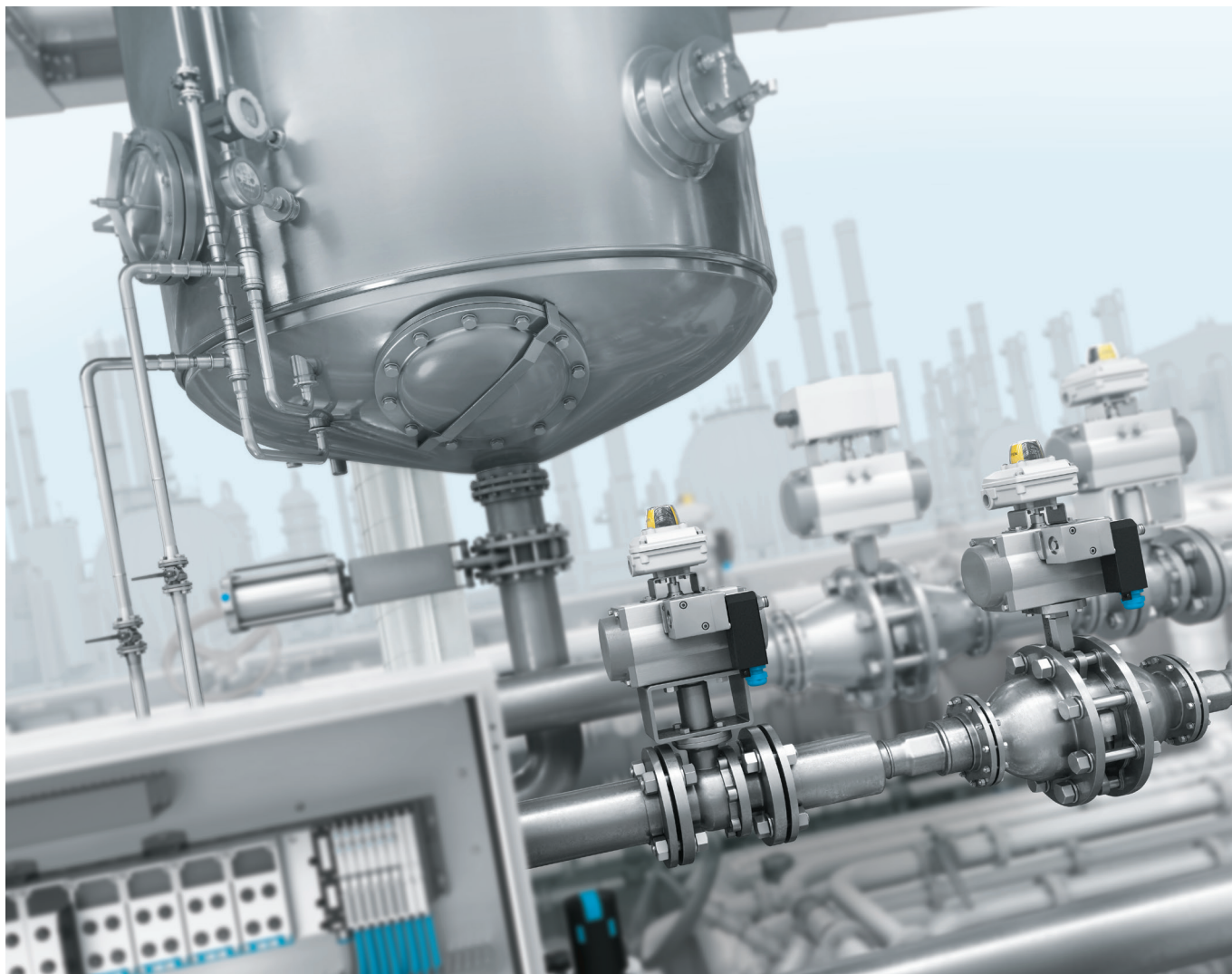


Livre blanc

Contrôle des vannes de procédé et prise en compte de la sécurité fonctionnelle (SIL)



La sécurité fonctionnelle dans la production par processus est un sujet qui a beaucoup évolué depuis l'entrée en vigueur de la norme CEI 61508. Elle est souvent indiquée uniquement par l'abréviation SIL. Mais qu'est-ce que le SIL exactement et comment peut-il être utilisé pour contrôler les vannes de procédé ?

Ce livre blanc contient des informations sur les sujets suivants :

- Qu'est-ce que le SIL (Niveau d'intégrité de sécurité) ?
- Les normes
- Analyse des risques
- Certificats et déclarations du fabricant
- Exemple de dispositif de protection dans un réacteur avec agitation mécanique
- Des performances éprouvées et une durée de vie prolongée grâce à l'exemple d'un électrodistributeur
- Activations redondantes des actionneurs sur le terrain.

1. Qu'est-ce que le SIL (Niveau d'intégrité de sécurité) ?

L'objectif des fonctions de sécurité est de minimiser les risques que présentent les processus pour les personnes, l'environnement et les biens. Le SIL (Niveau d'intégrité de sécurité) décrit la mesure dans laquelle le risque est réduit à un niveau raisonnable. La norme CEI 61508 explique la méthode d'évaluation des risques (graphique des risques) et les mesures requises pour concevoir des fonctions de sécurité adaptées, allant des capteurs et des circuits logiques aux actionneurs pour la prévention des erreurs (erreurs systématiques) et le contrôle des erreurs (erreurs aléatoires). Cette norme de base dépendant de l'application décrit les exigences relatives aux composants et aux systèmes pour les fonctions de sécurité et facilite le développement de normes spécifiques au secteur, telles que la norme CEI 61511-1 : « Sécurité fonctionnelle - systèmes instrumentés de sécurité pour le domaine de la production par processus ». La norme CEI 61511-1 définit, entre autres, les critères de sélection des composants pour les fonctions de sécurité telles que la fiabilité opérationnelle des capteurs et des actionneurs.

Capteur ≥ 35 %		Logique ≥ 15 %		Actionneur ≥ 50 %	
					
PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
SIL _{requis} (SIL _r)					
PFD _{total} /PFH _{total}					
Notifié par le fabricant À déterminer par l'opérateur du système					

2. Les normes

Les normes de sécurité fonctionnelle sont étendues et elles ne sont pas toujours faciles à comprendre, même pour les utilisateurs expérimentés. Dans ce livre blanc, nous nous concentrerons sur l'interprétation et l'application pratique de ces normes, mais nous ne nous concentrerons pas sur elles en détail.

Voici les normes pertinentes :

- CEI 61508 : « Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité »
< Norme de base pour la sécurité fonctionnelle
- EN 61511 « Sécurité fonctionnelle – systèmes instrumentés de sécurité pour le domaine de la production par processus ».
< S'applique à l'automatisation des processus

Important à savoir

L'exigence de la probabilité de défaillance conforme à la norme CEI 61508 se rapporte toujours à un dispositif de protection complet et non à des composants individuels. Un composant ne peut donc pas avoir par lui-même de niveau SIL ; seul un circuit de sécurité complet, ou SIS (Système Intégré de Sécurité), peut avoir un niveau SIL.

Normalement, un circuit de sécurité comprend les composants suivants :

- Sensors, e.g. pressure, temperature, fill level gauge
- Evaluation and output unit, e.g. a safety PLC
- Automated process valve comprising solenoid valve, actuator and process valve

Répartition type du PFD/PFH entre les sous-systèmes d'une fonction de sécurité dans les systèmes à canal unique

3. Analyse des risques

Pour minimiser les risques, les normes CEI 61508 et CEI 61511 requièrent essentiellement les étapes suivantes :

- Définition et évaluation des risques selon les probabilités détaillées des défaillances pour tout ce qui s'étend des capteurs aux contrôleurs et actionneurs pour toute la durée de vie des composants.
- Définition et mise en œuvre de mesures visant à minimiser le risque résiduel.
- Utilisation de dispositifs adaptés (évalués ou certifiés).
- Des tests et des inspections réguliers pour garantir le respect des fonctions de sécurité.

3.1. Analyse HAZOP et autres méthodes

Les risques sont définis comme des écarts potentiellement critiques par rapport aux plans du processus de production. En d'autres termes, les risques sont des dangers qui constituent une menace réelle ou potentielle. Une analyse HAZOP (Analyse de risques et de sécurité de fonctionnement) est utilisée pour identifier systématiquement les erreurs et les problèmes de fonctionnement qui réduisent la productivité. De nos jours, cette méthode peut être utilisée pour tous les types de systèmes de production continue ou discontinue. Les étapes de base d'une analyse HAZOP sont les suivantes :

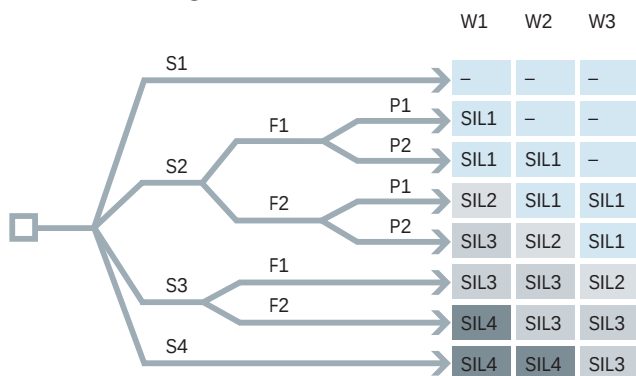
- 1) Prévoir un résultat possible
- 2) Rechercher les causes
- 3) Évaluer les conséquences
- 4) Contre-mesures

Parmi les autres méthodes utilisées dans l'évaluation des risques, on peut citer l'Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), l'Analyse des arbres d'événements (ETA) ou l'Analyse des arbres de défaillance (FTA). Ces méthodes peuvent

être classées en trois groupes : méthodes inductives, où les causes mais non les conséquences sont connues ; méthodes déductives telles que la FTA, où les conséquences sont connues mais pas les causes ; et méthodes exploratoires telles que l'HAZOP, où ni les causes ni les conséquences des déviations ne sont connues. Les différentes méthodes sont utilisées pour trouver l'information manquante.

Ces méthodes peuvent encore être subdivisées en recherches de bas en haut et en recherches de haut en bas. De bas en haut signifie commencer par une erreur critique et essayer d'en déterminer les conséquences (AMDEC). Les recherches de haut en bas impliquent de commencer par les conséquences dangereuses et d'essayer d'en déterminer les causes (FTA).

SIL (Niveau d'intégrité de sécurité)



Graphique des risques : quatre niveaux discrets (SIL1 à SIL4). Plus le SIL d'un système lié à la sécurité est élevé, plus la probabilité que le système ne puisse pas exécuter les fonctions de sécurité nécessaires est faible.

S	Étendue des dommages
S1	Blessure mineure sur une personne
S2	Blessure grave sur plusieurs personnes ou décès d'une personne
S3	Décès de plusieurs personnes
S4	Conséquences catastrophiques avec plusieurs décès
F	Fréquence et durée d'exposition
F1	Rare à relativement fréquent
F2	Fréquent à continu
P	Éviter / atténuer le danger
P1	Possible dans certaines conditions
P2	Presque jamais possible
W	Probabilité de survenue
W1	Relativement élevée
W2	Faible
W3	Très faible

3.2. Termes importants et valeurs caractéristiques

HFT

La tolérance aux pannes matérielles se rapporte à la capacité d'exécuter la fonction de sécurité même en cas d'erreurs et d'écarts (multiples). Si le SIL requis ne peut pas être obtenu selon ces valeurs, le SIL peut être atteint par le biais de redondances.

SFF

Le SFF (taux des défaillances en sécurité) détermine la proportion de défaillances en sécurité par rapport au nombre total de défaillances. Les défaillances en sécurité sont celles qui ne causent pas un état de système dangereux ou qui pourraient causer un état de système dangereux mais qui ne sont pas détectables.

L'adéquation d'un produit à un SIL requis peut être déterminée en fonction de plusieurs paramètres :

Faible demande

Mode de fonctionnement avec une faible fréquence de demandes pour activer le système de sécurité. Les demandes d'activation du système de sécurité ne peuvent pas dépasser la quantité d'une par an.

-> PFD (probabilité de défaillance à la demande) = la probabilité de défaillance à la demande se base sur les événements.

Forte demande

Mode de fonctionnement avec une fréquence élevée de demandes ou des demandes continues pour activer le système de sécurité. Le système de sécurité fonctionne en continu ou les demandes d'activation du système de sécurité dépassent la quantité d'une par an.

-> PFH (probabilité de défaillance par heure) = la probabilité de défaillance par heure se base sur la durée.

Type de dispositif A/B

Type A : le comportement de défaillance de tous les composants a été suffisamment décrit. Ce type inclut des dispositifs simples (nouveaux) ainsi que des dispositifs aux performances testées et éprouvées.

Type B : le comportement de défaillance d'au moins un composant n'est pas entièrement connu. Ce type inclut des dispositifs complexes ainsi que des produits récemment développés.

Cible : $SIL \geq SIL_r$

			Dispositif type A				Dispositif type B					
Niveau SIL			Taux des défaillances en sécurité (SFF)									
	Mode demande élevée	Défaillance acceptable max. du système de sécurité	< 60%	60...90%	90...99%	> 99%	< 60%	60...90%	90...99%	> 99%	Mode demande faible	Défaillance acceptable max. du système de sécurité
	$10^{-5} \leq PFH < 10^{-4}$	Un risque de défaillance toutes les 10 000 heures										
1	$3 \times 10^{-6} \leq PFH < 10^{-5}$	Un risque de défaillance tous les 1250 jours	HFT 0				HFT 1	HFT 0			$10^{-2} \leq PFD < 10^{-1}$	Une fois tous les 10 ans
	$10^{-6} \leq PFH < 3 \times 10^{-6}$	Un risque de défaillance tous les 115,74 ans										
2	$10^{-7} \leq PFH < 10^{-6}$	Un risque de défaillance tous les 115,74 ans	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \leq PFD < 10^{-2}$	Une fois tous les 100 ans
3	$10^{-8} \leq PFH < 10^{-7}$	Un risque de défaillance tous les 1157,41 ans	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \leq PFD < 10^{-3}$	Une fois tous les 1000 ans
4	$10^{-9} \leq PFH < 10^{-8}$	Un risque de défaillance tous les 11 574,1 ans		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \leq PFD < 10^{-4}$	Une fois tous les 10 000 ans
					HFT 2	HFT 2			HFT 2			
(par heure)												

(par heure)

Description générale de la probabilité de défaillance et de la tolérance de panne matérielle

4. Certificats et déclarations du fabricant

Les opérateurs du système exigent une preuve de la classification SIL des composants utilisés dans le SIS (système instrumenté de sécurité). Conformément à la norme CEI 61511, les déclarations du fabricant sont parfaitement adaptées à cette situation. Les certificats ne sont exigés ni par la loi ni par la norme. Une évaluation technique du composant de sécurité à utiliser est nécessaire pour émettre une déclaration ou un certificat du fabricant. Cette évaluation est souvent effectuée par une organisation indépendante telle que TÜV ou Exida. Si l'évaluation est réussie, le fabricant peut émettre une déclaration du fabricant et se référer au rapport d'essai de l'évaluation.

Contrairement aux déclarations du fabricant, les certificats ne peuvent être délivrés que par un organisme accrédité (tel que TÜV).

Plus le système doit être sûr, plus l'entité qui évalue la sécurité fonctionnelle et émet le certificat d'évaluation doit être indépendante

Niveau d'Intégrité de Sécurité	Entité d'évaluation
SIL 1	Personne indépendante
SIL 2	Département indépendant
SIL 3	Organisation indépendante
SIL 4	Organisation indépendante

5. Exemple de dispositif de protection dans un réacteur avec agitation mécanique

Dans un réacteur avec agitation mécanique, différents composants sont raccordés (via les vannes V1 et V2 dans l'exemple ci-dessous) et réagissent sous l'effet de l'entrée de chaleur (endothermiquement) ou de la libération de chaleur (exothermiquement). L'agitation du contenu les mélange complètement. La surchauffe doit être évitée pendant les réactions exothermiques.

Dans le schéma ci-dessous, la régulation de la pression pour le processus de réaction est un exemple de fonction nécessitant un dispositif de protection. Si la pression dans le réacteur augmente

rop, la chaleur risque de ne pas être dissipée correctement et de provoquer une anomalie. Par conséquent, la proportion du mélange ne serait pas correcte.

Ce scénario donnerait lieu à l'exigence suivante pour le dispositif de protection : fermer les vannes d'alimentation V1, V2 et la vanne de vapeur V5, tout en ouvrant simultanément la vanne de refroidissement V4 pour refroidir le réacteur.

Il existe différentes options pour résoudre le problème ci-dessus en fonction de la classification des risques :

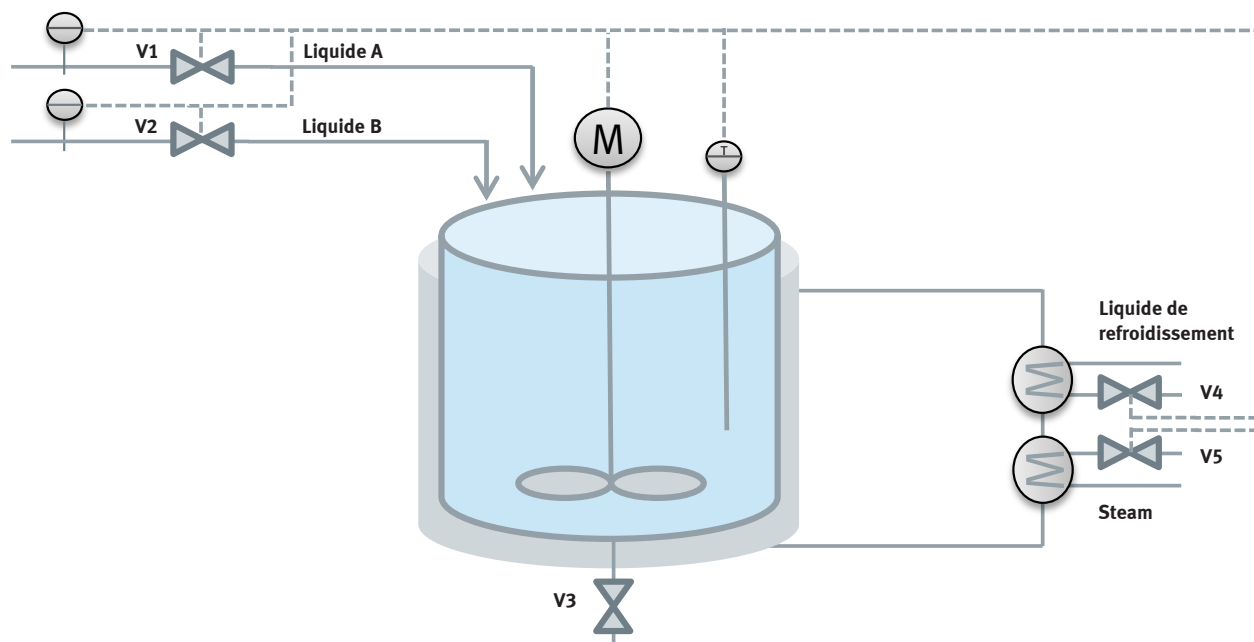
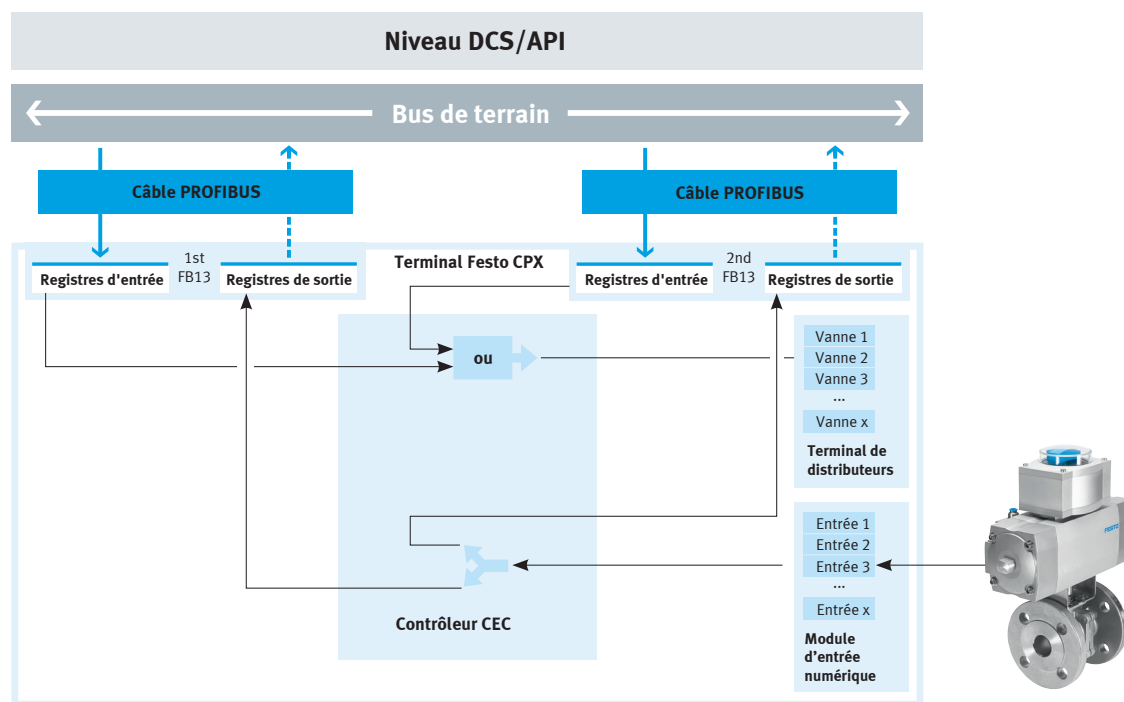


Schéma d'un réacteur avec agitation mécanique

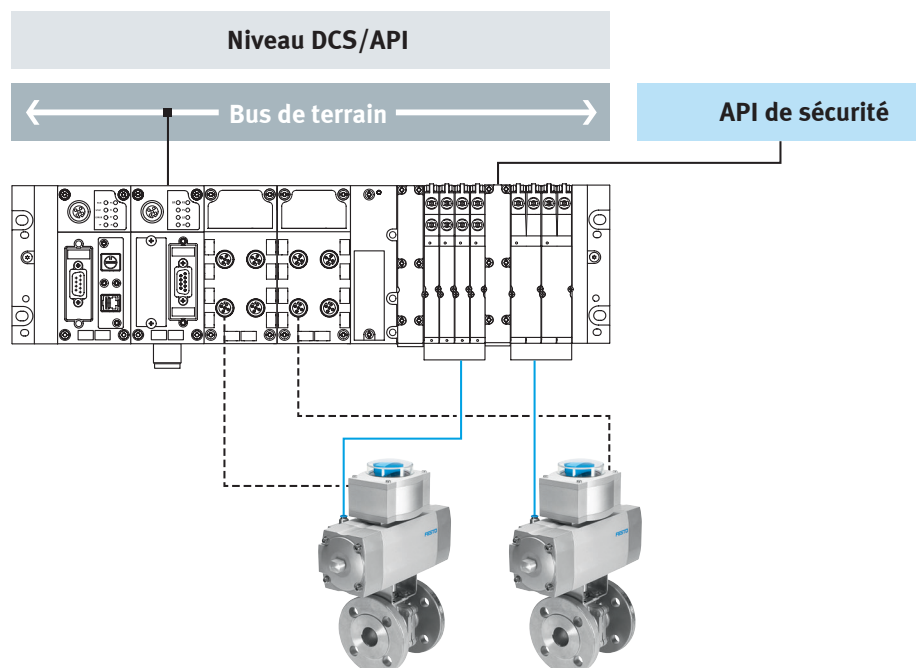
Si une ligne PROFIBUS est retirée ou si le nœud PROFIBUS est défectueux, la deuxième ligne / nœud PROFIBUS prend le relais. Ils continueront à envoyer et à recevoir de manière fiable les protocoles du système de contrôle.

On peut accéder directement aux E/S à distance sur le site au moyen d'un contrôleur doté d'une interface Ethernet et le paramétrage peut être effectué ou des processus supplémentaires peuvent être mis en œuvre. La technologie éprouvée des E/S à distance, avec ses modules d'entrée pour la connexion des capteurs NAMUR, prend en charge de manière fiable les tâches du niveau de contrôle. Les terminaux modulaires, associés au terminal de distributeurs de classe SIL2, constituent une alternative compacte.



Le mode de fonctionnement est activé par le biais de modules de bus de terrain et un terminal de distributeurs avec des actionneurs montés en série. Le terminal de distributeurs dispose d'une alimentation séparée vers l'API de sécurité, qui actionne les distributeurs séparés.

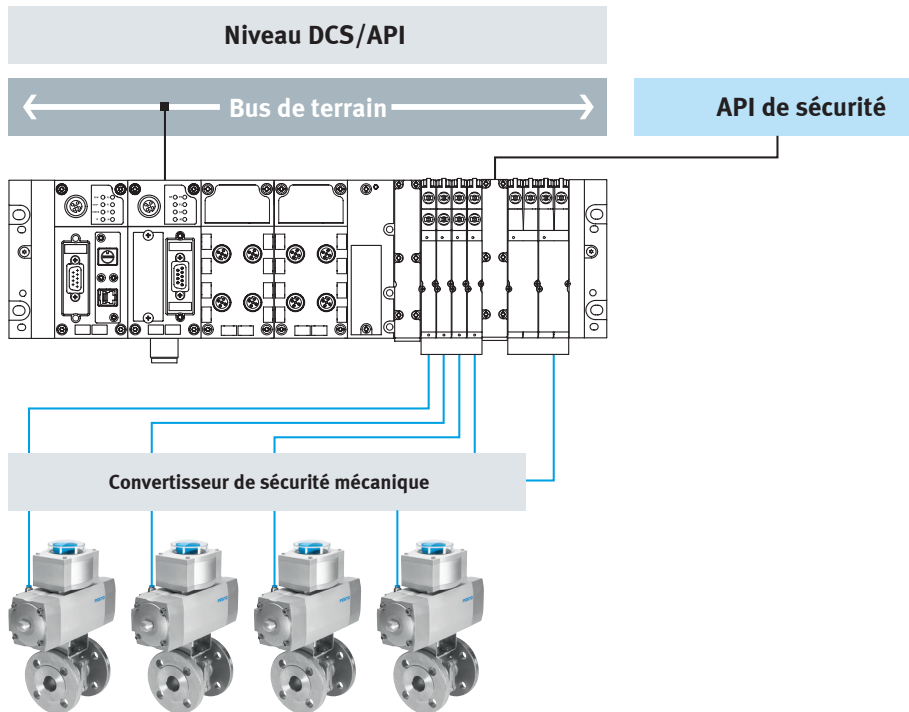
Il active également les actionneurs qui arrêtent le processus en toute sécurité. Cette solution est adaptée aux circuits SIL 2. Pour augmenter le niveau de sécurité, il est également possible d'interconnecter les vannes de manière redondante.



5.3. Terminal de distributeurs avec arrêt de sécurité intégré

En mode de fonctionnement, le terminal de distributeurs est activé au moyen d'un bus de terrain et commande les actionneurs dans le processus. En outre, le terminal de distributeurs dispose d'une alimentation séparée vers l'API de sécurité, qui actionne les vannes sur le terminal de distributeurs pour l'arrêt de sécurité. Il est évacué à travers un distributeur à 3/2 voies supplémentaire, qui fonctionne

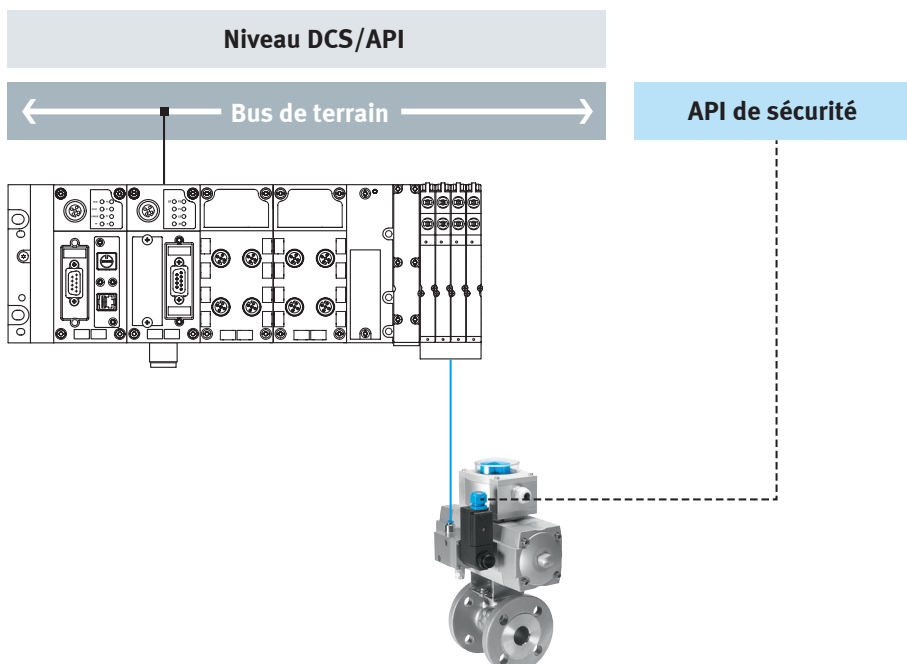
en mode normal, empêchant ainsi l'ouverture des clapets anti-retour installés dans les conduits de dérivation. En outre, la surveillance de la pression permet de sauvegarder la position de commutation du distributeur. Il commande également les mêmes actionneurs pour arrêter le processus en toute sécurité. Cette solution est adaptée aux circuits SIL 2. Pour augmenter le niveau de sécurité, il est également possible de commuter les vannes de manière redondante.



5.4. Terminal de distributeurs plus soupape individuelle pour l'arrêt de sécurité

Le mode de fonctionnement est activé par le biais du bus de terrain et du terminal de distributeurs et il est utilisé pour commander les actionneurs sur le terrain.

Le distributeur individuel monté sur le même actionneur est directement actionné par l'API de sécurité et, si nécessaire, s'éteint en toute sécurité. Ces distributeurs peuvent être utilisés dans les circuits de sécurité jusqu'au niveau SIL3.



6. Des performances éprouvées et une durée de vie prolongée grâce à l'exemple d'un électrodistributeur

La mondialisation, en particulier dans l'industrie chimique, force les sociétés à constamment augmenter le rendement de leurs systèmes. Cela sert principalement à compenser la baisse des prix sur le marché et à rester compétitifs. Les systèmes modernes d'ingénierie des processus étant hautement optimisés, on ne peut atteindre des niveaux de sortie élevés qu'avec un système fiable et hautement productif, sans temps d'arrêt. Cela implique de réduire les cycles et temps d'inspection, ainsi que d'éviter les temps de ralenti ou les temps d'arrêt causés par des réparations effectuées en dehors du calendrier de maintenance ou d'arrêts programmés.

L'un des moyens d'y parvenir consiste à utiliser des instruments électriques fiables et des composants de technologie de contrôle, tels que des électrodistributeurs certifiés conformes à la norme CEI 61508.

Cependant, même les électrodistributeurs certifiés varient considérablement en termes de performances et de spécifications concernant la sécurité. De nombreuses solutions d'électrodistributeurs sont disponibles sur le marché pour les installations de sécurité, en particulier pour le mode à faible demande. La plupart de ces solutions ont une durée de vie limitée ou ont des exigences en termes de temps d'arrêt ou de nombre de cycles de commutation requis par an afin de répondre aux spécifications de sécurité.

L'augmentation de la fiabilité constitue une exigence préalable pour prolonger les intervalles des essais. Cela signifie aussi de grandes économies. Dans les raffineries de pétrole, il est courant depuis longtemps que les arrêts n'aient lieu que tous les cinq ans. Le haut

niveau de fiabilité est principalement atteint grâce à la « philosophie deux sur trois » (2003) et il est supporté par des systèmes et dispositifs redondants. Cette option plus coûteuse est rentable grâce à la grande capacité de ces systèmes. Cela ne s'applique pas toujours aux usines chimiques.

De nos jours, les usines tentent d'atteindre un niveau de fiabilité semblable à celui des composants redondants en utilisant des dispositifs certifiés très fiables (moteurs électriques, transmetteurs, contrôleurs, électrodistributeurs ou même vannes de processus).

Des électrodistributeurs pilotés de type à clapet avec homologations TÜV, selon la norme CEI 61508 et jusqu'à SIL 3 inclus, sont disponibles sur le marché. Ces distributeurs, conformément à la dernière classification SIL, garantissent un taux de probabilité de défaillance de $2,41 \times 10^{-4}$. En d'autres termes, s'ils sont utilisés correctement, un maximum d'une défaillance se produit en 2410 cycles de commutation.

Les électrodistributeurs certifiés SIL sont désormais utilisés depuis 2002. Les niveaux de sécurité d'origine des électrodistributeurs qui datent de cette période et qui ont été utilisés depuis lors ont été vérifiés au cours d'essais en laboratoire. Cela signifie qu'il existe maintenant des électrodistributeurs certifiés SIL qui n'ont pas besoin de limite de temps sur leur certificat. Lorsque ces électrodistributeurs ont été testés de nouveau en laboratoire, les électrodistributeurs de type à clapet possédaient presque les mêmes courts délais de commutation, même après plus de 12 ans d'utilisation et même en comparaison avec les nouveaux électrodistributeurs. En outre, leur étanchéité, à l'extérieur et autour du siège d'étanchéité, est entièrement protégée.



Distributeur à clapet à piston 3/2 voies avec port NAMUR élargi et certificat TÜV, conformément à la norme CEI 61508

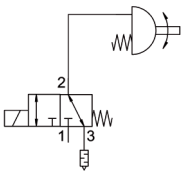
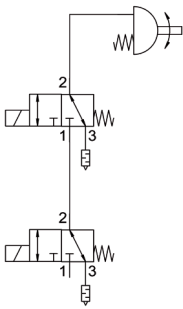
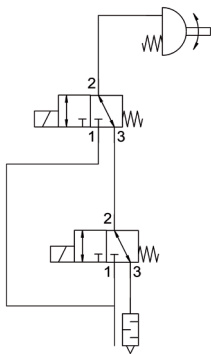
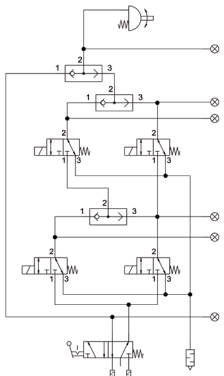
7. Activations redondantes des actionneurs sur le terrain

Si les mesures décrites sous « 6. Des performances éprouvées et une durée de vie prolongée grâce à l'exemple d'un électrodistributeur » ne sont pas suffisantes, les électrodistributeurs peuvent toujours être raccordés de manière redondante (HFT1 ou HFT2) comme décrit ci-dessus.

La sécurité et la disponibilité des processus sont toujours primordiales avec des redondances. Les circuits de sécurité actuels en ingénierie de processus sont 1oo2 (un sur deux), 2oo2 (deux sur deux) et 2oo3 (deux sur trois). Ils sont utilisés dans la production et le traitement de substances dangereuses et de grande valeur comme le pétrole brut, le gaz naturel, les produits chimiques, etc.

7.1. Les fonctions dans le schéma électrique

Pour fournir une redondance en cas de défaillance d'un distributeur, les systèmes sont installés dans des systèmes critiques en matière de sécurité ou de processus. Leur conception compacte réduit le coût de la tuyauterie ainsi que le risque de fuites dans le système. Cela permet de réduire les coûts d'assemblage et d'exploitation.

1oo1 (Un sur un)	1oo2 (Un sur deux)	2oo2 (Deux sur deux)	2oo3 (Deux sur trois)
			
Une seule défaillance peut entraîner une condition dangereuse.	Sécurité En cas de défaillance d'un distributeur, le système est complètement évacué. Cela entraîne une situation dangereuse et le système passe à une position sûre.	Disponibilité Ce n'est que lorsque les deux distributeurs sont défaillants que leur fonctionnement correct n'est plus assuré et que cela entraîne une situation dangereuse.	Sécurité et disponibilité Au moins trois défaillances doivent se produire simultanément pour provoquer une condition dangereuse. Pour la fonction, voir le point 7.5.2.

Description générale des activations redondantes les plus courantes d'actionneurs sur le terrain

7.2. Sécurité accrue (1oo2)

Avec une sécurité renforcée (1oo2), deux soupapes sont raccordées en série. Les deux sont sous tension pendant le fonctionnement. En cas de panne d'une soupape ou de l'un des signaux de contrôle pendant le fonctionnement, tout le système est évacué dans le but de se protéger contre des dommages éventuels. Les lignes de convoyeurs de médias exigent fréquemment ce niveau de sécurité supérieur.

7.3 Disponibilité accrue (2oo2)

Avec une disponibilité renforcée (2oo2), deux soupapes sont raccordées en parallèle. Les deux sont sous tension pendant le fonctionnement. En cas de panne d'une soupape ou de l'un des deux

signaux de contrôle pendant le fonctionnement, l'usine reste en activité et tout le système continue à fonctionner. Par exemple, les circuits de refroidissement requièrent cette disponibilité renforcée.

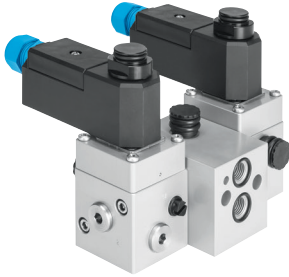
7.4 Sécurité et disponibilité accrues (2oo3)

Un circuit 2oo3 combine une sécurité accrue et une disponibilité accrue. Cela a pour avantage que la fonctionnalité des vannes individuelles peut être testée pendant le fonctionnement sans activer l'actionneur. Cette combinaison de vannes est également utilisée dans les applications hautement critiques dans l'industrie du pétrole et du gaz ainsi que dans les raffineries.

7.5. Solutions disponibles

7.5.1. Sécurité accrue du bloc NAMUR (1oo2) et disponibilité accrue (2oo2)

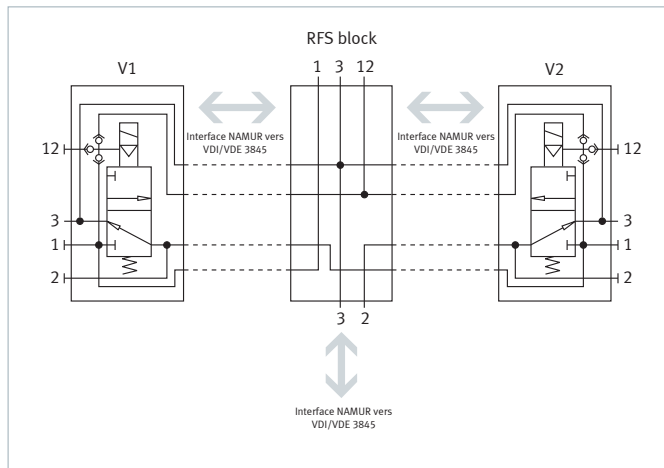
Le bloc NAMUR permet d'installer deux électrodistributeurs avec un modèle de port NAMUR. Les interfaces NAMUR facilitent la mise en œuvre de la redondance. Avantages : faibles coûts d'entreposage et facilité de remplacement des électrodistributeurs.



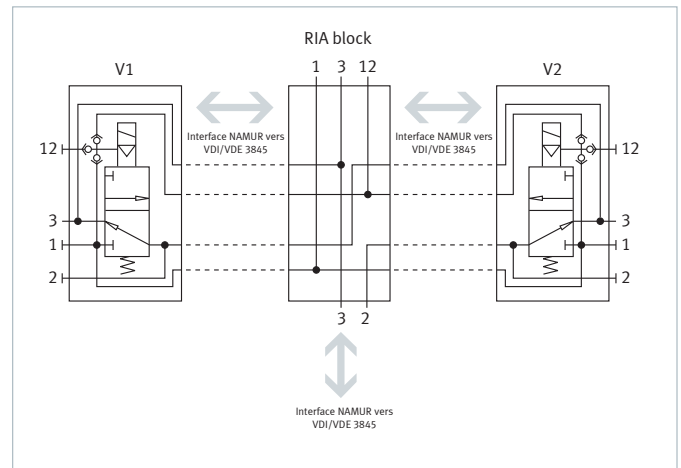
Bloc NAMUR redondant

Le bloc NAMUR peut être monté directement sur les actionneurs quart de tour à l'aide de l'interface NAMUR. Une installation séparée avec des tuyauteries adaptées est également possible.

Grâce à la borne d'alimentation auxiliaire supplémentaire, le bloc NAMUR peut également être utilisé avec des électrodistributeurs pilotés sur des actionneurs équipés de positionneurs pour des fonctions à sécurité intégrée.



Sécurité intégrée redondante – 1oo2

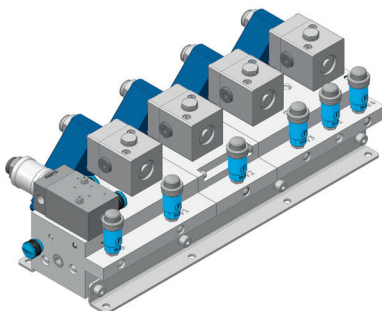


Disponibilité accrue redondante – 2oo2

7.5.2. Sécurité et disponibilité en ligne / Namur (2oo3)

Il existe une combinaison qui permet un maximum de sécurité et de disponibilité en même temps. Ce système dit 2oo3 combine les deux technologies et répond aux exigences les plus élevées d'un système.

Le bloc de distributeurs est une variante en ligne et il est intégré au système. Les distributeurs standard installés sur le bloc sont définis et montés sur le bloc par le biais de l'interface NAMUR conformément à la norme VDI/VDE 3845. Cette combinaison signifie que le bloc n'est installé qu'une seule fois et les distributeurs ne sont remplacés que selon les besoins par le biais de l'interface NAMUR conformément à un plan de cycle de vie de service / sécurité.



Exemple de bloc de fonction 2oo3

De plus, avec le système 2oo3, les fonctions des quatre distributeurs peuvent être contournées. Cette dérivation peut être déverrouillée à l'aide d'une clef pour permettre d'effectuer l'entretien pendant le fonctionnement. Les indicateurs de pression, montés directement sur le bloc de distributeurs, fournissent toujours une indication fiable et rapide lorsqu'un distributeur est sous pression.

Auteur :
Reiner Laun
Gérant de secteur industriel

Festo AG & Co. KG
Reichbergstr. 19
73770 Denkendorf, Allemagne
Tél.: +49 711 347 76585
reiner.laun@festo.com