

Préface

Lorsque les membres du groupe SEE, Cercle thématique 18.04 Constituants Intelligents pour l'Automatisation et la Mesure, m'ont demandé de préfacer cet ouvrage, j'ai été extrêmement flatté et je voudrais les en remercier.

Ce quatrième opus de la série éditée par Hermès, qui émane des diverses déclinaisons du groupe CIAME, est représentatif de l'évolution technologique et des préoccupations du monde de l'automatisation lors de ces dernières années.

Le premier ouvrage de la série s'intitulait *Capteurs intelligents et méthodologie d'évaluation*, le deuxième *Actionneurs intelligents* ; les titres exprimaient les interrogations relatives aux rôles et fonctions des producteurs et consommateurs d'information et faisaient abstraction plus ou moins explicitement du *medium* de communication, considérant que celui-ci assurait « au mieux » le transfert d'information, quasiment sans délai et sans défaillance...

Le troisième ouvrage *Réseaux de terrain : description et critères de choix* validait le constat que le « réseau de terrain universel » ne verrait jamais le jour, focalisait sur les caractéristiques techniques et tentait de fournir un guide de choix.

Ce quatrième volet s'intéresse plus particulièrement aux aspects sûreté de fonctionnement, ce qui à mon sens est révélateur de la réalité industrielle des « réseaux de terrain » et des interrogations concrètes des utilisateurs confrontés au respect de la normalisation en vigueur, normalisation qui doit évidemment prendre en compte les évolutions technologiques mais doit également offrir les mêmes garanties.

Préface rédigée par Michel ROBERT, professeur à l'université Henri Poincaré Nancy 1, Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (E.S.S.T.I.N.).

Je me permets de souligner également l'évolution linguistique que l'on rencontre au fil de la lecture de ces différents ouvrages, plus particulièrement appréhendable dans la langue anglaise. A la fin des années 1980, le vocable utilisé était plutôt *Fieldbus* alors qu'actuellement la littérature invoque (évoque) plus particulièrement *Networked Control System*, qui exprime que les méthodologies d'automatisation doivent intégrer l'échange d'informations numériques *via* des réseaux.

Enfin, pour conclure, je ne peux qu'émettre le vœu de voir se poursuivre cette série, avec par exemple la publication d'un cinquième ouvrage dédié justement à la « vulgarisation » de ces « nouvelles » méthodes et « nouveaux » outils d'automatisation.

Introduction

Ce livre fait suite au tome 1 intitulé, *Réseaux de terrain : description et critères de choix*, Hermès, Paris, 1999, publié à l'initiative du groupe CIAME. Le groupe CIAME était à cette époque une association, le CIAME/APIST (Comité Interprofessionnel pour l'Automatisation et la Mesure/Association pour la Promotion de l'Instrumentation Scientifique et Technique) qui avait repris le flambeau des travaux menés au sein de la CIAME (Commission Industrie-Administration pour la MESure) à partir de 1990. Les travaux menés à cette époque au sein des groupes de travail CIAME ont conduit à la publication de deux ouvrages de synthèse :

- M. Robert, M. Marchandiaux, M. Porte, *Capteurs intelligents et méthodologie d'évaluation*, Hermès, Paris, 1993 ;
- M. Staroswiecki, M. Bayart, *Actionneurs intelligents*, Hermès, Paris, 1994.

Depuis 2000, le CIAME est devenu Constituants Intelligents pour l'Automatisation et la MESure, groupe de travail 18-04 de la SEE (Société de l'Electricité, de l'Electronique, et des Technologies de l'Information et de la Communication).

Réseaux de terrain : description et critères de choix présentait les spécifications des réseaux de terrain les plus répandus et identifiait les principaux domaines d'applications afin d'aider le concepteur de système d'automatisation distribué au moment du choix.

Les réseaux de terrain ont été développés principalement durant les années 1980 et améliorés durant la décennie suivante. Sans reprendre en détail tous les aspects historiques qui sont évoqués dans le chapitre 4 du précédent ouvrage, nous pouvons rappeler que les principaux réseaux de terrain ont été développés, à l'initiative de constructeurs, dans le cadre de *consortia* regroupant les constructeurs, les utilisateurs et les chercheurs. Dès l'origine s'est posé le problème de l'interopérabilité, de l'interchangeabilité, les utilisateurs souhaitant pouvoir faire évoluer leur(s) installation(s) en fonction de leurs besoins. Les constructeurs, ayant plutôt tendance à privilégier la fidélisation de leur clientèle, ne favorisaient pas trop l'ouverture de leur(s) système(s).

Tous ces aspects ont finalement abouti à la norme IEC 61158 sur les communications de données numériques pour la mesure et le contrôle, les réseaux de terrain utilisés dans les systèmes de contrôle industriels (*Digital data communications for measurement and control - Fieldbus for use in industrial control systems*) [PEY 00] [Std 61158]¹. Cette norme est un catalogue de plusieurs milliers de pages qui est en fait la concaténation des spécifications des réseaux de terrain les plus connus : TS61158, ControlNet, Profibus, P-Net, Foundation Fieldbus, SwiftNet, WorldFIP, et Interbus.

Aujourd'hui, de manière plus aiguë encore qu'auparavant, notamment à cause de l'évolution de la normalisation, se pose le problème de la sûreté de fonctionnement. Le développement conjoint de la technologie (électronique numérique, réseaux de communication) et des besoins des utilisateurs (supervision, suivi, maintenance, etc.) a entraîné des difficultés inhérentes à l'évaluation de la sûreté de fonctionnement de ces systèmes complexes. Les méthodes classiques d'évaluation, en effet relativement bien adaptées aux systèmes mécaniques ou électroniques analogiques, s'appliquent plus difficilement aux systèmes numériques, en particulier lorsqu'il s'agit de systèmes pilotés ou commandés autour de réseaux de communication. Mais en contrepartie, les nouvelles technologies numériques ont ouvert la porte à la mise en place d'outils de supervision, d'enregistrements d'historiques, de maintenance prévisionnelle, qui permettent d'envisager une meilleure utilisation des outils de production et apportent des informations en temps réel sur l'évolution de paramètres de sûreté de fonctionnement.

Cet ouvrage souhaite apporter une aide aux concepteurs de systèmes d'automatisation à intelligence distribuée, en proposant une analyse approfondie de la fonction « communication » avec une vision « sûreté de fonctionnement » et/ou « sécurité ».

1. Dans l'ouvrage, les références bibliographiques sont listées en fin d'ouvrage et référencées dans le corps du texte de la manière suivante : [PEY 00]. Les normes sont listées dans une annexe distincte et référencées sous la forme [Std 61508].

Le chapitre 1 pose le problème et précise le contexte en rappelant l'évolution parallèle des besoins des utilisateurs et des nouvelles technologies. Cette partie décrit les développements, tant dans la recherche universitaire que dans le domaine industriel, d'une part des concepts d'« instruments intelligents » et leurs intégrations et d'autre part la généralisation des réseaux de communication, et plus particulièrement des réseaux de terrain.

Le chapitre 2 présente les concepts usuels de sûreté de fonctionnement, tels qu'ils sont utilisés par les spécialistes, ainsi qu'un tableau comparatif des principales méthodes de sûreté de fonctionnement avec leurs domaines d'application.

Le chapitre 3 pose le problème de la conception de systèmes d'automatisation à intelligence distribuée (SAID). Diverses méthodes de conception sont présentées. La conception d'un système d'automatisation, architecturé autour d'un ou plusieurs réseau(x) de communication, se doit d'être « intégrée » et envisagée dans une vision globale afin de ne pas oublier de paramètres, notamment dans les interfaces entre les sous-ensembles du système d'automatisation et de son environnement (y compris le processus piloté ou commandé) ou entre les corps de métier ou spécialisations.

Le chapitre 4 se focalise plus précisément sur le réseau, autrement dit la fonction ou le service de communication, tel qu'il doit être assuré au sein du SAID. Différents réseaux sont présentés et sont classés en fonction de leurs caractéristiques au regard de la sûreté de fonctionnement. Ainsi, des aspects liés au déterminisme, aux propriétés temps réel et à la cohérence temporelle sont abordés, mais également des aspects plus liés à la couche physique, tels que la robustesse aux perturbations électromagnétiques ou aux coupures accidentelles.

Le chapitre 5 entre dans le détail de quelques réseaux de terrain couramment utilisés dans l'industrie, en reprenant les spécifications de ces réseaux selon une démarche proche de celle adoptée pour le tome 1 *Réseaux de terrain : description et critères de choix* du CIAME. Il donne une analyse « critique » de leurs propriétés et spécifications en regard de critères de sûreté de fonctionnement.

Dans le chapitre 6, quelques domaines d'application sont envisagés afin d'avoir une vision pragmatique des besoins des utilisateurs. La problématique de la sécurité des machines, telle qu'elle est notamment envisagée par la normalisation, est présentée. L'utilisation des réseaux de terrain dans les matériels ferroviaires est ensuite abordée, toujours en regard de la normalisation en cours. Un dernier domaine applicatif concerne la domotique.

Le chapitre 7 ouvre une porte vers le futur (très proche ou plus lointain) en envisageant tout d'abord l'utilisation des réseaux de terrain dans des applications de sécurité (applications critiques ou applications dédiées à la sécurité). Sont ici

abordées les descriptions de quelques réseaux de sécurité existant sur le marché. Parmi les évolutions attendues, les réseaux sans fil commencent à être de plus en plus présents dans les systèmes tels que ceux qui nous préoccupent. Finalement, une ouverture sera donnée vers l'ethernet, ce réseau par définition interopérable et très répandu, mais non déterministe, afin de voir quelle est son utilisation aujourd'hui dans des problématiques industrielles et dans quelle mesure ce réseau pourrait jouer un rôle, dans le futur, dans des applications de sécurité.