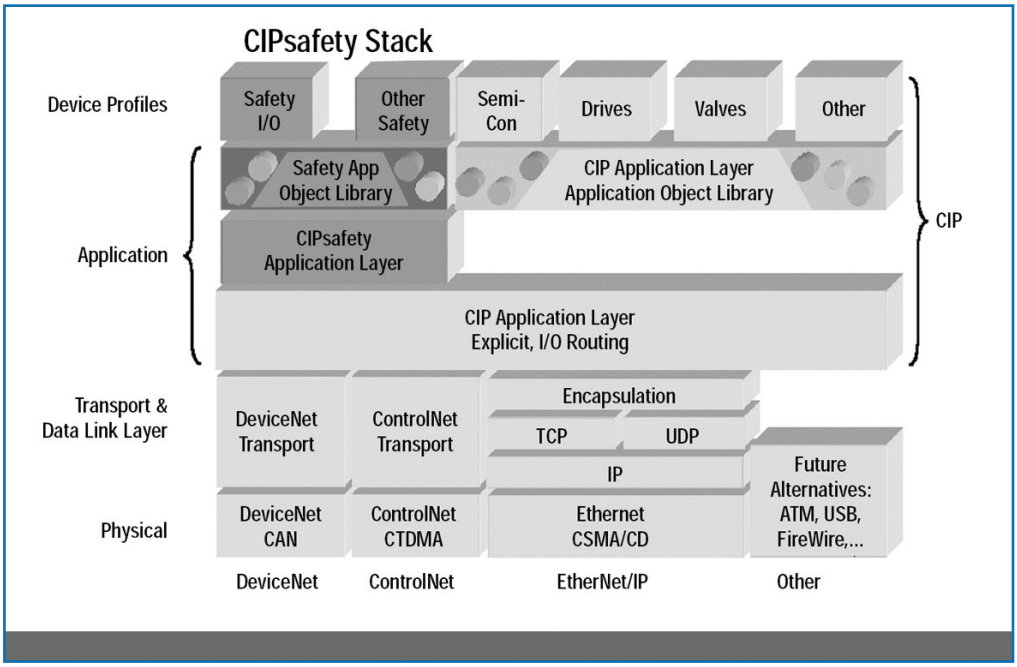
CIP Safety, c'est parti

CIP Safety est le fruit des derniers développements de l'ODVA en matière de sécurité. Publiés en janvier 2005, les spécifications de CIP Safety décrivent les extensions fonctionnelles apportées au protocole CIP pour les applications de sécurité. CIP Safety est destiné à des applications de sécurité de niveau SIL 3, suivant le standard IEC 61508. Il a été, à ce titre, approuvé par le TUV Rheinland.



Extensions de sécurité de l'architecture CIP

La sécurité : une préoccupation majeure

La sécurité est devenue l'une des préoccupations majeures de l'industrie manufacturière. Soumis à des pressions sociales et législatives sans cesse grandissantes, les industriels ont le devoir d'assurer la protection des ouvriers dans l'exercice de leur métier, voire de garantir la sécurité de populations entières dans le cas d'installations dites « à hauts risques ».

Dans le même temps, ils doivent faire face à des pressions économiques appelant à toujours plus de productivité. Il y a une dizaine d'années seulement, les technologies employées pour le contrôle commande et pour la sécurité ne semblaient pas permettre la conciliation de ces deux impératifs. La réponse à l'un semblait invariablement se faire au détriment de l'autre.

Par exemple, avec les systèmes traditionnels de sécurité câblés, la réaction typique à une alerte était la mise hors tension de l'ensemble des sorties API, avec pour conséquence l'immobilisation momentanée de l'unité de production tout entière. Quelle qu'ait été la nature du problème, la réponse du système était la même. Cela permettait d'éviter les catastrophes, mais à un prix relativement élevé.

Aujourd'hui la donne a changé. Les progrès effectués dans le domaine de l'automatisation permettent d'envisager la mise en œuvre de systèmes de sécurité intelligents, basés sur des technologies de réseau, que l'on retrouve dans les applications de contrôle standard.

Les bénéfices de l'installation de tels systèmes peuvent être importants, car en plus des économies de câblage et de la simplicité d'installation, les utilisateurs peuvent capitaliser leurs connaissances des process pour renforcer les capacités de diagnostic.

En cas d'alerte, le contrôleur de sécurité pourra décider quels sont les équipements qui doivent être déconnectés et quels sont ceux qui peuvent continuer à fonctionner. Si par exemple un capteur de sécurité détecte le mauvais alignement d'un bras de robot, la mise hors tension pourra être limitée à la seule cellule concernée. Le fait de ne pas avoir à interrompre l'ensemble de l'application se traduira par une perte amoindrie de la productivité.

CIP Safety

CIP Safety est une extension de la couche applicative CIP (Control and Information Protocol), sur laquelle reposent les solutions de communication DeviceNet, ControlNet et

EtherNet/IP. Les extensions CIP Safety ne concernent que les équipements de sécurité, qui peuvent être intégrés de façon totalement transparente aux réseaux de contrôle CIP traditionnels.

Les premiers équipements CIP Safety (blocks d'entrées/sorties, commutateurs, barrières immatérielles et automates de sécurité) seront disponibles mi-2005, pour les réseaux DeviceNet uniquement.

En raison de l'interopérabilité des réseaux CIP, il sera possible de transmettre des messages de sécurité aussi bien que des ensembles de données complexes à un ou plusieurs récepteurs situés à des niveaux différents de l'architecture d'un même réseau CIP. Par exemple, un réseau EtherNet/IP pourra être utilisé en tant que backbone pour un système constitué de plusieurs sous-réseaux DeviceNet Safety.

Dans l'avenir, CIP Safety équipera des éléments EtherNet/IP similaires, sous l'appellation Ethernet/IP Safety. EtherNet/IP Safety présentera deux avantages. Tout d'abord, il permettra de bénéficier des avantages d'Ethernet Industriel pour l'automatisation. Ensuite, il fournira un moyen d'intégrer les réseaux de sécurité dans les mêmes architectures que celles utilisées par les équipements de contrôle standard, Internet et le reste de l'entreprise.

Les capacités de routage de CIP permettront la création de cellules DeviceNet Safety avec des temps de réaction très faibles, interconnectées par le biais d'un backbone EtherNet/IP Safety. Seules les informations de sécurité nécessaires seront transmises aux cellules correspondantes.

Principes de base

CIP Safety n'empêche pas les erreurs de communication de se produire, mais il assure l'intégrité des données transmises en détectant les erreurs et en permettant aux équipements de mener les actions correctives.

La couche application CIP Safety est spécifiée en utilisant un objet baptisé « Safety Validator ». Celui-ci est responsable de la gestion des connexions CIP Safety et sert d'interface entre les objets d'applications Safety et les connexions vers les couches liaison de données. La sécurité des transferts et la vérification des données de sécurité incombe également aux « Safety Validators ».

Tous les transferts de sécurité CIP Safety utilisent le contrôle de redondance cyclique Safety CRC pour garantir l'intégrité des données. Le Safety CRC sert de première mesure permettant de détecter les éventuelles corruptions. Les Safety CRC sont générés par les producteurs Safety et vérifiés par les consommateurs. Les équipements intermédiaires servant au routage des données de sécurité n'examinent pas le Safety CRC. Ceci permet d'assurer que les CRC individuels effectués localement sur la couche liaison de données ne font pas partie de la fonction de sécurité afin de garantir l'indépendance de celle-ci vis-à-vis du media. Le Safety CRC fournit également un mécanisme de protection permettant de détecter les erreurs pouvant survenir au niveau liaison de données, telles que les erreurs de « bit-stuffing » ou de fragmentation.

La redondance et le contrôle croisé des données et des CRC constitue une mesure supplémentaire de sécurité pour la détection des corruptions. Ceci autorise le transfert sécurisé de paquets de données de sécurité pouvant aller jusqu'à 250 octets. Pour les paquets plus courts, de 2 octets ou moins, la redondance des données n'est pas nécessaire. Dans tous les cas, les CRC redondants sont néanmoins comparés.

Toutes les données CIP Safety sont horodatées par le producteur, ce qui permet aux consommateurs de déterminer l'âge des données reçues. Cette mesure de détection constitue une avancée par rapport aux timers de reception habituels, qui permettent généralement de savoir combien de temps s'est écoulé depuis la dernière réception, mais n'apportent aucune information concernant la date de production des messages. Un horodatage permet la transmission, l'arbitrage d'accès au média, une meilleure gestion des files d'attente, ainsi que la détection des délais de retransmission et de routage.

Etant donné que les extensions Safety ne reposent pas sur l'intégrité des couches CIP standard et liaisons de données, la redondance hardware des interfaces de communication de niveau liaison de données n'est pas nécessaire. Pour la même raison, un routeur standard peut être utilisé pour router les données de sécurité. Si une erreur se produit lors de la transmission, l'équipement final détectera cette erreur et prendra les mesures appropriées. ■

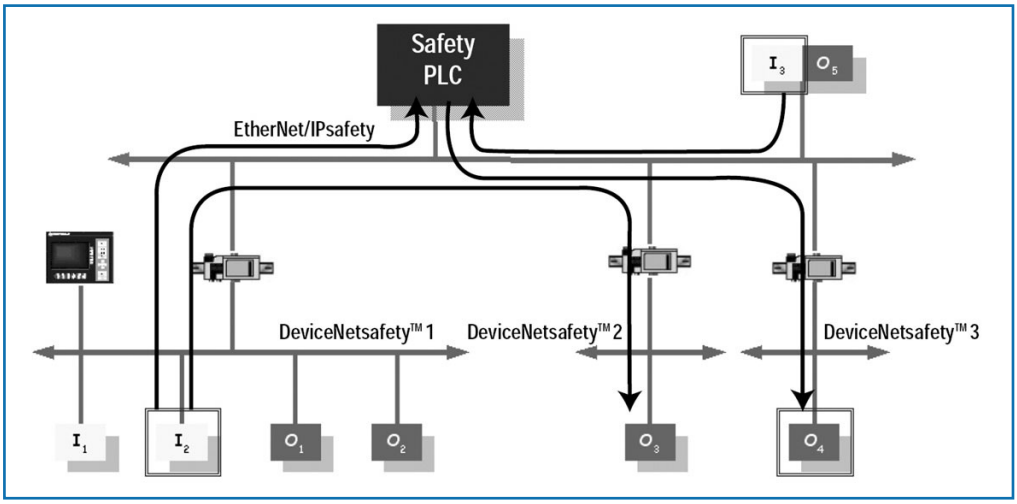


Illustration des capacités de routage de CIP Safety