OpenSafety pour tous les réseaux, ou presque

Avec OpenSafety, l'EPSG énerve quelque peu le monde du contrôle/commande. Le système dédié à la sécurité est apte à être installé sur les réseaux concurrents.

A peine annoncé, OpenSafety dérange le monde des automaticiens. Normal, à l'origine on retrouve l'un des protagonistes des bus Ethernet, à savoir Powerlink.

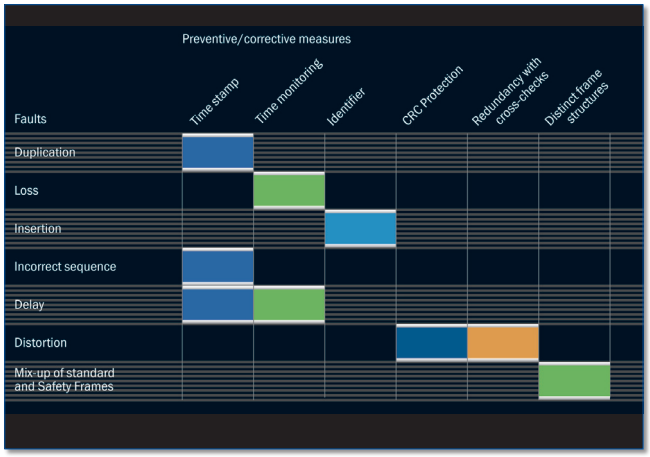
Inutile d'expliquer qu'entre les réseaux Ethernet, que ce soit Profinet, EthernetIP, Powerlink, Sercos, Ethercat et quelques autres, c'est une bataille sans merci, une guerre qui a remplacé, au fil des ans, celle des bus de terrain. Exit Worldfip et autres réseaux des années 80, aujourd'hui c'est Ethernet, si possible temps réel, qui domine. Et le gâteau est suffisamment stratégique pour que tous s'y ruent.

Dans cette bagarre, tout le monde se dit ouvert. Plus aucun réseau n'est propriétaire, les entreprises d'automatismes ont fait don de leur savoir auprès d'organisations indépendantes.

HOMOGÉNÉISER LA FONCTION SAFETY

Voilà pour le décor. En parallèle à ces nouveaux standards du marché, il a fallu les faire évoluer avec notamment la notion de sécurité.

Il paraît très loin le temps où les spécialistes claironnaient dans les salles de conférences que jamais une information de sécurité ne circulerait sur le même réseau que celui de contrôle/commande. Aujourd'hui, cela deviendrait même la règle. Chaque fournisseur, et chaque organisation, dans le monde de l'Ethernet, propose une réponse Safety.



Le tableau indique toutes les erreurs de transmissions connues ainsi que les mécanismes de détection d'erreurs d'OpenSafety.

Seulement, il reste toujours impossible de faire communiquer ensemble des installations utilisant plusieurs réseaux différents au sein d'une même entreprise, si ce n'est avec l'utilisation de passerelles, avec les inconvénients que cela induit. Pour la sécurité, c'est le même cas de figure.

Avec OpenSafety, l'EPSG (association qui regroupe les intérêts de Powerlink) vient bouleverser cette situation. Le groupement propose OpenSafety, avec un « Open » pouvant fonctionner sur la plupart des réseaux concurrents. L'organisation poussant le bouchon assez loin, en espérant que ses compétiteurs vont l'adopter.

Le buzz est suffisant pour que l'on s'intéresse quelque peu à cet outil qui devrait intéresser quelques intégrateurs et OEM qui doivent se dépatouiller avec des réseaux différents et se retrouvent avec un véritable casse-tête pour intégrer la sécurité. Pour le contrôle/commande, ils savent comment faire, mais pour la sécurité ? Le travail est immense.

Avec OpenSafety, ils n'auront théoriquement qu'à introduire l'outil dans chacun des réseaux et faire une sécurité unique de l'ensemble de leurs installations.

Mais, en dehors des aspects politiques, techniquement ça marche comment OpenSafety ?

COMMENT ÇA MARCHE ?

OpenSafety se distingue essentiellement par ses méthodes de transfert de données, par ses services de configuration et par le fait qu'il encapsule les données liées à la sécurité dans un format de télégramme flexible.

Dans toutes les applications, il utilise une trame dont le format est uniforme, que cette trame soit utilisée pour transférer des données utiles ou à des fins de configuration ou de synchronisation temporelle. La longueur de cette trame varie selon la quantité de données à transférer. Les nœuds dédiés à la sécurité sur le réseau reconnaissent automatiquement le contenu de la trame de sécurité. Nul besoin, donc, de configurer des types ou des longueurs de trame.

Une de ses caractéristiques c'est la distribution automatique des paramètres liés à la sécurité à travers le réseau. Le protocole permet de stocker dans l'automate de sécurité tous les paramétrages relatifs aux applications de sécurité (configuration de barrières im-

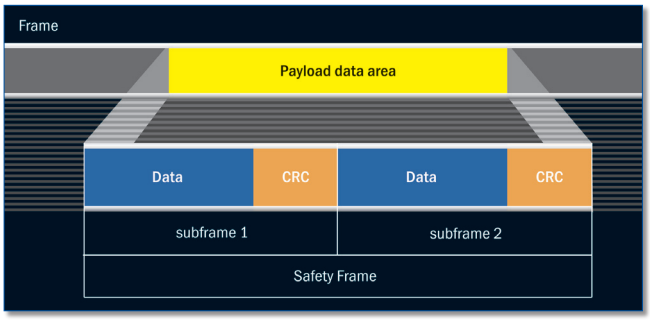
matérielles, par exemple). Si un composant matériel est remplacé, l'automate de sécurité charge automatiquement, sur l'application modifiée, la configuration stockée en mémoire. Ainsi, les utilisateurs n'ont pas besoin de configurer manuellement le nouveau nœud issu du remplacement du composant de sécurité.

En appliquant des procédures de checksum, il contrôle en permanence si le contenu des données transmises est complet. Ce protocole surveille aussi constamment le temps de transmission des données. Ses temps de cycle extrêmement courts permettent de détecter les défauts quasiment sans délai. Les anomalies dans le trafic de données sont identifiées et même les réseaux « non sûrs » ne compromettent pas les fonctionnalités de sécurité.

STRUCTURE D'UNE TRAME ET RÉSEAU

OpenSafety dédouble la trame à transmettre et joint les deux trames identiques au sein d'une seule trame. La trame se compose donc de deux sous-trames au contenu identique. Chaque sous-trame est fournie avec son propre checksum. Le destinataire compare le contenu identique des deux sous-trames.

La probabilité que les mêmes données soient modifiées ou détruites dans les deux sous-trames est extrêmement faible, et l'est encore plus lorsque la longueur de la trame augmente. Ceci étant dit, même si cela se produit, les checksums remplissent alors leur fonction corrective. Le format spécial des trames, c'est-à-dire deux sous-trames avec leur propre checksum, rend les « masquages » (masquerades en anglais) improbables et exclut tout traitement erroné d'un message standard masqué.



Un réseau OpenSafety peut contenir jusqu'à 1023 domaines de sécurité. Jusqu'à 1023 nœuds ou composants sont permis dans chacun de ces domaines. Les domaines de sécurité peuvent s'étendre sur plusieurs réseaux hétérogènes. Les nœuds de sécurité éparpillés sur ces réseaux peuvent donc être intégrés à un seul domaine. Les composants fonctionnant dans un même domaine peuvent être dédiés à la sécurité ou non (« sûrs » ou « non sûrs »).

La communication entre les différents domaines de sécurité est assurée par des passerelles. OpenSafety permet aux utilisateurs d'établir des séparations hiérarchiques ainsi que des zones de sécurité sur un réseau. Ainsi, par exemple, il est possible de monter des installations dans une zone alors que la production, dans d'autres zones, se déroule sans entrave. Dans chaque domaine, un Safety Configuration Manager (SCM) a la responsabilité de surveiller en permanence tous les nœuds de sécurité. ■

TYPES D'ERREUR DE TRANSMISSION ET MÉCANISMES UTILISÉS

Causes des erreurs de transmission

Une part importante des erreurs de transmission de données est due à des transferts incorrects de données par les passerelles. Par exemple, il se peut que des données soient dupliquées si un réseau est relié à d'autres réseaux via deux passerelles et si ces deux passerelles transmettent le même groupe de données. Par ailleurs, des paquets de données peuvent être perdus si une passerelle ne transmet aucune donnée ou n'aiguille pas les données vers le bon réseau.

Si des paquets de données, en raison de leur longueur, ne peuvent être transmis que sous la forme d'une séquence de paquets partiels, il se peut que des chemins de transmission différents, via des passerelles différentes, conduisent à des interversions ou à des insertions erronées de segments de paquets. L'acheminement de certaines données peut être aussi retardé en raison d'un grand afflux de données sur une passerelle.

Les perturbations électromagnétiques sont aussi une cause potentielle d'altération des données ; les distorsions vont alors du « basculement » de certains bits à la destruction de sections entières d'informations. Enfin, dans les réseaux véhiculant à la fois des données standard et des données dédiées à la sécurité, les données standard peuvent être considérées comme étant des données de sécurité suite à des interversions ou à des insertions erronées, ce qui peut entraîner de graves dysfonctionnements.

Identification et prévention des erreurs

Le mécanisme d'horodatage d'OpenSafety permet une transmission exempte de duplications, interversions et retards. Chaque paquet de données est « estampillé » avec l'heure courante lorsqu'il est émis. Cette estampille permet au destinataire d'éviter les doubles lectures et de connaître l'ordre chronologique des différents paquets ainsi que les retards.

OpenSafety ne dépend pas d'horloges distribuées ; un procédé spécial permet une synchronisation des horloges des microcontrôleurs dans les nœuds du réseau. Une surveillance temporelle est effectuée pour éviter les erreurs dues à des pertes de données ou à des retards excessifs.

En outre, les consommateurs du réseau, s'ils sont invités à le faire, détectent si la liaison reste établie ; OpenSafety implémente ce mécanisme appelé « chien de garde » sous forme de fonction logicielle.

L'identificateur exclut toute interversion ou confusion du côté du destinataire : les trames incluent un label d'identification unique de 8 ou 16 bits codant des parties du champ adresse, le type de télégramme contenu dans la trame, et le type de trame.

La méthode la plus fiable pour identifier d'éventuels changements dans le contenu d'origine est le CRC : avec ce procédé, à l'aide d'une clé, un checksum est généré pour chaque groupe de données puis, avec la clé, joint au groupe de données sous la forme d'une séquence de bits. Ce checksum constitue un codage univoque du groupe de données. En utilisant la séquence de bits et la clé, le destinataire détermine par calcul le groupe de données d'origine et vérifie le résultat en le comparant au groupe de données non codé. Si une quelconque déviation par rapport aux données d'origine est détectée, le message sera ignoré.