance et de l'expérience. Les deux exigences sont parfois en opposition car l'expérience peut mener à avoir une vision tunnel. Le rôle du président (externe) est d'une importance primordiale. HAZOP est couramment utilisé pour des installations importantes et matures dans l'industrie de process.

AMDEC/FMEA

AMDEC (« FMEA »), Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. La méthode a été développée par la NASA. Elle démarre avec l'inventaire des causes de défaillance de l'installation. Chaque composant de l'installation est analysé par l'équipe projet du début à la fin du cycle complet.

Chaque cause de défaillance possible est consignée. Chacune reçoit un indice de fréquence et un autre de gravité et la probabilité de détection est estimée. Ces trois variables sont fondues dans une expression de criticité par cause de défaillance. Ensuite, une hiérarchie est définie suivant les criticités.

SWIFT

Une variante plus rapide de la méthode AMDEC est SWIFT (« Que Se Passerait-il Si ? »). Par composant (« nœud ») une check-liste renseigne les dérives qui pourraient se présenter. Au cours d'une session de brainstorming, toutes les conséquences pour l'homme, l'environnement et les coûts sont inventoriés. Il est ainsi possible d'évaluer les risques et de prendre les mesures qui s'imposent.

ADD/FTA

L'analyse déductive par arbre de défaillance ADD (« FTA ») définit les causes exactes menant à un défaut redouté à partir d'événements de base. Cette méthode est plus qualitative que quantitative. L'ADD est pratique pour gérer les défaillances complexes.

LOPA

Cette méthode traite de la protection en couches. La « Layer Of Protection Analysis » définit si, dans l'installation, une couche de protection supplémentaire s'impose pour réduire le risque. LOPA est fréquemment utilisée pour les classifications SIL (voir ci-dessous).

BowTie

Le nœud-papillon (« BowTie »), relativement nouveau, est une forme graphique d'analyse de risque. Comme la matière complexe est représentée visuellement, la méthode donne avec clarté les causes et les conséquences liées à un événement redouté Central. Le BowTie est souvent utilisé comme complément au HAZOP.

Relation avec l'EN IEC 61511

Pour l'industrie de process, la norme EN CEI 61511 est la « traduction » de la norme plus complexe à gérer EN CEI 61508 (sécurité fonctionnelle).

Pour la construction de machines, l'EN IEC 62061 est la mise en œuvre pratique de la même norme.

L'EN IEC 61511 définit les exigences minimales des systèmes instrumentés de sécurité dans l'industrie de process. Une de ces exigences est de réaliser une analyse de danger et de risque suivie par l'établissement d'une spécification des systèmes de sécurité. Les méthodes décrites sont quelques-unes des possibilités pouvant servir de base à cette analyse. La méthode d'analyse SIL (« Safety Integrity Level ») quantifie le niveau exigé d'intégrité de sécurité. SIL consiste en quatre classifications qui forment la base des sécurités à considérer pour le process. Après la réduction réelle des risques, l'on examine si la nouvelle situation répond effectivement au niveau d'intégrité SIL prédéterminé.

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Factor	Reduction
SIL 4	>99,99%	0,001% to 0,01%	100,000 to 10,000	
SIL 3	99,9% to 99,99%	0,01% to 0,1%	10,000 to 1,000	
SIL 2	99% to 99,9%	0,1% to 1%	1,000 to 100	
SIL 1	90% to 99%	1% to 10%	100 to 10	

La classification SIL détermine les mesures sécuritaires à prendre.

Source : Maintenance Magazine N° 138 – Décembre 2017