

Le présent fichier PDF **Sommaire** reproduit des extraits du document

Identification radiofréquence et cartes à puce sans contact

Description

RFID

L'auteur est Dominique Paret

Edité par Dunod en 2001

Cet ouvrage est disponible sous le numéro **AC 26786** dans l'inventaire de la collection de l'ACONIT, Association pour un conservatoire de l'informatique et de la télématique, Grenoble.

Il comprend 313 pages, structurées en 5 parties, avec de nombreux schémas, et des descriptions de normes. Depuis la date d'édition de cet ouvrage ces normes ont évolué, afin d'inclure de nouvelles situations.

Cet ouvrage montre comment les dispositifs RFID peuvent être utilisés.

Les extraits fournis dans le présent PDF donnent en copie :

- Les pages de couverture,
- La page d'Avant-Propos,
- Les 11 pages de la Table des Matières,
- Les 7 pages de l'Introduction,
- Les 3 pages de liste des normes de l'annexe-2.

Pour utiliser ce document, mentionnez l'auteur et Dunod, ainsi que la Base de Données ACONIT n° 26786.

Il est rappelé que la loi sur les droits d'auteur n'autorise que les reproductions partielles de documents à titre individuel et pour des motifs de recherche.

Dominique Paret

Identification radiofréquence et cartes à puce sans contact

Description

RFID



DUNOD

Collection EEA
Série Technologie électronique



Dominique Paret

IDENTIFICATION RADIOFRÉQUENCE ET CARTES À PUCE SANS CONTACT

Description

L'identification sans contact est en pleine effervescence. Qu'il s'appuie sur une liaison optique, infrarouge, hyperfréquence ou plus fréquemment sur une liaison radiofréquence, le « sans contact » est appelé à un avenir rayonnant. Badges d'accès, cartes bancaires, télépaiement, identification de bagages, identification de livres en bibliothèque, localisation de matériels en magasin, suivi du stock en rayon et changement de prix à distance, voilà un petit échantillon de ce que le « sans contact » autorise.

Le but de ce premier ouvrage sur le sujet – le second étant dédié aux applications – est d'offrir un panorama le plus complet possible concernant ce domaine d'activité. Il s'agit donc d'une dense introduction technique où tous les aspects du « sans contact » sont étudiés et décortiqués par un des plus grands experts actuels sur le sujet.

Table des matières :

- Notion de communication sans contact
- Marché et champs d'applications du « sans contact »
- Principes généraux du « sans contact »
- Examen technique détaillé et choix des solutions techniques en fonction des applications
- Identification simple et identification multiple
- Sécurité de la communication
- Le transpondeur et la *base station*
- Les composants électroniques
- Les normes
- Annexes (lexique, liste des normes, adresses utiles)

DOMINIQUE PARET
Ingénieur innovation et systèmes, et responsable du support technique Identification et Automobile chez Philips Semiconductors, il enseigne à l'ESIEE, l'ESISAR, l'EFREI et l'ESEO. Il est l'auteur chez Dunod d'ouvrages tels que *Le bus CAN* en deux volumes et *Le bus I2C*.



ISBN 2-10-004263-7
Code 044263

<http://www.dunod.com>



A VANT-PROPOS

À ce jour, l'identification sans contact est un thème en pleine effervescence. Travaillant dans ce domaine depuis de nombreuses années, nous ne pouvions manquer de « communiquer » sur ce sujet. En effet, à ce jour, peu d'informations, de formations et de techniques de bases et applicatives sont disponibles pour les ingénieurs, techniciens et étudiants. Nous espérons que cet ouvrage comblera au moins partiellement ce manque.

Le but de cet ouvrage est donc d'offrir, à une date donnée, le b.a.-ba le plus complet concernant ce domaine d'activité. Ce livre ne se veut donc pas encyclopédique mais une longue et dense introduction technique à ce sujet. Il est dense dans le sens où tous les « vrais » sujets des applications « sans contact » (principes, anti-collision, sécurité, composants, normes, applications, etc.) sont abordés concrètement.

Par ailleurs, au niveau pédagogique, au lieu de bloquer toutes les théories et équations dans un chapitre spécifique et de risquer ainsi une indigestion, nous avons décidé de saupoudrer celles-ci tout au long de l'exposé des chapitres, de façon à ce que le lecteur puisse faire le point à tout instant entre théorie et aspects technologiques, économiques, etc.

Nous vous souhaitons maintenant une bonne lecture... et nous espérons rester « en contact » avec vous tout au long des pages de cet ouvrage!

NOTE TRÈS IMPORTANTE

Dès à présent, nous désirons attirer l'attention des lecteurs sur le fait important que, pour couvrir correctement le sujet du « sans contact », cet ouvrage décrit de très nombreux principes techniques brevetés, soumis à exploitation de licences, leurs droits associés (codages bit, techniques de modulation, dispositifs d'anticollision, etc.), qui ont déjà été publiés au sein de textes/communications techniques professionnelles officielles ou lors de conférences/séminaires publics... mais surtout, dont l'usage doit être fait selon les règles légales en vigueur.



TABLE DES MATIÈRES

PARTIE 1

LA GENÈSE

CHAPITRE 1 - INTRODUCTION	3
1.1 À quoi et à qui ça sert?	3
1.2 Historique	4
1.3 L'identification électronique et ses ramifications	5
1.3.1 Identification à contact	5
Circuits « mémoire » et associés	5
Carte à puces	5
1.3.2 Identification sans contact (<i>contactless</i>)	5
Vision optique	5
Liaison radiofréquence	6
Liaison en hyperfréquence	6
Liaison infrarouge	7
1.3.3 Dispositifs passifs ou actifs	7
Dispositifs passifs	7
Dispositifs actifs	7
1.4 Les nombreuses appellations	8
1.4.1 L'élément déporté	8
1.4.2 L'élément fixe	9



CHAPITRE 2 - NOTION DE COMMUNICATION SANS CONTACT	11
2.1 Notion de distance de communication sans contact	11
2.1.1 Très courte distance, ou encore, du « sans contact » au « contact »	11
2.1.2 Courte distance	12
2.1.3 Proximité (<i>proximity</i>)	12
2.1.4 Voisinage (<i>vicinity</i>)	12
2.1.5 Longue distance	12
2.1.6 Très longue distance	12
2.2 Notion d'alimentation	13
2.2.1 Téléalimentation	13
2.2.2 Alimentation par batterie	13
<i>Sans dispositif de recharge</i>	13
<i>Avec dispositif de recharge</i>	13
2.3 Notion de mode de fonctionnement	14
2.3.1 Les différentes familles de transpondeurs classées selon leur mode de fonctionnement	14
<i>Lecture seule</i>	14
<i>Lectures et écritures multiples</i>	14
<i>Lecture et écriture protégées</i>	15
<i>Lecture et écriture sécurisées</i>	16
<i>Lecture et écriture cryptées</i>	16
<i>Lecture et écriture d'un transpondeur unique présent dans le champ magnétique</i>	16
<i>Lecture et écriture de transpondeurs multiples dans le champ magnétique</i>	16
2.3.2 Déclenchement de l'échange entre <i>base station</i> et transpondeur	17
<i>Tag Talks First (TTF) et Answer To Reset (ATR)</i>	17
<i>Reader Talks First (RTF) et Answer To Request (ATQ)</i>	17
<i>Coexistence TTF et RTF</i>	18
2.4 Communication et modèle de communication	18
2.4.1 Communication	18
<i>Message à transmettre</i>	19
<i>Transmission</i>	19
<i>Mode de transmission</i>	19
<i>Usage du message</i>	19
2.4.2 Le modèle ISO/OSI	19

CHAPITRE 3 - MARCHÉ ET CHAMPS D'APPLICATIONS DU SANS CONTACT	21
3.1 Le marché du « sans contact »	21
3.1.1 Segment des RFID industriels	21
3.1.2 Segment des immobiliseurs	21
3.1.3 Segment des cartes à puces sans contact	22
3.1.4 Segment de l'étiquetage « intelligent » ou « communicant » – le <i>labelling</i>	22
3.2 Les diverses applications des transpondeurs	24
À 125 kHz	24
À 13,56 MHz	25
À 443, 886 et 9xx MHz	28
À 2,45 et 5,8 GHz	28
En IR	29
3.3 Acteurs et participants du marché	29
3.3.1 Principaux fabricants de transpondeurs et de matériels	30
Fabricants et fondeurs de silicium de transpondeurs et de bases stations	30
Antennes	30
Encarteurs ou « encapsuleurs »	30
Intégrateurs de systèmes	31
Cabinets d'engineering	31
3.3.2 Prescripteurs	31
3.3.3 Utilisateurs	31

PARTIE 2

LES PRINCIPES TECHNIQUES

CHAPITRE 4 - PRINCIPES GÉNÉRAUX DU « SANS CONTACT »	35
4.1 Présentation du fonctionnement général de l'ensemble	35
4.1.1 Le transpondeur	35
4.1.2 L'air	35
4.1.3 La <i>base station</i>	36
4.1.4 Le système <i>host</i>	36
4.2 Principes généraux de fonctionnement du couple <i>base station/transpondeur</i>	37
4.2.1 Transfert d'énergie	37
Remarque 1	40
Remarque 2	42
Remarque 3	45

4.2.2	Communication entre <i>base station</i> et transpondeur	46
	<i>Liaison montante</i>	47
	<i>Liaison descendante</i>	48
4.2.3	Dualité transfert d'énergie/communication	50
4.2.4	Remarques concernant les <i>bases stations</i> /transpondeurs en mouvements relatifs	50
4.2.5	Annexe : rappels et compléments concernant la liaison électromagnétique RF	51
	<i>Les circuits à couplage magnétique</i>	51
	<i>Mutuelle</i>	51
	<i>Coefficient de couplage k</i>	53
	CHAPITRE 5 - EXAMEN TECHNIQUE DÉTAILLÉ DES DIFFÉRENTES PARTIES ET CHOIX DES SOLUTIONS TECHNIQUES À EMPLOYER EN FONCTION DES APPLICATIONS	65
5.1	Principes et problèmes généraux de fonctionnement de la transmission de données	67
5.1.1	Selon les applications visées	67
	<i>Topologie de l'application</i>	67
	<i>Temps de transaction</i>	67
5.1.2	Tailles des mémoires	69
5.1.3	Débits numériques choisis ou nécessaires	70
5.2	Problèmes spécifiques des systèmes « longue distance »	70
5.2.1	Spécificités du marché longue distance	70
5.2.2	Paramètres clés des systèmes longue distance	71
	<i>Lecture en volume</i>	71
5.3	Transfert d'énergie et échange de données	71
5.4	Modes de transfert d'énergie et de communication	73
5.4.1	Modes de transfert d'énergie	73
	<i>Non simultané, énergie et communication en deux temps</i>	73
	<i>Simultané, énergie et communication en un seul échange</i>	73
5.4.2	Modes de communication	73
	<i>Half duplex</i>	73
	<i>Full duplex</i>	73
5.5	Aspects numériques de la communication	74
5.5.1	Codage bit	74
	<i>Codage bit à distinguer selon les phases de fonctionnement</i>	74
5.5.2	Les différents types de codage bit utilisables pour le sans contact	76
	<i>No Return to Zero (NRZ) et No Return to Zero Inverted (NRZI)</i>	76
	<i>Return to Zero (RZ) et Return to Zero Inverted (RZI)</i>	77
	<i>RZI coded pulse</i>	78

	Differential Biphase Coding (DBP), biphase différentiel et Conditioned Diphas Procedure (CDP)	80
	AC code	82
	Miller	83
	Miller modifié (MM)	83
	Manchester	86
	Manchester codé sous-porteuse – Manchester Sub-Carrier (MSC)	88
	Miller modifié codé sous-porteuse	91
	Binary Phase Shift Keying (BPSK)	92
	Frequency Shift Keying (FSK)	93
	Differential Frequency Shift Keying (DFSK)	95
	Binary Pulse Length Modulation (BPLM) ou codage de largeur ou de répétition	96
	Codage de position par nombre d'impulsions	96
	Codages par modulation de position d'impulsion – Pulse Position Modulation (PPM)	98
5.5.3	Résumé des différents codages bit	103
	Performances attendues du codage bit d'une liaison montante	105
	Performances attendues du codage bit d'une liaison descendante	105
5.6	Aspects analogiques de la communication	106
5.6.1	Valeur de la fréquence porteuse et type de modulation	106
	Les fréquences possibles et permises	106
	Choix des types de modulation de porteuse	106
	Les normes et les niveaux à respecter	108
	Incidence type de modulation/codage/bit/débit/normes	108
5.6.2	Types de modulation de porteuse pour la liaison montante base station vers transpondeur	108
	Modulation ASK – Amplitude Shift Keying	109
	Modulation FSK (Frequency Shift Keying), PSK (Phase Shift Keying) et BPSK (Binary Phase Shift Keying)	116
	Modulation par étalement de spectre et saut de fréquence – DSSS et FHSS	116
5.7	La communication	117
5.7.1	Protocole de communication	117
	Débit binaire brut et net du protocole	117
	Représentation de l'échange	118
5.7.2	Gestion du protocole de communication	119
	Problème du temps de retournement émission vers réception de la base station	119
	Problème de temps de cryptage et décryptage	120
	Problème du faible rapport S/N du signal provenant du transpondeur	120

5.8	Relations, imbrications, performances dues au choix des codages bit et aux types de modulation utilisés	121
5.8.1	Répercussions du choix des codages bit et types de modulation	121
5.8.2	Liaison montante	122
	<i>Efficience de la source énergie et efficacité énergétique</i>	122
	<i>Fiabilité de la communication, immunité au bruit, rapport signal à bruit et détection du signal incident</i>	125
5.8.3	Liaison descendante	129
	<i>Efficacité énergétique du codage bit</i>	129
5.8.4	En conclusion des codages bit et types de modulations	130
	<i>En liaison montante, de la base station vers le transpondeur</i>	130
	<i>En liaison descendante, du transpondeur vers la base station</i>	130
5.9	Conclusion générale du chapitre	131

PARTIE 3

ÇA SE COMPLIQUE !

CHAPITRE 6 - IDENTIFICATION SIMPLE ET MULTIPLE		135
6.1	Numéro unique	135
6.1.1	Intérêt d'un numéro unique	135
6.1.2	Sur combien de bits	136
6.1.3	Unique, vous avez dit unique	137
6.2	Anticollision et sélection	137
6.2.1	Origine des collisions	138
	<i>Les systèmes courtes distances</i>	138
	<i>Les systèmes longues distances</i>	139
	<i>Weak collisions</i>	139
6.2.2	Quelques grands principes de gestion des collisions	141
	<i>« Yaka » !</i>	141
	<i>Réalité des choses</i>	142
6.2.3	Les différentes méthodes possibles de gestion des collisions	146
	<i>Méthodes déterministes</i>	146
	<i>Méthodes probabilistes</i>	146
	<i>Autres méthodes</i>	146
	<i>États logiques et commandes principales intervenant dans une procédure d'anticollision</i>	147

6.3	Méthode déterministe de gestion des collisions	148
6.3.1	Principe	148
6.3.2	Exemple de gestion déterministe des collisions	148
	<i>Fonctionnement de l'algorithme</i>	149
	<i>Conclusion</i>	158
6.4	Méthode probabiliste de gestion des collisions	160
6.4.1	Principe de la technologie du <i>time slot</i>	160
	<i>Technique de la hashvalue (valeur de hachage)</i>	161
	<i>Sélection du transpondeur</i>	162
	<i>Optimisation du nombre de transpondeurs détectables et du nombre de time slots</i>	162
6.4.2	Exemple de gestion probabiliste des collisions	163
	<i>Principe de fonctionnement</i>	163
	<i>Commande de requête REQ_B</i>	165
	<i>Réponse à la requête (ATQ_B pour Answer To reQuest)</i>	168
	<i>Constitution du message de Time slot marker</i>	168
	<i>Structure du message ATQ_B</i>	169
	<i>Commande d'attribution</i>	170
6.5	Autres principes de singularisation de transpondeurs	171
CHAPITRE 7 - SÉCURITÉ DE LA COMMUNICATION		173
7.1	Les aspects sécuritaires et les attaques	173
7.1.1	Notion de cible de sécurité	173
7.1.2	Notion d'attaques	173
7.2	Authentification	175
7.2.1	Principe de l'authentification	175
7.2.2	Quelques exemples de méthodes d'authentification	176
	<i>Challenge</i>	176
	<i>Authentification mutuelle</i>	178
	<i>Comparaison challenge/authentification mutuelle</i>	180
7.3	Sécurisation d'accès, de transmission et de secret de la transmission	180
7.3.1	Sécurisation de l'accès aux informations	181
	<i>Le mot de passe, ses qualités, ses limites</i>	181
	<i>Les codes évolutifs ou encore codes tournants</i>	183
7.3.2	Sécurisation de la transmission	184
7.3.3	Secret du contenu de la transmission	185
	<i>Cryptographie</i>	185

PARTIE 4

LES TECHNOLOGIES

CHAPITRE 8 - LE TRANSPONDEUR ET LA BASE STATION	189
8.1 Le transpondeur	189
8.1.1 Le concept du transpondeur	189
8.1.2 Zone mémoire	190
<i>Zone de l'identificateur</i>	191
<i>Zone mémoire (des registres) de configuration</i>	191
<i>Zone mémoire de password</i>	193
<i>Zone mémoire réellement utilisateur (user)</i>	194
<i>Nombre de cycles effacement/écriture de la mémoire</i>	194
8.1.3 Logique de contrôle	195
8.1.4 Réception du signal montant et de l'énergie d'alimentation	195
<i>Récupération d'énergie</i>	196
<i>Récupération d'horloge (ou non)</i>	196
8.1.5 Antenne du transpondeur	198
8.1.6 Consommation minimale et maximale d'un transpondeur	198
8.2 Les bases stations	199
8.2.1 Généralités	199
8.2.2 La partie analogique de la base station	201
<i>Émission</i>	202
<i>Réception</i>	205
8.2.3 Partie numérique de la base station	215
CHAPITRE 9 - LES COMPOSANTS ÉLECTRONIQUES	219
9.1 Le transpondeur	219
9.1.1 Dimension des cristaux	219
9.1.2 Les différentes possibilités de conception	220
9.1.3 Les différentes possibilités de conditionnement	221
9.1.4 Les familles de composants disponibles sur le marché	223
<i>Stratégie</i>	224
<i>Fonctionnalités</i>	225
9.2 Les produits existants	227
<i>Spécification générale d'un produit</i>	227
<i>Examen d'une data sheet particulière</i>	227

9.3	La <i>base station</i>	228
9.3.1	Dimension de la <i>base station</i>	228
9.3.2	Les différentes possibilités de conception	228
9.3.3	Les différentes possibilités de conditionnement	230
9.3.4	Les composants disponibles sur le marché	230
	Stratégie	230
	Les produits existants	231
9.3.5	Spécification générale d'un produit « <i>base station</i> »	231
	Examen d'une data sheet particulière	231

PARTIE 5

LES NORMES

CHAPITRE 10 - LES NORMES	235
10.1 Pourquoi des normes internationales?	235
10.1.1 Le but des normes	235
10.1.2 Les demandeurs et protagonistes des normes	235
10.2 Les modèles ISO/OSI en couches	236
10.2.1 L'architecture des couches	236
<i>Couche 0 – Médium</i>	236
<i>Couche 1 – Physique (PL pour Physical Layer)</i>	237
<i>Couche 2 – Liaison de données (DLL pour Data Link Layer)</i>	238
<i>Remarques concernant les couches 1 et 2 :</i>	239
<i>Couche 3 – Réseau</i>	239
<i>Couche 4 – Transport</i>	240
<i>Couche 5 – Session</i>	240
<i>Couche 6 – Présentation</i>	241
<i>Couche 7 – Application</i>	242
10.3 Les normes ISO du « sans contact »	243
10.3.1 En sans contact, qui fait quoi?	243
10.3.2 Le grand distinguo des applications à cartes et non à cartes	245
<i>JTC 1/SC 17</i>	245
<i>JTC 1/SC 31</i>	246
<i>JTC 23/SC 19</i>	246
10.3.3 La hiérarchie des couches	246

10.3.4	La famille de normes ISO 14 443-x pour les cartes sans contact de proximité	247
	14 443 Part 1	248
	14 443 Part 2	248
	14 443 Part 3	255
	14 443 Part 4	255
	Annexe 1 – Comparaison entre les techniques A et B de la norme ISO 14 443 pour les applications cartes à puces sans contact de proximité	256
	Annexe 2 – Résumé des principales différences entre les parties A et B de la norme ISO 14 443	260
10.3.5	La famille de normes ISO/IEC 15 693-x pour les cartes sans contact de « voisinage »	263
	15 693 Part 1	263
	15 693 Part 2	264
	15 693 Part 3	272
10.3.6	Les familles de normes ISO 15 963-x et ISO 18 000-x pour l'identification sans contact industrielle	273
	Famille ISO 15 963-x	275
	Famille ISO 18 000-x	275
10.3.7	Les normes ISO 11 784, 11 785 et 14 223 spécifiques à l'identification animale	276
	ISO 11 784	276
	ISO 11 785	276
	ISO 14 223-x	277
10.4	Les relations avec d'autres normes	278
10.4.1	Normes de rayonnement et pollution RF	279
	États des normes	279
	Comment satisfaire les normes	285
	Une dernière remarque	287
	Remarques spécifiques concernant l'usage des fréquences UHF et SHF	288
10.4.2	Normes de sécurité relatives aux champs magnétiques et électriques dans un environnement humain (<i>human exposure</i>)	290
	Problème européen et international	290
	MPE et SAR	291
CONCLUSIONS		293
La suite		294
Rêvons un peu		295

ANNEXE 1 - PETIT VOCABULAIRE ET LEXIQUE SPÉCIFIQUES AUX NORMES DU « SANS CONTACT »	297
ANNEXE 2 - LISTE DES NORMES ISO/IEC ET ETSI LES PLUS COURANTES	299
ANNEXE 3 - LES BONNES ADRESSES	303
Organismes de normalisation et assimilés	303
Manifestations de la profession	304
<i>Salons et expositions</i>	304
<i>Conférences</i>	304
Liste de matériels, équipements et des fabricants de composants	305
<i>Appareils de mesure et de tests spécialisés</i>	305
<i>Logiciels d'aide au développement</i>	305
<i>Outils de développement</i>	306
<i>Kits de démonstration</i>	306
<i>Fabricants de composants</i>	306
Les revues professionnelles parlant de la RFID	306
Autres ouvrages complémentaires	307
INDEX	309

NTRODUCTION

Les termes génériques du titre de cet ouvrage – identification radiofréquence et cartes à puces sans contact – couvrent de très nombreux domaines et sujets, variés et controversés.

En effet, autant le mot « identification » fait plaisir à entendre à un industriel qui doit assurer le suivi de sa production ainsi que la traçabilité (*tracking*) de ses produits, autant le même mot évoque des craintes potentielles d'atteinte aux libertés individuelles des personnes. De même, le côté « étiquette » évoque lui aussi de grands bénéfices et des facilités d'utilisation pour des passages rapides en caisse de grandes surfaces, de souplesse pour effectuer des inventaires, de confort pour des réapprovisionnements industriels et domestiques, des ouvertures pour mieux assurer la sécurité contre des contrefaçons et marchés parallèles... mais les monstres d'études marketing encore plus fines qu'aujourd'hui se profilent derrière un achat quelconque.

Les « cartes à puces » sont elles aussi dans l'œil du cyclone. Quel plaisir en circulant sur notre planète que de savoir que l'on peut utiliser journalièrement nos cartes à puces pour valider avec un très bon niveau de sécurité le débit de nos achats ou encore effectuer des retraits de monnaie... comme DAB! Ceci amène naturellement à évoquer l'utilisation dans un futur proche du porte-monnaie électronique comportant à son bord de la vraie monnaie électronique, ouvrant ainsi la porte à toutes les convoitises d'hypothétiques émissions de fausse monnaie, aux problèmes d'éthique, et ici aussi, à la sacro-sainte pièce de liberté individuelle que constitue le billet ordinaire.

Voici donc introduit en quelques mots ce vaste monde fabuleux, très intéressant et contradictoire dans lequel, uniquement sous son aspect technique, « de la théorie à la pratique », cet ouvrage a pour but de vous entraîner.

1.1 À quoi et à qui ça sert ?

Jusqu'à ce jour, l'identification d'objets et de personnes était pratiquement toujours réalisée sur du support papier, carton, etc., à l'aide de codes écrits,

imprimés. Le traitement des données nécessitait soit le contact (pour l'écriture), soit la visibilité directe (pour la lecture) de l'identifiant.

Depuis quelques années, les liaisons radiofréquence et les composants électroniques associés devenant de plus en plus performants, la recherche et le développement se sont orientés vers la possibilité de remplacer et d'améliorer ces anciennes techniques d'identification par des techniques dites *Radio Frequency Identification* (RFID) ou encore *Contactless Identification* (identification sans contact).

Pendant de longues années, ces nouvelles techniques se sont trouvées limitées par l'impossibilité de réaliser la téléalimentation de l'identifiant, du fait principalement de sa consommation qui imposait la présence d'une alimentation locale (pile, accumulateur). Depuis, les technologies des circuits intégrés ayant fait d'immenses progrès, le rêve du vrai « sans contact » est devenu réalité.

Au cours des prochains paragraphes, nous allons examiner en détail à quoi (les applications) et à qui (le marché) ça sert.

1.2 Historique

Voici bien des années que l'identification existe sous de nombreuses formes. Si nous nous intéressons uniquement aux dernières décennies, il est évident que l'étiquetage permettant d'identifier de nombreux articles a « explosé » avec l'apparition des étiquettes papier codes barres et de leurs lecteurs associés.

Parallèlement, de nombreuses expériences et applications industrielles utilisant les étiquettes électroniques ont vu le jour, principalement dans les suivis de processus industriels et d'identification animale (ovins, bovins, domestiques, etc.) à l'aide d'implants. Aujourd'hui, cette notion d'étiquettes électroniques est en train de dépasser son cadre industriel pour s'aventurer vers de véritables identifications de haut niveau embarquant à leurs bords, à chaque fois que cela est nécessaire, tous les dispositifs de confidentialité et de secret que cela implique.

Depuis de nombreuses années, ces sujets pointus sont à l'étude et l'on peut dire que leur aboutissement de masse est imminent. En effet, beaucoup d'expériences et de projets voient actuellement le jour concrètement. Le projet industriel commercialement le plus évident lors des dernières années (en terme de composants fabriqués) est celui des applications aux dispositifs dits « d'antidémarrage électronique » pour les véhicules automobiles (plus de 200 millions de pièces installées en quelques années), fonctionnant sous ce principe de « sans contact » sécurisé... et pourtant Dieu sait si le marché automobile est difficile à satisfaire!

Cela a évidemment donné des idées aux utilisateurs de dispositifs « à contact », notamment aux utilisateurs de cartes à puces classiques rêvant de pouvoir enfin retirer ce fâcheux cordon ombilical qu'est une liaison/contact filaire.

1.3 L'identification électronique et ses ramifications

Au stade où nous en sommes, nous pouvons dès à présent diviser la branche de l'identification électronique en deux ramifications : celle de l'identification électronique « à contact » et celle de l'identification électronique « sans contact » (RFID).

1.3.1 Identification à contact

Ce type d'identification s'effectue à l'aide de dispositifs pour lesquels la communication est assurée par des contacts électriques. Citons deux exemples caractéristiques : les circuits « mémoire » et associés et les cartes à puces.

Circuits « mémoire » et associés

Des circuits, plus ou moins évolués, comportant des fonctions mémoire sont disposés sur des modules de formes mécaniques variées et dont l'une des classes majeures possède le format bien connu des cartes à puces conventionnelles. On peut citer aisément de nombreuses applications réalisées à l'aide de mémoires E2PROM, communiquant par exemple selon le protocole I2C bien connu (soit 4 connexions, le + 5V, la masse, et les deux fils de *Clock*, CLK, et de données, SDA), ainsi que certaines applications utilisant des circuits intégrés spécifiques (de la société Dallas par exemple), n'ayant besoin que de 2 contacts (une masse et un fil actif).

Carte à puces

La grande famille des cartes à puces possède des applications plus que variées orientées principalement autour de contrôles/conditions d'accès, d'applications bancaires, de débit de monnaie, etc., donc fondamentalement personnelles et identifiant l'utilisateur final.

1.3.2 Identification sans contact (*contactless*)

La branche de l'identification sans contact peut se décomposer en différentes sous-branches, dont les principales sont : la vision optique, la liaison radiofréquence, la liaison en hyperfréquence et la liaison infrarouge.

Vision optique

Cette vision nécessite la présence d'un détecteur fonctionnant en vision directe de l'identifiant à l'aide soit d'un œil humain, soit d'un lecteur (laser, etc.), soit encore d'une caméra CCD. L'exemple le plus largement répandu est celui des étiquettes imprimées standard ou encore de type codes à barres et codes 2D.

Le plus grand problème (si cela en est un) de ces systèmes réside dans le fait que la lecture doit être obligatoirement effectuée en vision directe et qu'elle est fortement soumise à la propreté intrinsèque de l'étiquette (tache, déchirure, etc.). Un deuxième problème est généralement soulevé par l'impossibilité d'actualiser aisément cette étiquette, sauf bien sûr en effectuant son remplacement pur et simple.

Ceci étant, il ne faut surtout pas oublier leur plus grand avantage qui est leur très faible coût !

Liaison radiofréquence

Le fait d'envisager une communication de type radiofréquence entre « identifiants » et « lecteurs » permet d'une part de rendre possibles des lectures à des distances plus importantes (non liées au pouvoir séparateur de l'œil de l'être humain ou à celui du lecteur optoélectronique) et d'autre part de ne pas nécessiter la vision physique, optique, directe de l'identifiant. Ces possibilités permettent aussi d'envisager des lectures « en volume », c'est-à-dire de traiter la présence simultanée de plusieurs identifiants dans le champ radiofréquence du lecteur, sans nécessairement les voir de façon optique. L'électronique aidant, ceci permet aussi d'envisager des protections, sécurités, etc. des informations présentes sur ou dans l'identifiant, ce qui amène fréquemment à l'élaboration d'identifiants souvent qualifiés de « code-barres intelligent » ou *intelligent labelling*, dont nous parlerons en détail au chapitre 10.

Les fréquences utilisées sous le nom de *radiofréquences* s'étalent de quelques kilohertz à quelques dizaines et centaines de mégahertz (UHF).

Liaison en hyperfréquence

Les fréquences porteuses de fonctionnement de ces dispositifs SHF sont de l'ordre de quelques gigahertz. Les applications les plus courantes se situent à 2,45-5,8 et 24 GHz.

Bien que ces identifiants comportent généralement une pile à leur bord, ces systèmes sont appelés « passifs » car ils n'émettent pas d'ondes électromagnétiques. En effet, pour se faire comprendre de l'émetteur, ces identifiants modulent leur degré/taux de réflexion (on parle d'effet de « miroir ») de l'onde hyperfréquence incidente. La source émettrice recevant aussi l'onde réfléchie devient alors capable de comprendre la modulation engendrée par l'identifiant.

La valeur de cette fréquence porteuse permet d'obtenir des débits de communication élevés et donc des temps de transaction faibles, de l'ordre de la dizaine de millisecondes. Il est alors possible d'identifier, à la volée, des objets se déplaçant rapidement (passages de trains, véhicules automobiles aux stations de péage autoroutiers par exemple, en se rappelant qu'une vitesse de 10 m/s est équivalente à 36 km/h, ou encore que 144 km/h est équivalent à 40 m/s, et qu'alors en 25 ms un véhicule a parcouru 1 m).

Le problème technique bien connu lié à ces applications hyperfréquences réside dans leur quasi-inaptitude à traverser les métaux, les liquides et le corps humain (80 % d'eau!) ainsi que leur assez grande directivité... qui peut être par ailleurs, parfois, une qualité!

Un autre problème des liaisons fonctionnant en hyperfréquence est celui lié à la téléalimentation de l'identifiant car, le fait (bénéfique) de disposer d'antennes de petite taille (donc de petite section) et les longueurs d'ondes associées à la fréquence entraînent une récupération d'énergie très limitée, et imposent généralement la présence d'une alimentation locale.

Liaison infrarouge

De la même façon que les liaisons hyperfréquences, les liaisons optiques de type infrarouge (longueur d'onde aux environs de 800 nm) servent souvent de relais à des dispositifs d'identification sans contact (péage sur autoroute par exemple), afin d'assurer un plus grand débit d'informations et une plus grande directivité du faisceau de communication. Ici aussi, les distances de fonctionnement sont généralement élevées et les transpondeurs sont alimentés de façon autonome.

1.3.3 Dispositifs passifs ou actifs

Toutes les familles de produits que nous venons d'évoquer sont habituellement à nouveau subdivisées en deux classes dites d'identifiants : les dispositifs passifs et les dispositifs actifs.

Dispositifs passifs

Les identifiants dits « passifs » ne comportent pas de source d'alimentation autonome à leurs bords et, pour fonctionner, ils doivent être téléalimentés par de l'énergie (champ magnétique par exemple) produite et fournie par le « lecteur ».

Dispositifs actifs

Les identifiants dits « actifs » comportent à leur bord une source locale d'alimentation indépendante (pile, batterie, accumulateur, etc.), ce qui peut leur donner des possibilités fonctionnelles plus importantes, notamment en ce qui concerne la portée de la communication, mais qui les lie directement à une notion d'autonomie énergétique temporelle (pile, batterie, accumulateur rechargeable...).

REMARQUE

Les dispositifs actifs que nous venons d'évoquer ci-dessus fonctionnent souvent comme des postes classiques de réception et d'émission radio.

Pour terminer ce chapitre de généralités et d'introduction et afin d'éviter une trop grande confusion dans les termes utilisés, nous allons passer rapidement en revue les nombreuses appellations dont sont affublés les composants principaux des applications sans contact.

1.4 Les nombreuses appellations

Notre belle profession n'est pas avare d'appellations en ce qui concerne la terminologie des divers éléments entrant dans les applications « sans contact ».

RFID (*Radio Frequency Identification*) est le terme définissant globalement le système d'identification radiofréquence.

1.4.1 L'élément déporté

Commençons par l'élément déporté. On rencontre fréquemment les termes suivants :

- *Identifiant* est le terme que nous avons utilisé jusqu'à présent pour introduire notre sujet car il était suffisamment parlant... pour l'instant.
- *TAG* provient du mot anglais *tag* qui signifie étiquette, et *to tag* cocher.
- *PIT* : de plus en plus fort ! PIT signifie *Programmable Identification Tag*, soit en français « étiquette programmable » dont le but est d'identifier une « chose ». Si l'on était rigoureux, le TAG, hors abus de langage, ne devrait pas être programmable, seul le PIT l'étant !
- *Data Carrier* est un terme générique qui définit le « porteur de données » dans le sens de celui qui renferme/contient les données, qui est bien évidemment le PIT.
- *Étiquette, label, smart label* : sans commentaire...
- *Transpondeur* : la technologie associée aux applications sans contact s'articule autour d'un dispositif électronique de type TRANSMetteur/réPONDEUR, dit « TRANSPONDEUR », qui est attaché à un objet et qui est capable de répondre à un signal radio émis par un « lecteur ». C'est le terme générique que nous emploierons le plus fréquemment au cours de cet ouvrage.
- *ICC, PICC, VICC* : les écrits de la normalisation ISO se référant aux applications cartes à puces sans contact évoquent fréquemment les termes de ICC, PICC, VICC qui ont pour traduction respective *Integrated Circuit Card*, *Proximity Integrated Circuit Card* et enfin *Vicinity Integrated Circuit Card*. Nous

détaillerons tous ces vocables et leur contenu au cours du chapitre 10 se rapportant aux normes en vigueur.

Passons maintenant de l'autre côté...

1.4.2 L'élément fixe

L'élément fixe, ou considéré comme fixe (en effet ce peut être un pistolet ou une douchette de relevé), porte lui aussi de nombreux noms :

- *Base station* désigne l'ensemble (généralement fixe) des commandes capable de lire, d'écrire, de gérer, etc. le transpondeur à l'aide de radiofréquences.
- *Lecteur/Reader* : fréquemment utilisé, ce terme est sur le principe un peu limitatif car généralement ce « lecteur » est aussi capable d'écrire des données dans le transpondeur. Il serait bon que l'on redonne son sens profond à ce terme afin d'éviter les équivoques entre les lecteurs purs, ceux qui ne savent que lire, et ceux qui sont capables de lire et d'écrire ! Merci d'avance ! Idem pour le terme de *tête de lecture*. Re-merci !
- *Interrogeur* : fréquemment utilisé par nos collègues américains, ce terme se rapproche plus de la réalité car il est vrai que la *base station* passe son temps à donner des ordres et/ou des commandes au transpondeur pour lui indiquer ce qu'il doit effectuer. En demandant à celui-ci de vider/renvoyer son contenu, on peut très bien comprendre que vu de la *base station* cela soit considéré comme une interrogation. Cependant, lorsque la *base station* envoie des données pour qu'elles soient inscrites dans le transpondeur, la *base station* est-elle vraiment un « interrogeur » ?

Passons encore à d'autres termes. Nous vous l'avons dit, nous ne sommes pas avares !

- *Modem* : si l'on est respectueux du terme « MODEM » (*MODulator/DEModulator*), celui-ci ne devrait être utilisé que pour désigner les parties électroniques concernées par les fonctions de modulation et démodulation des signaux des transpondeurs et des *bases stations*.
- *Coupleur CD, PCD, VCD, etc.* : ces termes utilisés par l'ISO font partie des termes les moins faux car ils désignent les *Proximity* et *Vicinity Coupling Device*, c'est-à-dire les éléments servant à assurer le couplage (dans quel(s) sens ?) entre le(s) transpondeur(s) et la (les) base(s) station(s).

RÉSUMÉ

Bref, pour éviter toute confusion, nous utiliserons le plus souvent possible dans cet ouvrage les termes génériques de « transpondeur » et de « *base station* », qui correspondent à notre avis aux termes les plus justes pour définir techniquement ces éléments.

LISTE DES NORMES **ISO/IEC ET ETSI** **LES PLUS COURANTES**

Nous vous proposons ci-dessous la liste des normes ISO/IEC et ETSI les plus couramment utilisées dans le cadre des dispositifs sans contact et principalement pour les *Identification cards*, *Radio Frequency Identification of Animals* et *Item Management*.

ISO/IEC 7811 : *Recording technique*

ISO/IEC 7812 : *Identification of issuers*

ISO/IEC 7812-1 : 1993 : *Part 1 : Numbering system.*

ISO/IEC 7812-2 : 1993 : *Part 2 : Application and registration procedures.*

ISO/IEC 78 13 : *Financial transaction cards.*

ISO/IEC 78 16 : *Integrated circuit(s) cards with contacts*

ISO/IEC 7816-1 : 1987 : *Part 1 : Physical characteristics.*

ISO/IEC 7816-2 : 1988 : *Part 2 : Dimensions and location of the contacts.*

ISO/IEC 7816-3 : 1989 : *Part 3 : Electronic signals and transmission protocols.*

ISO/IEC 10 536 : *Contactless integrated circuit(s) cards – Close coupled cards*

ISO/IEC 10536-1 : 1992 : *Part 1 : Physical characteristics.*

ISO/IEC 10536-2 : 1995 : *Part 2 : Dimensions and location of coupling areas*

ISO/IEC 10536-3 : 1996 : *Part 3 : Electronic signals and reset procedures*

ISO/IEC 10536-4 : 199x : *Part 4 : Answer to reset and transmission protocols*

ISO/IEC 14 443 : *Contactless integrated circuit(s) cards – Proximity cards*

ISO/IEC 14 443-1 *Part 1 : Physical characteristics*

ISO/IEC 14 443-2 *Part 2 : Radio-frequency power and signal interface*

ISO/IEC 14 443-3 *Part 3 : Initialization and anticollision*

ISO/IEC 14 443-4 *Part 4 : Transmission protocols*

ISO/IEC 15 693 : *Contactless integrated circuit(s) cards – Vicinity cards*ISO/IEC 15693-1 : 1999 : *Part 1 : Physical characteristics.*ISO/IEC 15693-2 : 1999 : *Part 2 : Radio frequency power and signal interface*ISO/IEC 15693-3 : 2000 : *Part 3 : Anticollision and Transmission protocols*ISO/IEC 15693-4 : ? : *Part 4 : Registration of application/issuers***ISO/IEC 10 373 : *Test methods***ISO/IEC 10373-1 : 1998 : *Test methods – generalities*ISO/IEC 10373-4 : 199x : *Test methods for contactless close coupling cards
(ISO 10 536-2)*ISO/IEC 10373-6 : 1998 : *Test methods for contactless proximity cards
(ISO 14 443-2)*ISO/IEC 10373-7 : 199x : *Test methods for contactless vicinity cards (ISO 15 693-2)***ISO/IEC 11 78x : *Radio Frequency identification of animals***ISO/IEC 11784 : 1998 : *Radio frequency identification of animals – code structure*ISO/IEC 11785 : 199x : *Radio frequency identification of animals – technical concept***ISO/IEC 14 223-x *Radio Frequency identification of animals***ISO/IEC 14 223-1 Part 1 : *interface par radio fréquence*ISO/IEC 14 223-2 Part 2 : *structure du code de commande (stade préliminaire)*ISO/IEC 14 223-3 Part 3 : *applications (stade préliminaire)***ISO/IEC 18 000-x *RFID for Item Management — Air Interface***ISO/IEC 18 000-1 *Part 1 : generic parameters for Air interface*ISO/IEC 18 000-2 *Part 2 : communications below 135 kHz*ISO/IEC 18 000-3 *Part 3 : communications at 13,56 MHz*ISO/IEC 18 000-4 *Part 4 : communications at 2,45 GHz*ISO/IEC 18 000-5 *Part 5 : communications at 5,8 MHz*ISO/IEC 18 000-6 *Part 6 : communications at UHF***ISO 15 963-x *RFID for Item Management***ISO/IEC 15 963-1 *Part 1 : host interrogator – Tag functional commands and
other syntax features*ISO/IEC 15 963-2 *Part 2 : data syntax*

ISO/IEC 15 963-3 *Part 3 : unique identification of RF tag and registration authority to manage the uniqueness*

ETSI 300 xx0 : *Radio equipment and systems; short range devices*

ETSI 300 330 : *Technical characteristics and test methods – 9 kHz to 25 MHz*

ETSI 300 220 : *Technical characteristics and test methods – 25 MHz to 1 000 MHz*

ETSI 300 440 : *Technical characteristics and test methods – 1 GHz to 25 GHz*

REMARQUE

Pour plus amples informations, nous conseillons aux lecteurs de se mettre en rapport avec l'AFNOR et l'ETSI dont les coordonnées sont données en annexe.
