US009270341B2

(12) **United States Patent**
Vaucher et al.

(10) **Patent No.: US 9,270,341 B2**
(45) **Date of Patent: Feb. 23, 2016**

(54) **WIRELESS POWER AND DATA CONNECTOR**

(71) Applicant: **NXP B.V.**, Eindhoven (NL)

(72) Inventors: **Cicero Silveira Vaucher**, Eindhoven (NL); **Raf Lodewijk Jan Roovers**, Eindhoven (NL)

(73) Assignee: **NXP B.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 165 days.

(21) Appl. No.: **14/180,174**

(22) Filed: **Feb. 13, 2014**

(65) **Prior Publication Data**

US 2014/0235164 A1 Aug. 21, 2014

(30) **Foreign Application Priority Data**

Feb. 21, 2013 (EP) 13156226

(51) **Int. Cl.**

H04B 5/00	(2006.01)
H04W 4/00	(2009.01)
H04W 92/00	(2009.01)
H02J 17/00	(2006.01)
H02J 7/02	(2006.01)
H02J 7/00	(2006.01)

(52) **U.S. Cl.**

CPC ***H04B 5/0031*** (2013.01); ***H02J 17/00*** (2013.01); ***H04B 5/0037*** (2013.01); *H02J 7/025* (2013.01); *H02J 2007/0001* (2013.01)

(58) **Field of Classification Search**

USPC 455/41.1, 41.2, 414.1, 420

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0143702	A1	6/2011	Hosokawa	
2011/0243702	A1	10/2011	Nakanishi et al.	
2013/0005246	A1 *	1/2013	Waters	H04B 5/02 455/41.1
2013/0029595	A1 *	1/2013	Widmer	H04B 5/0031 455/39
2013/0029597	A1	1/2013	Liu et al.	
2013/0262305	A1 *	10/2013	Jones	H04B 5/0031 705/44

FOREIGN PATENT DOCUMENTS

CN	102437626 A	1/2013	

OTHER PUBLICATIONS

Integrated Device Technology "IDT Wireless Power—IDPT9030, IDPT9020", 2 pgs.

Extended European Search Report for EP Patent Appln. No. 13156226.6 (Jul. 15, 2013).

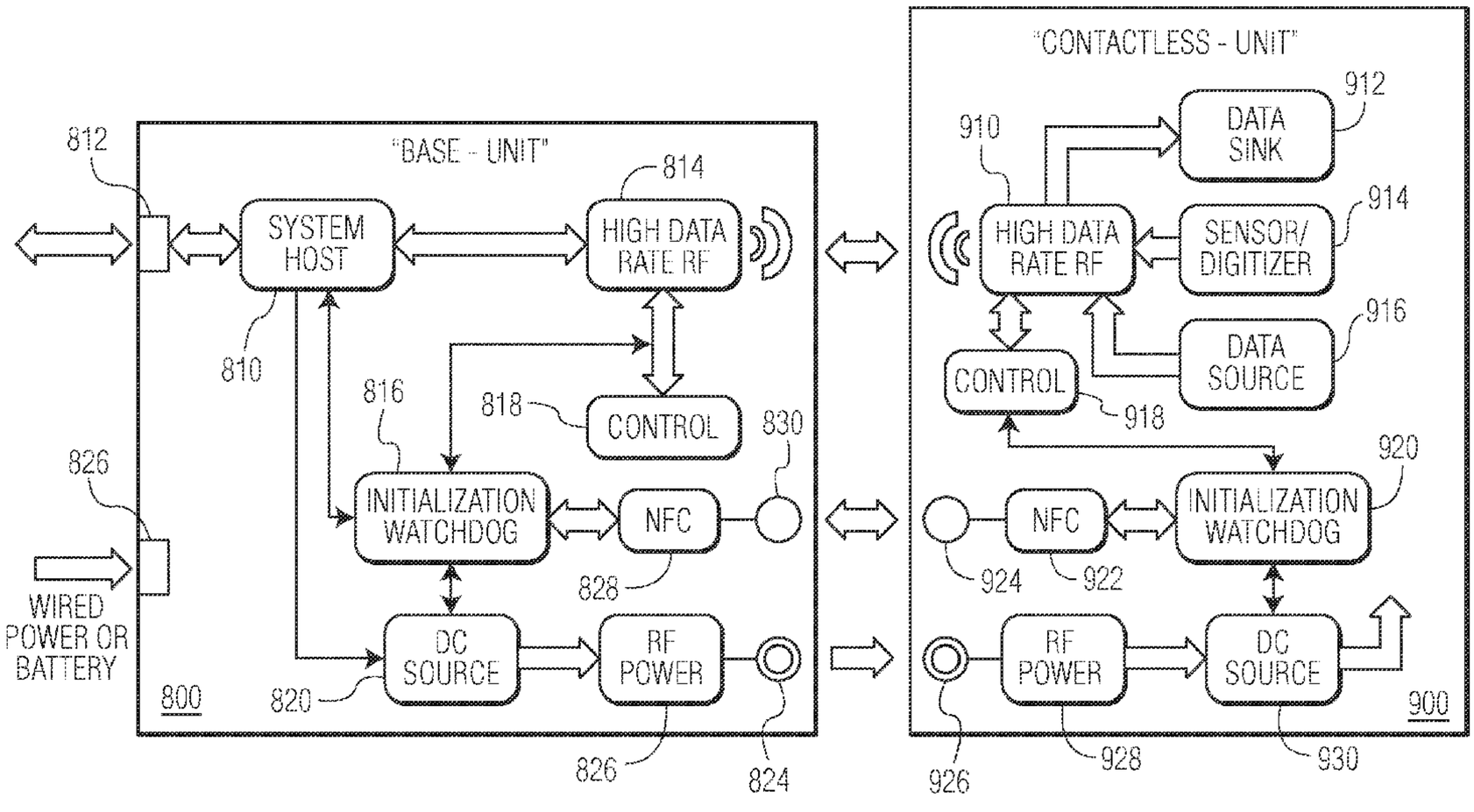
* cited by examiner

Primary Examiner — Blane J Jackson

(57) **ABSTRACT**

An apparatus for non-galvanic connection between two electrical circuits is described. A base-unit has an RF power source, a data link and an authentication controller. A contactless unit for communication with a base unit has an RF power receiver, a data link and an authentication controller. The base unit and contactless unit can form a non-galvanic connection to replace conventional connectors, for example in a USB wired bus connection.

16 Claims, 7 Drawing Sheets



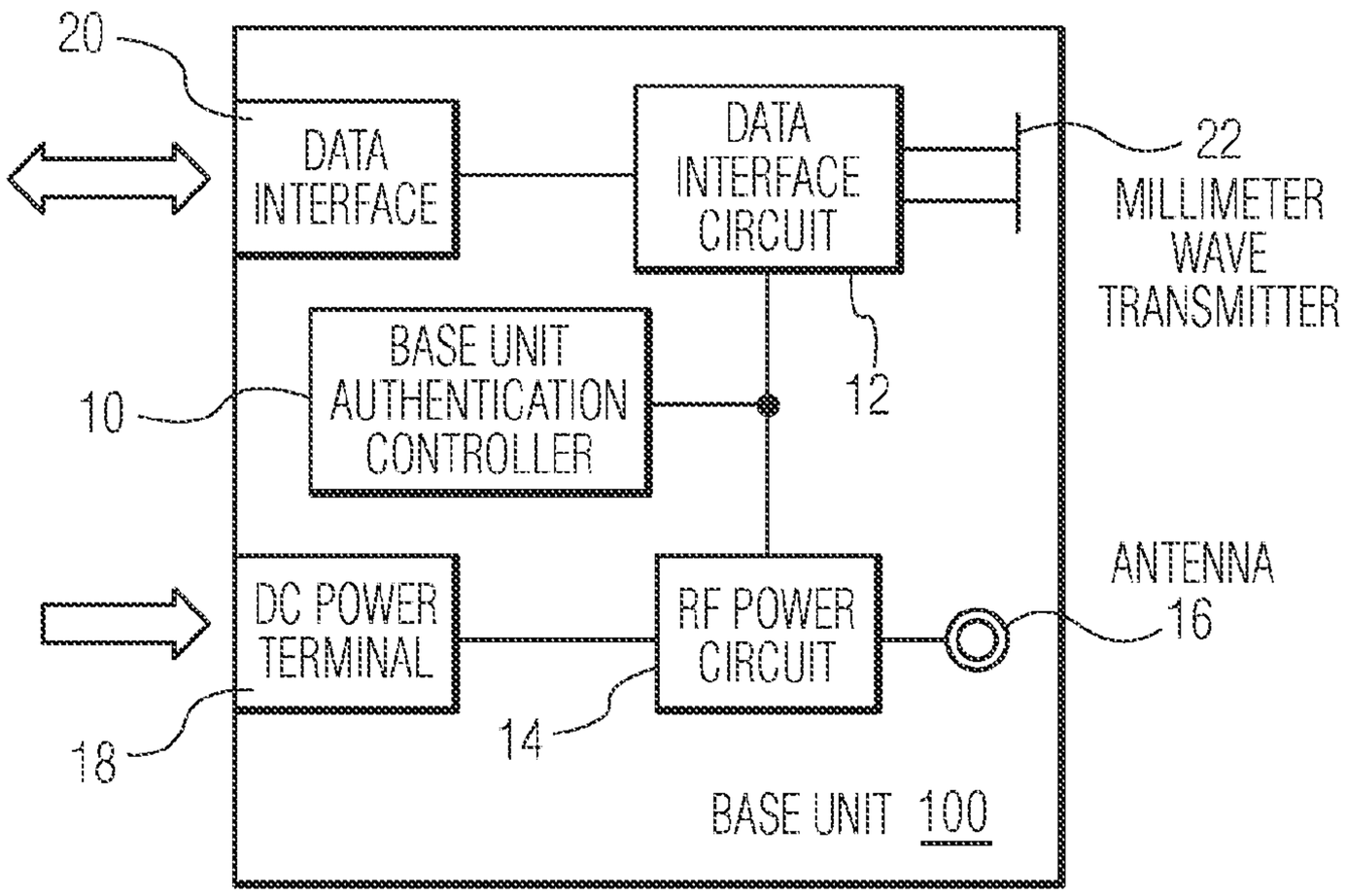

20
DATA INTERFACE
DATA INTERFACE CIRCUIT
22
MILLIMETER WAVE TRANSMITTER
BASE UNIT AUTHENTICATION CONTROLLER
10
12
DC POWER TERMINAL
RF POWER CIRCUIT
ANTENNA 16
18
14
BASE UNIT 100

FIG. 1

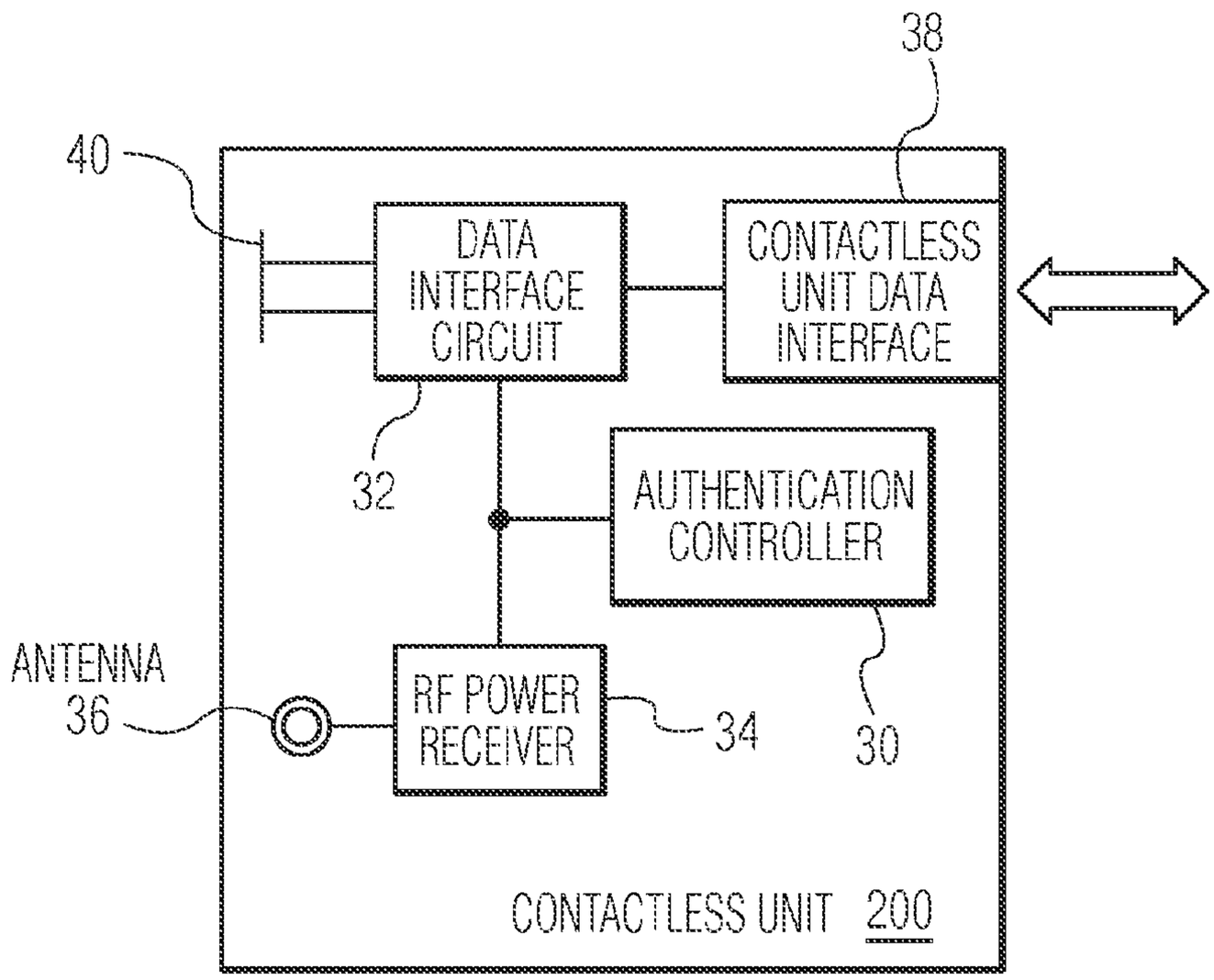

38
40
DATA INTERFACE CIRCUIT
CONTACTLESS UNIT DATA INTERFACE
32
AUTHENTICATION CONTROLLER
ANTENNA 36
RF POWER RECEIVER
34
30
CONTACTLESS UNIT 200

FIG. 2

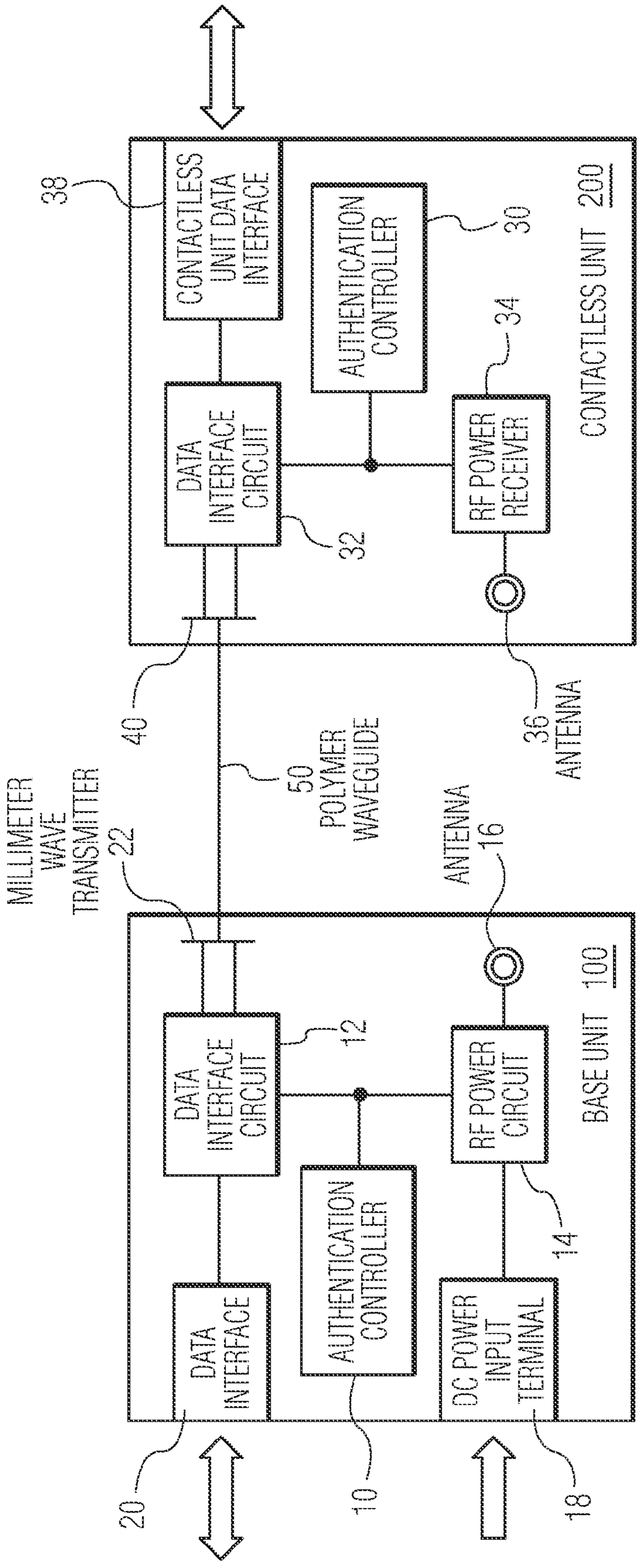

MILLIMETER WAVE TRANSMITTER
22
DATA INTERFACE
20
AUTHENTICATION CONTROLLER
10
DC POWER INPUT TERMINAL
18
RF POWER CIRCUIT
14
BASE UNIT 100
DATA INTERFACE CIRCUIT
12
ANTENNA
16
50 POLYMER WAVEGUIDE
40
DATA INTERFACE CIRCUIT
32
AUTHENTICATION CONTROLLER
30
RF POWER RECEIVER
34
CONTACTLESS UNIT 200
36 ANTENNA
CONTACTLESS UNIT DATA INTERFACE
38

FIG. 3

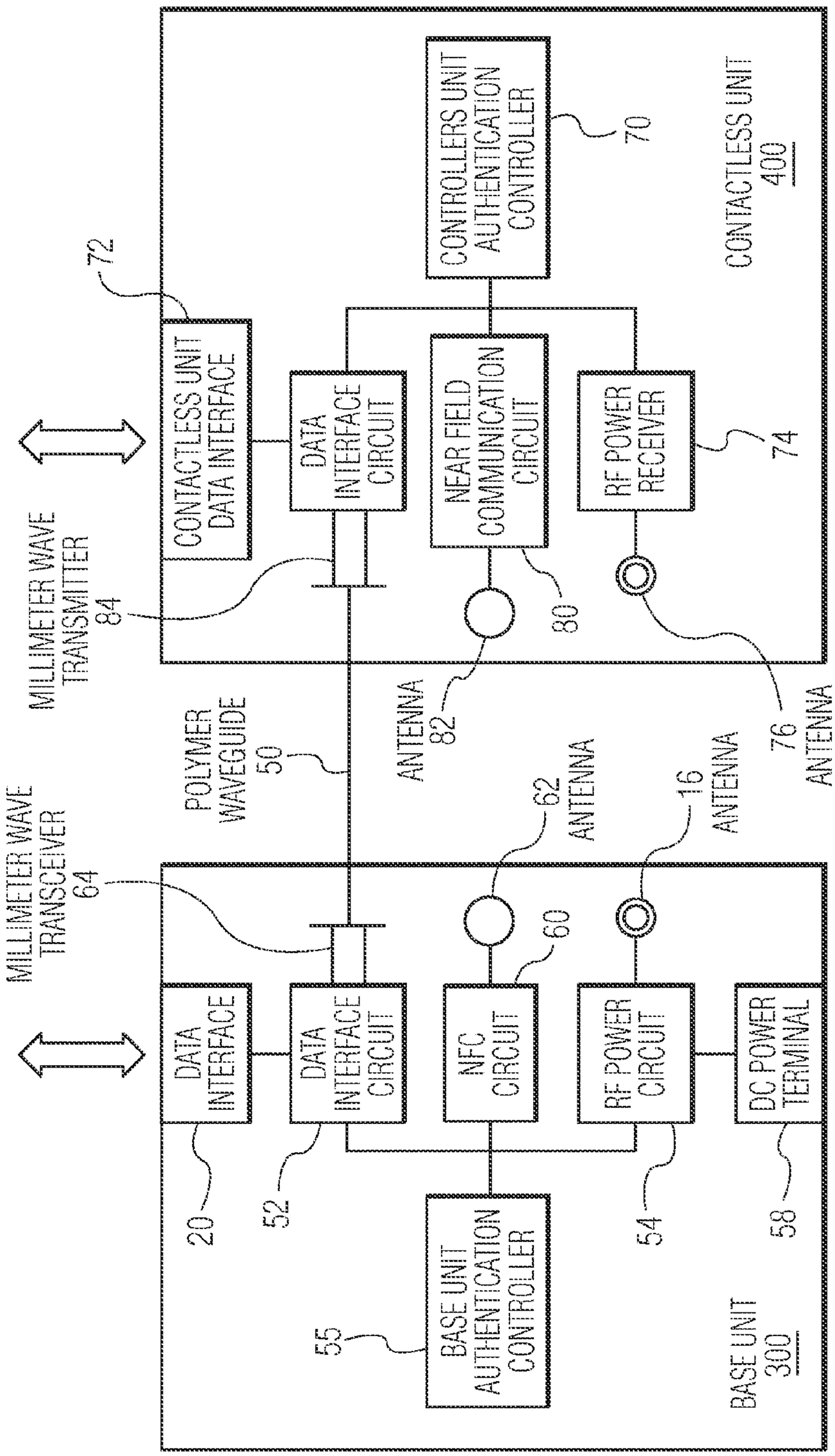

CONTACTLESS UNIT
400
CONTROLLERS UNIT AUTHENTICATION CONTROLLER
70
72
CONTACTLESS UNIT DATA INTERFACE
DATA INTERFACE CIRCUIT
NEAR FIELD COMMUNICATION CIRCUIT
RF POWER RECEIVER
74
MILLIMETER WAVE TRANSMITTER
84
POLYMER WAVEGUIDE
50
ANTENNA
82
80
76
ANTENNA
MILLIMETER WAVE TRANSCEIVER
64
62
ANTENNA
16
ANTENNA
DATA INTERFACE
DATA INTERFACE CIRCUIT
NFC CIRCUIT
60
RF POWER CIRCUIT
DC POWER TERMINAL
20
52
54
58
55
BASE UNIT AUTHENTICATION CONTROLLER
BASE UNIT
300

FIG. 4

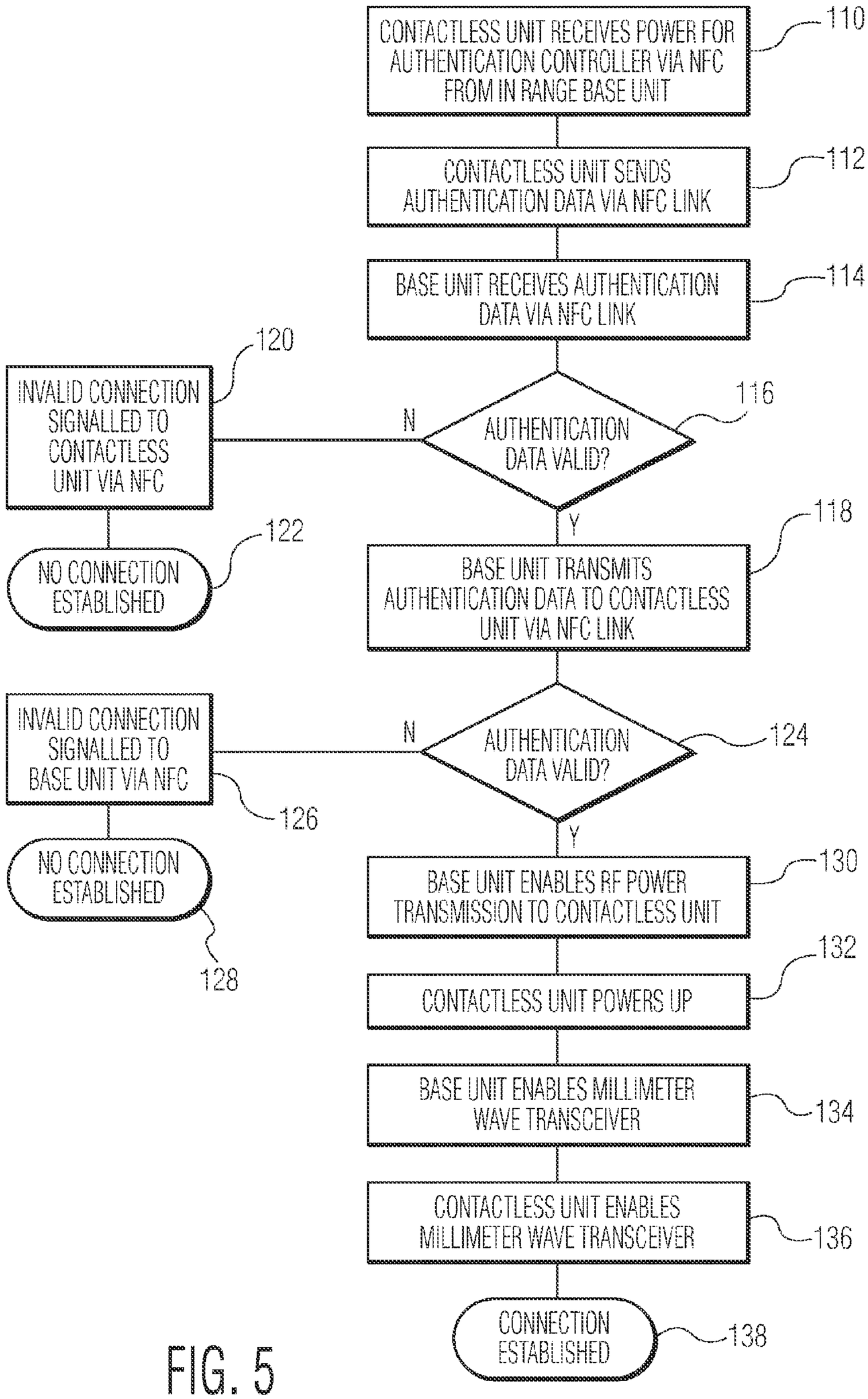

CONTACTLESS UNIT RECEIVES POWER FOR AUTHENTICATION CONTROLLER VIA NFC FROM IN RANGE BASE UNIT
110
CONTACTLESS UNIT SENDS AUTHENTICATION DATA VIA NFC LINK
112
BASE UNIT RECEIVES AUTHENTICATION DATA VIA NFC LINK
114
AUTHENTICATION DATA VALID?
116
N
Y
INVALID CONNECTION SIGNALLED TO CONTACTLESS UNIT VIA NFC
120
NO CONNECTION ESTABLISHED
122
BASE UNIT TRANSMITS AUTHENTICATION DATA TO CONTACTLESS UNIT VIA NFC LINK
118
AUTHENTICATION DATA VALID?
124
N
Y
INVALID CONNECTION SIGNALLED TO BASE UNIT VIA NFC
126
NO CONNECTION ESTABLISHED
128
BASE UNIT ENABLES RF POWER TRANSMISSION TO CONTACTLESS UNIT
130
CONTACTLESS UNIT POWERS UP
132
BASE UNIT ENABLES MILLIMETER WAVE TRANSCEIVER
134
CONTACTLESS UNIT ENABLES MILLIMETER WAVE TRANSCEIVER
136
CONNECTION ESTABLISHED
138

FIG. 5

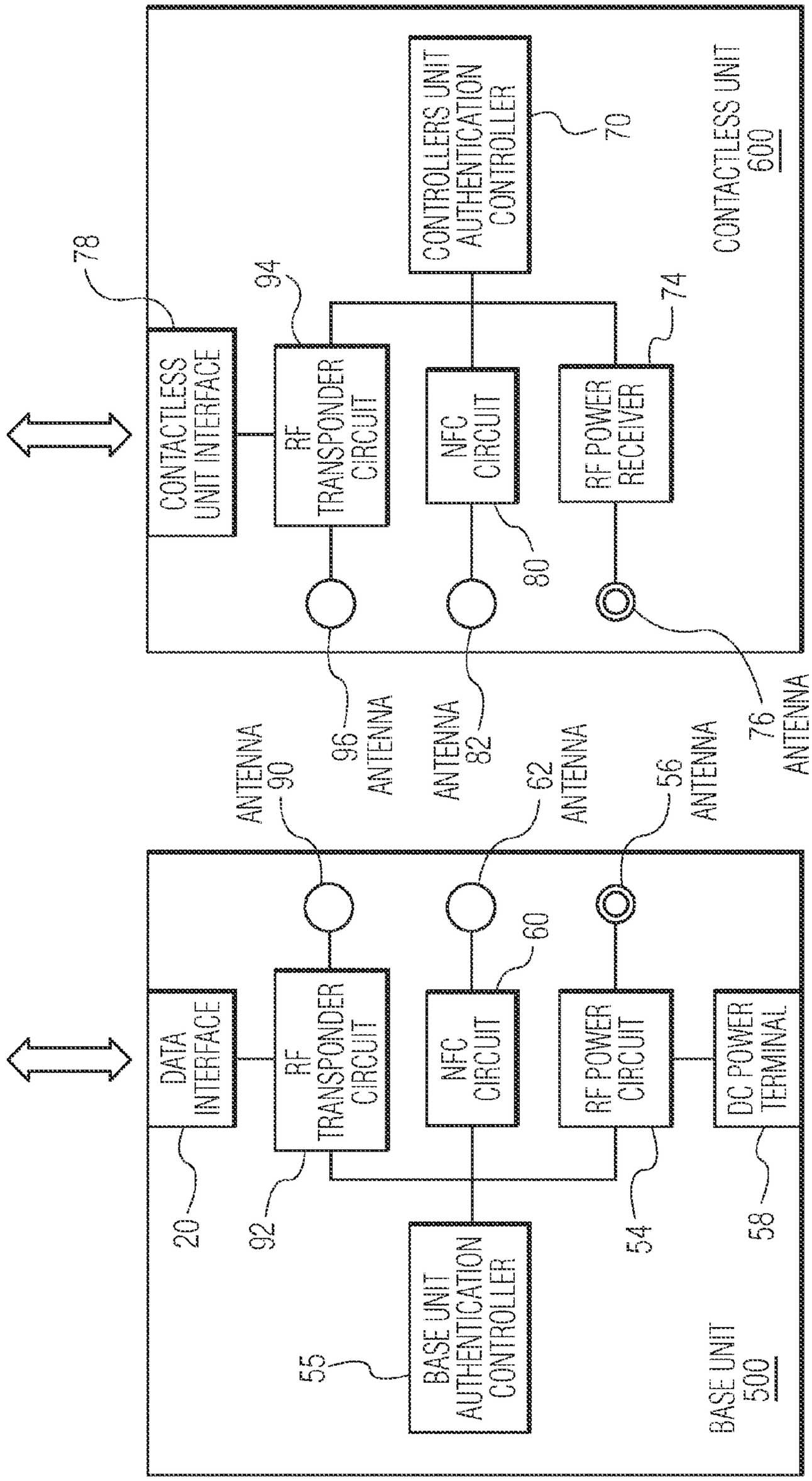

CONTACTLESS UNIT
600
CONTROLLERS UNIT AUTHENTICATION CONTROLLER
70
78
94
74
CONTACTLESS UNIT INTERFACE
RF TRANSPONDER CIRCUIT
NFC CIRCUIT
RF POWER RECEIVER
80
96 ANTENNA
ANTENNA 82
76 ANTENNA
ANTENNA 90
62 ANTENNA
56 ANTENNA
60
DATA INTERFACE
RF TRANSPONDER CIRCUIT
NFC CIRCUIT
RF POWER CIRCUIT
DC POWER TERMINAL
20
92
54
58
55
BASE UNIT AUTHENTICATION CONTROLLER
BASE UNIT
500

FIG. 6

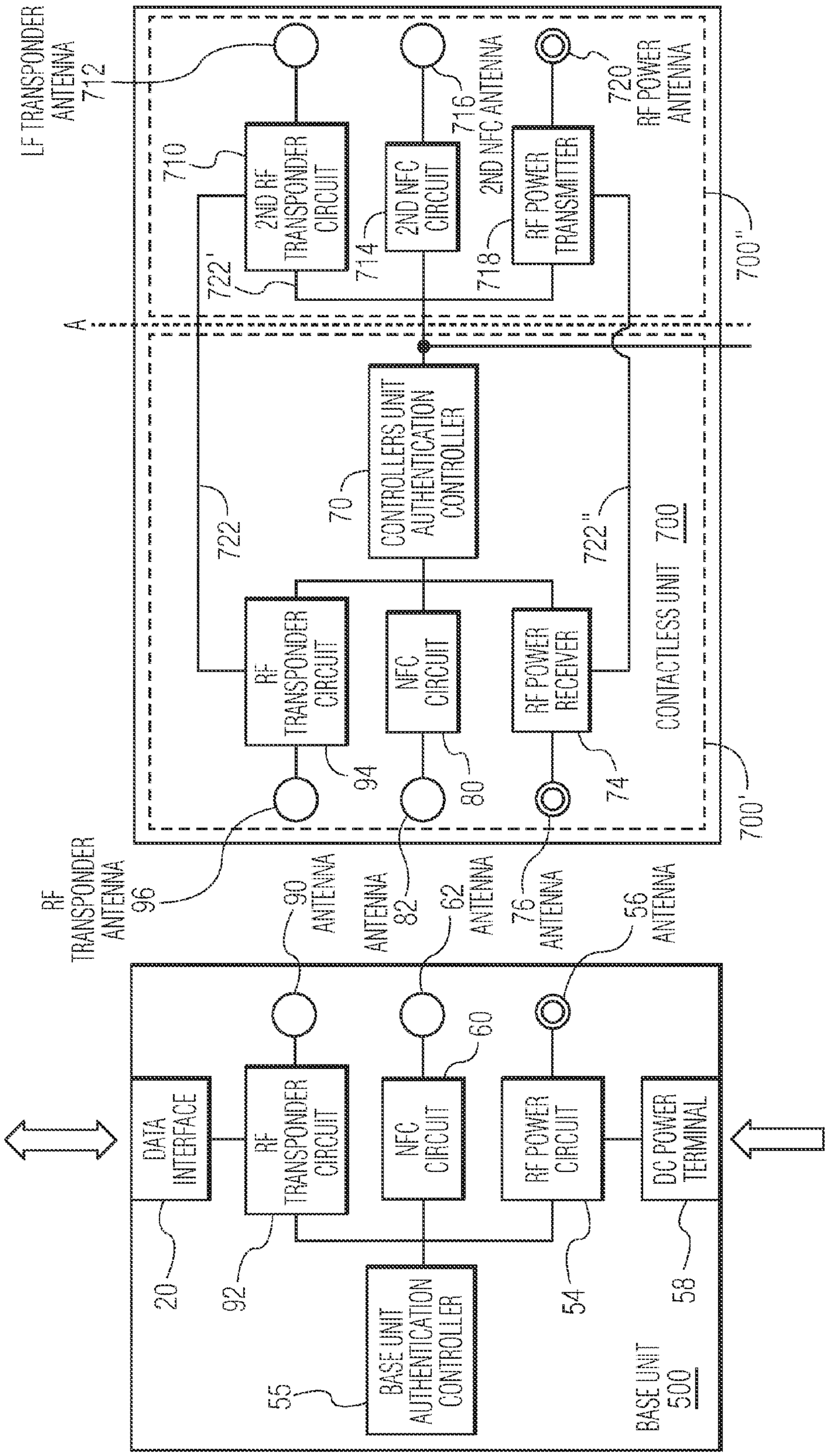

LF TRANSPONDER ANTENNA 712
710
2ND RF TRANSPONDER CIRCUIT
714
2ND NFC CIRCUIT
716
2ND NFC ANTENNA
718
RF POWER TRANSMITTER
720
RF POWER ANTENNA
700''
722'
722
70
CONTROLLERS UNIT AUTHENTICATION CONTROLLER
722''
RF TRANSPONDER CIRCUIT
NFC CIRCUIT
RF POWER RECEIVER
CONTACTLESS UNIT 700
94
80
74
700'
RF TRANSPONDER ANTENNA 96
90 ANTENNA
ANTENNA 82
62 ANTENNA
76 ANTENNA
56 ANTENNA
DATA INTERFACE
RF TRANSPONDER CIRCUIT
NFC CIRCUIT
RF POWER CIRCUIT
DC POWER TERMINAL
60
20
92
54
58
55
BASE UNIT AUTHENTICATION CONTROLLER
BASE UNIT 500

FIG. 7

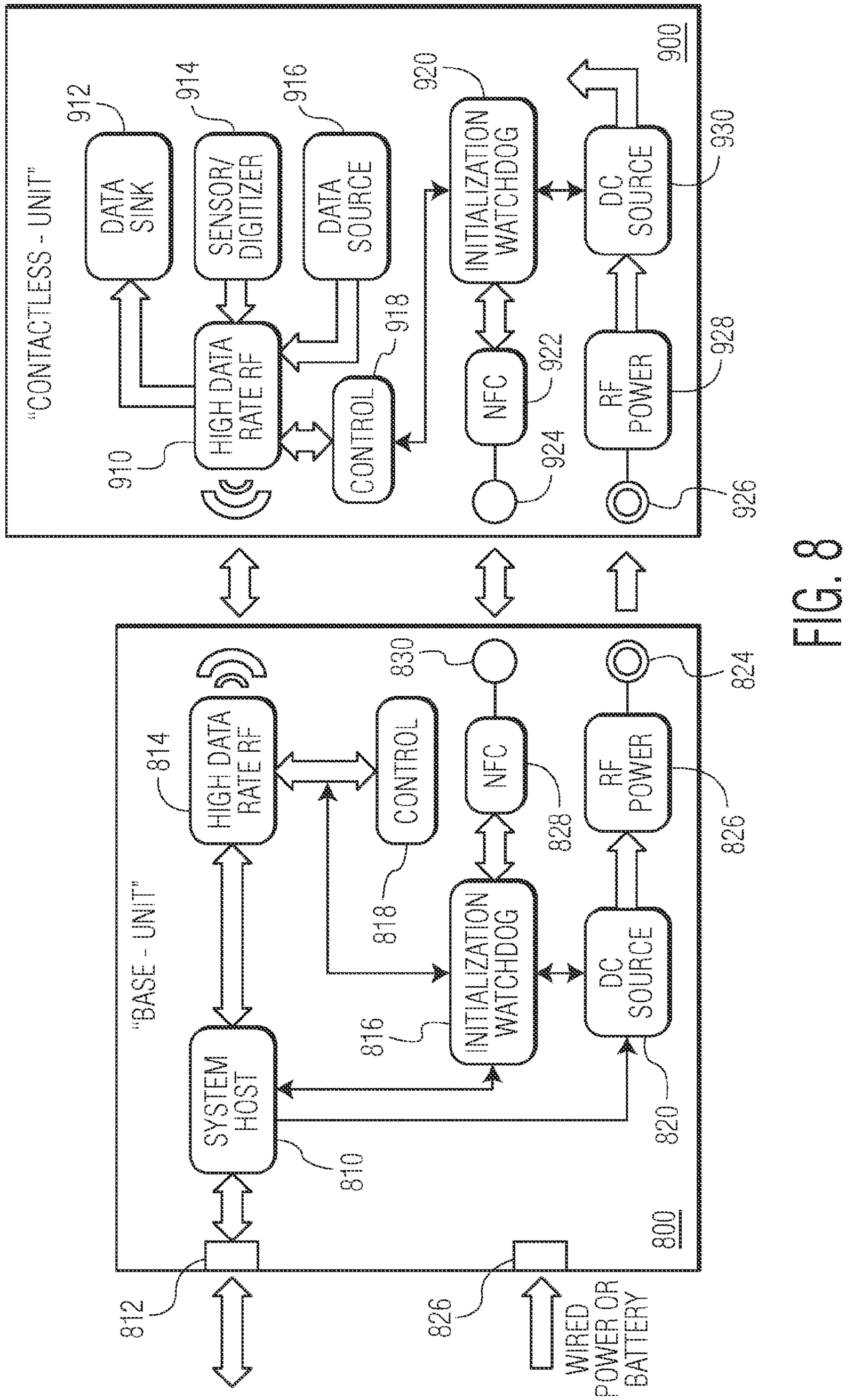

"CONTACTLESS - UNIT"
912
DATA SINK
914
SENSOR/ DIGITIZER
916
DATA SOURCE
920
INITIALIZATION WATCHDOG
900
930
DC SOURCE
910
HIGH DATA RATE RF
CONTROL
918
NFC
922
924
RF POWER
928
926
"BASE - UNIT"
814
HIGH DATA RATE RF
CONTROL
830
NFC
828
RF POWER
824
826
818
816
INITIALIZATION WATCHDOG
DC SOURCE
SYSTEM HOST
810
820
800
812
826
WIRED POWER OR BATTERY

FIG. 8

WIRELESS POWER AND DATA CONNECTOR

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the priority under 35 U.S.C. §119 of European patent application no. 13156226.6, filed on Feb. 21, 2013, the contents of which are incorporated by reference herein.

This invention relates to an apparatus for non-galvanic connection between two or more electrical circuits.

Galvanic connectors are widely used in electronic systems. An example of a galvanic connection is a peripheral device connected via an USB cable to a host device. In the most general case the host provides power to the peripheral device via the USB cable, and bi-directional high-speed data communication takes place across the same cable; in USB2.0 a separate pair of wires is allocated to power and data transfer. The galvanic connection via a cable forms an ohmic contact allowing a high degree of communication reliability between the host and the peripheral device whence the connection is made by plugging the cable into the USB port.

However, galvanic connectors are prone to wear and tear leading to functional failure consequence for example in a USB connection due to repeatedly plugging and unplugging a USB cable, both in consumer electronics as well as in professional systems. In addition, connectors for high-speed links such as HDMI and high-pin count applications such as docking station for a laptop increase the cost of the system considerably.

Consumer electronics systems show reliability problems with galvanic connectors, for example SD memory cards that get damaged due to mechanical stress during socket insertion and ejection.

Professional applications include reconfigurable MRI scanners and systems with moving parts such as wafer steppers. In these examples there is a large amount of data to be transferred from the MRI sensor/digitizer and from the wafer stage towards a central processing unit or host, in addition to the power function. The connectors tend to get dirty and/or break after a limited operation time, increasing machine down-time and maintenance cost for equipment owners.

Physical connectors also may limit the operational design freedom in industrial production lines, for example in conveyor belt systems.

Various aspects of the invention are defined in the accompanying claims. In a first aspect there is defined a base-unit for non-galvanic coupling to a contactless-unit, the base-unit comprising an antenna coupled to a radio frequency (RF) power source, at least one data-link, an authentication controller coupled to the at least one data-link, and a data interface for coupling at least one of a data source and data sink to the base unit, the data interface being coupled to the at least one data-link wherein the base-unit is operable to transmit and/or receive payload data via the data interface, wirelessly transmit RF power from the RF power source to a contactless-unit in physical proximity to the base-unit, transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a contactless-unit only when the contactless-unit is in physical proximity to the base-unit, and transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a contactless unit.

The replacement of the galvanic connection with a non-galvanic connection provides an increased level of robustness. The authentication controller provides an equivalent level of security as provided by a wired connection using a galvanic connector and ensures that the connection is formed between the base unit and the contactless unit only when intended. To be considered to be in physical proximity, the base unit should be within a distance of one meter of a contactless unit.

The term antenna may also be considered to include an inductor, a coil or other element capable of magnetic or electromagnetic coupling. Payload data may be considered to include any data other than data used to authenticate the connection. The term RF may include frequencies above 30 KHz.

In an embodiment of the base-unit, the authentication controller is coupled to the RF power source and the authentication controller is operable to disable RF power transmission if the authentication of the non-galvanic connection fails.

Disabling the power source in the base unit if authentication fails improves the security of the connection.

In an embodiment the authentication controller further comprises a watchdog timer, wherein the base-unit is operable to periodically re-authenticate a non galvanic connection to a contactless-unit, the re-authentication period being determined by the watchdog timer, and to disable further data transmission and/or reception if the re-authentication of the non-galvanic connection fails.

Periodically re-authenticating the connection further improves the security of the connection and provides an equivalent function to a galvanic wired connection being unplugged.

In an embodiment, the base unit may comprise at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the base-unit and a contactless unit non-galvanically coupled to the base unit is fixed.

Embodiments of a base unit may include a mechanical connector or coupling element which plugs into a mechanical connector of a contactless unit or vice versa. This may replace a conventional galvanic connector. Alternatively a ferromagnetic material may be used to magnetically secure the base unit and contactless unit in position such that the data links are physically aligned. The alignment required may be for example alignment of a photo transmitter in a base unit and a photodetector in a contactless unit. The alignment required may be the alignment of antennas or inductive coils between a base unit and contactless unit.

In an embodiment, the at least one data link comprises a first data-link element coupled to the at least one antenna and a second data-link element, the first and second data-link elements being coupled to the authentication controller, wherein the first data-link element comprises a near field communication circuit and the base-unit is operable to transmit and/or receive authentication data via the first data-link element to authenticate a non-galvanic connection to a contactless-unit in physical proximity to the base-unit, and transmit and/or receive data between the base-unit and the contactless-unit via the second data link element following the authentication of the non-galvanic connection via the first data-link element.

In embodiments using near field communication, the authentication controller may be coupled to the RF power source and wherein the authentication controller is operable to enable the RF power transmission following the authentication of the non-galvanic connection. Sufficient power to authenticate the connection may be supplied via the near field communication (NFC) data link. Following successful authentication the main power source can be enabled. This can reduce the power consumption of the base unit and also improve the security of the non galvanic connection.

In some embodiments the data-link may comprise a laser configured for optical data transmission and a photodetector for data reception, or a millimeter wave transmitter for data transmission and a millimeter wave receiver for data reception. Data transmission via optical or millimeter waves does not require a galvanic connection. A polymer waveguide can be used as an additional pipe offering high-speed data-communication, which may be at data rates up to many gigabits per second, across longer distances between the base-unit and the contactless-unit; for these embodiments, the link may not be considered as wireless in the most general sense of the word; however there is no reliance on galvanic connections to accomplish data transfer.

In embodiments, the base-unit may include a first antenna coupled to the RF power source, a second antenna coupled to the first data link and a third antenna coupled to the second data-link and wherein the second data link element is configured for RF transmission and/or reception. The second data link may comprise a third antenna coupled to at least one of an RF transmitter and an RF receiver.

In a second aspect there is described a contactless-unit for non-galvanic coupling to a base-unit, the contactless-unit comprising an antenna coupled to an RF power receiver, at least one data-link, and an authentication controller coupled to the at least one data-link, a data interface for coupling at least one of a data source and data sink to the contactless unit, the data interface being coupled to the at least one data-link, wherein the contactless-unit is operable to transmit and/or receive payload data via the data interface, receive RF power provided from a base-unit only when the base-unit is in physical proximity to the contactless-unit, convert the received RF power to supply power to circuits in the contactless-unit, transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a base-unit only when a base-unit is in physical proximity to the contactless-unit, and transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a base unit.

The features of the contactless unit are complementary to a base unit and allow a non-galvanic connection to transfer data and power between two or more circuits.

In an embodiment of the contactless-unit, the authentication controller further comprises a watchdog timer operable to periodically re-authenticate a non galvanic connection to a base-unit, the re-authentication period being determined by the watchdog timer, and to disable further data transmission and/or reception if the re-authentication of the non-galvanic connection fails.

In an embodiment, the contactless-unit comprises at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the contactless-unit and a base unit non-galvanically coupled to the contactless unit is fixed.

In an embodiment of the contactless unit, the at least one data-link comprises at least one of a millimeter wave transmitter, a millimeter wave receiver, a laser, and a photodetector.

In an embodiment of the contactless-unit the at least one data link comprises a first data-link and a second data-link, the first and second data-links being coupled to the authentication controller, wherein the first data-link comprises a second antenna coupled to a near field communication circuit and the contactless-unit is operable to transmit and/or receive authentication data via the first data-link to authenticate a non-galvanic connection to a base-unit only when the base unit is placed in physical proximity to the contactless-unit, and transmit and/or receive payload data via the second data link following the authentication of the non-galvanic connection to a base unit via the first data-link.

In embodiments the contactless-unit includes a third data-link coupled to the authentication controller, the third data-link comprising a near field communication circuit coupled to a fourth antenna, a fourth data-link coupled to the authentication controller, a fifth antenna coupled to an RF power source wherein the contactless-unit is further operable to transmit RF power to a further contactless-unit in physical proximity to the contactless unit, transmit and/or receive authentication data via the third data-link to authenticate a non-galvanic connection to a further contactless-unit only when the further contactless-unit is in physical proximity to the contactless-unit, and transmit and/or receive data between the contactless-unit and the further contactless-unit via the fourth data link element following the authentication of the non-galvanic connection.

Having a third and fourth data links allows daisy chaining of a base unit and multiple contactless units

In an embodiment the contactless unit may include at least one of a sensor (and a storage element coupled to the data interface.

In an embodiment, a second data link of the contactless unit may comprise a third antenna coupled to at least one of an RF transmitter and an RF receiver.

Embodiments of the invention are now described in detail, by way of example only, illustrated by the accompanying drawings in which:

FIG. **1** shows a base unit according to an embodiment.

FIG. **2** illustrates a contactless unit according to an embodiment.

FIG. **3** shows a base unit of the embodiment of FIG. **1** coupled to a contactless unit of the embodiment of FIG. **2**.

FIG. **4** illustrates a base unit and a contactless unit according to a further embodiment.

FIG. **5** shows an example authentication sequence of the embodiment of FIG. **4**.

FIG. **6** shows a base unit and a contactless unit according to a further embodiment.

FIG. **7** illustrates a base unit and a contactless unit according to a further embodiment.

FIG. **8** shows a base unit and a contactless unit according to a further embodiment.

FIG. **1** shows a base unit **100**. Base unit authentication controller **10** is connected to RF power circuit **14**. An output of RF power circuit **14** may be connected to antenna **16**. An input of RF power circuit **14** may be connected to DC power terminal **18**. Data Interface **20** may be connected to data Interface circuit **12**. An output of data interface circuit **12** may be connected to a millimeter wave transmitter **22**. Data interface circuit **12** and millimeter wave transmitter **22** and may form a base unit data link.

FIG. **2** illustrates an embodiment of a contactless unit **200**. Contactless unit authentication controller **30** may be connected to RF power receiver **34**. A terminal of RF power receiver **34** is connected to an antenna **36**. Contactless unit authentication controller **30** may be connected to data interface circuit **32**. A terminal of data interface circuit **32** may be connected to a millimeter wave receiver **40**. Contactless unit authentication controller **30** is connected to data input circuit **32**. An output of contactless unit authentication controller **30** may be connected to contactless unit data interface **38**.

FIG. **3** shows base unit **100** of FIG. **1** connected to a contactless unit **200** of FIG. **2** with a polymer waveguide **50**. The base unit authentication controller **10** may send authentication data at a first data rate via the base unit data link formed by data interface circuit **12** and millimeter wave trans-

mitter **22**. Payload data at a second data rate which may be higher than the authentication data rate may be received from data interface **20** and transmitted via the data link formed by the data interface circuit **12** and the millimeter wave transmitter. Power may be transmitted from RF power source **14** via antenna **16**. Power may be supplied to the base unit from DC power input terminal **18**. Provided that the contactless unit **200** is in physical proximity with the base unit **100**, the power transmitted by the RF power source may be received by the RF power receiver **34** via antenna **36**. The received RF power may be used to power the remaining circuitry in contactless unit **200**. Authentication data transmitted from the base unit **100** may be detected by the millimeter wave receiver **40** and received by contactless unit data interface circuit **32**. The authentication data may be received by contactless unit authentication controller **30**. Contactless unit authentication controller **30** may then authenticate the connection between the base unit **100** and the contactless unit **200**. Contactless unit authentication controller **30** may enable contactless unit data interface circuit **32** to couple further received payload data to contactless unit data interface **38**. Contactless unit data interface **38** may be connected by either a galvanic or non-galvanic connection to a further circuit. The data link and the RF power link form a non-galvanic connection between the base unit and the contactless unit. The authentication process prior to payload data transmission may be considered to be equivalent to plugging in a wired connection. The term contactless unit refers to the contactless property of the non-galvanic electrical coupling, so the contactless unit may touch the base unit.

In embodiments the RF power source **14** may supply sufficient power to power a contactless unit within a range of two meters of the base unit. In further embodiments the base unit **100** may have a millimeter wave receiver instead of a millimeter wave transmitter and the contactless unit **200** may have a millimeter wave transmitter instead of a millimeter wave receiver **40**. In this case the contactless unit **200** receives power from a base unit **100** in proximity to the contactless unit, and the contactless unit authentication controller **30** may transmit authentication data to the base unit **100**. The base unit **100** may enable the connection between the data interface circuit **12** and the data interface **20** for transmitting any received payload data from the contactless unit **200**. In some embodiments the authentication data may be periodically retransmitted either from the base unit **100** or the contactless unit **200**. In some embodiments, the polymer waveguide **50** coupling the base unit **100** and contactless unit **200** may be omitted if the base unit **100** and contactless unit **200** are physically aligned such that the millimeter wave receiver can detect data transmitted by the millimeter wave transmitter. In embodiments this may be achieved by forming at least part of the base unit into a plug and forming at least part of the contactless unit into a socket or vice versa. In embodiments the base unit and contactless unit may include a magnet or ferromagnetic material and the base unit and contactless unit may be physically aligned by magnetic coupling.

In embodiments the millimeter wave transmitter may be replaced by a light emitting diode (LED) or Laser transmitter and the millimeter wave receiver may be replaced by a photo-detector. In these embodiments an optical link may be formed between a base unit and contactless unit.

FIG. **4** shows a base unit **300**. Base unit authentication controller **50** may be connected to RF power circuit **54**. The output of RF power circuit **54** may be connected to antenna **56**. An input of RF power circuit **14** may be connected to DC power terminal **58**. Data Interface **20** may be connected to data Interface circuit **52**. An output of data Interface circuit **52** may be connected to a millimeter wave transceiver **64**. Data interface circuit **52** and millimeter wave transceiver **64** may form a base unit data-link. Base unit authentication controller **50** is connected to near field communication circuit **60**. Near field communication circuit **60** is connected to antenna **62**. Near field communication circuit **60** and antenna **62** may form a base unit NFC link.

FIG. **4** further illustrates an embodiment of a contactless unit **400**. Contactless unit authentication controller **70** may be connected to RF power receiver **74**. A terminal of RF power receiver **74** is connected to an antenna **76**. Contactless unit authentication controller **70** may be connected to data interface circuit **72**. A terminal of data interface circuit **72** may be connected to a millimeter wave-transceiver **84**. Data interface circuit **72** and millimeter wave transceiver **84** may form a contactless unit data link. Contactless unit authentication controller **70** is connected to data interface circuit **72**. An output of contactless unit authentication controller **70** may be connected to contactless unit data interface **78**. Contactless unit authentication controller **70** is connected to near field communication circuit **80**. Near field communication circuit **80** is connected to antenna **82**. Near field communication circuit **80** and antenna **82** may form a contactless unit NFC link.

In operation the base unit authentication controller **55** may enable authentication data to be sent via the base unit NFC link. When a contactless unit is in proximity to the base unit, the base unit NFC link may also provide power to the contactless unit NFC link and contactless unit authentication controller **70** in the contactless unit **400**, the RF power may be disabled until after the successful authentication of the connection between the base unit **300** and the contactless unit **400**. Payload data received from data interface **20** may be transmitted via the base unit data-link. Payload data received from a contactless unit **400** via the base unit data link may be transmitted to further circuitry via the data interface **20**. Power may be transmitted from RF power source **14** via antenna **16**. Power may be supplied to the base unit from DC power input terminal **18**. Provided that the contactless unit **200** is in physical proximity with the base unit **100**, the power transmitted by the RF power source may be received by the RF power receiver **34** via antenna **36**. The received RF power may be used to power the circuitry in contactless unit **400**.

Authentication data transmitted from the base unit NFC link may be detected and received by contactless unit NFC circuit **80**. The authentication data may be received by contactless unit authentication controller **70**. Contactless unit authentication controller **70** may then authenticate the connection between the base unit **300** and the contactless unit **400**. Contactless unit authentication controller **70** may enable contactless unit data circuit **72** to couple further received payload data to contactless unit data interface **78**. Contactless unit data interface **78** may be connected by either a galvanic or non-galvanic connection to a further circuit.

Authentication data transmitted from the contactless unit NFC link may be detected and received by base unit NFC circuit **60**. The authentication data may be received by base unit authentication controller **55**. Base unit authentication controller **55** may then authenticate the connection between the base unit **300** and the contactless unit **400**. Base unit authentication controller **55** may enable base unit data circuit **52** to couple further received payload data to base unit data interface **20**. The base unit data interface **20** may be connected by either a galvanic or non-galvanic connection to a further circuit.

Since the authentication takes place via the NFC link, the authentication process can use much lower power and frequencies than the subsequent payload data transfer.

The data link, the NFC link and the RF power link form a non-galvanic connection between the base unit **300** and the contactless unit **400**. The authentication process prior to payload data transmission may be considered as equivalent to forming a galvanic connection by plugging in a connector in a conventional wired connection.

Since the NFC link only works over a short range, typically less than 50 centimeters, the connection can only be established when the base unit **300** and the contactless unit **400** are in physical proximity. In some embodiments of the base unit, the RF power circuit **54** may share an antenna or coil with NFC circuit **60**. In embodiments of the contactless unit, the RF power receiver **74** may share an antenna or coil with contact-less unit NFC circuit **80**. Embodiments of the base unit NFC circuit **60** may include a secure element containing the authentication data required to authenticate the connection. Embodiments of the base unit NFC circuit **60** may include a secure element containing the authentication data required to authenticate the connection.

In embodiments, the millimeter wave transceiver may be replaced by a photo-transceiver in the base unit and the contactless unit.

FIG. **5** illustrates an example authentication sequence for the base unit **300** and contactless unit **400**. In step **110** contactless unit **400** receives power for the authentication controller **70** via the NFC link from a base unit **300** within range. Once the authentication controller **70** is powered up contactless unit **400** may send authentication data via the NFC link in step **112**. In step **114** base unit **300** receives authentication data via the NFC link. Base unit **300** may then check that the authentication data is valid in step **116**. If the base unit authentication controller **55** determines that the authentication data is not valid then in step **120** and invalid connection is signaled to contactless unit **400** via NFC. The authentication sequence is then terminated in step **122** and no connection is established. In step **116** if the authentication data is valid then the sequence moves to step **118** where base unit **300** may transmit authentication data to contactless unit **400** via the NFC link. In step **124** the contactless unit **400** then checks whether the authentication data received from the base unit **300** is valid. If the authentication data is not valid then contactless unit signals an invalid connection to base unit **300** via the NFC link in step **126**. The authentication sequence is then terminated in step **128** and no connection is established. The contactless unit powers up in step **132**. In step **134** base unit **300** enables the high data rate millimeter wave transceiver **52**. In step **136** the contactless unit **400** enables the high data rate millimeter wave transceiver **84**. The authentication sequence terminates in step **138** and the non galvanic between base unit **300** and contactless unit **400** is established.

FIG. **6** shows a base unit **500**. Base unit authentication controller **55** may be connected to RF power circuit **54**. The output of RF power circuit **54** may be connected to antenna **56**. An input of RF power circuit **54** may be connected to DC power terminal **58**. Data Interface **20** may be connected to RF transponder circuit **92**. An output of RF transponder circuit **92** may be connected to an antenna **90**. RF transponder circuit **92** and antenna **90** may form a high speed RF data link. Base unit authentication controller **55** is connected to near field communication circuit **60**. Near field communication circuit **60** is connected to antenna **62**. Near field communication circuit **60** and antenna **62** may form a base unit NFC link.

FIG. **6** further illustrates an embodiment of a contactless unit **600**. Contactless unit authentication controller **70** may be connected to RF power receiver **74**. A terminal of RF power receiver **74** is connected to an antenna **76**. Contactless unit authentication controller **70** may be connected to RF transponder circuit **94**. A terminal of RF transponder circuit **94** may be connected to a RF transponder antenna **96**. Data interface circuit **72** and photo-transceiver **84** may form a contactless unit data link. Contactless unit authentication controller **70** is connected to data interface circuit **72**. An output of contactless unit authentication controller **70** may be connected to contactless unit data interface **94**. Contactless unit authentication controller **70** is connected to near field communication circuit **80**. Near field communication circuit **80** is connected to antenna **82**. Near field communication circuit **80** and antenna **82** may form a contactless unit NFC link.

In operation the base unit authentication controller **55** may enable authentication data to be sent via the base unit NFC link. When a contactless unit is in proximity to the base unit, the base unit NFC link may also provide power to the contactless unit NFC link and contactless unit authentication controller **70** in the contactless unit **600**, the RF power may be disabled until after the successful authentication of the connection between the base unit **500** and the contactless unit **600**. Payload data received from data interface **20** may be transmitted via the base unit data link. Payload data received from a contactless unit **600** via the base unit data link may be transmitted to further circuitry via the data interface **20**. Power may be transmitted from RF power source **14** via antenna **16**. Power may be supplied to the base unit from DC power input terminal **18**. Provided that the contactless unit **600** is in physical proximity with the base unit **500**, the power transmitted by the RF power source may be received by the RF power receiver **74** via antenna **76**. The received RF power may be used to power the circuitry in contactless unit **600**.

Authentication data transmitted from the base unit NFC link may be detected and received by contactless unit NFC circuit **80**. The authentication data may be received by contactless unit authentication controller **70**. Contactless unit authentication controller **70** may then authenticate the connection between the base unit **500** and the contactless unit **600**. Contactless unit authentication controller **70** may enable contactless unit data circuit **94** to couple further received payload data to contactless unit data interface **78**. Contactless unit data interface **78** may be connected by either a galvanic or non-galvanic connection to a further circuit.

Authentication data transmitted from the contactless unit NFC link may be detected and received by base unit NFC circuit **60**. The authentication data may be received by base unit authentication controller **55**. Base unit authentication controller **55** may then authenticate the connection between the base unit **500** and the contactless unit **600**. Base unit authentication controller **55** may enable base unit data circuit **92** to couple further received payload data to base unit data interface **20**. The base unit data interface **20** may be connected by either a galvanic or non-galvanic connection to a further circuit.

Since the authentication takes place via the NFC link, the authentication process can use much lower power and frequencies than the subsequent payload data transfer. The data transfer speed of the NFC link may typically be 400 Kbits per second.

The data transfer speed of the base unit data link and the contactless unit data link may be up to 40 Gigabits per second. The typical data transfer speed of the base unit data link and the contactless unit data link may be in the region of 5 gigabits

per second for a USB transfer. For some applications the transfer speed may be in the region of a few hundred Megabits per second.

The contactless unit **700** illustrated in FIG. **7** has contactless unit authentication controller **70** which may be connected to RF power receiver **74**. A terminal of RF power receiver **74** is connected to an antenna **76**. Contactless unit authentication controller **70** may be connected to RF transponder circuit **94**. A terminal of RF transponder circuit **94** may be connected to a RF transponder antenna **96**. RF transponder circuit **94** and RF transponder antenna **96** may form a contactless unit data link. Contactless unit authentication controller **70** is connected to a near field communication circuit **80**. Near field communication circuit **80** is connected to antenna **2**. Near field communication circuit **80** and antenna **82** may form a contactless unit NFC link.

First RF transponder circuit **94** may be connected to a second RF transponder circuit **710** by flexible wiring **722**. A terminal of the second RF transponder circuit **710** may be connected to a second RF transponder antenna **712**. The second RF transponder circuit **710** and RF transponder antenna **712** may form a contactless unit data link. Contactless unit authentication controller **70** may be connected to second RF transponder circuit **710** by flexible wiring **722'**. Contactless unit authentication controller **70** is connected to second near field communication circuit **714** by a flexible wiring **722'**. The second near field communication circuit **714** may be connected to second NFC antenna **716**. Second near field communication circuit **714** and antenna **716** may form a second NFC link. Contactless unit authentication controller **70** may be connected to RF power transmitter **718** by flexible wiring **722'**. The RF power receiver **74** may be connected to a RF power transmitter **718** by flexible wiring **722"**. RF power transmitter **718** may be connected to RF power antenna **720**. In operation the contactless unit may receive power and data from a base unit **500** following successful authentication. The contactless unit **700** may then retransmit data via the second data link and may transmit power via the power transmitter following successful authentication of a further contactless unit via the second NFC link. The contactless unit may receive data via the second data link and transmit data to base unit **500**. This allows potentially daisy chaining of contactless units. The contactless unit **700** may be split along the axis A into a left hand portion **700'** and a right hand portion **700"**. Left hand portion **700'** and right hand portion **700"** may be able to move with respect to each other. In embodiments, contactless unit **700** may be mounted either side of a joint of a robot arm such that each portion of contactless unit can move independently. In other embodiments base unit **500** may be a PC docking station, left hand portion of contactless unit **700'** may be included in a PC and right hand portion of contactless unit **700"** may be included in a peripheral device such as a printer.

FIG. **8** shows a base unit **800** having a system host **810** which may connect to a data interface **812**. System host **810** may be connected to high data rate RF transponder **814**. System host **810** may be connected to initialisation watchdog **816**. System host **810** may be connected to DC source **820**. Initialisation watchdog **816** may be connected to control register **818**. Control register **818** may be connected to high data rate RF transponder **814**. DC source **820** may be connected to RF power source **822**. RF power source **822** may be connected to RF power antenna **824**. The power for base unit **800** may be supplied by a wired that power or battery connection connected to terminal **826**.

The system host **810** interacts with high data RF transponder **814**, NFC circuit **828** and RF power circuit **822**. High data rate RF transponder **814** may be capable of multi-gigabits per second data transfer capability. Additional features of the high data rate RF transponder **814** may be low latency, full duplex operation, and multiple channel operation. The high data rate RF transponder **814** may communicate with the system host **810** via a high-speed bidirectional digital bus. The high data rate RF transponder **814** may be configurable by parameters set in the control register **818**. The control register may be controlled from the initialisation watchdog circuit **816**. Initialisation watchdog circuit **816** may in turn be controlled either by system host **810** for by NFC circuit **828**. Control register **818** and initialisation watchdog circuit **816** may form an authentication controller. Initialisation watchdog circuit **816** may periodically trigger a repeat of the authentication cycle. If the separation between the base unit **800** and contactless unit **900** increases beyond the range of the NFC link after the original authentication, the data transfer is disabled. This gives an equivalent functionality to unplugging a conventional wired connection with galvanic or ohmic connections.

FIG. **8** further shows a contactless unit **900** having a high data rate RF transponder **910**. Direct data rate RF transponder **910** may be connected to data sink **912**. High data rate transponder **910** may be connected to sensor digitiser **914**. High data rate transponder **910** may be connected to data source **916**. Control register **918** may be connected to high data rate RF transponder **910**. Control register **918** may be connected to initialisation watchdog **920**. Initialisation watchdog **920** may be connected to NFC circuit **922**. NFC circuit **922** may be connected to NFC antenna **924**. RF power antenna **926** may be connected to RF power receiver circuit **928**. RF power receiver circuit **928** may be connected to DC supply circuit **930**. DC supply circuit **930** may supply power to the circuitry contactless unit **900**.

In the contactless unit **900**, the higher rate RF transponder **910** may be capable of multi-Gigabits per second data transfer capability, matching the properties of the RF transponder circuit of the base unit **800**. The high data rate RF transponder **910** may be configurable by parameters set in the control register **918**. The high data rate RF transponder **910** may interact with local storage elements which provide a data sink **912** and/or data source **916** function. The high data rate RF transponder **910** may further communicate with a sensor **914** and transfer the data from the sensor **914** to the base unit **800**. The NFC circuit **912** may communicate with initialisation watchdog circuit **920** via a data bus. Initialisation watchdog circuit **920** may communicate with DC supply **930** to provide the DC output parameters. RF power receiver **928**, RF power antenna **96**, and DC supply **930** may form a wireless RF power receiver section. RF power receiver **928** may convert energy from an RF carrier into an approximate DC voltage. DC supply **930** may provide further stabilisation and conditioning of the DC signal determined by the programmable output parameters obtained from the initialisation watchdog circuit **920**. The authentication protocol between base unit **800** and contactless unit **900** may be similar to that described for other embodiments.

Embodiments of base unit **800** and contactless unit **900** may be included in an MRI scanner where sensor data may be captured by the sensor digitizer **914** and transferred to a base unit **800** via the high speed RF data link.

Embodiments may include a replacement connection for a PC docking station including wireless charging pods and a multi-GBPS bidirectional data transfer function. Embodiments may include contactless USB connectors whereby at least part of the base unit is formed as part of a USB socket and at least part of a contactless unit is formed as part of a

USB plug. In embodiments a contactless unit may be included on an SD memory card, which may be inserted into a slot having a base unit. Base units and contactless units may be used to simplify backplane connections for example in Internet data centres. One or more base units and contactless units may also be used in MRI scanners to replace conventional connections. In embodiments, one or more base units and contactless units may be included in a wafer stepper. In embodiments at least part of a base unit may be incorporated into an Ethernet socket. At least part of a contactless unit may be incorporated into an Ethernet plug. Embodiments of the base unit and contactless unit may be incorporated into low voltage differential signaling (LVDS) connectors, replacing the conventional galvanic or ohmic connection.

Although the appended claims are directed to particular combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present invention.

Features which are described in the context of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub combination.

The applicant hereby gives notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present application or of any further application derived therefrom.

For the sake of completeness it is also stated that the term "comprising" does not exclude other elements or steps, the term "a" or "an" does not exclude a plurality, a single processor or other unit may fulfill the functions of several means recited in the claims and reference signs in the claims shall not be construed as limiting the scope of the claims.

The invention claimed is:

1. A base-unit for non-galvanic coupling to a contactless-unit, the base-unit comprising:

an antenna coupled to an RF power source,

at least one data-link,

an authentication controller coupled to the at least one data-link, and

a data interface for coupling at least one of a data source and data sink to the base unit, the data interface being coupled to the at least one data-link wherein

the base-unit is operable to

transmit and/or receive payload data via the data interface,

wirelessly transmit RF power from the RF power source to a contactless-unit in physical proximity to the base-unit,

transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a contactless-unit only when the contactless-unit is in physical proximity to the base-unit, and

transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a contactless unit; and

wherein the authentication controller further comprises a watchdog timer and wherein the base-unit is operable to periodically re-authenticate a non galvanic connection to a contactless-unit, the re-authentication period being determined by the watchdog timer, and to disable further payload data transmission and/or reception if the re-authentication of the non-galvanic connection fails.

2. The base unit of claim **1**, wherein the authentication controller is coupled to the RF power source and the authentication controller is operable to disable RF power transmission in response to the failure of the authentication of the non-galvanic connection.

3. The base unit of claim **1**, further comprising at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the base-unit and a contactless unit non-galvanically coupled to the base unit is fixed.

4. The base unit of claim **1**, wherein the at least one data-link comprises at least one of a millimeter wave transmitter, a millimeter wave receiver, a laser, and a photodetector.

5. The base unit of claim **1**, wherein the at least one data link comprises a first data-link and a second data-link, the first and second data-links being coupled to the authentication controller, and wherein

the first data-link comprises a near field communication circuit coupled to a second antenna and the base-unit is operable to

transmit and/or receive authentication data via the first data-link to authenticate a non-galvanic connection to a contactless-unit only when the contactless-unit is in physical proximity to the base-unit, and

transmit and/or receive payload data via the second data-link following the authentication of the non-galvanic connection to a contactless unit via the first data-link.

6. The base-unit of claim **5** wherein the authentication controller is coupled to the RF power source and wherein the authentication controller is operable to enable the RF power transmission following the authentication of the non-galvanic connection.

7. The base-unit of claim **4**, wherein the second data link comprises a third antenna coupled to at least one of an RF transmitter and an RF receiver.

8. A contactless-unit for non-galvanic coupling to a base-unit, the contactless-unit comprising:

an antenna coupled to an RF power receiver,

at least one data-link, and

an authentication controller coupled to the at least one data-link,

a data interface for coupling at least one of a data source and data sink to the contactless unit, the data interface being coupled to the at least one data-link, wherein the contactless-unit is operable to

transmit and/or receive payload data via the data interface,

receive RF power provided from a base-unit only when the base-unit is in physical proximity to the contactless-unit,

convert the received RF power to supply power to circuits in the contactless-unit,

transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a base-unit only when a base-unit is in physical proximity to the contactless-unit, and

transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a base unit; and

wherein the authentication controller further comprises a watchdog timer and wherein the contactless-unit is operable to periodically re-authenticate a non galvanic connection to a base-unit, the re-authentication period being determined by the watchdog timer, and to disable further data transmission and/or reception if the re-authentication of the non-galvanic connection fails.

9. The contactless unit of claim 8, further comprising at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the contactless-unit and a base unit non-galvanically coupled to the contactless unit is fixed.

10. The contactless unit of claim 8, wherein the at least one data-link comprises at least one of a millimeter wave transmitter, a millimeter wave receiver, a laser, and a photodetector.

11. The contactless unit of claim 8, wherein the at least one data link comprises a first data-link and a second data-link, the first and second data-links being coupled to the authentication controller, wherein

the first data-link comprises a second antenna coupled to a near field communication circuit and the contactless-unit is operable to

transmit and/or receive authentication data via the first data-link to authenticate a non-galvanic connection to a base-unit only when the base unit is placed in physical proximity to the contactless-unit, and

transmit and/or receive payload data via the second data link following the authentication of the non-galvanic connection to a base unit via the first data-link.

12. The contactless-unit of claim 11, further comprising:

a third data-link coupled to the authentication controller, the third data-link comprising a near field communication circuit coupled to a fourth antenna,

a fourth data-link coupled to the authentication controller, and

a fifth antenna coupled to an RF power source; wherein the contactless-unit is further operable to

transmit RF power to a further contactless-unit in physical proximity to the contactless unit,

transmit and/or receive authentication data via the third data-link to authenticate a non-galvanic connection to a further contactless-unit only when the further contactless-unit is in physical proximity to the contactless-unit, and

transmit and/or receive data between the contactless-unit and the further contactless-unit via the fourth data link element following the authentication of the non-galvanic connection.

13. The contactless unit of claim 12, further comprising at least one of a sensor and a storage element coupled to the data interface.

14. The contactless-unit of claim 12, wherein the second data link further comprises a third antenna coupled to at least one of an RF transmitter and an RF receiver.

15. A base-unit for non-galvanic coupling to a contactless-unit, the base-unit comprising:

an antenna coupled to an RF power source,

at least one data-link,

an authentication controller coupled to the at least one data-link, and

a data interface for coupling at least one of a data source and data sink to the base unit, the data interface being coupled to the at least one data-link wherein

the base-unit is operable to

transmit and/or receive payload data via the data interface,

wirelessly transmit RF power from the RF power source to a contactless-unit in physical proximity to the base-unit,

transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a contactless-unit only when the contactless-unit is in physical proximity to the base-unit, and

transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a contactless unit; and

at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the base-unit and a contactless unit non-galvanically coupled to the base unit is fixed.

16. A contactless-unit for non-galvanic coupling to a base-unit, the contactless-unit comprising:

an antenna coupled to an RF power receiver,

at least one data-link, and

an authentication controller coupled to the at least one data-link,

a data interface for coupling at least one of a data source and data sink to the contactless unit, the data interface being coupled to the at least one data-link, wherein the contactless-unit is operable to

transmit and/or receive payload data via the data interface,

receive RF power provided from a base-unit only when the base-unit is in physical proximity to the contactless-unit,

convert the received RF power to supply power to circuits in the contactless-unit,

transmit and/or receive authentication data via the at least one data-link to authenticate a non-galvanic connection to a base-unit only when a base-unit is in physical proximity to the contactless-unit, and

transmit and/or receive payload data via the at least one data link following the authentication of the non-galvanic connection to a base unit; and

at least one of a mechanical coupling element and a magnet and wherein in operation, the relative position of the contactless-unit and a base unit non-galvanically coupled to the contactless unit is fixed.

* * * * *