PROFIBUS • PROFINET

Description du système PROFIsafe

Technologie et application

PROFIsafe

Introduction

PROFIBUS et PROFINET sont les seuls systèmes de communication industrielle qui offrent une couverture complète, y compris l'automatisation des usines et des processus. Les deux protocoles sont spécifiés dans la famille de profils de communication 3 dans les normes internationales CEI 61158 et CEI 61784-1/-2.

L'un des événements majeurs de la vie de la communauté PROFIBUS & PROFINET International (PI) a été la première publication d'une spécification pour la communication de sécurité en 1999. Elle a provoqué un bond en avant dans les possibilités du monde de l'automatisation.

Le nom de cette technologie est PROFIsafe et son logo figure ci-dessous.

Depuis cet événement, PROFIsafe a évolué pour devenir la technologie de communication de sécurité la plus performante et la plus complète au monde. PROFIsafe est une norme internationale CEI 61784-3-3 depuis 2007.

L'objectif de ce document est de fournir un aperçu complet de la technologie PROFIsafe et des questions connexes sans trop s'attarder sur des détails spécifiques. Il n'est pas destiné à remplacer les normes ou les spécifications et lignes directrices officielles mentionnées ci-dessous. Celles-ci sont définitives et contraignantes.

PROFIsafe est approuvé par le TÜV et l'IFA.

La sécurité est un domaine sensible de l'automatisation. Ainsi, la diffusion, la mise en œuvre et le déploiement de la technologie PROFIsafe doivent être traités avec sérieux. Les entreprises et institutions concernées sont tenues de se comporter conformément à la « politique PROFIsafe ».

Cette brève description doit servir de complément et de modeste résumé des sources officielles.

Dans ce document, l'abréviation « F » signifie « sécurité intégrée » (pour Fail-safe), « sécurité fonctionnelle » ou simplement « lié à la sécurité ».

Table des matières

1. La sécurité dans l'automatisation. 1
1.1 Changement technologique 1
1.2 Réalisations de PI 1
1.3 Normes internationales 2

2. Exigences remplies 3

3. « Canal noir ».....5
3.1 Caractéristiques de base 5
3.2 Composantes du réseau 5
3.3. Sans fil 5
3.4 Types de données 5
3.5 Déclenchement sélectif 6

4. PROFIsafe - la solution 6
4.1 Mesures de sécurité 6
4.2 Formats PROFIsafe 7
4.3 Services PROFIsafe 7

5. Quelle mise en œuvre ? 8
5.1 Classes de sécurité 9
5.2 Appareil F 9
5.3. Hôte F 11

6. Conformité et certification 11
6.1 Les tests PROFIsafe 11
6.2 Évaluations de la sécurité 12

7. Déploiement de PROFIsafe.....12
7.1 Sécurité électrique 12
7.2 Alimentations électriques 13
7.3 Renforcement de l'immunité 13
7.4 Haute disponibilité 13
7.5 Directives d'installation 13
7.6 Transmission sans fil 15
7.7 Sécurité 15
7.8 Temps de réponse 16

8. Pour les intégrateurs 17
8.1 Directives et normes 17
8.2 Stratégie de réduction des risques 17
8.3 Application de la norme CEI 62061 17
8.4 Évaluation des risques 17
8.5 Détermination des SIL/PL/Cat 17
8.6 Conception de la fonction de sécurité .. 17
8.7 SIL atteint 18
8.8. Électromécanique 18
8.9 Pièces non électriques 18
8.10. Validation 18

9. Familles des appareils F.....18
9.1 E/S à distance 18
9.2. Capteurs optiques 18
9.3 Entraînements 18
9.4 Robots 19
9.5 Passerelles F 19
9.6 Appareils PA 19

10. Avantages pour les utilisateurs...20
10.1 Intégrateurs et utilisateurs finaux 20
10.2 Fabricants d'appareils 20
10.3 Pour les investissements futurs 20

11. PROFIBUS et PROFINET international (PI) 20
11.1 Responsabilités de PI 21
11.2 Développement technologique 21
11.3 Support technique 21
11.4 Certification 21
11.5 Formation 21
11.6 Internet 21

1. La sécurité dans l'automatisation

Tout processus industriel actif est plus ou moins associé au risque :

- de blesser ou de tuer des gens,
- de détruire la nature,
- de nuire aux investissements.

Pour la plupart des procédés, il est assez facile d'éviter les risques sans imposer de conditions particulières aux systèmes d'automatisation. Toutefois, il existe des applications typiques associées à un risque élevé, par exemple les presses, les scies, les machines-outils, les robots, les systèmes de transport et d'emballage, les processus chimiques, les opérations à haute pression, la technologie offshore, la détection des incendies et des gaz, les brûleurs, les téléphériques, etc. Ces applications nécessitent une attention et une technologie spécifiques.

Au fil du temps, le marché équilibre la fiabilité et la disponibilité de la technologie d'automatisation standard à un certain niveau de coût économique. Cela signifie que le taux de défaillance ou d'erreur de la technologie d'automatisation standard dans des circonstances normales est tout juste acceptable pour les opérations normales, mais pas suffisant pour les applications à haut risque susmentionnées.

Cette situation peut être comparée à un système de courrier public. Alors que la distribution normale du courrier devrait être aussi abordable que possible avec un certain niveau de fiabilité, tout le monde utilisera un courrier spécial pour les messages importants.

1.1 Changement technologique

Dans le passé, les microcontrôleurs, les logiciels, les ordinateurs personnels et les réseaux de communication ont eu une influence considérable sur les technologies d'automatisation standard, ce qui a permis de réduire les coûts, d'améliorer la flexibilité et d'accroître la disponibilité. En ce qui concerne la sécurité, les normes et réglementations existantes interdisent toute utilisation de ces technologies. L'automatisation de la sécurité devait être « câblée » et basée sur la technologie des « relais ». Voir la Figure 1.

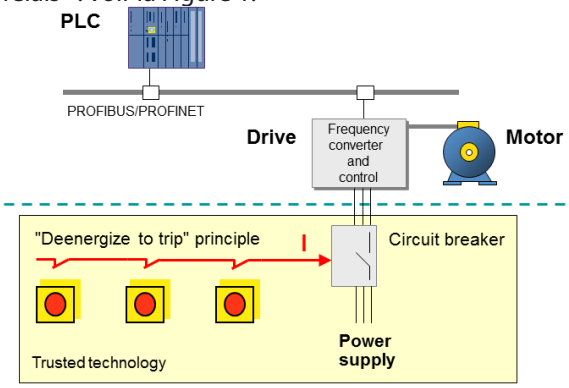

Figure 1 : Sécurité classique avec les relais

Cette dichotomie ou cette lacune est tout à fait compréhensible, car la sécurité repose sur une technologie ou un matériel fiable. La confiance, au contraire, est basée sur l'expérience et l'expérience a besoin de temps. Mais ajouter une sécurité « classique » aux solutions d'automatisation modernes conduit souvent à des situations décevantes. Par exemple, les coûts dus au câblage et à l'ingénierie supplémentaires, une flexibilité et une disponibilité moindres que prévu et d'autres inconvénients tels que des positions d'arrêt non définies des machines et des efforts fastidieux pour reprendre le fonctionnement.

Cette situation a maintenant changé de façon spectaculaire. Les microcontrôleurs et les outils logiciels ont fait leurs preuves dans des millions d'applications et les conditions préalables à leur utilisation dans des applications de sécurité sont données depuis l'introduction de la norme internationale CEI 61508.

Les mécanismes de détection des erreurs de nombreux types de systèmes de communication numérique ont été étudiés et sont bien compris. Des normes comme la norme CEI 62280-1 ont ouvert la voie.

1.2 Réalisations de l'IP

C'est pourquoi PI a développé la technologie PROFIsafe comme une couche supplémentaire qui vient s'ajouter aux protocoles PROFIBUS et PROFINET existants. Elle réduit la probabilité d'erreur résiduelle de la transmission de données entre un hôte F (contrôleur de sécurité) et un appareil F (dispositif de sécurité) au niveau requis par les normes pertinentes ou à un niveau supérieur.

PROFIsafe peut être entièrement réalisé sous forme logicielle, ce qui le rend facile à mettre en œuvre tout en couvrant tout le spectre des applications de sécurité utilisant PROFIBUS et PROFINET dans l'automatisation des processus et des usines. Il est même approuvé pour les canaux de transmission sans fil tels que WLAN et Bluetooth. Grâce à des dispositions de sécurité telles que les zones et les conduits, il peut être utilisé sur des dorsales Ethernet industrielles ouvertes.

Il couvre le besoin de haute disponibilité et de faible consommation d'énergie dans le domaine de l'automatisation des processus ainsi que la demande de temps de réaction courts en quelques millisecondes pour l'automatisation des usines.

Les appareils F modernes tels que les scanners laser ou les entraînements avec sécurité intégrée peuvent maintenant prospérer selon les besoins. La gestion de leurs paramètres de sécurité individuels (iParameters) est facilitée par le support du serveur iPar. Ce support système comprend des interfaces pour les outils appareils F dans des cadres d'ingénierie (par exemple l'interface d'appel d'outil) et des options de stockage et de récupération des iParamètres (serveur iPar). Il est important de noter que les interfaces des outils et la fonction de serveur iPar peuvent également être utilisées par tout appareil non lié à la sécurité.

La norme CEI 61508 définit des exigences particulières telles que l'augmentation de l'immunité électromagnétique sans en préciser les détails. Une ligne directrice supplémentaire intitulée « Environnement PROFIsafe » comble cette lacune et d'autres pour le développement et le déploiement des appareils F et des hôtes F.

Il est communément admis au sein de PI que seuls les appareils F et les hôtes F dans les réseaux PROFIBUS et PROFINET qui sont certifiés selon la norme CEI 61508 sont autorisés. La conformité au protocole PROFIsafe est testée par les laboratoires d'essai de PI et certifiée par le bureau de PI. Un document complémentaire intitulé « Spécification d'essai PROFIsafe » définit les rôles et les tâches des organismes d'évaluation tels que le TÜV et les rôles et les tâches des laboratoires d'essai PI.

Consulter les sites www.profisafe.netpour des informations concrètes sur PROFIsafe et www.profibus.compour des informations générales sur PROFIBUS et PROFINET.

1.3 Normes internationales

Dans la plupart des pays, les lois nationales réglementent la manière dont les personnes et l'environnement doivent être protégés. En Europe, par exemple, la « Directive basse tension », la « Directive CEM » et la « Directive machines » sont des exemples de cette législation. Les lois se réfèrent à leur tour à des normes internationales approuvées.

Dans la Figure 2, vous trouverez une sélection de normes CEI et ISO pertinentes traitant des questions de sécurité et de bus de terrain et de leurs liens.

La norme de base pour la sécurité fonctionnelle est la norme CEI 61508 qui couvre la sécurité fonctionnelle des équipements électriques et les principes et procédures de base. Elle introduit une approche quantitative pour le calcul de la probabilité résiduelle de défaillance des fonctions dites de sécurité (Niveaux d'intégrité de sécurité ou SIL). Elle est principalement utile aux développeurs d'appareils F et d'hôtes F. La norme sectorielle CEI 62061 décrit les aspects de sécurité spécifiques aux applications de machines telles que celles que l'on trouve dans l'automatisation des usines. Cette norme traite des systèmes, sous-systèmes et éléments prêts à l'emploi et de la manière d'évaluer les fonctions de sécurité pour certaines combinaisons de ceux-ci. La norme ISO 13849-1 est le successeur de la norme EN 954-1 (abolie en 2011) et a un champ d'application similaire. Toutefois, elle introduit un modèle de calcul légèrement différent (niveaux de performance - PL) et couvre les dispositifs non électriques tels que les soupapes hydrauliques, etc. Pour la sécurité des machines, la terminologie de base et les principes de conception sont définis dans la norme ISO 12100, ainsi que l'évaluation et la réduction des risques. La norme CEI 60204-1 spécifie les exigences et recommandations générales relatives à l'équipement électrique des machines. Il s'agit notamment de l'alimentation

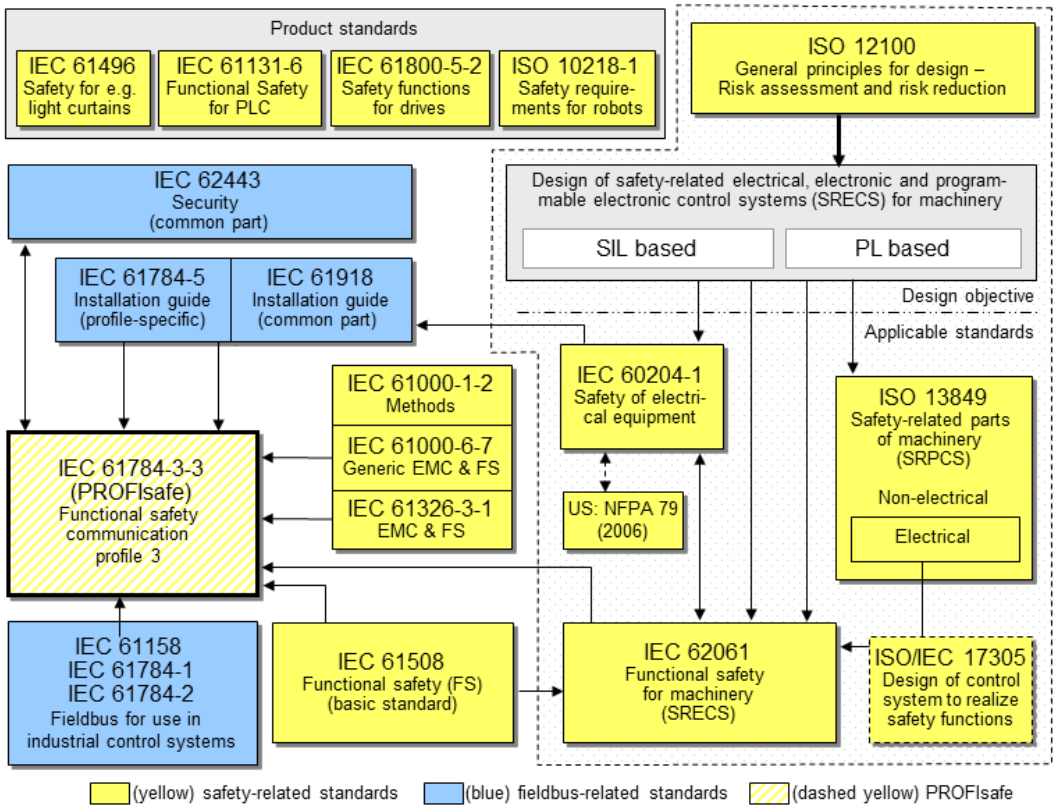

Figure 2 : Normes internationales de bus de terrain et de sécurité pour l'automatisation des usines

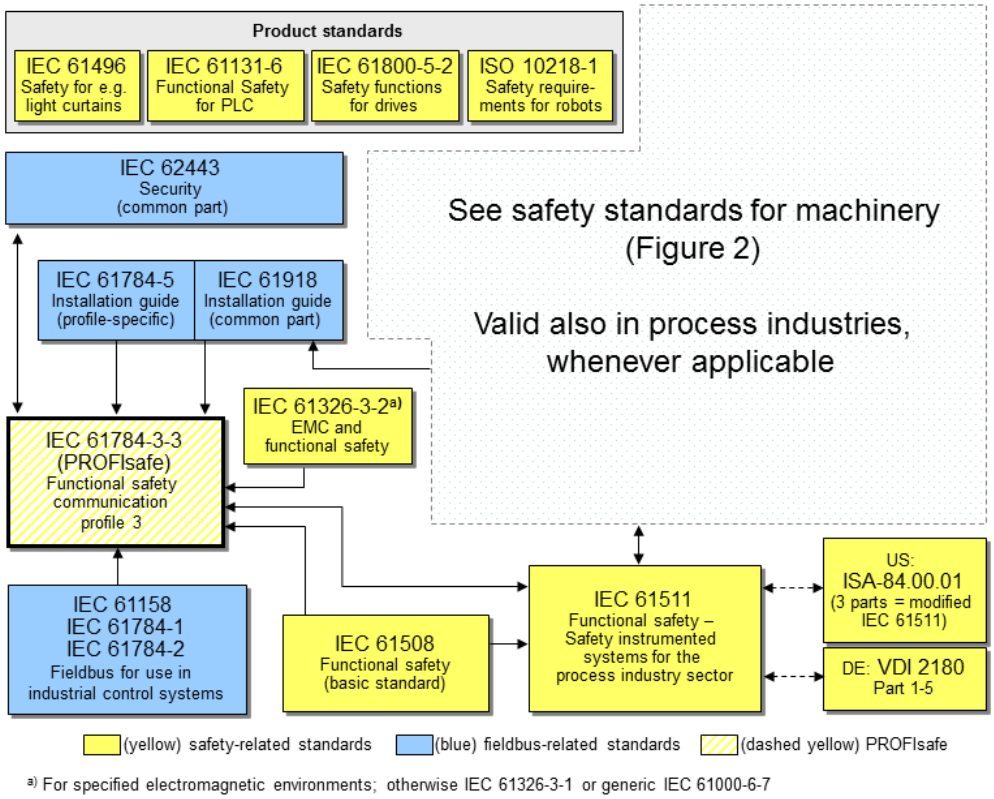

Figure 3 : Normes internationales de bus de terrain et de sécurité pour l'automatisation des processus

électrique, de la protection contre les chocs électriques, des arrêts d'urgence, des conducteurs et des câbles, etc. Les normes de produits telles que les normes CEI 61496, CEI 61800-5-2, CEI 61131-6 et ISO 10218-1 par exemple, traitent des exigences relatives aux différentes familles de produits.

L'annexe de la « Directive machines » européenne énumère les machines et pièces qui doivent légalement être certifiées, par exemple par un « organisme notifié » (IFA, TÜV, FM-Factory Mutual, etc.). S'il existe une norme de produit harmonisée correspondante (par exemple, CEI 61496), une déclaration du fabricant peut être suffisante.

Les exigences relatives aux appareils F et aux hôtes F pour assurer une immunité électromagnétique accrue sont définies dans la norme générique CEI 61000-6-7 et dans la norme sectorielle CEI 61326-3-1. Des critères de performance spéciaux DS (« état défini ») permettent un fonctionnement incorrect dans des conditions d'interférences électromagnétiques accrues au-delà des niveaux normalement requis. Toutefois, dans ces cas, l'équipement testé (EUT) doit au moins passer dans un état sûr.

Les normes des bus de terrain sont spécifiées dans les normes CEI 61158 et CEI 61784-1. Les variantes d'Ethernet en temps réel telles que PROFINET IO sont définies dans la norme CEI 61784-2. Les parties communes des directives d'installation sont résumées dans la norme CEI 61918, tandis que les parties spécifiques aux profils sont rassemblées dans la norme CEI 61784-5. Les parties communes des directives de sécurité sont résumées dans la norme CEI 62443, tandis que des parties spécifiques aux profils sont prévues pour une future norme CEI 61784-4.

Dans la Figure 3, vous trouverez une sélection similaire des normes CEI et ISO adaptées aux exigences de l'automatisation des processus. Ici, la norme sectorielle CEI 61511 tient compte de la situation particulière d'une expérience de longue date (« éprouvée en service ») avec des instruments de procédé très sensibles et un environnement électromagnétique spécifique dans ce domaine. Ainsi, la norme sectorielle CEI 61326-3-2 tient compte de ces exigences CEM.

2. Exigences remplies

Dès le début, l'intention de PROFIsafe était de définir une solution complète et efficace pour le développeur d'appareils de sécurité et l'utilisateur final. Le protocole PROFIsafe est adapté aux réseaux PROFIBUS et PROFINET sans impact sur ces normes de bus de terrain existantes. Il est possible de transmettre des messages de sécurité sur les câbles de bus standard existants en coexistence avec des messages standard (Figure 4).

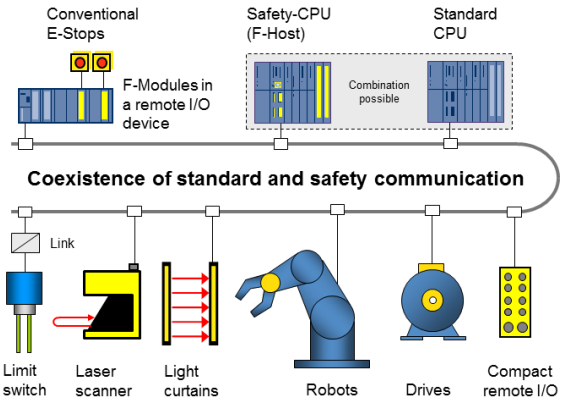

Figure 4 : Approche à « canal unique »

Cette approche « à canal unique » permet également d'utiliser des automates programmables standard avec un traitement de sécurité intégré mais logiquement séparé. De cette façon, la redondance des médias pour obtenir une plus grande disponibilité pourrait être réalisée comme une option. La séparation physique de la communication standard et de la communication de sécurité est bien sûr également soutenue, sans aucun inconvénient induit par PROFIsafe. Même dans ce cas, les utilisateurs peuvent toujours bénéficier de la technologie commune PROFIsafe sur les différents réseaux de communication.

Le protocole PROFIsafe n'a aucune incidence sur les protocoles de bus standard. D'autre part, il est complètement indépendant du canal de transmission de base et fonctionne aussi bien sur des câbles en cuivre, des fibres optiques, des liaisons de communication sans fil ou des fonds de panier. Par exemple, PROFIsafe ne fait aucune hypothèse concernant les taux de transmission ou les mécanismes de détection des erreurs. C'est ce qu'on appelle le principe du « canal noir » (Figure 5).

Le protocole PROFIsafe élimine la nécessité d'une évaluation de la sécurité des communications individuelles de la carte-mère ou d'autres voies de transmission au-delà des réseaux PROFINET et PROFIBUS. Par conséquent, il sécurise l'ensemble du chemin entre le lieu d'origine d'un signal de sécurité (par exemple, le module F d'un appareil d'entrée/sortie distant) et le lieu où il est traité (hôte F) et vice versa (Figure 6).

Le protocole PROFIsafe peut être utilisé pour des applications de sécurité jusqu'à SIL3 selon la norme CEI 61508 /CEI 62061, ou PL « e » /catégorie 4 selon la norme ISO 13849.

Les paramètres du protocole PROFIsafe sont définis, maintenus et conçus avec les moyens standards de PROFIBUS ou PROFINET, c'est-à-dire via GSD. Toutefois, les paramètres doivent être sécurisés pendant le stockage, l'interprétation, l'attribution de valeur et le transfert de l'outil de configuration au contrôleur d'E/S ou au Maître DP et, de là, à l'appareil F. Il doit y avoir le même ensemble de paramètres PROFIsafe (protocole) pour tous les appareils F ou modules F d'un appareil d'E/S distant afin de garantir une manipulation uniforme (appelé paramètre F).

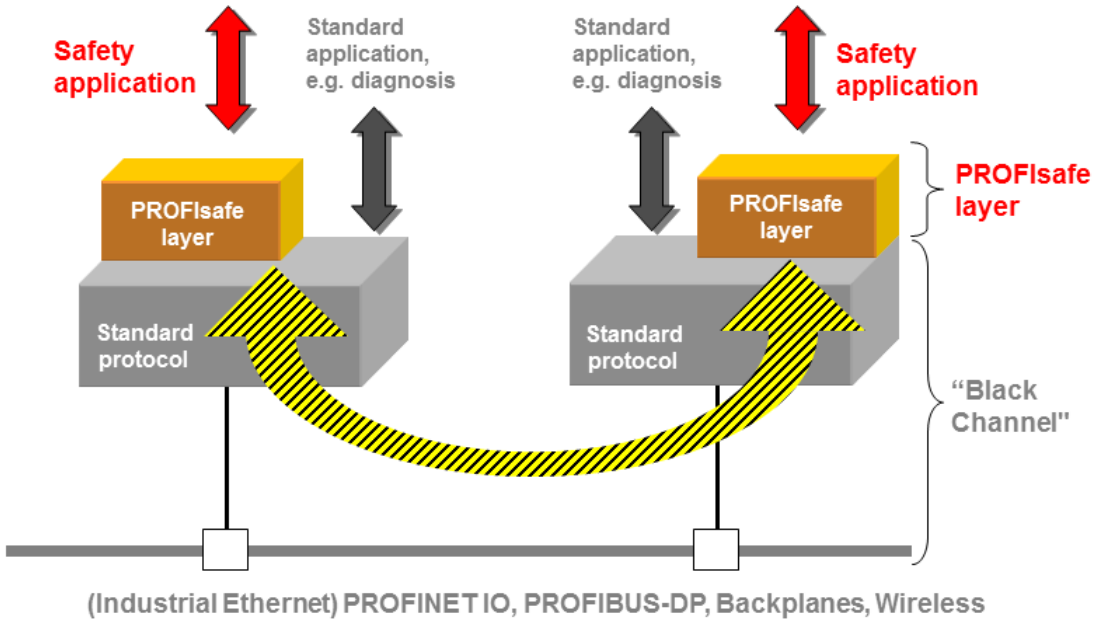

Figure 5 : Le principe du « Canal noir »

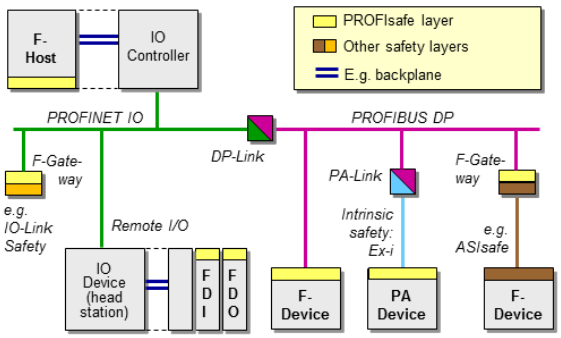

Figure 6 : Voies de communication de sécurité complètes

Les paramètres de sécurité individuels d'un appareil F sont spécifiques à la technologie, par exemple les entraînements avec sécurité intégrée, les scanners laser, etc. Le traitement de ces iParamètres via GSD impliquerait des efforts considérables et des dépendances inutiles. Il doit donc être possible pour les développeurs d'appareil F d'intégrer leurs outils individuels de configuration, de paramétrage et de diagnostic (outils CPD) via des interfaces appropriées dans les outils d'ingénierie des fournisseurs de systèmes. Cela facilite la navigation et la communication vers l'appareil F ou le module F spécifique.

Pour un remplacement rapide des appareils F en cas de panne, le système doit prendre en charge la fonctionnalité « Sauvegarde et restauration » pour les paramètres de sécurité individuels (iPar-Server) de manière uniforme. Habituellement, le serveur F ou le contrôleur qui fournit le paramétrage de base du démarrage du bus offre également cette fonction.

La documentation complémentaire définit tous les aspects du déploiement des appareils PROFIsafe, tels que les exigences relatives

- Installation
- Sécurité électrique
- Alimentation électrique
- Compatibilité électromagnétique
- Sécurité des données

Enfin, les développeurs d'appareils F ou de modules F PROFIsafe bénéficient d'un soutien important sous la forme de kits de développement, de centres de compétence et de centres de test PROFIsafe.

Dans sa version actuelle, PROFIsafe répond à toutes ces exigences. Le concept final est encore simple et facile à comprendre.

Avant d'en savoir plus sur PROFIsafe, examinons quelques conditions préalables et contraintes.

3. « canal noir »

Cême si PROFIsafe utilise le principe du « canal noir », certaines caractéristiques de base de PROFIBUS et PROFINET ont été prises en compte pour sa conception.

3.1 Caractéristiques de base

L'une de ces caractéristiques est la communication cyclique entre un contrôleur de bus et ses appareils de terrain associés (principe de réponse en émission et en réception). Cette opération de sondage permettra de détecter immédiatement tout appareil défaillant. PROFIsafe a adopté ce principe.

L'autre caractéristique est la relation de communication 1:1 entre un contrôleur de bus et ses appareils de terrain associés. PROFIsafe adopte également ce principe pour garantir l'authenticité des messages.

3.2 Composantes du réseau

Un « canal noir » peut comprendre plusieurs types de composants de réseau transparents tels que des commutateurs, des routeurs, des liens et des canaux de transmission sans fil. Pour PROFIsafe, il existe des contraintes mineures afin de satisfaire aux exigences du SIL3.

Tout type d'interrupteur est autorisé mais seulement 100 peuvent être connectés à la suite. L'espace des noms de code au sein d'une île PROFIsafe doit être unique. Les îles connectées ayant le même espace de nom de code doivent être séparées par des routeurs multiports. Il n'y a pas de restrictions pour les liens tels que de PROFINET à PROFIBUS et de là à la version à sécurité intrinsèque MBP-IS (Figure 6).

3.3. Sans fil

La transmission sans fil est autorisée pour autant qu'une disponibilité suffisante (pas de déclenchements gênants) et une sécurité puissent être garanties.

PROFIsafe spécifie certaines exigences de sécurité pour la transmission sans fil et pour les réseaux câblés qui sont connectés à des dorsales Ethernet industrielles ou à l'Internet (réseaux ouverts).

3.4 Types de données

En général, la communication par bus de terrain utilise différents types de données pour le transfert d'informations (voir l'encadré sur la documentation à la page 11). Afin de réduire la complexité, PROFIsafe propose un sous-ensemble raisonnable.

3.5 Déclenchement sélectif

Le document de PI « E/S à distance pour l'automatisation des usines (RIO pour FA) » spécifie des bits qualificatifs associés aux valeurs du processus pour indiquer la validité. Cela permet une réaction individuelle de l'utilisateur par valeur de processus. PROFIsafe offre une prévention supplémentaire configurable contre le démarrage automatique des machines.

4. PROFIsafe - la solution

C'est l'objectif de la communication de sécurité entre deux partenaires qui doit être atteint :

- des données actualisées et correctes (intégrité des données),
- vers la destination prévue (authenticité),
- juste-à-temps (ponctualité).

Diverses erreurs peuvent se produire lorsque des messages sont transférés dans des topologies de réseau complexes, que ce soit en raison de défaillances matérielles, d'interférences électromagnétiques extraordinaires ou d'autres influences. Un message peut être perdu, se répéter, être inséré depuis un autre endroit, apparaître en retard ou dans une séquence incorrecte, et/ou afficher des données corrompues. Dans le cas des communications de sécurité, il peut également y avoir un adressage incorrect : un message apparaît par erreur sur un appareil F erroné et prétend être un message de sécurité correct. Des vitesses de transmission différentes peuvent en outre entraîner des effets de stockage des composants du bus. Parmi les nombreux remèdes connus de la littérature, PROFIsafe se concentre sur ceux présentés dans la matrice illustrée à la Figure 7.

Measure: / Error:	Monitoring Number (sign of life)	Time-out (with receipt)	Codename (for sender and receiver)	Data Consistency Check (CRC)
Data corruption				X
Unintended repetition		X		
Incorrect sequence	X			
Loss	X	X		
Unacceptable delay		X		
Insertion	X		X	
Masquerade (standard message mimics failsafe)				X
Incorrect adressing	X		X	
Out-of-sequence	X			
Loopback of messages	X			

Figure 7 : Types d'erreurs et mesures de sécurité

4.1 Mesures de sécurité

Ces mesures de sécurité comprennent :

- La numérotation des messages PROFIsafe (détection des erreurs de séquence utilisée pour la « ponctualité »)
- Une attente de temps avec accusé de réception (détection d'erreur de délai d'attente utilisée pour la « ponctualité »)
- Un nom de code entre l'expéditeur et le destinataire (« authentification »)Contrôles d'intégrité des données (CRC = contrôle de redondance cyclique)

Grâce au Numéro de suivi, un récepteur peut voir s'il a reçu ou non les messages dans la bonne séquence. Lorsqu'il renvoie un message avec le Numéro de suivi uniquement comme accusé de réception à l'expéditeur, ce dernier sera lui aussi assuré. Fondamentalement, un simple « bit de basculement » se serait avéré suffisant. Cependant, en raison des tampons de stockage de certains composants du bus, par exemple les commutateurs, un numéro de surveillance de 32 bits a été choisi pour PROFIsafe.

Les systèmes de sécurité étant des systèmes en temps réel, les signaux de processus doivent être délivrés non seulement correctement, mais aussi à temps. En cas d'erreur de ponctualité, le système de sécurité déclenchera une réaction sûre, par exemple arrêter le mouvement d'un entraînement en toute sécurité. À cette fin, les appareils F utilisent un minuteur de surveillance qui est redémarré à l'arrivée d'un nouveau message PROFIsafe avec un nouveau numéro de surveillance ultérieur.

La relation 1:1 entre l'hôte F et un appareil F facilite la détection des trames de messages mal dirigées. L'expéditeur et le destinataire doivent simplement disposer d'une identification (nom de code) unique dans le réseau, qui peut être utilisée pour vérifier l'authenticité d'un message PROFIsafe. Le nom de code de PROFIsafe est appelé « adresse F ».

Un contrôle de redondance cyclique (CRC) joue un rôle clé dans la détection des bits de données corrompus. L'examen probabiliste nécessaire utilise les définitions de la norme CEI 61508 qui prend en compte la probabilité de défaillances dangereuses de fonctions de sécurité entières. PROFIsafe suit cette approche (Figure 8).

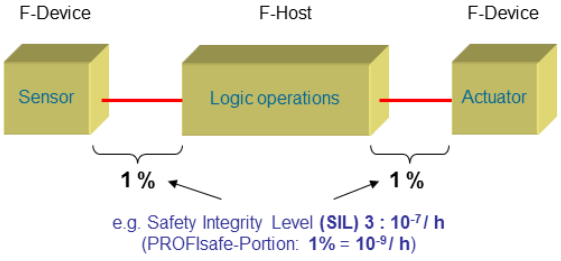

Figure 8 : Fonction de sécurité et SIL

Selon la norme CEI 61508, un circuit de sécurité comprend tous les capteurs, actionneurs, éléments de transfert et processus logiques qui interviennent dans une fonction de sécurité. La norme CEI 61508 définit des valeurs globales pour la probabilité de défaillances pour différents niveaux d'intégrité de la sécurité.

Par exemple, pour le SIL3, il s'agit de 10^{-7}/h. PROFIsafe utilise un polynôme générateur CRC 32 bits soigneusement sélectionné, qui garantit une probabilité de défaillances dangereuses par heure inférieure à 10^{-9}/h. Cette valeur est garantie, indépendamment du « canal noir » utilisé. Ainsi, même dans les applications de SIL3, moins de 1 % du budget global de 10^{-7}/h par fonction de sécurité est consommé par PROFIsafe, ce qui laisse 99% du budget pour les défaillances des capteurs, des actionneurs ou des opérations logiques.

4.2 Formats PROFIsafe

Un message PROFIsafe échangé entre l'hôte F et son appareil F est transporté dans la charge utile d'un message PROFIBUS ou PROFINET standard. Dans le cas d'un appareil F modulaire comportant plusieurs modules F, la charge utile est constituée de plusieurs messages PROFIsafe. La Figure 9 montre le format d'une unité de données de protocole de sécurité (SPDU).

F-Input/Output data	Status / Control Byte	CRC signature
		across F-Parameter, F-I/O data, Status/Control Byte, Monitoring Number
1 to 12/13 (max. 123) bytes	1 byte	4 bytes

Figure 9 : Format de la SPDU PROFIsafe

L'unité de données se compose de trois champs. Le premier champ contient les données Entrée F ou Sortie F en utilisant le sous-ensemble de types de données déjà mentionné. Ces structures de données d'un appareil F particulier sont généralement définies par le biais du fichier GSD (General Station Description) qui lui est associé. Normalement, l'automatisation des usines et des processus impose des exigences différentes à un système de sécurité. L'un concerne les signaux courts (« bit ») qui doivent être traités à très grande vitesse, l'autre concerne des valeurs de traitement plus longues (« virgule flottante ») qui peuvent prendre un peu plus de temps. PROFIsafe recommande d'utiliser 1 à 12/13 octets de données d'Entrée/Sortie F pour les applications d'automatisation industrielle, car tous les hôtes F sont tenus de prendre en charge au moins cette longueur de données. Toutefois, les mesures de PROFIsafe (signature CRC) sont conçues de telle sorte que des données d'une longueur maximale de 123 octets peuvent être prises en charge.

Le deuxième champ est constitué d'un octet de contrôle si la SDPU a été envoyée par l'hôte F ou d'un octet de statut s'il a été envoyé par l'appareil F. Ces informations permettent de synchroniser l'émetteur et le récepteur des SPDU PROFIsafe.

Le troisième champ d'une SPDU PROFIsafe est une signature CRC 32 bits.

Le numéro de suivi n'est pas transmis au sein d'une SPDU PROFIsafe. L'émetteur et le récepteur utilisent leurs propres générateurs de numéros de suivi qui sont synchronisés via l'octet de contrôle et l'octet de statut. La synchronisation correcte est contrôlée par l'inclusion des valeurs du numéro de suivi dans le calcul de la signature du CRC. Les générateurs sont basés sur un générateur de nombres pseudo-aléatoires efficace. Chaque connexion utilise une graine différente pour le générateur, dérivée de son nom de code respectif (« adresse F »).

4.3 Services PROFIsafe

L'émetteur et le récepteur des SPDU PROFIsafe sont situés en couches au-dessus des couches de communication du « canal noir » (Figure 5). Habituellement, ces couches PROFIsafe sont réalisées dans des logiciels (« pilotes »). Leur fonctionnalité centrale est une machine d'état qui contrôle le traitement cyclique régulier des messages PROFIsafe et les exceptions telles que le démarrage, la mise sous/hors tension, le traitement des erreurs CRC, etc. La Figure 10 montre comment les couches PROFIsafe interagissent avec la partie technologique dans les appareils F et avec le programme utilisateur dans les hôtes F.

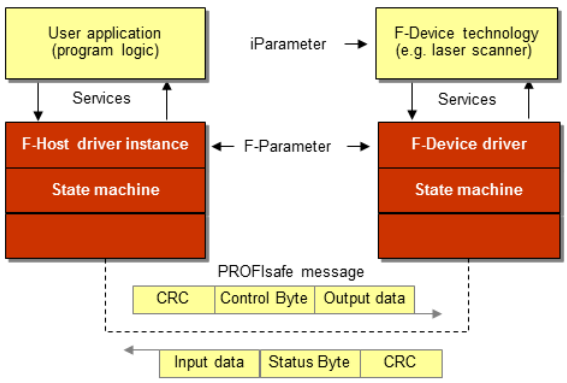

Figure 10 : Structure de la couche PROFIsafe dans les systèmes hôte F et appareil F

Services d'hôtes F

Les principaux services permettent l'échange de données Sortie F et Entrée F. Lors du démarrage, ou en cas d'erreurs, les valeurs réelles du processus sont remplacées par des valeurs à sécurité intégrée (FV). Ces valeurs de sécurité doivent être toutes à « 0 » pour forcer le récepteur à se mettre dans un état sûr (par exemple, se mettre hors tension).

Pour les appareils F dont la mise hors tension n'est pas le seul état de sécurité possible, comme les ventilateurs de brûleur, PROFIsafe fournit des services supplémentaires via un marquage « activate_FV » dans l'octet de contrôle. En retour, un appareil F peut informer le programme utilisateur qu'il a activé son état de sécurité via un marquage « FV_activated » dans l'octet de statut.

Les erreurs de communication PROFIsafe font passer le conducteur de l'hôte F dans un état sûr. Une fonction de sécurité n'est généralement pas autorisée à passer automatiquement d'un état sûr à un fonctionnement normal sans interaction humaine. Pour informer le programme utilisateur qu'une intervention et un acquittement de l'opérateur sont demandés, PROFIsafe fournit un service supplémentaire « OA_Req ». PROFIsafe informe l'appareil F qu'une demande est en cours, de sorte que ce dernier puisse l'indiquer au moyen d'une DEL (facultatif). L'accusé de réception de l'opérateur peut être transmis du programme utilisateur au conducteur de l'hôte F par le biais d'un service correspondant « OA_C ».

Les paramètres spécifiques à la technologie d'un appareil F sont appelés iParamètres. Si un appareil F a besoin de différents iParamètres au moment de l'exécution, une autre série de services est disponible. Le service « iPar_FR » permet au programme utilisateur de faire passer l'appareil F dans un mode au cours duquel il acceptera de nouveaux iParamètres. Le service d'accompagnement « iPar_OK » indique au programme utilisateur la disponibilité à reprendre un fonctionnement normal de sécurité.

Services de disposifs F

Les services PROFIsafe pour la technologie Appareil F comprennent l'échange correspondant de données Sortie F et Entrée F, la possibilité supplémentaire d'activer et de communiquer des valeurs de sécurité, les indicateurs pour le traitement des iParamètres et pour la demande de l'opérateur déjà mentionnée.

En outre, la technologie Appareils F est capable de signaler les défauts des appareils F au pilote de l'hôte F via le marquage « Device_Fault » dans l'octet de statut.

La durée de la demande d'un Appareil F pour une réaction de sécurité doit être suffisamment longue pour être transmise par la communication PROFIsafe (au moins deux numéros de surveillance ultérieurs). Un service spécial informe la technologie sur les nouveaux numéros de suivi afin de faciliter la réalisation de cette exigence.

Les informations de diagnostic de la couche PROFIsafe peuvent être transmises à la partie technologique via un service spécial.

Enfin, la technologie est capable de passer des paramètres F à la couche PROFIsafe. Le dispositf F reçoit ces paramètres F ainsi que tous les autres paramètres lors du démarrage. Quel est l'objectif de ces paramètres F ?

Paramètres F

Les paramètres F fournissent à la couche PROFIsafe des informations qui lui permettent d'adapter son comportement aux besoins particuliers des clients et de vérifier l'exactitude des missions :

- F_S/D_Address (abréviation : « Adresse F »)
- F_WD_Time
- F_SIL
- F_iPar_CRCF_Par_CRC

L'« adresse F » est une identification de connexion unique pour les appareils F/modules F au sein d'une île PROFIsafe et correspond au nom de code. La technologie Appareil F compare cette « adresse F » avec la valeur attribuée localement à un microcommutateur ou avec d'autres informations saisies pour garantir l'authenticité de la connexion.

Le F_WD_Time spécifie un nombre de millisecondes pour une minuterie de chien de garde. Cette minuterie surveille la réception de la SPDU PROFIsafe suivante valide.

F_SIL indique le SIL attendu par l'utilisateur pour un appareil F particulier. Il est comparé aux informations du fabricant stockées localement.

F_iPar_CRC est une signature sur tous les iParamètres de la technologie de l'appareil F.

Enfin, le F_Par_CRC est une signature sur tous les F-Paramètres. Il est utilisé pour assurer la bonne livraison des paramètres F.

5. Quelle mise en œuvre ?

Tout d'abord, il faut s'assurer que toute la documentation nécessaire et utile au travail, et disponible auprès de PI a été obtenue (voir encadré Documentation à la page 11). Utilisez la version indiquée ou une version ultérieure. Une version antérieure V1.30 de la spécification PROFIsafe a été retirée.

Ensuite, il est recommandé d'étudier au moins la norme de sécurité de base CEI 61508 ou d'obtenir des conseils sur ce qui doit être établi dans vos processus de développement et dans votre organisation pour obtenir la sécurité nécessaire pour votre appareil. En règle générale, il n'est pas possible de transformer un appareil standard en un appareil de sécurité en se contentant de mettre en œuvre le protocole PROFIsafe. Cela est dû au fait que PROFIsafe protège contre les erreurs de transmission sur le canal noir, mais pas contre les erreurs survenant au sein même des appareils F. L'architecture de la technologie de sécurité de l'appareil F, ainsi que le protocole et la manière dont ils sont mis en œuvre, définissent le SIL final de l'appareil.

5.1 Classes de sécurité

Même si PROFIsafe est adapté aux fonctions de sécurité jusqu'au niveau SIL3, il n'est peut-être pas nécessaire de concevoir et de développer l'appareil F également pour le niveau SIL3. La classe de sécurité requise dépend de l'application finale du client et de la façon dont les fonctions de sécurité sont définies. Il peut être possible, par redondance ou par d'autres mesures, d'atteindre des niveaux d'intégrité de sécurité plus élevés avec des appareils F d'une classe de sécurité encore plus basse (voir chapitre 9.6. « Appareils PA »).

5.2 Appareil F

Outre la possibilité de mettre en œuvre la spécification PROFIsafe à partir de zéro, des kits de développement sont disponibles sur le marché. Pour plus d'informations, voir le moteur de recherche de produits sur le site de PI. L'avantage d'utiliser un kit de développement est évident : des logiciels de pilotage pré-certifiés, des informations et des outils supplémentaires précieux, ainsi qu'une assistance.

Pour l'interface PROFIBUS et PROFINET, vous pouvez utiliser n'importe quel ASIC et des piles de couches disponibles, et adapter le logiciel du pilote PROFIsafe.

Sécuriser le GSD

Pour chaque appareil sur PROFIBUS ou PROFINET, une description générale de la station (fichier GSD) est nécessaire. Après avoir défini la partie commune de la DSG pour un appareil F, le codage des paramètres F est nécessaire. Cette section des paramètres F doit être protégée par une signature CRC spéciale « F_ParamDescCRC » contre la corruption des données sur les supports de stockage. Un outil de configuration peut vérifier l'intégrité des données de la section de description des paramètres F en utilisant cette signature spéciale, qui fait également partie du fichier GSD.

Sécurisation des configurations

Le fichier GSD contient également des descriptions pour les structures de données Entrée F et/ou Sortie F. Afin de sécuriser cette partie du fichier GSD, une autre signature CRC « F_IO_StructureDescCRC » est utilisée.

iParamètre

En fonction des nombreuses technologies d'appareils de sécurité, il existe une grande variété de paramètres de sécurité individuels (iParameter).

La quantité de iParamètres va de quelques octets pour un module F à plusieurs dizaines de kilo-octets pour un scanner laser. Pour la plupart des appareils de sécurité, il existe déjà des outils logiciels spéciaux de paramétrage et de diagnostic (outil CPD) : Il n'est donc pas logique de traiter les iParamètres via la GSD. PROFIsafe recommande ainsi d'utiliser un nouveau mécanisme, le serveur de paramètres universel (iPar-Server). Il incombe aux fabricants de l'hôte F de fournir cette capacité, qu'elle soit réalisée dans la partie non sécurisée de

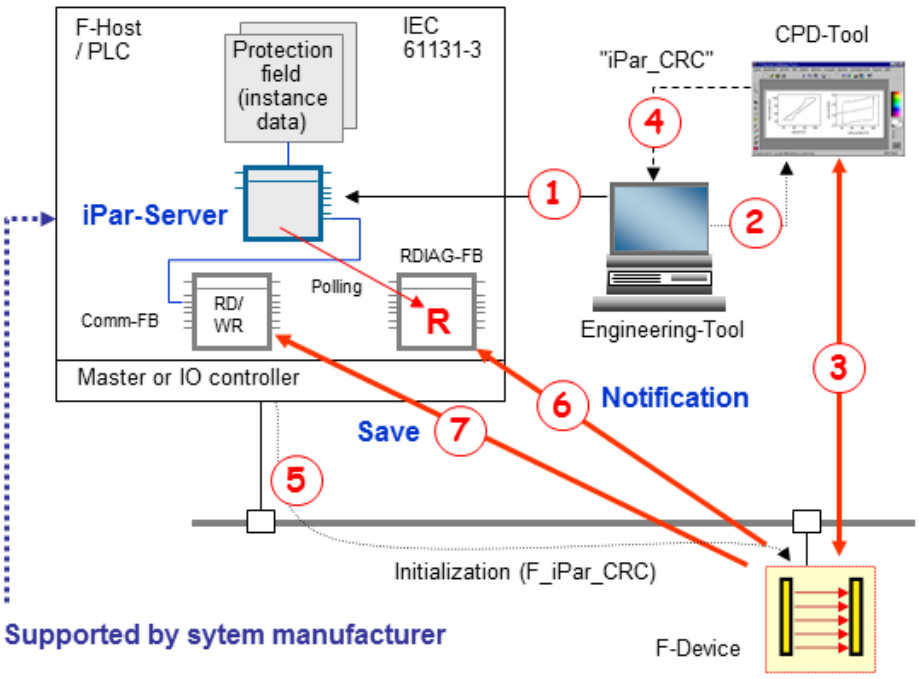

Figure 11 : Le concept de serveur iPar

l'hôte F agissant comme maître de paramétrage du bus de terrain ou dans un sous-système contrôlé tel qu'un automate programmable non sécurisé ou un ordinateur industriel sur le même réseau.

La Figure 11 illustre les principales étapes du mécanisme iPar-Server par un exemple. Avec la configuration du réseau et le paramétrage F d'un appareil F, une fonction iPar-Server associée est instanciée (1). L'appareil F est capable de passer en mode d'échange de données tout en utilisant un état sécurisé (FV). Un outil CPD associé peut être lancé via une interface appropriée (2) telle que TCI (Interface d'appel d'outil) ou FDT (Outil pour les appareils de terrain) à partir de l'outil d'ingénierie, en propageant au moins l'adresse de noeud de l'appareil configuré. Le paramétrage, la mise en service, les tests, etc. peuvent être exécutés à l'aide de l'outil CPD (3). Après finalisation, la signature iPar_CRC est calculée et affichée sous forme hexadécimale pour (au moins) copier et coller cette valeur dans le champ d'entrée « F_iPar_CRC » de la partie configuration de l'outil d'ingénierie (4). Un redémarrage de l'appareil F est nécessaire pour transférer le paramètre « F_iPar_CRC » dans l'appareil F (5). Après la vérification finale et la libération, l'appareil F est autorisé à lancer une notification de téléchargement (6) vers son instance iPar-Server. Il utilise ainsi le mécanisme de diagnostic standard. Le serveur iPar interroge les informations de diagnostic (par exemple RDIAG FB) pour interpréter la demande (R) et établir le processus de téléchargement (7), en stockant les iParamètres comme données d'instance dans l'hôte du serveur iPar en utilisant des services acycliques (Read Record).

Après le remplacement d'un appareil F défectueux, le nouvel appareil F reçoit ses paramètres F, y compris le « F_iPar_CRC », au démarrage. Comme les iParamètres sont normalement manquants dans un appareil F de remplacement ou non retenu, il détecte une différence entre le « F_iPar_CRC » et ses iParamètres stockés et lance une notification de téléchargement (6) vers son instance iPar-Server, en utilisant là encore le mécanisme de diagnostic standard. Le serveur iPar interroge les informations de diagnostic pour interpréter la demande (R) et pour établir le processus de téléchargement (Write Record). Grâce à ce transfert, l'appareil F est en mesure de fournir la fonctionnalité d'origine sans avoir recours à d'autres outils d'ingénierie ou de CPD.

PROFIdrive

La norme CEI 61800-5-2 définit certaines caractéristiques de sécurité pour les entraînements à sécurité intégrée. Ces caractéristiques comprennent un groupe de fonctions d'arrêt :

- Couple de sécurité désactivé (mise hors tension)
- Arrêt de sécurité 1
- Arrêt de sécurité 2
- Arrêt d'exploitation en toute sécurité

Et un groupe d'autres sous-fonctions de sécurité :

- Accélération limitée en toute sécurité
- Vitesse limitée en toute sécurité
- Force/couple limité en toute sécurité
- Position (absolue) limitée en toute sécurité
- Augmentation limitée en toute sécurité
- Direction sûre
- Température du moteur limitée en toute sécurité

La Figure 12 illustre la façon dont l'électromécanique est remplacée par des arrêts de sécurité électroniques et des sous-fonctions de surveillance. Un objectif majeur est de surveiller principalement les opérations de la commande d'entraînement et de ne couper l'alimentation qu'en cas de défaillance. Le groupe de travail PROFIdrive au sein de PI spécifie certaines parties de ces sous-fonctions dans une modification spéciale de sa spécification PROFIdrive (voir l'encadré sur la documentation).

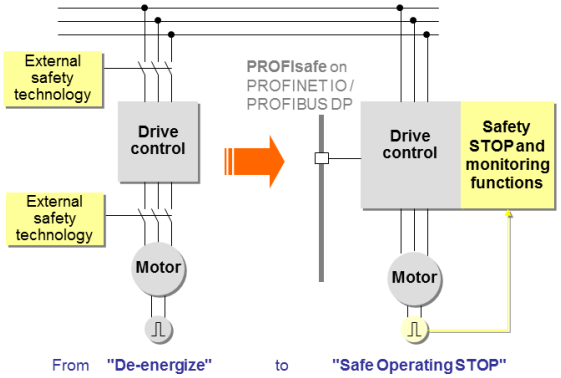

Figure 12 : Entraînements avec arrêt de sécurité intégré et sous-fonctions de surveillance

Appareils PA

Les appareils F pour l'automatisation des processus suivent la norme sectorielle CEI 61511, qui prend en compte l'aspect particulier de la notion « éprouvé en service ». Dans certaines conditions, un appareil PA peut atteindre un meilleur SIL s'il est considéré comme ayant fait ses preuves. Les appareils PA suivent généralement les modèles de conception de la norme CEI 61804. La description des appareils électroniques (EDD) joue un rôle important à cet égard. C'est pourquoi le groupe de travail PI « Appareils PA » a également précisé, dans un amendement distinct à sa spécification sur les appareils PA, comment utiliser la plate-forme PROFIsafe pour ses appareils et ses méthodes de paramétrage (voir l'encadré « Documentation »).

Fonctions I&M

Depuis 2005, les fonctions I&M sont obligatoires pour tous les appareils PROFIBUS et PROFINET fournissant des services acycliques. I&M est l'abréviation de « Identification et Maintenance » et permet de retrouver de manière standardisée des informations sur le code du fabricant de

l'appareil, son catalogue et son numéro de série, ainsi que ses versions matérielles et logicielles. Grâce au code du fabricant et à des informations complémentaires sur le site web de PI, l'utilisateur peut être dirigé vers les informations les plus récentes concernant le produit sur le site web du fabricant. Voir la ligne directrice sur le profil (encadré sur la Documentation).

Diagnostic

L'un des principaux avantages de PROFIBUS et PROFINET est la possibilité pour les appareils de communiquer des informations de diagnostic à l'opérateur dans des situations exceptionnelles telles que des pannes ou des erreurs. De bonnes informations de diagnostic contribuent à réduire les temps d'arrêt des installations et donc les coûts. Les concepts couvrent non seulement la manière de coder les informations, mais aussi la manière de fournir un support en langue étrangère et de fournir des informations d'AIDE sur ce qu'il faut faire dans une situation particulière. Voir la ligne directrice du profil correspondant (encadré sur la Documentation).

Boîte à documentation

- Politique PROFIsafe V1.5 ; Ordre n° 2.282
- PROFIsafe - Profil des technologies de sécurité sur PROFIBUS DP et PROFINET IO, V2.6.1 ; Ordre n° 3.192
- PROFIsafe - Exigences environnementales, V2.6 ; Ordre n° 2.232
- PROFIsafe - Spécification d'essai pour les esclaves F, les appareils F et les hôtes F, V2.2 ; Ordre n° 2.242
- PROFIsafe pour les appareils PA, V1.0.1 ; Ordre n° 3.042
- PROFIdrive sur PROFIsafe, V3.00.4 ; Ordre n° 3.272
- Spécification pour la description des appareils PROFIBUS et l'intégration des appareils, Volume 1 : GSD, V5.1 ; Ordre n° 2.122
- Spécification GSDML pour PROFINET IO, V2.3.2 ; Ordre n° 2.352
- Ligne directrice sur les profils, partie 1 : Fonctions d'identification et de maintenance, V2.0 ; Ordre n° 3.502
- Ligne directrice sur les profils, partie 2 : Types de données, langages de programmation et plates-formes, V1.0 ; Ordre n° 3.512
- Ligne directrice sur les profils, partie 3 : Diagnostic, alarmes et horodatage, V1.0 ; Ordre n° 3.522
- Ligne directrice sur les profils, partie 4 : Serveur des paramètres universels, V1.0.1 ; Ordre n° 3.532
- Diagnostic pour PROFINET IO, V1.1 ; Ordre n° 7.142
- Chemin rapide vers PROFIBUS DP ; Ordre n° 4.072
- Communications industrielles avec PROFINET ; Ordre n° 4.182

5.3. Hôte F

Selon la stratégie des fabricants de systèmes, différents types d'architectures pour les hôtes F avec communication PROFIsafe sont possibles : F-CPU autonomes ou traitement de sécurité intégré mais logiquement séparé au sein d'unités centrales standard.

Structures possibles

Le traitement de la sécurité lui-même peut être réalisé de nombreuses manières différentes : par exemple, par la redondance du matériel et la vérification des écarts ou par la « redondance du logiciel » ou encore par la « sauvegarde » ou en utilisant des plates-formes matérielles diverses déjà existantes. Des kits de développement sont disponibles.

Classes de conformité

Afin de garantir que tous les appareils F seront pris en charge par tous les hôtes F PROFIsafe du marché, PROFIsafe définit des classes de conformité pour les hôtes F. Les hôtes F PROFIsafe doivent satisfaire aux exigences de ces classes de conformité, condition préalable à la certification PI (Figure 13).

6. Conformité et certification

Plusieurs produits de différents types et provenant de divers fournisseurs communiquent au sein d'une île PROFIsafe. Les produits doivent être mis en œuvre conformément à la spécification PROFIsafe pour que cette communication fonctionne correctement. En général, la conformité est documentée par un certificat du bureau de certification PI basé sur le rapport de test émis par l'un des laboratoires de test PI accrédités.

6.1 Les tests PROFIsafe

Les mécanismes du protocole PROFIsafe sont basés sur des machines en état fini. Il a été possible de prouver mathématiquement que PROFIsafe fonctionne correctement, même dans les cas où plus de deux erreurs ou défaillances indépendantes se produisent. Cela a été réalisé en générant systématiquement tous les cas possibles pour les situations de « test to pass » (test pour réussir) et de « test to fail » (test pour échouer). Ils ont été extraits comme cas de test pour un testeur de couche PROFIsafe entièrement automatisé, qui est utilisé pour vérifier la conformité PROFIsafe des appareils F et des hôtes F. Il s'agit d'une partie de la procédure en trois étapes du processus global de certification de la sécurité selon la norme CEI 61508 par les organismes d'évaluation (Figure 13).

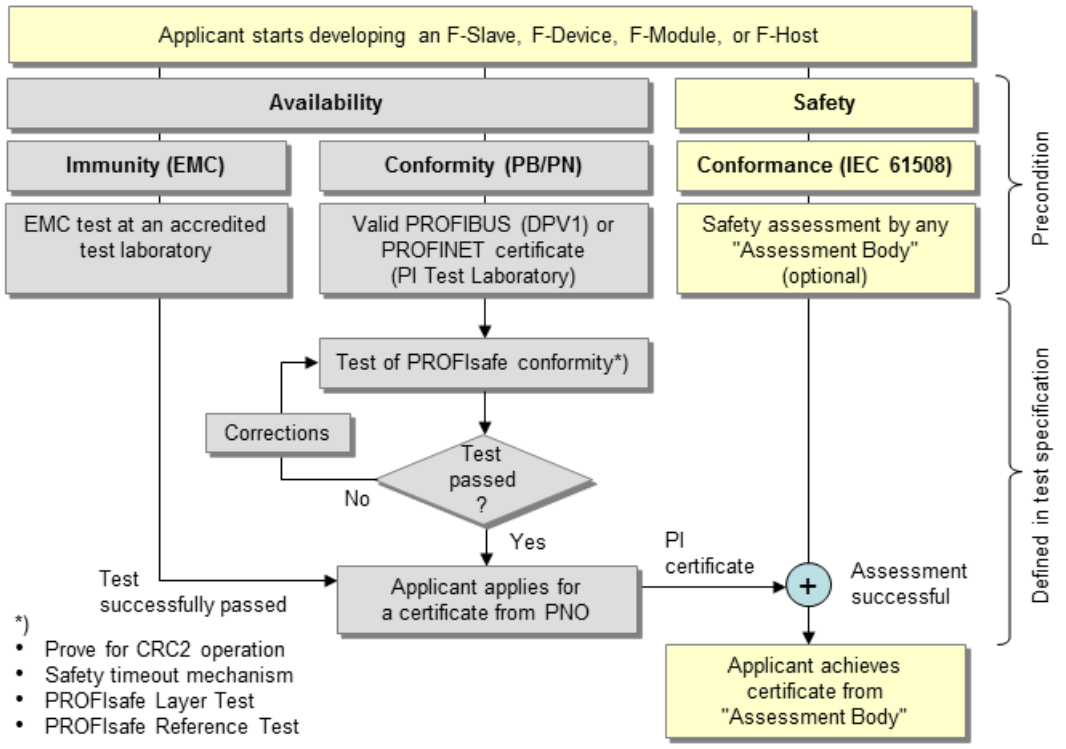

Figure 13 : Procédures d'essai et de certification

6.2 Évaluation de la sécurité

Il est important de noter que les laboratoires d'essai PI effectuent les tests de la couche PROFIsafe approuvés pour le compte d'organismes d'évaluation comme, par exemple :

- TÜV (dans le monde entier)
- IFA (Allemagne)
- SP (Suède)
- SUVA (Suisse)
- HSE (Royaume-Uni)
- FM, UL (ÉTATS-UNIS)

Ce sont les seuls à être responsables des évaluations de sécurité selon la norme CEI 61508.

Le manuel de sécurité obligatoire de chaque appareil F doit fournir des informations sur le SIL_{CL} (limite de réclamation), Cat, PL, et le PFH_d (probabilité de défaillance dangereuse par heure).

PROFIsafe fournit un cahier des charges pour les tests et la certification. Actuellement, quatre laboratoires de test PI sont accrédités pour les tests PROFIsafe dans le monde entier (voir www.profibus.com/test-labs).

7. Déploiement de PROFIsafe

La ligne directrice « PROFIsafe - Lignes directrices environnementales » (voir encadré) traite de tous les aspects environnementaux des protocoles de communication PROFIsafe et répond à des questions telles que :

- Dois-je protéger mon appareil F contre les très hautes tensions qui traversent le câble PROFIBUS /PROFINET en provenance d'une autre source inconnue ?
- Est-il sûr d'utiliser la même alimentation 24 V que celle que j'utilise pour les appareils standard de mon réseau ?
- Comment puis-je tester mes appareils F pour l'« immunité accrue » requise par la norme CEI 61508 ?
- Quelles sont les règles d'installation ?
- Quelles sont les exigences en matière de sécurité ?

Les sections suivantes résument rapidement cette ligne directrice.

7.1 Sécurité électrique

Les normes de bus de terrain CEI 61158 et CEI 61784-1 /-2 exigent que tous les appareils du réseau « soient conformes aux exigences légales du pays où ils sont déployés » (par exemple, comme indiqué

par le marquage CE). Les mesures de protection contre les chocs électriques (c'est-à-dire la sécurité électrique) dans les applications industrielles doivent être basées sur la série de normes CEI 61010, en fonction du type d'appareil qui y est spécifié. Ces mesures sont appelées PELV (Très basse tension protégée) et limitent les tensions autorisées en cas de défaillance à des plages qui ne sont pas dangereuses pour l'homme.

En raison de cette exigence normalement légale, il est possible de limiter l'effort de protection au sein d'un appareil F ou d'un hôte F.

7.2 Alimentation électrique

Il est possible d'utiliser les mêmes alimentations 24 V pour les appareils/hôtes F et standards. Dans les deux cas, les alimentations doivent fournir une PELV en raison des exigences légales.

7.3 Renforcement de l'immunité

Pour chaque application de sécurité, la SRS (Spécification des exigences de sécurité) correspondant doit définir les limites d'immunité électromagnétique (voir CEI 61000-1-1) qui sont nécessaires pour atteindre la compatibilité électromagnétique. Ces limites doivent être établies en tenant compte à la fois des phénomènes électromagnétiques (voir CEI 61000-2-5) et des niveaux d'intégrité de sécurité requis.

Pour les applications industrielles générales, la norme générique CEI 61000-6-7 ou CEI 61326-3-1 définit respectivement les exigences d'immunité pour les équipements qui remplissent ou sont destinés à remplir des fonctions liées à la sécurité.

Les normes de produits telles que la CEI 61496-1 (par exemple, les scanners laser) peuvent définir des exigences d'immunité accrues pour certains phénomènes.

Les conditions environnementales dans les industries de transformation peuvent être différentes de celles des environnements industriels généraux. Ainsi, les exigences spécifiques et les critères de performance décrits dans la norme CEI 61326-3-2 peuvent être utilisés pour les appareils PA.

Pour PROFIsafe, un banc d'essai CEM particulier est défini.

7.4 Haute disponibilité

L'objectif de *sécurité* est de maintenir les *fonctions de sécurité* afin d'éviter que le personnel ne soit blessé, par exemple en désactivant les éléments dangereux. Une mesure caractéristique pour une fonction de sécurité est le SIL (Safety Integrity Level). Il décrit la probabilité d'une défaillance dangereuse de la fonction de sécurité par heure, par exemple 10^{-7}/h pour SIL3. En revanche, l'objectif de *haute disponibilité (tolérance aux pannes)* est de maintenir l'automatisation même en cas de défaillance. Une mesure caractéristique de la haute disponibilité est le rapport entre le temps de disponibilité et la durée totale de fonctionnement, par exemple 99,99 %. La redondance est un moyen qui peut être utilisé conjointement avec d'autres pour atteindre cet objectif.

PROFIsafe est conçu de telle sorte qu'il peut être déployé avec ou sans redondance pour la tolérance aux pannes. La Figure 14 montre les combinaisons possibles.

7.5 Directives d'installation

L'objectif de PROFIsafe est d'intégrer la communication de sécurité dans les réseaux standard PROFIBUS et PROFINET avec un impact minimal sur les directives d'installation existantes. Afin d'obtenir des performances fiables et de satisfaire aux exigences légales, il est fortement recommandé de suivre les spécifications et les lignes directrices PROFIsafe. Certaines questions importantes à prendre en compte sont mentionnées ci-dessous.

	PROFIsafe	Redundancy	PROFIsafe and Redundancy
Application	Factory and process automation: Presses, robots, level switches, shutdown valves, as well as burner control and cable cars	Process automation; Tranportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels	Process automation; Transportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels
High Availability	-	No downtimes at best (fault tolerance)	No downtimes at best (fault tolerance)
Safety	No dangerous failures (required by law or insurances)	Redundancy by itself does not provide safety	No dangerous failures (required by law or insurances)

Figure 14 : Sécurité et haute disponibilité (tolérance aux pannes)

Conditions préalables

Tous les appareils standard et F du réseau doivent être électriquement sûrs, comme indiqué au chapitre 7.1.

Tous les appareils F doivent être certifiés conformément à la norme CEI 61508 et, dans le cas de l'automatisation des processus, conformément à la norme CEI 61511. Ils sont testés et approuvés pour la conformité PROFIsafe par les laboratoires d'essai PI.

Tous les autres appareils standards d'un réseau PROFIsafe doivent prouver leur conformité à PROFIBUS ou PROFINET par un certificat PI ou une preuve équivalente.

Contraintes

Pour PROFIBUS DP, aucun embranchement ou ligne secondaire n'est autorisé.

- Pour PROFINET IO, les règles suivantes s'appliquent :Moins de 100 interrupteurs à la suite
- Un seul hôte F par sous-module
- Tous les composants du réseau doivent être adaptés à l'environnement industriel (par exemple, CEI 61131-2)
- Routeur nécessaire pour séparer les îles PROFIsafe (caractérisé par des noms de code et des adresses F uniques)

Câblage

PROFIBUS et PROFINET indiquent tous deux l'utilisation de câbles blindés et la connexion bilatérale du blindage avec le boîtier du connecteur pour une meilleure immunité électromagnétique. En conséquence, une liaison équipotentielle est généralement requise. Si cela n'est pas possible, des fibres optiques peuvent être utilisées.

Au risque d'une fréquence élevée de déclenchements intempestifs, les concepteurs de machines peuvent utiliser des câbles sans blindage en cas de compatibilité électromagnétique spécifiée, avec des interférences mineures par salves et surtensions.

Disponibilité

Même avec des câbles blindés, un bruit de signal inacceptable peut être introduit sur les lignes de données d'un appareil si, par exemple, la liaison CC intermédiaire d'un convertisseur de fréquence ne filtre pas suffisamment bien. D'autres sources de qualité de signal inacceptable peuvent être dues à l'absence de résistances de terminaison et autres. Il ne s'agit pas d'un problème de sécurité mais de disponibilité. Une disponibilité suffisante des fonctions de contrôle est une condition préalable à la sécurité. Les fonctions de sécurité sur des équipements dont la disponibilité est insuffisante peuvent provoquer des déclenchements intempestifs et, par conséquent, inciter le personnel de production à manipuler ou même à supprimer ces fonctions de sécurité.

Les sociétés PI fournissent de nombreux outils, procédures et listes de contrôle pour étudier la qualité de transmission des réseaux.

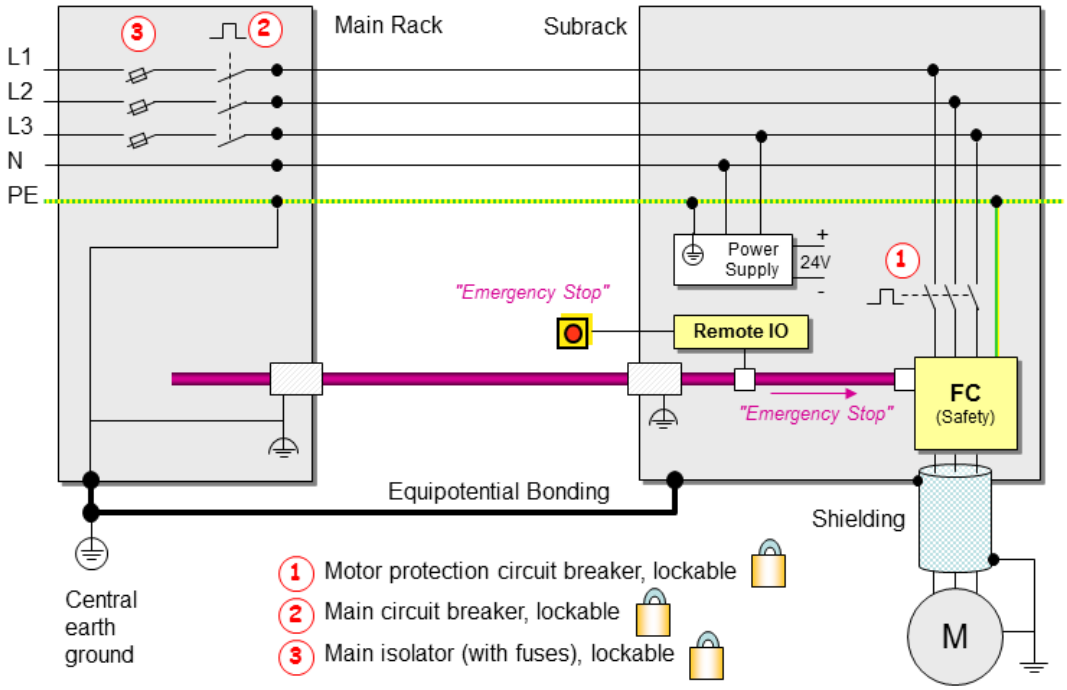

Figure 15 : Concept d'arrêt d'urgence (CEI 60204-1)

PROFIsafe a été la technologie habilitante de nombreux appareils de sécurité, en particulier des entraînements à sécurité intégrée. De nos jours, les entraînements peuvent fournir des états sûrs sans mettre le moteur hors tension. Par exemple, la sous-fonction de sécurité « SOS » (arrêt de fonctionnement sûr) maintient le moteur sous contrôle en boucle fermée dans une certaine position. Cette nouvelle possibilité exige un changement de paradigme pour l'utilisateur. Auparavant, le fait d'appuyer sur un bouton d'arrêt d'urgence provoquait la déconnexion physique des lignes électriques du moteur et, par conséquent, il n'y avait pas de danger électrique pour une personne qui échangeait le moteur.

La nouvelle norme CEI 60204-1 fournit des concepts sur la manière de se protéger contre les chocs électriques (coupure d'urgence) avec des disjoncteurs de protection de moteur verrouillables, des disjoncteurs principaux et des isolateurs principaux avec fusibles. La Figure 15 illustre ces concepts. Elle montre également les connexions recommandées pour les lignes électriques à 5 fils (TN-S) avec des lignes N et PE séparées et les câbles blindés recommandés entre les entraînements et les moteurs. La norme CEI 60204-1 est une source précieuse pour de nombreuses autres questions de sécurité qui complètent la technologie PROFIsafe. La norme nationale correspondante NFPA 79 tient compte de certains écarts pour le marché nord-américain (Figure 3).

7.6 Transmission sans fil

De plus en plus d'applications telles que les véhicules guidés automatiques (AGV), les machines tournantes, les robots à portique et les panneaux d'apprentissage utilisent la transmission sans fil dans les réseaux PROFIBUS et PROFINET. PI précise les détails pour le WLAN et le Bluetooth également. PROFIsafe, avec son mécanisme de détection d'erreurs pour des probabilités d'erreurs sur les bits allant jusqu'à 10^{-2}est approuvé pour toutes sortes de « canaux noirs ». Toutefois, les questions de sécurité ci-dessous doivent être prises en compte en plus.

7.7 Sécurité

PROFINET étant basé sur l'Ethernet industriel en tant que réseau ouvert et en particulier dans le contexte de la transmission sans fil, la question de la sécurité a été soulevée.

PI pousse le concept de construction de zones dites de sécurité qui peuvent être considérées comme des réseaux fermés (Figure 16). La seule possibilité de traverser des réseaux ouverts tels que les dorsales d'Ethernet industriel d'une zone de sécurité à une autre est de passer par des *Portes de sécurité*. Les *Portes de sécurité* utilisent des mécanismes généralement acceptés tels que le VPN (Réseau privé virtuel) et les pare-feu pour se protéger contre les intrusions. Les réseaux PROFIsafe doivent toujours être situés à l'intérieur de zones de sécurité

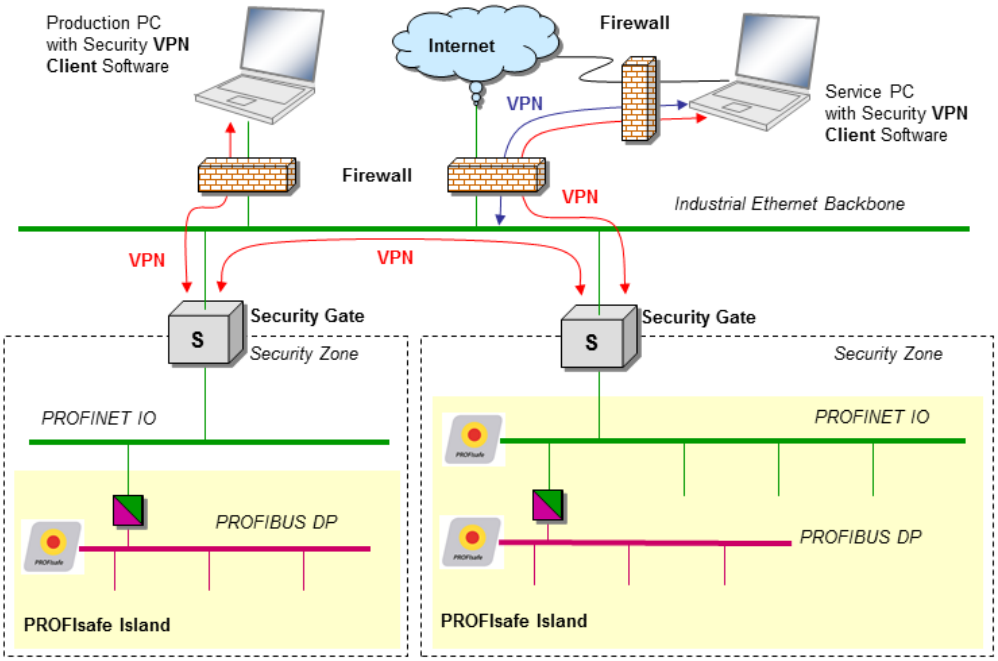

Figure 16 : Concepts de sécurité pour les réseaux « fermés » et « ouverts »

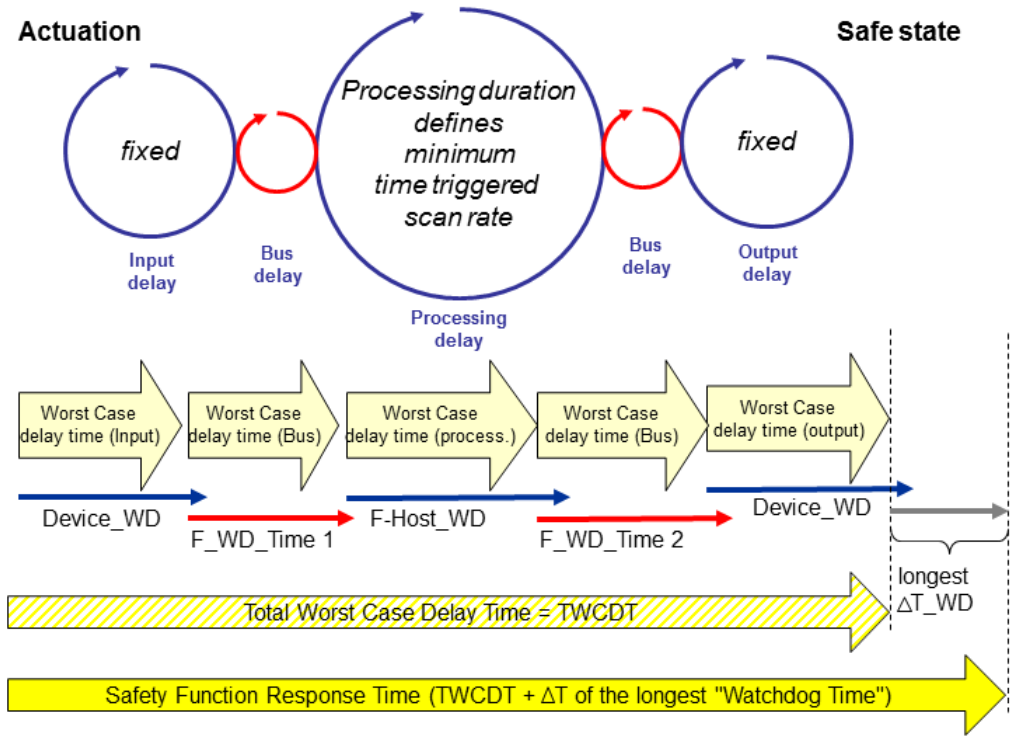

Figure 17 : Temps de réponse de la fonction de sécurité (SFRT)

et protégés par *Portes de sécurité*. Si des connexions aux réseaux ouverts ne peuvent être évitées, se référer à la directive de sécurité PROFINET, V2.0 ; Ordre n° 7.002.

Pour la transmission sans fil, la norme IEEE 802.11 prévoit des mesures de sécurité suffisantes pour les réseaux PROFIsafe. Seul le mode Infrastructure est autorisé ; le mode Adhoc ne doit pas être utilisé. Vous trouverez plus de détails dans la spécification PROFIsafe.

7.8 Temps de réponse

Habituellement, les temps de réponse des fonctions de contrôle normales sont assez rapides pour les fonctions de sécurité également. Toutefois, certaines applications de sécurité à délai de réponse critique nécessitent une étude plus approfondie des temps de réponse des fonctions de sécurité (SFRT), comme les presses protégées par des barrières immatérielles. Un concepteur de machine doit savoir à quelle distance le rideau lumineux doit être monté de la presse dangereuse. Il est communément admis qu'une main se déplace au maximum de 2 m/s. La distance minimale à considérer est alors s = 2 m/s x SFRT si la résolution du rideau lumineux est suffisamment élevée pour détecter un seul doigt (EN 999). Sinon, des sommations de correction sont nécessaires.

Le modèle de la Figure 17 est utilisé pour expliquer le calcul du SFRT. Le modèle comprend un équipement F d'entrée, une transmission par bus PROFIsafe, le traitement du signal dans un hôte F, une autre transmission par bus PROFIsafe et un équipement F de sortie, chacun ayant ses propres temps de cycle statistiques. Le temps maximum pour qu'un signal de sécurité passe à travers cette chaîne est appelé TWCDT (pour Total Worst Case Delay Time), étant donné que toutes les parties nécessitent leur temps de cycle maximum particulier. En cas de sécurité, les considérations vont encore plus loin : Le signal pourrait être encore plus retardé si l'une des parties tombe en panne à ce moment-là. Il faut donc ajouter un temps delta pour cette partie particulière qui représente la différence maximale entre son temps de garde et son temps de retard dans le pire des cas (il n'est pas nécessaire de considérer plus d'une défaillance à la fois). Finalement, le TWCDT plus ce temps delta forment le SFRT.

Chaque appareil F doit fournir des informations sur son délai d'attente le plus défavorable, conformément à la spécification PROFIsafe, afin que les outils d'ingénierie puissent estimer les SFRT.

8. Pour les intégrateurs

8.1 Directives et normes

Dans de nombreux pays, les exigences de sécurité pour les machines dangereuses sont réglementées par la loi. Au sein de l'UE, il s'agit de la directive Machines 2006/42/CE. Cette directive contient une liste de normes dites harmonisées. Pour un constructeur de machines, il existe une présomption de conformité aux directives si les normes pertinentes sont respectées.

Les normes pertinentes dans le contexte de PROFIsafe sont, par exemple, les normes CEI 62061, ISO 13849 et ISO 12100 (voir chapitre 1.3. et Figure 2).

8.2 Stratégie de réduction des risques

Il est toujours préférable de concevoir une machine avec une sécurité inhérente telle qu'elle évite tout danger. Dans sa première partie, la norme ISO 12100 énumère toutes sortes de dangers possibles. Dans sa deuxième partie, elle présente une stratégie itérative sur la manière de réduire le risque de tout équipement automatisé par le biais d'une évaluation des risques. Cette évaluation des risques consiste en une analyse et une évaluation des risques :

- Préciser les limites et l'utilisation prévue de la machine
- Identifier les dangers et les situations dangereuses associées pendant tout le cycle de vie de la machine
- Estimer le risque pour chaque danger et situation dangereuse identifiés
- Évaluer le risque et prendre des décisions sur la nécessité de réduire les risques

En utilisant la « méthode des trois étapes »

- des mesures de conception intrinsèquement sûres, des mesures de
- sauvegarde et éventuellement des mesures de protection complémentaires,
- des informations à utiliser sur le risque résiduel,

le concepteur peut éliminer les dangers ou réduire le risque associé à ces dangers par des mesures de protection.

Les mesures de sauvegarde et de protection complémentaires sont la mise en place de fonctions de sécurité telles qu'un rideau lumineux, le fonctionnement logique associé et un disjoncteur pour mettre le moteur hors tension.

8.3 Application de la norme CEI 62061

Les normes CEI 62061 et ISO 13849 fournissent toutes deux des méthodes pour traiter les fonctions de sécurité. Si la norme CEI 62061 s'adapte bien à la technologie PROFIsafe et aux automates programmables de sécurité (hôtes F), la norme ISO 13849 comble le vide pour les composants hydrauliques, pneumatiques, électriques et mécaniques.

La norme CEI 62061 exige un plan de sécurité pour l'ensemble du cycle de vie de la machine, couvrant les stratégies de conception, les rôles et responsabilités du personnel, la mise en service, le changement et la maintenance jusqu'au démontage.

Les normes ISO et CEI sont maintenant désireuses d'harmoniser et d'améliorer les deux approches des normes CEI 62061 et ISO 13849 par le biais du projet « ISO/CEI 17305 » (Figure 2).

8.4 Évaluation des risques

Les normes de sécurité fonctionnelle proposent des concepts similaires pour l'évaluation des risques des fonctions de sécurité, sur la base de la norme ISO 12100 :

Risque = gravité du préjudice et probabilité d'occurrence de ce préjudice

La probabilité d'occurrence est constituée par l'exposition des personnes, l'occurrence et la possibilité d'évitement.

8.5 Détermination des SIL/PL/Cat

Les normes CEI 62061 et ISO 13849 fournissent toutes deux des caractéristiques calculées. L'une est le SIL requis et l'autre le PL et la catégorie requis (voir chapitre 1.3.). Il est possible de transformer l'un en l'autre. À long terme, on peut s'attendre à ce que la différence disparaisse pour l'utilisateur lorsque l'évaluation des risques est effectuée dans des outils d'ingénierie par le biais de « questionnaires ». On s'attend à ce que la nouvelle norme ISO/CEI 17305 soit utile à cet égard.

8.6 Conception de la fonction de sécurité

La norme CEI 62061 définit ce qu'on appelle le système de commande électrique lié à la sécurité (SRECS) pour les fonctions de sécurité avec des sous-systèmes de détection, de traitement et d'actionnement. Les sous-systèmes peuvent contenir des éléments (par exemple des interrupteurs).

La façon la plus simple de concevoir une fonction de sécurité est d'utiliser des appareils F certifiés ou préévalués (capteurs, actionneurs) et un hôte F certifié connecté via PROFIsafe.

8.7 SIL atteint

Les appareils F fournissent les informations nécessaires dans leur manuel de sécurité pour déterminer le SIL atteint d'une fonction de sécurité particulière. Dans un premier temps, le plus petit SIL_{CL} (limite de réclamation) de tous les appareils de sécurité (appareils F, hôtes F) est sélectionné. Cela détermine le SIL maximal réalisable de l'ensemble de la fonction de sécurité. Dans certains cas, les fabricants de systèmes peuvent offrir une assistance système pour passer à un SIL plus élevé grâce à la redondance des appareils F et des logiciels système correspondants.

Dans un deuxième temps, les valeurs PFH_d sont additionnées et le résultat est comparé aux fourchettes de valeurs autorisées pour un SIL particulier.

La valeur la plus faible de ces deux étapes détermine le SIL réalisable.

Dans les sections suivantes, vous verrez comment vous pouvez combiner les modules F dans les E/S/à distance avec les appareils de sécurité électromécaniques classiques tels que les boutons d'arrêt d'urgence, les interrupteurs de porte, etc. comme le montre la Figure 4.

8.8 Électromécanique

La norme CEI 62061 prévoit quatre architectures prédéterminées A, B, C et D pour les sous-systèmes permettant de connecter des appareils de sécurité classiques. Des formules permettant de calculer les probabilités de défaillance sont fournies pour ces circuits. Avec l'aide des valeurs B_{10}pour les interrupteurs mécaniques, le nombre estimé de cycles de commutation, la couverture du diagnostic et un facteur de cause commune, la probabilité nécessaire de défaillances dangereuses peut être calculée à l'aide des formules et ajoutée pour déterminer le SIL global.

8.9 Pièces non électriques

La norme ISO 13849-1 définit ce qu'on appelle les SRP/CS (Safety-Related Parts of Control Systems, pièces relatives à la sécurité des systèmes de commande) également pour les composants hydrauliques, pneumatiques, électriques et mécaniques. Une valeur PL et PFH_d peut être déterminée pour un tel composant à l'aide de cette norme et transformée en détermination du SIL pour la fonction de sécurité selon la norme CEI 62061.

8.10. Validation

La norme CEI 62061 exige qu'un plan de validation fasse partie du plan de sécurité global. Selon ce plan, la machine doit être testée, contrôlée et documentée.

9. Familles des appareils F

PROFIsafe, en tant que technologie habilitante, a ouvert de nouvelles possibilités pour les appareils standards et de sécurité. Le présent chapitre donne un bref aperçu de quelques appareils F importants et d'applications typiques.

9.1 E/S à distance

Les E/S à distance standards peuvent désormais intégrer des modules de sécurité sans changer les stations de tête. Des modules F tels que l'entrée/sortie numérique, l'entrée/sortie analogique, les modules de puissance, les démarreurs de moteur et les convertisseurs de fréquence à sécurité intégrée sont disponibles. Les modules F peuvent être regroupés et permettent la fermeture en groupe. Les boutons d'arrêt d'urgence nécessitent des inspections annuelles très coûteuses car chaque bouton doit être testé individuellement. La nouvelle technologie permet de collecter facilement tous les événements survenus au cours de l'année. De cette façon, seuls les boutons non actionnés restants doivent être testés, ce qui permet de réaliser des économies.

9.2 Capteurs optiques

Les capteurs optiques de sécurité tels que les rideaux lumineux et les scanners laser sont normalisés dans le cadre de la norme CEI 61496. Les capteurs optiques sont parfaitement adaptés pour protéger les portails d'entrée et de/sortie de manière flexible. L'exemple de la Figure 18 montre également comment PROFIsafe complète les appareils de sécurité des scanners et lecteurs laser par une sécurité intégrée. Voir les détails ci-dessous.

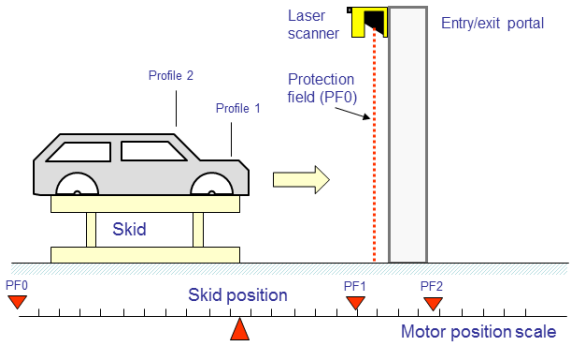

Figure 18 : Logiciel « Capteurs de silencieux » pour les scanners laser

9.3 Entraînements

Les sous-fonctions de sécurité des entraînements sont normalisées dans la norme CEI 61800-5-2. Ces sous-fonctions de sécurité nécessitent généralement un indicateur de position de sécurité. Cette valeur est accessible à l'utilisateur via PROFIsafe et peut remplacer les interrupteurs physiques de « fin de course » ou les capteurs physiques de « silencieux ». Comme le montre la

Figure 18, la position du moteur affecte les champs de protection des scanners laser en fonction des profils des carrosseries de voitures aux portails d'entrée/sortie d'une cellule de fabrication.

La section 5.2 énumère de nombreuses autres sous-fonctions de sécurité possibles qui entraîneront des applications révolutionnaires dans un avenir proche.

9.4 Robots

Les nouvelles sous-fonctions de sécurité pour les entraînements encouragent les robots à intégrer ces fonctions et fournissent de nouvelles fonctionnalités telles que les « robots collaboratifs », où les personnes travaillent main dans la main avec les robots.

9.5 Passerelles F

Pour PROFIsafe, il existe des passerelles F vers AS-i Safety-at-work (ASIsafe). Ces appareils combinent les avantages des deux mondes. Alors qu'ASIsafe peut facilement collecter les signaux de nombreux boutons d'arrêt d'urgence connectés en série, PROFIsafe est aisément capable de traiter des appareils F sophistiqués tels que des entraînements à sécurité intégrée.

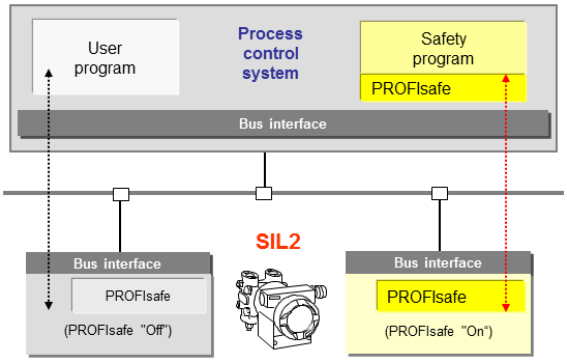

Figure 19 : PROFIsafe et NE97 pour les appareils PA

9.6 Apapreils PA

Il a déjà été mentionné que la sécurité de l'automatisation des processus suit sa propre norme sectorielle CEI 61511. La NAMUR, en tant qu'organisme de normalisation pour les industries chimiques et pharmaceutiques, publie la norme complémentaire NE97 qui précise comment la communication de sécurité peut être utilisée avec les appareils de sécurité sur le terrain. Un appareil PA « éprouvé en service », équipé d'une interface PROFIBUS MBP-IS, accueille un pilote PROFIsafe qui peut être configuré en mode « Arrêt » ou « Marche ». En mode « Arrêt », il représente un appareil PA standard, en mode « Marche », un appareil F (Figure 19).

Par ailleurs, la NAMUR a lancé une autre norme complémentaire, la VDI 2180, qui facilite le développement d'appareils PA liés à la sécurité.

Actuellement, la plupart des applications PROFIsafe dans le domaine de l'automatisation des processus déploient des entrées/sorties à distance avec des modules F pour la communication 4-20 mA ou HART. La Figure 20 illustre les deux possibilités d'utilisation de PROFIsafe avec des appareils PA « éprouvés en service ». Il s'agit d'un bon compromis même s'il souffre de l'absence des avantages directs du bus de terrain tels que les mesures à large gamme, le paramétrage et le diagnostic sophistiqué.

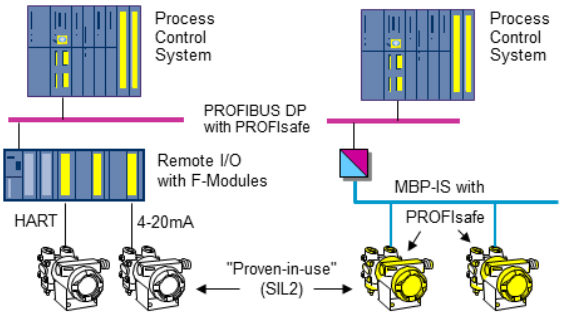

Figure 20 : Deux possibilités pour les appareils PROFIsafe et PA

Commutateurs de niveau

Les contacteurs de niveau pour réservoirs bénéficient largement de la technologie PROFIsafe. PROFIBUS PA, avec ses technologies de transmission antidéflagrantes MBP-IS et RS485-IS, répond parfaitement aux exigences de ces appareils F. PROFIsafe assure la transmission sécurisée des signaux d'arrêt, tandis que le « canal noir » standard informe l'utilisateur de l'état des capteurs.

Valves ESD

Des améliorations similaires peuvent être obtenues pour les vannes ESD (Electronic Shut-Down, arrêt électronique). L'objectif principal est ici de tester périodiquement la fonction de la vanne par des « courses partielles de la vanne » et un suivi de la tendance de la position finale et du temps écoulé pour atteindre cette position. Cela peut être fait automatiquement via les hôtes F et permet une maintenance prédictive chaque fois que cela est pratique pour l'utilisateur. La communication RS485-IS associée aux barrières permet une mise hors service rapide même dans un environnement Ex-i.

Transmetteur de pression

Les transmetteurs de pression sûrs combinent la fonction de mesure du remplissage du réservoir et de protection contre le débordement (« détecteur de niveau ») par comparaison avec une valeur de consigne.

Capteurs de gaz et de feu

Ces capteurs sont en service sur les plateformes pétrolières sans équipage par exemple. Des informations complémentaires sur la position permettent de fermer automatiquement les écoutilles concernées.

10. Avantages pour les utilisateurs

Dans l'intervalle, plus de 5 millions de nœuds PROFIsafe ont été installés.

Plus de 50 millions d'appareils PROFIBUS et plus de 10 millions d'appareils PROFINET ont été installés à ce jour.

Par conséquent, la priorité en matière de développement a toujours été et continuera d'être de veiller à ce que le système reste pleinement compatible avec les appareils déjà en service.

Grâce au protocole de communication de sécurité fonctionnelle autonome de PROFIsafe et à son approche « canal noir », il est même possible de passer de PROFINET à PROFIBUS sans difficultés majeures. Le même logiciel pilote PROFIsafe peut être utilisé dans les appareils PROFINET et PROFIBUS.

- L'introduction de PROFIsafe a provoqué un saut quantique en trois étapes :De la logique de relais de sécurité à la logique programmable de sécurité
- De la communication multifilaire à la communication en série fonctionnelle et sûre
- Des appareils de sécurité isolés à ceux qui coopèrent

Les déclarations suivantes résument parfaitement les avantages de plusieurs points de vue.

10.1 Intégrateurs et utilisateurs finaux

- Mêmes économies qu'avec l'introduction du PROFIBUS standard : réduction du câblage, flexibilité des configurations, paramétrage et diagnostic
- Conception de systèmes simples et rentables avec une large gamme de produits de tous types de fabricants
- En général, aucune restriction particulière en matière d'installation
- Des applications de sécurité très innovantes grâce à une communication aisée entre des appareils F sophistiqués
- Grande souplesse dans le remplacement de la technologie des relais existants ainsi que dans l'extension et la modernisation des installations existantes
- Technologie intégrée pour l'automatisation des usines et des processus
- Formation, documentation et maintenance requises pour une seule technologie de bus
- Programmation d'applications standards et liées à la sécurité avec un seul outil et des blocs de fonctions certifiés
- Documentation aisée des configurations et des logiques liées à la sécurité
- L'acceptation de systèmes à moindre coût grâce à des appareils certifiés
- Acceptation internationale grâce à une technologie conforme à la norme CEI 61508.
- Évaluations positives par l'IFA et le TÜV

10.2 Fabricants d'appareils

- Un logiciel certifié par le TÜV permet une mise en œuvre facile et une reproduction économique d'une solution PROFIsafe
- Différentes architectures de contrôleurs programmables de sécurité peuvent adopter la communication PROFIsafe
- Pionnier des nouvelles fonctions innovantes des appareils

10.3 Pour les investissements futurs

- Vaste base installée d'appareils PROFIBUS et PROFINET
- Les organisations et centres de soutien PROFIBUS/PROFINET sont présents dans le monde entier
- Utilisation de toutes les normes existantes et futures définies par PI également pour les applications liées à la sécurité
- PROFIsafe est une norme internationale de la CEI 61784-3-3 et la norme GB/T en Chine
- Futur logiciel pour assister le cycle de vie des applications de sécurité depuis la conception jusqu'à l'évaluation, la validation et la documentation, ce qui réduira encore les efforts

11. PROFIBUS et PROFINET International (PI)

En ce qui concerne la maintenance, le développement continu et la pénétration du marché, les technologies ouvertes ont besoin d'une institution indépendante de l'entreprise qui puisse servir de plate-forme de travail. En ce qui concerne les technologies PROFIBUS et PROFINET, cela a été réalisé en fondant la PROFIBUS Nutzerorganisation e.V. (PNO) en 1989 sous la forme d'un groupe d'intérêt à but non lucratif pour les fabricants, les utilisateurs et les institutions. La PNO est membre de PI (PROFIBUS &PROFINET International), un groupe de coordination fondé en 1995. PI compte aujourd'hui plus de 25 organisations régionales

d'utilisateurs (RPA : Regional PI Associations) et environ 1 400 membres, ce qui signifie qu'elle est représentée sur tous les continents et constitue le plus grand groupe d'intérêt au monde dans le domaine des communications industrielles (Figure 21).

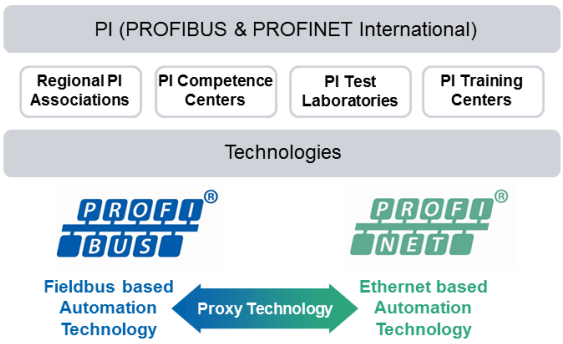

Figure 21 : PROFIBUS et PROFINET International (PI)

11.1 Responsabilités de PI

Les principales tâches effectuées par PI sont les suivantes :

- Maintenance et développement de PROFIBUS et PROFINET
- Promotion de l'implantation mondiale de PROFIBUS et PROFINET
- Protection des investissements des utilisateurs et des fabricants par l'influence sur la normalisation internationale
- Représentation des intérêts des membres auprès des organismes de normalisation et des syndicats
- Soutien technique mondial aux entreprises par l'intermédiaire des centres de compétence PI (PICC)
- Contrôle de la qualité par un système de certification des produits dans les laboratoires d'essai PI (PITL) basé sur des tests de conformité standardÉtablissement d'une norme de formation mondiale par le biais des centres de formation PI (PITC)

11.2 Développement technologique

PI a confié la responsabilité du développement technologique à la PNO en Allemagne. Le conseil consultatif de PNO Allemagne supervise les activités de développement. Le développement technologique s'effectue dans le cadre de plus de 50 groupes de travail avec la participation de plus de 500 experts.

11.3 Support technique

PI soutient plus de 50 PICC accrédités dans le monde entier. Ces installations fournissent aux utilisateurs et aux fabricants toutes sortes de conseils et de soutien. En tant qu'institutions de PI, elles sont des prestataires de services indépendants et adhèrent à des règlements mutuellement convenus. Les PICC sont régulièrement contrôlés pour vérifier leur adéquation dans le cadre d'un processus d'accréditation personnalisé. Les adresses actuelles se trouvent sur le site web de PI.

11.4 Certification

PI soutient 10 PITL accrédités dans le monde entier, qui aident à la certification des produits avec une interface PROFIBUS/PROFINET. En tant qu'institutions de PI, ils sont des prestataires de services indépendants et adhèrent à des règlements mutuellement convenus. Les services de test fournis par les PITL sont régulièrement audités selon un processus d'accréditation strict afin de s'assurer qu'ils répondent aux exigences de qualité nécessaires. Les adresses actuelles se trouvent sur le site web de PI.

11.5 Formation

Les PITC ont été mis en place dans le but spécifique d'établir une norme de formation globale pour les ingénieurs et les techniciens d'installation. Les centres de formation et leurs experts sont officiellement accrédités. Leur compétence en matière de formation PROFIBUS et PROFINET et de services d'ingénierie et d'installation associés avait été vérifiée. Une formation de trois jours « Concepteur certifié PROFIsafe » existe pour PROFIsafe. Les adresses actuelles se trouvent sur le site web de PI.

11.6 Internet

Le site web de PI www.profibus.com met à disposition des informations réelles sur l'organisation de PI et les technologies PROFIBUS et PROFINET. Vous y trouverez un outil de recherche de produits en ligne, un glossaire, diverses formations en ligne, ainsi que la zone de téléchargement avec des spécifications, des profils d'application, des directives d'installation et d'autres documents.

Place pour les notes

Description du système PROFIsafe
Technologie et application

Version avril 2016
Numéro d'ordre 4.342

Éditeur :

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 • 76131 Karlsruhe • Allemagne
Téléphone : +49 721 96 58 590 • Fax : +49 721 96 58 589
Courrier électronique : info@profibus.com
www.profibus.com • www.profinet.com

Exclusion de responsabilité

Bien que la PROFIBUS Nutzerorganisation e.V. (PNO) ait apporté le plus grand soin à la compilation des informations contenues dans cette brochure, elle ne peut garantir que le contenu soit totalement exempt d'erreurs, et l'organisation PROFIBUS Nutzerorganisation e.V. (PNO) ne peut assumer aucune responsabilité, quelle que soit la base juridique des éventuelles réclamations. Les informations contenues dans cette brochure sont régulièrement révisées. Les corrections nécessaires seront apportées dans les éditions suivantes. Nous vous serions reconnaissants de nous faire part de vos suggestions pour en améliorer le contenu.

Toutes les désignations qui figurent dans cette brochure pourraient potentiellement constituer des marques. Toute utilisation de ces marques par des tiers à leurs propres fins risque de porter atteinte aux droits des propriétaires concernés.

Cette brochure n'est pas destinée à remplacer les normes CEI pertinentes, telles que les normes CEI 61158 et CEI 61784, ou les spécifications et directives pertinentes de PROFIBUS et PROFINET International. En cas de doute, ces normes, spécifications et lignes directrices font autorité.© Copyright by PROFIBUS Nutzerorganisation e.V. (PNO) 2016, tous droits réservés.

Un soutien mondial avec PI !

Pour plus d'informations et les coordonnées de contact, consultez le site : www.profibus.com/pi-organization/

Association régionale PI (RPA)	Les associations régionales PI (RPA) représentent PI dans le monde entier et sont vos points de contact locaux. Elles sont responsables des activités de marketing local pour la diffusion de PROFIBUS, PROFINET et IO-Link, qui comprennent entre autres des participations à des salons, des séminaires, des ateliers et des conférences de presse, ainsi que des activités de relations publiques.
Centre de compétence PI (PICC)	Les centres de compétence PI (PICC) collaborent étroitement avec les RPA et sont votre premier point de contact lorsque vous avez des questions techniques. Les PICC sont à votre disposition pour vous aider dans le développement des appareils PROFIBUS ou PROFINET et la mise en service des systèmes, et ils fournissent une assistance et une formation aux utilisateurs.
Centre de formation PI (PITC)	Les Centres de formation PI (PITC) aident les utilisateurs et les développeurs à acquérir de l'expérience avec les technologies PROFIBUS et PROFINET et leurs utilisations possibles. Les personnes qui réussissent l'examen final du cours d'installateur ou d'ingénieur certifié reçoivent un certificat de PI.
Laboratoire d'essai PI (PITL)	Les Laboratoires d'essai PI (PITL) sont autorisés par PI à effectuer des tests de certification pour PROFIBUS et PROFINET. Vous recevez un certificat de PI pour votre produit une fois qu'il a passé le test avec succès. Le programme de certification joue un rôle majeur dans l'assurance qualité durable des produits et garantit ainsi que les systèmes utilisés présentent un niveau élevé de fonctionnement et de disponibilité sans problème.

© Copyright par PI 4/16 - tous droits réservés - 4.342

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 • 76131 Karlsruhe · **Allemagne**
Téléphone : +49 721 96 58 590 - • Fax : +49 721 96 58 589
E-Mail : info@profibus.com
www.profibus.com • www.profinet.com