Outil d'inspection
Mesures Actives Préventives

JANVIER 2008

Services belges d'inspection Seveso

Cette brochure peut être obtenue gratuitement auprès de la:

Division du controle des risques chimiques
Service Public Fédéral Emploi, Travail et Concertation sociale
Rue Ernest Blerot 1
1070 Bruxelles
Tél: 02 233 45 12
Fax: 02 233 45 69
E-mail: CRC@emploi.belgique.be

La brochure peut également être téléchargée à partir du site internet suivant : www.emploi.belgique.be/drc

Deze brochure is ook verkrijgbaar in het Nederlands

La rédaction de cette brochure a été clôturée le 8 janvier 2008

Rédaction finale: Peter Vansina

Couverture: Sylvie Peeters

Impression: Service offset

Référence: CRC/SIT/002-F

Version: 1

Editeur responsable:
SPF Emploi, Travail et Concertation sociale

Dépôt légal: D/2007/1205/54

Introduction

Cette note d'information est une publication commune des services belges d'inspection Seveso suivants :

a) pour la Région flamande : de dienst Toezicht zwarerisicobedrijven van de Afdeling Milieu-inspectie van het Departement Leefmilieu, Natuur en Energie ;

b) pour la Région wallonne: la Division de la Police de l'Environnement de la Direction Générale des Ressources Naturelles et de l'Environnement du Ministère de la Région Wallonne

c) pour la Région de Bruxelles-Capitale: Environnement Bruxelles - IBGE

d) pour le niveau fédéral : la Division du contrôle des risques chimiques du SPF Emploi, Travail et Concertation sociale.

Ces services sont désignés comme service d'inspection compétent à l'article 5, §3 de l'Accord de coopération[1].

Dans le cadre d'une politique d'ouverture, cet outil d'inspection est mis gratuitement à la disposition des entreprises pour leur permettre de réaliser elles-mêmes un examen et d'en tirer les conclusions adaptées pour l'amélioration de la prévention des accidents majeurs.

[1] Accord de coopération du 21 juin 1999 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses (M.B. du 16 juin 2001).
Appelé « Accord de coopération » dans la suite du texte.

Contenu

1. COMMENTAIRES SUR L'OUTIL D'INSPECTION 7

1.1. CHAMP D'APPLICATION 8
1.1.1. Mesures actives préventives 8
1.1.2. Système mécanique de décharge de pression 8
1.1.3. Sécurités instrumentales 8
1.2. UTILISATION DE L'OUTIL D'INSPECTION 9
1.3. CADRE DE RÉFÉRENCE 10

2. LISTE DE CONTRÔLE AVEC DES CAUSES DE PRESSION ÉLEVÉE 11

2.1. GÉNÉRALITÉS 12
2.2. CAUSES SPÉCIFIQUES POUR DES TOURS DE DISTILLATION 12
2.3. CAUSES SPÉCIFIQUES POUR DES RÉACTEURS 12

3. QUESTIONNAIRE POUR UN SYSTÈME MÉCANIQUE DE DÉCHARGE DE PRESSION 13

3.1. SPÉCIFICATION DE LA MESURE 14
3.1.1. Identification et documentation de la conception 14
3.1.2. Efficacité 17
3.1.3. Evaluation du risque et fiabilité 23
3.1.4. Risques introduits par le fonctionnement de la sécurité 25
3.2. RÉALISATION TECHNIQUE 25
3.3. MAINTIEN EN ÉTAT DE LA MESURE 27
3.3.1. Inspection et entretien 27
3.3.2. Mise hors service 32
3.3.3. Modifications 33

4. QUESTIONNAIRE POUR DES SÉCURITÉS INSTRUMENTALES 35

4.1. SPÉCIFICATION DE LA MESURE 36
4.1.1. Identification et fonctionnalité 36
4.1.2. Efficacité 39
4.1.3. Indépendance 41
4.1.4. Fiabilité 42
4.1.5. Comportement lors de défaillance 47
4.1.6. Risques dus au fonctionnement 50
4.2. RÉALISATION TECHNIQUE 51
4.2.1. Mesures 51
4.2.2. Vannes 53
4.3. MISE EN SERVICE DE LA MESURE 54
4.4. MAINTIEN EN ÉTAT DE LA MESURE 56
4.4.1. Inspection et entretien 56
4.4.2. Mise hors service temporaire 57
4.4.3. Entretien et réparations 58
4.4.4. Modifications 59

1

Commentaires sur l’outil d’inspection

1.1. Champ d'application

1.1.1. Mesures actives préventives

Cet outil d'inspection vise deux types de mesures qui jouent un rôle très important dans l'industrie des procédés pour prévenir les accidents majeurs, à savoir les systèmes mécaniques de décharge de pression et les sécurités instrumentales. De telles sécurités sont considérées dans la littérature sur la sécurité comme « actives » , en opposition aux mesures dites « passives ». Des mesures actives sont des mesures qui présentent un fonctionnement actif et réagissent à une situation déterminée avec comme objectif de réaliser un effet correctif.

1.1.2. Système mécanique de décharge de pression

Les systèmes mécaniques de décharge de pression considérés ici sont des systèmes utilisant des soupapes de sécurité ou des disques de rupture.
Les soupapes de respiration ("breather valves", en anglais) ne sont pas prises en considération dans cette rubrique.

Dans sa forme la plus simple, un système de décharge de pression est constitué d'une soupape de sécurité ou d'un disque de rupture, ainsi qu'éventuellement d'une tuyauterie en amont et en aval. La tuyauterie en amont relie l'enceinte à protéger à la soupape de sécurité ou au disque de rupture et la tuyauterie en aval draine les substances libérées via la soupape de sécurité ou le disque de rupture vers un endroit sécurisé ou un système de recueil.

Un système de décharge de pression peut également être constitué d'un disque de rupture et d'une soupape de sécurité en série ou de deux disques de rupture en série. Ces montages en série peuvent naturellement être également pourvus de tuyauteries en amont et/ou en aval. Il faut remarquer qu'un montage en série d'un disque de rupture et d'une soupape de sécurité ou de deux disques de rupture doit toujours être considéré comme une seule mesure.

A côté des montages en série, sont également possibles des montages en parallèle de soupapes de sécurité ou de disques de rupture. Lorsque les capacités des systèmes de décharge de pression montés en parallèle doivent être additionnées pour atteindre la capacité d'évacuation requise pour le scénario concerné, les soupapes montées en parallèle font naturellement partie d'une seule et même mesure.

Si la capacité de chacun des systèmes de décharge de pression montés en parallèle est suffisante pour le scénario concerné, ceux-ci doivent être considérés comme redondants.

Un système de décharge de pression peut donc consister en la combinaison de l'un ou de plusieurs des items suivants:

- soupape de sécurité
- disque de rupture
- système d'alimentation
- système d'évacuation.

1.1.3. Sécurités instrumentales

Dans le cadre de cet outil d'inspection, une sécurité instrumentale est une boucle fonctionnant de manière complètement automatique, avec laquelle un ou plusieurs paramètres de procédé sont mesurés. Ces signaux de mesures sont traités par un organe décisionnel pour conduire un ou plusieurs éléments finaux (par ex. vannes ou moteurs).

Les sécurités exigeant une intervention humaine tombent en-dehors du contexte de ce questionnaire.

A ce sujet, il faut remarquer que des sécurités nécessitant une intervention humaine ont généralement une fiabilité plus faible que les systèmes automatiques et, dans beaucoup de cas, elles ne sont pas complètement indépendantes des évènements qui génèrent une activation de la sécurité.

La loi sur le bien-être impose de plus expressément que les risques d'avoir une blessure grave doivent être évités en prenant des mesures matérielles, de préférence à toute autre mesure.

1.2. Utilisation de l'outil d'inspection

Un premier objectif de cet outil d'inspection est de vérifier si les entreprises attachent suffisamment d'attention à la spécification, la conception détaillée, l'exécution technique et l'entretien de ces mesures, de manière à ce qu'elles puissent remplir leur fonction de sécurité efficacement et d'une manière pertinente avec une fiabilité suffisamment élevée.

C'est dans ce but, qu'un ou plusieurs systèmes mécaniques de décharge de pression et des sécurités instrumentales sont sélectionnés comme échantillons et soumis à un questionnaire détaillé et approfondi. Les éventuels manquements constatés pour une mesure préventive active concrète seront, dans beaucoup de cas, caractéristiques pour la méthode générale de travail que l'entreprise utilise pour ces mesures.

La sélection des mesures préventives pour un examen approfondi a lieu dans le cadre d'un examen préalable de l'analyse de risque de l'installation concernée.
Une évaluation de l'analyse de risque est un deuxième objectif de cet outil d'inspection.
Lors de cette évaluation, il va être examiné si l'identification des risques fait preuve d'exhaustivité et que, le cas échéant, les risques d'accidents majeurs ont été formellement évalués.

L'objectif ne peut naturellement pas être que l'équipe d'inspection Seveso réalise elle-même une identification complète de tous les risques possibles en examinant la complétude de l'identification des risques. Ici également, il est recommandé d'utiliser une méthode de travail via une sélection d'échantillons. Dans le cadre de cet outil d'inspection, l'équipe Seveso va surtout sonder si certains types de causes d'accidents majeurs ont été déterminés, plus spécifiquement cette sorte de causes qui, dans beaucoup de cas (mais pas tous), est maîtrisée avec des mesures de prévention actives.

Pour cette discussion, aucun questionnaire fixe n'a été rédigé. L'équipe d'inspection Seveso prépare dans la mesure du possible cette inspection sur base de l'information reprise dans le rapport de sécurité ou d'autres données sur l'installation dont elle dispose.

Pour quand même offrir un certain soutien et une certaine systématique, une liste avec des causes très courantes de pression élevée a été rédigée. Souvent (mais pas toujours), les risques de surpression (pression plus élevée que la pression de design)sont maitrisés via des sécurités instrumentales ou des systèmes mécaniques de décharge de pression. Bien entendu, les sécurités instrumentales peuvent également être utilisées pour maîtriser d'autres risques (par exemple les risques liés à un niveau élevé, une température élevée, …).

La liste ne doit pas être parcourue de A à Z et d'autres phénomènes qui ne se retrouvent pas dans la liste de contrôle peuvent également être discutés.

Cette liste n'a pas la prétention ou l'objectif d'identifier toutes les causes possibles de pression élevée, mais a été sciemment limitée aux causes les plus courantes. En effet, la

liste est une partie d'un outil d'inspection qui doit rester utilisable en pratique, et pas une partie d'une technique d'analyse de risque.

1.3. Cadre de référence

Le questionnaire système mécanique de décharge de pression est basé sur les codes API suivants:

- API Recommanded Practice 520 Sizing, selection and installation of pressure relieving devices in refineries
- API Recommanded Pratcice 521 Guide for Pressure-Relieving and Depressuring Systems
- API Recommanded Practice 576 Inspection of Pressure-relieving Devices.

Le questionnaire pour les sécurités instrumentales a été inspiré par les standards internationaux IEC61508 (Functional safety of electrical/electronic/programmable electronic safety related systems) et IEC61511 (Functional Safety - Safety instrumented systems for the process industry sector).

Pour des raisons pratiques, les questionnaires contiennent seulement une sélection des prescriptions de ces standards et ne peuvent bien entendu pas être vus comme un substitut à ces standards. Il ne peut pas non plus en être conclu que les prescriptions non abordées dans ces questionnaires sont de moindre importance.

2

Liste de contrôle avec des causes de pression élevée

2.1. Généralités

1. Alimentation vers réservoir avec sortie (complètement ou partiellement) fermée
2. Réaction chimique indésirée par introduction de substances non désirées
3. Décomposition thermique par hautes températures
4. Explosion interne
5. Feu externe
6. Percée d'une alimentation à haute pression (défaillance d'un détendeur)
7. Perte de refroidissement
8. Input de chaleur vers une enveloppe isolée
9. Input de chaleur maximum
10. Fuite dans le circuit interne de refroidissement
11. Input de chaleur démesuré via l'alimentation (flux d'alimentation trop chaud)
12. Dilatation thermique

2.2. Causes spécifiques pour des tours de distillation

13. Perte de refroidissement dans le condenseur
14. Perte de reflux au sommet (vanne fermée ou pompe de reflux à l'arrêt) (la conséquence est la plupart du temps le remplissage du condenseur et la perte de refroidissement du flux vapeur entrant)
15. Perte du reflux intermédiaire
16. Apport excessif de chaleur dans le rebouilleur
17. Pression hydrostatique due à un niveau élevé de liquide

2.3. Causes spécifiques pour des réacteurs

18. Production excessive de chaleur (c'est-à-dire plus que ce qui peut être évacué via le refroidissement normal) due à :
    - trop de catalyseur
    - débit trop élevé d'un ou de plusieurs réactifs (continu ou semi-batch)
    - quantité initiale de réactif trop importante (batch ou semi-batch)
    - ordre erroné d'introduction des réactifs
    - réaction d'un excès de réactif(s) après accumulation due à l'arrêt ou la diminution de la réaction à cause de :
        - l'arrêt de l'agitateur
        - trop peu de catalyseur
        - température trop basse
19. Refroidissement insuffisant (c'est-à-dire trop faible pour évacuer la production normale de chaleur) dû à :
    - arrêt du circuit d'eau de refroidissement
    - arrêt de l'agitateur
    - écoulement insuffisant dans un réacteur à flux continu
    - défaut de solvant

3

Questionnaire pour des systèmes mécaniques de décharge de pression

3.1. Spécification de la mesure

3.1.1. Identification et documentation de la conception

Identification et feuille de spécification de soupapes de sécurité

1. L'entreprise dispose-t-elle d'une feuille de spécification pour la soupape de sécurité?
2. La soupape de sécurité a-t-elle un numéro d'équipement univoque (confirmé sur la soupape)?
3. La feuille de spécification mentionne-t-elle ce numéro d'équipement?
4. La feuille de spécification mentionne-t-elle le code de localisation et l'équipement sur lequel la soupape de sécurité est placée?

Il est en fait primordial que la bonne soupape soit installée à la bonne place dans l'installation. C'est pourquoi, il doit y avoir un lien univoque entre la soupape (en tant qu'appareil) et sa localisation dans l'installation.
Un numéro de série apposé par le producteur ou un code d'identification apposé par l'utilisateur sur la soupape peut être utilisé pour une identification univoque de la soupape et le lien avec la localisation dans l'installation.

De manière générale, la feuille d'identification doit contenir des informations dont il doit ressortir que la soupape est une couche de protection efficace et ensuite toutes les spécifications techniques auxquelles doit satisfaire la soupape, de manière à ce que le cas échéant, une nouvelle soupape identique puisse être achetée.

Données de construction de la soupape de sécurité

5. La feuille de spécification mentionne-t-elle le type de soupape (à ressort, « balanced-bellows », commandée par pilote, …) ?
6. La feuille de spécification mentionne-t-elle s'il s'agit d'une soupape de sécurité (à ressort) avec une « action pop » ou avec une ouverture proportionnelle ?
7. La feuille de spécification mentionne-t-elle le constructeur et le modèle de la soupape ?
8. La feuille de spécification mentionne-t-elle les dimensions des brides d'entrée et de sortie ?

Les soupapes de sécurité avec une « action pop » s'ouvrent complètement lorsque la pression de tarage est atteinte. Ces soupapes sont utilisées pour l'évacuation de gaz ou de vapeurs. Les soupapes de sécurité avec une ouverture proportionnelle s'ouvrent progressivement en fonction de la pression.

Différents matériaux peuvent être utilisés dans une soupape de sécurité pour:

- le corps (« body »)
- le ressort
- le disque de fermeture (« disk »)
- le siège (« seating surface »)
- les soufflets (« bellows »)

Résistance de la soupape de sécurité face à la corrosion

9. La soupape de sécurité peut-elle être exposée à des conditions corrosives?
10. Quelles mesures ont été prises par l'entreprise pour éviter la corrosion de la soupape de sécurité?
11. La feuille de spécification mentionne-t-elle les matériaux de construction utilisés dans la soupape

Mesures possibles relatives à l'attaque de la soupape de sécurité par la corrosion:

- choix de matériaux de construction résistant à la corrosion
- utilisation de soufflets pour protéger certaines parties de la soupape
- placement d'un disque de rupture avant la soupape de sécurité
- fréquence d'inspection et d'entretien adaptée

Les soufflets ("bellows"), aussi bien dans les soupapes de sécurité "balanced bellow" que dans les "unbalanced bellow", isolent la tige, le ressort et les autres parties sur la face supérieure de la soupape de sécurité, des substances à évacuer.

Feuille de spécification de disques de rupture

12. L'entreprise dispose-t-elle d'une feuille de spécification pour le disque de rupture?
13. Cette feuille mentionne-t-elle un numéro de localisation?
14. Cette feuille mentionne-t-elle l'information nécessaire sur la marque et le modèle du disque de rupture?

L'API 520 donne un exemple de document de spécification pour des disques de rupture
En règle générale, la feuille de spécification doit contenir des informations dont il doit ressortir que le disque de rupture est une couche de protection efficace et en plus toutes les spécifications techniques pour acheter un exemplaire adéquat.

Une petite plaque avec une série de spécifications (e.a. la pression d'éclatement) pend au disque de rupture. Les informations sur la feuille de spécification doit permettre de vérifier que le bon disque de rupture a été installé.

Données de construction du disque de rupture

15. La feuille de spécification mentionne-t-elle le type de disque de rupture ?
16. La feuille de spécification mentionne-t-elle les dimensions du disque de rupture et du support de disque de rupture ?
17. La feuille de spécification mentionne-t-elle le constructeur et le modèle de disque de rupture ?
18. Dans le cas où un disque de rupture doit évacuer un liquide en surpression: la spécification du producteur confirme-t-elle que le disque de rupture est adéquat pour des liquides?

Il existe différents types de disque de rupture

- "Forward acting" ou "Tension type" (pression sur le côté concave)
- "Reverse acting" ou "Compression type" (pression sur le côté convexe)
- Disques de rupture pre-incisés
- Disques de rupture "composite" (constitués de plusieurs couches).

Il n'est pas évident que la rupture sous l'influence d'un liquide assure une ouverture suffisante du disque de rupture.

Résistance du disque de rupture face à une dépression

19. Le vide peut-il se faire dans le réservoir sous pression?
20. Si oui, la feuille de spécification du disque de rupture mentionne-t-elle qu'il doit être résistant face à cette dépression ou qu'un soutien de vide (« vacuum support ») doit être prévu?

Les disques de rupture "reverse acting" résistent au vide. Les disques de rupture "forward acting" ont normalement besoin d'un soutien au vide.

Pour les disques de type "forward acting", c'est la face concave qui est soumise à la pression. Ce type est également appelé "tension type". Ce type est plus sensible à la fatigue. Ces disques (sans support ou sans support (grille) de vide) ne résistent

normalement pas au vide.

Pour les disques de type "reversed acting", c'est la surface convexe qui est soumise à la pression. Ce type est également appelé "compression type". Ce type est moins sensible à la fatigue et résiste au vide (pas besoin de support (grille) de vide). Ces disques de rupture sont soit pré-incisés, soit pourvus d'un système coupant.
La durée de vie de tels disques de rupture serait aussi nettement plus grande (jusqu'à 10 fois). La probabilité de dépôts ou d'obstruction au niveau du disque est également plus faible.
Inversement, les disques de rupture pourvus d'un système coupant n'autorisent qu'une pression de procédé ne s'élevant qu'à 90% de la pression d'éclatement.

Résistance du disque de rupture à la fatigue

21. Le disque de rupture est-il exposé à des conditions menant à une fatigue?
22. Si oui, la feuille de spécification du disque de rupture mentionne-t-elle qu'il doit être résistant à la fatigue?
23. Le rapport entre la pression de fonctionnement et la pression d'éclatement est-il conforme aux spécifications du disque de rupture?

La fatigue peut être un problème lorsque le disque de rupture est exposé à des variations de pression cycliques ou à des pulsations (par exemple après un compresseur ou une pompe). Des vibrations dans les tuyauteries d'entrée peuvent également donner lieu à une diminution de la pression d'éclatement et de la durée de vie du disque de rupture.

Le fait que le disque de rupture doit être résistant à la fatigue doit être mentionné dans le document de spécification (data sheet) du disque de rupture.

Pour une durée de vie acceptable du disque de rupture, la pression d'éclatement ne doit pas être trop proche de la pression de fonctionnement du réservoir sous pression. On retrouve le rapport maximal entre la pression de fonctionnement et la pression d'éclatement ("operating ratio") dans les spécifications du producteur.
Valeurs typiques:

- disques de rupture "forward acting", non entaillés: 70%
- disques de rupture "forward acting", entaillés: 85%
- disques de rupture "reverse acting" : 90%
- disques de rupture en graphite: 70%.

Le caractère non fragmentable du disque de rupture

24. Dans le cas où un disque de rupture est monté avant une soupape de sécurité, s'agit-il d'un disque de rupture de type non fragmentable?
25. Est-ce mentionné sur la feuille de spécification du disque de rupture ?

Le caractère non fragmentable du disque de rupture est important pour éviter la détérioration des soupapes de sécurité qui sont placées après le disque de rupture.
La plupart des nouveaux modèles de disques de rupture sont pré-incisés dans le but de contrôler le mode d'éclatement et d'éviter la formation de fragments. Ces disques de rupture peuvent également être fabriqués en plus grosse épaisseur.
Cela doit ressortir des spécifications du fournisseur.

Un système coupant est employé pour des disques de rupture du type "reversed acting" qui n'ont pas été pré-incisés. Certains disques sont, d'origine, pourvus d'un système coupant.

Résistance du disque de rupture face à la corrosion

26. Le disque de rupture peut-il être exposé à des conditions corrosives?
27. Quelles mesures ont été prises par l'entreprise pour éviter la corrosion du disque de rupture?
28. La feuille de spécification mentionne-t-elle la matériau de construction du disque de rupture et du support de disque de rupture?

La présence ou non de problèmes de corrosion doit ressortir des résultats d'inspection. Bien que des disques de rupture soient remplacés périodiquement dans beaucoup de cas, il est quand même important que l'entreprise documente l'état du disque de rupture démonté.

Certains types de disques de rupture ont une grande résistance à la corrosion comme, par exemple, ceux réalisés en matériaux composites ("composite rupture disks") ou en graphite. Les disques en matériaux composites sont constitués de différents composants ayant chacun une fonction spécifique, et sous lesquels on place une feuille protectrice séparant du procédé la partie métallique du disque. Cette feuille peut être constituée de téflon ou de métaux nobles.
Les disques de rupture en graphite existent en deux exécutions. La première consiste en un disque rigide en graphite pouvant être placé entre deux brides standards. La seconde est constituée d'une fine membrane en graphite placée dans un support en graphite.

3.1.2. Efficacité

Contre-pression dans le système d'évacuation

29. Le système de décharge de pression souffle-t-il vers un système d'évacuation dans lequel une contre-pression constante peut être présente (cette pression est une partie de la "superimposed backpressure")?
30. Une contre-pression peut-elle se développer suite à l'évacuation simultanée de plusieurs soupapes de sécurité (cette pression est également une partie de la superimposed backpressure)?
31. La feuille de spécification du système de décharge de pression mentionne-t-elle ces contre-pressions?

Une contre-pression constante dans le système d'évacuation et une contre-pression constante suite à l'évacuation simultanée de plusieurs soupapes de sécurité dans ce système forment ensemble la "superimposed backpressure" selon l'API RP 520. La valeur de cette pression devrait pouvoir se retrouver sur la feuille de spécification du système de décharge de pression.

La perte de charge dans le système d'évacuation suite au flux est la "built-up backpressure".
Une grande longueur et des coudes à angle aigu donnent lieu à des pertes de charge relativement élevées.
Pour des soupapes de sécurité conventionnelles, la perte de charge suite à l'évacuation doit être inférieure à 10% de la pression de tarage (conformément à l'API RP 520). Les calculs de pertes de charge à travers le système d'évacuation doivent démontrer que la perte de charge reste en-dessous des 10 % de la pression de tarage.
Dans le cas de soupapes de sécurité balancées, la "built up back pressure" peut prendre des valeurs plus élevées, conformément aux spécifications du producteur (30% à 55%).

Pression de tarage de la soupape de sécurité

32. La feuille de spécification de la soupape de sécurité spécifie-t-elle la pression de tarage de la soupape de sécurité, ainsi que la pression de conception du réservoir sous pression?
33. La pression de tarage de la soupape de sécurité est-elle plus petite ou égale à la pression de conception du réservoir sous pression?
34. A-t-on tenu compte d'une éventuelle "superimposed back pressure"?
35. Y a-t-il une marge suffisante entre la pression maximale qui peut être attendue en fonctionnement normal et la pression de tarage de la soupape de sécurité ?

Selon les standards API et ASME, la pression de tarage d'une soupape de sécurité unique ne peut pas être plus élevée que la pression maximale de fonctionnement admissible ("maximum allowable working pressure") du réservoir sous pression. Souvent, cette valeur est égale à la pression de conception du réservoir.
La pression de conception est une spécification qui est donnée au fabricant lors de la commande d'un réservoir. La pression de fonctionnement maximum admissible est la pression qui peut être déterminée après la construction à partir des détails de construction (épaisseur des matériaux, etc.). Cependant, cette pression n'est pas souvent calculée et l'on doit se référer à la pression de conception pour le tarage des soupapes de sécurité. Pour des raisons de lisibilité, dans ce questionnaire, on fera toujours référence à la pression de conception à la place de la pression de fonctionnement maximum admissible.

Si des soupapes de sécurité complémentaires ont été prévues pour un scénario de feu, les soupapes supplémentaires peuvent avoir une pression de tarage s'élevant jusqu'à 110% de la pression de conception.
Si des soupapes complémentaires ont été prévues pour des scénarios autres que celui de feu, la pression de tarage des soupapes supplémentaires peut s'élever jusqu'à maximum 105% de la pression de conception du réservoir.

Il faut tenir compte du fait que des soupapes de sécurité peuvent s'ouvrir à une pression plus faible que la pression de tarage théorique (suite à la marge de sécurité tolérée sur la pression de tarage). Si la pression maximale de fonctionnement opérationnelle est très proche de la pression de tarage de soupape de sécurité, il y a un risque réel que la soupape s'ouvre en fonctionnement normal et reste ouverte aussi longtemps que cette pression persiste.

Pression d'éclatement du disque de rupture

36. La feuille de spécification du disque de rupture spécifie-t-elle la température de fonctionnement aux conditions d'éclatement (température d'éclatement), la pression d'éclatement à la température d'éclatement et la pression de conception du réservoir sous pression?
37. La pression d'éclatement est-elle plus petite ou égale à la pression de conception du réservoir?
38. Lors de la détermination de la pression d'éclatement du disque de rupture a-t-on tenu compte de la température à laquelle le disque de rupture doit travailler?
39. La pression d'éclatement tient-elle compte d'une éventuelle "superimposed back pressure"?

Pour la pression d'éclatement d'un disque de rupture, les mêmes règles que pour la pression de tarage des soupapes de sécurité sont valables. La pression d'éclatement d'un disque de rupture est indiquée sur le disque de rupture lui-même et peut donc être vérifiée sur place.

Il faut tenir compte de la température à laquelle le disque de rupture doit fonctionner. La pression d'éclatement d'un disque de rupture diminue lorsque la température augmente.
En fonction du montage, il se peut que le disque de rupture aura la température du

procédé ou la température ambiante (ou une valeur intermédiaire). Si la déviation dans le procédé se déroule rapidement, la température du disque de rupture ne va pas immédiatement suivre, la température d'éclatement du disque de rupture n'est pas nécessairement la température du procédé pendant le scénario d'urgence.

Un producteur de disques de rupture dispose de facteurs de conversion permettant de calculer les pressions d'éclatement à partir de la pression d'éclatement à température ambiante.

Débit à évacuer

40. Tous les scénarios de surpression pour lesquels le système de décharge de pression doit assurer une protection, sont-ils documentés?
41. L'entreprise a-t-elle vérifié si un flux biphasique (gaz + liquide) pouvait exister en traversant la soupape (pour le scénario sélectionné ou pour d'autres scénarios)?
42. A-t-on déterminé pour chaque scénario le débit de décharge requis?
43. Ces calculs sont-ils bien documentés?
44. La feuille de spécification fait-elle référence aux feuilles de calcul des scénarios ?
45. La feuille de spécification mentionne-t-elle le débit maximum à évacuer?
46. La feuille de spécification mentionne-t-elle les caractéristiques nécessaires du flux à évacuer, telles que composition, phase, température, densité ?

L'apparition d'un flux biphasique dépend de la nature des substances et des conditions dans le réservoir sous pression ainsi que du scénario, en d'autres mots du phénomène donnant lieu à l'activation de la décharge de pression.

Capacité d'évacuation requise et installée

47. La surface de passage requise a-t-elle été déterminée pour chaque scénario de surpression?
48. Ces calculs sont-ils bien documentés?
49. La feuille de spécification du système de décharge de pression mentionne-t-elle la plus grande surface de passage requise?
50. La feuille de spécification du système de décharge de pression mentionne-t-elle la surface de passage de la soupape de sécurité ou du disque de sécurité installé?
51. La surface de passage du système de décharge de pression installé est-elle égale ou plus grande que la plus grande surface de passage requise?

Pour un scénario déterminé, on calcule la surface de passage requise à partir du débit à évacuer. Ensuite, on choisit une soupape dont la surface de passage effective est égale ou plus grande que ce qui est exigé.

Pour les soupapes API, la dimension d'une soupape est exprimée via une combinaison d'un chiffre, d'une lettre et d'un chiffre. Le premier chiffre est le diamètre (en pouces) de la connexion d'entrée de la soupape, la lettre est une mesure du passage interne de la soupape (qui est finalement déterminante pour le débit) et le troisième chiffre, une mesure de l'échappement de la soupape (6Q8 par exemple).

Calcul de la surface de passage

52. Lors du calcul de la surface de passage requise, est-on parti d'une surpression tolérable qui est en conformité avec le code de construction du réservoir sous pression?
53. Pour les flux subcritiques, a-t-on tenu compte de la contre-pression totale?
54. Dans le cas d'un flux biphasique: en a-t-on tenu compte dans les calculs de la surface de passage requise?
55. L'entreprise dispose-t-elle d'une directive univoque pour le calcul des flux biphasiques dans les systèmes de décharge de pression?
56. La feuille de spécification mentionne-t-elle l'existence d'un flux biphasique?
57. Dans le cas d'une combinaison d'un disque de rupture et d'une soupape de sécurité, a-t-on tenu compte de la diminution de capacité de cette combinaison?

Pour la détermination de la surface de passage requise, on fait une distinction entre les flux en phase gazeuse, en phase liquide et les flux biphasiques.

Pour le flux en phase gazeuse, on fait une distinction entre les flux critiques et subscritiques. Lors de flux critique, la vitesse de sortie est égale à la vitesse maximale possible, à savoir la vitesse du son dans le gaz. La pression correspondante dans le passage de la soupape de sécurité est appelée la pression critique. Lors de flux critiques, la pression dans la soupape de sécurité ne peut pas passer en-dessous de la pression critique, même s'il y a une pression beaucoup plus faible présente en aval dans le système d'évacuation.
Si la contre-pression dans le système d'évacuation est donc plus faible que la pression critique, on a affaire à un flux critique et le débit est maximal (pour la pression donnée à l'entrée de la soupape). Si la contrepression dans le système d'évacuation est plus élevée que la pression critique, le flux est subcritique et le débit d'évacuation sera donc plus faible (pour la même pression à l'entrée).

La pression critique peut être calculée à partir de la pression d'évacuation (pression à l'entrée de la soupape de sécurité) et des propriétés du gaz (le rapport entre la chaleur spécifique à pression constante et la chaleur spécifique à volume constant).

Pour les flux critiques, la surface de passage requise dépend de la surpression dans le réservoir (normalement 110% de la pression de conception), du débit d'évacuation requis, de la température, des propriétés du gaz et des facteurs de correction (dépendant de la soupape). La contrepression ne joue donc ici aucun rôle sauf via un facteur de correction pour des soupapes de sécurité balancées.

Pour des flux subcritiques, il faut tenir compte en plus de la contrepression dans les calculs.

Pour les flux de liquides, la surface de passage requise est déterminée sur base de la surpression dans le réservoir (normalement 110% de la pression de conception), de la contrepression totale, des propriétés du liquide et des facteurs de correction (dépendants de la soupape).
Pour les flux biphasiques, il y a trois méthodes de calcul courantes:

- "maximal area" (le diamètre de soupape requis est calculé séparément pour le gaz et le liquide; le plus grand des diamètres est retenu)
- "Added areas" (le diamètre de soupape requis est calculé séparément pour le gaz et le liquide ; la surface retenue est la somme des deux surfaces)
- "Driers omega" (calcul selon un modèle informatique).

Les résultats des trois méthodes peuvent fortement diverger !
Il est important que l'entreprise ait une approche cohérente, et choisisse donc toujours la même méthode au lieu de, par exemple, retenir d'office le plus petit des trois résultats possibles.

Pour les disques de rupture, on peut utiliser les mêmes formules que pour les soupapes

de sécurité.

La surface de passage de la tuyauterie d'évacuation doit au moins être aussi grande que la valeur requise et le disque de rupture doit avoir les dimensions de la tuyauterie d'évacuation. La surface projetée d'un système coupant ou d'une grille de dépression doit être soustraite de la surface de passage de la tuyauterie d'évacuation.

La surpression maximale admissible est spécifiée dans le code de construction du réservoir sous pression.
Pour les réservoirs sous pression conçus selon les standards ASME, ce sont les valeurs suivantes qui sont d'application:

- 110% de la pression de conception du réservoir (pour d'autres scénarios que celui de feu externe et pour un système de décharge de pression unique)
- 121% de la pression de conception pour des scénarios de feu externe
- 116% de la pression de conception dans le cas de plusieurs systèmes de décharge de pression.

Cfr API RP 520 ou ASME section VIII division 1

Pour les réservoirs sous pression conçus selon l'AD-Merkblätter, la pression en cas de feu externe doit être limitée à 110 % de la pression de conception.

Une valeur inférieure à celles conformes aux standards de conception est pensable, par exemple dans le cas où l'on tient compte de la dégradation et d'une diminution (calculée) de la résistance initiale.
Il n'est pas conseillé de faire correspondre la surpression maximale admissible à la pression d'épreuve. La pression d'épreuve est en effet une propriété d'un nouvel équipement à des températures qui peuvent diverger des températures opérationnelles. Il n'est pas évident qu'un réservoir sous pression reste résistant à la pression d'épreuve suite à la dégradation due à l'usage.
Le raisonnement qu'un réservoir sous pression ne défaillira pas de manière catastrophique lors d'un dépassement de la pression de conception, mais va seulement fuir au niveau des points faibles, ne peut pas non plus être accepté sans plus. De petites fuites ne feront pas non plus dévier suffisamment la montée en pression et aussi longtemps que c'est le cas, la fissure va continuer à grandir jusqu'à ce que la force motrice soit partie.

Selon le standard ASME (section VIII, division I), la pression d'éclatement d'un disque de rupture ne peut pas être supérieure à la pression de conception du réservoir à protéger.

En général, il est admis que la capacité d'une combinaison disque de rupture – soupape de sécurité est égale à la capacité de la soupape de sécurité multipliée par un facteur de combinaison égal à 0,9, à moins que le producteur du disque de rupture n'avance d'autres chiffres.

Forces statiques et dynamiques sur la tuyauterie d'évacuation

58. La tuyauterie d'évacuation est-elle soutenue?
59. Des liquides sont-ils évacués et, si oui, le système d'évacuation est-il conçu contre le poids du liquide lorsque ces tuyauteries seront remplies de liquide?
60. Les forces de réaction qui apparaissent lors de l'évacuation ont-elles été déterminées?
61. L'entreprise a-t-elle vérifié si le système d'évacuation est résistant contre ces forces de réaction?

Les tuyauteries d'évacuation ne peuvent pas seulement être soutenues par la soupape de sécurité. Un soutien complémentaire est nécessaire pour éviter que le poids statique de la tuyauterie d'évacuation puisse donner lieu à des tensions dans la soupape de sécurité qui pourraient conduire à des fuites ou à un fonctionnement incorrect.
Les forces de réaction qui apparaissent lors d'une évacuation atmosphérique sont en général plus grandes que les forces de réaction en cas de décharge dans un système

fermé. API 520 donne quelques formules pour des systèmes simples d'évacuation vers l'atmosphère.

Dans un système fermé, de plus grandes forces apparaîtront surtout dans des endroits où a lieu une subite expansion. La combinaison d'un flux biphasique et de coudes à 90 degrés génère également de grandes forces.
Le calcul des forces dans un système fermé est en général très compliqué.

Diminution de la température lors de l'évacuation des soupapes de sécurité

62. Lors de l'évacuation peut-on avoir de basses températures dans la soupape de sécurité et dans la tuyauterie d'évacuation?
63. Si oui, la diminution de température est-elle indiquée sur la feuille de spécification?
64. De petites fuites dans la soupape de sécurité peuvent-elles occasionner de basses températures et la formation de glace autour de la soupape?
65. Si oui, la soupape de sécurité est-elle dans ce cas inspectée périodiquement pour détecter la formation de glace?
66. Le matériau de construction de la soupape de sécurité et de la tuyauterie d'évacuation peut-il résister à d'éventuelles chutes de température suite à l'évacuation ou à des fuites?

Lors de l'évacuation de gaz sous haute pression ou de gaz liquéfiés, de très basses températures peuvent-elles se produire suite à l'expansion?
De petites fuites internes dans la soupape de sécurité peuvent également dans certains cas générer de basses températures entraînant un givrage autour de celle-ci. On doit évidemment dans ce cas se poser la question de savoir si la soupape fonctionne encore correctement (et n'est donc pas bloquée par un givrage interne).
Une vérification sur place doit permettre d'élucider la présence d'un givrage autour de la soupape de sécurité.

Vitesse de montée en pression

67. Y a-t-il certains scénarios de surpression pour lesquels la pression se développe très rapidement?
68. Si pour ces scénarios de surpression, on compte sur une soupape de sécurité, a-t-on alors vérifié si la soupape de sécurité peut réagir suffisamment vite?

Pour des temps de réaction très courts, l'utilisation d'une soupape de sécurité peut être exclue et il faut le cas échéant utiliser un disque de rupture.

Perte de charge dans le système d'évacation

69. A-t-on déterminé la perte de charge générée à la suite du passage à travers le système d'évacuation?
70. Cette perte de charge est-elle suffisamment faible, conformément aux codes utilisés pour le dimensionnement de la soupape de sécurité?

La perte de charge dans le système d'évacuation suite au flux est la "built-up backpressure".
Une grande longueur et des coudes à angle aigu donnent lieu à des pertes de charge relativement élevées.
Pour des soupapes de sécurité conventionnelles, la perte de charge suite à l'évacuation doit être inférieure à 10% de la pression de tarage (conformément à l'API RP 520). Les calculs de pertes de charge à travers le système d'évacuation doivent démontrer que la perte de charge reste en-dessous des 10 % de la pression de tarage.
Dans le cas de soupapes de sécurité balancées, la "built up back pressure" peut prendre des valeurs plus élevées, conformément aux spécifications du producteur (30% à 55%).

Perte de charge dans la tuyauterie d'entrée

71. A-t-on calculé la perte de charge dans la tuyauterie d'entrée?
72. A-t-on également tenu compte de la perte de charge au travers d'un éventuel disque de rupture dans la tuyauterie d'entrée?
73. Cette perte de charge est-elle suffisamment petite pour ne pas compromettre la fonction de protection du système de décharge de pression?

Une grande longueur et des coudes à angle aigu donnent lieu à des pertes de charge relativement élevées.

Selon l'API RP 520 (part II), la perte de charge entre la soupape de sécurité et le réservoir sous pression ne peut pas s'élever à plus de 3% de la pression de tarage de la soupape. Si dans la tuyauterie d'entrée vers une soupape de sécurité, on a installé un disque de rupture, il faut tenir compte de la perte de charge au travers du disque de rupture (ensemble avec la perte de charge sur la tuyauterie d'entrée de la soupape de sécurité).

Si la perte de charge s'élève à plus de 3% de la pression de tarage, il faut faire une analyse sur l'influence de la perte de charge sur le fonctionnement de la soupape.
Pour la détermination de la perte de charge au travers d'un disque de rupture, on peut prendre comme règle générale que la perte de charge correspond à la perte de charge sur une distance de 75 fois le diamètre de la tuyauterie. On peut éventuellement trouver des valeurs plus précises dans les spécifications du producteur.

3.1.3. Evaluation du risque et fiabilité

Réalisation de l'évaluation des risques

74. Les scénarios de surpression pour lesquels le système de décharge de pression doit assurer une protection, ont-ils été soumis à une évaluation des risques pour déterminer si le risque de surpression est suffisamment maîtrisé?
75. Ces évaluations de risques sont-elles bien documentées?
76. Quelle fiabilité l'entreprise donne-t-elle au système de décharge de pression dans ces évaluations des risques?
77. Quelle est la réduction de risques totale des couches de protection?

Une évaluation des risques objective et consistante n'est pas possible sans que l'on se forme une quelconque idée de la fiabilité des mesures, et de la probabilité et de la gravité des conséquences.
Une bonne documentation de l'évaluation des risques comprend:

- une bonne description des causes (l'évènement initial ou condition qui donne lieu au scénario)
- une estimation de la probabilité de l'évènement initial
- une description des conséquences possibles du scénario
- une estimation de la gravité des conséquences du scénario
- une énumération de toutes les couches de protection
- une estimation de la fiabilité des couches de protection.

Gestion de l'évaluation des risques

78. Le formulaire d'évaluation des risques est-il un document contrôlé?
79. L'entreprise dispose-t-elle de critères clairs pour l'exécution d'une évaluation des risques?
80. Les critères ont-ils été approuvés par la direction?

Le fait que l'évaluation d'un scénario déterminé est réalisée en concertation entre différentes personnes est une bonne pratique. L'évaluation de chaque scénario doit être

bien documentée, c'est-à-dire que non seulement le résultat final doit être documenté mais également le raisonnement qui a mené à ce résultat (les hypothèses, les réflexions, etc.).
Des mesures doivent être prises pour assurer que la décision prise en groupe, ne puisse être modifiée sans plus par après. C'est pourquoi il est recommandé de laisser signer le rapport de l'évaluation des risques (pour chaque scénario) par tous les participants.

Les critères d'évaluation des risques déterminent directement le niveau de sécurité vers lequel tend l'entreprise et c'est pourquoi, ils doivent être formellement approuvés par la direction.

Fiabilité

81. Sur quoi se base l'entreprise pour attribuer une certaine fiabilité au système de décharge de pression?
82. Utilise-t-on les résultats de "pré-tests" (test de pression de tarage avant démontage et entretien) pour estimer la fiabilité de la soupape de sécurité?
83. Dans le cas où le système de décharge de pression est constitué de plusieurs soupapes ou disques de rupture en parallèle, la fiabilité de l'ensemble est-elle alors déterminée sur base de la fiabilité des composants individuels?
84. A-t-on tenu compte ici des fautes communes?

Lorsque plusieurs soupapes ou disques de rupture sont nécessaires pour fournir la capacité d'évacuation requise, les probabilités de défaillance de ces soupapes de sécurité ou disques de rupture doivent être additionnées.
Lorsque les soupapes ou disques de rupture sont installés de façon redondante, cela veut dire que chaque soupape ou disque de rupture a séparément une capacité d'évacuation suffisante, les probabilités de défaillance peuvent être multipliées ensemble avec un facteur appelé « beta » qui tient compte des fautes communes.

Des fautes communes pour des soupapes de sécurité montées en parallèle sont par exemple:

- tuyauterie d'entrée commune (qui peut être fermée ou encrassée)
- corrosion ou encrassement de deux soupapes exposées au même milieu
- erreurs humaines communes lors du calcul, du montage, du réglage, de l'inspection, etc.

Dans le cas d'interdépendances, le produit des probabilités de défaillance individuelles donne une fiabilité erronée (trop optimiste) pour l'ensemble.
Le facteur « beta » est une mesure quantitative pour la dépendance utilisée dans les formules pour le calcul de la fiabilité des sécurités instrumentales. Ces formules peuvent également être appliquées pour le calcul de montages en parallèle de soupapes de sécurité ou de disques de rupture. Pour des soupapes montées en parallèle, le facteur « beta » peut se chiffrer à 20%.

Fréquence de sollicitation réelle

85. Dans la pratique, combien de fois la soupape de sécurité a-t-elle déjà été sollicitée?

Le nombre de fois qu'une soupape de sécurité a été sollicitée peut être déduit du nombre de révisions ou de contrôles que celle-ci a subit, en dehors des révisions périodiques. Dans la plupart des cas, une soupape qui a déjà été sollicitée ne fermera plus entièrement et une révision de celle-ci s'avèrera nécessaire. Cette information devrait se retrouver dans le dossier d'entretien de la soupape en question.
Les disques de rupture doivent naturellement toujours être changés après sollicitation.
La fréquence de sollicitation réelle de la soupape de sécurité doit, dans les grandes lignes, concorder avec celle escomptée sur base du scénario. Si la fréquence réelle de sollicitation est plus élevée que celle estimée dans un scénario unique, cela signifie que la fiabilité d'autres mesures antérieures dans le scénario a été surestimée.

3.1.4. Risques introduits par le fonctionnement de la sécurité

Libérations via le système de décharge de pression

86. Les effets d'une libération via le système de décharge de pression ont-ils été examinés?
87. Ces risques ont-ils également été évalués?
88. Le cas échéant, des mesures pour limiter les dommages ont-elles été prises?

Les quantités qui sont évacuées, la suite de l'émission et les éventuels dommages pouvant survenir en conséquence d'une libération doivent être examinés.
Dans le cas d'un disque de rupture, la liaison du réservoir sous pression avec l'environnement reste ouverte, à l'opposé des soupapes de sécurité qui sont supposées se refermer lorsque la pression dans le réservoir a suffisamment baissé. A côté du risque d'une émission plus importante, le risque d'introduction d'air ou d'humidité dans le réservoir sous pression est également à considérer.

Une évaluation des risques doit être réalisée pour vérifier si la probabilité d'une émission vers l'environnement via le système de décharge de pression est suffisamment faible, vis à vis de la gravité de cette émission.

Pour les disques de rupture, on peut utiliser une détection de rupture pour initier des mesures de limitation des dommages (par ex. une évacuation de la zone autour de l'évacuation vers l'atmosphère). Une détection automatique est possible par exemple via une détection de rupture ou via une mesure de pression dans le système d'évacuation.

Libérations via le "bonnet vent" ou des ouvertures de drainage

89. Des éventuelles libérations via l'ouverture de ventilation dans la coiffe du ressort ("bonnet") ou via l'ouverture de drainage de la tuyauterie d'évacuation forment-elles un risque?
90. Ces risques ont-ils été analysés?

Des soupapes de sécurité "balanced bellow" ont une ouverture de ventilation dans la coiffe du ressort ("bonnet vent").
Via cet évent, de petites quantités des substances à évacuer peuvent aboutir dans l'environnement. Dans certaines circonstances (par ex. dans un bâtiment ou avec des substances très dangereuses), ces libérations limitées peuvent former un risque.

3.2. Réalisation technique

Rétrécissements dans les tuyauteries d'entrée et d'évacuation

91. Le diamètre de la tuyauterie d'entrée n'est-il nulle part plus petit que le diamètre de la bride d'entrée de la soupape de sécurité?
92. Le diamètre de la tuyauterie d'évacuation n'est-il nulle part plus petit que le diamètre de la bride d'évacuation de la soupape de sécurité?
93. Y a-t-il des vannes dans les tuyauteries d'alimentation ou d'évacuation?
94. La surface de passage de ces vannes est-elle plus grande ou égale à, respectivement, la surface d'entrée et d'évacuation de la soupape de sécurité?

Les dimensions de la bride d'alimentation et de la bride d'évacuation de la soupape de sécurité devraient être mentionnées sur la feuille de spécification de la soupape de sécurité. Les dimensions des tuyauteries d'entrée et d'évacuation devraient pouvoir être retrouvées sur le P&ID.

La présence de vannes dans les tuyauteries d'entrée ou d'évacuation devrait être indiquée sur le P&ID et peut éventuellement aussi être vérifiée sur place.

La surface minimale de passage ("minimum flow area") de la vanne d'isolation dans la tuyauterie d'entrée doit être égale ou plus grande que l'ouverture d'entrée ("inlet area") de la soupape de sécurité. La surface minimale de passage de la vanne d'isolation dans la tuyauterie d'évacuation doit être égale ou plus grande que l'ouverture d'évacuation ("outlet area") de la soupape de sécurité. La surface de passage des vannes d'isolation devrait être mentionnée dans les feuilles de spécification de ces vannes.

Accumulation de liquides

95. Peut-on avoir une accumulation d'eau ou d'un autre liquide au-dessus de la soupape de sécurité ou du disque de rupture, par exemple par condensation de l'humidité, la pluie, l'activation d'autres systèmes de décharge de pression?
96. A-t-on prévu des mesures pour contrer l'accumulation d'eau ou d'autre liquide?
97. Des liquides peuvent-ils s'accumuler plus loin dans le système d'évacuation?
98. Des mesures ont-elles été prises pour éviter la condensation et/ou l'accumulation de liquides?
99. La tuyauterie d'entrée a-t-elle une pente libre de sorte qu'aucun produit ne peut s'y accumuler?

L'accumulation de liquide au-dessus de la soupape de sécurité ou du disque de rupture peut engendrer différents problèmes : contre-pression due à la pression statique du liquide, blocage par la glace de la tuyauterie d'évacuation, corrosion de la soupape ou du disque de rupture ainsi que de la tuyauterie d'évacuation, détérioration des tuyauteries d'évacuation due à l'impact du liquide projeté.

Des mesures possibles sont : une pente libre vers un puits d'évacuation, des trous de purge ou des capots anti-pluie.

Il est également important d'éviter la condensation et l'accumulation de liquide dans d'autres endroits du système d'évacuation et dans la tuyauterie d'entrée. Des liquides dans le système d'évacuation peuvent engendrer de grandes forces lors de l'évacuation et peuvent donner lieu à de la corrosion.

Des liquides dans la tuyauterie d'entrée peuvent également influencer de manière négative le fonctionnement de la soupape ou engendrer plus d'entretien.

Obstructions

100. Les substances évacuées peuvent elles engendrer des obstructions, telles que des poudres, des substances polymérisantes, des produits collants, des substances à haut point de fusion, etc.?
101. Si oui, des mesures ont-elles été prises pour remédier aux problèmes avec ces substances?
102. Dans le cas où un chauffage ("tracing") a été prévu: des mesures nécessaires ont-elles été prises pour en assurer la fiabilité?
103. Dans le cas d'isolation: les ouvertures de ventilation dans la coiffe du ressort de la soupape de sécurité (« bonnet ») sont-elles maintenues libres?

Les soupapes de sécurité commandées par pilote peuvent présenter une sensibilité plus importante pour des produits salissants, collants, très visqueux ou polymérisants que des soupapes de sécurité normales ou des soupapes de sécurité balancées. En cas de doute, les circonstances de travail acceptables doivent être demandées auprès du producteur.

Une isolation et/ou un chauffage peut être nécessaire:

- pour éviter la condensation (et la corrosion qui peut en être la conséquence)
- pour éviter des problèmes avec des liquides visqueux

- pour éviter la solidification de produits.

Le bon fonctionnement du chauffage peut être assuré par des alarmes, des inspections et des entretiens périodiques.

Contre-pression pour des disques de rupture

104. Dans le cas d'un montage en série d'un disque de rupture et d'une soupape de sécurité (ou de 2 disques de rupture en série), des mesures ont-elles été prises pour éviter une montée en pression dans l'espace entre le disque de rupture et la soupape de sécurité (ou entre les 2 disques de rupture)?
105. La mesure de pression (avec ou sans alarme) entre le disque de rupture et la soupape de sécurité est-elle périodiquement inspectée?

Lors du montage en série d'un disque de rupture avec un autre disque ou avec une soupape de sécurité, une contrepression peut se développer du côté de l'évacuation du fait d'une fuite dans le disque. De telles fuites peuvent, par exemple, résulter d'une corrosion par piqûre ("pitting").
Notez les mesures prises par l'entreprise pour solutionner ce problème.
Une première alternative est de placer un indicateur permettant de lire la pression localement. La question est de savoir à quelle fréquence la lecture est effectuée ?
Une seconde alternative est une mesure de la pression (mesure en continu, de préférence) déclenchant une alarme en salle de contrôle.
Une troisième alternative est de relier l'espace clos à l'atmosphère ou au système d'évacuation. En cas de liaison à l'atmosphère, il faut se poser la question de savoir comment une fuite éventuelle pourra être détectée. Une liaison au système d'évacuation peut avoir pour conséquence un reflux du système d'évacuation et entraîner la corrosion du disque de rupture.

3.3. Maintien en état de la mesure

3.3.1. Inspection et entretien

Programme d'entretien de soupape de sécurité

106. La soupape est-elle reprise dans un programme d'entretien périodique ?
107. Comment la fréquence d'entretien a-t-elle été choisie ?
108. A-t-on examiné si un entretien était nécessaire chaque fois qu'une soupape de sécurité a été sollicitée ?
109. Y a-t-il un dossier d'entretien disponible pour la soupape de sécurité?
110. Ce dossier contient-il tous les rapports des tests et tours d'entretien réalisés ?
111. Des expériences opérationnelles sont-elles également documentées?

API576 prescrit que l'intervalle d'inspection est déterminé sur base d'un pré-test.
API510 donne 10 ans comme limite supérieure pour l'intervalle d'inspection.

La fréquence d'entretien est en principe choisie en fonction des :

- risques de surpression
- résultats des pré-tests et des inspections visuelles (voir ci-dessous).

La probabilité qu'une soupape de sécurité qui a fonctionné, fuie, est réelle.

Des expériences opérationnelles intéressantes sont par exemple:

- certaines perturbations qui ont fait ouvrir la soupape (ou qui ont eu un autre effet sur la soupape)
- les fuites de la soupape.

Pré-test de soupape de sécurité

112. L'entretien de la soupape de sécurité comprend-il l'exécution d'un pré-test?
113. A-t-on déterminé la pression à laquelle la soupape doit s'ouvrir sur le banc d'essai (« cold differentiel test pressure ») ?
114. Quelqu'un de l'entreprise assiste-t-il (de temps en temps) aux pré-tests des soupapes de sécurité?
115. Le rapport de test donne-t-il une évolution graphique du pré-test?
116. Y a-t-il une instruction qui décrit ce qu'il faut faire lorsqu'il est constaté que l'ors du pré-test, la soupape s'ouvre à une pression plus élevée ou plus faible que la « cold differentiel test pressure » ?
117. Ressort-il des rapports des pré-tests qu'en cas de déviations, des mesures correctives ont été prises ?
118. Peut-on déduire des résultats des pré-tests que l'intervalle d'entretien n'a pas été choisi trop grand ?

La pression à laquelle la soupape doit s'ouvrir sur le banc d'essai est la "cold differential test pressure". Cette pression peut diverger de la pression dans l'installation à laquelle la soupape commence à s'ouvrir dans le cas où des corrections sont nécessaires à cause de la contre-pression ou de températures élevées.
Dans le cas d'une contre-pression constante, le réglage du ressort d'une soupape de sécurité conventionnelle actionnée par ressort doit être adapté en fonction de la contre-pression. De telles soupapes de sécurité ne sont donc pas adaptées pour des contre-pressions variables. Dans ce cas, il faut utiliser des soupapes de sécurité balancées ("balanced").

L'objectif du pré-test est de vérifier à quelle pression la soupape de sécurité s'ouvre dans les conditions dans lesquelles elle se trouvait dans l'installation. Ce test donne donc des informations très importantes sur la fiabilité de la soupape.
La pratique montre que les résultats de tests moyens peuvent différer de façon significative en fonction de la présence ou non d'un témoin de l'entreprise.
Cela mérite de recommander que les tests des soupapes de sécurité aient lieu, si pas toujours, au moins à intervalles réguliers, en présence de la firme donneuse d'ordre. Une entreprise se doit en définitive de pouvoir démontrer que la qualité des inspections est garantie.
Une évolution graphique du pré-test donne une sécurité plus importante sur l'exécution correcte du pré-test.

Lorsque la soupape est très sale, on peut renoncer au pré-test car les petites particules peuvent endommager le siège de la soupape. L'intervalle d'inspection doit alors être diminué pour que lors du prochain entretien (on l'espère), l'état de la soupape soit suffisamment bon pour pouvoir réaliser un pré-test.

Il doit y avoir des critères fixés afin de juger d'un pré-test, à savoir les marges par rapport à la pression de tarage, au sein desquelles on peut considérer le pré-test comme réussi. Lorsque les résultats du pré-test se trouvent en dehors de ces marges, des actions correctives doivent être prises. Les causes de la pression d'ouverture divergente doivent être cherchées, ainsi que des mesures pour remédier à ces causes. Le cas échéant, la fréquence d'entretien de la soupape de sécurité doit être augmentée.

Entretien et réglage de soupapes de sécurité

119. L'entretien comprend-il un démontage et un nettoyage des composants ?
120. Après l'entretien et l'assemblage de la soupape, réalise-t-on à nouveau un ou plusieurs tests de pression pour s'assurer que la soupape s'ouvre bien à la pression de test (« cold differential test pressure »).
121. Réalise-t-on un test d'étanchéité après exécution de ce test de pression ?
122. Le rapport de test mentionne-t-il la pression à laquelle le test d'étanchéité a été réalisé et le résultat ?
123. Existe-t-il des critères clairs pour l'évaluation du test d'étanchéité ?
124. Dans le cas de soupapes de sécurité de type « balanced bellow », l'étanchéité du soufflet est-elle testée ?
125. La soupape a-t-elle été testée avant qu'elle ne soit mise en service pour la première fois ?

Certains producteurs conseillent de réaliser au moins 3 tests pop lors du réglage de la soupape. Lors du premier test pop, les composants de la soupape vont se « mettre en place ».

Le test d'étanchéité a lieu la plupart du temps à 90 % de la pression de test. Une méthode couramment utilisée pour déterminer l'étanchéité consiste à compter le nombre de bulles d'air qui s'échappent pendant une période donnée à travers la soupape de sécurité.

Pour le test d'étanchéité du soufflet d'une soupape de sécurité balancée, on peut utiliser une surpression limitée (par ex. 0,5 bar).

Avant que la soupape ne soit mise en service pour la première fois, il est nécessaire de réaliser un test pop pour s'assurer que la pression de tarage est correcte.

Inspection visuelle des soupapes de sécurité après démontage

126. Y a-t-il des instructions qui prévoient l'inspection visuelle de la soupape de sécurité après démontage hors de l'installation?
127. Y a-t-il des instructions qui prévoient une inspection visuelle des tuyauteries d'entrée et d'évacuation?
128. Les résultats de cette inspection visuelle sont-ils documentés?
129. Y a-t-il des instructions pour nettoyer les tuyauteries dans le cas d'un encrassement important?

Certains dépôts et produits de corrosion dans la soupape de sécurité peuvent tomber dehors pendant le transport. C'est pourquoi il est recommandé de réaliser l'inspection visuelle dès que la soupape est démontée hors de l'installation.

Montage et démontage de soupapes de sécurité

130. Dans le cas où une vanne d'isolation a été placée avant et/ou après la soupape de sécurité : a-t-on prévu une petite vanne d'évent pour évacuer la pression entre la vanne d'isolation et la soupape de sécurité ?
131. Y a-t-il des instructions pour le montage et le démontage des soupapes de sécurité?
132. Y a-t-il une instruction qui détermine si la soupape de sécurité doit être nettoyée ou non et comment cela doit se faire le cas échéant?
133. Le personnel qui place les soupapes de sécurité, est-il formé à ce sujet?

La pression dans l'espace entre la vanne d'isolation et la soupape de sécurité doit pouvoir être évacuée avant de réaliser un entretien.

Ci- dessous sont listés quelques aspects qui peuvent être abordés dans les instructions pour le montage et le démontage des soupapes de sécurité.

Aspects liés au montage des soupapes de sécurité

- les engins de levage qui sont éventuellement à mettre en œuvre pour apporter la soupape sur place.
- les joints à utiliser (dimensions et matériel). Les joints doivent laisser l'entrée et l'évacuation complètement libres, et doivent bien entendu être résistants à la pression et à la température qui règnent.
- l'élimination des arrêts dans les coiffes de ressort des soupapes de sécurité balancées ("plugs" dans les "bonnet vents").
- l'ouverture et le verrouillage (ou le scellement) des vannes manuelles après le montage de la soupape de sécurité.

Aspects liés au démontage des soupapes de sécurité

- les EPI à utiliser
- le nettoyage éventuel des soupapes de sécurité
- la manière dont la soupape de sécurité doit être isolée de l'installation (par ex. fermeture des vannes dans un ordre déterminé)
- la mise à l'évent de l'espace entre la vanne d'isolation et la soupape de sécurité
- l'isolation des tuyauteries d'entrée et d'évacuation ouvertes, après enlèvement de la soupape de sécurité

Dans certains cas, après démontage, la soupape peut contenir des substances dangereuses qui peuvent former un risque lors du transport et lors du test et du démontage. Un nettoyage de la soupape peut alors être indiqué. D'un autre côté, un nettoyage peut avoir une influence sur le pré-test.
Il faut donc bien réfléchir pour déterminer si la soupape doit être nettoyée et de quelle manière ce nettoyage doit avoir lieu.

Transport et stockage de soupapes de sécurité

134. Dispose-t-on d'instructions concernant le transport des soupapes?
135. Ces instructions demandent-elles que les soupapes de sécurité soient fermées avant le transport?
136. Ces instructions demandent-elles que les soupapes soient transportées en position debout?
137. Les soupapes de sécurité sont-elles stockées dans un endroit propre et sec?

La propreté est d'importance capitale pour le bon fonctionnement et l'étanchéité des soupapes de sécurité. L'introduction de saleté dans la soupape doit donc absolument être évitée.

Les soupapes de sécurité doivent être transportées en position debout.

Les soupapes de sécurité sont des appareils très délicats. Un traitement sans précaution peut compromettre l'étanchéité de la soupape ou le réglage correct. Les soupapes de sécurité devraient être transportées dans des équipements spéciaux et, par exemple, pas jetées en un tas sur une palette.

Ces prescriptions de transport sont valables aussi bien pour le transport de l'installation vers l'atelier d'entretien que pour le transport inverse.

Contrôle visuel des soupapes de sécurité en service

138. Les soupapes de sécurité sont-elles périodiquement soumises à des contrôles visuels?
139. Ces inspections sont-elles enregistrées?
140. Une inspection visuelle est-elle également menée après que la soupape se soit ouverte?
141. Pour les soupapes qui évacuent vers un système de recueil, vérifie-t-on également si elles fuient ?

Les aspects suivants (pour autant qu'ils soient d'application) peuvent êtres abordés lors de telles inspections:

- les vannes manuelles dans les tuyauteries d'entrée et d'évacuation sont en position ouverte et correctement verrouillées
- le scellé de la coiffe du ressort ou de la vis de réglage ("adjusting screw") du ressort est intact
- le scellé de l' « adjusting ring » avant la « huddling chamber » (au niveau du siège de la soupape) est intact
- la soupape ne fuit pas
- le soufflet (des soupapes de sécurité de type "balanced bellows" et "unbalanced bellow") ne fuit pas
- l'ouverture d'évent du soufflet ("bellow vent") et/ou de la coiffe du ressort (« bonnet vent ») est ouverte et libre
- les ouvertures de drainage dans le système d'évacuation ne sont pas bouchées
- le capot contre la pluie est présent
- le levier ("lifting levers") se trouve en position correcte et n'est pas attaché
- l' isolation est en bon état et l'éventuel chauffage fonctionne
- l'éventuel disque de rupture est orienté correctement.

Des détecteurs de flux à ultrasons peuvent être utilisés pour vérifier si une soupape de sécurité fuit vers un système d'évacuation. Des analyses des substances collectées par le système d'évacuation peuvent également être utilisées pour détecter des fuites.

Inspection des mesures de pression entre les disques de rupture et les soupapes de sécurité

142. Les mesures de pression entre les disques de rupture et les soupapes de sécurité sont-elles inspectées ?

Le fonctionnement correct de la mesure doit être contrôlé périodiquement. Si une alarme est transmise ou si une autre action est générée, cela doit bien entendu également être testé.

Inspections périodiques ou entretien des disques de rupture

143. Le disque de rupture est-il périodiquement inspecté et/ou remplacé?
144. Les tuyauteries d'entrée et d'évacuation sont-elles périodiquement inspectées?
145. Les éventuels systèmes-coupant sont-ils périodiquement inspectés?
146. Les résultats de ces inspections visuelles sont-ils documentés?

Lorsque la rupture prématurée d'un disque de rupture ne pose aucun problème, le disque de rupture peut en principe rester en service de façon illimitée. Sinon, le disque de rupture doit être remplacé périodiquement selon une fréquence basée sur l'information du producteur, et sur base de sa propre expérience d'utilisation.

Pour assurer que les tuyauteries d'entrée et d'évacuation sont complètement libres, il est important qu'il soit vérifié périodiquement qu'elles ne sont pas encrassées ou bouchées. Lorsque pour l'inspection des tuyauteries, le disque de rupture doit être enlevé de son support, le disque de rupture doit être remplacé, même s'il n'est pas fissuré ou abimé. Certains disques de rupture sont montés dans des supports qui peuvent être emportés en un tout, sans que la tension avec laquelle le disque de rupture est serré, ne change. De tels supports ont également l'avantage que les disques de rupture peuvent être montés dans le support en atelier, où les conditions pour l'exécution d'un tel travail délicat sont en général meilleures que dans l'installation.

Lors d'une inspection visuelle d'un système coupant, on examine si les couteaux sont encore suffisamment acérés.

Montage et démontage de disques de rupture

147. Dans le cas où une vanne d'isolation a été placée avant et/ou après le disque de rupture : a-t-on prévu une petite vanne d'évent pour évacuer la pression entre la vanne d'isolation et le disque de rupture ?
148. Y a-t-il des instructions pour le montage et le démontage des disques de rupture?
149. Le personnel qui place les disques de rupture, est-il formé à ce sujet?

La pression dans l'espace entre la vanne d'isolation et le disque de rupture doit pouvoir être évacuée avant de réaliser un entretien.

Ci-dessous sont listés quelques aspects qui peuvent être abordés dans les instructions pour le montage et le démontage des disques de rupture.

Aspects liés au montage des disques de rupture

- Le nettoyage approfondi des brides
- Les joints à utiliser (dimensions et matériel). Les joints doivent laisser l'entrée et l'évacuation complètement libres, et doivent bien entendu être résistants à la pression et à la température qui règnent.
- Instructions pour le serrage des supports de disques de rupture (outillage à utiliser, ordre des boulons, moment à exercer sur les boulons).
- l'ouverture et le verrouillage (ou le scellement) des vannes manuelles après le montage du disque de rupture.

Aspects liés au démontage des disques de rupture

- les EPI à utiliser
- la manière dont le disque de rupture doit être isolé de l'installation (par ex. fermeture des vannes dans un ordre déterminé)
- la mise à l'évent de l'espace entre la vanne d'isolation et le disque de rupture
- l'isolation des tuyauteries d'entrée et d'évacuation ouvertes, après enlèvement du disque de rupture

Inspection du système d'évacuation

150. Le système d'évacuation est-il repris dans un programme d'inspection?

Le système de décharge doit être inspecté en fonction du risque de corrosion. Le bon état des appuis des tuyauteries de décharge doit également être assuré.

3.3.2. Mise hors service

Isolation des tuyauteries d'entrée et d'évacuation

151. La tuyauterie d'entrée peut-elle être isolée (par exemple à l'aide d'une vanne manuelle)?
152. Le système d'évacuation (y compris l'éventuelle torchère) peut-il être isolé (par exemple à l'aide d'une vanne manuelle)?
153. Les vannes d'isolation sont-elles verrouillées en position ouverte ?
154. Y a-t-il une liste actualisée avec toutes les vannes d'isolation (ou brides à lunettes ou plateaux pleins) dans les tuyauteries d'entrée ou les systèmes d'évacuation des systèmes de décharge de pression ?
155. Cette liste mentionne-t-elle les raisons de la fermeture des vannes d'isolation ?
156. Y a-t-il des inspections périodiques pour vérifier si les vannes d'isolation sont dans la bonne position et si le verrouillage est toujours présent ?

La présence ou non de vannes d'isolation sur les tuyauteries d'entrée ou d'évacuation peut être constatée à l'aide des P&ID's et sur place dans l'installation.

Les vannes d'isolation doivent être verrouillées en position ouverte. Le verrouillage peut se faire avec des chaines et des cadenas, mais éventuellement aussi avec des colsons en plastique qui en cas d'urgence peuvent facilement être cassés pour fermer ou ouvrir la vanne sans qu'une clé ne soit nécessaire. On parle alors de "car sealed open" ou de "car sealed closed".

Sur certains P&ID's, il est noté si les vannes sont "locked open" ("lo") ou "locked closed" ("lc") avec l'indication des numéros de clés. Le verrouillage réciproque des vannes peut être indiqué via une ligne en pointillés qui relie les vannes.

La gestion administrative des vannes d'isolation est prescrite par l'API 520 part II.

Mise en service d'une soupape de réserve

157. Dans le cas où une soupape de réserve est montée sur le réservoir sous pression, les mesures nécessaires sont-elles prises pour assurer que la mise en et hors service des vannes ait lieu dans le bon ordre?
158. Dans le cas où l'on utilise une vanne à trois voies pour monter ensemble une soupape de réserve et la soupape active, y a-t-il une indication claire de quelle soupape est en service?

L'API 520 part II autorise aussi bien un verrouillage mécanique que des procédures administratives pour assurer l'ordre correct des manipulations lors de l'alignement de la soupape de réserve.

3.3.3. Modifications

Modification de la pression de tarage

159. La pression de tarage de la (des) soupape(s) de sécurité a-t-elle déjà été modifiée?
160. Cette modification est-elle documentée dans le dossier de la soupape de sécurité?
161. Cette modification a-t-elle eu lieu selon une procédure prévoyant les analyses nécessaires?

Un document de contrôle en bonne et due forme suppose qu'une modification de la pression de tarage soit notée sur le formulaire technique de la soupape (avec indication de la révision de la pression de tarage).
Dans le cas d'une modification, il convient de vérifier les raisons motivant la modification et si les analyses nécessaires ont été réalisées. Une telle modification doit dans tous les cas être considérée comme significative du point de vue de la sécurité et doit être exécutée suivant les procédures conformes de l'entreprise.

4

Questionnaire pour des sécurités instrumentales

4.1. Spécification de la mesure

4.1.1. Identification et fonctionnalité

Identification et documentation de spécification

1. La sécurité instrumentale a-t-elle un code d'identification univoque?
2. L'entreprise dispose-t-elle d'un document de spécification pour la sécurité instrumentale?
3. L'entreprise dispose-t-elle d'une représentation logique schématique (un "logic diagram")?

Pour documenter tous les aspects d'une sécurité instrumentale, un document de spécification doit être rédigé pour chaque boucle. Les aspects qui doivent y être abordés, ressortent des questions ci-dessous.

Dans ce questionnaire, on suppose que tous ces aspects sont documentés d'une manière claire dans un seul document. Si certaines entreprises documentent ces aspects dans différents documents, il faut vérifier dans quelle mesure la cohésion entre ces documents est garantie.

Une autre question fondamentale à ce sujet: quel est le document de base. De quoi part-on lors de l'implémentation de la sécurité instrumentale?

Fonctionnalité et causes initiales

4. Le document de spécification donne-t-il une description textuelle de la fonctionnalité de la sécurité instrumentale?
5. Le document de spécification mentionne-t-il les causes initiales, donnant lieu au fonctionnement de la sécurité instrumentale?

La base pour la fonctionnalité de chaque sécurité instrumentale est une description textuelle rédigée par un ingénieur process ou qui découle directement d'une analyse de risques.

Certaines entreprises décrivent la fonctionnalité des sécurités instrumentales via ce que l'on appelle des "cause and effect diagrams". Ces diagrammes définissent schématiquement (via un tableau) quels éléments finaux sont enclenchés en fonction de quelles mesures. Cependant, la pratique nous apprend que tous les aspects de la fonctionnalité d'une sécurité instrumentale ne peuvent pas être représentés dans un tel diagramme. C'est toujours le cas lorsque la fonctionnalité est complexe.

La fonctionnalité textuelle doit alors être traduite en une représentation schématique logique ("logic diagram") qui est clairement lisible par un programmeur. Un « logic diagram » est un outil important pour assurer que la fonctionnalité exigée sur base de l'analyse de risques soit bien programmée et non pas seulement comme le programmeur pense que la sécurité instrumentale doit travailler.
De plus, cela peut apporter aux opérateurs une représentation simplifiée et claire d'une logique qui peut être relativement complexe.

Il est très important de bien documenter quelles sont les causes initiales, en d'autres mots pour quelles circonstances déviantes la sécurité instrumentale doit offrir une protection. Cette information est nécessaire pour évaluer l'efficacité de la sécurité.

Il faut remarquer que "réaction de runaway" n'est pas une cause initiale. Une réaction d'emballement est la conséquence de certaines perturbations. La notion de "run away

reaction" est utilisée pour décrire toute une série de problèmes liés aux réactions. Ce que contient exactement cette réaction d'emballement, doit être clairement déterminé.

Paramètre de procédé surveillé

6. Le document de spécification mentionne-t-il le paramètre de procédé qui est surveillé par la sécurité instrumentale?
7. Le document de spécification mentionne-t-il la valeur limite (sûre) de ce paramètre?
8. Le document de spécification mentionne-t-il l'argumentation pour cette valeur?

Le paramètre de procédé surveillé est le paramètre qui doit être maintenu entre certaines limites par la sécurité instrumentale, par exemple une pression, une température, une concentration.

Dans beaucoup de cas, le paramètre surveillé sera également le paramètre mesuré. Il est cependant possible que le paramètre de procédé surveillé soit déduit d'une série d'autres mesures (par ex. via un calcul), lorsqu'il est difficile de mesurer directement le paramètre surveillé.
Pensez par exemple à la situation où une concentration doit être surveillée à partir d'une combinaison de mesures de la pression, de la température, des quantités et des débits.

La valeur limite sûre de ce paramètre n'est en principe pas égale à la valeur à laquelle la sécurité instrumentale va entrer en action, vu que la sécurité instrumentale intervient – en fonction du temps de réponse de la sécurité instrumentale – avant que cette valeur maximale ne soit atteinte. De plus, il peut y avoir plusieurs mesures qui surveillent le même paramètre (par ex. une sécurité instrumentale et une soupape de sécurité) et qui interviennent consécutivement.

Variable de procédé mesurée

9. Le document de spécification mentionne-t-il la variable de procédé mesurée et la valeur à laquelle la sécurité instrumentale est activée (valeur d'enclenchement)?
10. Le document de spécification mentionne-t-il la marge d'erreur acceptable sur la variable de procédé mesurée?
11. Le document de spécification mentionne-t-il pour chaque variable mesurée le code d'identification de l'élément de mesure?
12. Le document de spécification mentionne-t-il le voting pour les éléments de mesure?

Le paramètre de procédé mesuré est le paramètre de procédé servant d'input à la sécurité instrumentale.

La valeur d'enclenchement est la valeur du paramètre pour laquelle la sécurité instrumentale doit entrer en action.

La marge d'erreur est la déviation tolérée sur la valeur d'enclenchement. La marge d'erreur de l'appareil de mesure (voir plus loin) devra naturellement être plus petite.
Une marge d'erreur de, par exemple, 5% signifie que l'élément de mesure peut présenter une déviation de 5% avant de devoir être recalibré. Lors de la calibration, une précision de 5% est suffisante.

Certains appareils de mesure sont relativement plus sensibles à des déviations:

- pressiomètres
- mesures de différence de pression à travers un "orifice" (usure de l'ouverture dans le cas d'un fonctionnement érodant ou déviation due à l'obstruction du "tubing").

Relation entre variable surveillée et mesurée

13. La relation entre la valeur limite des variables mesurées et la valeur limite du paramètre surveillé est-elle claire?
14. Dans le cas où cette relation n'est pas évidente, a-t-elle alors clairement été documentée?

Si cette relation n'est pas clairement déterminée, l'efficacité de la sécurité ne peut pas être évaluée.

Variables manipulées et éléments finaux

15. Le document de spécification mentionne-t-il la variable manipulée, l'élément final et l'action de l'élément final?
16. Est-il clair quelles actions sont essentielles pour la fonction de sécurité et quelles actions ont plutôt un caractère complémentaire?
17. Le document de spécification mentionne-t-il l'ordre des actions et des éventuels retards?
18. Le document de spécification mentionne-t-il le voting pour les éléments finaux?

La variable manipulée est la variable qui est modifiée par la sécurité instrumentale pour influencer les paramètres surveillés. Cela peut par exemple être: le débit d'un certain flux de procédé.

Les éléments finaux sont en général des vannes mais peuvent également être des appareils électriques (moteurs, pompes). L'arrêt d'appareils électriques (pompes, moteurs) a lieu via le MCC ("motor control center").

Dans certains cas, une boucle instrumentale exécute plus d'actions que ce qui est nécessaire afin de réaliser la fonction de sécurité (prévenir que le paramètre surveillé ne soit dépassé). Ces actions complémentaires peuvent par exemple être prises pour éviter que d'autres sécurités ne soient sollicitées, pour éviter des dérèglements opérationnels, pour qu'un éventuel démarrage ultérieur se déroule plus facilement, pour limiter des dommages, etc.

Dans un tel cas, les actions qui sont essentielles pour la fonction de sécurité doivent être clairement identifiées. C'est important pour l'analyse de la fiabilité et de l'efficacité de la sécurité instrumentale.
Supposons par exemple qu'une sécurité instrumentale ferme cinq vannes. Il est quasi impossible de réaliser une sécurité qui fermera les cinq vannes avec une probabilité de défaillance de moins de 1 sur 10 par sollicitation. De plus, la probabilité de défaillance de la fermeture simultanée des 5 vannes est 5 fois plus élevée que la probabilité de fermeture d'une seule vanne.
Dans le cas où beaucoup de vannes sont commandées, il faut donc se poser la question de savoir si toutes les vannes sont aussi essentielles pour la réalisation de la fonction de sécurité. Dans le cas d'une réponse positive, se pose alors la question de savoir si l'installation a par contre bien été conçue.

Le voting de vannes peut au mieux être expliqués à l'aide d'un exemple. Dans le cas où 2 vannes sont fermées par la sécurité instrumentale, un voting de "2 de 2" (2oo2) signifie que les deux vannes doivent se fermer pour prévenir la situation dangereuse. Un exemple typique à ce sujet est un réservoir avec deux tuyauteries d'alimentation différentes, chacune équipée d'une vanne. Pour éviter le surremplissage ou une surpression, les deux vannes doivent se fermer. Réaliser une certaine fiabilité pour un voting 2oo2 (pour les éléments finaux) est cependant un plus grand défi que d'atteindre cette même fiabilité pour un voting 1oo2. Une configuration 1oo2 typique est une seule conduite d'alimentation avec 2 vannes en série. Si une seule des 2 se ferme, le scénario est évité.

Signalisation de l'activation

19. L'activation de la sécurité instrumentale est-elle signalée aux opérateurs dans la salle de contrôle?
20. Quelle réaction attend-t-on de l'opérateur?

Il est en effet important que les opérateurs sachent qu'une sécurité instrumentale a fonctionné.

Dans certains cas, il peut être nécessaire qu'ils doivent exécuter des manipulations complémentaires (par ex. contrôle sur place) après l'action automatique.

"Reset conditions" et "reset actions"

21. A quelles conditions doit-on satisfaire avant que les actions de la sécurité instrumentale puissent être débloquées (ce que l'on appelle les "reset conditions") et que le fonctionnement (normal) du procédé puisse être repris ?
22. De quelle manière réalise-t-on un "reset" d'une boucle de sécurité ("reset action")?
23. De quelle manière l'entreprise assure-t-elle que l'on examine systématiquement si, pour chaque sécurité instrumentale, des "reset conditions" ou "reset actions" particulières sont d'application?
24. Dans le cas où ces "reset conditions" ou "reset actions" divergent de la procédure standard, ces conditions ou manipulations sont-elles alors clairement identifiées?

Lorsque la sécurité instrumentale a fonctionné, le déroulement normal du procédé a été interrompu. Les "reset conditions" ou actions de réarmement sont les actions à prendre pour neutraliser l'effet de « blocage » de la sécurité instrumentale.
Le réarmement de la sécurité instrumentale peut se faire automatiquement ou manuellement (via le DCS, un bouton en salle de contrôle, ou localement).
Il est parfois recommandé de n'effectuer le réarmement qu'après un contrôle de la situation sur place.

Comportement au démarrage et à la mise à l'arrêt

25. La sécurité instrumentale peut-elle fonctionner de la même manière lors du démarrage ou de la mise à l'arrêt de l'installation que lors du fonctionnement normal de l'installation?
26. De quelle manière l'entreprise assure-t-elle que l'on examine systématiquement si le fonctionnement d'une sécurité instrumentale doit être adapté pendant le démarrage ou la mise à l'arrêt du procédé?
27. Dans le cas où le fonctionnement lors du démarrage et de la mise à l'arrêt diffèrent du fonctionnement en conditions normales, ces conditions ont-elles alors clairement été documentées?

Les sécurités au démarrage des fours et des chaudières en sont un exemple typique. Le démarrage de ces installations doit aller de paire avec des sécurités spécifiques (par exemple un cycle de rinçage).

4.1.2. Efficacité

Effet de l'action sur le procédé

28. Peut-il être démontré que l'action exécutée par la sécurité instrumentale (le changement de la variable manipulée) mène à l'effet souhaité?

Dans certains cas, ceci n'est pas évident. Pensez par exemple au refroidissement d'urgence d'un réacteur. Dans de tels cas, l'entreprise doit démontrer (par ex. à l'aide de calculs ou d'échantillons) que l'action réalisée est bien efficace.

Un autre exemple: la mise à l'arrêt d'une pompe centrifuge ne ferme pas un flux de procédé s'il reste une différence de pression au travers de la pompe.

Fonctionnement à temps de la sécurité

29. Examine-t-on systématiquement si le temps de réaction des sécurités instrumentales est critique ?
30. A-t-on examiné si la sécurité instrumentale est activée suffisamment à temps pour éviter que le paramètre surveillé ne dépasse sa valeur critique ?
31. A-t-on estimé pour ce faire avec quelle vitesse le paramètre surveillé évolue dans la direction de sa valeur critique ?
32. A-t-on estimé pour ce faite le temps entre le moment où l'on atteint la valeur de déclenchement (dans l'installation) et la détection de cette valeur par l'élément de mesures ?
33. A-t-on estimé pour ce faire le temps nécessaire pour traiter l'information des mesures et pour envoyer un signal aux éléments finaux ?
34. A-t-on tenu compte pour ce faire du temps nécessaire pour faire fonctionner les vannes ?
35. A-t-on tenu compte pour ce faire du temps dont a besoin l'action pour réaliser l'effet souhaité ?

Vérifier systématiquement si le temps de réaction d'une sécurité instrumentale est critique, peut être réalisé en prévoyant un champ d'information à ce sujet sur le document de spécification.

Un aspect important lié au temps de réaction de la boucle est la valeur de déclenchement. Plus la valeur de déclenchement de la boucle est éloignée de la valeur critique (qui ne peut pas être dépassée), plus la sécurité instrumentale fonctionne tôt et plus il y a de temps pour réaliser l'action corrective.

Certaines mesures peuvent être relativement lentes, comme par exemple les mesures de température incorporées dans un « thermowell ».

Le temps nécessaire pour traiter le signal mesuré, se situe entre 2 à 3 secondes pour des systèmes DCS. . Lorsqu'un grand nombre d'alarmes arrivent en même temps, le temps de réaction peut augmenter dans un système DCS. Avec un système ESD, le temps de réaction se chiffre à environ 100 à 500 msec.

Le temps d'enclenchement des vannes peut varier de 1 sec à quelques minutes (grosses vannes, vannes électriques,...). Ce temps doit toujours être mentionné sur la feuille de spécification de la vanne ("instrument specification").

Etanchéité aux fuites de la vanne

36. L'étanchéité interne (aux fuites) de la vanne est-elle critique?
37. Quelle est la classe de fuite de la vanne?
38. L'entreprise utilise-t-elle un standard interne en ce qui concerne la classe de fuite des vannes?

Aucune vanne n'est étanche à 100%. Les fuites internes découlent des propriétés inhérentes à la vanne et de l'usure. L'étanchéité interne de la vanne est une mesure de la fuite interne dans celle-ci. Il peut, dans certains cas, s'avérer important qu'absolument aucun produit (même pas un débit de fuite négligeable) ne puisse s'échapper de la vanne lors de la fermeture de celle-ci.
La norme ANSI/FCI 70 2 1976 (R1982) définit 6 classes d'étanchéité. Les classes les plus courantes sont les suivantes:

- CLASS IV: métal sur métal (metal plug on a metal seat)
- CLASS VI: soft seat (plug and or seat in composition material (entres autres Teflon).

Les vannes de contrôle ont d'ordinaire une classe d'étanchéité plus basse que les vannes d'arrêt. Du fait qu'elles sont d'ordinaire également plus sollicitées, elles s'usent également plus vite que les vannes d'arrêt.

4.1.3. Indépendance

Indépendance des éléments de mesure

39. La sécurité instrumentale peut-elle être activée à la suite de la défaillance des éléments de mesure faisant partie des boucles de contrôle?
40. Si oui, les éléments de mesure faisant partie de la sécurité instrumentale sont-ils différents et complètement séparés des éléments de mesure des boucles de contrôle concernées?

Lorsque la sécurité instrumentale doit fournir une protection contre une situation qui peut être occasionnée par une mesure erronée, cette même mesure ne peut en effet pas faire partie de la sécurité.

La séparation des mesures signifie par exemple qu'elles ne peuvent pas être montées sur la même déviation. En cas d'obstruction de la déviation, les 2 mesures sont alors touchées.

Indépendance de l'organe décisionnel

41. La sécurité instrumentale peut-elle être activée à la suite d'une faute dans l'organe décisionnel utilisé pour le contrôle du procédé?
42. L'organe décisionnel de la sécurité instrumentale est-il différent et complètement séparé de l'organe décisionnel pour le contrôle du procédé?

Si la sécurité instrumentale doit offrir une protection contre une situation qui peut être occasionnée par une faute dans un organe décisionnel (par ex. un système DCS), ce même organe de contrôle ne peut en principe pas faire partie de la sécurité.
En pratique, cela signifie que des organes décisionnels séparés sont utilisés pour le contrôle et la sécurité.
Certaines entreprises intègrent quand même des systèmes de contrôle et le système de sécurité, malgré le fait que cela va à l'encontre des standards et recommandations en la matière (y compris de l'IEC61511 et de l'IEC61508). De telles entreprises doivent être capables de démontrer elles-mêmes (à l'aide d'une enquête approfondie) que les probabilités de modes communs de défaillance dans les systèmes de contrôle et de sécurité ont été suffisamment restreintes.

Indépendance des éléments finaux

43. La sécurité instrumentale peut-elle être activée à la suite d'une défaillance d'éléments finaux utilisés dans des boucles de contrôle?
44. Si oui, les éléments finaux utilisés dans la sécurité instrumentale sont-ils différents et complètement séparés de ces éléments finaux?

Si la sécurité instrumentale doit fournir une protection contre une situation qui peut être occasionnée par une faute dans un élément final (par ex. une vanne qui se bloque dans une position déterminée), ce même élément final ne peut en effet pas faire partie de la sécurité.

La séparation des éléments finaux signifie que différents solénoïdes sont utilisés.

4.1.4. Fiabilité

Fiabilité souhaitée

45. La fiabilité souhaitée de la sécurité instrumentale a-t-elle été déterminée sur base d'une évaluation du risque?
46. Quelle est la fiabilité souhaitée de la sécurité instrumentale?
47. Quelle est la réduction totale du risque des couches de protection?

Une évaluation des risques objective et consistante n'est pas possible sans que l'on se forme une certaine idée de la fiabilité des mesures, et de la probabilité et de la gravité des conséquences.

La fiabilité souhaitée ou postulée de la sécurité instrumentale est déterminée sur base d'une évaluation des risques.
Si la fiabilité postulée n'est pas déterminée, l'entreprise ne peut pas non plus démontrer qu'elle a pris les mesures nécessaires.

La fiabilité souhaitée peut être exprimée de différentes manières:

- Niveau SIL: 1, 2 ou 3
- Réduction du risque: un nombre entre 1 et ∞
- Probabilité de défaillance ou "PFD" ("probability of failure on demand"): un chiffre entre 0 et 1.

Documentation et gestion de l'évaluation des risques

48. Ces évaluations des risques sont-elles bien documentées?
49. Le formulaire d'évaluation des risques est-il un document contrôlé?
50. L'entreprise dispose-t-elle de critères clairs pour l'exécution d'une évaluation des risques?
51. Les critères ont-ils été approuvés par la direction?

Une bonne documentation de l'évaluation des risques comprend:

- une bonne description des causes (l'évènement initial ou la condition qui donne lieu au scénario)
- une estimation de la probabilité de l'évènement initial
- une description des conséquences possibles du scénario (l'évènement dont la gravité est estimée)
- une estimation de la gravité des conséquences du scénario
- une énumération de toutes les couches de protection (indépendantes)
- une estimation de la fiabilité des couches de protection.

C'est une bonne pratique que l'évaluation d'un scénario déterminé soit réalisée par différentes personnes. Pour des raisons pratiques (emploi du temps), cette évaluation a souvent lieu séparément de l'identification du risque, lors d'une réunion à part.

Une bonne documentation de l'évaluation des risques ne comprend pas uniquement le résultat final mais aussi les éléments qui contribuent à la décision.

Des mesures doivent être prises pour assurer que la décision prise en groupe, ne puisse pas être modifiée sans plus par après. C'est pourquoi il est recommandé de faire signer, l'enregistrement de l'évaluation des risques (pour chaque scénario), par les participants à la décision.

Les critères d'évaluation du risque déterminent directement le niveau de sécurité vers lequel tend l'entreprise et c'est pourquoi, ils doivent être formellement approuvés par la direction.

Fréquence de sollicitation

52. Quelle est la fréquence de sollicitation estimée?
53. Avec quelle fréquence la sécurité a-t-elle effectivement déjà été activée?
54. La sollicitation de la sécurité est-elle enregistrée?

La fréquence de sollicitation (« demand rate ») est la fréquence à laquelle il sera fait appel à la mesure.
On fait la différence entre, d'une part, une fréquence de sollicitation basse (« low demand mode ») et d'autre part, une fréquence de sollicitation élevée ou continue (« high or continuous demand mode »). Pour une fréquence de sollicitation basse, la fiabilité de la sécurité instrumentale est exprimée en tant que PFD (« probability of failure on demand »). Pour une fréquence de sollicitation élevée, la fiabilité est exprimée en tant que probabilité de défaillance par unité de temps (heures ou années).

Selon l'IEC61508, on peut parler de fréquence de sollicitation basse si celle-ci n'est pas plus élevée que 1 fois par an, ET qu'elle ,'est pas plus grande que 2 fois la fréquence de test. Des fréquences plus importantes sont à considérer comme des fréquences de sollicitation élevées.

Le nombre de fois qu'une sécurité instrumentale est sollicitée devrait d'une façon ou d'une autre être enregistré. Sur base de cet enregistrement, on pourra déduire si la fréquence de sollicitation estimée concorde avec les données expérimentales.
Il est possible qu'à cause de modifications dans le déroulement du procédé, une sécurité instrumentale existante puisse être sollicitée plus fréquemment. Pensez par exemple, à un réservoir remplacé par un autre de plus petite capacité. Si les débits entrants restent les mêmes, la protection de niveau haut sera éventuellement sollicitée plus fréquemment. De nombreuses entreprises ne définissent pas la fréquence de sollicitation de leurs fonctions de sécurité.

Redondance pour les sécurités SIL2

55. Dans le cas où la boucle doit répondre à la classe de fiabilité SIL2, a-t-on au moins prévu 2 mesures et 2 éléments finaux (mesures et éléments finaux dans une architecture 1oo2)?
56. Si non, quelle explication donne-t-on à ce sujet et cette explication est-elle conforme à l'IEC61508 ou IEC61511?

Le standard IEC61511 demande pour une sécurité instrumentale avec un niveau de fiabilité "SIL2", une tolérance aux fautes minimale de 1 pour les mesures et les éléments finaux, à condition, il est vrai, que lorsqu'une faute intervient, il y ait plus de 50% de chance que la faute ne crée pas de situation non sûre, ou que la faute soit détectée.

La tolérance aux défauts (« hardware fault tolerance ») est la mesure dans laquelle un composant déterminé ou un sous-système de la sécurité instrumentale résiste à l'apparition de défauts (en dépit de la probabilité d'apparition de ceux-ci) sans que la sécurité instrumentale ne perde sa fonctionnalité en matière de sécurité à cause de cette faute.

Une tolérance aux défauts de 1 pour les mesures signifie qu'un seul défaut dans les mesures (la défaillance d'1 mesure), ne peut pas engendrer la perte de la fonction de sécurité de la sécurité instrumentale. Cela signifie dans la pratique qu'il faut prévoir 2 mesures dans une architecture 1oo2. Une tolérance aux fautes de 1 pour des éléments finaux suppose 2 éléments finaux dans une architecture 1oo2.

La tolérance aux défauts est en fin de compte une condition complémentaire attribuée à la sécurité instrumentale en plus de la fiabilité. Dans la terminologie des standards IEC61508 et IEC61511, il s'agit là de ce que l'on appelle des "architectural constraints". Cette condition supplémentaire a été introduite pour compenser d'éventuels manquements dans

la conception de la sécurité instrumentale, à la suite d'hypothèses faites pendant la conception et aussi pour tenir compte des incertitudes dans les probabilités de défaillance utilisées dans les calculs de fiabilité. En d'autres mots, les "architectural constraints" freinent une confiance exagérée dans l'exactitude des probabilités de défaillance et des modèles de calcul.

On peut déroger à la règle donnée ci-dessus sous certaines conditions. Une tolérance aux fautes de 0 est alors quand même acceptable pour une sécurité de SIL2. Une des conditions pour cette dérogation est que l'entreprise dispose de suffisamment d'expérience, de laquelle il doit ressortir que l'élément de mesure ou l'élément final est adéquat pour être utilisé dans une sécurité instrumentale. Le standard IEC61511 attend qu'une entreprise dresse une liste avec des instruments de mesure et des éléments finaux approuvés (pour des conditions de procédé déterminées) et ce, sur base d'une vaste expérience avec ces composants. Cette liste doit être actualisée périodiquement.

Une entreprise peut également choisir de suivre les critères en matière de tolérance aux fautes du standard IEC61508. Selon le standard IEC61508, le niveau de tolérance aux fautes est fonction de la classe SIL, de la complexité de l'équipement et de la "safe failure fraction" (SFF) de l'équipement.

Redondance pour des boucles SIL3

57. Dans le cas où une boucle doit répondre à la classe de fiabilité SIL3, a-t-on prévu au minimum 3 mesures et 3 éléments finaux (mesures et éléments finaux dans une architecture 1oo3)?
58. Si non, quelle explication donne-t-on à ce sujet et cette explication est-elle conforme à l' IEC61508 ou IEC61511?

Le standard IEC61511 demande pour une sécurité instrumentale avec un niveau de fiabilité "SIL3", une tolérance aux fautes minimale de 2 pour les mesures et pour les éléments finaux (à condition que le mode de défaillance dominant est sûr ou détecté).

On peut déroger à la règle donnée ci-dessus sous certaines conditions. Une tolérance aux fautes de 1 est alors quand même acceptable pour une sécurité de SIL3. Une des conditions pour cette dérogation est que l'entreprise dispose de suffisamment d'expérience, de laquelle il doit ressortir que l'élément de mesure ou l'élément final est adéquat pour être utilisé dans une sécurité instrumentale. Le standard IEC61511 attend qu'une entreprise dresse une liste avec des instruments de mesure et des éléments finaux approuvés (pour des conditions de procédé déterminées) et ce, sur base d'une vaste expérience avec ces composants. Cette liste doit être actualisée périodiquement.

Une entreprise peut également choisir de suivre les critères en matière de tolérance aux fautes du standard IEC61508. Selon le standard IEC61508, le niveau de tolérance aux fautes est fonction de la classe SIL, de la complexité de l'équipement et de la "safe failure fraction" (SFF) de l'équipement.

Autodiagnostic

59. Les mesures sont-elles équipées d'un autodiagnostic?
60. Les éléments finaux sont-ils équipés d'un autodiagnostic?
61. L'organe décisionnel est-il équipé d'un autodiagnostic?

L'autodiagnostic pour des mesures peut être réalisé par comparaison avec d'autres mesures. On peut ainsi par exemple, comparer une mesure utilisée pour le contrôle avec une mesure utilisée dans une sécurité instrumentale. Dans le cas d'une architecture MooN (avec N>1), on peut également comparer les N mesures entre elles.
Certains appareils de mesure sont pourvus d'un autodiagnostic.
Le diagnostic peut améliorer la fiabilité d'une mesure d'un facteur 10 ou plus.
Certains appareils de mesure n'offrent aucune possibilité de diagnostic: une mesure de

niveau via un flotteur par exemple, un indicateur de niveau magnétique ou un manomètre à contact. Seul un 'life test' peut fournir à 100% des renseignements sur le fonctionnement de telles mesures.

Pour des vannes de contrôle, un certain degré d'autodiagnostic est possible. En effet, si une vanne de contrôle ne régule plus, cela sera repéré par les opérateurs dans certains procédés.

Pour les vannes d'arrêt ("on/off valves"), le diagnostic n'est possible que via ce que l'on appelle un "partial stroke monitoring". Lors de ce test, la vanne est déplacée rapidement de 10 à 20%. Cela ne permet pas de tester l'entièreté du fonctionnement de la vanne mais permet cependant de détecter un certain nombre de défaillances de celle-ci, surtout le fait pour l'élément mobile de rester collé sur son siège. Le désavantage d'un tel test réside dans le fait qu'il peut être la cause du fonctionnement non désiré d'une sécurité instrumentale, et que seulement une partie des défaillances possibles sont détectées.

Les PLC's de sécurité sont caractérisés par un degré très élevé d'autodiagnostic (plus de 99% des défauts possibles sont détectés et signalés).
Les systèmes relais ne disposent d'aucun diagnostic interne. Le risque existe toutefois que les contacts des contacteurs restent « collés ». Ceci n'est donc pas détecté automatiquement. Il existe cependant des relais approuvés SIL2 et SIL3.

Un désavantage supplémentaire des systèmes relais est que l'on ne peut pas rattacher simplement ainsi des mesures analogiques à un relais. Un relais attend en effet un signal digital comme input. Il faut donc installer un limitateur (trip amplifier) entre les instruments de mesure et le relais, qui traduit le signal analogique de la mesure (typiquement 4mA- 20mA) en un signal digital. La fiabilité de ce limitateur doit également être incorporée dans les calculs de fiabilité.

Note de calcul

62. L'entreprise dispose-t-elle d'une note de calcul qui démontre la fiabilité de la boucle?

La fiabilité d'une sécurité instrumentale peut être calculée à partir des probabilités de défaillance des composants, des intervalles de test et des temps de réparation. Lors du calcul, il faut également tenir compte du voting et des éventuels modes communs de défaillance.

Le fait de fixer une valeur-cible quantitative pour la fiabilité permet d'avoir un but objectif, afin d'évaluer une conception déterminée et de la comparer avec d'autres réalisations techniques. Cependant, il est important d'être conscient que beaucoup de modes de défaillance potentiels d'une sécurité instrumentale ne sont pas quantifiables. Pour les modes défaillances que l'on peut quantifier, les chiffres disponibles ne sont que des estimations. Afin d'éviter de faire trop confiance aux calculs (qui peuvent donner une image trop optimiste de la fiabilité) lors de la conception de sécurités, une série de conditions supplémentaires en matière de tolérance aux défaillances ont été formulées dans l'IEC61511. Ces conditions ont déjà été abordées plus haut dans les questions sur la redondance pour les boucles SIL2 et SIL3.

Probabilités de défaillance

63. Quelle est l'origine des probabilités de défaillance utilisées dans la note de calcul pour les éléments de mesure, l'organe décisionnel et les éléments finaux?
64. Lors du calcul, a-t-on également tenu compte de la probabilité de défaillance des solénoïdes?

Plusieurs types de mesures ont une fiabilité basse:

- les manomètres de type Bourdon.
  Les manomètres de type Bourdon peuvent être équipés de contacts

électriques. Le signal peut alors être utilisé dans des sécurités instrumentales. L'emploi de telles mesures pour des applications de sécurité est à déconseiller.
- manomètres à contact.
  Les manomètres à contact peuvent donner relativement vite des valeurs erronées. C'est pourquoi l'utilisation de tels manomètres pour des applications de sécurité est à déconseiller. Beaucoup d'entreprises ont déjà remplacé ce type de mesure.
- indicateurs de niveau magnétiques en verre
- contacteurs de niveau à flotteur.
  Les contacteurs de niveau à flotteur peuvent poser plusieurs problèmes: le flotteur peut fuir (détérioration lors du montage) ou peut avoir été oublié lors du montage.

De manière générale, les contacteurs digitaux sont de plus en plus remplacés par des mesures continues. Si des contacteurs digitaux sont quand même encore utilisés dans de nouvelles installations, ils devraient être équipés d'autodiagnostic.

Beaucoup de PLC's de sécurité (récents) sont livrés avec un certificat pour un usage dans une sécurité instrumentale avec un niveau SIL 2 ou 3.

Le solénoïde transpose le signal électrique (provenant de l'organe décisionnel) en un signal pneumatique. La probabilité de défaillance d'un solénoïde est du même ordre de grandeur que la probabilité d'une vanne de procédé.

Modes communs de défaillance

65. Dans le cas où plusieurs éléments de mesure ou éléments finaux sont utilisés, a-t-on tenu compte d'un facteur pour l'occurrence de fautes communes (le facteur appelé "beta-factor")?
66. Comment ce facteur a-t-il été déterminé?

Le "beta factor" ou "common cause factor" donne la dépendance réciproque des composants faisant partie d'un même élément de la sécurité instrumentale (mesures, organe décisionnel ou éléments finaux). Ce facteur (symbole β) doit être complété dans les formules pour des architectures plus élevées (MooN avec $M,N \geq 2$).
La norme IEC61508 donne un tableau dans lequel le facteur beta peut être déterminé. Le tableau donne des valeurs de 1, 2, 5 ou 10%. Le facteur β peut aussi être calculé.

Intervalles de test et temps de réparation

67. Tient-on compte dans les calculs des intervalles de test (effectifs) pour les mesures, l'organe décisionnel et les éléments finaux?
68. Tient-on compte dans les calculs des temps de réparation pour les éléments de mesures, les éléments finaux et l'organe décisionnel?

Les temps de réparation doivent être réalistes et tenir compte du fait que l'installation doit oui ou non être mise à l'arrêt pour faire la réparation. De plus, il faut également tenir compte de la disponibilité de personnel qualifié et des pièces nécessaires.

Couverture de diagnostic

69. Tient-on compte dans les calculs du "diagnostic coverage" (DC) des éléments de mesure, de l'organe décisionnel et des éléments finaux? Comme alternative du "diagnostic coverage", peut-on compter sur la "safe failure fraction" (SFF) (SFF et DC peuvent être déduits l'un de l'autre)?

L'autodiagnostic est la réalisation de tests automatisés (parfois continus) pour vérifier qu'un composant fonctionne encore correctement.

Le degré selon lequel les défauts de hardware peuvent être automatiquement détectés est exprimé en tant que "diagnostic coverage" (abréviation: DC). Il s'agit de la diminution en pour cent de la probabilité que des défauts dangereux (non détectés) puissent survenir. Le DC est un paramètre qui peut être introduit dans le calcul de fiabilité.

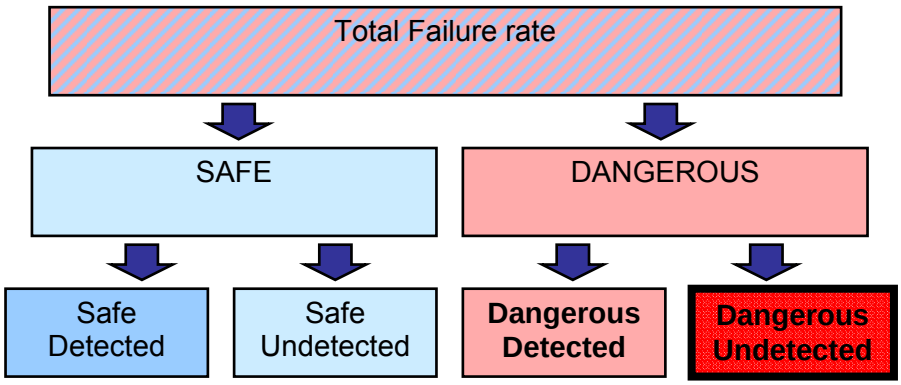
Si des mesures sont comparées entre elles, le "diagnostic coverage" est typiquement mis égal à 90%.

Pour des vannes "on/off", le DC est égal à 0, à moins que du "partial stroke testing" ne soit appliqué. Dans la littérature, la plupart du temps, on attribue un DC de 60% dans le cas de « partial stroke testing", bien que des valeurs plus élevées se rencontrent également. La pratique démontre cependant que certaines vannes se ferment, mais pas complètement. Ceci n'est alors pas détecté par "partial stroke testing".

Pour des vannes de régulation, on peut introduire un facteur pour le DC si la défaillance de la vanne est (suffisamment rapidement) détectée par les opérateurs.

Les PLC's de sécurité ont typiquement un DC plus grand que 99%.
Les relais n'ont pas d'autodiagnostic (DC = 0).

La figure et la formule ci-dessous illustrent la notion de « safe failure fraction » et de « diagnostic coverage ».



$$\text{Safe Failure Fraction} = \frac{\Sigma \text{ Safe failure rate} + \Sigma \text{ DD failure rate}}{\Sigma \text{ Total failure rate}}$$

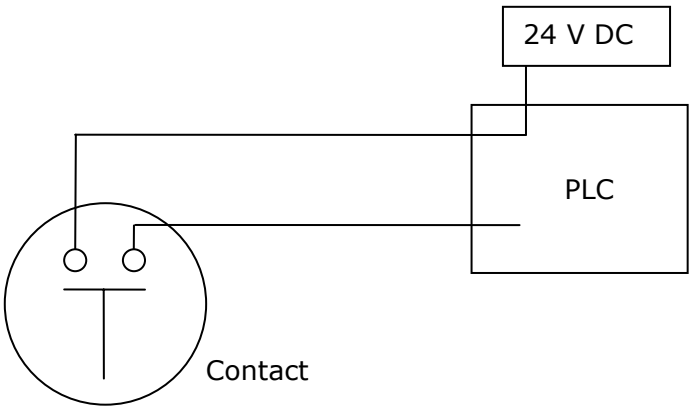
$$\text{Diagnostic coverage} = \frac{\Sigma \text{ Safe detected rate} + \Sigma \text{ Dangerous detected failure rate}}{\Sigma \text{ Total failure rate}}$$

4.1.5. Comportement lors de défaillance

Comportement en cas de rupture de fil

70. En cas de rupture de fil, la sécurité est-elle alors activée ou la faute est-elle signalée aux opérateurs?
71. Dans le cas d'un contacteur (mesure discrète ou "switch"): le signal qui est envoyé vers l'organe décisionnel est-il différent de 0 lorsque le paramètre de procédé surveillé a une valeur sûre?
72. La feuille de spécification mentionne-t-elle le comportement souhaité de la sécurité instrumentale en cas de rupture de câble ?

Pour le contacteur, le schéma ci-dessous peut apporter des éclaircissements.



Supposons que le contact est ouvert lorsque le paramètre surveillé (pression, niveau, …) a une valeur sûre. Le PLC reçoit alors 0 V comme signal. Si le paramètre surveillé dépasse la valeur sûre, le contact se ferme et le PLC reçoit un signal de 24 V. En cas de rupture de fil, le PLC continue à recevoir le signal 0 V et il existe donc une faute non détectée. Pour réaliser un mode de défaillance sûre, le contact doit donc être fermé lorsque le paramètre a une valeur sûre et ouvert lors d'une valeur non sûre. 0 V correspond alors à un signal "non sûr". On parle dans ce cas d'un "contact normalement fermé". Cela signifie qu'en conditions normales, le contact est fermé.

Comportement lors du diagnostic d'une faute dans l'élément de mesure

73. Dans le cas où l'élément de mesure dispose d'un autodiagnostic: lors de la détection d'une faute, la sécurité est-elle activée ou une alarme est-elle générée vers les opérateurs?
74. La feuille de spécification mentionne-t-elle le comportement souhaité de la sécurité instrumentale en cas de valeurs de mesure divergentes ?

La plupart des mesures continues envoient un signal électrique vers l'organe décisionnel, qui (lorsque la valeur mesurée reste dans sa portée) se situe entre 4 mA et 20 mA. Si le signal tombe en-dehors de cet intervalle, il s'agit d'une indication que quelque chose ne va pas.

Lorsque le câble de l'alimentation électrique vers l'instrument de mesure se rompt, le signal de l'instrument de mesure vers l'organe décisionnel retombe bien entendu à 0 mA. La même chose a lieu lors de la rupture du fil allant de l'instrument de mesure vers l'organe décisionnel.
Des instruments de mesure programmables peuvent être programmés de sorte que lors d'une faute détectée, ils envoient un signal qui est > à 20 mA ou < 4 mA.
La question qui se pose ici est comment l'organe décisionnel réagit à de telles valeurs extrêmes.

Un exemple peut éclaircir ceci. Supposons que l'organe décisionnel doit s'enclencher lors d'un niveau haut (90% du champ de mesure). L'organe décisionnel exécute l'action (fermeture d'une vanne sur l'alimentation) lorsqu'il reçoit un signal de 18,8 mA (16 mA x 0,9 + 4mA). Si l'instrument de mesure est réglé de manière à ce que lors de la détection d'une faute, il envoie une valeur élevée (20 mA ou plus), la boucle sera activée en cas de faute (signal > 18,8 mA). Ceci est favorable pour la sécurité mais pas pour la productivité. Il est également possible que l'instrument soit réglé de sorte qu'il envoie une valeur faible vers l'organe décisionnel (plus petit que 4 mA). A ces faibles valeurs, différentes réactions de l'organe décisionnel sont possibles (en fonction de la programmation):

- rien (ce qui en fait n'est pas acceptable parce qu'une faute a été détectée sans qu'une action ne soit prise)
- la génération d'une alarme (cela permet de réparer la mesure sans que l'installation ne soit mise à l'arrêt par la boucle de sécurité)
- activation de la fonction de sécurité.

Position de sécurité des actuateurs pneumatiques

75. La feuille de spécification de la sécurité mentionne-t-elle la position de sécurité en cas de perte d'air comprimé (il s'agit de la position de sécurité pneumatique)?
76. La feuille de spécification de la sécurité mentionne-t-elle la position de sécurité en cas de perte d'alimentation électrique vers le solénoïde (il s'agit de la position de sécurité électrique)?
77. Si les positions de sécurité pneumatique et électrique sont différentes, les raisons ont-elles été documentées?
78. Les positions de sécurité électrique et pneumatique des vannes sont-elles les mêmes que la position de sécurité de la vanne, c'est-à-dire la position dans laquelle les vannes sont enclenchées par la sécurité instrumentale?
79. Si non, les raisons en sont-elles documentées?
80. Est-il souhaitable que les vannes puissent encore être commandées en cas de perte d'air comprimé?
81. A cette fin, dispose-t-on d'un réservoir d'air comprimé local?
82. Contrôle-t-on régulièrement si la pression est suffisante dans ce réservoir d'air comprimé ou est-ce suivi en continu à partir de la salle de contrôle?

L'actuateur est le moteur de la vanne. Pour les actuateurs pneumatiques, on peut faire une distinction entre les actuateurs du type simple effet "spring return" et ceux du type double effet "double acting". Pour les actuateurs du type "spring return", un ressort repousse la vanne dans une position définie en cas de rupture d'alimentation en air comprimé (c'est la position de sécurité de la vanne). Pour les actuateurs pneumatiques du type double effet, la vanne reste dans sa dernière position à moins qu'un récipient d'air comprimé n'ait été prévu sur place. Le récipient d'air comprimé est raccordé de façon telle qu'il entre automatiquement en service en cas de défaillance du réseau d'air comprimé et qu'il est constamment maintenu sous pression par ce réseau. Si cependant, la liaison pneumatique entre le récipient sous pression et la vanne a été endommagée, la vanne ne se fermera plus.

Le solénoïde transforme un signal électrique (provenant de l'organe décisionnel) en un signal pneumatique. En conséquence de l'enclenchement du solénoïde, l'air comprimé sera envoyé vers l'actuateur ou la pression d'air comprimé de l'actuateur sera éventée. Ici se pose donc la question de savoir ce qui se passe avec la pression d'air comprimé vers l'actuateur si aucun courant ne va vers le solénoïde.
Si la position de sécurité électrique n'est pas spécifiée, on en déduit la plupart du temps qu'elle est identique à la position de sécurité pneumatique.

Lorsque la position de sécurité ne peut pas être déterminée de manière univoque ou lorsqu'il y a un grand conflit entre l'opérabilité et la sécurité, il peut être souhaitable que les vannes puissent encore être commandées en cas de perte d'air comprimé.
Considérons par exemple une vanne faisant partie d'un système de décharge de pression (Emergency Depressurisation System) qui est ouverte par une protection instrumentale en cas de surpression. La dépressurisation (vers l'atmosphère ou vers un système de réception) en cas de rupture d'alimentation en air comprimé, peut se révéler indésirable vis à vis de l'opérabilité et/ou de la sécurité. Dans le cas d'une telle vanne "ormalement ouverte" (fail open), il reste naturellement nécessaire que celle-ci reste, en cas de rupture d'alimentation en air comprimé, manœuvrable par la sécurité instrumentale.
On peut, dans de tels cas, prévoir un récipient d'air comprimé (ou d'azote) sur place ou une alternative au réseau d'air comprimé. Dans ce dernier cas, on bascule automatiquement (via une vanne à trois voies) du réseau d'air comprimé vers le réseau d'azote, par exemple, dès que la rupture d'alimentation en air comprimé a été détectée.
Il va de soi que la pression du récipient local ou du réseau alternatif doit être surveillée (par des contrôles périodiques, des alarmes, …).

Position de sécurité des vannes avec des actuateurs électriques

83. La feuille de spécification de la sécurité mentionne-t-elle la position de sécurité de la vanne en cas de perte de courant électrique (vers l'actuateur)?
84. Est-il souhaitable que les vannes puissent encore être alimentées en cas de perte de courant?
85. Si oui, comment est-ce réalisé en pratique (par ex. un générateur de secours)?
86. Comment une défaillance locale dans la vanne manœuvrée électriquement devrait-elle être détectée?
87. Dans le cas où la vanne est utilisée dans des scénarios où le feu peut intervenir: les câbles d'alimentation et les câbles pour le signal de conduite sont-ils d'un type résistant au feu et protégé par un matériel résistant au feu?

Les actuateurs électriques ont besoin de courant électrique pour fonctionner. Certaines exécutions utilisent un ressort ou un système hydraulique pour pousser la vanne dans une position déterminée en cas de panne de courant. En l'absence d'un tel système, de telles vannes ne peuvent être fabriquées en exécution "fail safe".

La conduite de la vanne peut être rendue impossible par une défaillance locale (par ex. fil détaché). Si la vanne n'a pas de position de sécurité sûre, il peut de ce fait y avoir une défaillance dangereuse et dormante.
Une alarme signalant la perturbation d'une vanne, peut dans une certaine mesure diminuer la probabilité d'une telle défaillance dormante, mais en général, il faut quand même sérieusement remettre en doute l'utilisation de vannes manœuvrées électriquement, sans position de sécurité sûre, pour des applications liées à la sécurité.

Rupture de câble pour la manœuvre de la pompe

88. Si le câble entre l'organe décisionnel et l'unité de commande du moteur de la pompe se rompt, le moteur va-t-il s'arrêter (ou démarrer si c'est l'action de sécurité) ou la rupture de câble sera-t-elle signalée par alarme aux opérateurs?

La question qui se pose ici est de savoir ce que l'unité de commande du moteur de la pompe va faire s'il reçoit un signal de 0 V. Tout comme lors de la rupture de câble pour des mesures, les possibilités suivantes apparaissent:

- rien (de sorte que l'on a une défaillance dormante dans la sécurité)
- alarme (de sorte que la défaillance peut être réparée)
- l'action souhaitée (arrêt ou démarrage du moteur).

Avec des moteurs à haute tension, dans beaucoup de cas, le moteur ne va pas s'arrêter en cas de rupture de câble et ce, pour des raisons de sécurité de fonctionnement. L'utilisation de tels moteurs dans des boucles de sécurité nécessite une évaluation approfondie et critique.

4.1.6. Risques dus au fonctionnement

89. L'activation de la sécurité instrumentale engendre-t-elle des risques?

L'activation de la sécurité instrumentale peut-elle engendrer certains autres problèmes ? L'arrêt d'un flux défini peut-il, par exemple, provoquer un surremplissage en amont?
Un autre problème envisageable lors de la fermeture d'une tuyauterie est le fait de pomper contre une vanne fermée provoquant ainsi un échauffement de la pompe avec tout ce qui peut s'ensuivre (surpression, température élevée, choc thermique).

Si l'activation non désirée d'une sécurité instrumentale peut s'accompagner de graves problèmes de sécurité, des mesures devront être envisagées pour éviter tout fonctionnement non souhaité.

On peut se protéger contre une activation non désirée à la suite d'une défaillance dans les mesures, en prévoyant plusieurs mesures, pour lesquelles plus d'une mesure doit enregistrer une valeur déterminée avant que l'action corrective ne soit exécutée. Une configuration typique est 2oo3.

Pour des vannes, une telle architecture est cependant très difficile à réaliser dans la pratique.

4.2. Réalisation technique

4.2.1. Mesures

Schéma de montage

90. Y a-t-il un schéma de montage ou "hook up" disponible pour les mesures?

Si le projet du hook-up n'a pas été développé, l'installateur va pouvoir exécuter l'installation à sa guise, sans tenir compte des prescriptions de sécurité et des propriétés des produits.

Localisation de l'appareil de mesure

91. L'appareil de mesure est-il placé de manière à ce qu'il donne une valeur représentative?
92. Dans le cas d'une mesure de niveau, la localisation de l'instrument de mesure peut-elle perturber la mesure?

La mesure doit être placée de manière à ce qu'une détection efficace et rapide du problème soit possible.

Le fonctionnement correct de la mesure peut, dans certains cas, être perturbé par la localisation dans le réservoir. Exemples:

- les mesures de niveau par ultrasons peuvent être perturbées si un flux de liquide coupe le chemin de l'onde.
- les mesures par radar (niveau) peuvent être perturbées si un flux de liquide coupe le chemin de l'onde.
- les mesures par radar (niveau) ne peuvent pas être placées symétriquement.

Colmatage du "tubing"

93. Dans le cas où l'instrument de mesure fait usage d'un "tubing" ou d'un tube de mesure, ce dernier peut-il être colmaté?
94. Si oui, des mesures sont-elles prises pour l'éviter?

Les "tubing" (pour les mesures de pression) et les tubes de mesures peuvent être colmatés par des substances visqueuses, des substances à point de fusion élevé, des liquides contenant de petites particules solides ou des substances souillées.
Si la mesure fait usage d'un "tubing" (pour les mesures de pression) ou d'un tube de mesure, vérifier si celui-ci ne peut s'obturer.
Les instruments de mesure suivants font usage d'un tube de mesure:

- mesure de niveau magnétique (installée dans un tube de mesure)
- capteur de déplacement (niveau) (installé dans un tube de mesure)
- certains systèmes de mesure de niveau pour lesquels la pression différentielle est mesurée au travers d'une colonne de liquide (dans un tube de mesure)
- mesure par tube à bulle (niveau)
- tube de Pitot (débit)
- rotamètre (débit)

Dans le cas de mesures de pression, on peut éviter les obstructions du "tubing" en utilisant des "seals" et un capillaire.

Dégâts au "tubing"

95. Dans le cas où l'élément de mesure fait usage d'un "tubing", y a-t-il une protection prévue contre les impacts mécaniques? Par exemple le soutien des morceaux plus longs de "tubing"?
96. Existe-t-il un standard à ce sujet dans l'entreprise?

Les dégâts mécaniques au "tubing" peuvent par exemple avoir lieu pendant des travaux à l'installation.

Influence de changements des conditions de procédé

97. La valeur exacte de la mesure peut-elle être influencée par des changements dans le milieu à mesurer (densité, pression, température, concentration, …)?

Certaines mesures dépendent des conditions (telles que la densité, la pression, la température ou la concentration) du milieu dans lequel elles se trouvent.
Il faut dans ce cas vérifier si on peut s'attendre à des modifications de densité, de pression ou de température, et si cela peut mener à une valeur mesurée erronée (dangereuse).
Les principes de mesure suivants sont sensibles à des changements de conditions du milieu:

- flotteur (densité de la phase liquide)
- capteur de déplacement (densité de la phase liquide)
- mesure de niveau basée sur la pression d'une colonne de liquide (densité de la phase liquide)
- mesure par tube à bulle (niveau) (densité de la phase liquide)
- mesure de niveau par ultrasons (limitée en pression, la vitesse du son varie en fonction de la pression, pas adaptée aux gaz liquéfiés, la surface du liquide ne peut pas être couverte de mousse et doit être uniforme)
- mesures capacitives (niveau) (sensible à la conductivité et donc, par exemple, à l'infiltration d'humidité)
- mesures de pression différentielle (débit) (température, pression et densité). Un tracing ou une isolation sont éventuellement installés pour éviter ces fluctuations. Il faut, dans ce cas, également surveiller le tracing et inspecter l'isolation.
- rotamètre (débit) (viscosité, température, densité).

Vibrations

98. L'élément de mesure est-il soumis à des vibrations et peut-il de ce fait se casser plus facilement ou donner des résultats de mesure erronés?

Certaines mesures telles que les mesures vortex (débit) peuvent donner des valeurs erronées sous l'influence de vibrations.

Dépôts

99. Du produit peut-il se déposer sur la surface de l'appareil de mesure?
100. La mesure peut-elle de ce fait donner des valeurs fautives ou mener à un temps de réponse plus important?

L'inertie des capteurs de température est par exemple plus grande si une couche isolante se dépose dessus.

4.2.2. Vannes

Actuateur suffisamment puissant

101. La feuille de spécification mentionne-t-elle pour la vanne, de combien l'actuateur doit être surdimensionné?
102. L'entreprise dispose-t-elle d'un standard sur le dimensionnement des actuateurs pour des vannes critiques en matière de sécurité?

Le dimensionnement de l'actuateur doit être fait pour les conditions de procédé "les pires possibles". Des substances visqueuses ou collantes peuvent demander un plus grand couple, ainsi que l'existence d'une grande contre-pression (anormale).

Le dimensionnement souhaité de l'actuateur peut changer tout au long de la durée de vie d'une vanne, par exemple à la suite d'une modification d'une condition de procédé ou à la suite d'une expérience avec le fonctionnement de la vanne.
Il s'agit donc d'une spécification de la vanne que l'on doit toujours pouvoir retrouver et, le cas échéant, pouvoir modifier.

Humidité dans l'air d'instrumentation

103. L'air d'instrumentation est-il séché?
104. L'humidité de l'air d'instrumentation est-elle surveillée?

L'humidité dans l'air d'instrumentation va geler par temps de gel et, de ce fait, la vanne ou le solénoïde peuvent se bloquer.
Un point de rosée typique de l'air d'instrumentation est -40°C (ou moins).

Tuyauterie de by-pass de la vanne

105. Y a-t-il une tuyauterie de by-pass de la vanne prévue?
106. Cette vanne de by-pass est-elle scellée en position fermée?
107. L'ouverture d'une telle vanne de by-pass est-elle soumise à une procédure ?

Une telle tuyauterie de by-pass peut par exemple être utilisée pour tester la vanne (la fermer) sans avoir d'impact sur la production. En circonstances normales, cette tuyauterie de by-pass ne peut naturellement jamais rester ouverte.

Manipulation locale

108. La vanne peut-elle être commandée localement (via un interrupteur)?
109. Si oui, le signal de la sécurité a-t-il priorité sur le signal qui est donné en local?
110. Le solénoïde peut-il être manœuvré localement (via un "manual override")?
111. Dans le cas où une commande locale est possible, quelles mesures l'entreprise a-t-elle prises pour éviter un usage incontrôlé de cette possibilité?

Dans certains cas, un interrupteur est prévu au niveau de la vanne pour commander la vanne sur place. Cela se présente surtout avec des vannes appelées MOV's ("motor operated valves" ou vannes avec moteur électrique). Cette commande locale ne peut pas neutraliser la fonction de sécurité. C'est pourquoi le signal de la sécurité doit avoir priorité sur le signal local. Cela doit ressortir du schéma logique de la sécurité.

Certaines vannes électromagnétiques prévoient un "manual override" qui permet de commander les vannes localement. Cette disposition n'est pas à conseiller pour les vannes dans des applications de sécurité.

Coup de bélier

112. Les risques de coup de bélier suite à la fermeture rapide d'une vanne ont-ils été analysés?

Des ralentissements peuvent être introduits de sorte que le coup de bélier soit limité.

Des ralentissements peuvent être réalisés à l'aide d'une vanne d'étranglement qui évente au ralenti la pression d'air. Si cette vanne est bouchée, la pression d'air ne peut plus s'échapper et elle ne peut plus enclencher la vanne. Si cette vanne est trop ouverte, la vanne peut se fermer trop vite. Ces problèmes doivent être résolus par l'entretien préventif.

Bruit

113. La feuille de spécification de la vanne mentionne-t-elle le niveau de bruit?

Les vannes de régulation peuvent parfois faire beaucoup de bruit.

4.3. Mise en service de la mesure

Réalisation d'une inspection lors de la mise en service

114. L'entreprise dispose-t-elle d'une procédure qui prescrit que lors de la mise en service d'une sécurité instrumentale, il faut contrôler si elle répond entièrement aux spécifications prescrites ?
115. A-t-on rédigé une instruction pour la sécurité instrumentale afin de contrôler si elle répondait entièrement aux spécifications prescrites ?
116. Les résultats de ces contrôles ont-ils été enregistrés ?

Le standard IEC61511 attache beaucoup d'importance à la validation de la sécurité après la réalisation technique de cette dernière.
L'objectif de la validation est d'assurer à l'aide de tests et d'inspections que la sécurité fonctionne conformément aux spécifications.

Validation des mesures et des alarmes lors de la mise en service

117. Le champ de mesure de chaque élément de mesure a-t-il été contrôlé ?
118. A-t-on vérifié si l'élément de mesure fonctionnait correctement (signal de sortie correcte en fonction de la valeur mesurée)?
119. A-t-on vérifié si les alarmes ont bien été réglées aux valeurs correctes?
120. A-t-on vérifié si les alarmes sont effectivement générées aux valeurs réglées?
121. A-t-on vérifié si les alarmes de diagnostic avaient été réglées correctement et si elles fonctionnent correctement?

Pour des mesures continues, il faut vérifier si le champ de mesure est correct. Cela signifie que lorsqu'une mesure de pression a un champ de mesure de 0 – 10 barg, cela doit correspondre à 4 – 20 mA. Si le champ de mesure n'est plus correct, alors la mesure de pression doit à nouveau être calibrée. Un champ de mesure fautif peut avoir comme conséquence que la sécurité ne fonctionne plus correctement. Supposons par exemple que le champ de mesure est dépassé et que 0 – 12 barg correspond à 4 – 20 mA (au lieu de 0 – 10 barg). Une valeur de déclenchement de Een schakelwaarde van 9 barg correspond alors à 16 mA au lieu de 18.4 mA. La pression devra monter jusqu'à 10.8 barg (au lieu de 9 barg) avant que la sécurité ne soit activée.

Pour des contacteurs discrets (par exemple des manomètres à contact), ce n'est pas le champ de mesure que l'on doit contrôler, mais bien la valeur de déclenchement.

On ne peut pas se limiter, certainement pas lors de la mise en service, à apporter un signal électrique simulé (entre 4 mA et 20 mA) pour tester le bon fonctionnement de la boucle, parce que de cette façon, l'élément de mesure et le transmetteur restent complètement en dehors du contrôle.

Validation des éléments finaux lors de la mise en service

122. A-t-on vérifié si la numérotation de la vanne et des câbles était correcte?
123. A-t-on vérifié si l'élément final s'enclenche correctement (position correcte en fonction du signal de conduite)?
124. A-t-on vérifié si la vanne se met dans la position souhaitée en cas de coupure de l'air comprimé?
125. A-t-on vérifié si la vanne se met dans la position souhaitée en cas de coupure de courant (vers le solénoïde)?
126. A-t-on vérifié si les éventuels indicateurs de position fonctionnaient correctement?

Ces contrôles supposent que la position souhaitée en cas de coupure d'air comprimé et de courant est mentionnée sur la feuille de test.

Validation de la fonction de sécurité lors de la mise en service

127. A-t-on vérifié si le point d'enclenchement a été correctement réglé ?
128. A-t-on vérifié si la sécurité fonctionne conformément à la spécification :
    - voting correct des mesures
    - enclenchement correct des éléments finaux (simultané ou en série, avec des retards éventuels, …)
129. A-t-on vérifié sur place l'enclenchement correct des vannes (position correcte, du premier coup, sans ratés) ?
130. A-t-on vérifié si la sécurité réagit correctement en cas de rupture de câble (signal de 0 mA)?
131. A-t-on vérifié si la sécurité réagit correctement au signal envoyé par l'élément de mesure en cas de détection d'une faute (dans le cas où la mesure est équipée d'un autodiagnostic)?
132. A-t-on vérifié si l'alarme qui signale le fonctionnement de la boucle de sécurité fonctionne ?
133. Ressort-il de ce rapport que l'on a testé si les fonctions de pontage fonctionnent correctement?
134. Ressort-il de ce rapport que l'on a testé si les fonctions "reset" fonctionnent correctement?
135. Ressort-il de ce rapport que l'on a testé si l'activation manuelle de la boucle (par exemple comme élément d'"emergency shut down") fonctionne correctement?

La meilleure manière de tester une sécurité instrumentale est de générer de façon contrôlée la situation de procédé pour laquelle la sécurité instrumentale doit fonctionner. Ce n'est cependant pas toujours évident et cela peut comporter un risque. Une alternative est de simuler les conditions de fonctionnement de la sécurité instrumentale à l'aide d'une substance non dangereuse (de l'eau, par exemple).
Une troisième possibilité est de ne simuler la variable de procédé qu'au niveau de l'élément de mesure (donc pas dans l'installation elle-même). Cela ne permet cependant pas de vérifier si la mesure fonctionne lorsque les conditions de procédé apparaissent dans l'installation. L'interaction du procédé avec l'instrument de mesure n'est donc pas testée. Qui plus est, le risque subsiste qu'après le test, la mesure ne soit pas raccordée ou soit erronément raccordée.
Tester uniquement un instrument de mesure en atelier n'est pas à recommander. Les erreurs potentielles introduites lors du montage ou du démontage ne sont, dans ce cas, pas détectées. De plus, le fonctionnement de l'appareil est testé dans d'autres circonstances que dans l'installation. Un manomètre à contact réagit par exemple de façon différente selon qu'il est monté en position verticale ou horizontale. Dans le cas où un appareil de

mesure est calibré en atelier, il est également nécessaire de le tester après montage sur l'installation.
Une cinquième manière de tester est d'appliquer le signal électrique envoyé par l'instrument de mesure à l'organe décisionnel. Un tel test n'est pas complet parce qu'il ne teste ni le fonctionnement de l'instrument de mesure lui-même, ni l'interaction de l'instrument de mesure avec le procédé.

4.4. Maintien en état de la mesure

4.4.1. Inspection et entretien

Réalisation d'inspections périodiques

136. La sécurité instrumentale est-elle reprise dans un programme d'inspection?
137. La fréquence d'inspection est-elle basée sur les calculs de fiabilité?
138. L'entreprise dispose-t-elle d'une instruction écrite pour le test de la sécurité instrumentale?
139. Les rapports de tests sont-ils disponibles?
140. Peut-on démontrer que les actions résultant du test ont été réalisées?

La mise à disposition d'instructions de tests écrites est une exigence explicite du standard IEC61511.

Dans le cas où l'organe décisionnel est un PLC de sécurité certifié (pour des applications SIL 3), la fréquence d'inspection est déterminée par les fiabilités des éléments finaux et des éléments de mesures. Le PLC de sécurité est la plupart du temps testé complètement tous les 10 ans par le fournisseur.

Les systèmes à relais doivent par contre être testés régulièrement. Cela consiste essentiellement à vérifier si les contacts ne restent pas collés. Les systèmes à relais ne disposent pas non plus de diagnostic interne. La fréquence devrait être fonction des calculs de fiabilité.

Contenu de l'instruction pour l'inspection périodique

141. Ressort-il de cette instruction que le fonctionnement correct de chaque élément de mesure est testé (champ de mesure, signal de sortie correct en fonction de la valeur mesurée)?
142. L'instruction décrit-elle la méthode de travail à suivre pour vérifier si la sécurité fonctionne conformément aux spécifications, en tenant compte:
    - du voting des mesures
    - de l'action souhaitée des éléments finaux (simultané ou en série, retards éventuels, …) ?
143. Ressort-il de cette instruction que le bon fonctionnement des alarmes est testé:
    - les alarmes lorsque l'on atteint les valeurs limites des paramètres mesurés
    - les alarmes lors de l'activation de la sécurité les alarmes de l'autodiagnostic)?

Il est recommandé de reprendre intégralement la procédure de test suivie lors de la mise en service lors de l'exécution des inspections périodiques. Ainsi on peut détecter des fautes pouvant avoir été faites lors de travaux sur les sécurités instrumentales (modifications, réparations, entretien, …). Bien entendu, ces travaux doivent également aussi se dérouler de manière contrôlée, mais il n'est pas à exclure qu'une intervention sur la sécurité échappe à ces contrôles et que malgré le suivi des procédures, des fautes soient commises. Un contrôle périodique approfondi peut servir de filet complémentaire pour de tels cas.

En ce qui concerne le test de la fonctionnalité de la boucle, on peut faire les mêmes

remarques que pour les tests lors de la mise en service. La fonctionnalité complète telle que décrite dans le document de spécification doit être contrôlée. La préférence va à un test tête-queue qui se rapproche le plus possible des conditions réelles de fonctionnement de la sécurité.
Pour un test périodique, on peut cependant également accepter que le fonctionnement complet de la boucle soit testé en deux étapes:

- test de la partie de la sécurité instrumentale à partir de la mesure jusqu'à l'organe décisionnel
- test de la partie de la sécurité instrumentale allant de l'organe décisionnel à l'élément final.

4.4.2. Mise hors service temporaire

Mise hors service de la sécurité (dans son ensemble)

144. Existent-ils des boutons-poussoirs ou des contacteurs « hard wired » pour ponter la sécurité instrumentale (dans son ensemble) (appelés « Process Override Switches »?
145. Si oui, ces contacteurs sont-ils verrouillés à l'aide d'une clé ?
146. La sécurité instrumentale peut-elle être débranchée via le système de contrôle (via un lien en série avec le système de sécurité) ?
147. L'accès à ces fonctions dans le système de contrôle est-il protégé à l'aide d'un code ou d'une clé ?
148. Rend-on clairement visibles aux opérateurs dans la salle de contrôle quelles sécurités instrumentales ont été débranchées ?

Idéalement, chacune des sécurités instrumentales individuelles pontées devrait être visible pour les opérateurs via, par exemple, un tableau donnant une vue d'ensemble sur lequel les boucles déconnectées apparaîtraient. Une alternative est une signalisation par installation ou par partie d'installation.

Mise hors service des mesures

149. Les mesures peuvent-elles être pontées?
150. Quelles mesures matérielles l'entreprise a-t-elle prise pour éviter que la mesure ne soit mise hors service de manière non contrôlée?
151. De quelle manière les mesures pontées sont-elles signalées aux opérateurs?

Certaines installations sont équipées de ce que l'on appelle des "MOS" (Maintenance Override Switches) permettant de mettre la mesure hors service si le composant nécessite un entretien ou une réparation. Un MOS est donc en principe manipulé par le personnel d'entretien.
Cela peut se passer de 3 manières différentes:

- dans l'armoire ESD avec un interrupteur par instrument
- dans le système DCS
- en salle de contrôle avec des interrupteurs à câblage fixe « hard wired ».

En l'absence de ces MOS, le pontage se fera le plus souvent en ajoutant des câbles dans la boîte à bornes. A chaque fois se présente le risque que le pontage ne soit pas ou soit enlevé trop tard.
L'utilisation de MOS se doit d'être visualisée de façon à ce que l'on ait toujours un aperçu (visuel) clair des mesures hors service.

Différentes mesures matérielles sont possibles pour éviter le pontage incontrôlé. Si le pontage a lieu via l'armoire ESD, l'emploi d'une clef doit être exigé pour permettre de rendre actif le pontage par mesure. Si le pontage a lieu via le DCS, on peut également travailler avec une clef ou un code. Ces clefs ne peuvent naturellement pas être présentes en permanence sur l'armoire ESD ou sur le système DCS.

Le TÜV (un institut international de certification) prescrit que si le pontage se fait via le DCS, il doit toujours exister un contacteur à câblage fixe « hard wired » (ou une autre méthode) permettant d'annuler tous les pontages.

Procédure pour la mise hors service

152. Existe-t-il une procédure pour la mise hors service d'une sécurité instrumentale (dans son ensemble ou en partie)?
153. Dans le cas du pontage d'une sécurité, détermine-t-on des mesures alternatives?
154. Quelles mesures l'entreprise prend-t-elle pour éviter que les sécurités instrumentales ne restent hors service pendant des (exagérément) longues périodes?

Les informations suivantes sont-elles formellement enregistrées:

- date de la mise hors service
- durée maximale de la mise hors service
- raisons de la mise hors service
- mesures alternatives temporaires
- approbation par une personne compétente.

Signalisation

155. Les composants d'une sécurité instrumentale sont-ils marqués sur place comme critiques pour la sécurité?

Un tel marquage a pour principal objectif d'éviter des travaux non contrôlés sur des composants de sécurités instrumentales.

4.4.3. Entretien et réparations

Inspection après entretien ou réparations

156. Existe-t-il une procédure qui prescrit qu'après un entretien ou des réparations à une sécurité instrumentale, la sécurité doit être testée partiellement ou dans son ensemble?
157. Lorsqu'une vanne est démontée pour révision et entretien, teste-t-on après remontage de la vanne si cette dernière fonctionne correctement conformément aux spécifications de la sécurité instrumentale (comportement à l'enclenchement, position de sécurité, retards éventuels, etc) ?

En fonction de l'étendue de l'entretien ou des réparations, il doit être déterminé si la sécurité instrumentale dans son ensemble ou seulement une partie déterminée, doit être testée.

Des vannes qui ont été révisées, doivent à nouveau être testées. Des fautes potentielles pouvant survenir avec des vannes, sont: position de sécurité inversée, les câbles du signal de conduite mal ou pas connectés, idem pour les câbles de l'indication en retour de la position de la vanne,....

Lien des mesures avec l'installation de procédé

158. Existe-t-il un système pour assurer que les éléments de mesure isolés de l'installation pendant des travaux, sont à nouveau reliés à l'installation après la fin des travaux ?

Certains éléments de mesure peuvent être séparés de l'installation de procédé au moyen de vannes manuelles.

Exemple typique: contacteur de niveau avec tube de niveau. Si l'on n'ouvre pas les vannes vers le tube de niveau, la sécurité ne fonctionnera plus et cela ne sera pas remarqué. Ceci

est un argument supplémentaire pour utiliser des mesures analogiques qui alors peuvent être comparée en continu avec les mesures normales de contrôle (qui, par définition, doivent être en ordre pour pouvoir démarrer).

Dans beaucoup d'entreprises, il est convenu que seul le personnel de production peut manipuler ces vannes. Le personnel de production est dans ce cas responsable pour remettre ces éléments de mesure en liaison avec l'installation après que le personnel d'entretien y ait effectué des travaux.

De telles vannes devraient être reprises dans une liste avec les vannes qui doivent se trouver dans une position déterminée (et si possible devraient être verrouillées dans cette position) avant que l'installation ne puisse démarrer.

4.4.4. Modifications

Contrôle des modifications

159. La modification de sécurités instrumentales est-elle soumise à une procédure?
160. Les modifications sont-elles documentées dans le document de spécification?
161. Cette procédure prévoit-elle l'exécution des analyses nécessaires?

Chaque changement à une sécurité instrumentale devrait se dérouler selon un processus contrôlé. Dans beaucoup d'entreprises, une modification à une sécurité instrumentale tombe sous le champ d'application de la procédure pour la modification de l'installation.

Mise en service après modifications

162. Existe-t-il une procédure qui prévoit l'exécution des tests nécessaires pour assurer que la sécurité instrumentale satisfait encore complètement après modifications aux spécifications prescrites?

Le standard IEC61511 prescrit qu'après des modifications à la logique de la sécurité instrumentale, la fonctionnalité toute entière doit être testée dans son ensemble.

Modifications dans l'organe décisionnel

163. Comment gère-t-on la clé qui permet de faire des modifications de software dans le programme du PLC de sécurité?

Chaque PLC de sécurité dispose d'une clef indispensable pour les modifications de software ou pour les pontages ("forçage de signaux"). Ce n'est pas la même clef pour le déverrouillage des MOS.
Cette clef ne peut pas être laissée sur le système. Cette forme de protection n'aurait naturellement dans ce cas qu'une faible valeur ajoutée.