Computers and Electronics in Agriculture
24 (1999) 109–117

Computers and electronics in agriculture

www.elsevier.com/locate/compag

Future developments on devices for animal radiofrequency identification

Mans B. Jansen *,[1], Wim Eradus [2]

Institute of Agricultural and Environmental Engineering (IMAG-DLO), Mansholtlaan 10-12, Wageningen, The Netherlands

Abstract

This article describes the work that is currently being carried out by the Technical Sub-Working Group of ISO/TC23/SC19/WG3 on the definition of an extended standard for advanced transponders. This extended standard will be a logical continuation of the existing International Standardization Organization (ISO) 1996a, 11784 and 1996b, ISO 11785, an International Standard on Radio Frequency Identification of Animals (RFID) transponders. A number of transponder types and authentication methods which will be included in the extended standard are discussed, together with the solutions for the communication protocols which will be needed. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Animal identification; Animal RFID; Animal tags; Animal transponders; Authentication; ISO 11785; Radiofrequency identification

1. Introduction

Passive electronic identification transponders consist of an electric resonance circuit (induction coil and capacitor), acting as a receiving/transmitting antenna, connected to an electronic microchip. When such a transponder is placed in an electromagnetic field of sufficient field strength, the induced voltage in the resonance circuit powers the microchip which will turn on and starts sending back its stored identification number via the resonance circuit. The reader which generates the electromagnetic field receives the transmitted code and displays it on a screen.

* Corresponding author.
[1] Chairman of the Technical Working Group of ISO-WG3.
[2] Secretary of the Technical Working Group of ISO-WG3.

PII: S0168-1699(99)00041-1

Transponders can be manufactured in several shapes such as the implantable variety, a glass capsule of a few millimetres in diameter and 12–32 mm in length. Other types are electronic ear tags for cattle and the so-called bolus transponders which can be swallowed by cows and goats and will remain in the gastrointestinal tract. In the past the ISO (International Standardization Organisation) has issued two standards describing the bit structure and the technical concept of the ISO-compatible transponders. These ISO-compatible transponders for animal identification applications are widely used now in many parts of the world. At this moment, 1g transponder manufacturers have acquired an ICAR (International Committee on Animal Recording) manufacturer's number after successfully passing ICAR's manufacturer's approval test. This indicates that a global standardisation of this generation of RFID (radiofrequency identification) systems will be reached in the near future. It is expected that other RFID protocols will phase out in the next years in favour of the ISO 11784/11785 protocol. In the mean time, work will be done on the standardisation of the next generation RFID systems for animal applications. These so-called advanced transponders will have one or more features such as authentication, on-board sensors and additional memory pages. It is very clear that the compatibility with the existing ISO 11784/11785 protocol is essential so that every animal transponder can be read anywhere by any reader, since animals will be transported from one country to another. Therefore, an advanced reader must be able to read an existing technology transponder and an existing technology reader must be able to read at least the first page of an advanced transponder.

2. Types of advanced transponders

A number of additional features can be added to the existing read-only transponder. These features will be discussed in this section.

2.1. Authentication transponders

The code of all today's generation animal transponder brands can be copied into an 'empty' chip, causing duplicate animal numbers. In the case of ISO-compatible transponders, the manufacturer's databases or the country databases guarantee that such fraudulent duplications will be discovered. Nevertheless, it is highly desirable that next generation's transponders are far more difficult to copy. Depending on the application of the transponder the need for this security will be more severe or relaxed. A very expensive racing horse, for instance, needs a transponder with a very high security level. On the contrary, pigs on a farm are 'satisfied' with a low security authentication. This is important because the security level influences production cost and size of the transponder. The principle of the various types of authentication will be discussed later in this article.

2.2. Multipage transponders

In today's generation transponders only a limited amount of data is stored. There is a growing demand for transponders which are capable of storing additional data such as animal characteristics, farmer's data, medical history of the animal, etc. In those cases it must be possible to safely write data to the transponder's memory. Additionally it must be possible to protect the data in the transponder against unauthorised reading by third parties. All this requires a different kind of reader which not only supplies the transponder with electromagnetic energy but also transfers data from the reader to the transponder. The memory in the transponder is mapped into so-called pages. Every page contains a predefined number of bits which can be read-only memory, write once/read many times memory or random access memory.

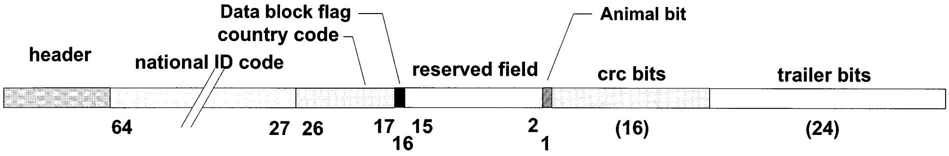
2.3. Sensor transponders

The ability of instantaneous measurement of animal's physiological body parameters opens exciting applications in the future. Simple sensors for temperature are already found in some brands of transponders. Temperature sensors can be read out during interrogation at the feeding station. Sensors like heart rate and activity measurements are more difficult to implement since they require an uninterrupted power source for continuous measurement which is usually not present in today's transponders. Ongoing research on miniature battery fed sensor transponders and on alternative power sources for sensor transponders looks promising.

3. Transmission protocols

Fig. 1 shows the bit pattern of the ISO 11784 transponder. The 14 bits of the reserved field contain all zeros and are meant for future applications such as advanced transponders.

As mentioned before, the next generation's readers must be capable of sending a message to the transponders (downlink) which are to be interrogated. These



Bit 1: Animal/non-animal flag (1/0)
Bit 2...15: reserved field (all zeroes)
Bit 27...64: national ID code
Bit 16: additional data flag (0/1)
Bit 17...26: country code (0 ... 999)

Fig. 1. Bit pattern of the existing ISO transponder.

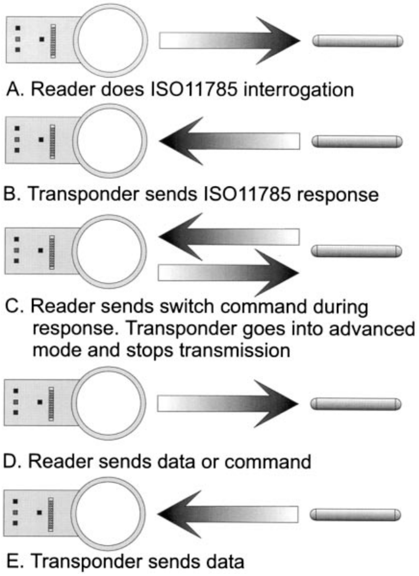

A. Reader does ISO11785 interrogation
B. Transponder sends ISO11785 response
C. Reader sends switch command during response. Transponder goes into advanced mode and stops transmission
D. Reader sends data or command
E. Transponder sends data

Fig. 2. Interrogation procedure for an advanced transponder.

messages will contain a random number in case of authentication transponders, page switching and page blocking information in case of multipage transponders and sensor switching or sensor calibration data in case of sensor transponders. There is another problem to overcome in case of FDX (full-duplex) transponders since today's generation transponders must be fully upwards compatible with advanced readers and next generation's transponders must be downwards compatible for the first page containing the ID code with existing readers. The next generation's FDX transponders must have a means to be switched into the advanced mode. When an advanced transponder is interrogated with an unmodulated activation field they must react like a read only transponder, giving only the ID code according to the ISO transmission protocol. In this way it is possible to read the advanced transponder with an existing technology reader. When the advanced transponder is interrogated with an advanced reader, the reader starts the interrogation sequence with generating an unmodulated interrogation field just like an existing technology reader (Fig. 2A). The advanced transponder responds with the normal ISO 11785 protocol (Fig. 2B), with the only difference that there is a type code in the reserved bit field of this protocol (Fig. 1). The advanced reader interprets the type code which is in the reserved bit field. This type code contains information for the reader which type of transponder is being interrogated. The reader now knows which transmission protocol must be used to transfer data to the transponder and how the transponder can be forced into the advanced mode. During the on-going response of the transponder the reader sends the switch command to the transponder (Fig. 2C). This can be done without interference with the transponder's response code because of the exact clock synchronisation between transponder and reader. When this happens, the transponder stops sending its ID code and starts listening for following commands from the reader. In this mode the reader is the master in the communication process and the transponder is the slave. From now on, the reader can send a command or a data stream to the transponder (Fig. 2D), resulting in a response from the transponder with data or status information (Fig. 2E). In case of HDX (half-duplex)[3] transponders, the type code in the reserved field also tells the reader which kind of transponder is in the interrogation field. However, no separate switching into the advanced mode is necessary since HDX transponders are waiting to respond until the interrogation field of the reader ceases. After the reader has found out which kind of transponder is in the field, It sends directly a command to the transponder in the second half of the interrogation field pulse of 50 ms which time duration may be extended for longer messages. At the time the transponder must send back its information, it already knows which kind of information is requested by the reader. Both with FDX and HDX transponders, the uplink protocol (transponder to reader) has in the advanced mode a word length of 128 bits, which is the same as described in ISO 11784. The modulation type and depth as well as the bit rate are the same as described in ISO 11785. However, the subdivision of the bit stream into separate fields depends on the application and is defined by the type code. For the downlink however, HDX and FDX have different modulation methods, while FDX will have a low modulation depth protocol and a high modulation depth protocol, each having different advantages for various applications. The length of the bit stream will be dependent on the type of application and will be dictated by the type code in the reserved field of the transponder which is previously transmitted to the reader.

4. Types of authentication

It has already been mentioned that the level of security against fraudulent copying has a cost and size impact on the transponder. Moreover, also the maintenance of a central database which is necessary with some types of authentication will have cost consequences. Therefore the extended standard, which is being developed now, will contain several levels of authentication, ranging from very simple ones to very sophisticated ones. Basically, there will be three levels of authentication which will be discussed in this section.

4.1. Low level authentication

In this case a reasonable level of security will be derived for low cost transponders. Essentially, every produced transponder chip will contain an unique serial

[3] The ISO 11785 protocol describes the full duplex (FDX) and half-duplex (HDX) transmission protocols. Each transmission protocol has its own pros and cons. Therefore it was decided to include both protocols in the standard.

number. This serial number is produced at the chip manufacturer's site and cannot be changed afterwards. There are several ways to deal with this serial number, all with their specific advantages for different fields of application. Also in this case, the reader knows from the type code it receives during the first read of the transponder which type of authentication is used. Two possible low level authentication scenarios will be discussed

4.1.1. Low level authentication with a database

The unique die serial number is programmed during production of the chip wafers and cannot be altered afterwards. During programming of the ID code by the tag manufacturer a consistency check number is calculated from the die serial number and the ID code. This check number is stored in the 24 trailer bits of the ISO 11785 protocol. The ID code and the consistency check number are stored in a central database and/or marked in the animal's passport. This must be done by authorised persons and access to the database must be controlled. When the transponder is read out, the reader can check if the consistency check number matches with the die serial number and the ID code. This already gives a limited level of protection. Additionally, the ID code and the unique die serial number can be checked in the central database where they are stored. With this type of authentication it is essential that all chip manufacturers only deliver chips with the unique die serial number. It is expected that this will be the case since the number of chip manufacturers is rather limited.

4.1.2. Low/mid level authentication with hidden random number in ISO 11785 trailer bits

This method is suitable in those cases where incidentally a transponder must be checked for authenticity. A random number, only known by the manufacturer, is hidden in the trailer bits. Normally, the transponder returns all zeroes in the trailer bits on interrogation. When doubt has arisen about the unicity of the transponder code, the random number and the access code can be asked for by the manufacturer by submitting the ID number of the transponder. A suitable reader can be loaded with the random number and the access code. When the transponder receives the correct access code, it responds with its ID code and its random number in the trailer bits. The reader can compare the random number, obtained from the manufacturer and the received one. When these numbers are equal the transponder is authenticated. This kind of authentication will only have minor cost consequences for the transponder.

4.2. Mid level authentication

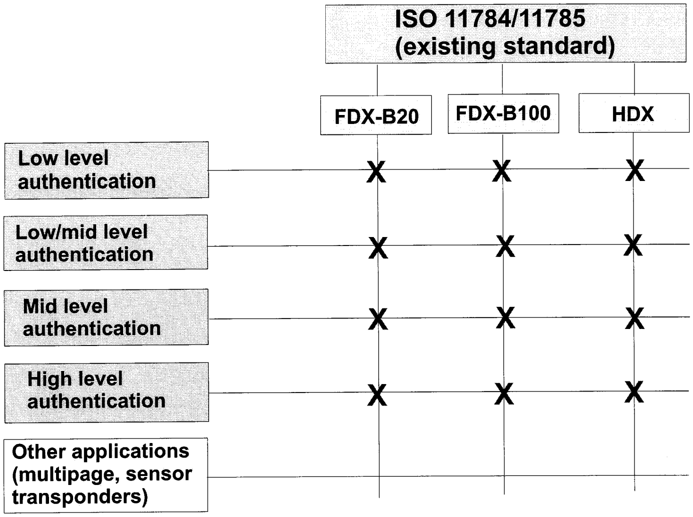
A more secure method to prevent fraud on transponders is a data encryption system based on a random number sent by the reader to the transponder. After the reader has read the ISO 11785 message of the transponder it knows from the type code that a mid level authentication transponder is in the field. The reader now sends a random number to the transponder, which calculates an answer code from this number, the hidden secret key and the standard ID code and sends it back to the reader. The reader now validates the message of the transponder by using the same secret key which is also hidden in the reader. Since the random number the reader sends to the transponder is different every time, it is hard to counterfeit such a transponder. However, it is essential that the secret key is kept secret all the time. It is estimated that this level of authentication can be implemented at moderate extra cost and chip size.

4.3. High level encryption

This most secure encryption scheme uses the Data Encryption Standard (DES) (US Department of Commerce, 1988, 1993), a patented encryption algorithm invented at IBM. The encryption process is controlled by a secret key of 56 bits. The encryption process involves 19 stages in a DES chip performing several transpositions and substitutions on the original message in which the secret key is used. The process at the receiver end and the transmitter end is symmetrical i.e. every encryption step taken at the transmitter side will be performed in reverse at the receiver side. So the same secret key is needed at both ends. However the encryption algorithm may be public. Without having the secret key, it is almost impossible to break the encryption. Because the encryption an decryption process is very complicated it will cost a lot of chip space, making the transponder far more expensive and bigger. It is clear that this kind of transponders are only meant for special occasions, such as racehorses, etc.

5. The new ISO standard for advanced transponders

The Technical Working Group (TWG), a subgroup of ISO Working Group 3 is working on the new standard for advanced transponders. TWG decided to define an open standard to ensure maximum flexibility in the implementation. Every combination of transmission protocols and authentication methods is possible (Fig. 3). At first the transmission protocols and the authentication methods will be defined, followed by the multi page definitions and protocols for sensor transponders. The starting point is the full downwards compatibility with the existing ISO 11784/11785 standards. An important point is the decision to use type codes in the reserved field of the ISO 11784 standard. This gives the opportunity to ‘teach’ a reader how to interrogate an advanced transponder of a certain class. In the future, new types of transponders can be added, simply by adding new type codes. A reader can be updated with new type codes by downloading the interrogation protocols from Internet or via another medium. In any case, advanced transponders can be of the HDX or FDX type as they exist now in the ISO 11785 standard.



	ISO 11784/11785 (existing standard)		
	FDX-B20	FDX-B100	HDX
Low level authentication	X	X	X
Low/mid level authentication	X	X	X
Mid level authentication	X	X	X
High level authentication	X	X	X
Other applications (multipage, sensor transponders)			

Fig. 3. Overview of the possible combinations of transmission protocols and authentication methods.

6. Conclusion

Animal radiofrequency identification has grown out since the last years to a widespread accepted means for identifying all kinds of animals, including pets, zoo animals and fishes. Thanks to the ISO standardisation it is now possible to identify animals coming from any country in the world in every place with just a standard ISO reader. The next generation of transponders and readers will possess several new features which will enhance the usefulness of the system considerably.

Acknowledgements

The progress on the development of the extended standard for advanced RFID transponders has been made possible by the enthusiastic co-operation of all the members of the Technical Working group of ISO.TC23/SC19/WG3: R. Artmann (Institut für Betriebstechnik FAL-BS); K. Aslanidis (TIRIS); K. Bischof (Mikron/Philips); J. Bolscher (TIRIS); D.H. Clemons (Destron-Fearing); H.U. Fritsch (Diehl Ident Gmbh); R. Geers (KU-Leuven); P. Hassan Zade (Datamars); J.H.L. Hogen Esch (Nedap); Z. Mejia (Destron Fearing); H. Pirkelmann (Bayerische Landesanstalt für Tierzucht); H. Ruppert (Ing-Buro Ruppert); C.W. Schenk (AEG-ID); Inga Lill Solberg (Alfa Laval Agri AB); P. Stegmaier (Datamars); Valloton (Sokymat); G. Wendl (TUM Landtechnik).

References

US Department of Commerce, 1988. Data Encryption Standard (DES), 22 January 1988. FIPS PUB 46-1 (c13.52).

US Department of Commerce, 1993. Data Encryption Standard (DES), 30 December 1993. FIPS PUB 46-2 (c13.52).