RÉSEAUX DE TERRAIN DÉDIÉS À LA SÉCURITÉ - LA QUESTION DES TEMPS DE RÉPONSE

☐ Sécurité des systèmes
☐ Automate programmable
☐ Machine
☐ Système homme-machine
☐ Commande

► *Jean-Pierre BUCHWEILLER, Patrick BERTRAND,*
INRS, département Ingénierie des équipements de travail

L'usage des réseaux de terrain dédiés à la sécurité (RdTdS), comme celui des automates programmables dédiés à la sécurité (APIdS), est aujourd'hui admis par les différents intervenants dans le domaine de la sécurité des machines. Leur performance de sécurité intrinsèque, lorsqu'elle a été validée par des organismes compétents, n'est pas remise en cause. Cependant, la mise en œuvre de ces réseaux est loin d'être évidente et des difficultés importantes sont rencontrées par les utilisateurs, concernant en particulier la maîtrise des temps de réponse des fonctions de sécurité auxquelles participent ces dispositifs. L'objet de cet article n'est pas de livrer un exposé théorique sur la transmission des informations ou sur l'intérêt de tel ou tel protocole, ni de jongler avec les couches du modèle de communication... mais d'énoncer les difficultés posées par la mise en oeuvre de ces dispositifs et la maîtrise des temps de réponses.
Sans remettre en cause les caractéristiques techniques ou les performances de sécurité annoncées par les constructeurs des RdTdS, ni, bien entendu, leur possible utilisation pour la transmission d'informations relatives à la sécurité dans les machines, nous montrons en quoi cette problématique de maîtrise des temps de réponse, qui assurément n'est pas apparue avec ces dispositifs, a été amplifiée par le recours à un tel choix technologique.

Les réseaux ou bus de terrain sont des dispositifs assurant la transmission d'informations entre des capteurs, des actionneurs et des systèmes de contrôle/commande par l'intermédiaire d'un support unique (câble, fibre optique, etc.). Ils sont apparus au début des années 80 au sein des systèmes automatisés de production. Le besoin de communication d'informations relatives à la sécurité, renforcé en particulier par la banalisation des APIdS, se faisant de plus en plus pressant, la question de l'application des réseaux de terrain à la sécurité des machines s'est posée. Les réseaux standards n'ayant pas été spécifiés et conçus pour la transmission d'informations relatives à la sécurité des personnes, ils ne pouvaient pas convenir en l'état. Pour répondre à cette demande, des consortiums se sont constitués dans le but de définir les spécifications techniques d'un certain nombre de réseaux dédiés à la sécurité, dérivés de différents réseaux standards existants.

L'apparition de la logique séquentielle, puis programmable, dans les automatismes a grandement complexifié l'estimation des temps de réponse des systèmes, qui nécessite maintenant d'avoir une vue précise sur la structure des programmes, leur nombre d'instructions, etc. L'utilisation des réseaux de terrain a encore accru cette difficulté en ajoutant les délais qui leur sont propres pour la scrutation des entrées, la prise en compte des transmissions, etc.

Ces mêmes complications touchent le domaine de la sécurité des personnes travaillant sur les machines avec, en plus, la nécessité pour les composants utilisés de présenter des garanties sur leur aptitude intrinsèque à assurer une fonction de sécurité, sur leur comportement en présence de défaillances, etc.

SAFETY-DEDICATED FIELD BUSSES - THE RESPONSE TIME ISSUE

Use of safety-dedicated field busses, e.g. safety-dedicated PLCs, is currently accepted by the various operators involved in machinery safety. When confirmed by competent bodies, their intrinsic safety performance remains unchallenged. However, implementation of these networks is far from obvious and major difficulties are encountered by users, especially in relation to controlling the response time of safety functions, in which these systems take part. The aim of this paper is neither to deliver a theoretical description of data transfer or of the advantage of a specific procedure, nor to juggle with communication model levels, etc., but to set out the problems raised by implementation of these systems and control of safety function response time.
We call into question neither the technical or performance characteristics quoted by safety-dedicated field bus manufacturers nor, of course, their possible use for transmitting machine safety-related data. But, we do show how this problem of response time control, which has certainly not arisen with the arrival of such systems, has been aggravated by resorting to this type of technological choice.

☐ System safety
☐ Programmable logic controller (PLC)
☐ Machine
☐ Man-machine system
☐ Control

Malgré les garanties offertes par les composants, il subsiste des paramètres pouvant avoir une incidence forte sur la sécurité des personnes, qui dépendent de la mise en œuvre de ces composants parfois d'usage complexe et souvent difficiles à appréhender.

C'est précisément le cas pour les RdTdS. À ce jour, de plus en plus de dispositifs de ce type sont disponibles sur le marché (AS-i Safety at Work, PROFIsafe, SafetyBUS p, CAN Open Safe, Device net Safety, Interbus Safe Guard, etc.). D'autres évoluent et d'autres encore sont en cours d'étude. C'est un domaine où, comme très souvent pour les dispositifs mettant en œuvre des logiciels, les évolutions succèdent aux évolutions.

Comme il n'est pas question de présenter ici l'ensemble de l'offre des RdTdS, nous l'avons simplement esquissée en annexe de cet article en nous limitant aux trois premiers cités, qui sont représentatifs de l'ensemble de l'offre disponible en sécurité des machines et couvrent l'étendue du domaine d'utilisation des réseaux : du capteur à la cellule de production, voire à l'atelier.

Nous présenterons d'abord la problématique générale liée aux RdTdS et situerons brièvement ces dispositifs par rapport à la réglementation – directive Machines [1] – concernant les *composants de sécurité*.

Nous montrerons ensuite que, si les RdTdS répondent incontestablement aux performances de sécurité annoncées par leur concepteurs, il existe cependant, pour les constructeurs et utilisateurs de machines, une difficulté certaine à **assurer et garantir le temps de réponse des fonctions de sécurité** traitées par de tels dispositifs, alors que ce paramètre est un des éléments essentiels de la spécification de ces fonctions.

Nous conclurons enfin en précisant les précautions minimales à prendre par les constructeurs et utilisateurs de machines pour mettre en œuvre de tels dispositifs dans le traitement de leurs fonctions de sécurité. Notre approche, au final, portera moins sur le détail des caractéristiques intrinsèques de ces dispositifs que sur les précautions générales à prendre pour leur mise en œuvre, la réussite du développement se situant, à notre sens, très souvent à ce niveau.

LES RÉSEAUX DÉDIÉS À LA SÉCURITÉ

Le concept général

Le concept général sur lequel reposent les réseaux de terrain dédiés à la sécurité peut être schématisé par la *Figure 1*.

La communication relative à la sécurité se déroule comme suit :

- lors de son émission, le message relatif à la sécurité est conditionné par la couche de sécurité avant d'être transmis sur le médium selon le protocole du réseau standard,
- à la réception, le message est prélevé sur le médium du réseau standard puis reconnu, validé, etc. par la couche de sécurité du réseau avant d'être transmis à l'application relative à la sécurité.

Pour tous les RdTdS, la couche de sécurité impliquée est constituée d'un protocole de communication (logiciel) développé spécifiquement pour assumer la performance de sécurité visée par le réseau (SIL, Catégorie). Ce protocole est mis en œuvre et contrôlé par des composants matériels spécifiques au réseau dédié à la sécurité en question (redondance, chien de garde, dynamisme, etc.).

La couche de sécurité s'appuie elle-même sur le protocole et le matériel du réseau de terrain standard, non dédié à la sécurité qui lui sert de base.

L'incidence potentielle de leur défaillance sur la sécurité des personnes

Le maintien de la fonction de sécurité d'une machine ou d'une installation intégrant plusieurs éléments dépend du bon fonctionnement de chacun des éléments intervenant dans cette fonction. À ce titre, s'il participe à une fonction de sécurité de l'installation, le réseau de terrain sera impliqué.

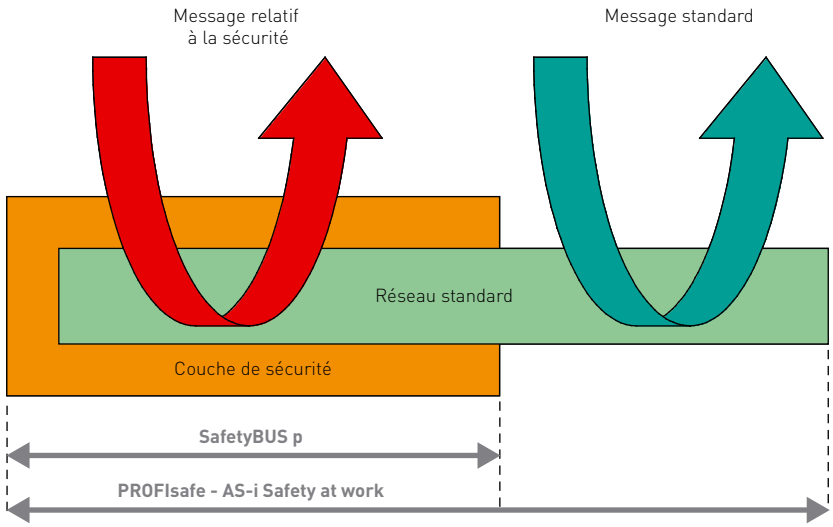
MODES DE DÉFAILLANCE DES RÉSEAUX DE TERRAIN

Les référentiels normatifs précisent les différents modes de défaillance dont les concepteurs RdTdS devront s'affranchir :
- corruption des données transmises,
- répétition inattendue de messages,
- ordre des messages incorrect,
- perte d'informations,
- retard inacceptable dans la transmission des messages,
- insertion d'un message inattendu,
- amalgame de messages standards et de messages de sécurité,
- fautes d'adressage.

Le problème général posé par les réseaux de terrain dans les applications relatives à la sécurité est celui des situations dangereuses qui pourraient être

FIGURE 1

Concept général des Réseaux de terrain dédiés à la sécurité
General concept of safety-dedicated field busses



générées sur l'installation suite à un dysfonctionnement du réseau.

Les référentiels normatifs[1] précisent les différents modes de défaillance envisageables pour les réseaux. Nous pouvons les résumer à deux causes globales :

- une altération du traitement des informations,
- un retard dans le traitement des informations.

Les différents travaux conduits à l'INRS sur des RdTdS ont montré que rien ne permettait de remettre en cause les concepts mis en œuvre dans les RdTdS. Nous avons en effet pu constater que les concepteurs de tels dispositifs avaient eu recours à des mécanismes et des architectures leur permettant de s'affranchir des différents modes de défaillance des réseaux dont les performances avaient été validées par des organismes de contrôle compétents.

Nécessité d'un concept et de composants valides

Les spécifications édictées par les différents consortiums ayant en charge chacun de ces réseaux dédiés à la sécurité définissent le protocole, les mécanismes de contrôle, la structure matérielle, etc. qui devront être appliqués par les constructeurs de composants désirant proposer des produits compatibles avec ces profils de communication. Parmi ces composants, on peut citer :

- des automates programmables dédiés à la sécurité (ou leurs cartes spécifiques réseau),
- des contrôleurs indépendants spécifiques,
- des esclaves d'entrée,
- des esclaves de sortie,
- des alimentations dédiées.

Un réseau de terrain ne pourra prétendre être de sécurité (donc RDTdS) que si :

- le concept général (protocole, architecture matérielle, etc.) a été validé dans un premier temps par un organisme compétent,
- chacun des composants pour lequel son constructeur revendique une compatibilité avec le profil de communication de sécurité en question a été ensuite validé par un organisme compétent. En général, ces composants sont propres à chacun des constructeurs impliqués dans un réseau donné.

Les utilisateurs potentiels de ces composants devraient donc avoir accès aux divers documents attestant que le concept du réseau retenu[2] a été validé ainsi qu'aux certificats de chacun des composants pressentis[3] pour son application.

Des composants aptes à traiter une fonction de sécurité et non pas des « composants de sécurité »

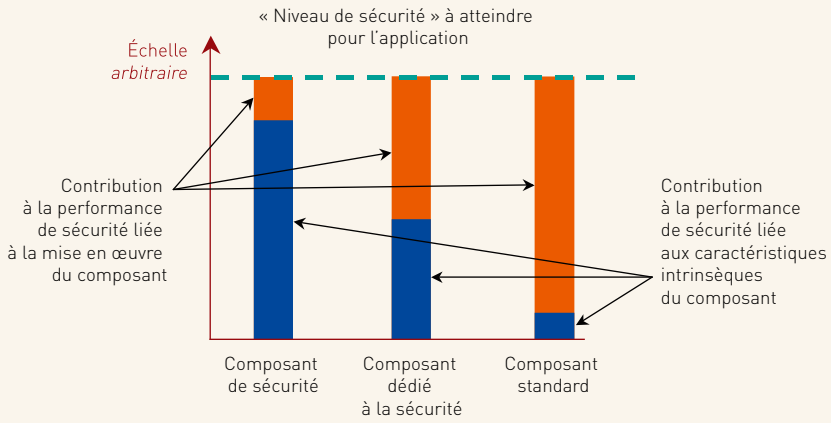
Que des composants dédiés à la sécurité, en particulier les RdTdS, puissent être utilisés pour le traitement des fonctions de sécurité[4] peut apparaître une évidence première. En effet,

Composants de sécurité vs composants dédiés (ou non) à la sécurité

Si le législateur a porté son attention sur les *composants de sécurité* c'est qu'ils sont destinés à faciliter l'action des utilisateurs devant mettre leurs machines en conformité. À cette fin, par la directive Machines, il a établi des prescriptions applicables à ces composants afin qu'ils :

- assurent une fonction de sécurité définie,
- prennent en compte des exigences de sécurité à la conception,
- prévoient l'information complète des utilisateurs pour leur mise en œuvre.

On peut tenter d'illustrer l'apport des composants de sécurité par rapport aux autres types de composants pour satisfaire une prescription de sécurité particulière d'une installation.



Ce graphique montre la participation de chacun des composants liée à ses caractéristiques intrinsèques et le chemin restant à parcourir, lié à la mise en œuvre de ces composants pour atteindre l'objectif fixé.

Plus un composant est conçu et spécialisé pour exécuter une fonction de sécurité définie particulière d'une machine, plus sa mise en œuvre s'en trouvera simplifiée.

Dans le cas contraire, moins le composant est dédié à une fonction particulière, plus sa mise en œuvre deviendra prépondérante devant ses qualités intrinsèques, pour satisfaire un besoin de sécurité spécifié.

En d'autres termes, l'engagement du concepteur d'une installation relative à la sécurité, c'est-à-dire ses moyens, responsabilités, etc., sera différent en fonction du type de composant qu'il aura retenu.

[1] *CEI 61784-3 [5].*

[2] *Dans la version logicielle correspondante.*

[3] *Dans la version logicielle correspondante.*

[4] *En déclinant des principes et des architectures adaptés (redondance, dynamisme, etc.) sur la base des référentiels normatifs adaptés.*

au quotidien, certains constructeurs de machines ou de dispositifs de sécurité traitent déjà des informations de sécurité à l'aide de composants logiques standards, même complexes (microprocesseurs, FPGA, etc.), non conçus spécifiquement pour des applications de sécurité. De plus, force est de constater que les réseaux de terrain dédiés à la sécurité apportent un « plus » incontestable par rapport à ces composants logiques standards : la couche de sécurité supportée par des composants adaptés.

L'essentiel des difficultés liées aux RdTdS ne réside pas dans leur qualité et leurs performances intrinsèques mais dans la complexité de leur mise en œuvre.

En effet, lorsqu'ils sont mis sur le marché, les composants qui constituent les RdTdS ne sont pas capables en l'état de traiter une fonction de sécurité particulière. Ils devront être installés, câblés, programmés, paramétrés pour prendre en charge une partie de la fonction de sécurité qu'ils auront à traiter. Ces composants sont donc commercialisés **pour leur aptitude à traiter la fonction de sécurité qui leur sera confiée**.

Cette caractéristique des RdTdS, bien que n'interdisant en rien leur usage dans les applications de sécurité, les situe en dehors du cadre des composants de sécurité défini par la réglementation : par définition, les RdTdS ne peuvent pas être assimilés aux composants de sécurité au sens de la directive Machines[5].

RÉSEAUX DE TERRAIN DÉDIÉS À LA SÉCURITÉ – LE PROBLÈME DU TEMPS DE RÉPONSE

Les causes de dangers potentiels liées aux RDTdS sont, pour résumer, un retard ou une altération des informations traitées.

Nous avons également déjà précisé que les concepteurs de tels réseaux avaient implémenté des architectures redondantes, chiens de garde, mécanismes de détection d'erreur de transmission, de contrôle du séquencement des logiciels, etc. aptes à garantir les caractéristiques de sécurité revendiquées.

Or, si l'utilisateur, lors de la mise en œuvre de tels réseaux, ne peut pas altérer l'architecture ou la performance de tel ou tel mécanisme de détection d'erreurs, il n'en est pas de même pour le temps de réponse. En effet, les utilisateurs de ces dispositifs doivent être conscients qu'il ne sera pas toujours évident de respecter les temps de réponse spécifiés pour les fonctions de sécurité mais également qu'un allongement des temps de réponse initiaux des fonctions de sécurité traitées par ces dispositifs pourra être induit par des interventions n'ayant pas toujours de rapport direct avec la partie sécurité de l'installation, ni même directement avec le temps de réponse. À titre d'exemple, on peut citer des modifications de longueur de brins du réseau avec ou sans adjonction de répéteur, l'adjonction de nouveaux esclaves, la modification de la partie fonctionnelle, etc.

Pour que ces altérations potentielles des temps de réponse puissent être maîtrisées, elle doivent être connues et les outils permettant d'estimer, voire de mesurer l'incidence réelle d'une modification sur le temps de réponse d'une installation, disponibles et promus par les concepteurs de RdTdS.

LE TEMPS DE RÉPONSE : UNE CARACTERISTIQUE FONDAMENTALE DE LA FONCTION DE SÉCURITÉ

Lors de la démarche de conception de la partie du circuit de commande relative à la sécurité d'une machine et, quel que soit le référentiel normatif retenu[6], la spécification des exigences de sécurité doit, en fonction de l'appréciation du risque, prescrire un temps de réponse maximum requis pour chacune des fonctions de sécurité.

Il faut insister sur le fait que la rédaction de ces spécifications doit avoir lieu dans les phases initiales du développement et que cette caractéristique est de même importance que la spécification d'intégrité de sécurité (SIL, catégorie ou Performance Level) de chacune des fonctions.

Par ailleurs, le temps de réponse requis pour une fonction particulière pourra avoir des incidences fortes sur les options technologiques retenues pour son traitement et pourra même conduire à choisir des automates très performants par exemple, voire à renoncer à certaines technologies dans le cas d'un besoin de temps de réponse très court.

L'obtention des caractéristiques spécifiées devra être vérifiée au terme du développement.

En conséquence, la spécification *a priori* du temps de réponse pour une fonction de sécurité ne doit jamais être négligée ni sous-estimée sous peine d'échec du développement en cours.

RÉSEAUX ET TEMPS DE RÉPONSE

Parler de temps de réponse lié à l'utilisation d'un RdTdS conduira en fait à évoquer deux aspects des temps de réponse :

- le temps de réponse fonctionnel et
- le temps de réponse dysfonctionnel.

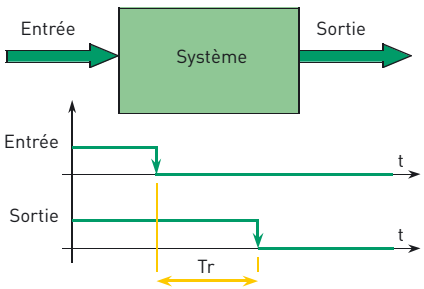
Le temps de réponse qui devra au final être retenu comme valeur effective pour le système devra bien entendu être la valeur la plus importante des deux.

Le temps de réponse *fonctionnel*

Le temps de réponse fonctionnel représente le temps de passage des sorties de sécurité dans une configuration sûre, en réponse au changement d'état d'une entrée, en état nominal de fonctionnement du système *(cf. Figure 2)*.

FIGURE 2

Le temps de réponse fonctionnel
Function response time



Tr = Temps de réponse fonctionnel du système

[5] *Que ce soit dans la directive 98/37/CE ou sa remplaçante 2006/42/CE [6].*
[6] *EN ISO 13849-1, NF EN 62061 ou NF EN 61508.*

Pour les systèmes relatifs à la sécurité intégrant des réseaux de terrain, divers facteurs interviendront sur ce temps de réponse comme :

- la fréquence d'exécution du programme de sécurité,
- le protocole de communication du RdTdS,
- les mécanismes mis en place pour traiter les erreurs de données transmises,
- la topographie du réseau.

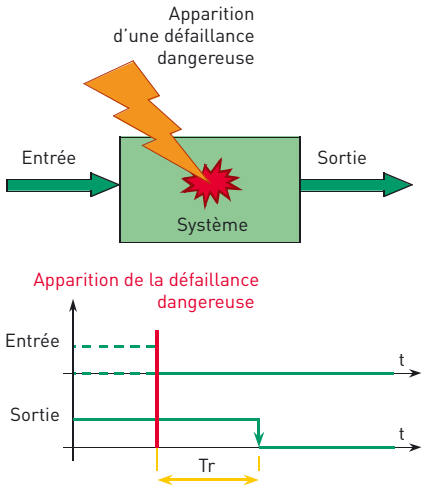
Nombre de ces paramètres sont du ressort de l'utilisateur du réseau de terrain.

Le temps de réponse *dysfonctionnel*

Le temps de réponse dysfonctionnel représente le temps de passage des sorties dans une configuration sûre du système en réponse à une défaillance dangereuse apparaissant dans le système *(cf. Figure 3)*.

FIGURE 3

Le temps de réponse dysfonctionnel
Malfunction response time



Tr = Temps de réponse fonctionnel du système

Pour les systèmes relatifs à la sécurité intégrant des réseaux de terrain[7], ce temps de réponse dépendra essentiellement des valeurs retenues pour les différents chiens de garde ayant en charge la surveillance de l'exécution des programmes assurant la fonction de sécurité et du bon déroulement de la transmission des informations.

[7] *En plus des facteurs intervenant sur le temps de réponse fonctionnel.*

En fonction du type de réseau de terrain utilisé, l'utilisateur peut intervenir sur le réglage de ces paramètres.

Le temps de réponse effectif

Dans l'esprit des utilisateurs de réseaux de terrain, le temps de réponse d'une application est très souvent restreint au seul temps de réponse fonctionnel. En effet, si ce temps de réponse est généralement bien compris, la notion de temps de réponse dysfonctionnel reste souvent obscure, voire ignorée, malgré son apparition ancienne avec la logique séquentielle, en général, et les automates programmables, en particulier. Les RdTdS n'ont fait qu'accroître les difficultés du fait de leur incidence potentielle sur la sécurité.

De plus, la documentation disponible auprès des différents constructeurs de réseaux de terrain reste parfois discrète quand elle aborde le sujet des temps de réponse de leurs dispositifs. De ce fait, les utilisateurs de ces réseaux ne sont pas toujours conscients de l'incidence du réglage ou du choix d'un paramètre sur le temps de réponse effectif de leur installation.

Comment aborder ces difficultés ?

Deux approches pratiques sont envisageables pour aborder les difficultés liées aux temps de réponse.

La première, qui, à notre sens, doit être écartée, consiste à mesurer les temps de réponse obtenus au terme du développement de l'application, puis éventuellement à corriger l'application configurée pour atteindre ou approcher les valeurs spécifiées. Cette approche présente deux inconvénients majeurs :

- le résultat de la mesure d'un temps de réponse n'est pas toujours représentatif du temps de réponse effectif de l'installation,
- la correction *a posteriori* de l'application présente des risques certains et doit être conduite avec les mêmes règles que le développement initial.

La deuxième consiste à prendre en compte les temps de réponse au plus tôt dans le développement de l'application en procédant à une analyse *a priori* du pire cas des temps de réponse accessibles avec les matériels envisagés. Cette fois, la difficulté réside dans la complexité de la tâche à accomplir et dans les limites des outils disponibles. C'est pourtant cette voie qui permettra d'atteindre les résultats escomptés.

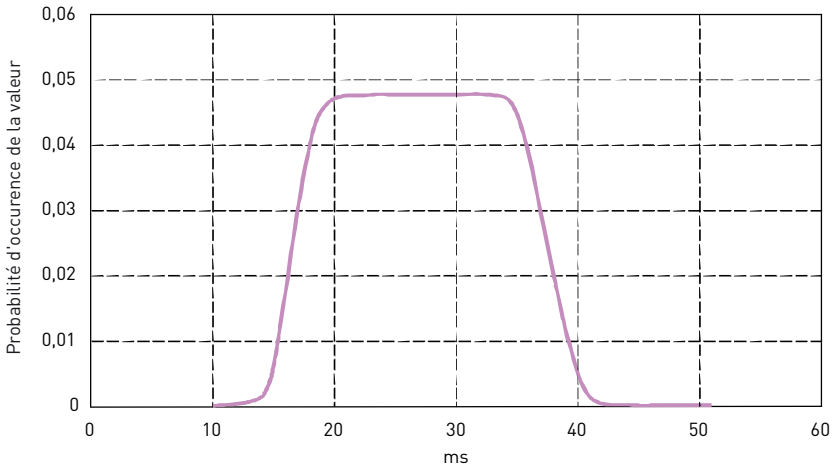
Limites de la mesure du temps de réponse des systèmes intégrant des réseaux

La première difficulté dans la mesure du temps de réponse d'une fonction de sécurité est liée aux conditions de charge du réseau de terrain au moment de la mesure. En effet, pour certains, le temps de réponse mesuré peut être minimisé par des conditions optimales de fonctionnement.

Une autre difficulté, liée à la logique séquentielle en général et aux principes de fonctionnement des réseaux en particulier, est illustrée par la *Figure 4*.

FIGURE 4

Courbe typique de mesure du temps de réponse d'un RdTdS
Typical response time measurement curve for a safety-dedicated field bus



Elle est extraite de la norme CEI 61784-3 et illustre la courbe typique des résultats d'un grand nombre de mesures de temps de réponse sur une fonction de sécurité dans le traitement de laquelle intervient un réseau de terrain. Comme on peut le constater, il est illusoire d'envisager de qualifier les temps de réponse d'un tel système simplement par quelques mesures qui, indépendamment l'une de l'autre, ne seront pas significatives du temps de réponse maximum envisageable. Or, c'est seulement la valeur maximale du temps de réponse qui doit être prise en compte par exemple dans le calcul des distances d'implantation des dispositifs de protection.

La simple mesure des temps de réponse montrant ses limites, il est indispensable d'estimer *a priori* la valeur maximale du temps de réponse prévisible pour l'installation projetée – le pire cas –, pour s'assurer de la compatibilité des mesures de protection envisagées, par exemple.

La notion de « pire cas »

L'expérience montre que la correction a posteriori du circuit de commande pour satisfaire les temps de réponse prescrits reste la plupart du temps illusoire, car une réduction significative dépendra souvent de remaniements importants aux conséquences très lourdes. Il est donc essentiel d'intervenir au plus tôt, c'est-à-dire au début du développement de l'application.

Avant de préciser cette notion de pire cas pour le temps de réponse, nous nous proposons d'illustrer les différents intervenants dans la valeur nominale du temps de réponse et dans son maintien. La *Figure 5*, extraite de la norme CEI 61784-3, décrit les composants classiques d'une chaîne de sécurité.

Le temps de réponse global de cette chaîne sera égal à la somme des temps de réponse de chacun des éléments de la fonction de sécurité. Par voie de conséquence, le pire cas pour le temps de réponse fonctionnel sera obtenu en additionnant les valeurs maximales envisageables pour chacun de ces composants.

De plus, dans ce type d'architecture, comme la majorité des composants participant au traitement et à la transmission des informations de sécurité est réalisée en logique séquentielle, le temps de réponse de chacun de ces composants peut varier de manière importante.

Il est donc nécessaire que celui qui a en charge le développement d'une application de sécurité dispose d'outils, de méthodes, etc. lui permettant cette estimation préalable indispensable pour atteindre l'objectif de sécurité fixé. Or, qui d'autre que le concepteur du réseau de terrain est capable de concevoir et de fournir de tels outils ?

À ce jour, certains de ces outils existent, mais leur manipulation est délicate et les valeurs qu'ils délivrent sont parfois le résultat d'une simple estimation.

Illustrations pratiques de ces difficultés

Des temps de réponse annoncés et garantis : parfois oui, mais...

Certains fabricants de RdTdS s'engagent formellement sur le temps de réponse maximum garanti par conception de toute fonction de sécurité traitée, quels que soient la configuration du réseau, le nombre d'esclaves, la longueur de câble, etc. C'est le cas d'AS-i Safety at Work qui garantit :

- le temps maximum de transmission de l'information entre l'esclave d'entrée et l'unité de traitement,
- le temps maximum de traitement des informations,
- le temps maximum de réaction des sorties de sécurité.

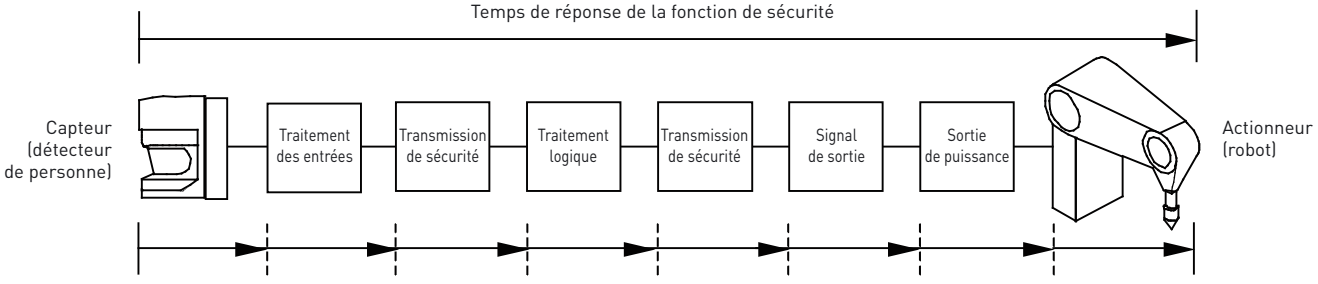
Pour ce dispositif, le temps de réponse global de la fonction traitée sera, dans le pire cas, égal à la somme de ces trois valeurs. De plus, cette valeur limite est fixe et indépendante de la configuration du réseau par l'utilisateur.

Pour ses utilisateurs, la seule difficulté concernant ce dispositif est de trouver une indication précise et fiable de cette valeur maximale de temps de réponse dans les diverses documentations qu'ils auront à leur disposition. En effet, nous avons trouvé la valeur de 35 ms dans une documentation éditée par le consortium en charge de ce réseau, et de 40 ms, voire de 50 ms dans diverses documentations techniques de constructeurs de composants spécifiques, sans être capable de discerner si cette variation de temps de réponse était due à des erreurs de documentations, des évolutions techniques, etc.

Cet exemple, concernant un des produits du marché les plus simples à mettre en œuvre, illustre bien que les utilisateurs de RdTdS devront s'investir dans la recherche et la traçabilité des éléments techniques concernant le temps de réponse de la partie sécurité de leur installation et, en particulier, de la partie réseau.

FIGURE 5

Exemple de chaîne de sécurité
Example of a safety line



Des temps de réponse annoncés et garantis : parfois non !

Pour d'autres réseaux, le temps de réponse ne peut plus être ni annoncé ni garanti par conception car de multiples paramètres peuvent interférer.

Dans de tels cas, le temps de réponse obtenu au final dépendra du concept et des composants du réseau proprement dit et de l'installation réalisée (nature du médium, longueur des branches du réseau, fonctionnel de l'application, etc.). La communication des différents constructeurs de RdTdS sur le sujet est parfois relativement imprécise et les informations techniques détaillées difficiles à extraire des documentations souvent volumineuses.

le compromis sécurité/disponibilité

La conséquence d'une modification de la fréquence d'exécution du programme de sécurité est illustrée par les *Figures 6 et 7* extraites de la norme CEI 61784-3.

La *Figure 6* montre différentes possibilités de répartition des temps de l'automate pour l'exécution des programmes applicatifs standards et de sécurité.

Dans le diagramme du haut, la priorité est donnée à l'exécution du programme de sécurité. L'applicatif de la machine est exécuté dans les périodes laissées disponibles. Dans le diagramme du bas, au contraire, la priorité est donnée à l'exécution du programme applicatif standard, la fréquence d'exécution du programme de sécurité s'en trouvant fortement diminuée.

Comme l'illustre la *Figure 7*, un tel choix de paramétrage aura une incidence forte sur les temps de réponse du système. Dans cet exemple, lorsque le programme de sécurité est lancé toutes les 10 ms, le temps de réponse maximum de la partie sécurité est mesuré à 30 ms alors que le temps de réponse du logiciel standard est de l'ordre 60 ms.

Par contre, lorsque le programme de sécurité est lancé toutes les 30 ms, le temps de réponse maximum de la partie sécurité augmente à 50 ms et le temps de réponse du logiciel standard passe à 40 ms.

Dans la réalité, une telle dérive est souvent le résultat d'un accroissement non maîtrisé du logiciel applicatif standard de la machine, lié par exemple à l'adjonction de nouvelles fonctionnalités, de nouvelles entrées standards, etc. faisant suite, le plus souvent, à une sous-évaluation de la puissance nécessaire pour l'unité de traitement.

FIGURE 6

Exemple des modes d'exécution des programmes de sécurité et standard dans le cas de certains RdTdS

Example of safety and standard programme execution methods for certain safety-dedicated field busses

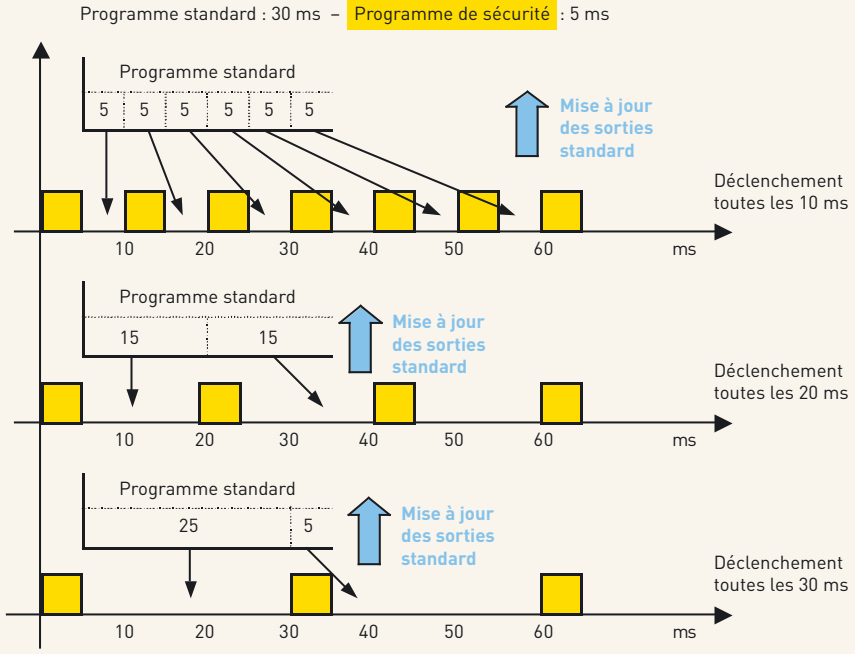
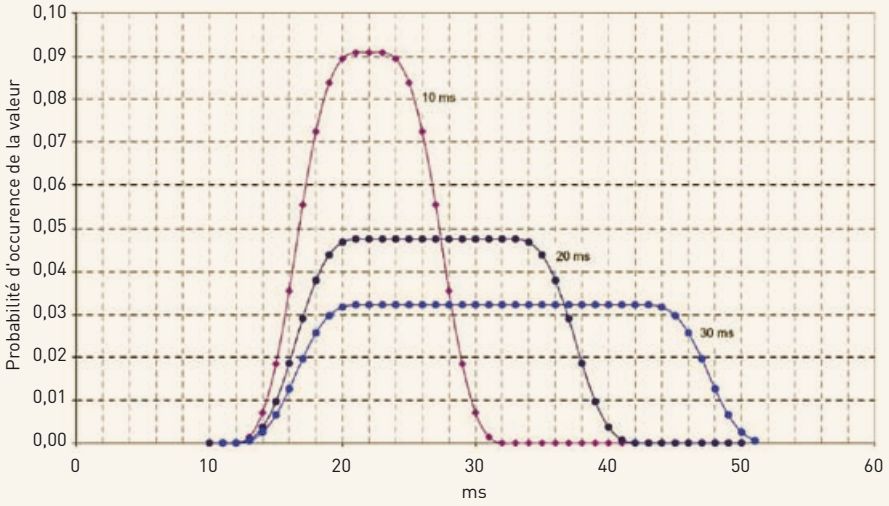


FIGURE 7

Exemple des temps de réponse obtenus en fonction des modes d'exécution des programmes de sécurité et standard

Example of response times obtained depending on safety and standard programme execution method



Pour illustrer en quoi le concepteur peut altérer de manière indirecte la performance de sécurité de son application de sécurité, nous allons montrer comment, pour certains réseaux, le logiciel exclusivement fonctionnel peut interférer sur la sécurité.

L'exemple retenu est celui d'un réseau de type PROFIsafe pour lequel l'application de sécurité s'exécute cycliquement, lors d'interruptions périodiques de l'exécution de l'application fonctionnelle de la machine. La fréquence d'exécution du programme de sécurité est paramétrable par l'utilisateur du réseau. Ce paramétrage est déterminé en fonction des besoins de traitement de l'application de sécurité et **ne doit surtout pas l'être pour répondre aux besoins de l'application fonctionnelle**. En effet, **la performance de sécurité d'une installation ne doit pas être l'otage d'un quelconque compromis sécurité/disponibilité**.

CONCLUSION

Le temps de réponse des réseaux de terrain dédiés à la sécurité

La spécificité des RdTdS a donc pour conséquence d'impliquer fortement le concepteur de l'application de sécurité dans la satisfaction des prescriptions qu'il a établi.

Cette implication forte des concepteurs de machines n'enlève cependant rien aux obligations des constructeurs de RdTdS ou de leurs composants spécifiques. Or, si les composants mis sur le marché remplissent parfaitement la fonction et la performance de sécurité pour lesquelles ils ont été conçus, la documentation qui les accompagne n'est pas exempte de lacunes.

En effet, les informations précises et lisibles permettant d'estimer les temps de réponse fonctionnels au moment de la définition du matériel ne sont pas toujours aisément accessibles. De plus, les outils de calculs n'ont en général ni la lisibilité, ni la commodité d'emploi qui pourrait en être attendues. Enfin, l'incidence sur le temps de réponse dysfonctionnel de chacun des réglages accessibles pour les différents chiens de garde est documentée avec économie.

La documentation relative aux différents RdTdS souvent pléthorique a parfois raison de la motivation des utilisateurs de tels composants. Donc, sans un effort continu des constructeurs de composants pour réseaux, la situation risque de se dégrader, du fait en particulier de la complexité croissante des nouveaux réseaux disponibles sur le marché. Les informations et les outils pour réaliser ce travail d'analyse indispensable devraient être disponibles en toute transparence et même promus au même titre que le SIL 3 ou la Catégorie 4 que ces mêmes réseaux permettent d'atteindre !

Les réseaux de terrain dédiés à la sécurité

La ligne de conduite à adopter face à l'utilisation des RdTdS est on ne peut plus claire : il est possible de traiter les fonctions de sécurité par l'intermédiaire des RdTdS à la seule condition que les intervenants dans un tel développement en aient la capacité et puissent disposer des moyens pour mettre en place la démarche de conception nécessaire.

Par ces termes, notre objectif n'est pas de dissuader les concepteurs potentiels de s'engager vers de telles solutions techniques pour traiter leurs applications relatives à la sécurité, mais de s'assurer, avant de s'engager vers de telles solutions techniques, que les concepteurs potentiels sont conscients et ont les moyens d'assumer :

- les implications techniques liées au choix de ces composants,
- la responsabilité propre de chacun des acteurs d'une telle opération de (re) conception.

Pour ceux qui sont décidés à franchir ce pas technologique, la mise en œuvre de tels dispositifs aura une incidence forte sur :

- le concepteur habituel de circuits de commande relatifs à la sécurité, qui devra s'adapter à la spécificité de ces composants,
- l'utilisateur de machines envisageant le recours à cette technologie, qui devra endosser le rôle du concepteur de circuit de commande relatif à la sécurité.

Les RdTdS en résumé...

Nous pouvons formuler un certains nombre de constats concernant les réseaux de terrain dédiés à la sécurité.

Les réseaux de terrain dédiés à la sécurité ainsi que les composants compatibles disponibles sur le marché :

- ne sont pas des composants de sécurité au titre de la directive « Machines »,
- sont conformes à leurs spécifications (sous réserve de validation des concepts et composants par un organisme compétent),
- sont capables de traiter des fonctions de sécurité répondant selon les cas à un SIL 1, 2 ou 3 ou à une Catégorie 2, 3 ou 4, lorsqu'ils sont convenablement mis en oeuvre,
- sont souvent complexes à mettre en œuvre (documentation abondante, accès difficile aux informations essentielles, notion de temps de réponse délicate à manier, etc.),
- sont ouverts, pour la plupart, sur le monde extérieur à l'application de sécurité :
  - par le matériel, en cas d'utilisation d'un médium non dédié à l'application de sécurité,
  - par le logiciel, en cas de gestion du fonctionnel de l'installation en plus des fonctions de sécurité par un dispositif unique.

  Cette ouverture peut entraîner des difficultés à appréhender et maîtriser les influences externes.
- sont conçus et promus par leurs concepteurs pour faciliter l'évolutivité des installations.

De plus, le développement et la maintenance des circuits de commande relatifs à la sécurité doivent se faire dans un cadre de conception strict pris en charge par une structure projet et orientée vers la performance de sécurité visée.

Cette exigence fondamentale dans le cadre habituel des applications de sécurité se trouve renforcée par le recours à une technologie qui étend le domaine des possibles pour le traitement des fonctions de sécurité. L'ouverture permise par ces dispositifs multipliant les sources d'erreurs, de défaillances systématiques, etc., il devient indispensable d'encadrer plus strictement encore le traitement des fonctions de sécurité par de tels composants complexes.

Les concepteurs d'applications relatives à la sécurité se doivent de concevoir leur système pour atteindre la Catégorie, le Niveau de Performance ou le SIL déterminé lors de l'analyse des risques **dans le respect des temps de réponse fonctionnels et dysfonctionnels spécifiés**.

Ils peuvent s'appuyer sur les normes applicables à la conception des circuits de commande relatifs à la sécurité, qui définissent des prescriptions applicables à chacune des étapes de la conception, et en particulier sur les normes NF EN 62061 et EN ISO 13849-1 qui sont des textes adaptés à l'intégration d'un réseau dédié à la sécurité.

L'encadré ci-contre présente un certain nombre de points clés à considérer pour la mise en œuvre des réseaux de terrain dédiés à la sécurité.

Reçu le : 25/02/2008
Accepté le : 06/03/2008

Quelques obligations pour le concepteur lors de la conception de son système relatif à la sécurité

- S'assurer du niveau de formation des différents intervenants d'un projet basé sur ces technologies. Cette formation proposée, en particulier, par les fabricants de composants de réseaux devra leur permettre :
  - d'avoir une parfaite compréhension de la mise en œuvre et de la configuration du matériel utilisé dans l'application à concevoir,
  - de posséder la maîtrise des outils et des langages de paramétrages et de programmation.
- Respecter les consignes énoncées dans les différents guides et notices rédigés en support au bus utilisé :
  - les fournisseurs doivent mettre à disposition une documentation complète et lisible pour chacun des composants impliqués dans le fonctionnement du bus,
  - les fournisseurs doivent fournir les certificats et avis délivrés par des organismes compétents.
- Prendre en compte les incidences de la compatibilité électromagnétique. En l'absence de référentiel spécifique, les concepteurs pourront s'appuyer sur les exigences fixées par la norme CEI 62061 en termes d'immunité aux perturbations. Ils devront également appliquer les prescriptions particulières (matériels spécifiques, montage, câblage, etc.) édictées par les constructeurs des composants du bus.
- Valider que le niveau de sécurité spécifié pour l'installation est effectivement atteint. Cette validation sera facilitée par le recours à un organisme compétent, qui devra alors être associé dès la phase de spécification de l'installation.

Quelques obligations pour les utilisateurs/concepteurs lors de l'évolution de leur système relatif à la sécurité

- Maintenir leur système pour conserver la Catégorie, le Niveau de Performance ou le SIL déterminé par l'analyse des risques initiale dans le respect des temps de réponse fonctionnels et dysfonctionnels spécifiés.
- Maîtriser l'évolution matérielle de l'installation, lors :
  - de l'ajout de composants supplémentaires,
  - de l'évolution des spécifications des composants existants,
  - de l'apparition de nouveaux composants...
- Maîtriser l'évolution logicielle de l'installation tant sur le plan sécurité que sur le plan fonctionnel pour les solutions intégrées, en veillant :
  - à l'équilibre sécurité/disponibilité mis en cause par l'accroissement des ressources nécessaires au fonctionnel de l'application,
  - aux nouvelles versions des logiciels...
- Qualifier formellement après chaque évolution les temps de réponse fonctionnels et dysfonctionnels de l'installation.

ANNEXE

PRÉSENTATION DE TROIS RÉSEAUX DE TERRAIN DÉDIÉS À LA SÉCURITÉ REPRÉSENTATIFS DE L'ENSEMBLE DE L'OFFRE DISPONIBLE SUR LE MARCHÉ

AS-I SAFETY AT WORK

AS-i Safety at Work est un RdTdS utilisant comme support matériel et logiciel le réseau AS-i[8] *(cf. Figure 8)*.

Pour permettre la transmission des données de sécurité sur le câble AS-i, des esclaves et des moniteurs de sécurité spécifiques associés à une solution logicielle dédiée ont été développés pour atteindre une performance de sécurité de Catégorie 4 selon EN ISO 13849-1 [2] ou de SIL[9] 3 selon NF EN 61508[10] [3]. Bien que le raccordement des organes de sécurité soit entièrement compatible avec le réseau AS-i standard et que les échanges des données standards et des données de sécurité soient toujours gérés par l'intermédiaire du maître AS-i et d'un automate programmable standard, le réseau AS-i Safety at Work est conçu pour rendre sa performance de sécurité entièrement indépendante de la partie d'AS-i standard.

Les moniteurs de sécurité pilotent les sorties de l'application de sécurité. Ils sont déclinés en versions simple ou double circuits de commande indépendants, délivrant chacun 2 contacts de sécurité libres de potentiel. Les esclaves d'entrée permettent le raccordement d'une entrée de sécurité en catégorie 3 et 4, ou de deux entrées de sécurité en catégorie 2.

Certains composants de sécurité et dispositifs de protection (boutons d'arrêt d'urgence, barrières immatérielles, etc.) intègrent leur propre esclave de sécurité et peuvent ainsi être raccordés directement sur le câble AS-i.

AS-i est un réseau de terrain principalement utilisé pour réduire le câblage des capteurs/actionneurs au niveau des machines. Initialement conçu pour des fonctions tout ou rien, il a évolué pour permettre d'acquérir des informations de capteurs analogiques.

L'alimentation des périphériques AS-i et la transmission des données sont assurées par un câble unique à deux fils. Une alimentation spécifique fournit l'énergie nécessaire aux esclaves et assure le découplage des signaux de données des communications, une surveillance de mise à la terre, de courts-circuits et de surcharge.

La communication entre un boîtier maître AS-i et les esclaves présents sur le bus s'effectue par des échanges de données utilisant un codage synchrone de type Manchester.

Principes généraux

ASIMON est l'outil logiciel de configuration graphique pour le paramétrage de l'application de sécurité. L'utilisateur dispose d'une bibliothèque de fonctions pour la concevoir. Une fois achevée, celle-ci est transférée dans le moniteur de sécurité. Elle inclut une signature numérique qui lui est propre ainsi qu'une protection par un mot de passe.

Au cours du fonctionnement, le moniteur de sécurité surveille les trames de données qui circulent sur le médium et reste le seul décisionnaire

[8] *Actuator Sensor interface.*
[9] *Safety Integrity Level.*
[10] *Ou encore NF EN 62061 [4].*

FIGURE 8

Exemple d'une installation AS-i intégrant AS-i Safety at Work
Example of an AS-I installation integrating AS-i Safety at Work

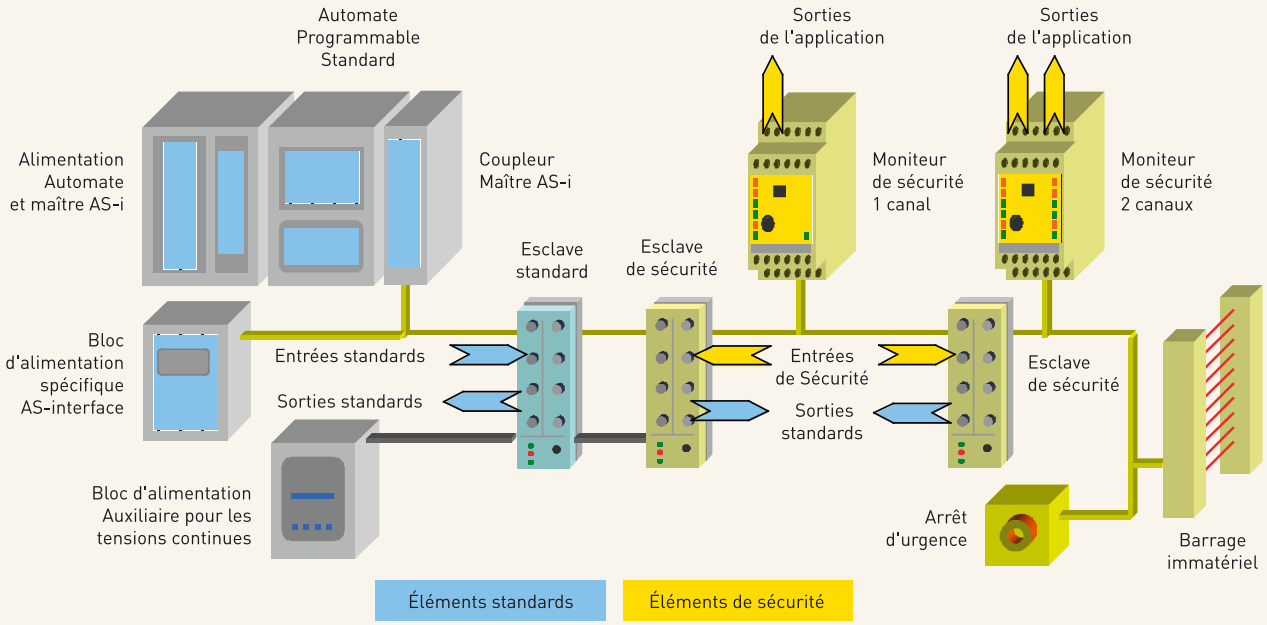
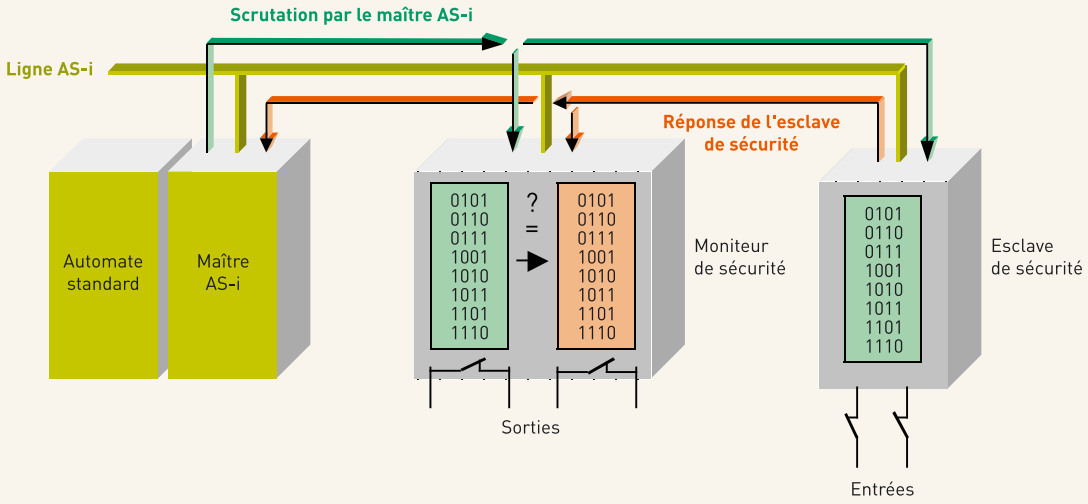


FIGURE 9

Principe du dialogue AS-i Safety at Work
AS-i Safety at Work dialogue principle



de l'état de ses sorties de sécurité. La configuration de l'application de sécurité est enregistrée dans le moniteur, lui permettant ainsi de contrôler les esclaves de sécurité qui lui sont affectés *(cf. Figure 9)*.

La transmission des informations est sécurisée par l'utilisation de tables de codes dynamiques propres à chacun des esclaves de sécurité. En réponse au maître AS-i qui interroge tous les esclaves par une scrutation cyclique, l'esclave de sécurité transmet sa table de code qui est comparée avec celle inscrite dans le moniteur de sécurité. En cas de codes différents suite à une modification de l'état des entrées de l'esclave de sécurité, ou encore à l'absence ou au retard d'un message, le moniteur de sécurité commute ses sorties à l'état d'arrêt. Ce principe garantit également la mise en repli de l'installation en cas de codes erronés suite par exemple à des perturbations électromagnétiques.

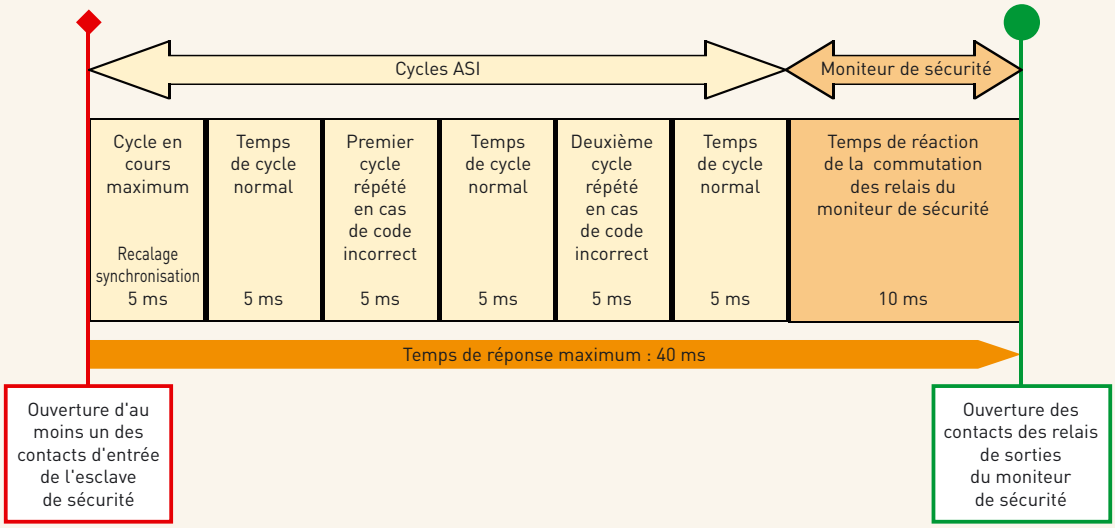
Toutes modifications de la configuration du système, comme l'ajout ou le retrait d'un esclave de sécurité sans passer par une phase de reconfiguration provoquera la mise en repli du moniteur de sécurité.

Le temps de réponse

La durée d'un cycle de scrutation est proportionnelle au nombre d'esclaves interrogés par le maître AS-i, soit 5 ms pour 31 esclaves maximum en version 2.0 AS-i. Le nombre maximal d'esclaves sur un brin AS-i étant limité et le temps de réaction du moniteur de sécurité connu, le temps de réponse maximum d'AS-i Safety at Work à un signal d'entrée d'un esclave de sécurité quelconque est donc déterminé. Il est toujours inférieur à 40 millisecondes *(cf. Figure 10)*.

FIGURE 10

Temps de réaction dans le *pire cas* du système pour un moniteur de sécurité dont le temps de réponse est de 40 ms
System *worst case* reaction time for a safety monitor with a 40 ms response time



Des constructeurs proposent toutefois des moniteurs de sécurité spécifiques avec des temps de réponse supérieurs (50 ms) pour des installations privilégiant la disponibilité du réseau au détriment du temps de réponse. Ces solutions sont destinées à des applications développées pour des environnements électriques très perturbés.

Évolutions d'AS-i Safety at Work

Les évolutions prévues à ce jour pour les spécifications d'AS-i Safety at Work ne devraient avoir d'influence ni sur la performance de sécurité du réseau ni sur les temps de réponse. Elles portent essentiellement sur des fonctions annexes.

PROFISAFE

PROFIsafe est un profil applicatif[11] du réseau de terrain PROFIBUS[12], dédié à la gestion des fonctions de sécurité : PROFIsafe peut donc être assimilé à un RdTdS. Cette déclinaison particulière de PROFIBUS a été spécifiée pour assurer une coexistence des communications sécurisées et standards, sans conflit, sur un médium unique et permettre d'atteindre une performance de sécurité jusqu'à la catégorie 4 selon EN ISO 13849-1 ou le SIL 3 selon NF EN 61508 *(cf. Figure 11)*.

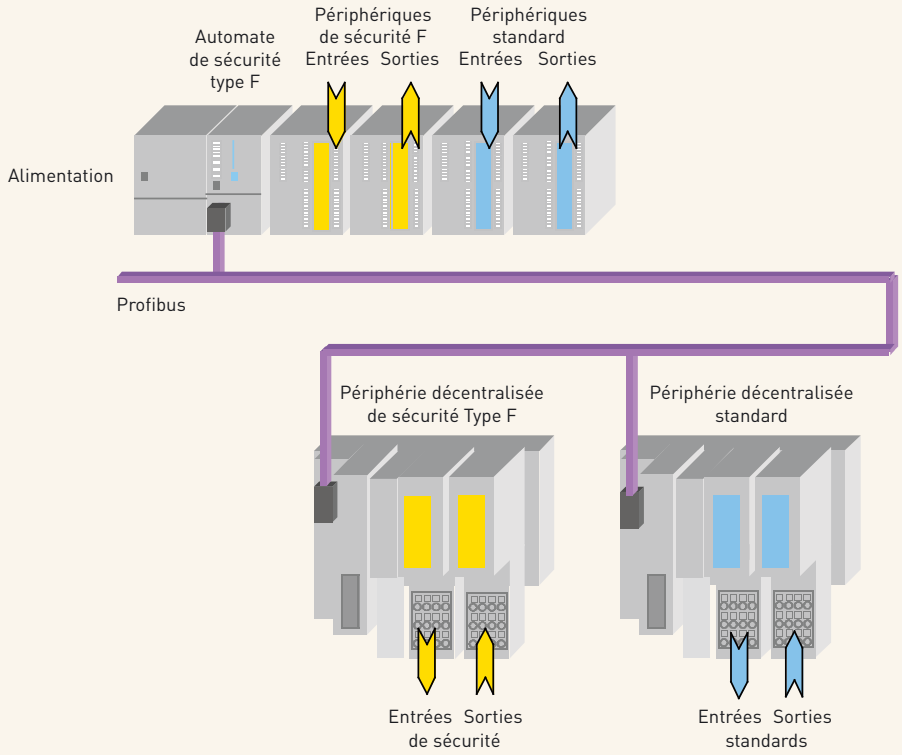
Parmi les divers automates programmables dédiés à la sécurité compatibles disponibles sur le marché, un choix précis doit être fait en fonction de l'application à développer afin de garantir le fonctionnement conforme aux spécifications du projet, notamment en termes de vitesse d'exécution du programme, de capacité mémoire pour supporter l'application, de temps de réponse, etc.

Dans le cas de système de périphéries décentralisées, le média (câble bifilaire blindé en cuivre ou fibre optique) relie des îlots composés de modules d'interfaces de signaux et d'alimentation de sécurité associés à des modules d'entrées et de sorties TOR[13] de sécurité. Le mode de câblage des entrées/sorties sur ces modules, le type du ou des capteurs adaptés (simple ou redondance), ainsi que le paramétrage logiciel doivent être en adéquation avec les choix précédents. Ils sont essentiels pour atteindre le niveau de sécurité visé.

Des capteurs, actionneurs ou des dispositifs de protection équipés d'une interface PROFIsafe pouvant se connecter directement à ce bus sont également disponibles sur le marché.

FIGURE 11

Exemple d'une installation PROFIBUS intégrant PROFIsafe
Example of a PROFIBUS installation integrating PROFIsafe



Profibus est un réseau de terrain conçu pour l'industrie manufacturière et de processus.

Profibus DP est le protocole de communication pour les périphériques décentralisés.

Plusieurs profils applicatifs dits aussi profils métiers (Profibus PA pour l'automatisation des procédés, PROFISafe pour la sécurité, etc.) définissent l'emploi des protocoles de communication et des profils physiques pour différents types d'applications.

Profibus DP permet la communication avec des périphériques décentralisés et la commande de périphériques intelligents. Il utilise une transmission RS485 numérique et différentielle. L'utilisation de répéteurs augmente la distance de communication et l'utilisation de fibres optiques permet une amélioration de l'immunité aux perturbations électriques et une transmission sur de longues distances.

Principes généraux

La programmation d'une application de sécurité se fait au moyen du logiciel S7 Distributed Safety, intégré dans un environnement logiciel STEP 7.

STEP 7 permet la programmation de la partie standard de l'application et fournit des fonctionnalités pour les différentes phases du projet d'automati-

[11] *Appelé aussi profil métier.*
[12] ***P**rocess **F**ield **Bus**.*
[13] *Tout ou rien.*

FIGURE 12

Principe d'une communication standard et relative à la sécurité sur PROFIsafe V2
Standard and safety-related communication principle using PROFIsafe V2

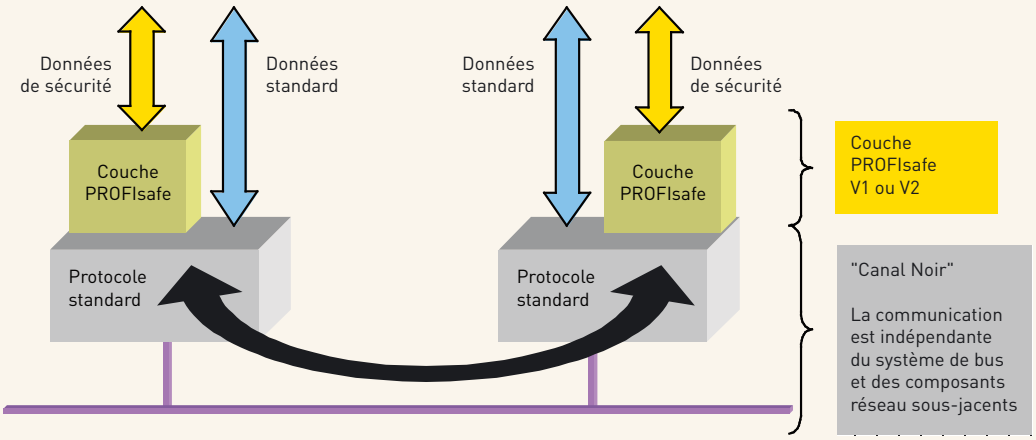
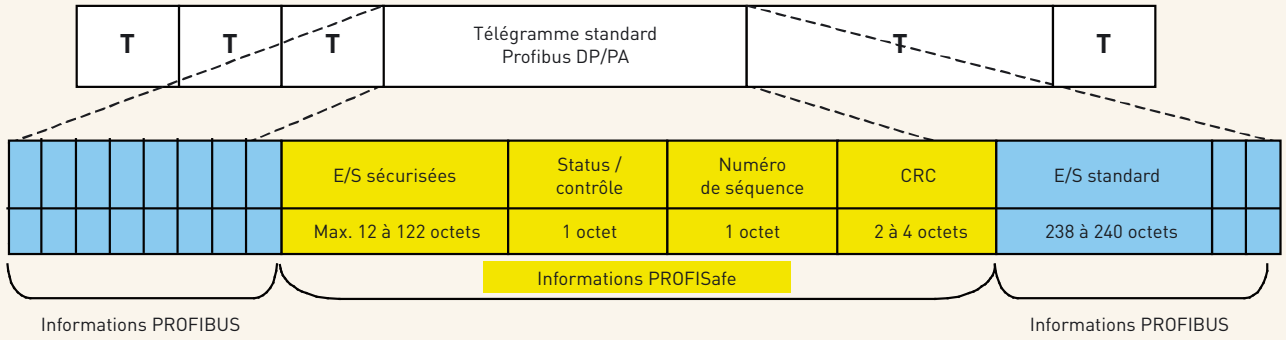


FIGURE 13

La trame de sécurité PROFIsafe est encapsulée dans le télégramme PROFIBUS
PROFIsafe safety channel is embedded in the PROFIBUS telegram



sation : configuration, mise en service, test, maintenance, etc. STEP 7 couvre aussi bien la configuration matérielle de l'installation que le paramétrage des modules. La configuration des modules de sécurité se fait de la même manière que pour la périphérie standard. Les liaisons de communication au sein d'un projet sont définies sur une interface utilisateur graphique.

S7 Distributed Safety propose des instructions, opérations et bloc fonctionnels permettant la réalisation de programmes de sécurité dans les langages CONT (schéma à contacts) et LOG (logigramme). Une bibliothèque comportant des blocs prêts à l'emploi et certifiés par le TÜV[14] est disponible pour réaliser les fonctions de sécurité (de type F - FailSafe).

Le programme de sécurité est appelé à partir du programme utilisateur standard s'exécutant sur la même CPU de type F *(cf. Figure 12)*.

Pour sécuriser ces communications, un format de données et un protocole spécifiques sont utilisés *(cf. Figure 13)*.

Quatre mécanismes corrigent ou détectent les erreurs de transmission :

- une numérotation en continu des télégrammes de sécurité assurée par l'émetteur comme signe de vie des périphériques,
- un délai de scrutation pour chaque récepteur de l'arrivée des messages et des acquittements par une technique de chien de garde,
- une identification des communications entre l'émetteur et le récepteur agissant comme un mot de passe. À titre d'exemple, un message envoyé sur le réseau arrivant par erreur à un équipement de sécurité suite à un adressage erroné sera détecté (erreur de type mascarade),
- une vérification de cohérence des données par un polynôme CRC[15], clé de contrôle supplémentaire calculée à partir des données de la trame PROFIsafe et des données de configuration de l'élément de sécurité.

En plus de ces différents mécanismes, un dispositif breveté, le moniteur de SIL, garantit le respect du niveau de SIL requis pour l'application. Son fonctionnement est basé sur la surveillance des messages erronés pendant une fenêtre temporelle configurée en fonction du niveau de SIL exigé. Les erreurs de transmission détectées par le maître ou les esclaves de sécurité sont comptabilisées et un calcul statistique détermine le

[14] *Technischer Überwachungs-Verein.*
[15] *Contrôle de Redondance Cyclique.*

FIGURE 14

Outil développé par la société Siemens permettant l'estimation du temps de réponse de l'application envisagée

Tool developed by the SIEMENS company for estimating response time for of a projected application

s7tcotic.xls

	A	B	C	E
19	**Entrée**			
20	Périphérie F (entrée)	Temps de discordance max.	10 ms	
21		Temps de réaction max. en l'absence d'erreur	14 ms	
22		Temps de réaction max. en cas d'une erreur	14 ms	
23		Temps de surveillance PROFIsafe configuré	50 ms	
24	Pour l'ET 200M et l'ET 200S	Allongement max. dû à l'IM et à son bus	2 ms	
25	PROFIBUS-DP	Target-Rotation-Time max.	5 ms	
26	CP PROFIBUS	Temps de retard DP supplémentaire	0 ms	
27	**Traitement dans la 1e CPU F**			
28	1. Groupe d'exécution F	Temps de cycle max. de l'OB	30 ms	
29		Temps de cycle max. (temps de surveillance	40 ms	
30		Temps d'exécution max.	20 ms	
31	2. Groupe d'exécution F (optionnel)	existant ?	Oui	
32		Temps de cycle max. de l'OB	60 ms	
33		Temps de cycle max. (temps de surveillance	70 ms	
34		Temps d'exécution max.	30 ms	
35	**Traitement dans la 2nde CPU F (optionnel)**		Oui	
36	Communication CPU-CPU	TIMEOUT	80 ms	
37	*Communication CPU-CPU via les liaisons S7*		Oui	
38	*Communication maître-esclave I ou esclave I-esclave I*		Non	
39	CP PROFIBUS	Temps de retard DP supplémentaire	0 ms	
40	PROFIBUS-DP	Target-Rotation-Time max.	5 ms	
41	*Communication maître-maître via coupleur DP/DP*		Non	
42	CP PROFIBUS	$T_{DP\_DLY\_F\_SENDDP}$	0 ms	
43	PROFIBUS-DP	$T_{TR\_F\_SENDDP}$	5 ms	
44	Coupleur DP/DP	T_{COPY}	2 ms	
45	PROFIBUS-DP	$T_{TR\_F\_RCVDP}$	5 ms	
46	CP PROFIBUS	$T_{DP\_DLY\_F\_RCVDP}$	0 ms	
47	1. Groupe d'exécution F	Temps de cycle max. de l'OB	30 ms	
48		Temps de cycle max. (temps de surveillance	40 ms	
49		Temps d'exécution max.	20 ms	
50	2. Groupe d'exécution F (optionnel)	existant ?	Oui	
51		Temps de cycle max. de l'OB	60 ms	
52		Temps de cycle max. (temps de surveillance	70 ms	
53		Temps d'exécution max.	30 ms	
54	**Sortie**			
55	CP PROFIBUS	Temps de retard DP supplémentaire	0 ms	
56	PROFIBUS-DP	Target-Rotation-Time max.	5 ms	
57	Pour l'ET200M et l'ET200S	Allongement max. dû à l'IM et son bus interne	2 ms	
58	Périphérie F (sortie)	Temps de surveillance PROFIsafe configuré	50 ms	
59		Temps de réaction max. en l'absence d'erreur	9 ms	
60		Temps de réaction max. en cas d'une erreur	9 ms	
61				
62	**Temps de réaction max.**			
63	**de la borne d'entrée de la périphérie F (entrée) à la borne de sortie de la périphérie F (sortie)**			
64	En l'absence d'erreur		397 ms	
65	En cas d'une erreur		477 ms	
66	Quel que soit le temps d'exécution du système standard		433 ms	

Tps exec. max. groupe exec. F | Tps d'exéc. min. du programme F | **Temps de réaction max.**

nombre d'erreurs qui n'ont pas été détectées. Le résultat de ce calcul, s'il dépasse la limite correspondante au niveau de SIL défini, interrompt la transmission et met l'installation en repli.

Le temps de réponse

L'outil S7cotic, proposé par la société SIEMENS[16] pour estimer ce temps de réaction de l'application de sécurité, est un fichier de type Excel ; les champs de données issus de nombreux paramètres du projet doivent être renseignés dans le tableau fourni afin d'obtenir les valeurs des temps de réponse. Nous pouvons citer comme exemple d'informations requises : le type des modules, leur mode de fonctionnement, le nombre et type de composants logiciels de la librairie *Distributed Safety*, les types et nombres d'opérateurs logiques utilisés pour le développement logiciel de l'application, le nombre d'entrées de sécurité, le temps de cycle maximum du bloc d'organisation, etc *(cf. Figure 14)*.

Les temps de cycle de PROFIBUS DP sont fonction du nombre d'esclaves, des données de service, du format des données, du nombre d'octets d'entrées et de sorties et de la vitesse de transmission etc. propres à l'application.

Il sera donc indispensable de veiller à ce que l'évolution de ces différentes grandeurs, lors de l'avancement ou de la maintenance du projet, n'entraîne pas de dérive du temps de réponse initialement spécifié pour la fonction.

De plus, comme le programme de sécurité est appelé à partir du programme standard s'exécutant sur la même CPU de type F, l'augmentation du volume du logiciel gérant la partie standard de l'application ne devra pas non plus nuire au temps de réponse de la partie sécurité de l'application.

Il sera donc primordial de choisir les différents composants, paramètres, etc. pour ne pas avoir à dégrader la performance de sécurité de l'application dans le seul but d'en assurer la disponibilité.

Évolution de PROFISAFE

Les besoins croissant de communication dans les applications standards ou de sécurité – augmentation des nombres d'entrées/sorties, débit, portée du réseau, compatibilité, etc. – ont conduit le consortium en charge de PROFIBUS à développer la spécification d'un nouveau réseau, PROFINET, reposant sur une base Ethernet, et à ouvrir PROFIsafe, initialement basé sur PROFIBUS DP, à ce nouveau bus. La nouvelle déclinaison PROFIsafe V2 a donc été spécifiée pour supporter la communication de sécurité sur PROFIBUS DP et sur PROFINET et permettre ainsi les ouvertures attendues.

SAFETYBUS P

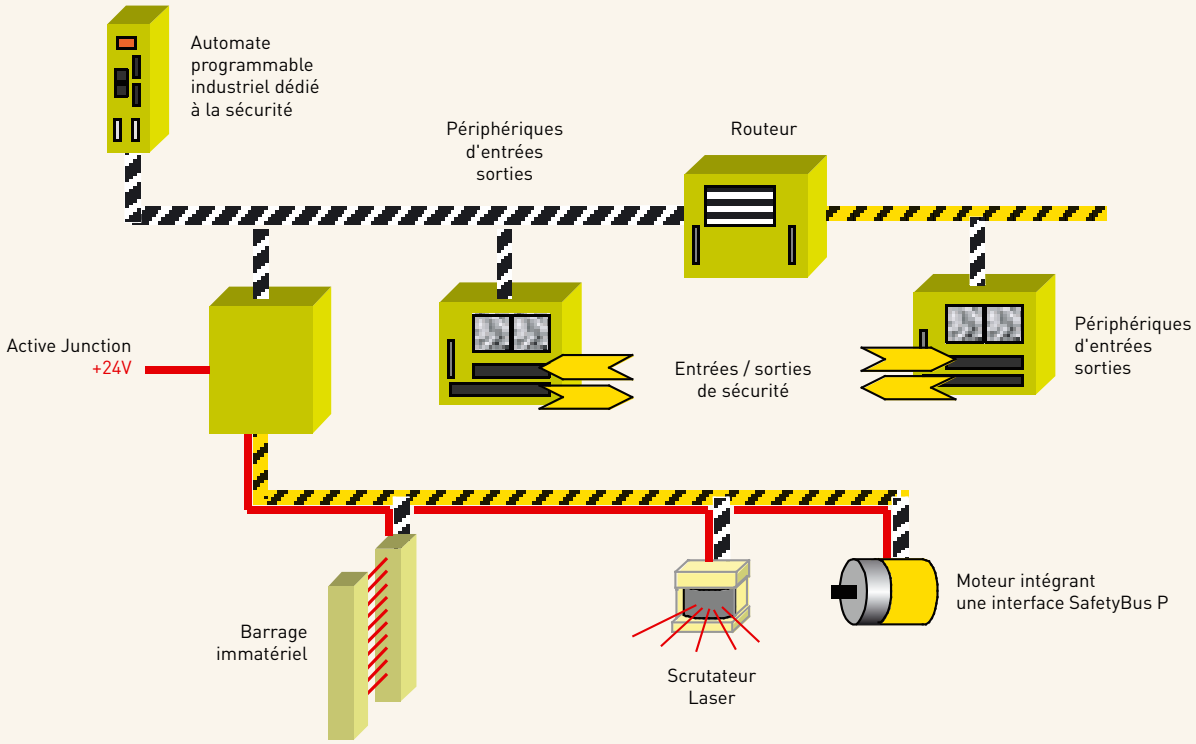
SafetyBUS p est un bus dédié exclusivement à la mise en réseau de la partie sécurité d'applications d'automatisme. Il a été développé dans le but d'atteindre une performance de sécurité de catégorie 4 selon EN ISO 13849-1 ou de SIL 3 selon NF EN 61508 *(cf. Figure 15)*.

Le concept adopté par SafetyBUS p est foncièrement différent de celui qui a prévalu aux deux bus précédemment évoqués. En effet, SafetyBUS p repose sur le principe de séparation physique et logique des signaux de sécurité par rapport à ceux de la voie de commande standard. Ce principe de séparation permet au processus d'automatisation standard de ne pas interférer sur les fonctions de sécurité de l'installation. Cette séparation entre le réseau orienté

[16] *Membre du consortium PROFIsafe.*

FIGURE 15

Exemple d'une installation SafetyBUS p
Example of a SafetyBUS p installation



sécurité et le réseau standard a pour objectifs une augmentation de la disponibilité et une réduction de la charge du bus. SafetyBUS p est un système multi-maîtres avec une topologie de bus linéaire[17] sur la base du système de bus CAN[18].

Le câblage du bus comprend quatre conducteurs, deux pour l'alimentation et deux pour la communication.

Les APIdS de SafetyBUS p doivent être sélectionnés suivant l'application prévue. Les sorties des divers modules d'entrée/sortie de sécurité (Fail-Safe) sont équipées soit de relais électromécaniques, soit de semi-conducteurs. Ces modules sont connectés sur des têtes de station Fail-Safe permettant de créer ainsi des plates-formes de commande décentralisées. Ces périphériques répondent aux exigences de la norme EN CEI 61508 jusqu'au SIL3 et de la norme NF EN 13849-1 jusqu'à la catégorie 4. Sur le marché, on trouve également nombre de composants de sécurité s'interfaçant directement sur ce bus.

Des composants spécifiques (routeurs, répéteurs, ponts, boîtier active junction) peuvent être utilisés pour les longues distances et pour bâtir des topologies de réseau en arbre ou en étoile. De plus, certains de ces modules spécifiques permettent de traduire les informations comme les données de périphériques, les messages d'erreur, etc. à d'autres types de réseaux industriels sans influence sur la partie sécurité.

CAN a été conçu pour transmettre les informations entre capteurs et actionneurs intelligents sur les véhicules automobiles. Il est aujourd'hui utilisé pour l'automatisme et les applications de contrôle. La transmission physique se fait généralement par une paire torsadée blindée ou non. La topologie est celle de bus linéaire.

Le protocole CAN est basé sur le principe de la diffusion générale. Les trames de dialogues sont formées de succession de bits codés par la méthode NRZ (non retour à zéro).

Il est multi-maître, chaque participant est en mesure d'émettre sur le bus si celui-ci est libre. Un message envoyé est écouté par toutes les stations présentes sur le réseau. Le récepteur concerné est averti, les autres ignorent cette séquence.

En cas d'envoi simultané d'une séquence par plusieurs participants, un arbitrage s'établit. La détection des erreurs repose sur des informations intégrées dans la trame des messages. L'émetteur du message erroné est averti afin de renouveler sa demande. En cas de défauts permanents, la station concernée est déconnectée automatiquement du réseau.

[17] *Les différents périphériques du réseau sont reliés à un même câble.*
[18] *Controller Area Network.*

FIGURE 16

Structure schématique du télégramme SafetyBUS p
Diagrammatic structure of the SafetyBUS p telegram

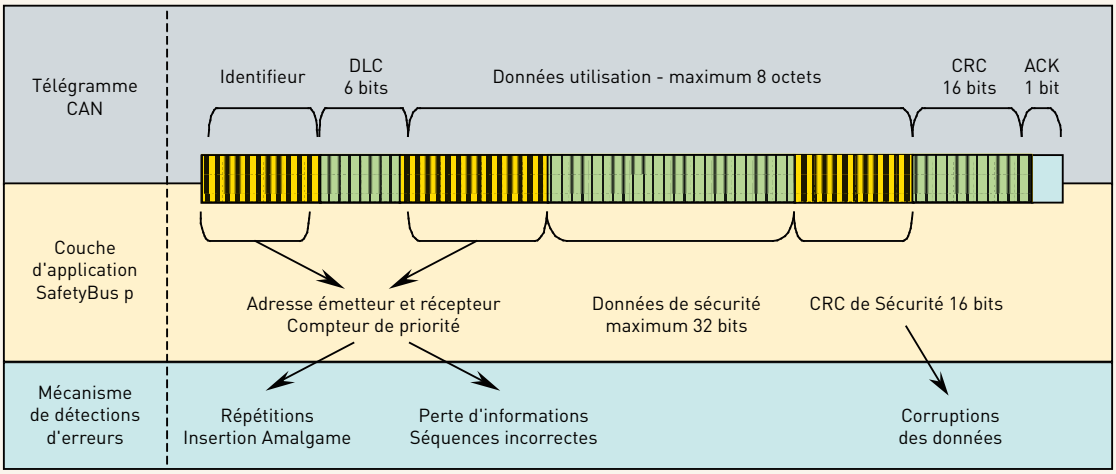
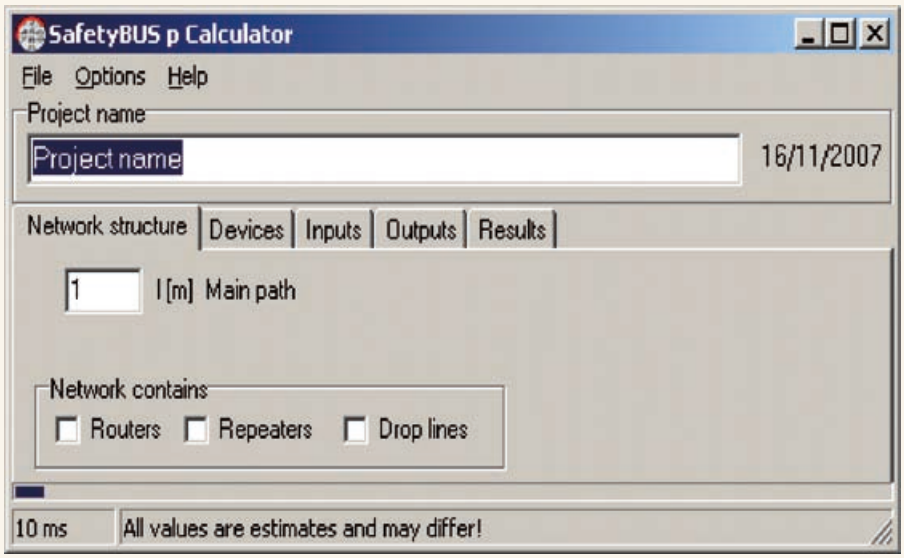


FIGURE 17

Outil développé par la société PILZ permettant l'estimation du temps de réponse de l'application envisagée
Tool developed by the PILZ company for estimating response time of a projected application



Principes généraux

L'atelier logiciel configurateur PSS WIN-PRO commercialisé par la société PILZ, permet de développer un projet. Plusieurs langages de programmation sont disponibles : IL (liste d'instructions), LD (langage à contacts) et FDB (langage de blocs fonctions). Pour les applications de sécurité, des blocs fonctions homologués par le BG et le TÜV sont mis à la disposition des utilisateurs.

La sécurité est réalisée au moyen d'un protocole additionnel à celui du bus CAN et par l'utilisation de composants dédiés à la sécurité. Les capteurs et les actionneurs sont raccordés à un APIdS par l'intermédiaire de modules d'entrées/sorties décentralisés spécifiques à SafetyBUS p.

SafetyBUS p est orienté sur l'événement. Les informations ne sont envoyées qu'en cas de changement d'état sur une des entrées/sorties de l'automate ou d'un module déporté ; par principe, différents maîtres peuvent simultanément demander l'accès au bus.

Les mécanismes de sécurité de SafetyBUS p reposent tout d'abord sur la détection d'erreur des informations transmises sur le bus (répétitions, perte, séquences incorrectes et corruption des données), ainsi que sur la surveillance du temps de réaction en cas de dépassement de délai fixé (Timeout).

Le traitement des informations est effectué par un APIdS ayant une structure redondante. Les têtes de stations qui ont pour mission de traiter les signaux d'un APIdS maître et de les transmettre aux modules d'entrées et de sorties qui lui sont raccordés ont des mécanismes de protection intégrés. Elles disposent de processeurs multicanaux et sont l'objet d'autocontrôles cycliques *(cf. Figure 16)*.

Le temps de réponse

SafetyBUS p Calculator est à la disposition de l'utilisateur pour l'aider dans l'estimation du temps de réponse auquel pourra prétendre son installation. Ce programme de calcul, basé sur un modèle mathématique, permet d'évaluer le temps de réponse de l'application en fonction des paramètres qui seront renseignés par l'utilisateur. Il faut toutefois préciser que l'apport de cet utilitaire est limité par un avertissement précisant que les résultats du calcul découlent uniquement d'une estimation *(cf. Figure 17)*.

Trois modes d'utilisation sont possibles : les modes standard et expert, ainsi qu'un mode relatif à la vitesse de transmission des informations, utilisable pour l'évaluation d'un segment de réseau.

Le résultat de l'estimation du temps de réaction dans le pire cas s'affiche directement, au fur et à mesure de la saisie des paramètres d'entrée, et dépend principalement :

- de la structure du réseau (longueurs du réseau principal et des segments secondaires), du nombre de routeurs et de répéteurs présents et des types du matériel utilisés,
- du nombre de périphériques d'entrées/sorties,
- du nombre d'automates dédiés à la sécurité,
- du nombre de bits d'entrées et de sorties utilisés.

Évolution de SafetyBUS p

SafetyNET p, évolution de SafetyBUS p, est un concept certifié depuis janvier 2007 basé sur un réseau Ethernet déterministe temps réel pour l'environnement industriel. La performance de sécurité visée est identique à celle de SafetyBUS p, mais la finalité de cette nouvelle plate-forme de sécurité SafetyNET p est de faire transiter sur un seul et même câble les données de contrôle commande et les données de sécurité. La mise en réseau d'îlots de production et de machines est possible conformément aux exigences SIL 3 de la norme EN 61508.

BIBLIOGRAPHIE

[1] Directive 98/37/CE *du Parlement Européen et du Conseil du 22 juin 1998 concernant le rapprochement des législations des États membres relatives aux machines.*

[2] NF EN ISO 13849-1. *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception.* Février 2007, 102 p.

[3] NF EN 61508 parties 1 à 7. *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.* Mars 2002, 439 p.

[4] NF EN 62061. *Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité.* Juillet 2005, 106 p.

[5] IEC 61784-3. *Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.* Décembre 2007, 47p.

[6] Directive 2006/42/CE *du Parlement Européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 98/37/CE (refonte).*