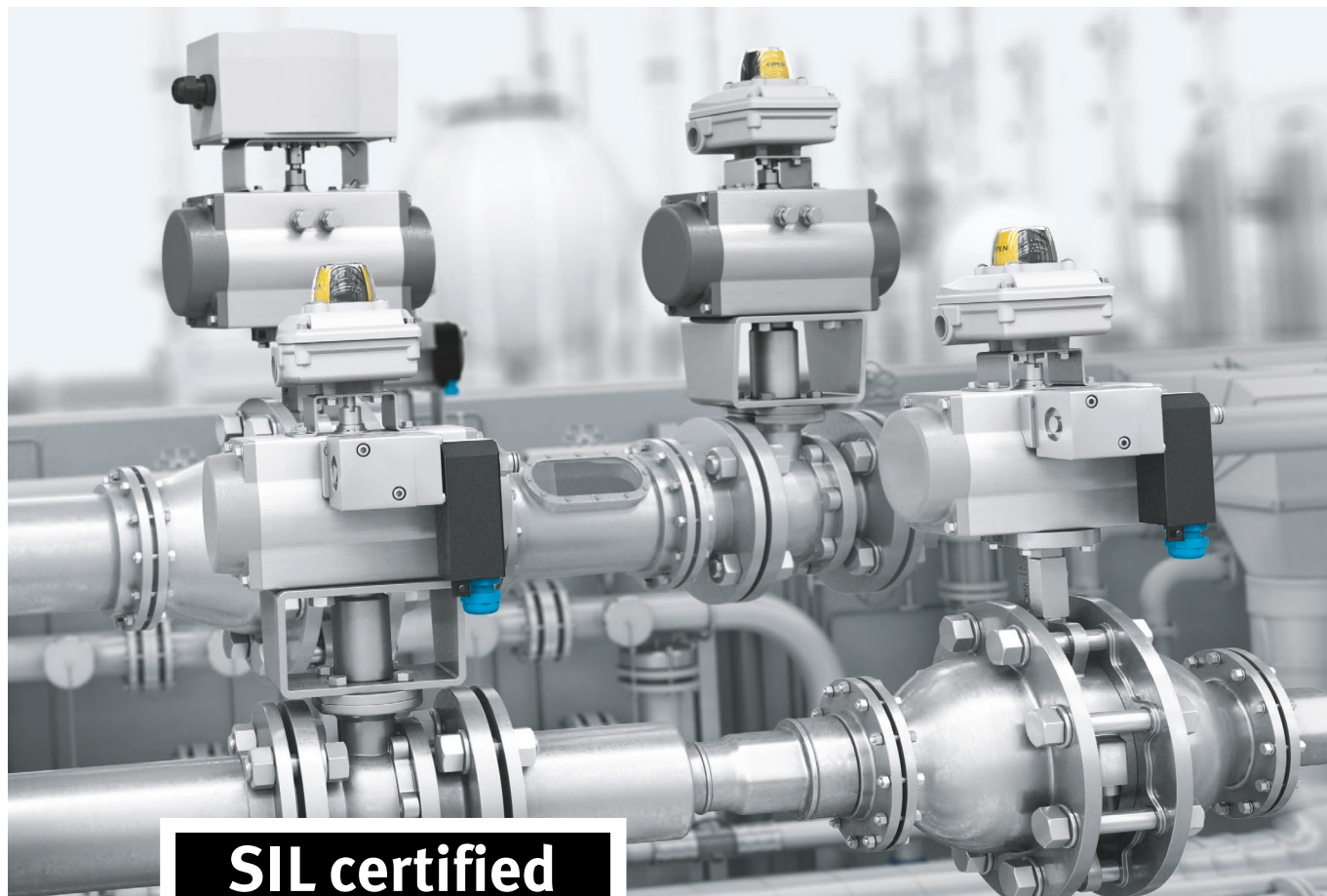


Risque réduit SIL pour l'industrie chimique

FESTO



Ce livre blanc traite des sujets suivants :

- Qu'est-ce que SIL, pourquoi ce sujet est-il important pour les exploitants d'installation et quels sont les malentendus courants dans ce contexte ?
- Que signifient les certificats et comment les lire correctement ?
- Dans quelle mesure les composants durables sont-ils utiles ?

Résumé

Les dispositifs de sécurité des installations industrielles doivent garantir que les risques venant de l'installation, pour les personnes ou l'environnement, soient minimisés. Plus les risques engendrés par l'installation sont élevés, plus la probabilité de défaillance de la chaîne de sécurité doit être faible. L'installation est classée selon un niveau d'intégrité de sécurité SIL (Safety-Integrity-Level) en fonction du danger potentiel.

Pour atteindre le niveau SIL requis, il est nécessaire de prendre en compte à la fois les composants et le circuit de sécurité complet. Les valeurs de sécurité des composants sont indiquées dans les certificats. Cependant, des malentendus sont possibles. En effet, il se peut que certains détails spécifiques à la norme ne soient pas mentionnés dans un certificat. Être capable d'interpréter correctement les certificats est donc une condition préalable importante.

La fréquence à laquelle un composant doit être testé dépend du niveau SIL requis et de la probabilité de défaillance. Ceci représente toutefois un argument économique important pour de nombreuses entreprises. Les produits à faible risque de défaillance augmentent la productivité. Ils demandent en effet moins de contrôle et, dans certains cas, ils en sont même dispensés. Cela signifie également que la production ne doit plus être temporairement arrêtée. Le distributeur à piston Festo utilisé dans le monde entier dans l'industrie chimique constitue un exemple emblématique de composant efficace dans les circuits SIL.

Sécurité, risque et réduction des risques

La sécurité a de nombreux aspects. La défaillance des équipements de sécurité peut être coûteuse à plusieurs égards : les incidents dans les installations peuvent entraîner des dommages matériels, mais aussi, en fonction du secteur d'activité, des dommages aux personnes et à l'environnement. Parallèlement, la plus petite dérive dans le processus a toujours un aspect économique. L'installation doit être mise hors service et contrôlée. Les dispositifs de sécurité des installations industrielles doivent réduire ces dangers à un niveau de risque résiduel acceptable le plus bas possible.

En fonction du potentiel de risque, l'installation ou les parties de l'installation sont classées selon un niveau d'intégrité de sécurité – le SIL. SIL 1 représente le risque le plus faible et SIL 4 le risque hypothétique le plus élevé avec des effets catastrophiques en cas de pannes. SIL ne décrit pas l'aptitude d'un composant, mais se réfère à un circuit de sécurité complet, également appelé SIS (Safety Instrumented System). Il couvre tout, de la technologie de capteurs à la logique en passant par la technique des actionneurs. Les appareils et composants utilisés pour le circuit de sécurité doivent toutefois être adaptés pour le niveau respectif.

En règle générale, plus le risque résiduel du processus est élevé, plus les dispositifs de sécurité doivent être fiables. Lorsqu'un composant a été classé dans un niveau SIL particulier, les mesures de protection passives et actives nécessaires doivent être respectées. Le risque d'un processus non sécurisé est ainsi minimisé. Des dispositifs de protection réduisent les risques à un niveau résiduel acceptable.

➤ Le niveau d'intégrité de sécurité SIL (Safety-Integrity-Level) décrit le potentiel de danger d'une installation ou d'une partie d'installation. Il détermine dans quelle mesure un risque doit être réduit. Il ne se rapporte pas aux composants individuels mais au circuit de sécurité complet. Il est bien sûr nécessaire à cet égard d'utiliser les composants appropriés.

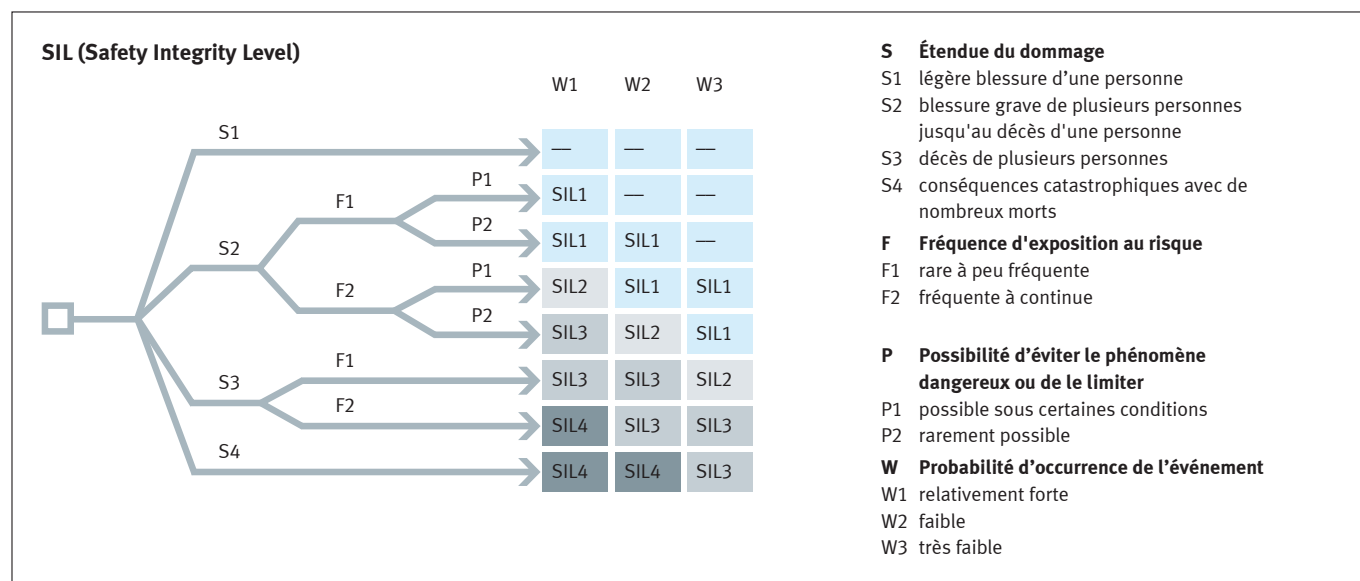


Illustration : Graphique de risque pour l'évaluation SIL

Normes, règles et principes fondamentaux

« Il existe toujours un risque résiduel. », explique Reiner Laun, Directeur sectoriel des produits chimiques chez Festo. Tous les experts sont d'accord sur le fait que le risque nul absolu n'existe pas. Il est donc important de maintenir le risque à un niveau généralement acceptable.

Différentes normes ont servi entretemps à créer un standard international permettant une comparaison rapide et claire. Pour les exploitants d'installations, une réponse claire doit être donnée à la question : comment puis-je atteindre la fiabilité requise des dispositifs de sécurité ?

La norme IEC 61508 spécifie à la fois le type d'évaluation des risques et les mesures pour les fonctions de sécurité respectives des capteurs ou du traitement logique interne. Il est primordial ici que les erreurs systématiques soient évitées et que les erreurs qui se produisent par hasard restent gérables. Cette norme est indépendante de l'application. Elle est donc également appelée norme de base et est considéré dans le monde entier comme la base des spécifications, de la conception et du fonctionnement des systèmes techniques de sécurité.

Des normes spécifiques à l'industrie en ont été dérivées, telles que la norme IEC 61511 pour les exploitants d'installations dans l'automatisation de process. Cette norme spécifie les critères de conception pour les composants des fonctions de sécurité. Cela inclut, par exemple, l'expérimentation en service des capteurs et des actionneurs. Un produit est considéré comme « expérimenté en service » s'il a fonctionné de manière fiable et documentée, dans les circonstances particulières de l'exploitation concernée, sur une période prolongée, conformément à la norme NE 130 ¹.

Un exemple concret permettra de comprendre exactement comment ces normes régulent le risque et la sécurité. Posons le postulat que des pannes peuvent toujours survenir dans un processus de production. « Les composants électriques, mécaniques et électromécaniques peuvent tomber en panne car ils sont sujets à l'usure et exposés aux agents atmosphériques. », explique Carsten Schindler, Responsable des grands comptes Chimie chez Festo : « Le processus de production peut également basculer dans un état critique. » Le facteur décisif est que la protection et les contre-mesures puissent rétablir un état sûr.

➤ Un risque résiduel existera toujours – ce qui importe c'est de le réduire à un niveau acceptable. Les normes spécifient à la fois le type d'évaluation des risques et les mesures pour les fonctions de sûreté appropriées. L'utilisation de systèmes redondants est une mesure courante pour atteindre le niveau SIL 3.

¹ Recommandation NAMUR 130 :
Appareils éprouvés pour les dispositifs de protection PLT
et calcul simplifié SIL.

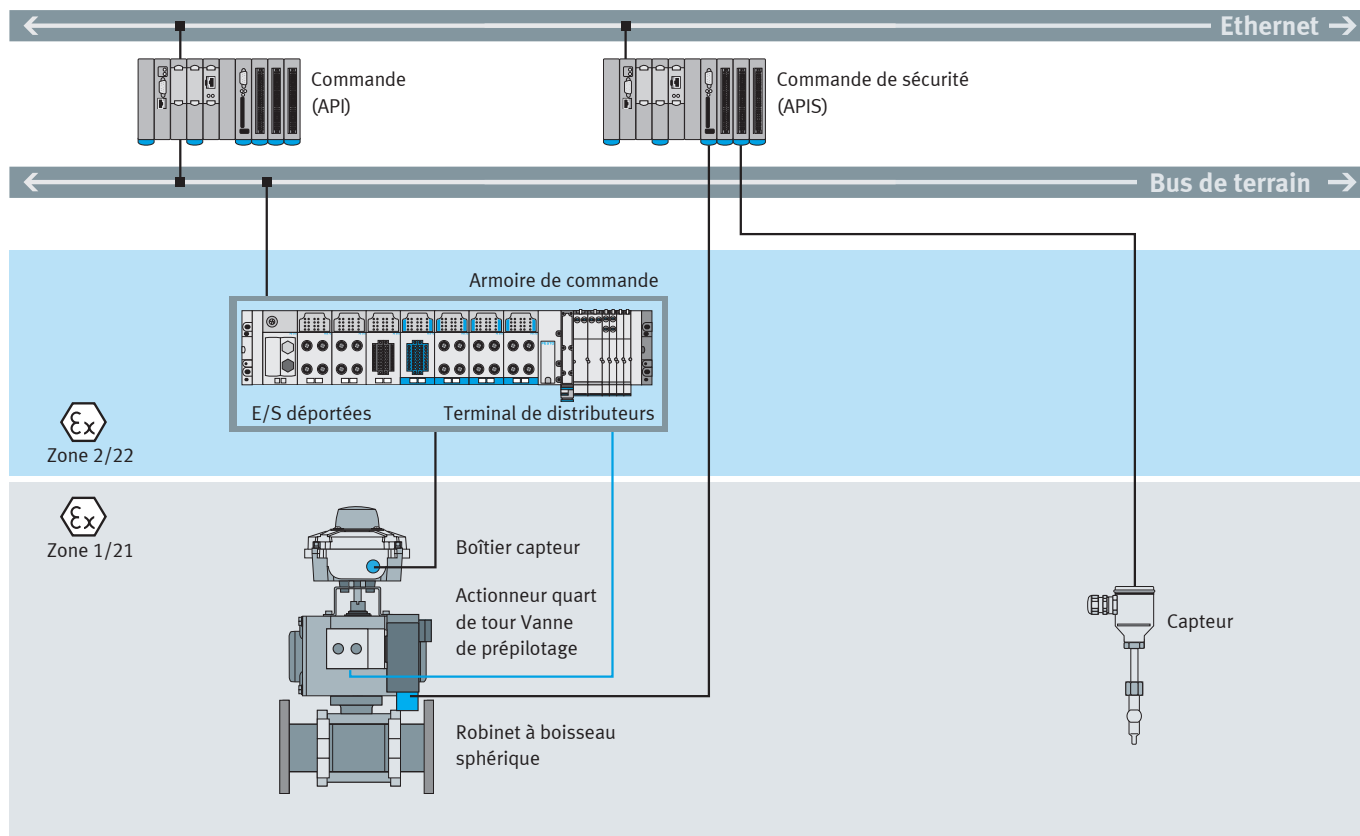


Illustration : Exemple de circuit de sécurité SIL 2

L'illustration est un exemple de circuit de sécurité permettant d'automatiser un mélangeur. Le mélangeur est rempli via les conduites d'alimentation. Le flux de matière traverse une vanne de process. Cette dernière n'est généralement pas dotée de fonction de diagnostic à l'exception de la détection de position. Elle atteint ainsi un niveau maximum de SIL 2 dans ce circuit. L'automate programmable industriel (API) détermine quand la vanne de process s'ouvre ou se ferme. Un risque pour la sécurité survient si le signal de l'API n'arrive pas correctement au distributeur : par exemple, si le terminal de distributeurs ne se commute pas en raison d'impuretés dans la conduite d'air comprimé et ne ferme donc pas la vanne de process. Le liquide continue donc de s'écouler librement dans le mélangeur.

Contre-mesure appropriée : un capteur dans le mélangeur signale que la limite de remplissage critique a été atteinte. Il envoie son signal à l'API de sécurité (APIS), qui à son tour ferme une vanne de préilotage, faisant office de soupape de sécurité et qui est exclusivement chargée de cette tâche. Le processus est amené à l'état sûr. Cet exemple n'offre toutefois aucune autre mesure de protection si l'ensemble de l'actionneur ou la vanne de process est elle-même défectueuse. La seule issue possible reste un message d'erreur et le contrôle sur site par un employé.

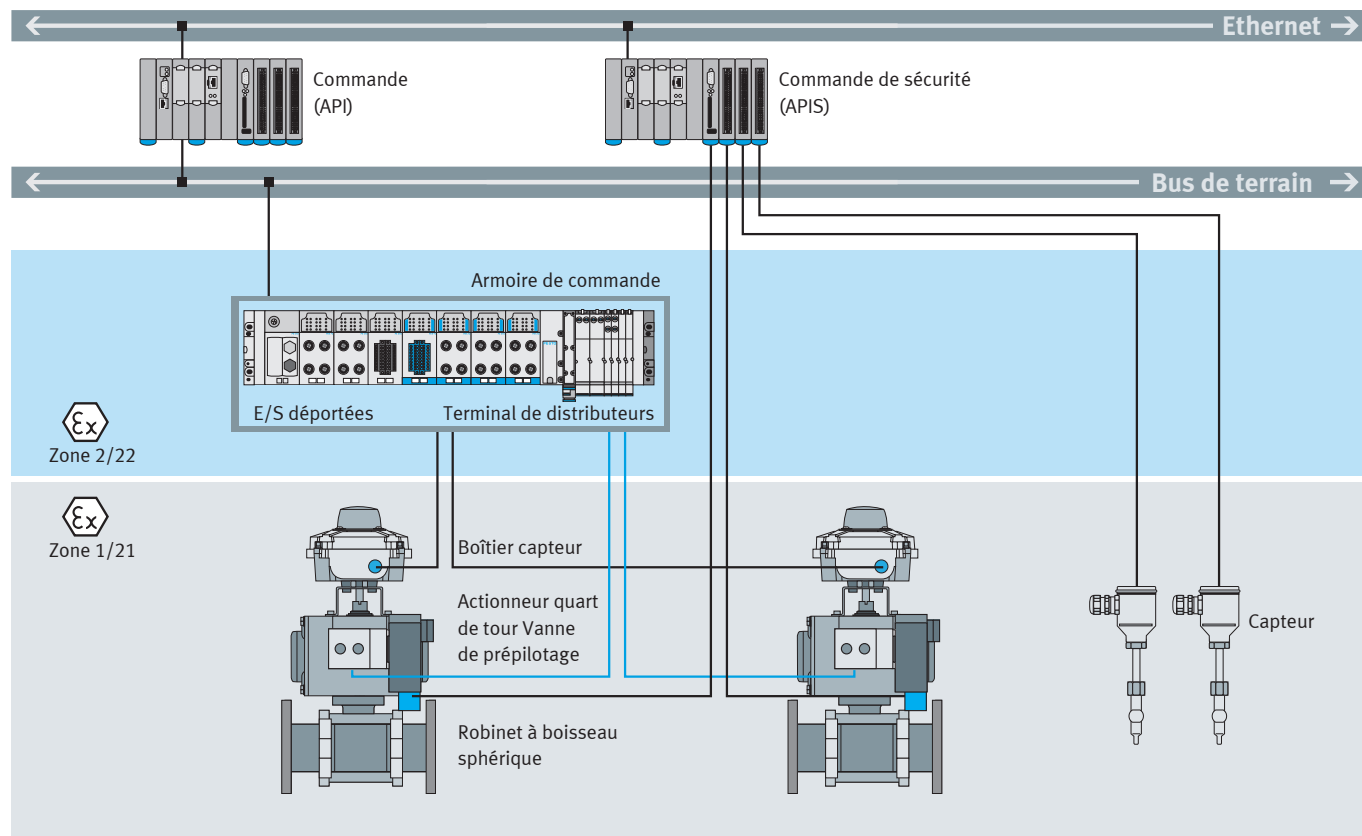


Illustration : Exemple de circuit de sécurité SIL 3

Si le circuit SIL 2 illustré précédemment n'est pas suffisant parce qu'un débordement du réservoir aurait de graves conséquences, il est alors nécessaire de concevoir une structure permettant de minimiser encore plus le risque : la redondance.

Deux vannes de process, au lieu d'une seule, sont connectées en série ici. La probabilité que les deux vannes tombent en panne simultanément est extrêmement faible. Le risque peut encore être minimisé en installant deux capteurs supplémentaires pour qu'ils soient eux aussi redondants. Le cas échéant, des mesures de protection peuvent alors être déclenchées par un capteur. Un niveau SIL 3 peut être réalisé de cette manière même avec des composants sans fonction de diagnostic.

Cependant ici aussi, une erreur systématique affectant par exemple les capteurs pourrait empêcher la commutation des deux vannes. Les erreurs systématiques comprennent les erreurs qui existent déjà au moment de la livraison (erreurs logicielles par ex.), qui se produisent en raison de matériaux inadaptés ou peut-être aussi parce que le produit utilisé ne convient pas à la tâche ou aux conditions ambiantes prévues.

Une contre-mesure possible consiste à utiliser des composants diversifiés, c'est-à-dire des composants ayant des principes de fonctionnement et de conception différents.

Conseil : bien lire les certificats

Les exploitants d'installations doivent avoir la preuve de l'adéquation des composants utilisés, de préférence via une déclaration du fabricant ou le certificat d'un organisme indépendant tel que TÜV ou Exida. Les certificats n'attestent cependant que l'adéquation-

tion des composants individuels dans un circuit de sécurité – l'architecture requise n'est souvent pas évidente au premier regard. L'exemple précédent a montré qu'avec des composants sans fonction de diagnostic un niveau SIL 3 n'est possible qu'avec un circuit redondant. C'est la seule manière de compenser la défaillance d'un composant. Ceci est clairement décrit dans la norme IEC 61511, mais souvent mal interprété à cause des différentes formulations dans les déclarations du fabricant et les certificats. Il existe en outre des certificats en circulation dont la rédaction du texte n'a pas encore été standardisée, ce qui peut également conduire à des malentendus.

1. Un certificat SIL 4 n'est pas forcément ce qu'il y a de mieux

Lorsque les premiers certificats SIL ont été délivrés pour les composants au début des années 1990, la fourchette complète du graphique des risques a été incluse – jusqu'à SIL 4. En réalité, en raison du risque induit élevé, on évite de construire des éléments d'installation qui nécessiteraient des circuits de sécurité SIL 4. Ils seraient tout simplement trop dangereux pour l'homme et l'environnement et l'équipement des circuits SIL avec maintenance et contrôles ultérieurs serait trop coûteux. C'est pourquoi, seuls les certificats de niveau SIL 3 sont émis maintenant. Cependant, des certificats de niveau SIL 4 délivrés à une date antérieure sont encore en circulation. Cela signifie que si quelqu'un trouve aujourd'hui des certificats qui attestent que « Ces composants conviennent aux systèmes jusqu'au niveau SIL 4 », alors qu'un autre certificat ne détermine que l'adéquation au niveau SIL 3, il peut en fait s'agir d'un même produit. Dans le second cas, il s'agit seulement d'un certificat plus actuel qui ne prend délibérément plus en compte le niveau SIL 4. Dans ce contexte, il convient de rappeler que le niveau SIL fait référence au potentiel de danger d'une installation – les mesures de protection à définir en dépendent toujours.

2. Un certificat avec beaucoup de restrictions n'est pas moins bon

Il existe actuellement plusieurs variantes et formulations de certificats sur le marché. Elles expriment en principe la même chose. Dans les certificats plus récents, la formulation de l'adéquation à l'utilisation tend à devenir plus détaillée. « Cela deviendra progressivement la règle » estime M. Schindler. Mais avant cela, des variantes très différentes pourront se trouver sur le marché.

Selon la norme IEC 61508, les appareils de la série mentionnée ci-dessus peuvent être utilisés dans des systèmes de sécurité jusqu'au niveau SIL 3 inclus.

Illustration : Ancienne formulation dans un certificat

La déclaration « jusqu'au niveau SIL 3 » de ce certificat prête à confusion : comme il a été démontré ci-dessus, un distributeur individuel sans fonction de diagnostic ne peut être utilisé que jusqu'au niveau SIL 2. Le niveau SIL 3 n'est possible que si un circuit redondant est utilisé. Certes, le certificat l'indique indirectement par la note « selon IEC 61511 », étant donné que la norme définit clairement cette relation. Il subsiste néanmoins une source potentielle d'interprétation erronée. Un composant de niveau SIL 2 en configuration redondante n'est pas automatiquement apte pour les circuits de niveau SIL 3. Cette aptitude est indiquée par la valeur de la probabilité de défaillance (valeur PFD) indiquée dans le certificat.

➤ Il est essentiel que les erreurs éventuelles soient détectées et que les contre-mesures appropriées puissent être prises. Les normes permettent de définir clairement quels composants et processus sont nécessaires à cet effet. Pour atteindre un niveau SIL 3, par exemple, une redondance des vannes (double vanne) est requise.

Les nouveaux certificats sont plus détaillés :

Les distributeurs peuvent être utilisés dans les systèmes de sécurité jusqu'au niveau SIL 2, en mode faible et forte sollicitation. En tenant compte de la tolérance aux erreurs matérielles minimale requise de $HFT = 1$, ils peuvent également être utilisés en exécution redondante jusqu'au niveau SIL 3.

Illustration : Nouvelle formulation explicite dans le certificat

La formulation « peuvent être utilisés dans des systèmes de sécurité jusqu'au niveau SIL 2 » donne l'impression d'un déclassement d'aptitude SIL du produit par rapport au certificat précédent. En réalité, il n'y a pas de différence de sens : les deux formulations ont la même signification, mais la deuxième formulation est plus transparente et décrit plus clairement les possibilités d'utilisation et le niveau SIL en résultant.

3. Le certificat ne dit pas tout – tenir compte du "Safety Manual" !

La mention « Se reporter au Safety Manual » peut être trouvée de manière récurrente dans tous les certificats. Il s'agit là d'une mention qui a plus de signification que la référence habituelle à un manuel ou à une notice d'un produit. Un examen du Safety Manual est particulièrement utile pour au moins une raison : comparer les valeurs et les intervalles de contrôle spécifiés.

Pour des raisons de cohérence et afin de faciliter les comparaisons, un intervalle de contrôle nécessaire d'un an est toujours présumé dans le certificat. La probabilité de défaillance est calculée sur cette base. Il existe en réalité des composants qui doivent être contrôlés plus fréquemment, mais surtout, il existe aussi des produits ne nécessitant pas un contrôle aussi fréquent. Dans l'industrie chimique en particulier, beaucoup de clients préféreraient arrêter leurs installations le moins souvent possible pour les contrôles. Un seul jour d'immobilisation peut facilement entraîner une perte de production d'un million d'euros dans une raffinerie. Il est donc décisif de savoir si un composant est certifié pour satisfaire aux exigences SIL pendant deux ou cinq ans. La probabilité de défaillance (valeur PFD) varie avec l'intervalle de contrôle : plus cet intervalle est long, plus la probabilité de défaillance est élevée. « L'intervalle de contrôle d'un an indiqué dans le certificat peut donc renfermer une valeur cachée à fort impact économique. Elle peut être avantageuse ou désavantageuse et doit donc être prise en compte avec discernement » explique Reiner Laun.

Ce que disent les certificats – et ce qu'ils ne disent pas

Les trois exemples montrent qu'un certificat sert, entre autres, à l'uniformisation des normes. Un certificat permet aux exploitants d'installation de savoir rapidement et clairement si un composant est en principe adapté à une fonction de sécurité spécifique dans un dispositif de sécurité PLT. Cependant, dans certains cas, les composants certifiés seuls peuvent ne pas être suffisants pour atteindre le niveau SIL requis. En fonction de l'évaluation des risques de l'installation partielle, l'architecture doit également être contrôlée avec soin.

Ignorer cette réalité peut au final engendrer des coûts supplémentaires : si l'autorité d'audit découvre qu'il existe un risque de sécurité inadmissible malgré les composants certifiés, un rattrapage long et coûteux sera nécessaire.

➤ Les certificats indiquent si un composant est fondamentalement adapté à un niveau SIL particulier. Des malentendus ne sont malheureusement pas exclus car certains détails ne sont pas spécifiquement mentionnés dans un certificat ou parce que différentes variantes en circulation disent en fait la même chose. Une bonne maîtrise du sujet permet d'économiser temps et argent.

L'avantage des composants durables

Tout le monde en convient : les cycles de contrôle peuvent être coûteux. La rentabilité dépend essentiellement de la fiabilité des différents éléments de l'installation. C'est pourquoi les exploitants souhaitent, si possible, des composants qui ne nécessitent aucun contrôle.

Les installations modernes sont souvent largement optimisées en termes de technique de process. Un rendement plus élevé n'est possible que si l'installation est à la fois hautement productive et fiable, ce qui implique un minimum de temps de révision ou de temps d'arrêt pour réparations. Prenons par exemple les électrodistributeurs de pilotage : l'humidité, la saleté de même que la température ou la simple utilisation régulière provoquent le vieillissement ou l'usure du joint d'étanchéité d'un distributeur. « Un distributeur est un produit à durée de vie limitée car les joints peuvent devenir poreux », explique Carsten Schindler : « L'âge est le facteur prédominant, suivi par les conditions ambiantes. Il n'est pas rare que des distributeurs à tiroir comptant jusqu'à six joints d'étanchéité soient utilisés. Cela augmente le risque d'un effet de broutage. » Mais que se passerait-il si un distributeur ne possédait aucun joint d'étanchéité ? La série VOFC de Festo en est l'illustration parfaite : un électrodistributeur à piston qui ne nécessite aucun joint dynamique. Cela signifie que le vieillissement dû à l'usure des joints n'a pas lieu. Cela réduit considérablement la probabilité de défaillance.

Mais comment adapter le distributeur pour qu'une étanchéité équivalente soit garantie, malgré l'absence de joint souple ? Il a fallu faire appel au savoir-faire de l'ingénierie : le siège des électrodistributeurs VOFC est étanchéifié en dur, le polyuréthane remplace le joint souple habituel.

Les électrodistributeurs VOFC garantissent, conformément à l'essai de type et à la certification SIL du TÜV Rheinland, un nombre maximal d'une seule défaillance pour 2 410 commutations, en cas d'utilisation conforme. En supposant une cadence de sollicitation de un an, cela signifie une seule défaillance de commutation en 2 410 ans. En bref : grâce à son principe de conception, il est extrêmement peu probable que le distributeur ne commute pas lorsqu'il est sollicité.

Exemple pratique : installation à usages multiples de Bayer CropScience

Le distributeur a prouvé son aptitude à l'emploi dans l'installation à usages multiples de Bayer sur le site de Dormagen. La mise en service de l'installation a eu lieu 2002. Divers processus sont rassemblés sous un même toit par l'entreprise : du développement de nouveaux principes actifs pour la protection des cultures en passant par le traitement en laboratoire et les essais pilotes jusqu'à la production. C'est pourquoi les installations et appareils doivent être raccordés et utilisés de manière aussi souple que possible dans différentes configurations : séchoirs, centrifugeuses, unités de distillation ou agitateurs sont utilisés dans des agencements différents en fonction de la tâche à accomplir : 67 systèmes d'automatisation sont en charge de l'exécution.

Ces processus sont protégés par de nombreux dispositifs de sécurité du domaine de la technique de mesure et du contrôle électrique : en cas d'urgence, les vannes de dosage, les distributeurs de mise en pression et d'échappement rapide ou les vannes vapeur sont commutées sur des positions de sécurité. Afin que ces vannes se ferment assez rapidement en cas d'urgence, il existe généralement, entre le régulateur de position et l'actionneur, des pilotes qui contrôlent l'actionneur (voir également l'exemple du chapitre « Normes, règles et principes fondamentaux »).

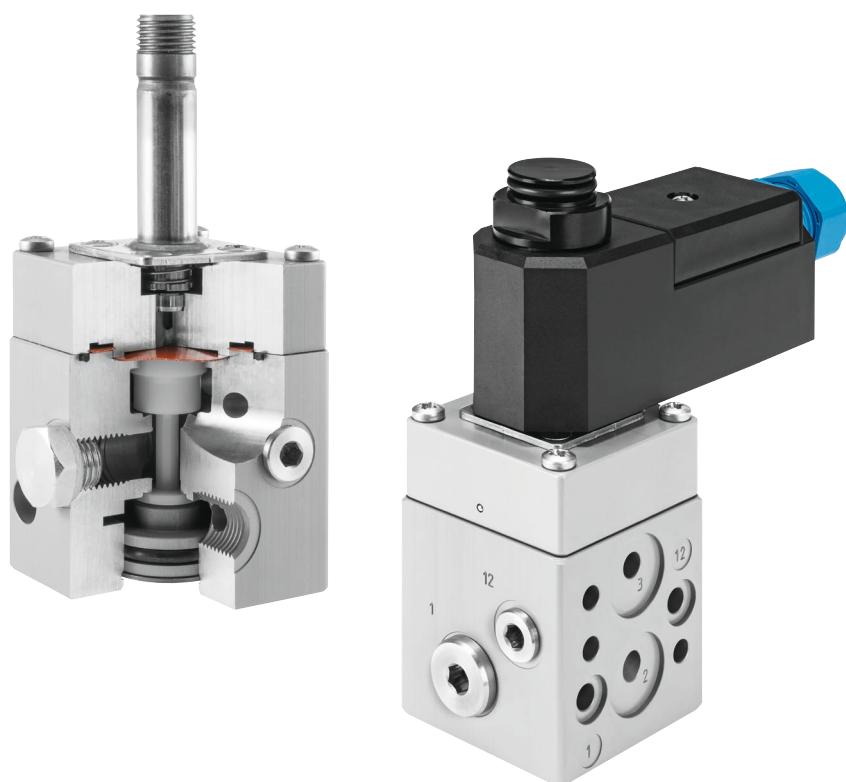


Illustration : Électrodistributeur de la série VOFC Festo

En tout Bayer a installé plus de 1 500 de ces distributeurs dans l'installation à usages multiples. Aucune défaillance des électrodistributeurs n'a été enregistrée au cours des 15 années qui ont suivi la mise en service de l'installation.

En 2015, 14 électrodistributeurs ont été récupérés sur l'installation à usages multiples pour être testés minutieusement par Festo. Compte tenu des quinze années de fiabilité opérationnelle prouvées, d'un test de laboratoire déjà effectué en 1998 et du contrôle réussi, le TÜV Rheinland a délivré un certificat stipulant qu'un test d'étanchéité n'est nécessaire que tous les sept ans pour ce type de distributeur. Naturellement, l'exploitant est néanmoins responsable du montage, du fonctionnement et de la maintenance appropriés et professionnels. Il peut cependant ainsi étendre considérablement les intervalles de contrôle des électrodistributeurs.

Conclusion

SIL est un sujet qui peut devenir non seulement critique pour la sécurité, mais également en termes de coûts : des erreurs dans la planification et la mise au point d'un circuit de sécurité peuvent entraîner la nécessité d'un rééquipement coûteux. Chaque inspection régulière ou même la défaillance d'un composant peut entraîner des coûts importants dus aux arrêts de production. Il est donc particulièrement important de sélectionner des composants durables et dûment certifiés. De plus, il est primordial de considérer l'ensemble du système et de tester différentes approches dès la phase d'ingénierie.

➤ Les exploitants d'installation souhaitent avoir le moins possible de révisions ou de temps d'arrêt. Les composants tels que les joints souples sont essentiellement des produits à durée de vie limitée. Grâce au développement innovant de composants, il est possible de produire des distributeurs sans joint souple et donc plus durables. Les électrodistributeurs VOFC Festo, par exemple, sont certifiés et ont fait leurs preuves depuis plus de 15 ans dans une installation Bayer.

Publié par :
Festo AG & Co. KG

process@festo.com
→ www.festo.com/process

Votre interlocuteur personnel :
Reiner Laun
Reiner.Laun@festo.com

Carsten Schindler
Carsten.Schindler@festo.com