Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2590152 A1 2006/06/22

(21) 2 590 152

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2005/12/14
(87) Date publication PCT/PCT Publication Date: 2006/06/22
(85) Entrée phase nationale/National Entry: 2007/06/12
(86) N° demande PCT/PCT Application No.: US 2005/045488
(87) N° publication PCT/PCT Publication No.: 2006/066035
(30) Priorité/Priority: 2004/12/15 (US11/013,244)

(51) Cl.Int./Int.Cl. *A61B 19/00* (2006.01), *A61F 9/007* (2006.01), *G06K 19/07* (2006.01)

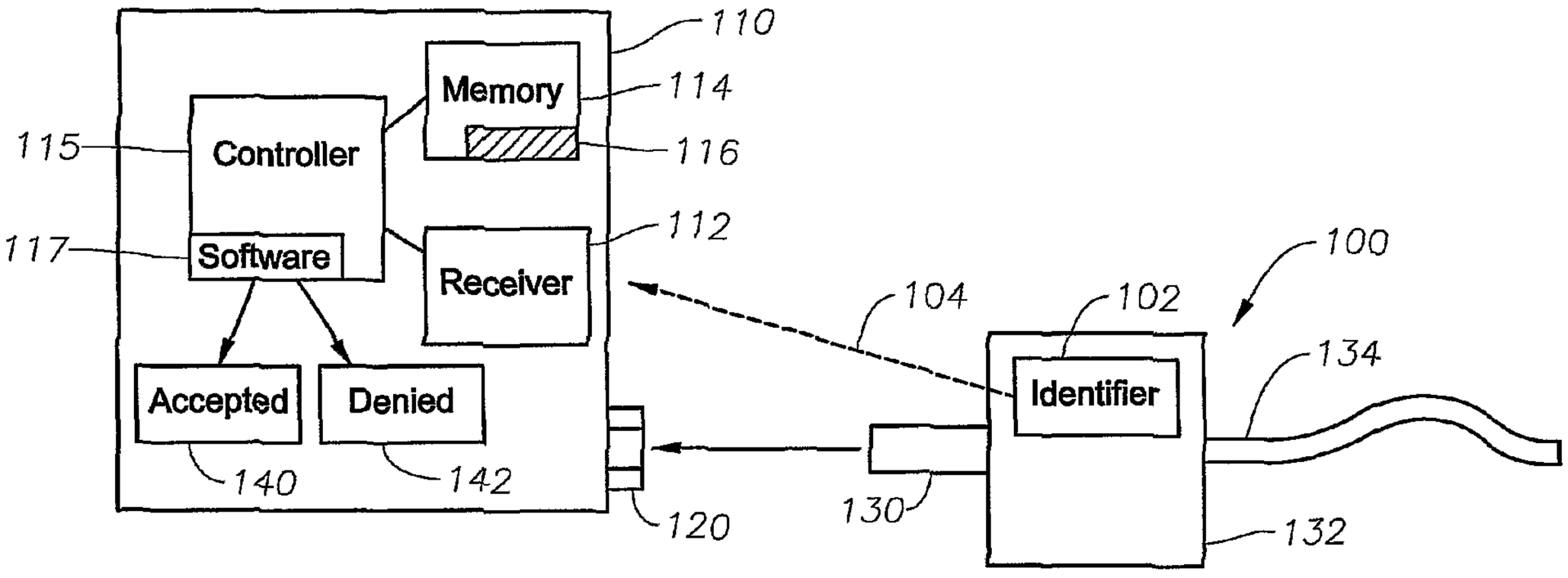
(71) Demandeur/Applicant:
ALCON, INC., CH

(72) Inventeurs/Inventors:
HORVATH, CHRISTOPHER, US;
ROWE, T. SCOTT, US;
REED, FREDERICK M., US;
EKVALL, JOHAN G., US;
TODD, KIRK W., US

(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : SYSTEME ET PROCEDE D'IDENTIFICATION ET DE VERIFICATION DE D'UN INSTRUMENT DE CHIRURGIE OPHTALMIQUE ET DE SES COMPOSANTS

(54) Title: SYSTEM AND METHOD FOR IDENTIFYING AND CONTROLLING OPHTHALMIC SURGICAL DEVICES AND COMPONENTS



(57) Abrégé/Abstract:
System and method for identifying a component, such as an optical probe or pneumatic scissors, of an ophthalmic surgical device. A component of a surgical device includes an identifier (102), such as a RFID tag. Data from the RFID tag is transmitted to a RFID reader in the device. A controller (115) determines whether the component corresponding to the received data is operable with the surgical device based on criteria, such as whether the received data is an authorized code that matches data stored in memory or whether the received data solves or satisfies an algorithm. The authorized codes are selected from a larger set of available codes. The controller enables or disables the operation of the device with the component based on whether the criteria is satisfied, the number of uses of the component, an amount of time that has passed since the component has been used, or a geographic location. The RFID data can also be used to calibrate the surgical device for use with the particular component and for inventory and monitoring purposes.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/066035 A3

(51) International Patent Classification:
A61B 19/00 (2006.01) *G06K 19/07* (2006.01)
A61F 9/007 (2006.01)

(21) International Application Number:
PCT/US2005/045488

(22) International Filing Date:
14 December 2005 (14.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/013,244 15 December 2004 (15.12.2004) US

(71) Applicant *(for all designated States except US)*: **ALCON, INC.** [CH/CH]; P.O. Box 62, Bosch 69, CH-6331 Hunenberg (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HORVATH, Christopher** [US/US]; 5051 Alton Parkway #76, Irvine, California 92604 (US). **ROWE, T., Scott** [US/US]; 28465 Danafir, Dana Point, California 92629 (US). **REED, Frederick, M.** [US/US]; 4791 New Mexico Lane, Cypress, California 90630 (US). **EKVALL, Johan** [SE/US]; 992 Miramar Street, Laguna Beach, California 92651 (US). **TODD, Kirk, W.** [US/US]; 20340 Via Manresa, Yorba Linda, California 92887 (US).

(74) Agents: **PASTRANA, Armando, Jr.** et al.; 6201 South Freeway, Fort Worth, Texas 76134 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

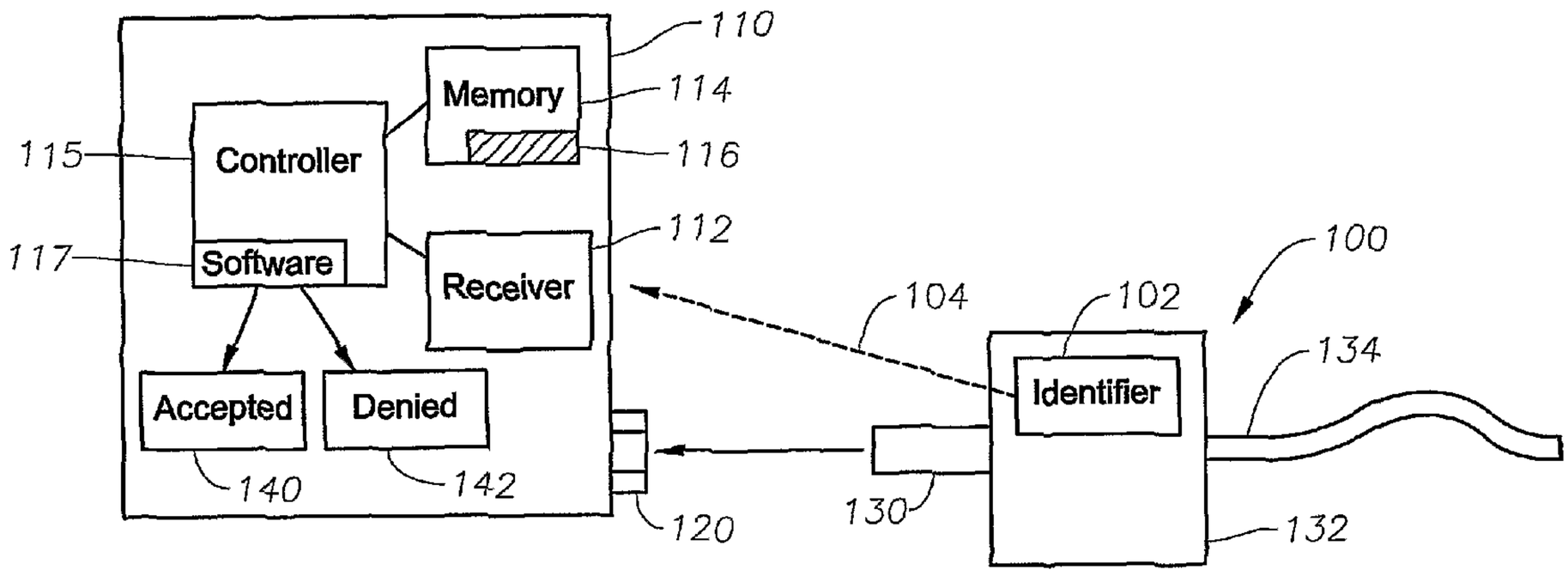
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
10 August 2006

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR IDENTIFYING AND CONTROLLING OPHTHALMIC SURGICAL DEVICES AND COMPONENTS



(57) Abstract: System and method for identifying a component, such as an optical probe or pneumatic scissors, of an ophthalmic surgical device. A component of a surgical device includes an identifier (102), such as a RFID tag. Data from the RFID tag is transmitted to a RFID reader in the device. A controller (115) determines whether the component corresponding to the received data is operable with the surgical device based on criteria, such as whether the received data is an authorized code that matches data stored in memory or whether the received data solves or satisfies an algorithm. The authorized codes are selected from a larger set of available codes. The controller enables or disables the operation of the device with the component based on whether the criteria is satisfied, the number of uses of the component, an amount of time that has passed since the component has been used, or a geographic location. The RFID data can also be used to calibrate the surgical device for use with the particular component and for inventory and monitoring purposes.

WO 2006/066035 A3

WO 2006/066035 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR IDENTIFYING AND CONTROLLING OPHTHALMIC SURGICAL DEVICES AND COMPONENTS

TECHNICAL FIELD OF THE INVENTION

The present invention relates to ophthalmic surgical devices, and, more particularly, to the use of electronic identifiers on components of ophthalmic surgical devices that can be used to transmit and receive data related to the components and use thereof with the ophthalmic surgical device.

BACKGROUND OF THE INVENTION

Various surgical devices operate using components that are discarded or replaced for various reasons. For example, components may be discarded because they are contaminated or because they have exceeded a certain useful life. Thus, unlike permanent surgical equipment, some components are used one time, or a limited number of times, and then must be replaced for safety and/or other considerations. Determinations regarding whether a particular component is suited for a particular surgical device are typically made by a technician or surgeon, for example, based on whether the component fits within or attaches to the surgical device, and the operating specifications of the component and the device. Other aspects related to the use of particular components are also left to user discretion, including activation of the surgical device, calibration of the device to operate with a particular component, and the manner in which the device operates with a particular component. Thus, the selection of components and operation of the device are often subject to user discretion.

Known systems and techniques for matching surgical devices and components, however, can be prone to error and require additional time and effort to ensure that the correct component is attached to the correct surgical device. Further, there are problems associated with third parties manufacturing components for replacement of original surgical components. Third-party replacement components can have a number of shortcomings. For example, they may be lower quality components compared to components from original manufacturers. They may also not function as intended and be less reliable than original manufacturer components, thus causing system operation and safety concerns. Additionally, manufacturers of

original equipment experience increased competition from third parties who manufacture and sell components that are intended to replace original equipment.

There have been attempts to address some of these concerns, but only with specific types of medical equipment and with limited effectiveness. One approach has been to utilize Radio Frequency Identification (RFID) systems. RFID systems are well known and use electronic tags or transponders for storing data. Some RFID systems use passive tags that are activated when they are brought into proximity to a transmitted radio signal, whereas other RFID systems use active tags that include an independent power source to operate independently.

RFID tags (devices) have been used with specific types of medical equipment but, to the Applicants' knowledge, not with ophthalmic surgical devices. For example, one known system uses RFID devices in connection with disposable optical fiber components of a medical laser system in which fiber optic strands are inserted into the body. The strands are exposed to body fluids and must be disposed of after every use, or thoroughly disinfected. Other known systems use RFID devices with catheters that are inserted into the vascular system and directed into the heart. These known systems, however, use RFID devices for particular surgical devices and provide limited functionality for identifying replacement components that are not original equipment components.

Another known system is used to track surgical implements. A sensor system records the time each surgical implement is checked-out / used. When the surgical implement has been used, it is placed on or near the sensor and check-in information is recorded. This system is used to track surgical implements during a procedure and to ensure that no medical implements are inadvertently left behind inside a patient.

Thus, known systems and techniques for identifying surgical equipment, in particular, ophthalmic surgical equipment, can be improved. To the Applicants' knowledge, RFID technology has yet to be effectively applied to ophthalmic surgery systems and components. Further, the use of RFID tags in other medical devices is typically limited to basic identification functions and enabling or disabling equipment. Thus, known systems do not provide other, more useful data concerning the component and its functionality, which can assist surgeons when using the equipment. Such information may include, for example, calibration data and data related to the history of the component. Accordingly, the manner in which components of ophthalmic surgical systems and equipment are utilized can be improved, including

the integration of data transmission devices, such as RFID devices, to perform identification and other functions that are not provided by known systems, and by providing the ability to provide additional information relating to the component to surgeons.

BRIEF SUMMARY OF THE INVENTION

According to one embodiment of the present invention, a system for identifying a component that is used with an ophthalmic surgical device includes a radio frequency identification (RFID) tag that is part of the component, a receiver, a memory for storing criteria and a controller, which are included in the surgical device. Data from the RFID tag is transmitted to the receiver in the ophthalmic surgical device. The controller determines whether the component corresponding to the received data can be used with the ophthalmic surgical device based on whether the received data satisfies the criteria stored in memory.

In a further embodiment, a system for identifying a component that is used with an ophthalmic surgical device includes a radio frequency identification (RFID) tag that is part of the component, a receiver, a memory for storing criteria and a controller, which are included in the surgical device. Data from the RFID tag is transmitted to the receiver in the ophthalmic surgical device, and the controller determines whether the component corresponding to the received data can be used with the ophthalmic surgical device by determining whether the received data is an authorized code that satisfies the criteria stored in the memory. The authorized codes are selected from a larger set of codes, including both authorized and unauthorized codes.

In a further alternative embodiment, a system for identifying a component that is used with an ophthalmic surgical device includes a radio frequency identification (RFID) tag in the component, a receiver, a memory for storing criteria and a controller in the surgical device. Unencrypted data from the RFID tag is transmitted to the receiver. The controller determines whether the component corresponding to the received unencrypted data can be used with the ophthalmic surgical device based on whether the received unencrypted data is an authorized code that satisfies the criteria in memory. Authorized codes are selected from a larger set of available codes, including both authorized and unauthorized codes.

Yet a further alternative embodiment is a method of identifying a component that can be used with an ophthalmic surgical device. The method includes establishing criteria and storing criteria in a memory of the ophthalmic surgical device and transmitting data from an identifier in the component to a receiver in the ophthalmic surgical device. Data received from the identifier is processed to determine whether the received data is an authorized code that satisfies the criteria

stored in the memory to determine whether the component corresponding to the received data can be used with the ophthalmic surgical device.

In various embodiments, the criteria can be authorized data, e.g., authorized numbers, that are stored in the memory. The data that is received from the identifier is compared to the authorized data to determine whether the component can be used with the ophthalmic surgical device. For example, the device can be enabled if the received data matches the authorized data criteria. Further, the criteria can be an algorithm, a formula or other pre-defined criteria (generally "algorithm"). The algorithm is applied to the data that is received from the identifier to determine whether the component can be used with the ophthalmic surgical device based on, for example, whether the received data solves or satisfies the algorithm or formula.

In various embodiments, different ophthalmic surgical devices and components can be utilized. For example, the ophthalmic surgical device can be a laser or laser console, and the component can be an optical probe that is attached to the laser. In other embodiments, the ophthalmic surgical device is a vitreoretinal surgical device, and the component can be a vitrectomy probe, a pneumatically or electrically powered scissors, or an endoilluminator probe that is attached to the vitreoretinal surgical device.

Further, in embodiments using RFID components, the receiver can be a RFID reader, and the identifier can be a RFID tag, and the data in the RFID tag or identifier may be unencrypted.

One manner of selecting authorized codes that satisfy the criteria is to select authorized codes from a larger set of available codes, which includes both authorized and unauthorized codes. For example, in one embodiment, the number of authorized codes is at least three orders of magnitude greater than a number of available codes; e.g., one billion authorized codes are selected from one trillion codes. In one embodiment, the identifier data includes 14 bytes. Two bytes are used to identify the type of component, and 12 bytes are used to identify one trillion codes.

System embodiments can be configured to enable or disable a surgical device. If the data received from the identifier satisfies the criteria, then the device can be enabled. The device can also be conditionally enabled based on, for example, whether the component has been used before, or based on an amount of time that has passed since a first or prior use of the component. A certain number of repeat uses of

a component may be allowed, but the device can be disabled after a certain number of uses or after a certain amount of time. Other safety precautions can also be implemented, such as generating a message to a surgeon that the component has been previously used. Further, data can be written back to the component identifier for future reference. The data may include a date of usage, a number of uses of the component, a duration of use of the component, or a power setting of the component. The device can also be enabled based on geographic restrictions.

In various embodiments, the identifier can also include calibration data that indicates how the ophthalmic surgical device should be configured to work with a particular component. Further, identification data and/or calibration data can be used for various purposes. For example, a user interface that is presented on a display screen can be generated based on the particular component that is utilized. Data can also be used to enable operating parameters that are compatible with the identified component and to disable operating parameters that are incompatible with the identified component. The data can be used to implement safety procedures, for example, limiting the value of power, exposure range and other operating parameters, and checking whether a safety component, such as a filter that is associated with the identified component, is present.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of embodiments and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings, in which like reference numbers indicate like features and wherein:

Figure 1 is a block diagram of a system according to one embodiment that includes an ophthalmic surgical device and a component that is used with the device and that includes an identifier;

Figure 2 illustrates an exemplary RFID system that can be used with ophthalmic surgical devices and components thereof;

Figure 3 illustrates an identifier of a component according to one embodiment;

Figure 4 illustrates an identifier and an unencrypted security code or number of a component according to one embodiment;

Figure 5 illustrates a system according to one embodiment in which authorized unencrypted identifier codes or numbers are selected from a larger set of available codes or numbers;

Figure 6 illustrates an alternative embodiment in which an ophthalmic surgical device is disabled or conditionally enabled depending on the number of uses of a component;

Figure 7 illustrates a further embodiment in which an ophthalmic surgical device is disabled or conditionally enabled depending on an amount of time that has lapsed since a first or earlier use of the component;

Figure 8 illustrates how unencrypted authorized codes can be serialized to define groups or lots of components that can be used with a surgical device;

Figure 9 illustrates an alternative embodiment in which data transmitted from the identifier in the component includes information for calibrating an ophthalmic surgical device;

Figure 10 illustrates another alternative embodiment including read/write applications involving a transceiver in an ophthalmic surgical device and an identifier in a component used with the device; and

Figures 11A-B are flow charts illustrating a manner of identifying components and controlling an ophthalmic surgical device according to various embodiments.

DETAILED DESCRIPTION OF ILLUSTRATED EMBODIMENTS

In the following description, reference is made to the accompanying drawings, which form a part hereof, and which show by way of illustration specific embodiments. It is to be understood that structural changes may be made without departing from the scope of the embodiments.

System and method embodiments provide for electronic identifiers to be integrated into ophthalmic surgical equipment. The electronic identifiers can perform various functions, including identifying a component or adaptation that can be used with an ophthalmic surgical device, selectively enabling and disabling equipment that is used with components, identifying unauthorized components, such as components that are not compatible with a device and components from third party manufacturers, providing calibration data, and providing for read/write applications between an ophthalmic surgical device and a component used with the device. Thus, embodiments allow for more accurate determinations whether certain components or adaptations are compatible with certain surgical devices. Further, embodiments provide for enhanced functionality, thus improving the effectiveness and safety of ophthalmic surgical procedures by ensuring that only suitable components are used with the device. Additionally, embodiments allow original surgical equipment manufactures to retain tighter control over their inventory and the use of original and valid components, thereby providing improved performance, regulatory compliance and tracking of products. These and other aspects of embodiments are discussed in further detail below.

Referring to Figure 1, according to one embodiment, a system "S" includes an ophthalmic surgical device 110 and an ophthalmic surgical component or adaptation 100 that is attached to and used with the surgical device 110. The component 100 is connected to the surgical device 110 via an input port or connector 120 of the surgical device 110 and a connector 130 of the component 100. Wireless communications between certain surgical devices and components may also be utilized.

An identifier 102 is integrated into the component 100. The identifier 102 transmits data 104 to a receiver 112 of the surgical device 110. The identifier data 104 can be used to determine whether the component 100 is an authorized component that can be used with the surgical device 110. More particularly, each component 100 can be programmed with particular data 104. The surgical device 110 includes a memory 114 that stores criteria 116, such as a set of authorized codes or data, or an

algorithm, formula or other pre-defined criteria (generally, "algorithm"). The memory can be a memory element that is readily accessible or a memory element that is integrated within other system components, depending on security requirements.

A controller 115, such as a processor or micro controller (generally "controller"), is programmed with software and/or hardware 117 that processes the data 104 received from the identifier 102 and the criteria 116 stored in memory 114 to determine whether the component 100 should be accepted 140 or denied 142 and whether the surgical device 110 should be enabled or disabled.

In one embodiment, the surgical device 110 is an ophthalmic laser console and the component 100 is an optical probe. As generally illustrated in Figure 1, an optical probe 100 includes a connector 130 for attachment to the console 110 via a connector 120 of the console 110, a housing 132, and an optical fiber 134. Light generated by the console 110 is provided to the probe 100, which is manipulated by a surgeon so that the light is delivered by the optical fiber 134 to the surgical site.

One exemplary laser console 110 and optical probe 100 combination that can be used with embodiments of the invention include the Eyelite laser system, part no. 806550001, available from Alcon Laboratories Inc., 6201 South Freeway, Fort Worth, Texas 76134. Other laser consoles from Alcon Laboratories may also be utilized. Exemplary components for connection to a laser console 110, such as the Eyelite laser system, include fiber optic probe connectors that are used with the LIO-AT Headset system, such as connector part nos. 8065741019, 8065501003, and 8065501101; a fiber that is provided with the LIO-AT Headset system, such as part no. 8065741106; and various Endo Probe fibers, such as part nos. 8065010719, 8065010503, 8065010219, 8065010203, 8065010739, 8065010419, 8065010319, 8065010403, and 8065010404, which are also available from Alcon Laboratories, Inc.

Persons skilled in the art will appreciate that embodiments can be used with other ophthalmic surgical devices 110 and components or adaptations 100. As a further example, the control console 110 may be a vitrectomy console, and the components 100 that are attached to the console can include, but are not limited to, a vitrectomy probe, a pneumatically or electrically powered scissors, an endoilluminator probe and a retinal surgery component. An exemplary vitrectomy console 110 is part no. 8065741008, available from Alcon Laboratories, Inc. Exemplary components that can be attached to the vitrectomy console include vitrectomy probe part no. 8065741018, pneumatic scissors part no. 8065808101, and

endoilluminator part no. 8065740264, all of which are also available from Alcon Laboratories, Inc. For purposes of explanation, not limitation, this specification refers to an ophthalmic surgical device 110 that is a laser console and a component or adaptation 100 that is an optical probe that is connected to the console 110 and used to deliver laser energy to a surgical site. However, persons skilled in the art will appreciate that a vitrectomy console and various related components can also be utilized.

According to one embodiment, the receiver 112 in the console 110 and the identifier 102 in the probe 100 are Radio Frequency Identification (RFID) components. One exemplary RFID system that can be used with various embodiments include part no. MCRF355, available from Microchip Technology, Inc., as described in Specification Sheet AN707, MCRF 355/360 Applications, the contents of which are incorporated herein by reference as though set forth in full.

Figure 2 generally illustrates one exemplary RFID system 200 that can be used with embodiments. A RFID tag 210 typically includes an Integrated Circuit (IC), such as an Application Specific Integrated Circuit (ASIC), that includes a memory for storing data. A transponder 212 is activated by Radio Frequency (RF) instruction or signal 224 from the reader 220, which is sent through the reader antenna 226, for example, in response to a micro-controller unit 230, and received by an antenna 216 of the transponder 212 to wirelessly write data to or read data from the memory of the transponder 212.

For example, when the RFID tag 210 is to be read, the reader 220 sends out a 134.2KHz power pulse to the antenna 226 lasting approximately 50ms. The magnetic field generated is collected by the antenna 216 in the tag 210 that is tuned to the same frequency. This received AC energy is rectified and stored in a small capacitor within the transponder 212. After completion of the power pulse, the transponder 212 transmits back its data, using the energy stored in the capacitor as a power source. In total, 128 bits are transmitted (including error detection information) over a period of 20ms. This data is received by the antenna 226 and decoded by the reader unit 220 and controller 230. The capacitor is discharged after the data has been transmitted, and the transponder 212 is reset and ready for the next read cycle.

The RFID configuration described above is "passive" since the transponder is powered by power stored in a capacitor that is generated by the RF signal from the reader. Thus, a passive RFID identifier is normally inactive and does not have an

independent power source. The RFID system may also be active if a separate power source or battery is provided. Further details concerning the manner in which RFID systems operate is well known in the art and, therefore, is not discussed in further detail in this specification. For purposes of explanation, not limitation, this specification refers to RFID components that are used for transmitting data between a console 110 and a probe 100. However, persons skilled in the art will recognize that other transmitter, receiver and transceiver components can also be utilized.

When RFID components are applied to embodiments to provide communications between the laser console 110 and probe components 100, the identifier 102 in the probe component 100 is a RFID tag or transponder 210, and the receiver 112 of the console 110 is a RFID reader 220. The RFID tag or identifier 102 includes the identification and, if applicable, other data relating to the component. The controller 115 includes software and/or hardware 117 to implement the criteria 116 to determine whether data 104 sent by the RFID tag 102 of the probe 100 and received by the RFID reader 112 of the console 110 indicates that the probe 100 can be used with the console 110.

For example, the console 110 can be enabled if the data 104 is accepted 140, or disabled if the data 104 is denied 142. The console 110 can also be conditionally enabled. For example, the console 110 may operate normally or, alternatively, in a safe mode at lower power levels. The console 110 can also be conditionally enabled when, for example, the same probe 100 has been used too many times before. The controller 115 can configure the console 110 to operate in a different manner in view of safety and other considerations since the probe 100 may not function as intended due to, for example, incompatible specifications, excessive use and wear, or expiration of the probe 100.

More particularly, referring to Figure 3, according to one embodiment, data 104 transmitted by the RFID tag 102 includes a two byte code or identification data 300. The two byte code can represent numbers 00-99 to identify 100 different types of probes 100. The controller 115 can apply the criteria 116 to the data 300 stored in memory 114 to determine whether the data 104 is accepted 140 or denied 142 and whether the console 110 should be enabled or disabled.

Referring to Figures 4 and 5, according to another embodiment, the data 104 transmitted by the RFID tag or identifier 102 is a 14 byte code. The 14 bytes are divided into two groups: two bytes of identification data 300 (as discussed above

with respect to Figure 3) and 12 bytes of security data 400. The security data 400 is selected from a larger set of potential security codes 510. A subset of the potential codes 510 is selected as authorized codes 520. Persons skilled in the art will appreciate that the security data 400 and authorized codes 510 can be numeric, alpha-numeric, or another representation. Additionally, they may use different number systems, such as binary, hexadecimal or decimal. Thus, "code" is not intended to be limited to a particular type of code.

The 12 bytes of the security code 400 provide one trillion possible security codes 510, i.e., numbers 000000000000 to 999999999999. This is represented in Figure 5 as (A+U) 510, or authorized codes (A) 520 + unauthorized codes (U) 522. Certain codes are selected from these one trillion potential codes 510 as authorized codes 520. In one embodiment, the set of potential security codes 510 includes one trillion codes, and one billion codes are selected as authorized codes (A) 520. The remaining codes are unauthorized codes (U) 522. Thus, in this embodiment, the number of potential codes 510 is at least three orders of magnitude greater than the number of authorized codes (A) 520. The one billion authorized codes (A) 520 can be selected using, for example, a random number generator or another suitable algorithm or selection criteria. The selection algorithm can have different levels of complexity for different security levels and applications.

Identifiers 102 of each probe 100 from an original manufacturer are programmed with one of the authorized codes (A) 520. The authorized codes (A) 520 satisfy the criteria 116 stored in memory 114. For example, if the criteria 116 is a set of authorized data that is stored in memory 114, the authorized data 116 may be the same as or match the authorized codes (A) 520, whereas the unauthorized codes (U) 522 would not match the authorized data criteria 116. As a further example, if the criteria 116 is an algorithm, then the authorized codes (A) 520 would satisfy or solve the algorithm, whereas the unauthorized codes (U) 522 would not solve or satisfy the algorithm criteria 116.

In the embodiment in which the criteria 116 is an algorithm, it is not necessary to store a set of authorized data in memory since the algorithm is applied to security data received from the identifier. This may be beneficial when memory capabilities and security are concerns. An algorithm can be programmed with varying levels of complexity to provide different levels of security. Further, an algorithm can be stored in memory of various system components so that the criteria can be difficult to determine. Accordingly, although Figure 5 shows the authorized codes (A) 520 being

stored to memory, this is representative of the authorized codes that satisfy or solve the algorithm, since it is not necessary to store the authorized codes in memory when using an algorithm.

Thus, the security data 400 stored in the RFID tag 102 of a probe 100 may or may not satisfy the criteria 116 stored in memory 114. In the event that the probe 100 is from an original manufacturer, the identifier 102 includes an authorized code (A) 520 that would satisfy the criteria 116. However, if the probe 100 is from a third party manufacturer, the identifier 102 may or may not include an authorized code (A) 520, as discussed in further detail below.

When a probe 100 is connected to the laser console 110, the RFID tag 102 transmits the 2-digit identification code 300 and the 12-digit security code 400 to the RFID reader 112. The controller 115 determines whether the 2-digit identification code and/or the 12-digit security code 400 satisfies the criteria 116 stored in memory 114 of the console 110.

If, for example, the security code 400 satisfies the criteria 116, e.g., the security code 400 matches one of the one billion authorized codes (A) 520 stored in memory 116 or satisfies or solves an algorithm, then the console 110 can be enabled by the controller 115. In contrast, the console 100 can be disabled if the code 400 does not satisfy the criteria 116 and is one of the unauthorized (U) codes 510 or an unrecognized code. Thus, as shown in Figure 5, the probe 100A includes authorized security data 400 and, therefore, can be used with the console 110, whereas the probe 100U cannot be used with the console 110 because it is programmed with an unauthorized code (U) 522, which does not satisfy the criteria 116.

Selecting authorized codes 520 from a sufficiently large set of possible codes 510 facilitates the ability of manufactures of original probe components 100 to ensure that only original components are utilized and that replacement components from third parties are likely to block operation of the console 110. This can be accomplished even without having to utilize encryption/decryption techniques and the additional encryption/decryption hardware and software, which can increase the costs and complexities of the system. Rather, the authorized codes (A) 520 can remain unencrypted, and sufficient security is provided by the fact that the subset of authorized codes (A) 520 is selected from a sufficiently large pool of potential codes (A+U) 510 so that the probability of a third party manufacturer selecting an authorized code 520 is sufficiently low. This can ensure that components from

original manufactures are the primary components that enable the console 110, which may be particularly useful considering that some third party replacement components may not meet the original component specifications and may not function as well as components from original manufactures and, therefore, present safety and liability concerns when using the console 110. Of course, persons skilled in the art will appreciate that encryption and decryption components can be utilized to provide additional security.

For example, in the embodiment in which one billion different authorized codes (A) 520 are selected from one trillion potential codes (A+U) 510, the total number of possible codes 510 is at least three orders of magnitude greater than the selected number of authorized codes. In this embodiment, there would only be a 1/1000 probability that the third party replacement component would satisfy the criteria 116 and be accepted by controller 115 of the console 100, thus enabling the console 100 to work with the component. The probability can be increased or decreased by adjusting the number of bytes in the security code 400, the number of authorized codes 520, and/or the number of unauthorized codes 522. Accordingly, the example involving one billion authorized codes (A) 520 and one trillion total potential codes (A+U) 510 is not intended to be limiting.

It is possible for a third party to repeatedly use a probe 100 that has been accepted by the console 100 since the accepted probe 100 includes an authorized code (A) 520. A third party manufacturer may also purchase a small number of original equipment probes and then use the security data 400 from those probes to program other replacement components. However, embodiments can be configured to disable the console 100 after a certain number of uses or occurrences of a particular security code 400 or after a pre-determined amount of time following the first instance of a number. For example, when the criteria 116 is an algorithm, the algorithm 116 can be configured or programmed to allow a certain number of uses or a use within a period of time.

For example, referring to Figure 6, when the RFID tag 102 of an original probe 100 transmits the security code 400 to the RFID reader 112, the security data 400 matches, satisfies or solves the criteria 116. Thus, the console 110 will be enabled to operate with that component 100. There may be attempts to re-use the same probe since it has an authorized code (A) 520 that satisfies the criteria 116. Multiple uses of a probe 100 may be suitable in some instances, however, in order to ensure that proper regulatory and safety guidelines are followed, it is advisable that

each authorized probe 100 be used a single time. To address these concerns, the controller 115 can be programmed to disable the console 110 after a pre-determined number of uses of the same probe 100 or after a pre-determined number of instances of the same security code 400. Thus, the console 110 is enabled under normal circumstances, but can be disabled after a pre-determined number of repeat uses of the same probe 100.

In the illustrated embodiment, the console 110 is enabled to allow the same probe 100 to be used a second time, but is disabled when an attempt is made to use the same probe a third time. Indeed, the controller 115 may be programmed to allow different numbers of repeat uses of the same probe 100. As a result, a new probe 100 will be required since the same probe 100 can no longer be used with the console 110. Alternatively, or in addition, the controller 115 can be programmed to generate a visual or audible warning or message to the user that the probe 100 has been used before using a display 600 or a speaker 610. The controller 115 may also be configured to indicate the number of prior uses of the probe 100.

As a further example, referring to Figure 7, it is possible that the same probe 100 can be used multiple times within a pre-defined period of time. The pre-defined period of time can be, for example, hours, days, weeks, or months. The probe 100 can be used a second or subsequent time if the second or subsequent use occurs during a pre-defined period of time following a prior or previous use of the probe 100. However, if the probe 100 is used outside of this authorized window, then the controller 115 can disable the console 110, thus requiring a new probe 100. The controller 115 can also be programmed to generate a warning or message as discussed with reference to Figure 6.

Another example is associating an authorized code with a console 100 and/or component 110 that are manufactured or used in a pre-defined geographic area, country or group of countries. Thus, when the received data satisfies the criteria 116, indicating that the geographic requirements are met, the controller 115 enables the console 110 to be used with the component 100.

Referring to Figure 8, according to another embodiment, the authorized security codes 520 can be serialized 800 so that particular lots or groups 810 of probes 100 can be identified based on the serialized codes. This may be helpful if, for example, there is a recall of a group of probes 100. The probes 100 that must be

recalled can be quickly identified using the serialized security code data 800 and defined lots or groups 810 of probes.

In a further embodiment, referring to Figure 9, the RFID tag 102 can include the identification data 300 and security data 400, as discussed above, and, in addition, calibration data 900, which is necessary to calibrate the console 110 to work with a particular probe 100 or component. For example, calibration data 900 may be instructions or parameter settings including, for example, laser calibration settings for a particular probe or adaptation. Each probe or adaptation may require the use of a different and unique optical fiber, which changes the optical coupling into the probe or adaptation, and therefore results in a particular calibration.

As a further example, when using a vitrectomy console, calibration data 900 may include instructions or parameter settings relating to laser probe transmissivity, pneumatic vitrecomy probe actuation pressure points, and endoilluminator transmissivity.

Indeed, other calibration may be used depending on the ophthalmic surgical device and component that are utilized. The console 110 can automatically calibrate itself based on the received calibration data 900. Alternatively, the console 110 can be calibrated by a surgeon using the received calibration data 900.

In addition, the identification and/or calibration data may used for various purposes including, for example, enabling or disabling operating parameters that are compatible with the identified component, and invoking certain safety features associated with the identified component. For example, the system may be configured to limit power ranges and/or exposure ranges given a particular type of component. Additionally, the system can be configured to determine whether safety accessories, such as filters, are present so that the identified component can be used without injury to the surgeon. Further, the identification and/or calibration data can be used to generate a user interface that is related to the particular component and presented on a display screen for a surgeon.

In a further embodiment, referring to Figure 10, the RFID readers and tags of the system and component can be configured to two-way or read/write applications 1000. This application may require larger RFID tag 102 data capabilities, e.g., >100 bytes. In this embodiment, the reader (or transceiver) can write different types of data back to the RFID tag 102 for future use or reference. For example, the RFID reader

112 can write information, such as the date of use of a probe 100, a number of times a probe 100 was used, the amount of time the probe 100 was active, the power setting of the probe 100 when active, etc. This information can be particularly useful when the probe 100 is used at a later time, because, for example, a surgeon can review the information and make an assessment regarding the wear and useful life of the probe 100. For example, the useful life of a probe 100 may be decreased when the probe 100 is active for a longer period of time, used at a higher power setting and used multiple times.

Considering the description of system embodiments, a method for identifying and controlling ophthalmic surgical devices and components is summarized in the flow charts shown in Figures 11A-B. Beginning with step 1100, a set of potential identification codes and a set of potential security codes are selected. The potential set of codes includes both authorized and unauthorized codes which will and will not satisfy a set criteria. In step 1105, a set of authorized codes is selected from the larger set of potential codes. In step 1110, the identifiers or RFID tags of authorized components, e.g., components from original manufacturers, are programmed with one of the authorized codes. In step 1115, if the controller implements a criteria based on comparing authorized data to data received from an identifier, the authorized codes are stored in memory of the ophthalmic laser system, such as an ophthalmic laser or vitreoretinal surgical device. If an algorithm is used, the algorithm can be stored in memory without storing authorized data.

In step 1120, a component is provided to be connected to the laser device. In step 1125, data from the RFID tag of the component is transmitted to the receiver or RFID reader in the laser device. The data received from the RFID tag is used to identify the component in step 1130. Data from the RFID device can be used for various purposes including, for example, generating a user interface for presentation on a display screen, enabling or disabling operating parameters that are compatible with the identified component, and invoking certain safety features associated with the identified component. For example, values of certain parameters, such as power and exposure, can be limited to ensure that the device is not operated outside of the specified ranges of operating parameters. Further, the system can be configured to check for safety equipment, such as a filter, that is used with the component.

In step 1135, the data from the RFID tag is processed to determine whether it satisfies certain criteria. In step 1140, the ophthalmic surgical device is disabled if the received data does not satisfy the criteria. In step 1145, the controller determines

whether the component has been used before. If the component is being used for the first time, the ophthalmic surgical device can be enabled to work with the component in step 1150. If the component has been used before, in step 1155, the ophthalmic surgical device can be conditionally enabled.

For example, the ophthalmic surgical device can be enabled if the probe has previously been used a certain number of times 1160 or has been previously used within a certain period of time 1165. The controller may also generate a message or warning 1170 for the user to indicate that the probe has been previously used or set the laser device to operate in a safe mode 1175, e.g., at lower power.

Persons skilled in the art will appreciate that there are various modifications that can be made without departing from the scope of embodiments. Embodiments can be used with other types of ophthalmic surgical equipment. Further, embodiments can be used for different purposes, including identification, calibration, compatibility, and lockout purposes. Thus, the illustrative examples set forth above are not intended to be limiting.

Although references have been made in the foregoing description to various embodiments, persons skilled in the art will recognize that insubstantial modifications, alterations, and substitutions can be made to the described embodiments without departing from the invention as claimed in the accompanying claims.

CLAIMS

WHAT IS CLAIMED:

1. A system for identifying a component that is used with an ophthalmic surgical device, comprising:

a receiver,

a radio frequency identification (RFID) tag;

a memory, the memory storing criteria; and

a controller, the controller, the memory and the receiver being included in the ophthalmic surgical device, the RFID tag being included in the component used with the ophthalmic surgical device, data from the RFID tag in the component being transmitted to the receiver in the ophthalmic surgical device,

the controller determining whether the component corresponding to the received data can be used with the ophthalmic surgical device based on whether the received data satisfies the criteria stored in the memory.

2. The system of claim 1, wherein the criteria is authorized data that is stored in the memory, data received from the identifier being compared to the authorized data to determine whether the component can be used with the ophthalmic surgical device.

3. The system of claim 1, wherein the criteria is an algorithm, the algorithm being applied to the data received from the identifier to determine whether the component can be used with the ophthalmic surgical device.

4. The system of claim 1, the ophthalmic surgical device being a laser.

5. The system of claim 4, the component being an optical probe that is attached to the laser.

6. The system of claim 1, the ophthalmic surgical device being a vitreoretinal surgical device.

7. The system of claim 6, the component being a vitrectomy probe that is attached to the vitreoretinal surgical device.

8. The system of claim 6, the component being a pneumatically or electrically powered scissors that is attached to the vitreoretinal surgical device.

9. The system of claim 6, the component being an endoilluminator probe that is attached to the vitreoretinal surgical device.

10. A system for identifying a component that is used with an ophthalmic surgical device, comprising:

a receiver,

an identifier;

a memory, the memory storing criteria; and

a controller, wherein the controller, the memory and the receiver are included in the ophthalmic surgical device, and the identifier is included in the component, data from the identifier in the component being transmitted to the receiver in the ophthalmic surgical device;

the controller determining whether the component corresponding to the received data can be used with the ophthalmic surgical device based on whether the data received from the identifier is an authorized code that satisfies the criteria stored in memory, authorized codes being selected from a larger set of available codes.

11. The system of claim 10, wherein the criteria is authorized data that is stored in the memory, data received from the identifier being compared to the authorized data to determine whether the component can be used with the ophthalmic surgical device.

12. The system of claim 10, wherein the criteria is an algorithm, the algorithm being applied to the data received from the identifier to determine whether the component can be used with the ophthalmic surgical device.

13. The system of claim 10, the receiver being a Radio Frequency Identification (RFID) reader.

14. The system of claim 10, the identifier being a Radio Frequency Identification (RFID) tag.

15. The system of claim 10, the data transmitted by the identifier being unencrypted.

16. The system of claim 10, wherein a number of authorized codes is at least three orders of magnitude greater than a number of available codes.

17. The system of claim 16, wherein one billion authorized codes are selected from one trillion available codes.

18. The system of claim 16, wherein the authorized codes are randomly selected from available codes.

19. The system of claim 10, the ophthalmic surgical device being a laser.

20. The system of claim 19, the component being an optical probe that is attached to the laser.

21. The system of claim 10, the ophthalmic surgical device being a vitreoretinal surgical device.

22. The system of claim 21, the component being a vitrectomy probe that is attached to the vitreoretinal surgical device.

23. The system of claim 21, the component being a pneumatically or electrically powered scissors that is attached to the vitreoretinal surgical device.

24. The system of claim 21, the component being an endoilluminator probe that is attached to the vitreoretinal surgical device.

25. The system of claim 10, the identifier data including 14 bytes, wherein 2 bytes are used to identify the component, and 12 bytes are used to identify one trillion available codes, including authorized and unauthorized codes.

26. The system of claim 10, the received data satisfying the criteria, the controller enabling the ophthalmic surgical device to be used with the component.

27. The system of claim 10, the controller being configured to determine a number of times the component has been used based on a number of times the same identifier data is received.

28. The system of claim 27, the component being used more than one time so that the same received data satisfies the criteria, the controller disabling the ophthalmic surgical device from being used with the component after a predetermined number of uses of the component.

29. The system of claim 27, the component being used more than one time so that the same received data satisfies the criteria, the controller generating a message to a user that the component has been previously used.

30. The system of claim 10, the controller disabling the ophthalmic surgical device from being used with the component after a predetermined amount of time following a use of the component.

31. The system of claim 10, the received data not satisfying the criteria, the controller disabling the ophthalmic surgical device from being used with the component.

32. The system of claim 10, the receiver being a transceiver, wherein the transceiver reads data from the identifier of the component and writes data to the identifier of the component.

33. The system of claim 32, the transceiver writing data to the identifier of the component relating to a date of usage, a number of uses of the component, a duration of use of the component, or a power setting of the component.

34. The system of claim 10, the data from the identifier including calibration data, the calibration data indicating the configuration of the ophthalmic surgical device for use with the component.

35. The system of claim 10, authorized codes being serialized so that a component is associated with a batch or lot of components, the batch or lot being defined by a components associated with a group of serialized authorized codes.

36. The system of claim 10, the criteria being associated with a pre-defined geographic area, when the received data satisfies the criteria, the controller enables the ophthalmic surgical device to be used with the component in the pre-defined geographic area.

37. A system for identifying a component that is used with an ophthalmic surgical device, comprising:

a receiver;

a radio frequency identification (RFID) tag;

a memory, the memory storing criteria; and

a controller, the controller, the memory and the receiver being included in the ophthalmic surgical device, the RFID tag being included in the component, unencrypted data from the RFID tag in the component being transmitted to the to the receiver in the ophthalmic surgical device,

the controller determining whether the component corresponding to the unencrypted data received from the RFID tag can be used with the ophthalmic surgical device based on whether the received data is an authorized code that satisfies the criteria stored in memory, authorized codes being selected from a larger set of available codes.

38. The system of claim 37, wherein the criteria is authorized data that is stored in the memory, data received from the identifier being compared to the authorized data to determine whether the component can be used with the ophthalmic surgical device.

39. The system of claim 37, wherein the criteria is an algorithm, the algorithm being applied to the data received from the identifier to determine whether the component can be used with the ophthalmic surgical device.

40. The system of claim 37, the receiver being a RFID reader.

41. The system of claim 37, wherein a number of authorized codes is at least three orders of magnitude greater than a number of available codes.

42. The system of claim 37, wherein one billion authorized codes are selected from one trillion available codes.

43. The system of claim 37, wherein the authorized codes are randomly selected from the larger group of available codes.

44. The system of claim 37, the ophthalmic surgical device being a laser.

45. The system of claim 44, the component being an optical probe that is attached to the laser.

46. The system of claim 37, the ophthalmic surgical device being a vitreoretinal surgical device.

47. The system of claim 46, the component being a vitrectomy probe that is attached to the vitreoretinal surgical device.

48. The system of claim 46, the component being a pneumatically or electrically powered scissors that is attached to the vitreoretinal surgical device.

49. The system of claim 46, the component being an endoilluminator probe that is attached to the vitreoretinal surgical device.

50. The system of claim 37, the unencrypted data including 14 bytes, wherein 2 bytes are used to identify the type of component, and 12 bytes are used to identify one trillion available codes.

51. The system of claim 37, the received data satisfying the criteria, the controller enabling the ophthalmic surgical device to be used with the component.

52. The system of claim 37, the controller being configured to determine a number of times the component has been used based on a number of times the same identifier data is received.

53. The system of claim 52, the component being used more than one time so that the same received data satisfies the criteria, the controller disabling the ophthalmic surgical device from being used with the component after a predetermined number of uses of the component.

54. The system of claim 52, the component being used more than one time so that the same received data satisfies the criteria, the controller generating a message to a user that the component has been previously used.

55. The system of claim 37, the controller disabling the ophthalmic surgical device from being used with the component after a predetermined amount of time following a use of the component.

56. The system of claim 37, the received data not satisfying the criteria, the controller disabling the ophthalmic surgical device from being used with the component.

57. The system of claim 37, the receiver being a transceiver, wherein the transceiver reads data from the identifier of the component and writes data to the identifier of the component.

58. The system of claim 57, the transceiver writing data to the identifier of the component relating to a date of usage, a number of uses of the component, a duration of use of the component, or a power setting of the component.

59. The system of claim 37, the data from the component including calibration data, the calibration data indicating the configuration of the ophthalmic surgical device for use with the component.

60. The system of claim 37, authorized codes being serialized so that a component is associated with a batch or lot of components, the batch or lot being defined by a components associated with a group of serialized authorized codes.

61. The system of claim 37, the criteria being associated with a pre-defined geographic area, when the received data satisfies the criteria, the controller enables the ophthalmic surgical device to be used with the component in the pre-defined geographic area.

62. A method of identifying a component that can be used with an ophthalmic surgical device, comprising:

providing an ophthalmic surgical device and a component that is attached to the ophthalmic surgical device;

establishing criteria and storing the criteria in a memory of the ophthalmic surgical device;

transmitting data from an identifier in the component to a receiver in the ophthalmic surgical device;

determining whether the component corresponding to the received data can be used with the ophthalmic surgical device based on whether the received data is an authorized code that satisfies the criteria stored in the memory.

63. The method of claim 62, establishing criteria comprising selecting authorized data that is stored in the memory, data received from the identifier being compared to the authorized data to determine whether the component can be used with the ophthalmic surgical device.

64. The method of claim 62, establishing criteria comprising selecting an algorithm, the algorithm being applied to the data received from the identifier to determine whether the component can be used with the ophthalmic surgical device.

65. The method of claim 64, selecting the algorithm comprising selecting a random number generator algorithm.

66. The method of claim 62, further comprising identifying the type of component based on the identifier data.

67. The method of claim 66, further comprising generating a user interface for presentation on a display screen based on the identified component.

68. The method of claim 66, further comprising enabling operating parameters that are compatible with the identified component.

69. The method of claim 66, further comprising disabling operating parameters that are incompatible with the identified component.

70. The method of claim 66, further comprising limiting a value of an operating parameter based on the identified component.

71. The method of claim 66, limiting the value of the operating parameter comprising limiting a value of power or an exposure range.

72. The method of claim 66, further comprising determining the presence of a safety component that is associated with the identified component.

73. The method of claim 72, determining the presence of the safety component comprising determining the presence of a filter.

74. The method of claim 62, transmitting data from the identifier to the receiver comprising transmitting data to a Radio Frequency Identification (RFID) reader.

75. The method of claim 62, transmitting data from the identifier comprising transmitting data from a RFID tag.

76. The method of claim 62, further comprising selecting authorized codes from a larger set of available codes.

77. The method of claim 62, selecting authorized codes comprising selection a number of authorized codes from a number of available codes that is at least three orders of magnitude greater than a number of authorized codes.

78. The method of claim 62, transmitting data from the identifier in the component to the receiver in the ophthalmic surgical device comprising transmitting unencrypted data.

79. The method of claim 62, providing the ophthalmic surgical device comprising providing a laser.

80. The method of claim 79, providing the component comprising providing an optical probe that is attached to the laser.

81. The method of claim 62, providing the ophthalmic surgical device comprising providing a vitreoretinal surgical device.

82. The method of claim 81, providing the component comprising providing a vitrectomy probe that is attached to the vitreoretinal surgical device.

83. The method of claim 81, providing the component comprising providing a pneumatically or electrically powered scissors that is attached to the vitreoretinal surgical device.

84. The method of claim 81, providing the component comprising providing an endoilluminator probe that is attached to the vitreoretinal surgical device.

85. The method of claim 62, the received data satisfying the criteria, further comprising enabling the ophthalmic surgical device to be used with the component.

86. The method of claim 62, further comprising determining a number of times a component has been used.

87. The method of claim 86, further comprising disabling the ophthalmic surgical device from being used with the component after a predetermined number of uses of the component.

88. The method of claim 86, further comprising generating a message that the component has been previously used.

89. The method of claim 62, further comprising determining a duration of time following a use of the component.

90. The method of claim 89, further comprising disabling the ophthalmic surgical device from being used with the component after a predetermined amount of time following a use of the component.

91. The method of claim 62, further comprising writing data to the identifier of the component.

92. The method of claim 91, writing data comprising writing a date of usage, a number of uses of the component, a duration of use of the component, or a power setting of the component to the identifier of the component.

93. The method of claim 62, data from the identifier of the component including calibration data, further comprising calibrating the ophthalmic surgical device for use with the component based on the calibration data.

94. The method of claim 62, further comprising

serializing authorized codes; and

defining a group or lot of components based on the serialized codes.

95. The method of claim 62, further comprising

encoding the identifier in the component with data with an authorized code that satisfies the criteria, and

transmitting data comprising transmitting the encoded data from the identifier in the component to the receiver in the ophthalmic surgical device.

Fig. 1

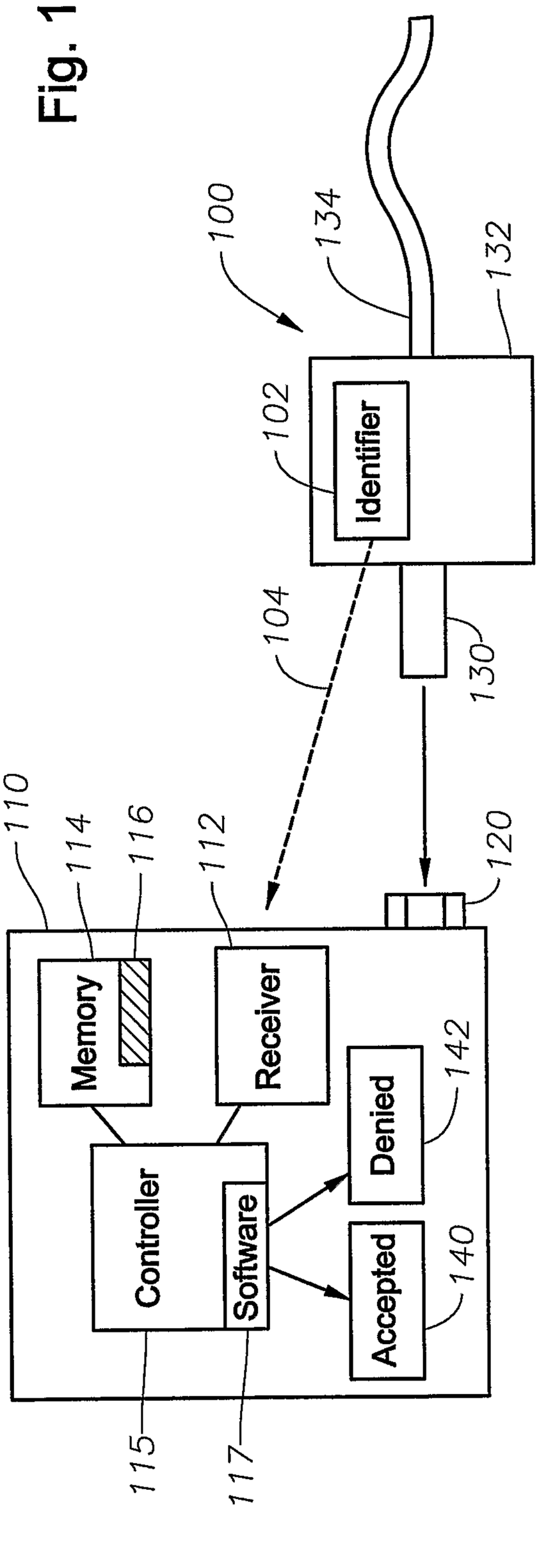

100
102
Identifier
104
130
132
134
110
112
114
115
116
117
120
Memory
Receiver
Controller
Software
Denied
Accepted
140
142

Fig. 2

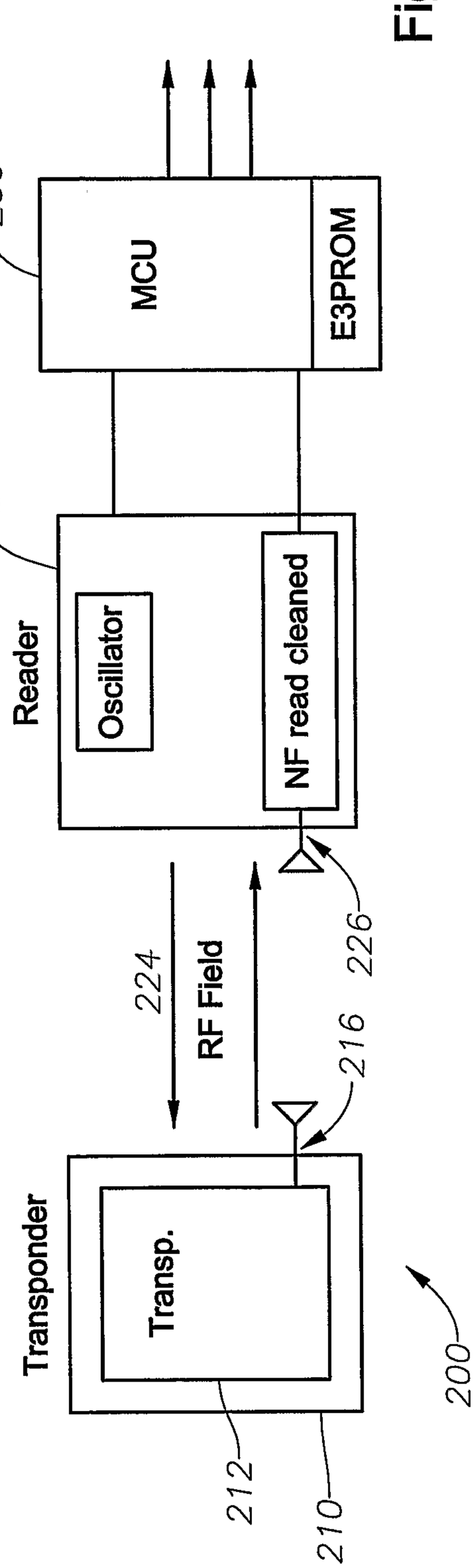

230
MCU
E3PROM
220
Reader
Oscillator
NF read cleaned
224
RF Field
226
216
Transponder
Transp.
212
210
200

Fig. 3

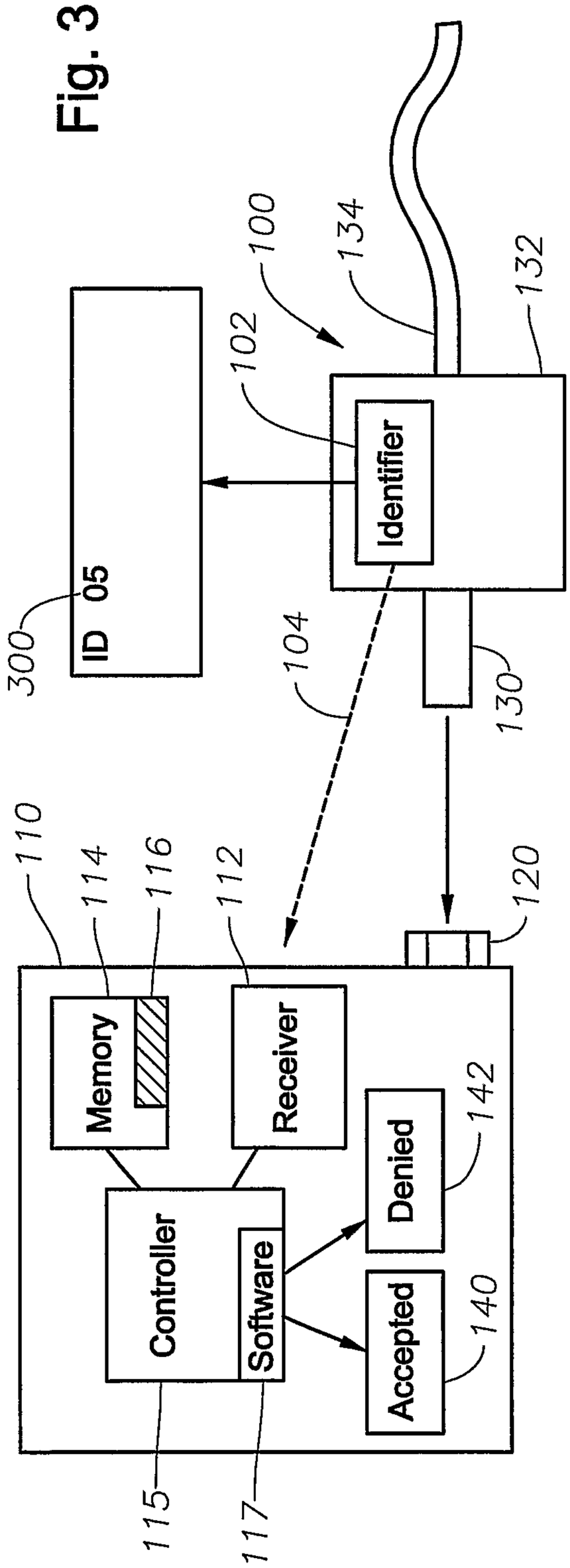

100
134
132
102
Identifier
ID 05
300
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117

Fig. 4

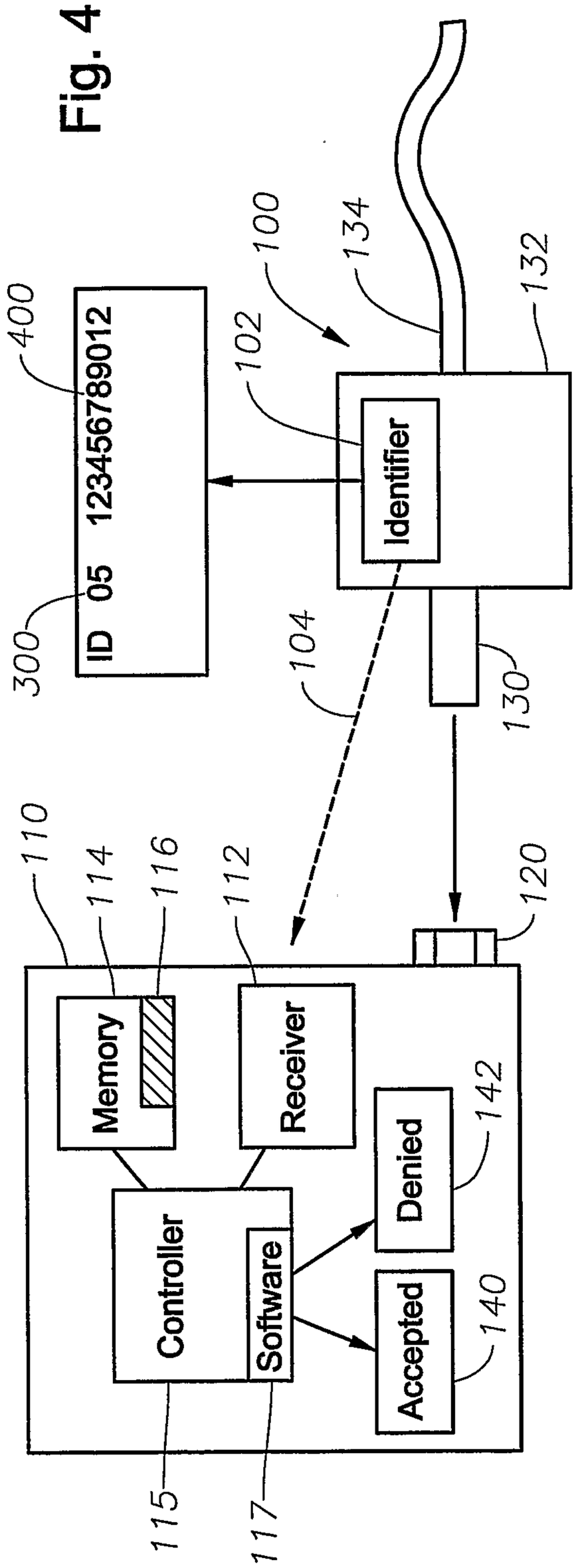
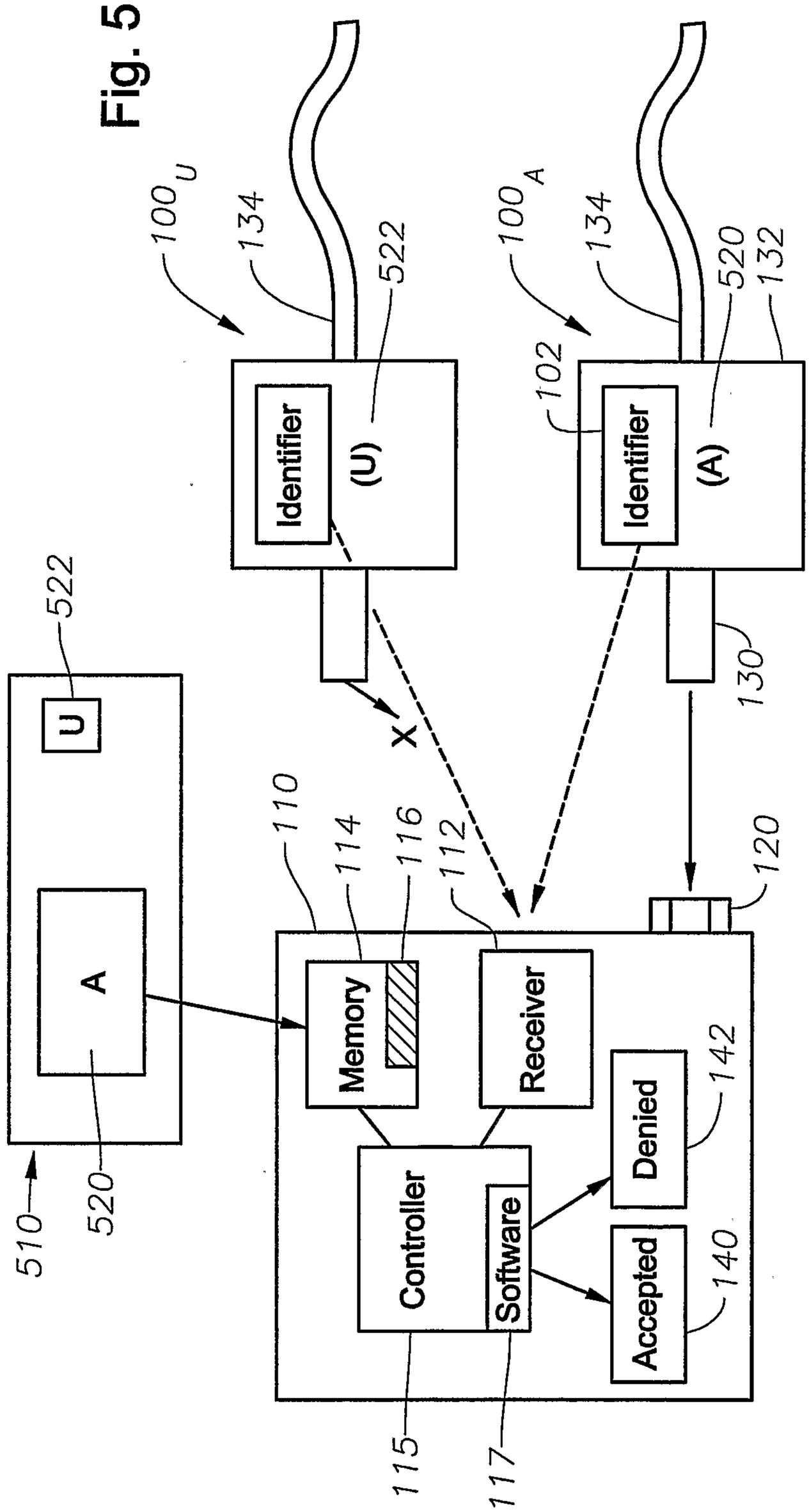

400
ID 05 123456789012
300
100
102
134
132
Identifier
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117

Fig. 5


100U
134
522
100A
134
520
132
102
Identifier
(U)
Identifier
(A)
522
U
A
510
520
130
X
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117

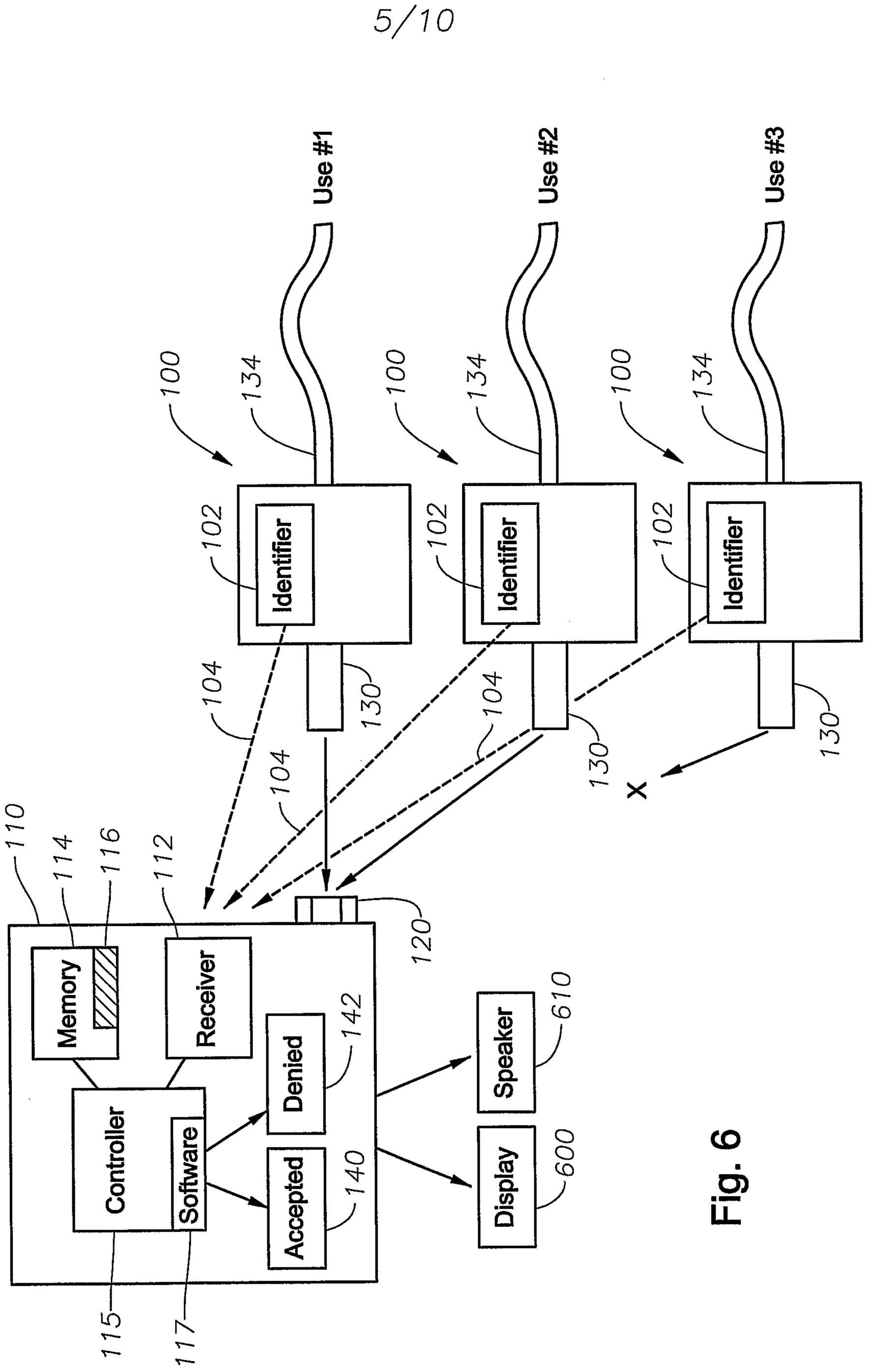

Use #1
Use #2
Use #3
100
134
102
Identifier
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
Speaker
610
Display
600
115
117
X

Fig. 6

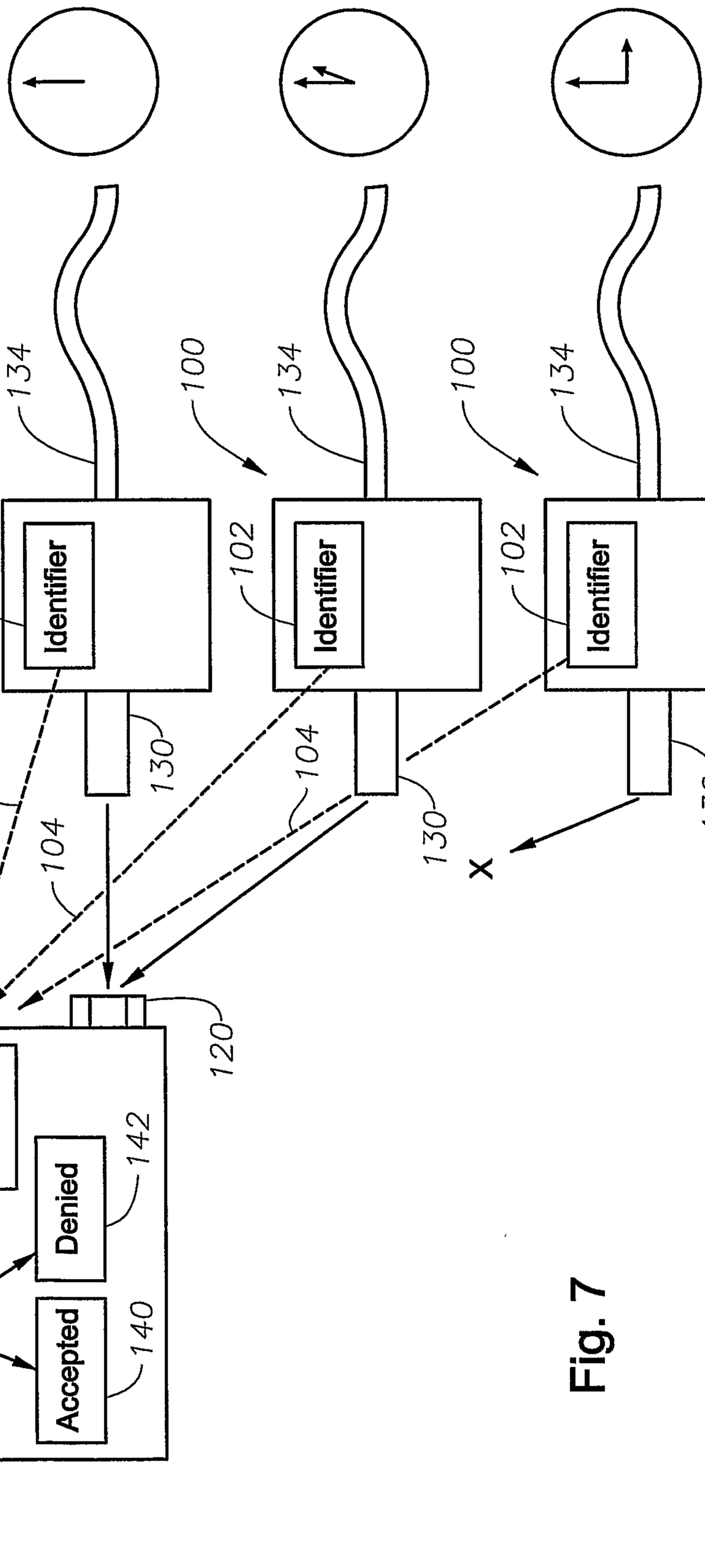

100
134
102
Identifier
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117
X

Fig. 7

Fig. 8

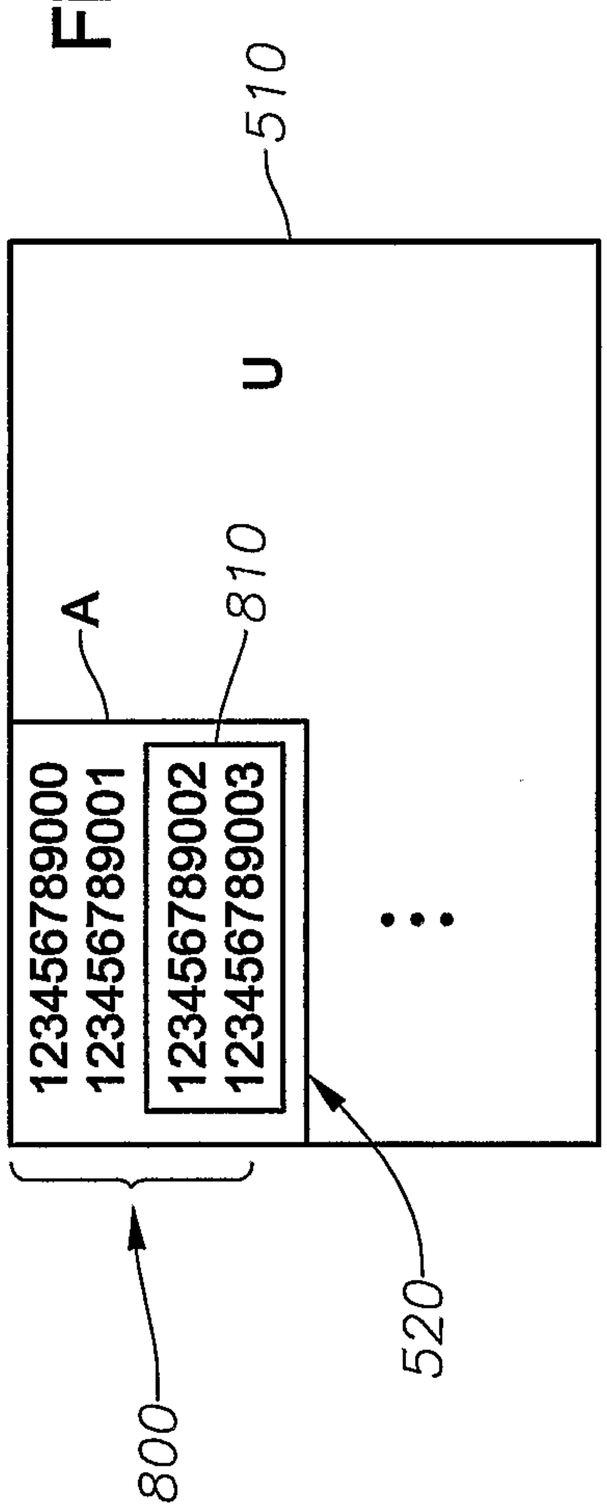

510
U
A
810
123456789000
123456789001
123456789002
123456789003
800
520

Fig. 9

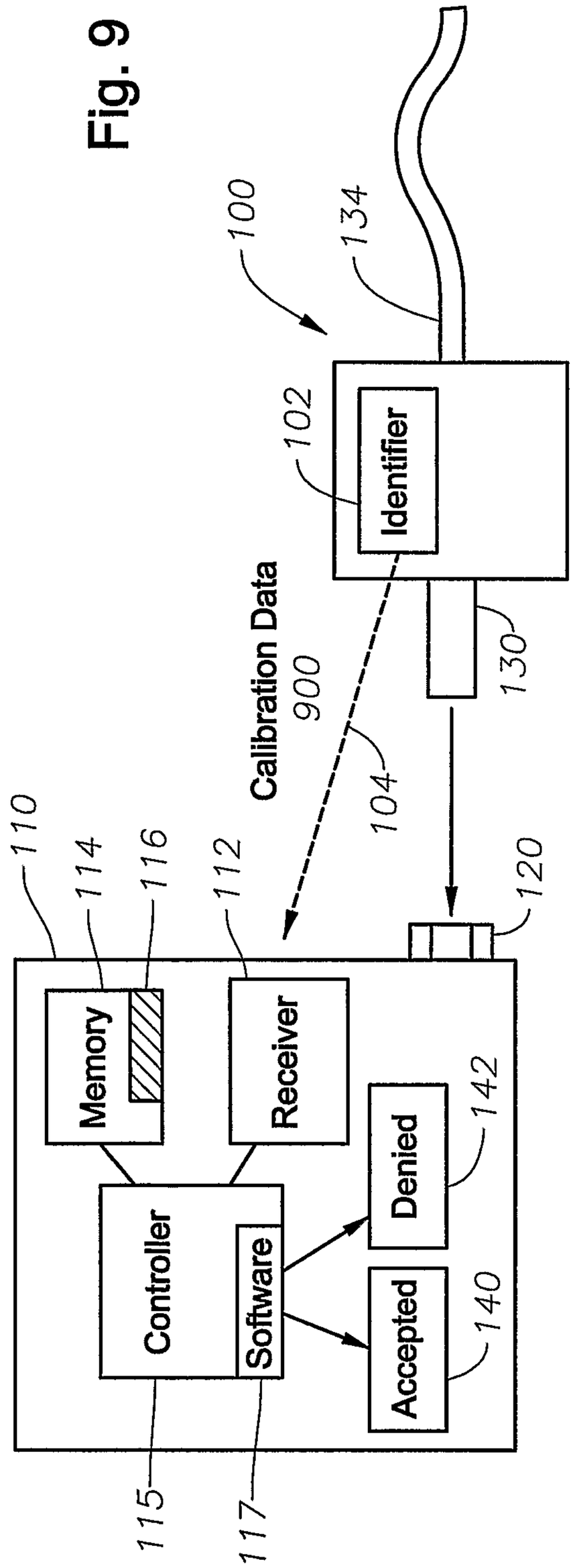
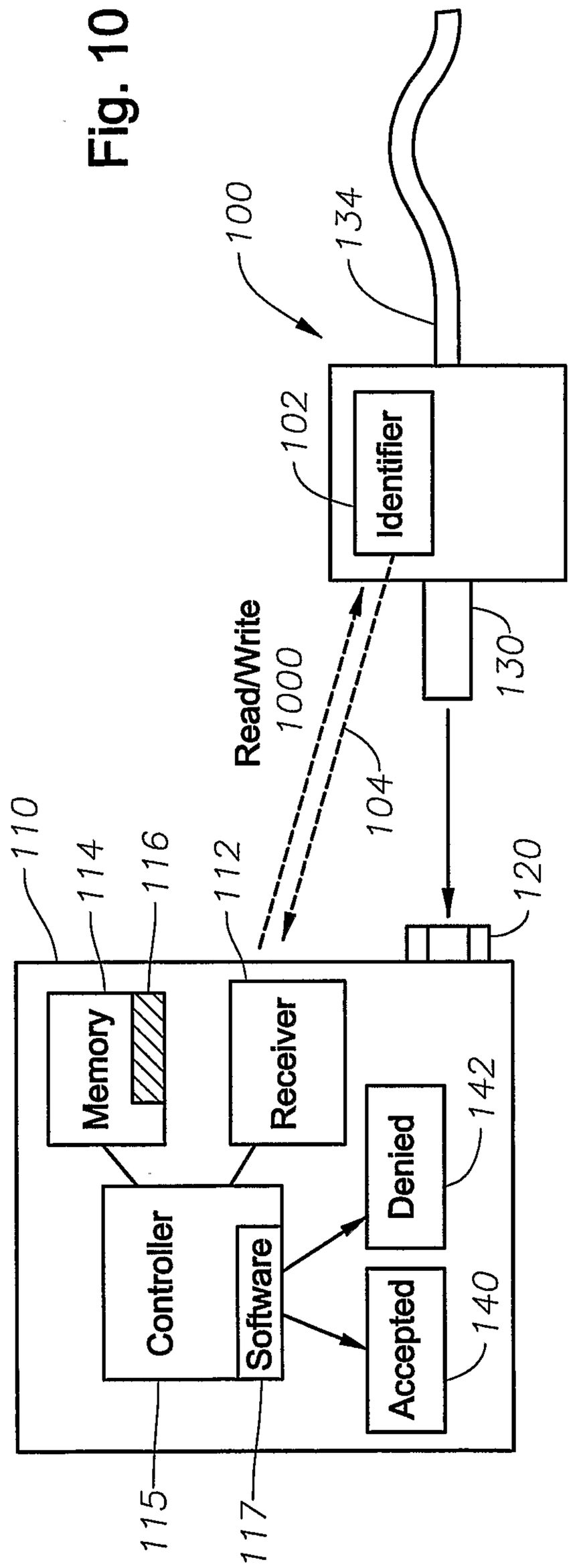

100
134
102
Identifier
Calibration Data
900
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117

Fig. 10


100
134
102
Identifier
Read/Write
1000
104
130
110
114
116
112
120
Memory
Receiver
Controller
Software
Denied
142
Accepted
140
115
117

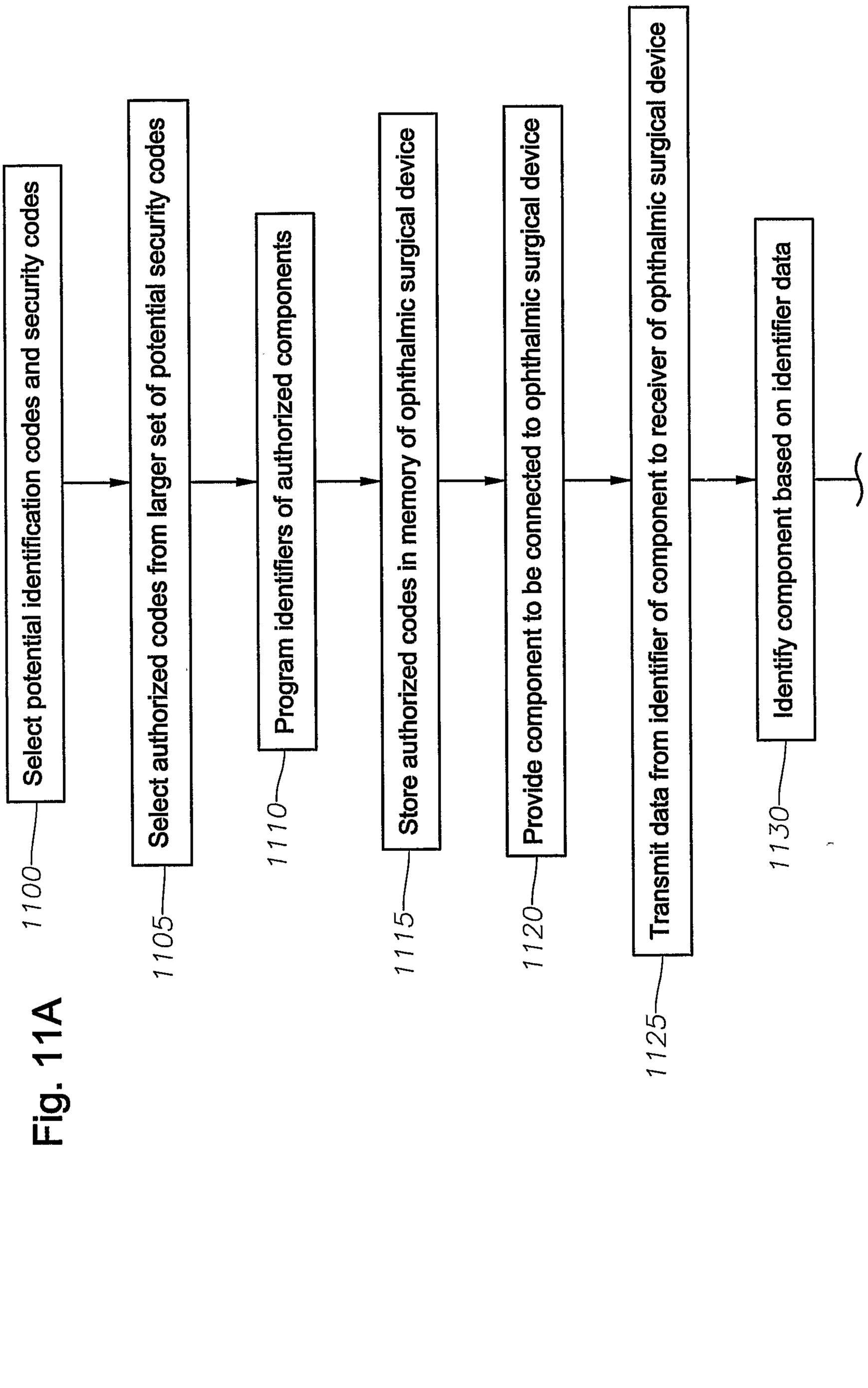
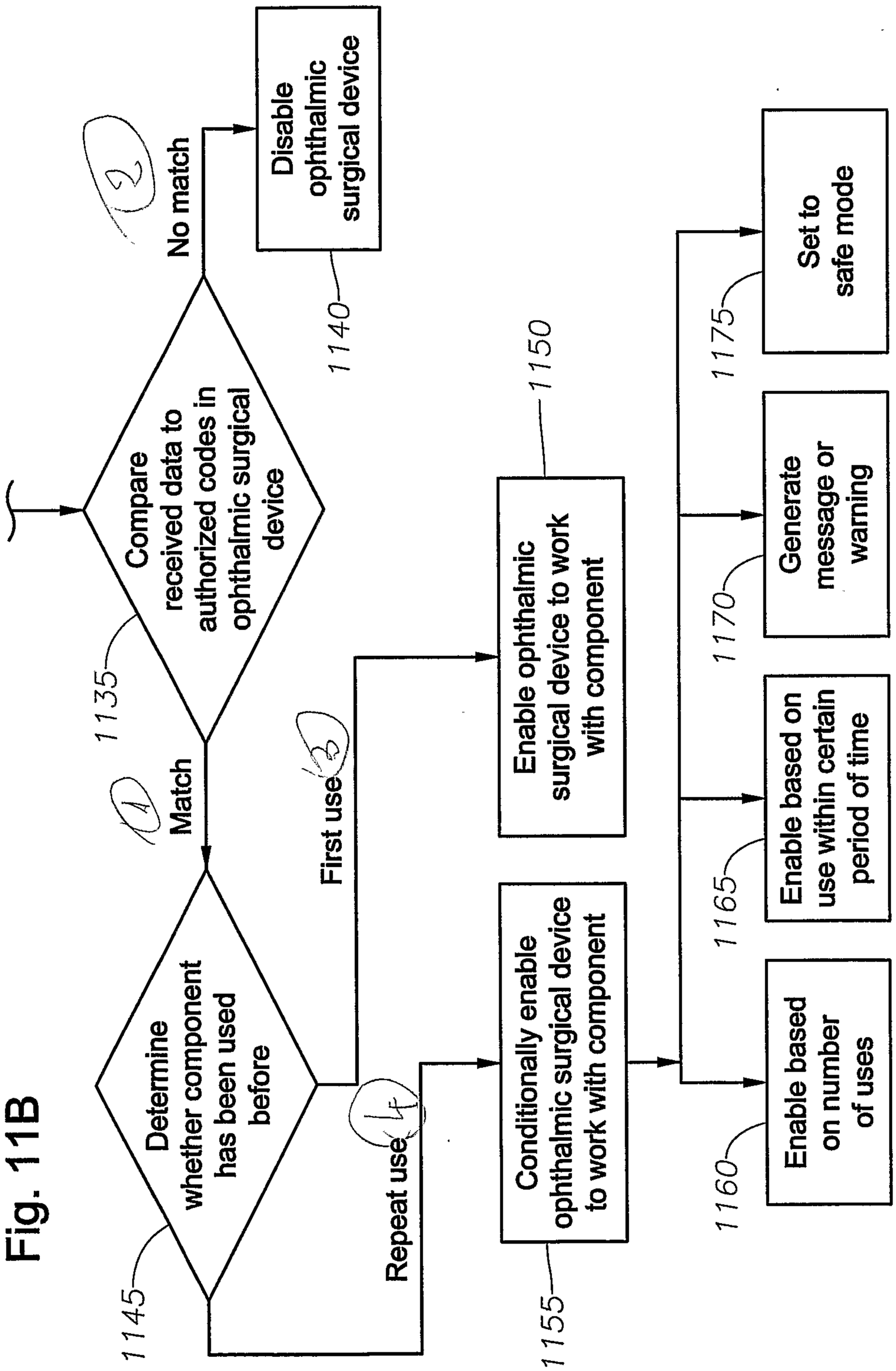
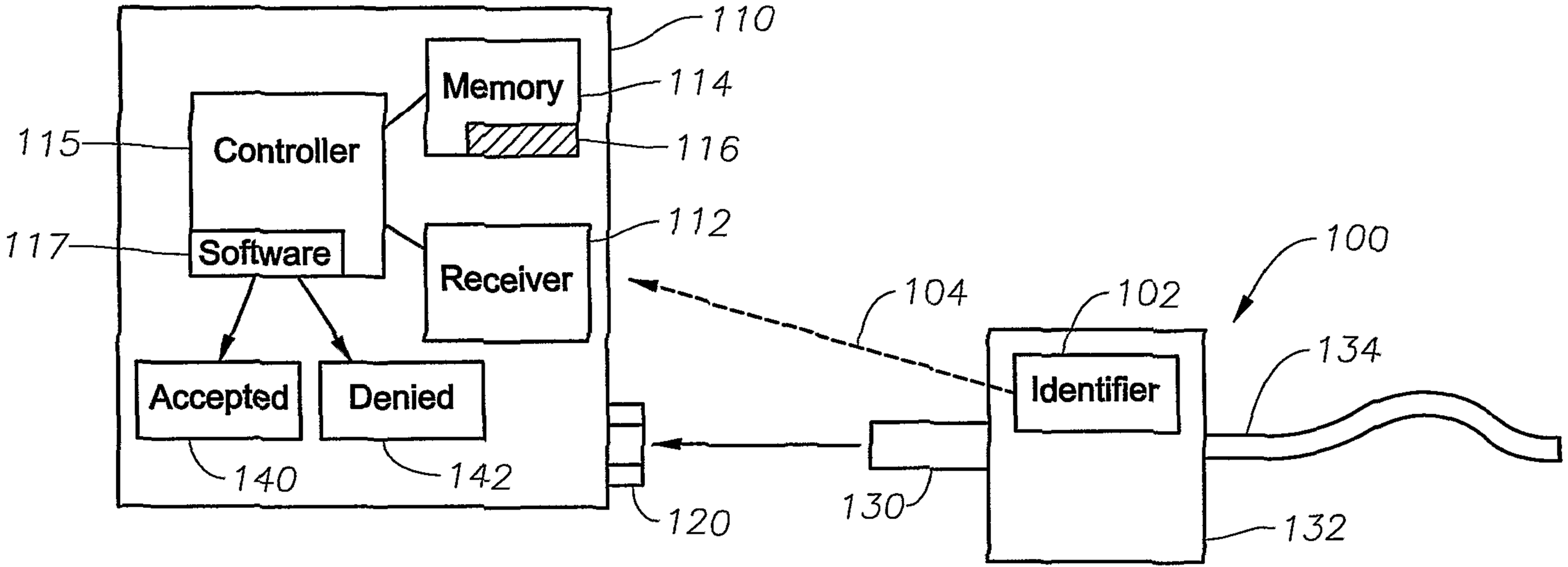

Select potential identification codes and security codes
1100
Select authorized codes from larger set of potential security codes
1105
Program identifiers of authorized components
1110
Store authorized codes in memory of ophthalmic surgical device
1115
Provide component to be connected to ophthalmic surgical device
1120
Transmit data from identifier of component to receiver of ophthalmic surgical device
1125
Identify component based on identifier data
1130

Fig. 11A

Fig. 11B


Compare received data to authorized codes in ophthalmic surgical device
1135
No match
Disable ophthalmic surgical device
1140
Match
Determine whether component has been used before
1145
First use
Enable ophthalmic surgical device to work with component
1150
Repeat use
Conditionally enable ophthalmic surgical device to work with component
1155
Enable based on number of uses
1160
Generate message or warning
1170
Enable based on use within certain period of time
1165
Set to safe mode
1175


110
Memory
114
115
Controller
116
112
117
Software
Receiver
100
104
102
Accepted
Denied
Identifier
134
140
142
130
120
132