Les BUS de Sécurité

On ne plaisante pas avec la sécurité. Que celle-ci concerne les personnes ou le matériel, elle constitue une notion d'importance croissante, dans tous les secteurs de production industriels. De plus en plus, en effet, " sécurité " rime avec " productivité".

Et comme toujours quand il s'agit de productivité, on cherche à améliorer, à optimiser : par exemple pour gagner de précieuses minutes lors des opérations de maintenance ; ou encore pour ne pas mettre hors service l'ensemble d'une installation lorsqu'il n'est nécessaire d'en isoler qu'une partie. D'autres contraintes, comme la nécessité rencontrée parfois de redémarrer une application sous des conditions initiales précises, ont poussé les ingénieurs à mettre au point des systèmes de sécurité toujours plus intelligents, intégrant des fonctionnalités toujours plus complexes et évoluées.

Avec l'apparition des bus de terrain, il y a une vingtaine d'années, et le développement des technologies de communication, les milieux industriels ont connu une révolution majeure, tant dans la manière de véhiculer les informations issues des capteurs et actionneurs, que dans celle de piloter les applications. Les bénéfices ont été largement décrits : réduction des coûts de câblage, d'ingénierie, de maintenance, de flexibilité …

Mais pendant longtemps, cela n'a concerné que les équipements de contrôle commande, et pas la sécurité. En effet, jusqu'il y a quatre ou cinq ans, il n'était pas question de mêler sécurité et bus de terrain. Pas assez sûrs, pas assez performants, pas assez ouverts.

Aujourd'hui la donne a changé et les mentalités ont évolué. Les technologies de la communication de terrain sont désormais éprouvées, et il ne se pose plus de problèmes de sécurité intrinsèques aux supports ou aux protocoles utilisés. Des automates spécialement dédiés au traitement des informations de sécurité ont été développés (voir notre article sur les APIdS dans le numéro 29 de la revue), et c'est tout naturellement que les premiers bus de sécurité ont vu le jour, dès 1999.

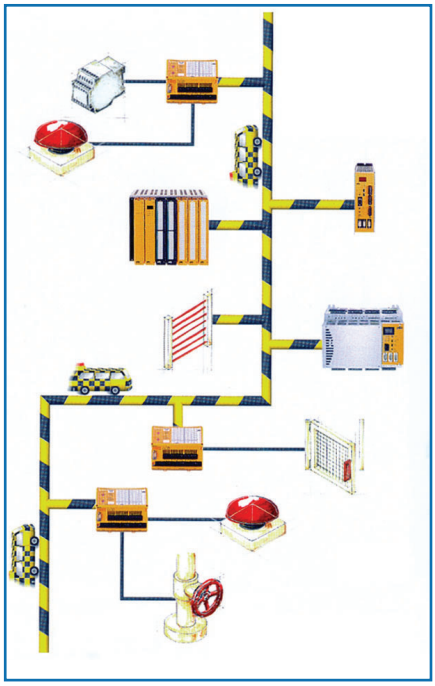
Tout d'abord cantonnés aux applications de sécurité " simples " dans les domaines de l'industrie manufacturière et du batch, ils font aujourd'hui leur apparition dans l'industrie de process, preuve que la complexité des procédures de sécurité ne constitue plus un frein à la démocratisation des bus dédiés.

Il existe aujourd'hui différents types de bus de sécurité, parmi lesquels des solutions exclusivement dédiées à la sécurité comme le Safetybus p ou des solutions venant s'intégrer à une offre de bus de terrain existante. C'est le cas de Profibus avec Profisafe, As-interface avec As-i Safety at Work …

Safety, niveau 4

Historiquement, la société Pilz fut la première à se lancer sur le marché des bus de sécurité, avec le développement d'automatismes dédiés (automates, blocs d'entrées-sorties déportés, etc..), puis la définition d'un protocole de communication orienté sécurité, dérivé du CAN et baptisé Safetybus p.

Comme le précise Olivier Arbogast, chef de produit chez Pilz : *" Nous sommes partis d'un système basé sur CanOpen. Des modifications ont été apportées au niveau de la couche d'échange de données CSMD afin de rendre le protocole plus sûr. Avec de nouvelles fonctionnalités de contrôle des signaux intégrées, des fonctions timers pour l'envoi et la réception des messages, et des fonctionnalités de diagnostic intégrées ; Safetybus p est un protocole sûr, garantissant l'intégrité des données avec une absence totale d'échos, de fantômes et de signaux dupliqués sur la ligne ".*



La sécurité avec Safetybus p

Aujourd'hui le Safetybus p est le bus de sécurité le plus répandu, avec plus de 5000 réseaux installés à travers le monde, dans des milieux aussi divers que ceux de l'agroalimentaire, du process continu, de l'industrie automobile…

Le Safetybus p est un système multi-maîtres avec topologie de bus linéaire, destiné à la mise en réseau d'applications de sécurité déportées. Il nécessite l'utilisation d'un ou plusieurs automates de sécurité. Ceux-ci sont redondants, voire tri-redondants, c'est-à-dire qu'ils possèdent jusqu'à trois processeurs exécutant les mêmes instructions et comparant leurs résultats dans le but d'assurer une parfaite intégrité des données. C'est ce qui permet à Safetybus p de garantir une sécurité de niveau

4, conformément à la norme EN 954-1. Rappelons pour mémoire que cette dernière est basée sur l'évaluation de la capacité des fonctions de sécurité à supporter et à détecter les défauts.

Tout comme CAN, Safetybus p est un système évènementiel, qui permet une coupure quasi instantanée. Avec des temps de cycles automates de l'ordre de 15 ms et un temps de propagation sur le bus inférieur à 3 ms, Safetybus p permet de garantir des délais de coupure inférieurs à 50 ms. Cela constitue, pour Safetybus p, un avantage concurrentiel sur les protocoles de sécurité imbriqués tels que Profisafe, As-i Safety, qui mélangent sur le même support les données de contrôle commande et de sécurité. Mais nous y reviendrons plus longuement dans la suite…

Que l'on ne s'y trompe pas : si Safetybus p nécessite impérativement l'utilisation d'automates de sécurité, ce n'est pas un bus propriétaire et il se veut un protocole ouvert, comme en témoigne Olivier Arbogast : *" Safetybus p permet la connexion de toutes sortes d'équipements de sécurité, et un nombre croissant de constructeurs intègrent nativement une interface Safetybus p dans leurs appareils. On y retrouve les éléments de sécurité traditionnels tels que des barrières immatérielles, des boutons d'arrêt d'urgence, mais également des systèmes plus sophistiqués tels que des robots, des dispositifs de contrôle d'axes de sécurité ou encore des systèmes pneumatiques ainsi que divers appareils sans fil ".*

Les niveaux de sécurité SIL :

Niveau SIL (Safety Integrity Level)	Mode Opératoire *Probabilité Moyenne de Défaillance sur Sollicitation*	
	Sollicitation Faible	Sollicitation Elevée ou Continue
SIL4	$10^{-5} < p < 10^{-4}$	$10^{-9} < p < 10^{-8}$
SIL3	$10^{-4} < p < 10^{-3}$	$10^{-8} < p < 10^{-7}$
SIL2	$10^{-3} < p < 10^{-2}$	$10^{-7} < p < 10^{-6}$
SIL1	$10^{-2} < p < 10^{-1}$	$10^{-6} < p < 10^{-5}$

Valenti Giocchino, responsable de la sécurité des machines chez Montupet, parlant de l'application du Safetybus p sur une ligne de fonderie de culasse en aluminium : *" Le choix de l'installation d'un bus de sécurité a été arrêté pour des raisons de facilité d'intégration, de flexibilité et de pérennité. L'installation d'un bus de sécurité permet de réaliser d'importantes économies de câbles, et même si les équipements nécessitent un investissement de départ plus important que ceux d'une solution de sécurité classique, ces surcoûts sont très vite absorbés par les gains lors de la mise en œuvre et de l'exploitation du système. Qu'il s'agisse d'ingénierie ou d'opérations de maintenance, les temps d'intervention sont réduits, et les opérations sont facilitées grâce aux fonctionnalités de diagnostic intégrées et à la convivialité des IHM. Par ailleurs, les chantiers de moulage ayant une durée de vie limitée, l'utilisation d'automates de sécurité reliés par bus présente l'avantage de la ré-utilisabilité lors d'un changement de ligne ".*

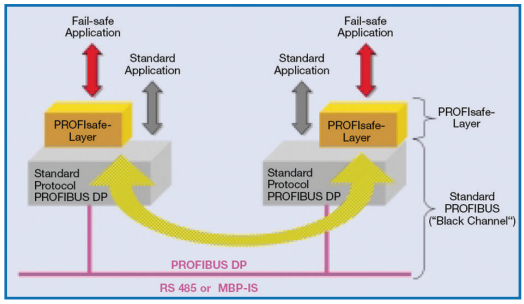
Mais si tout le monde est d'accord en ce qui concerne les avantages de l'utilisation d'un bus dédié à la sécurité, il n'en demeure pas moins que les industriels souhaiteraient, dans l'idéal, voir transiter sur un seul et même câble à la fois les données de contrôle-commande et les données de sécurité. C'est la raison pour laquelle les organisations telles que Profibus International, As-Interface, InterbusClub ou encore l'ODVA, tentent depuis plusieurs années déjà d'adapter les protocoles existants aux exigences des applications de sécurité. Cela a donné lieu à la naissance de nombreuses solutions, baptisées Profisafe, As-Interface Safety et Work, et plus récemment Interbus Safety, CIP Safety … Les premières annonces datent de 2001, qu'en est-il aujourd'hui ? C'est ce que nous avons tenté de savoir.

Profibus, l'offre la plus complète

Profisafe est sans doute la plus connue de ces solutions, et également la plus complète. Il y aurait aujourd'hui de par le globe plus de 3000 applications intégrant Profisafe pour la gestion de la sécurité, et cela concernerait autant l'industrie manufacturière que l'industrie de process.
Développé en 2001, Profisafe vient compléter la panoplie Profibus, sous

La Norme EN 954-1 :

Catégorie	Résumé des exigeances	Comportement du Système	Principe
B	Les commandes doivent être conçues de manière à supporter les contraintes attendues	Un défaut peut mener à la perte d'une fonction de sécurité	Principalement caractérisé par la sélection des composants
1	Les exigences de B doivent être remplies ; le matériel de sécurité utilisé doit avoir été testé et validé	Idem que pour B, mais avec une fiabilité plus grande des fonctions de sécurité	
2	Les exigences de 1 doivent être remplies ; des tests supplémentaires à intervalles réguliers doivent être réalisés	Le défaut est reconnu à l'étape de vérification suivante	Principalement caractérisé par la structure des commandes
3	Les exigences de 1 doivent être remplies ; un défaut isolé ne doit pas mener à la perte de la fonction de sécurité	Lorsqu'un défaut isolé se produit, la fonction de sécurité reste intacte	
4	Les exigences de 3 doivent être remplies ; les défauts isolés doivent être reconnus au préalable ou à la sollicitation suivante de la fonction de sécurité	Lorsque des défauts se produisent la fonction de sécurité reste intacte. Les défauts sont reconnus	



Le concept Profisafe intégré à Profibus

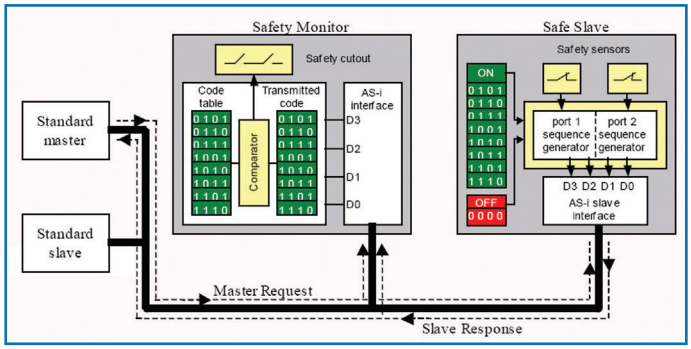
la forme d'un logiciel intégré aux équipements de sécurité. Il s'agit en fait d'un profil, au sens " profibussien " du terme, au même titre que Profibus DP, PA ou encore Profidrive, venant se greffer au niveau de la couche Application (niveau 7) de l'architecture existante. Le profil définit le raccordement via Profibus des éléments de sécurité (barrières immatérielles, boutons d'arrêt d'urgence, etc…) à des automatismes répondant aux normes de sécurité les plus sévères.

Les normes de référence en la matière sont les catégories définies dans EN 954-1, et les niveaux SIL (Safety Integrity Level) décrits dans CEI 61508. Rappelons au passage que ces derniers sont basés sur les probabilités de défaillance des fonctions de sécurité. Selon l'association Profibus International, Profisafe permet de garantir un niveau 3 de sécurité sur l'échelle SIL, et un fonctionnement de catégorie 4 suivant EN 954-1.

Profisafe étant défini en tant que profil à l'intérieur de la couche application, les mécanismes régissant les échanges sur le bus sont exactement les mêmes que pour les applications de contrôle commande classiques. Un contrôleur envoie des données sur le bus à destination d'un équipement de terrain, lequel y répond. L'évolution réside dans l'imbrication à l'intérieur des télégrammes, d'informations concernant la sécurité et l'intégrité des données transmises. Ces informations sont récupérées et interprétées en accord avec l'implémentation du profil Profisafe, au niveau de chaque station réceptrice.

La simplicité avec As-Interface Safety at Work

Profibus International n'est pas le seul fournisseur de bus de terrain à s'être lancé sur le marché de la sécurité. Dans le même esprit, As-Interface a développé un système baptisé As-i Safety at Work qui, à la différence de son homologue Profisafe, ne nécessite pas l'utilisation d'un automate de sécurité. Le seul élément à ajouter est un superviseur, chargé de surveiller les messages en provenance ou à destination des différents organes de sécurité. Ceci permet de décharger totalement les équipements de sécurité des tâches de surveillance et de redondance.



Les échanges de données avec As-i Safety at Work

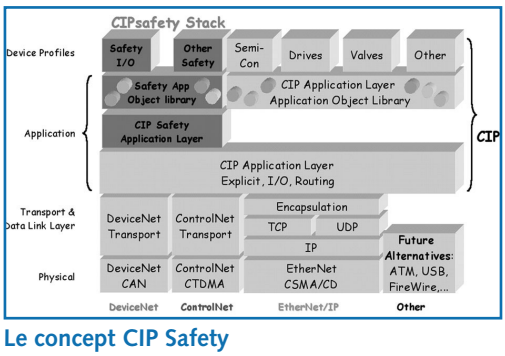
Les messages issus de ces équipements sont transmis sous forme de télégrammes As-i standard, et contiennent une portion de code spéciale, non exploitée par l'automate maître, mais passée au crible par le superviseur afin de détecter les défauts. En complément des profils As-i standard, les équipements de sécurité intègrent un profil spécifique, explicitant les fonctions de base telles que la commande bi-manuelle, le blocage du démarrage … Si la portion de télégramme relative à la sécurité vient à être différente de celle attendue par le superviseur, celui-ci déclenche la procédure de sécurité de l'élément concerné. Au niveau des performances, tout comme Profisafe, As-i Safety at Work permet d'atteindre le niveau de sécurité SIL 3 ou la catégorie 4 de l'EN 954-1, avec des temps de coupure garantis inférieurs à 35 ms.

Des solutions en cours de développement

D'autres solutions, aux caractéristiques proches de celles que nous venons de décrire, sont en cours de développement. C'est le cas notamment d'Interbus Safety, ainsi que du concept CIP Safety qui concerne l'ensemble des technologies développées par l'ODVA, c'est-à-dire en particulier les réseaux DeviceNet et EthernetIP.

Mais pour l'ensemble de ces solutions, il est trop tôt pour envisager des retours d'expérience. En effet, les premières applications viennent seulement de voir le jour dans le cas d'Interbus Safety et DeviceNet Safety, et il faudra sans doute attendre encore plusieurs années avant d'obtenir des témoignages d'utilisateurs.

Pour les utilisateurs de Profisafe et d'As-i Safety at Work, près de trois ans après la mise en œuvre des premières applications, nous avons eu beaucoup de mal à obtenir des témoignages d'utilisateur français. Souci de confidentialité, reflet d'un degré de maturité encore faible des technologies, blocage psychologique des services sécurité ? Cela est révélateur de la confusion qui semble planer aujourd'hui encore autour de ces questions de sécurité. Mais n'oublions pas que les plus grandes révolutions sont aussi, souvent, celles qui sont les plus longues à mettre en œuvre. Et si l'ensemble des principaux constructeurs de bus de terrain a pris le pari de se lancer dans l'aventure, on ne peut que se résoudre à penser que celle-ci portera, tôt ou tard, ses fruits. ■



Le concept CIP Safety