

SYSTÈME D'INFORMATION ET NUMÉRIQUE

SYSTEME DE SERRURES CONNECTÉES



- **Présentation de l'étude et questionnaire** pages 18 à 20
- **Documents techniques** pages 21 à 24
- **Documents réponses** pages 25 à 27

Dans la partie spécifique, vous devez choisir entre traiter la partie B (choix 1) ou la partie C (choix 2). La partie A est à traiter obligatoirement.

Mise en situation

La rénovation des locaux et des vestiaires a aussi été l'occasion de changer les casiers. Le choix s'est porté sur des casiers informatisés et automatisés, sécurisés par détecteurs anti-effraction, fonctionnant à badge RFID. Ce système comporte plusieurs avantages :

C'est un **système sûr**

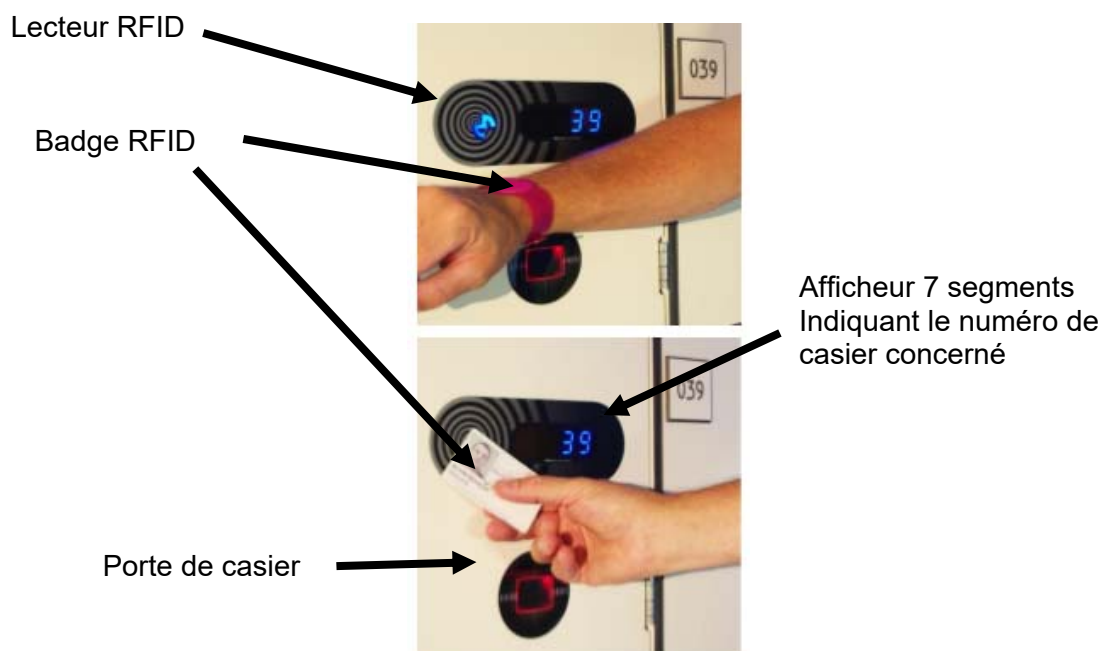
- Serrures entièrement intégrées et invisibles portes fermées pour être protégées contre le vandalisme.
- Serrures équipées de moteur et non d'électro-aimant afin de résister aux chocs.

C'est un **système fiable**

- Fonctionne sur secteur. Une alimentation de secours sur batterie permet le fonctionnement des contrôleurs et des serrures.
- Sans ces alimentations de secours, le fonctionnement des serrures est interrompu. Les casiers restent en l'état ouvert ou fermé et fonctionnent de nouveau dès la remise sous tension – comme s'il n'y avait pas eu de coupure.
- Tous les éléments du système de contrôle des casiers sont prévus pour fonctionner dans une atmosphère humide et chlorée.
- Le système devra être intégré au réseau informatique local de la piscine.

Présentation de serrure RFID (objet de cette étude)

Les casiers vestiaires sont organisés en plusieurs îlots de 32 casiers chacun. Au sein de chaque îlot, les casiers sont pilotés par un contrôleur possédant un afficheur, une antenne lisant les badges RFID. Chaque îlot est identifié par une adresse IP sur le réseau



Travail demandé

Partie A : une solution RFID sera-t-elle adaptée pour verrouiller les casiers vestiaires afin de permettre aux usagers de déposer leurs affaires en toute sécurité ?

Question A1 DTS1.5	Grace aux caractéristiques données par les tags sur le DTS1.5, déterminer le tag le mieux adapté pour notre utilisation. Justifier votre réponse.
-----------------------	---

Question A2 DTS1.2	Déterminer la valeur des 2 amplitudes maximale et minimale permettant la modulation en amplitude du signal transmis par le tag à l'antenne.
-----------------------	--

Question A3 DTS1.2	Déterminer la fréquence de la porteuse permettant la modulation en amplitude du signal transmis par le tag à l'antenne.
-----------------------	--

Question A4 DTS1.2, DRS1	En vous aidant des caractéristiques de la trame RFID du DTS1.2, décoder l'octet de la trame RFID envoyée par un tag en complétant le tableau sur le DRS1
--------------------------------	---

Question A5 DTS1.3	En déduire la valeur du code complet envoyé par le tag.
-----------------------	--

Pour le reste du sujet on considère que le code du tag sera (01 . 7C . A3 . 4F)₁₆

Question A6	Convertir cette valeur en décimal. Vérifier que l'identifiant du badge est bien 24 945 487.
-------------	---

Question A7 DTS1.3	Sachant que le code propre à chaque tag est toujours 1B, déterminer la valeur du checksum du badge étudié.
-----------------------	---

Choix 1

Partie B : La solution retenue est-elle la plus judicieuse pour transférer les données du lecteur RFID au microcontrôleur ?

- | | |
|---------------------------|---|
| Question B1
DTS1.4 | En vous aidant du DTS1.4, identifier le nombre de bits nécessaires à l'information « start » de la trame. |
| Question B2
DTS1.4 | Relever le temps de transmission de l'information « start » puis déterminer la vitesse de transmission normalisée de la liaison série. |
| Question B3
DTS1.4 | Déterminer le temps nécessaire à la transmission complète du code d'un tag RFID. |
| Question B4
DTS2, DRS2 | Compléter le tableau sur le document réponse DRS2, correspondant aux caractères ASCII émis par le lecteur RFID vers le microcontrôleur pour un code Tag de (01 7C A3 4F) ₁₆ . |

Choix 2

Partie C : La chaîne d'information de la serrure est-elle adaptée au besoin des utilisateurs ?

- | | |
|-----------------------------|---|
| Question C1
DRS3 | Compléter l'IBD de la serrure RFID sur le DRS3 avec les numéros correspondants aux termes qui vous sont donnés dans les rubriques composants et flux d'informations. |
| Question C2
DTS1.6, DRS4 | En vous aidant du principe de fonctionnement général de la serrure RFID (DTS1.6), compléter le diagramme d'état du fonctionnement de la serrure RFID sur le DRS4. |
| Question C3 | Conclure si la solution RFID correspond aux exigences définies dans le cahier des charges de la mise en situation ? |

DTS1 : Présentation des casiers et du RFID

Les casiers vestiaires sont organisés en plusieurs îlots de 32 casiers chacun. Au sein de chaque îlot, les casiers sont pilotés par un contrôleur possédant un afficheur, une antenne lisant les badges RFID.

Chaque îlot est identifié par une adresse IP sur le réseau.

DTS1.1 Principe du RFID

La **radio-identification**, le plus souvent désignée par le sigle **RFID** (de l'anglais radio frequency identification), est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« RFID tag » ou « RFID transponder » en anglais).

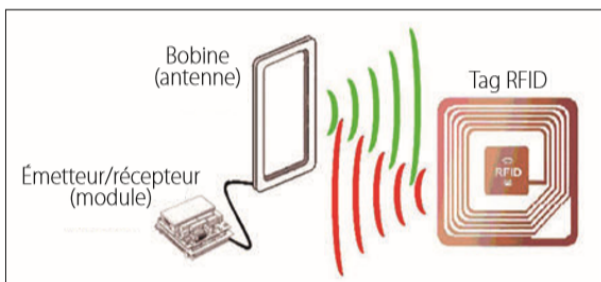
Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collés ou incorporés dans des objets ou produits et même implantés dans des organismes vivants (animaux, corps humain).

Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur.

Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.

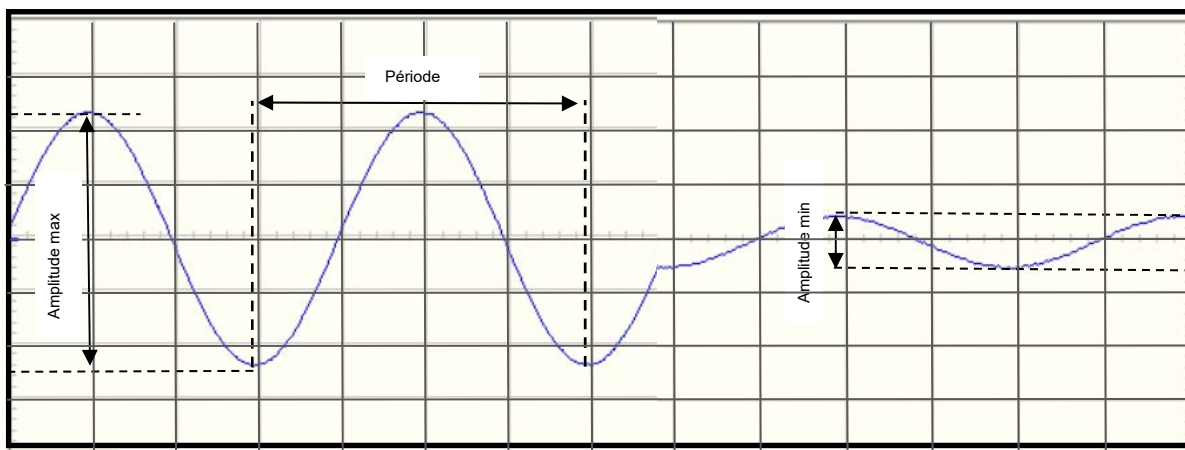
Le système est activé par un transfert d'énergie électromagnétique. Le lecteur agit généralement en maître, il envoie une onde électromagnétique en direction de l'objet à identifier. Il active ainsi le marqueur, qui lui renvoie de l'information.

Le lecteur envoie des requêtes aux tags RFID pour récupérer des données stockées dans leur mémoire. Le tag, généralement télé-alimenté par le signal du lecteur, génère en premier lieu un code permettant d'identifier l'objet sur lequel il est déposé. La communication entre les deux entités s'engage. Le lecteur peut procéder à une écriture d'information dans le tag.



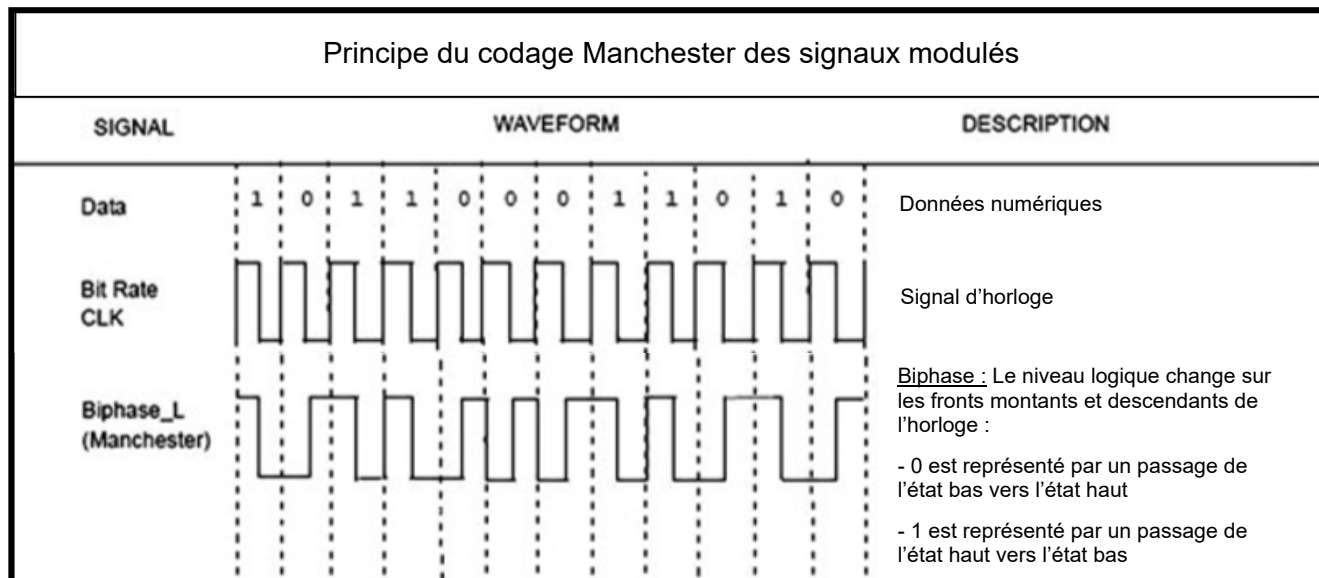
DTS1.2 Protocole de communication RFID

Le code d'un tag transmis au lecteur RFID est constitué de 4 octets, via une onde électromagnétique modulée en amplitude, comme le démontre la capture d'oscilloscope ci-dessous.



Réglages : 1V / division 2µs / division

Le codage utilisé est le code Manchester pour la transmission des données du tag vers l'antenne.



Le premier octet envoyé est l'octet de poids fort. Le tag émet les données par paquet de 4 bits suivi d'un bit de parité paire. Puis de nouveau 4 bits et un nouveau bit de parité jusqu'à émettre les 4 octets du code complet. Il n'y a n'y bit de start n'y de bit de stop. Le contrôle de parité se fait tous les demi-octets transmis. La trame est réémise toutes les secondes si le badge reste sur le lecteur.

DTS1.3 Traitement des données par le lecteur RFID

Le lecteur reçoit un code de 4 octets du tag soit 8 caractères hexadécimaux. Ce code subit un traitement de données afin d'être exploité par un microcontrôleur via une liaison série.

La trame envoyée au microcontrôleur possède le format suivant :

Information transmise par la liaison série au microcontrôleur				
Début de communication	Code propre à chaque Tag	Code du tag	Contrôle Cheksum	stop
1 octet	2 octets	8 octets	2 octets	1 octet
Valeur hexadécimale	Code Ascii des caractères			Valeur hexadécimale
0X 02	1 B	00 98 C1 E3	A1	0x 03

Le cheksum est obtenu en réalisant un ou-exclusif (XOR) entre les valeurs hexadécimales des 5 octets correspondants au code du tag.

Donc ici :

$$(0x\ 1B)\ \text{XOR}\ (0x\ 00)\ \text{XOR}\ (0x\ 98)\ \text{XOR}\ (0x\ C1)\ \text{XOR}\ (0x\ E3) = (0x\ A1)$$

0x 1B =	0	0	0	1	1	0	1	1
0x 00 =	0	0	0	0	0	0	0	0
0x 98 =	1	0	0	1	1	0	0	0
0x C1 =	1	1	0	0	0	0	0	1
0x E3 =	1	1	1	0	0	0	1	1

Ce qui revient à dire que pour une fonction OU-Exclusif à plus de 2 entrées la sortie est égale à 1 si le nombre d'entrées à 1 est impair.

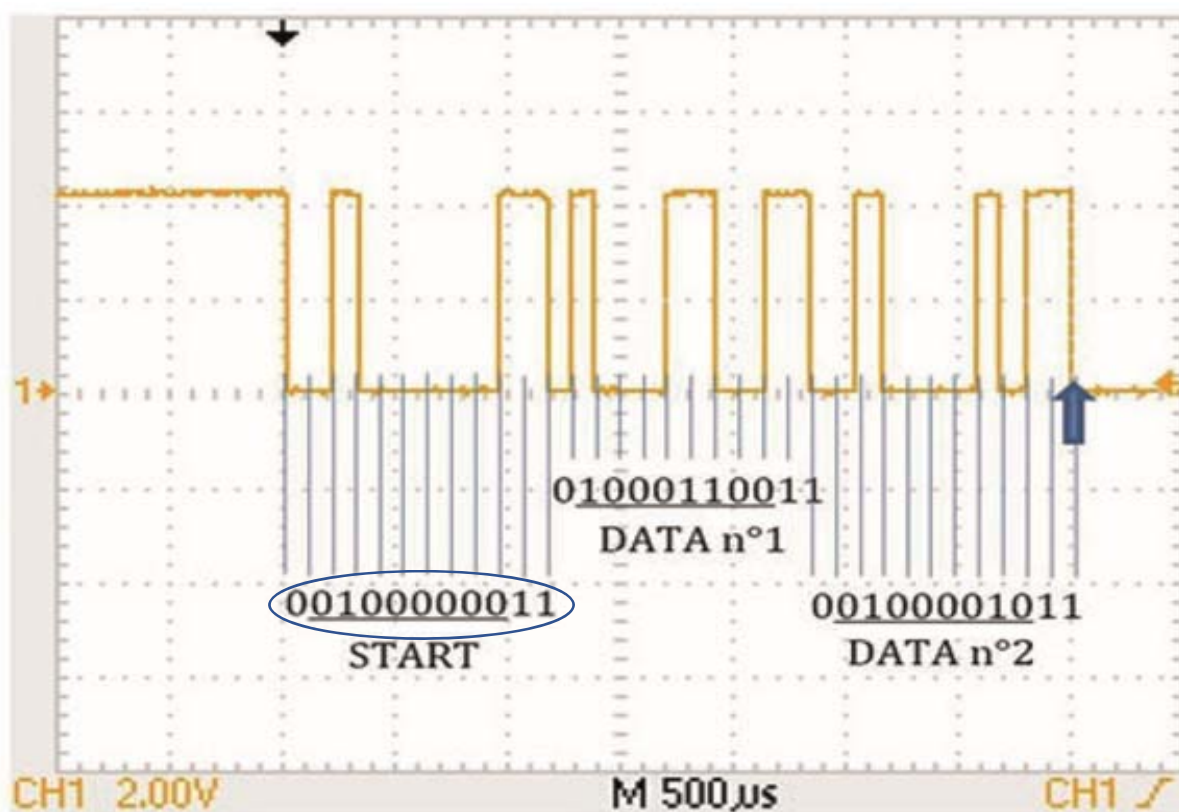
Résultat =

1	0	1	0	0	0	0	1
<div style="text-align: center;"> } (0x A1) </div>							

DTS1.4 La transmission série vers le microcontrôleur.

Le relevé suivant nous montre la trame envoyée par le lecteur de tags RFID au microcontrôleur via une liaison série classique. Chaque octet envoyé est transmis au standard suivant :

1 bit de start, suivi de 8 bits de données (le LSB étant envoyé le premier) et de 2 bits de stop, respectant le format TTL (0 / 5V). Les données sont envoyées au format ASCII (valeur en hexadécimal), ce qui revient à dire que le microcontrôleur va recevoir 10 caractères pour pouvoir identifier le code d'un badge RFID.



La transmission des données se fait à une des vitesses normalisées pour la liaison série.

Valeurs normalisées pour les liaisons série : 75, 110, 300, 600, 1200, 4800, 9600, 14400, 19200, 56000, 115200, 128000, 2560000. (bauds)

DTS1.5 Technologie des Tags RFID

Type de Tag	Famille de fréquence	Bandes de fréquences	Portée	Taux de transfert	Capacité de lecture près du métal ou des surfaces mouillées	Prix	Utilisation
Passif	LF	120-150 KHz	Contact - 10cm	Lent	Le meilleur	de 0,10 à 0,20 €	Suivi des animaux, gestion des accès
Semi-actif	HF	13,56 MHz	10 cm - 1m	Lent à moyen	Moyen sensible au métal	de 5 à 20 €	Suivi des bagages, des livres, surveillance électronique d'articles, porte-monnaie, contrôle d'accès
	UHF	433 MHz	1 m - 100m	Moyen à rapide	Mauvais		Suivi dans la chaîne d'approvisionnement et gestion d'entrepôt
Actif	SHF	2450-5800 MHz	1m – 100m	Très rapide	Le pire	de 15 à 40 €	Télépéage, suivi de chemin de fer, 802.11 WLAN.
	ULB	3,1-10 GHz	> 200 m	Très rapide	Très mauvais		

DTS1.6 Principe de fonctionnement générale de la serrure RFID

C'est un système sûr : les serrures sont entièrement intégrées et invisibles portes fermées. Les serrures sont équipées de servo moteur et non d'électro-aimant afin de résister aux chocs. Un détecteur d'ouverture sur chaque porte prévient des tentatives d'effraction (forçage de la porte) via une alarme dans le local et un report sur un PC serveur, la signature informatique des badges RFID ou code barre est communiquée en temps réel.

Le système lit uniquement le numéro de série unique, qui est une information publique, et l'associe au casier qui est fermé. L'information « casier X fermé » par la badge RFID numéro de série du badge est enregistrée dans le serveur et pas sur le badge. Le lecteur de badge n'inscrit aucune information sur le badge RFID.

C'est un système fiable : les casiers fonctionnent sur secteur et non sur piles Ils sont insensibles aux coupures de courant, car une alimentation de secours sur batterie permet le fonctionnement des contrôleurs et des serrures. Sans ces alimentations de secours, le fonctionnement des serrures est interrompu. Les casiers restent en l'état ouverts ou fermés, et fonctionnent de nouveau dès la remise sous tension – comme s'il n'y avait pas eu de coupure.

C'est un système pérenne et évolutif : compatible avec tous les supports de contrôle d'accès existants car il ne fait que lire ces supports, sans écrire de l'information dessus. Par simple modification de l'interface, les casiers peuvent fonctionner aussi avec des lecteurs biométriques, des claviers à codes secrets

Comment ouvrir et fermer son casier.

Le verrouillage se déroule en 3 phases :

- fermer la porte de votre casier en appuyant sur la porte jusqu'au signal sonore (signal continu pendant 2 secondes). L'activation d'un des interrupteurs d'un des 32 casiers génère une interruption du programme du microcontrôleur ;
- passer votre badge sur l'antenne RFID à côté de l'afficheur LCD dans les 8 secondes ;
- le numéro du casier s'affiche, le casier est verrouillé. Le servo moteur est en position 0°.

Pour déverrouiller le casier :

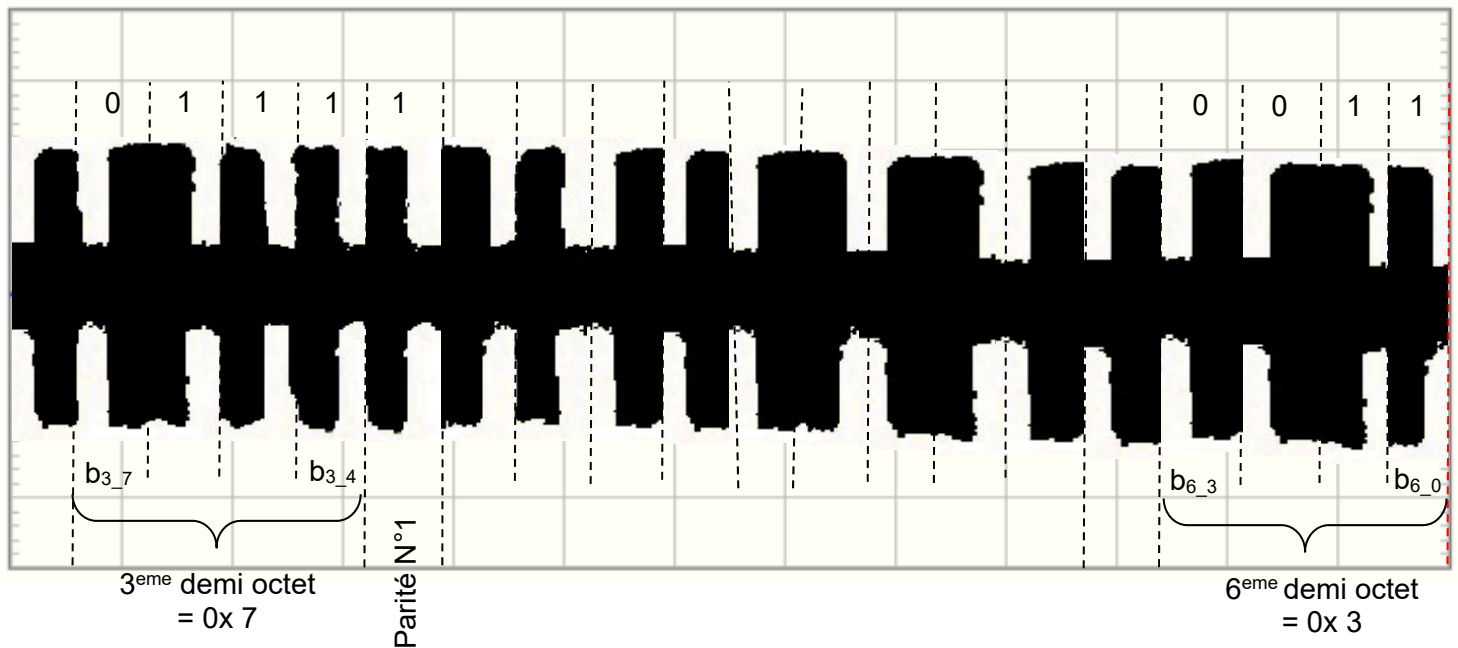
- passer votre badge sur l'antenne, le numéro de casier s'affiche 3 bips sonore sont émis (300 ms à intervalle de 300 ms) le casier s'ouvre. Le servo moteur est en position 180°.

DTS2 : Tableau du codage ASCII

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
32	20	40	[space]	48	30	60	0	64	40	100	@	80	50	120	P
33	21	41	!	49	31	61	1	65	41	101	A	81	51	121	Q
34	22	42	"	50	32	62	2	66	42	102	B	82	52	122	R
35	23	43	#	51	33	63	3	67	43	103	C	83	53	123	S
36	24	44	\$	52	34	64	4	68	44	104	D	84	54	124	T
37	25	45	%	53	35	65	5	69	45	105	E	85	55	125	U
38	26	46	&	54	36	66	6	70	46	106	F	86	56	126	V
39	27	47	'	55	37	67	7	71	47	107	G	87	57	127	W
40	28	50	(56	38	70	8	72	48	110	H	88	58	130	X
41	29	51)	57	39	71	9	73	49	111	I	89	59	131	Y
42	2A	52	*	58	3A	72	:	74	4A	112	J	90	5A	132	Z
43	2B	53	+	59	3B	73	;	75	4B	113	K	91	5B	133	[
44	2C	54	,	60	3C	74	<	76	4C	114	L	92	5C	134	\
45	2D	55	-	61	3D	75	=	77	4D	115	M	93	5D	135]
46	2E	56	.	62	3E	76	>	78	4E	116	N	94	5E	136	^
47	2F	57	/	63	3F	77	?	79	4F	117	O	95	5F	137	_

DRS1 : Décodage d'une trame RFID

Nous avons relevé à l'oscilloscope les signaux suivants



Compléter les tableaux suivants :

Octet N°2									
b _{3_7}	b _{3_6}	b _{3_5}	b _{3_4}	Parité N°1	b _{4_3}	b _{4_2}	b _{4_1}	b _{4_0}	Parité N°2
0	1	1	1	1					
Valeur Hexadécimale					Valeur Hexadécimale				
0x 7									

Octet N°3									
b _{5_7}	b _{5_6}	b _{5_5}	b _{5_4}	Parité N°1	b _{6_3}	b _{6_2}	b _{6_1}	b _{6_0}	Parité N°2
					0	0	1	1	0
Valeur Hexadécimale					Valeur Hexadécimale				
					0x 3				

DRS2 : Code envoyé via la liaison série

	Signification		10 Caractères Ascii										checksum		Stop	
Code Ascii	Start 0x 02		1	B	0	1					4	F	8	A	0x 03	
Code Hexadécimal	30	32	31	42	30	31					34	46	38	41	30	33

1.2

DRS3 : IBD de la serrure RFID

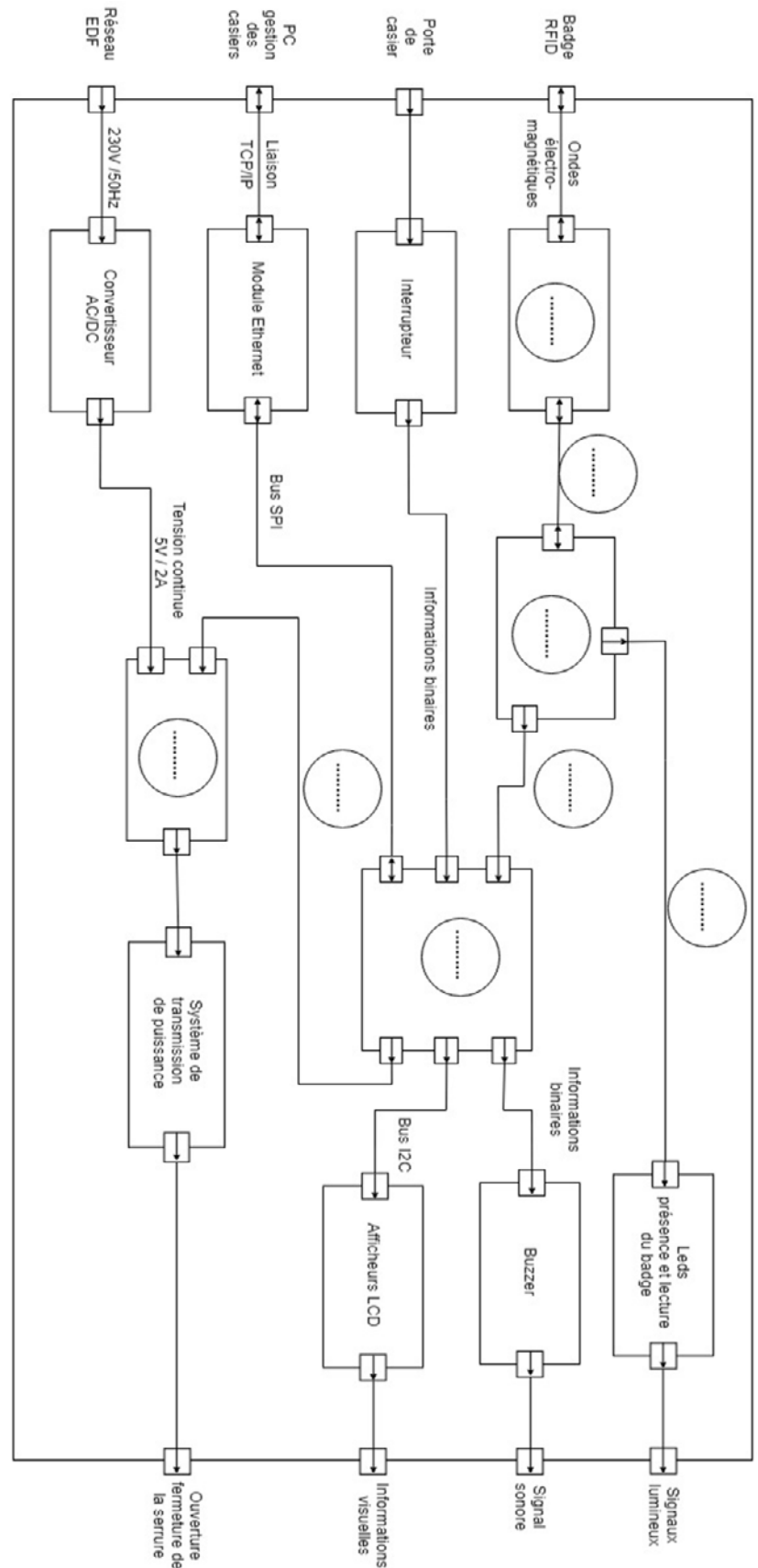
Mettre les expressions suivantes dans l'IBD de la serrure RFID

Composants :

- Microcontrôleur ①
- Lecteur RFID ②
- Servo moteur ③
- Antenne RFID ④

Flux d'informations :

- Liaison série ⑤
- Trame numérique modulée en amplitude ⑥
- Signal de commande à rapport cyclique variable ⑦
- Informations logiques ⑧



21-2D2IDSINME2

