

5 APPARATUS AND METHODS FOR ELECTROMAGNETIC IDENTIFICATION

TECHNICAL FIELD

This invention relates to electromagnetic identification systems, for example of a type commonly referred to as radio frequency identification (RFID) systems, devices for use in
10 RFID systems and methods for operating such systems and devices. In particular, embodiments of the invention relate to active transponder tags, networked reader devices, and messaging protocols suitable for communications over the wireless interface between such tags and readers.

15 BACKGROUND

RFID apparatus are a type of automatic identification system and, as such, provide means for collecting, monitoring and tracking systems. Known types of RFID networks use “passive” and “active” tags (transponders), although not always in the same network. A “passive” tag is a miniature transponder capable of returning a response to a stimulus from a
20 reader device. Passive tags tend not to have a power source and so respond with energy from backscattering or by harnessing electrical induction effects in antennae.

An “active” tag relies on its own transmitter for communicating with reader devices over the air interface and therefore usually also includes a power source and microcontroller.
25 As advances in active tag design enable the mass production of higher performance tags at lower costs, active tag technology can be expected to be deployed more widely in all types of RFID networks. In more sophisticated deployments active tags can be programmed to enable aspects of their function to be defined by the user, typically an RFID network administrator.

5 Applications for RFID technology are many and varied. However, applications include all manner of automatic identification, access, monitoring, tracking and remote sensing applications applied with personnel, animals, products and other assets.

As this technology has developed, the term "radio frequency" has been used increasingly broadly, to refer for example to such apparatus and methods employing a considerable range of frequencies of the electromagnetic spectrum in wireless communications. See for example Table 1, below which sets out typical frequencies which may be encountered:

TERM OF REFERENCE	TYPICAL FREQUENCY
Low Frequency	30 kHz to 300 kHz
Medium Frequency	300kHz to 3MHz
High and Very High Frequency	3 MHz to 300 MHz
Ultra-high Frequency	300 MHz to 2 GHz
Microwave	2 GHz to 6 GHz and beyond

15 **Table 1: Terms of reference in RFID art and associated frequency ranges**

Even the ranges indicated above are exemplary only for RFID applications and should not be construed as limiting. Within each frequency range indicated above, certain frequencies tend to be selected, for example, based on the availability of unlicensed spectral bands, standards, local legislation or other criteria. Low frequency applications often use 125 kHz or 134.2 kHz; high frequency applications often use 13.56 MHz; UHF applications tend to employ 433 MHz, 463 MHz, 868 MHz, 915 MHz or 956 MHz; and microwave

5 applications typically use 2.45 GHz or 5.8 GHz. However, a skilled person will appreciate that any suitable range corresponding to one or more of the exemplary ranges in Table 1 (or any combination) may be used with embodiments of the present invention. In some circumstances, embodiments of the present invention may employ frequency ranges outside those indicated in Table 1 and which are still suitable for wireless communication.

10

Increasingly, RFID applications require large and diverse populations of tags, often deployed in with high tag densities (100 tags per reader) and in rapidly evolving scenarios. As tag performance and the number of functions supported by tags increases to meet these demands, it becomes increasingly difficult to keep the cost of production down at acceptable levels for large scale deployments.

15

Embodiments of the present invention seek to provide improved electromagnetic identification systems, and particularly improved RFID networks, including active tags, reader devices, and communication protocols suitable for air interface communications between tags and readers in RFID networks.

20

SUMMARY

According to an aspect of the present invention, there is provided an active transponder for use in an RFID network comprising transponders and networked reader units for receiving messages from the transponders, the transponder comprising: transmission circuitry; a controller having access to a memory; a power supply, wherein the controller comprises control code for constructing a message packet corresponding to a transponder class to which the transponder belongs, said class of transponders being one of a plurality of classes each characterised by aspects of the configuration of peripheral devices of transponders in that class, and wherein the controller further comprises means adapted to

25

30

5 include in said message packet an indication the message packet is a message from a transponder and an indication of the class of transponder from which the message originates, and one or more peripheral data fields according to the message packet structure of the transponder class.

10 Preferably, the message packet comprises at least one user defined data field. In the disclosed embodiment, the content of a peripheral data field is at least partly defined by a user.

Disclosed the transponders also comprise an external programming interface capable of allowing direct programming of the transponder, without programming via a reader unit. Preferably, this programming interface is capable of allowing programming of the
15 transponder via a reader unit or built device.

Preferred transponders comprise two or more peripheral devices comprising one or more of a counter and a sensor. Alternatively, or in addition, a transponder may comprises two or more sensors selected from one or more of: a temperature sensor; a location sensor; a movement sensor; a vibration sensor; a seismic sensor; a magnetic sensor; a force sensor; a
20 strain sensor; a rotary sensor; a pressure sensor; a tamper sensor; another type of mechanical sensor; a chemical sensor; a biochemical; a biological sensor; a biometric sensor; a proximity sensor; humidity sensor; a position sensor; a light sensor; and other suitable types of sensors.

Exemplary types of sensor combinations include without limitation, a movement sensor and a tamper sensor; a tamper sensor and a temperature sensor; a location sensor, a
25 movement sensor and a temperature sensor.

In disclosed embodiments, transmission circuitry is arranged to operate at one or more of the following ranges: 30 to 300kHz; 300kHz to 3 MHz; 3 MHz to 300 MHz; 300 MHz to 2 GHz; and 2 GHz to 6 GHz. In other embodiments, the transmission circuitry is arranged to operate at one or more of: 125 KHz; 134.2 KHz; 13.56 MHz; 433 MHz; 463 MHz; 868 MHz;
30 915 MHz; 956 MHz; 2.45 GHz and 5.8 GHz.

According to another aspect of the present invention, there is provided a method of generating a transponder message in an RFID network comprising active transponders and networked reader units, the method comprising: providing a plurality of transponders and allocating the transponders into predefined classes based on aspects of peripheral

5 configurations of the transponders; establishing a predetermined format for a message packet applying to each predefined class of transponder such that each of the plurality of predefined transponder classes has a predetermined message packet structure according to the configuration of peripherals of transponders in that class; building a message packet based on said established message format, the message packet including an indication the message is a
10 transponder message, an indication of the class of the transponder from which the message originates, and one or more peripheral data fields.

Preferably, the message packet includes user data field. Preferably also the contents of a peripheral data field may be defined at least in part by a user.

Embodiments also include a method for programming one or more of: a peripheral
15 function of the transponder; a reporting function of the transponder; and user data on the transponder, by means of a programming interface.

Typically, a transponder comprises two or more peripherals, at least one of which is a sensor and the message packet includes a corresponding number of peripheral data fields. In another embodiment, the transponder comprises a plurality of peripheral sensors and the
20 message packet includes a corresponding plurality of peripheral data fields.

Preferably, the message packet also includes one or more fields selected from: a transponder identity field and an error checking field.

In at least one mode of operation, a transponder according to the present invention transmits in response to a predetermined criterion. For example, said criterion may comprise
25 receipt of a message from a reader requesting a response from the transponder. In this case, the criterion may comprise a predetermined delay from receipt of a message from a reader.

In another embodiment, the transponder in at least one mode of operation transmits only after predetermined intervals. In another embodiment, the transponder transmits in a time slot allocated to it via a reader unit. Alternatively, or in addition, the transponder may
30 transmit based on a frequency hopping algorithm.

In a disclosed embodiment, the transponder receives and responds to a message from a reader selected from one or more of the following types: get tag data; tag wake up; tag

5 sleep; set tag mode of operation; set tag peripheral function; set tag reporting function; set tag alarm criteria; set tag user information.

According to another aspect of the present invention, there is provided a transponder message packet format for message packets sent by a transponder to a reader unit in an RFID network, comprising: a message packet type field indicating the message is a transponder message; a transponder class field indicating a transponder class from a plurality of predefined transponder classes to which the transponder belongs; a plurality of peripheral data fields and, optionally, a user data field according to a predefined message format for the class to which the transponder belongs.

15 Preferably, their transponder message for much comprises a further field for user definable peripheral data. Alternatively, or in addition, the transponder message format comprises a further field selected from one or more of: a tag ID field; a network information field; and an error correction field.

The transponder message format may be recorded in a memory of the transponder ahead of being transmitted to another device in the network.

20 According to another aspect of the present invention, there is provided a set of transponder message formats for use in an RFID network, the set of message formats comprising: a plurality of message formats each comprising a transponder type field, indicating the message is a transponder message, and a transponder class field, indicating the class of transponder from which the message originates, and wherein a message format has a different predetermined peripheral data field configuration in dependence on the transponder class from which the message originates.

25 Preferably, each message format of the plurality of message formats has different predetermined peripheral data field configuration in dependence on the transponder class. Preferably said peripheral data fields of a message format comprise a plurality of sensor fields each for carrying data from a different type of sensor on a multi-functional transponder.

30 According to another aspect of the present invention, there is provided a reader unit capable of constructing a network message comprising a transponder data field for content from a transponder message, wherein substantially the entirety of transponder message is incorporated into a transponder data field of the network message.

5

Additional advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following and accompanying drawings or may be learned by practice of the invention.

10 BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention and as to how the same may be carried into effect reference will now be made, by way of example only, to the accompanying drawings, in which:

Figure 1 shows an exemplary RFID network;

15 Figure 2 shows an exemplary mesh network organisation;

Figure 3 shows a reader device according to an embodiment of the present invention;

Figure 4 shows a message packet structure according to an embodiment of the present invention;

20 Figure 5 shows a response packet structure according to an embodiment of the present invention;

Figure 6 shows a tag transponder according to an embodiment of the present invention;

Figure 7 shows a general message protocol suitable for use between tags and readers according to the present invention;

Figures 8A-8G show a plurality of exemplary tag message packet formats;

25 Figure 9 shows a further generalised message packet structure for potential tag classes; and

Figure 10 illustrates an exemplary process for how tag data is processed.

DETAILED DESCRIPTION

Fig.1 shows an exemplary RFID network according to an embodiment of the present invention. The network has a control interface 100 including an application server 120 for running an application program, a reader network 102, and a plurality of transponder tags 104, at least some of which are “active”. The numerous individual tags 105 are deployed, for example, on products or other assets, animals or humans, or combinations thereof.

The reader network 102 can be any hardwired or wireless network capable of being organised to support physically distributed readers 103 arranged to receive data from the tags 105 over the air interface 112, and to relay this information back to the control interface 100, as will be explained in more detail hereinafter. Whereas in conventional RFID networks readers are not always configured to send messages to tags and instead act as receive-only nodes for messages from tags, in the present embodiment each reader 103 can additionally send certain types of messages to tags 105 in its field via the air interface 112. Although, the exemplary reader network 102 in Fig. 1 is organised linearly, a skilled person will appreciate that a range of known, and future, network organisations may be used as the backbone of the reader network, for example the mesh network organisation shown in Fig. 2.

Fig. 3 shows an exemplary reader device 103 according to embodiments of the present invention. The reader 103 comprises an RF module 300 having an antenna and receiver circuitry. The RF module is coupled to a microcontroller 302. The microcontroller 302 has access to a non-volatile re-writeable memory 304 and is also independently connected to an indicator circuit 306 and the reader network interface circuitry 308.

5 In use, the RF module 300 receives analogue radio frequency signals transmitted
from tags within effective radio range of the reader and converts these signals to digital data
by means of known analogue-to-digital conversion technology. The RF module 300 also
includes buffers and the like (not shown) to queue inbound messages from tags ahead of
processing by the microcontroller 302. The microcontroller 302 can access control
10 information residing either locally (within the microcontroller) or in the memory 304. The
microcontroller uses this control information to control the reader operations. In particular
the microcontroller 302 controls the processing of tag messages it receives from the RF
receiver 300 and the processing of reader network messages received from, and placed onto,
the network interface 308. In this embodiment the indicator circuit 306 has a plurality of
15 LEDs which may be used, where desired, to indicate status of the reader.

The reader network 102 is automatically scalable so that readers can be added as
desired. The reader network 102 also allows the application program to individually address
reader nodes 103, and therefore direct messages to individual reader nodes. In this
20 embodiment it is also possible for the application program to address and direct messages to
all nodes 103 or to groups (subsets) of nodes 103. The messages sent over the reader network
may be bound for the application 120, a reader node or nodes 103, or a tag or tags 105.
General network architectures capable of supporting these routing criteria will be known to a
skilled person.

25

The reader network 102 handles two basic classes of application messages,
“command messages” and “response messages”.

5 Fig. 4 shows an exemplary message packet structure suitable for command messages transferable through the reader network. With reference to Fig. 4, the command message packet includes a header portion 402 indicating the message is a command message, a further field 404 indicating the number of bytes in a data section of the message, one or more further fields 406 including network addressing information such as reader node(s) ID and if
10 appropriate tag ID or multiple tag IDs, a field 408 indicating the command type, a data field 410, and a checksum 412. The overall length of the command message packet and the relative sizes of various fields within it will depend for example on the application, message configuration, network organisation and scale.

15 The number and nature of different command types supported by the reader network 102 will depend in particular on the application(s) but typically includes, for example: Get Tag Data; Tag Wake Up; Tag Sleep; Network Reset; Set Mode; Set Address Information; Set System Information; Measure Signal Strength (RSSI); Set Receiver Gain; Set Alarm Criteria; Set Report Criteria; Set Baud Rate; and Get Version information. Commands such as Get Tag
20 Data, Tag Wake Up and Tag Sleep support so called "speak when spoken to" applications. This type of application operates such that communications from tags are minimised or eliminated altogether unless a tag is specifically addressed by a reader. Speak when spoken to applications are important for example where the deployment has high tag densities, local legalisation precludes ordinary levels of beaconing or tag battery life needs to be extended
25 beyond normal bounds.

Fig. 5 shows an exemplary response packet structure, for response messages transferable through the reader network. With reference to Fig. 5, the response packet includes a header portion 502 indicating the message is a response message, a field 504

5 indicating the number of bytes in a data section of the message, a field 506 including network addressing information such as node(s) ID or equivalent information, a field 508 indicating the response type, a tag data field 510, and a checksum 512. The overall length of the message and the length and configuration of the various fields within it will depend for example on the application, message configuration, network organisation and scale.

10

The number and nature of different response message types supported by the reader network 102 may vary but typically includes at least response types for all supported commands for which the application might expect a response. In this embodiment the contents of the response type field 508 replicates that of the command type field in the
15 corresponding command. For example in the case of a response message to a "Get Tag Data" command, the response type field is identical to the command type field present in the issued command message. This combination of fields indicates that the response message packet contains relevant data from the tag probed by the corresponding command message. In this embodiment the tag data field contains the entire contents of the message packet from the
20 relevant tag to its reader, albeit after conversion from analogue to digital and after having been packaged in to the larger reader network message by the components of the reader. Exemplary tag message packet content is described hereinafter with reference to Fig. 7.

Fig. 6 shows a tag transponder suitable for use with embodiments of the present
25 invention. The tag has a microcontroller 602, an external programming interface 604, a plurality of peripheral devices, such as sensor devices 606 and counter devices 605, a power supply 608 such as a battery, and an RF transceiver module 609 provided with an oscillator 610 and an antenna 612. In this embodiment the RF transceiver is configured to transmit at 433.92 MHz. A memory 620 stores the unique identity of the tag, tag data recorded by the

5 peripherals and control code for controlling tag operations such as building and scheduling messages destined for the reader network. Alternatively, or in addition, control code may be stored in a local memory of the microcontroller 602.

In general, the tags deployed in a given network may comprise a mixture of active and
10 passive tags, and among the active tags different sensor capabilities may be supported. The peripheral devices typically include two or more peripherals capable of sensing an aspect of the external environment or location or event applying to the tag. For example, here the peripherals include a number of different sensors and counter devices. The counters can record for example the number of transmissions by the tag or the number of times a particular
15 sensor or other peripheral is activated. In this embodiment a plurality of different sensors is provided and the air interface protocol supports communication of tag data relating to the plurality of sensors and the counter devices simultaneously. In practice, sensor types may include two or more sensors selected from a temperature sensor, a location sensor (GPS receiver or the like), a movement sensor (accelerometer or the like), a vibration sensor, other
20 mechanical sensors (such as a latch), a tamper circuit, a chemical sensor, a biological sensor, a biometric sensor, a seismic sensor, proximity sensor, magnetic sensor, force sensor, strain sensor, humidity sensor, position sensor, rotary sensor, light sensor, pressure sensor etc...

Exemplary embodiments with two or more sensor functions include:

25 Tags with movement and tamper

Tags with tamper and temperature

Tags with GPS and accelerometer and tamper

5 The examples and combinations are not intended to be limiting and a skilled person will readily appreciate that a considerable number of different multi-peripheral combinations can be supported, including sensor combinations involving two, three, four, five, six or more sensor types, depending on the application or applications.

10 In this example the RF transceiver circuitry 609 is configured to transmit at 433.92 MHz, which is an unlicensed band in most countries. The tags typically also comply with well known FCC, SATRA, CE and ETSI requirements. In other embodiments a tag may support transmission to the reader network 102 at any frequency indicated, or proximate to those indicated, in the ranges of Table 1, or indeed combinations of such frequencies. The or
15 each tag 105 can be programmed to transmit for example at predetermined regular intervals, at irregular or random intervals, according to predetermined timing sequences, and/or based on frequency hopping algorithms. Further, or in addition, tags may be programmed to transmit in response to being addressed by a reader, and in certain embodiments to transmit only in response to such an address (so called “speak when spoken to” configurations). In
20 certain embodiments a tag can respond to reader after predetermined delays and this may be used as a mechanism for assigning transmission slots to a plurality of tags in the field of a particular reader. Such techniques have particular application in deployments involving high tag densities.

25 In this embodiment aspects of tag functionality, and particularly peripheral functions, can be programmed by a user via the programming interface 604. Such programmability is particularly useful in for example sophisticated remote sensing applications. For example where the sensors include a temperature sensor, a tag can be programmed to send an alert (or regular readings) in response to predetermined temperature conditions or a specific pattern of

5 temperatures. As another example, a tag with a GPS location sensor and a temperature sensor may be programmed to send temperature data when the tag is within a certain geographic area. In another embodiment, where a tag includes a biometric sensor it can be programmed with codes representative of individuals likely to employ the sensor. As an another example, a tag with a temperature sensor, humidity sensor and pressure sensor may be programmed to
10 send pressure data only if the temperature measurement and the humidity measurement falls within a preconfigured range.

The programming interface 604 typically includes a reed switch circuit, or suitable alternative device, representing an external programming interface via which the user can
15 program aspects of the tag directly, namely without necessarily programming via the reader network. In alternative embodiments, the tag programming interface 604 may include an RF receiver module capable of operating at a different frequency to the main RF module 609 of the tag (for example so called “dual band” tags). In this case it is possible to program tags, or to re-program them, remotely, i.e. through the reader network.

20

In general, any suitable modulation technique may be used over the wireless interface 112 between the tags 105 and readers 103. In this embodiment, amplitude shift keying ASK is used (with a modulation depth of 90%). However, any other suitable modulation technique may be used, for example FSK QPSK, BPSK and the like. Further aspects of the wireless
25 tag-reader protocol are defined herein below with reference to Fig. 7. Aside from synchronisation information, tag message packets tend to include: a header 702 indicating the message is a tag and its length; a tag class field 704 (which may also indicate a tag type within a class and/or a particular mode of operation), a tag unique ID field 706, a data field

5 710, and error checking information 712. In practice, the overall length of the message and configuration of the various fields within it will depend for example on the tag class.

Synchronisation information is required because in the exemplary embodiment, the wireless channel between the tag and reader is asynchronous. The header information is used
10 to achieve packet level synchronisation and to identify the type of message and its length in bytes. Another example of information typically included in the header is repetition rates for beaconing tags. In general the header information facilitates and optimises decoding of messages and avoids using unnecessary power. The information in the tag class field indicates a class of tag into which the tag falls from a plurality of tag classes, each tag class
15 having predetermined peripheral capabilities and hence a tag message format with corresponding data fields. Optionally, the tag class field can convey additional tag information, such as tag type or model and, where relevant, mode of operation. In this embodiment the tag unique ID is a multi-byte value which is assigned before deployment, for example during manufacturing. The data field contains tag data from the peripherals, which is
20 not user definable as well as tag data which is user definable, as will be described in more detail below. The error checking information is used for packet verification and validation, and may be implemented for example as a 16-bit LRC calculated by linear addition of all relevant bytes. A skilled person will appreciate that the precise tag message packet structures defined herein are exemplary only and for example that some fields are optional and certain
25 “header” or “field” information could feasibly be placed elsewhere or omitted altogether in some embodiments.

5 Fig. 8A-8G shows a plurality of exemplary tag message packet formats, each message packet having a different structure corresponding to the tag class from which the message originates.

With reference to Figure 8A, a first tag message packet (for tag class 1) has a header
10 702, tag class information 704, tag ID 708, and, optionally, error correction information 712. This tag message packet may be sent for example in situations where the tag is required only to provide tag identification under predetermined circumstances. An example is building access applications.

15 With reference to Fig. 8B, a further tag message packet (for tag class 2) has a header 702, tag class information field 704, a tag ID field 708, a data field 710 and error checking information 712. In this case the tag class information indicates that at a predetermined portion of the tag data field is used to report on "tag age" which is estimated by a counter that increments each time the tag transmits. Rather than being a true age based on time, this is in
20 fact a measure of age in terms of the tag life-cycle which is limited in practice by the battery life.

With reference to Fig. 8C, a further tag message packet (for tag class 3) has a header 702, tag class information 704, a tag ID field 708, a data field 710, and error checking
25 information 712. In this case the tag class information 704 indicates that at least a portion of the tag data field 710 is used to convey user defined data of some type. The application program is capable of decoding the user defined data.

5 With reference to Fig. 8D, a further tag message packet (for tag class 4) has a header 702, tag class information 704, a tag ID field 708, a data field 710, and error checking information 712. In this case the tag class information 704 indicates that at least a portion of the tag data field 710 is used to convey a user defined identity code from the tag.

10 With reference to Fig. 8E, a further tag message packet (for tag class 5) has a header 702, tag class information 704, a tag ID field 708, a data field 710, and error checking information 712. In this case the tag class information 704 indicates that predetermined portions of the tag data field 710 are used to convey predetermined peripheral data (P. DATA) and user defined data (USER DATA). The peripheral data may itself have user
15 defined elements. For example this tag message packet might be employed to send data from a tag having a temperature sensor and a user defined identity code.

 With reference to Fig. 8F, a further tag message packet (for tag class 6) has a header 702, tag class information 704, a tag ID field 708, a data field 710, and error checking
20 information 712. In this case the tag class information 704 indicates that predetermined portions of the tag data field 710 are used to convey data from first and second peripherals (P₁ DATA and P₂ DATA). The peripheral data from either peripheral may itself have user defined elements. For example this tag class packet might be employed to send data from a tag having a temperature sensor and a GPS location sensor. An example of peripheral data
25 having user defined elements is where a user has programmed the tag only to report temperature exceeding a predetermined temperature threshold. In this type of packet the tag class information may be supplemented with tag type information which indicates, for example, that the tag has a two sensor functions and is operating in a mode supporting (e.g.

5 temperature and GPS sensors). Either type of peripheral data, or both, may have user defined elements.

With reference to Fig. 8G, a further tag message packet (for tag class 7) has a header 702, tag class information 704, a tag ID field 708, a tag data field 710, and error checking
10 information 712. In this case the tag class information 704 indicates that at predetermined portions of the tag data field 710 is used to convey data from first and second peripherals, and user definable data. For example this tag message packet might be employed to send data from a tag having a chemical sensor, tamper sensor and a user definable identification code. As before, the tag class field may be supplemented by tag type information which indicates,
15 for example, that the tag has a two sensor function and is operating in a mode supporting a specific chemical sensor (say a gas sensor) and tamper sensor with a user definable tag ID code. Data from either or both peripherals may also have user defined elements.

With reference in particular to Fig. 9, which shows a schematic representation of a
20 generalised message packet structure for further potential tag classes, it will be apparent that the tag message packet scheme used in embodiments of the present invention is capable of supporting a number of multi-peripheral tag designs by virtue of a plurality of predetermined tag message packets provided with one or more fields defining the tag class from which the message originates, and optionally also a tag type or mode within that class.

25

Fig. 10 illustrates by means of an exemplary process chart how tag data is conveyed from the tag to the application program in embodiments of the present invention.

At 1000, the tag microprocessor initiates a tag message send process. For example, this may be in response to a reader inquiry or it may be under a type of beaconing regime

5 known in the RFID arts. At 1010, the microprocessor builds a message packet of a suitable type based on the tag class. In this example it is assumed that the tag message packet will adopt a format 1012 corresponding to a predetermined tag class from the number of possible tag classes (see Fig. 8) and extends to a total of packet length of 64 bytes. Relevant system information 1014 and tag data 1016 (including peripheral data and user defined data as may
10 be appropriate) is sourced from the tag memory and the message packet is constructed accordingly. The tag message packet is provided to the analogue transmission circuitry including the RF oscillator and the antenna and transmitted 1020 over the air interface 112 to a reader 103.

15 At 1030 the reader receives the tag message packet and processes it as necessary to convert it from analogue to digital format. The microprocessor of the reader then builds a reader network response type packet (or a general reader network packet of similar construction) 1032 and queues it in a reader buffer for transmission over the reader network to the application 120 of the control interface 100. For this building process the reader uses
20 the appropriate reader network format message format 1032 (see Fig. 5) which in this embodiment incorporates the tag message packet 1034 in its entirety. At 1040, the reader network sends the reader network message packet to the application program in accordance with the reader network backbone communication protocol.

25 Further it will be apparent that the described embodiment is useful in particular with tags having multiple sensors and the like, and which also permit user definable data to be programmed. The user definable data can be either independent of the peripheral function(s) or for controlling one or more aspects of the peripheral sensing or reporting functions.

5 In summary embodiments provide, among other things a functionally rich and versatile tag-reader communications protocol, capable of scalable deployment to support a wide range of current and future applications. At the same time embodiments described here achieve high data throughput and interoperability, whilst minimising power consumption.

10 Those skilled in the art will appreciate that while the foregoing has described what is considered to be the best mode and, where appropriate, other modes of performing the invention, the invention should not be limited to the specific configurations and methods disclosed in this description of the preferred embodiment. Those skilled in the art will recognise that the invention has a broad range of applications in many different types of
15 remote identification, data and sensor applications, and that the embodiments may take a wide range of modifications without departing from the inventive concept as defined in the appended claims. For example, the invention has applications in all manner of asset management, personal management, supply chain management and process control applications in various fields of operation such as industrial, medical, military, home, office
20 and other.

5 CLAIM:

1. An active transponder for use in an RFID network comprising transponders and networked reader units for receiving messages from the transponders, the transponder comprising:

transmission circuitry;

10 a controller having access to a memory;

a power supply;

wherein the controller comprises control code for constructing a message packet corresponding to a transponder class to which the transponder belongs, said class of transponders being one of a plurality of classes each characterised by aspects of the configuration of peripheral devices of transponders in that class, and wherein the controller further comprises means adapted to include in said message packet an indication the message packet is a message from a transponder and an indication of the class of transponder from which the message originates, and one or more peripheral data fields according to the message packet structure of the transponder class.

20 2. A transponder as in claim 1, wherein the message packet comprises at least one user defined data field.

3. A transponder as in any preceding claim, wherein the content of a peripheral data field is at least partly defined by a user.

4. A transponder as in any preceding claim, wherein the transponder comprises an external programming interface capable of allowing direct programming of the transponder, without programming via a reader unit.

5. A transponder as in any of claims 1 to 3, wherein the transponder comprises a programming interface capable of allowing programming of the transponder via a reader unit.

6. A transponder as in any preceding claim, wherein the transponder comprises two or more peripheral devices comprising one or more of a counter and a sensor.

30

- 5 7. A transponder as in any preceding claim, wherein the transponder comprises two or more sensors selected from one or more of: a temperature sensor; a location sensor; a movement sensor; a vibration sensor; a seismic sensor; a magnetic sensor; a force sensor; a strain sensor; a rotary sensor; a pressure sensor; a tamper sensor; another type of mechanical sensor; a chemical sensor; a biochemical; a biological sensor; a biometric sensor; a proximity
10 sensor; humidity sensor; a position sensor; a light sensor; and other suitable types of sensors.
8. A transponder as in claim 1, wherein the transponder comprises at least a movement sensor and a tamper sensor.
9. A transponder as in the claim 1, wherein the transponder comprises at least a tamper sensor and a temperature sensor.
- 15 10. A transponder as in claim 1, wherein the transponder comprises at least a location sensor, a movement sensor and a temperature sensor.
11. A transponder as in any preceding claim, wherein the transmission circuitry is arranged to operate at one or more of the following ranges: 30 to 300kHz; 300kHz to 3 MHz; 3 MHz to 300 MHz; 300 MHz to 2 GHz; and 2 GHz to 6 GHz.
- 20 12. A transponder as in any preceding claim, wherein the transmission circuitry is arranged to operate at one or more of: 125 KHz; 134.2 KHz; 13.56 MHz; 433 MHz; 463 MHz; 868 MHz; 915 MHz; 956 MHz; 2.45 GHz and 5.8 GHz.
13. A method of generating a transponder message in an RFID network comprising active transponders and networked reader units, the method comprising:
- 25 providing a plurality of transponders and allocating the transponders into predefined classes based on aspects of peripheral configurations of the transponders;
- establishing a predetermined format for a message packet applying to each predefined class of transponder such that each of the plurality of predefined transponder classes has a predetermined message packet structure according to the configuration of peripherals of
30 transponders in that class;
- building a message packet based on said established message format, the message packet including an indication the message is a transponder message, an indication of the

- 5 class of the transponder from which the message originates, and one or more peripheral data fields.
14. A method as in claim 13, wherein the message packet includes user data field.
15. A method as in claim 13 or 14, wherein the contents of a peripheral data field may be defined at least in part by a user.
- 10 16. A method as in any of claims 13 to 15, wherein the method further comprises programming one or more of: a peripheral function of the transponder; a reporting function of the transponder; and user data on the transponder, by means of a programming interface.
17. A method as in any of claims 13 to 16, wherein the transponder comprises two or more peripherals, at least one of which is a sensor and the message packet includes a
15 corresponding number of peripheral data fields.
18. A method as in any of claims 13 to 17, wherein the transponder comprises a plurality of peripheral sensors and the message packet includes a corresponding plurality of peripheral data fields.
19. A method as in any of claims 13 to 18, wherein the message packet includes a
20 transponder identity field.
20. A method as in any of claims 13 to 19, wherein the message includes an error checking field.
21. A method as in claim 13, wherein in at least one mode of operation the transponder transmits in response to a predetermined criterion.
- 25 22. A method as in claim 21, wherein said criterion comprises receipt of a message from a reader requesting a response from the transponder.
23. A method as in claim 21, wherein said criterion comprises a predetermined delay from receipt of a message from a reader.
24. A method as in any of claims 13 to 20, wherein in at least one mode of operation the
30 transponder transmits only after predetermined intervals.

- 5 25. A method as in any of claims 13 to 20, wherein in at least one mode of operation the transponder transmits in a time slot allocated to it via a reader unit.
26. A method as in any of claims 13 to 20, wherein the transponder transmits based on a frequency hopping algorithm.
27. A method as in any of claims 13 to 26, wherein the transponder receives and
10 responds to a message from a reader selected from one or more of the following types: get tag data; tag wake up; tag sleep; set tag mode of operation; set tag peripheral function; set tag reporting function; set tag alarm criteria; set tag user information.
28. A transponder message packet format for message packets sent by a transponder to a reader unit in an RFID network, comprising:
- 15 a message packet type field indicating the message is a transponder message;
- a transponder class field indicating a transponder class from a plurality of predefined transponder classes to which the transponder belongs;
- a plurality of peripheral data fields and, optionally, a user data field according to a predefined message format for the class to which the transponder belongs.
- 20 29. A transponder message format as in claim 28, comprising a further field for user definable peripheral data.
30. A transponder message format as in claim 28 or 29, comprising a further field selected from one or more of: a tag ID field; a network information field; and an error correction field.
- 25 31. A set of transponder message formats for use in an RFID network, the set of message formats comprising:
- a plurality of message formats each comprising a transponder type field, indicating the message is a transponder message, and a transponder class field, indicating the class of transponder from which the message originates, and wherein a message format has a
30 different predetermined peripheral data field configuration in dependence on the transponder class from which the message originates.

5 32. A set of messages as in claim 31, wherein each message format of the plurality of message formats has different predetermined peripheral data field configuration in dependence on the transponder class.

33. A set of messages as in claim 31 or 32, wherein said peripheral data fields comprise a plurality of sensor fields each for carrying data from a different type of sensor on a multi-
10 functional transponder.

34. A reader unit capable of constructing a network message comprising a transponder data field for content from a transponder message, wherein substantially the entirety of transponder message is incorporated into a transponder data field of the network message.

15