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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2004 (29.04.2004)

PCT

(10) International Publication Number
WO 2004/036521 A2

(51) International Patent Classification[7]: G08B 13/14

(21) International Application Number:
PCT/IB2003/004460

(22) International Filing Date: 8 October 2003 (08.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0223956.4 15 October 2002 (15.10.2002) GB

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MARSHALL, Christopher, B.** [GB/GB]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB). **CHAMPSAUR, Marc, H., J.** [FR/FR]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB). **HARLASHKIN, Igor, A.** [RU/RU]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB). **RIMMINGTON, Andrew, K.** [GB/GB]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB). **WALBROU, Pascal, R., M.** [FR/FR]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

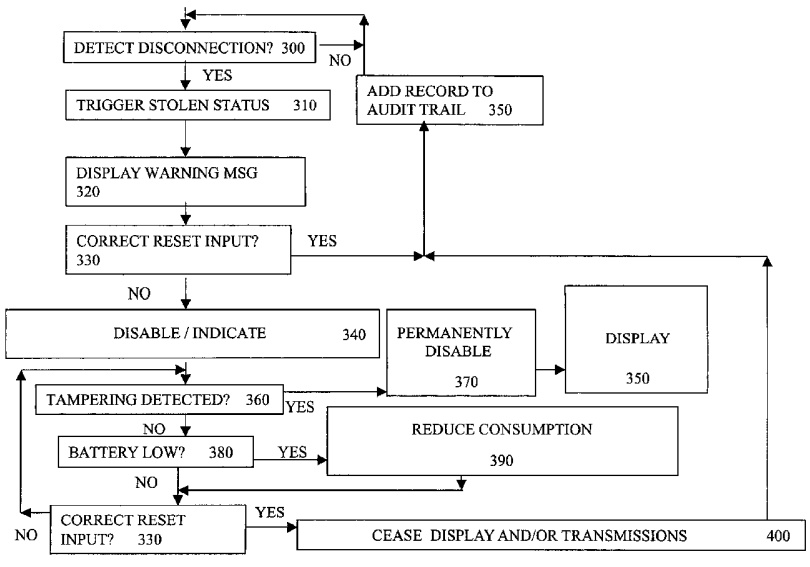
(74) Agent: **WHITE, Andrew**; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, 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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: SECURITY STATUS INDICATION FOR CONSUMER EQUIPMENT



(57) Abstract: An anti-theft system (40) for consumer equipment has a detector (10) for detecting theft by detecting disconnection of the consumer equipment from a network for power supply or for information transfer. This is used to cause a stolen status indication (20, 340) on the consumer equipment. The indication can be a display or RF transmission, and is persistent to deter possession of the equipment, but being removable by a secure reset process(100). This indication makes it riskier for a thief to possess stolen equipment that shows its stolen state, even when switched off, and even after lengthy storage. It is also harder to sell the stolen goods and hence it can deter theft. Similar principles can be applied to indicate on rented or shared equipment, a status of the equipment including a current user.

WO 2004/036521 A2

ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, 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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

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.

SECURITY STATUS INDICATION FOR CONSUMER EQUIPMENT

FIELD OF THE INVENTION

The invention relates to anti theft systems for consumer equipment, to display modules having such systems, to corresponding methods and software, to methods of offering a service of providing reset keys for such systems, to methods of detecting stolen equipment, and to management systems for monitoring use of portable equipment by many users.

BACKGROUND

It is known from European patent application 0,852,367 (Siemens) to provide an anti-theft system for electrical goods e.g. video recorders, by periodically transmitting identification numbers to a controller via the mains electricity supply. If the controller does not receive a particular identification number for a predetermined time, it assumes the item is stolen and raises an alarm. United States patent 5,963,131 shows theft protection systems for portable electrical items such as lap top computers. A motion detector and/or proximity detector detects the theft and triggers an audible alarm.

U.S.patent 6,150,923 (Johnson , et al.) provides an anti-theft system for example for a car radio, domestic electrical items, or electrical office items such as computers, video recorders, televisions or the like which locks the device off when theft is detected. Such detection involves detecting disconnection from its power supply, or when a movement detector such as a tilt detector is triggered. An audio alarm signal can also be provided, supplied by its own on board battery. In the case of the car radio, when the device is re-connected and switched on, a security code must be entered to enable the radio to operate. If the system is incorporated into a mobile phone, the alarm may include sending a message to a predetermined location. If the system is incorporated into a component of a computer, the alarm may include displaying a message on the screen of, or disabling the operation of any computer that the component is subsequently used in. A disadvantage of all these types of anti-theft system, is that while the equipment is not connected, it

is not immediately obvious whether it has been stolen, once the audio alarm has exhausted its battery.

It is also known to provide electronic tags attached to consumer equipment to deter theft. As shown in US patent 6,317,028 (Valiulis), such tags can be coupled to control electronics of the equipment to disable the equipment unless the tag receives a predetermined security code. The tag enables the security code to be received regularly by a short range RF interface or by mains power supply signalling system, from a central controller elsewhere in the consumer premises. Again there is nothing to help indicate the goods have been stolen, once the alarm is exhausted.

It is also known to provide a theft deterrent system for shop displays using tags attached to the products which if tampered with, cause the product and perhaps the thief, to be marked with an indelible dye. Although this is effective in making it obvious that the goods have been stolen, it is not removable, and not suitable for deterring theft from consumers premises for obvious reasons. It is also known to provide tracker systems for indicating the whereabouts of stolen cars. In this case a small radio transmitter is hidden in the car, capable of communicating with a nationwide radio network. It is normally not connected to the network, and is switched on and connected to the network only when triggered by the user reporting the theft and the identity of the car.

SUMMARY OF INVENTION

It is an object of the invention to provide improved apparatus or methods, addressing such problems. According to a first aspect of the invention, there is provided an anti-theft system for consumer equipment, the equipment in normal use having a connection to a network for power supply or for information transfer, the system having:

a detector for detecting disconnection of the consumer equipment indicating theft of the equipment, and

the system being arranged to respond to such a detection by causing a stolen status indication on the consumer equipment, the indication being

autonomous of the equipment being switched off, and being persistent to deter possession of the equipment, but being removable by a secure reset process.

An advantage of such a system is that it is riskier for a thief to possess such equipment that shows its stolen state, even when switched off, and even after lengthy storage. Also, it can make it harder for a thief to sell such equipment onwards, if a cursory inspection by prospective purchasers shows its status and discourages them from purchase, and hence it can act as an effective theft deterrent. The inventors have appreciated that alarms on such devices do not provide sufficient deterrent because the thief can often choose a time and place when there is little chance of people hearing or reacting to the alarm. As such alarms require high power input, if powered by battery, they will quickly run out of power, and so cannot provide a persistent indication of stolen status. The duration of the persistence should be sufficient to deter thieves from storing the goods until the indication power supply runs out, if the indication needs a power supply. This will depend on the rate at which the product is superseded, which will vary from product to product. Persistence can be for a substantial proportion of the shelf life, which can encompass periods of months or years for goods like car audio equipment, which develop technically and in appearance so as to lose much of their sale value within a few years or less. Similarly, the inventors realised that previous methods involving secure codes to be entered when the equipment is switched on, offer insufficient deterrent to illegal possession at least. The network can be a dedicated security network or a network having another primary purpose such as power supply or telecommunications. The term consumer equipment is intended to encompass any equipment which is sufficiently portable to be susceptible to theft, including computer equipment, household appliances, household electronics, and similar equipment used by organisations including schools, hospitals and businesses for example.

Additional features of some embodiments encompassed by the invention include the indication comprising a visible display, the display being a low power operating display of the consumer equipment, the indication

comprising an RF signal, or the enabling of a passive RF tag, having an internal battery to power the indication, having a tampering detector for detecting tampering with the system, or disabling the equipment permanently, in the event of detecting tampering. Further such features include outputting the indication intermittently, or only when movement is detected, the system being arranged to output an identifier traceable to the rightful owner, the system containing a unique key and arranged to receive another key and verify whether it is a matching key, to enable the reset process, or enable operation of the equipment, or the system being arranged to store permanently an audit trail of detection events.

Another aspect of the invention provides a display module for consumer equipment, the module having the above system.

Another aspect provides consumer equipment having the above system.

As an additional feature of particular embodiments, the equipment can be a computer, or a games console, or audio or video equipment for household or in- car use.

Another aspect provides a method of offering a service of providing a key on request for resetting the indication of theft as set by the above system, module or equipment, to a rightful owner of the equipment.

Another aspect provides a method of detecting stolen equipment, the method having the step of using an RF receiver to recognise an RF indication of a stolen status output by the above consumer equipment.

Another aspect provides software for consumer equipment, the equipment in normal use having a connection to a network for power supply or for information transfer, the software being coupled to a detector for detecting disconnection of the consumer equipment indicating theft of the equipment, and being arranged to respond to such a detection by causing a stolen status indication on the consumer equipment, the indication being autonomous of the equipment being switched off, and being persistent to deter possession of the equipment, but being removable by a secure reset process.

This aspect is claimed explicitly since such software can be a valuable, separately tradable commodity. Also, it is also intended to encompass software which "describes" or defines the configuration of hardware, such as HDL (hardware description language) software, as is used for designing silicon chips, or for configuring universal programmable chips, to carry out desired functions. It is not essential that all the software be located on the consumer equipment, conceivably the detection could be located in the network, and a command to set the indication could be sent to the consumer equipment form a remote location.

Another aspect provides a management system for monitoring use of portable equipment, the equipment being available for use by many users, the system having:

a detector for detecting removal of the equipment from a store, where the equipment is connected to a network for power supply or information transfer and

an indicator coupled to the detector for providing an indication on the equipment of its status following a detection of removal, including which of the users was responsible for taking it from the store.

This can bring advantages of clarity and transparency of responsibility for equipment, which in turn can lead to the equipment being maintained better and being utilised more efficiently. This has benefits whether the equipment is shared, lent, or rented, for example. Applications include hospitals, schools, centres for servicing equipment in the field, and rental shops for equipment including tools, electrical equipment, and media such as books, software, computer games, and video or audio recordings.

As an additional feature of particular embodiments, the indication includes an indication of a time limit or usage limit, or any combination of the additional features set out above.

Features of dependent claims can be combined with the features of any of the independent claims as would be apparent to those skilled in the art. Other advantages of the features will be apparent to those skilled in the art.

BRIEF DESCRIPTION OF DRAWINGS

To show by way of example how the invention can be implemented, embodiments will now be described with reference to the figures in which:

Fig 1 shows an overview of an embodiment,

Fig 2 shows a functional view of an embodiment,

Fig 3 shows an in car equipment embodiment,

Fig 4 shows a household equipment embodiment,

Fig 5 shows a chain of those parties affected by embodiments, and

Fig 6 shows an overview of a use management embodiment.

DETAILED DESCRIPTION

In at least some of the embodiments described, a stolen status is activated and maintained even if the equipment is switched off or disconnected from its normal power supply. The stolen status is made apparent in one or more ways, to potential buyers, and to the police so that the equipment is harder to sell and riskier to possess. The status may be displayed on the equipment and/or indicated by RF transmissions which can be detected by monitoring equipment which could be used by police or private security service agencies.

Figure 1 shows an overview including an anti theft system 40 in consumer equipment. The consumer equipment can be household, business or in-car equipment for example. It can be anything portable and valuable enough to be worth stealing, including computers, computer accessories, games consoles, audio or video equipment, modules, discs or cartridges having software or any valuable content for example. Consumer premises 80 can be a house, office, retail premises, school, hospital, vehicle, and so on. A disconnection detector 10 located optionally in the equipment or outside, detects a stolen state based at least in part on disconnection from a network 50 which can be a power supply, information network, base station or similar. If the equipment is portable and intended for mobile use, such as a camera, then the detection of theft could be delayed by a day for example, after

disconnection is detected. This could enable use for a day away from home or office without triggering an alarm for example.

The consumer equipment includes an indicator 20 giving out a persistent indication of the stolen status. The indicator can be a low power display such as an LCD (liquid crystal display), or a mechanical display which uses no power except to change state, for example. It can either be a dedicated display or be used for other purposes such as showing normal operation messages, as track number on a DVD player, or tuning information on a radio. The indicator can also include an addition or an alternative, an RF transmitter for sending the stolen status. Again this can be a dedicated transmitter, or be used for other purposes. It can be active or passive, in the sense of being arranged to transmit only when interrogated, or passive in the sense of using the received signal to power the response transmission. It can be an RF transmitter, using well known standards for short range transmission, e.g. less than 100m, such as Bluetooth, ZigBee, or cellular phone standards such as GSM, to enable use of SMS. Another alternative is to use optical frequencies such as infra red.

To increase the anti theft deterrence, the indicator and optionally other parts are preferably made resistant to tampering. This can be achieved by having a back up battery, by monitoring that the battery back up is not disconnected, and monitoring that the indication is still functioning. The display and the RF transmitter can be monitored by checking impedance and current consumption for example, or by measuring light or RF output respectively, for example.

Fig 1 also shows interactions with the environment outside the consumer equipment, such as potential buyers 90 seeing the display or checking the RF emissions. Police 70 may read the displays, or have RF detectors for detecting RF emissions showing the status. These may be located anywhere, including at sales locations for second hand equipment, at transport hubs such as ports, airports, road junctions and so on. Also shown is an external authorised resetting service 60, for resetting the indication once the stolen goods are returned to their owner, or in the case of false detection

of theft. The service sends a resetting key to the equipment once it is satisfied the goods are not stolen. This key is used by a secure resetting process 100 in the consumer equipment, which verifies the key matches an internal identifier or key.

Alternatively or as well, the secure reset process can be carried out with a matching key 30 provided by the consumer from elsewhere on the consumer premises. This can be a PIN (personal identification number) remembered and entered manually by the consumer, or sent automatically from a household security controller over mains signalling or RF, for example.

Figure 2 shows an example of functional steps of an embodiment of an anti theft system, such as that of fig 1. This may be embodied in software running on standard hardware such as a general purpose single chip microprocessor, or application specific integrated circuit for example. At step 300, if disconnection is detected, optionally supported by other factors indicating theft, such as unexpected operation or movement, then at step 310, stolen status is triggered. At step 320 optionally a message is displayed to warn a genuine user that theft has been detected. This message may warn of the consequences and prompt the user for a reset code. At step 330, if the correct reset code is entered within a given time limit, then no action is taken other than making a record in the audit log at step 350, and the process returns to step 300 to await another detection. The code can be in any form including biometric identifiers of a genuine owner for example.

If no correct reset is received, at step 340, the equipment is disabled temporarily, and an indication of the stolen status is displayed and or transmitted persistently. The indication can include an identifier in the form of information such as post code information to enable the owner to be traced, or coded information which the maker or retailer can relate to the owner or owner's address. It could indicate the value or type of the equipment, to aid police or other agencies to prioritise recovery efforts. This identifier can be output in a number of ways, including as part of the indication, or only when interrogated by an authorised system or person, to save battery power. Where the indication is a display, the identifier could be displayed in response to key

presses. Where the indication is an RF signal, an authorised RF detector could request further information. The equipment could enter a dialogue with the detector and send the identifier and other information on request to the detector.

Next a loop with three main actions is undertaken repeatedly at steps 360, 380, and 330, for which the order is not critical. At step 360, a check for tampering is carried out, as described above. (Of course this can be carried out continuously.) If tampering is detected, at 370, the equipment is permanently disabled, for example by deleting software, or ceasing to respond to requests from the equipment to enable it to operate. Preferably there should be a clear warning somewhere on the equipment of the consequence of tampering. At step 350, an indication of the permanent disabling is shown, and/or transmitted, and a corresponding record added to the audit log.

At step 380, a check on the level of the back up battery is carried out. If low, at step 390, consumption is reduced by displaying or transmitting intermittently, or only when movement is detected, or when the equipment detects inspection or interrogation in any form. At step 330, the system checks for a correct reset input. If no, the stolen status remains and the system repeats steps 360, 380 and 330. If yes, the indication of stolen status ceases, and after making an appropriate entry in the audit log, the system returns to step 300 to await another detection. The audit log can be stored in secure non volatile memory with appropriate safeguards to prevent unauthorised access or tampering, following established implementation methods.

In Figure 3, some of the principal hardware elements of an example of an anti theft system 440 for in car consumer equipment 430 are shown. The equipment could be a car radio, CD player, navigation system, traffic information system, television or video player or games player, for example. A microprocessor 450 is coupled to a low power display such as an LCD, to a back up battery 500, a disconnection detector 470, an audio alarm 490, and to an RF transmitter 495, including RF circuitry and an aerial, optionally in the form of an RF tag, either passive or active. The disconnection detection can optionally be carried out directly by the microprocessor or be detected by other

functions 480 of the equipment. It can be arranged to detect disconnection from the 12 volt supply from the car battery, or disconnection from the car aerial for example.

The microprocessor is arranged to run software for the rest of the functions of figure 2. It is arranged to drive the display, monitor the battery, establish the stolen status, and reset the stolen status under secure conditions, using a code or identifier held securely on chip or elsewhere. The microprocessor also drives the RF transmitter, checks for tampering, and optionally disables the equipment either temporarily or permanently. Another optional feature is an alarm, triggered by the stolen status, provided this does not drain the back up battery. The alarm could be provided with its own supply, or coupled so as to use a car alarm system.

The system 440 can be constructed in the form of a display module, with back up battery, microprocessor and RF transmitter built in. The module can accept inputs from the other functions of the equipment to enable the display to be used for normal operating messages, either to drive part of the display directly, or via the microprocessor.

In figure 4, a similar embodiment is shown, but arranged for household rather than in car equipment. Similar reference numerals have been used as appropriate. In this case, the disconnection detection can detect disconnection from a mains supply. A movement detector 520 can be used to make theft detection more certain. The audio alarm 530 in this case can be a household alarm system, coupled via mains signalling or RF, for example.

Figure 5 shows a graphical representation of a chain of parties involved in some types of consumer equipment, and will be referred to in conjunction with the following description of some of the effects of some of the embodiments of the anti theft systems of the invention. Component makers 610 can benefit from added value components, from running associated services, and from improved brand image. Such makers feed consumer equipment makers 620, who can see similar benefits, and benefits from product differentiation. They feed retailers 630, who could benefit from greater sales and reduced theft from their premises. The consumer 660 clearly

benefits from reduced theft, with consequences such as reduced insurance costs and improved sense of security. Also feeding the consumer are insurance companies 690, and alarm installers 650. The latter could see a larger market for related products and services, and fewer costs from false alarms. Corresponding benefits can arise for security system makers 640, supplying the installers.

Clearly the potential thieves 680 suffer from increased risk of capture, and greatly reduced value of stolen goods if they show they are stolen, and are disabled. The "fence" or receiver 670 who buys the stolen goods also suffers from the higher risk of capture, greater difficulty in "cleaning" the goods to try to remove evidence that it is stolen. All this leads to benefits to the police or private security firms 700, of reduced false alarms, higher detection rates, and reduced crime. As government 710 is ultimately responsible, it benefits from improved policing results, and from reduced tax and duty evasion from trade in stolen goods, and from more votes from a more contented electorate.

Figure 6 shows another embodiment, this time related to applying similar principles to a different problem, that of managing valuable portable equipment 740 for shared usage or for rental. Here there are benefits from indicating the status of the equipment on it. For example, hospitals or schools share much valuable equipment between many users, but once the equipment has been removed from a central store, it can be hard or expensive to keep track of who is responsible for it, or how long they have had it or how much time or usage is authorised. Likewise for rented equipment. Where the portable equipment is coupled to a network 750 for recharging, or for maintenance, the disconnection or removal from the network can be detected by a detector 710, and used to update the indicator 720, in the form of a status display and/or RF transmitter. To be more trustworthy, the indication should be tamper resistant, but resettable, using a secure reset process 790. A master key 730 for enabling the reset, can be controlled by the equipment owner. As shown in the figure, maintenance or security staff or auditors 760 can use the indication of status on the equipment, to provide a more up to date and reliable indication than paper records for example. Personnel or detectors at

boundaries of sites or permitted areas can be used to detect the indications and determine manually or automatically whether equipment has authorisation to pass.

In the case of rented equipment including rented media, such as books, video or audio or games discs or cartridges, these can have a miniature tag with a system on a chip attached to them permanently, and with a small display if the size of the cartridge, disc or packaging permits. At the rental shop, they can be coupled to a shop inventory network by RF or other connection. Disconnection can be detected automatically, and the tag can be updated at that time with a record identifying the renter and a time or amount of usage authorised. At any time the tag can be interrogated. The renter can be provided with a detector with a display, to enable the renter to see at any time how long the item has been rented for and so on.

Concluding remarks: Other variations will be apparent to those skilled in the art, within the scope of the claims. As has been described above, the anti-theft system for consumer equipment has a detector for detecting theft by detecting disconnection of the consumer equipment from a network for power supply or for information transfer. This is used to cause a stolen status indication on the consumer equipment. The indication can be a display or RF transmission, and is persistent to deter possession of the equipment, but being removable by a secure reset process. This indication makes it riskier for a thief to possess stolen equipment that shows its stolen state, even when switched off, and even after lengthy storage. It is also harder to sell the stolen goods and hence it can deter theft. Similar principles can be applied to indicate on rented or shared equipment, status including current user, of the equipment.

CLAIMS

1. An anti-theft system (40) for consumer equipment, the equipment in normal use having a connection to a network for power supply or for information transfer, the system having:

a detector (10) for detecting disconnection of the consumer equipment indicating theft of the equipment, and

the system being arranged to respond to such a detection by causing a stolen status indication on the consumer equipment the indication being autonomous of the equipment being switched off, and being persistent to deter possession of the equipment, but being removable by a secure reset process (100).

2. The system of claim 1 the indication comprising a visible display (460).

3. The system of claim 2, the display being a low power operating display of the consumer equipment.

4. The system of any preceding claim, the indication comprising an RF signal, or the enabling of a passive RF tag (495).

5. The system of any preceding claim, having an internal battery (500) to power the indication.

6. The system of any preceding claim, having a tampering detector for detecting tampering with the system (450).

7. The system of claim 6 arranged to disable the equipment permanently, in the event of detecting tampering (370).

8. The system of any preceding claim arranged to output the indication intermittently, or only when movement is detected (390).

9. The system of any preceding claim, arranged to output an identifier traceable to the rightful owner.

10. The system of any preceding claim, containing a unique key and arranged to receive another key (30) and verify whether it is a matching key, to enable the reset process, or enable operation of the equipment.

11. The system of any preceding claim, arranged to store permanently an audit trail of detection events (350).

12. A display module (440) for consumer equipment, the module having the system of any preceding claim.

13. Consumer equipment having the system of any of claims 1 to 11.

14. The consumer equipment of claim 13, being a computer, or a games console, or audio or video equipment for household or in- car use.

15. A method of offering a service (60) of providing a key on request for resetting the indication of theft as set by the system, module or equipment of any preceding claim, to a rightful owner of the equipment.

16. A method of detecting stolen equipment, the method having the step of using an RF receiver (70) to recognise an RF indication of a stolen status output by the consumer equipment of claim 13 or 14 when dependent on claim 4.

17. Software for consumer equipment, the equipment in normal use having a connection to a network for power supply or for information transfer, the software being coupled to a detector (470) for detecting disconnection of the consumer equipment indicating theft of the equipment, and being

arranged to respond to such a detection by causing (340) a stolen status indication on the consumer equipment, the indication being autonomous of the equipment being switched off, and being persistent to deter possession of the equipment, but being removable by a secure reset process (100).

18. A management system for monitoring use of portable equipment, the equipment being available for use by many users, the system having:

a detector (710) for detecting removal of the equipment from a store, where the equipment is connected to a network for power supply or information transfer and

an indicator (720) coupled to the detector for providing an indication on the equipment of its status following a detection of removal, including which of the users was responsible for taking it from the store.

19. The management system of claim 18, the indication including an indication of a time limit or usage limit.

20. The management system of claim 18 or 19, and having the features set out in any of claims 2 to 11.

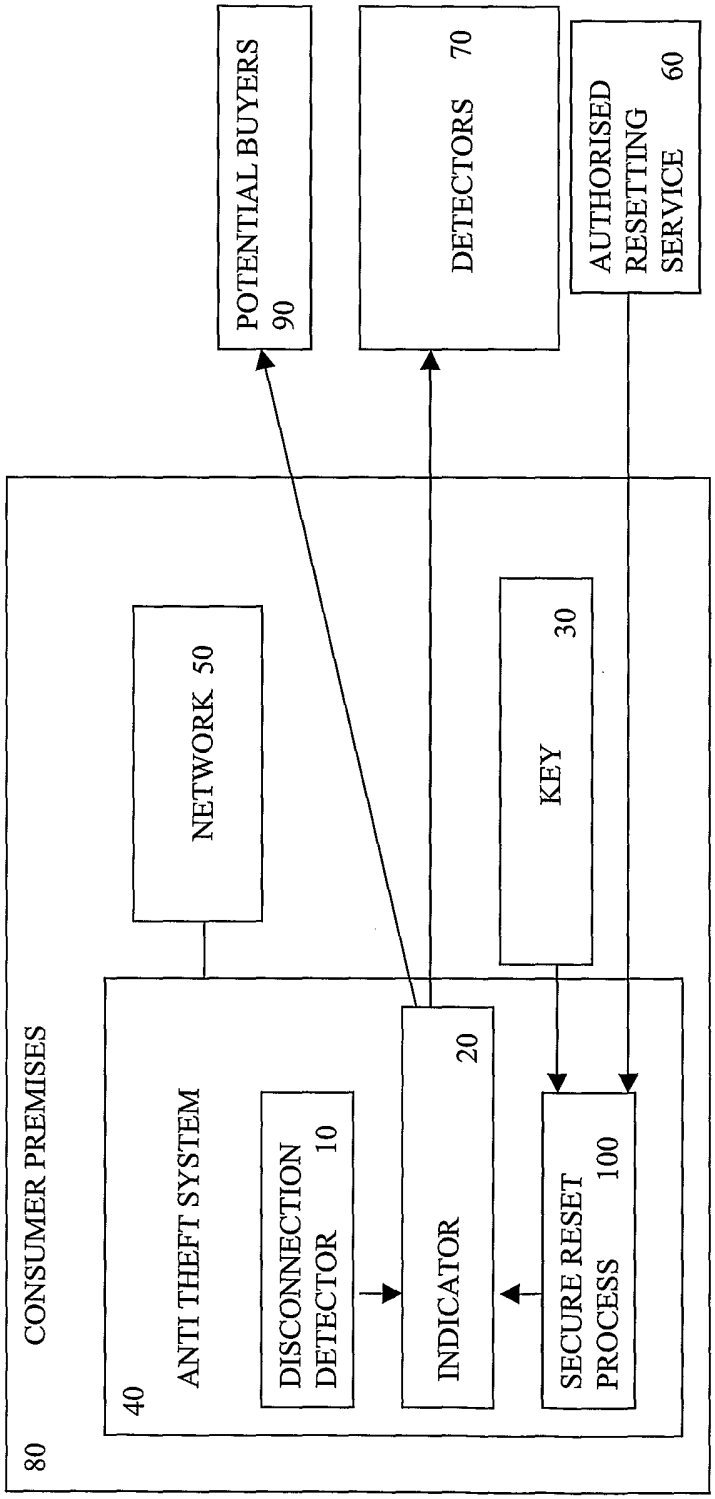

POTENTIAL BUYERS 90
DETECTORS 70
AUTHORISED RESETTING SERVICE 60
CONSUMER PREMISES 80
NETWORK 50
KEY 30
ANTI THEFT SYSTEM 40
DISCONNECTION DETECTOR 10
INDICATOR 20
SECURE RESET PROCESS 100

FIG.1

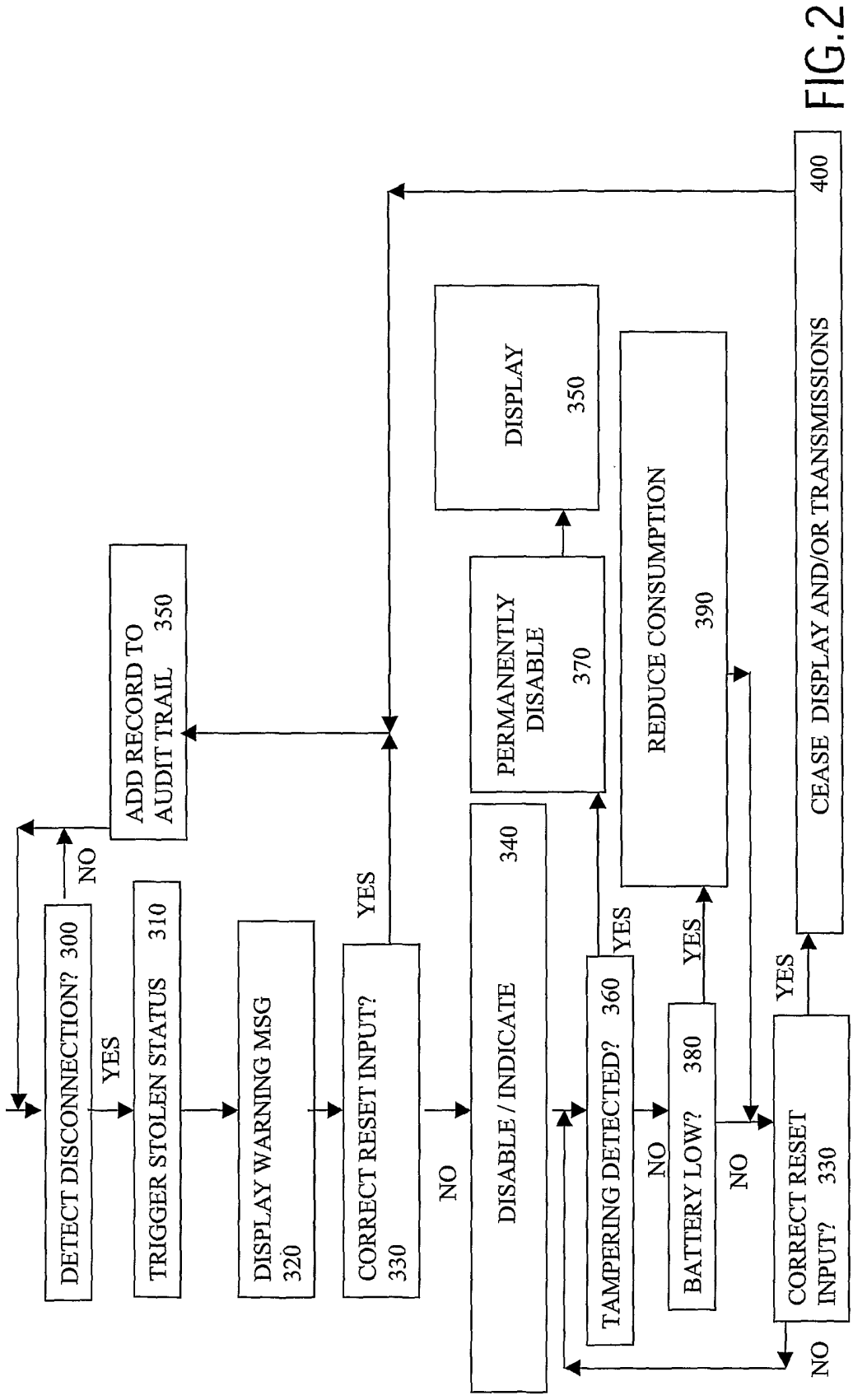

DETECT DISCONNECTION? 300
NO
YES
ADD RECORD TO AUDIT TRAIL 350
TRIGGER STOLEN STATUS 310
DISPLAY WARNING MSG 320
CORRECT RESET INPUT? 330
YES
NO
DISABLE / INDICATE 340
PERMANENTLY DISABLE 370
DISPLAY 350
TAMPERING DETECTED? 360
YES
NO
REDUCE CONSUMPTION 390
BATTERY LOW? 380
YES
NO
CORRECT RESET INPUT? 330
YES
NO
CEASE DISPLAY AND/OR TRANSMISSIONS 400

FIG.2

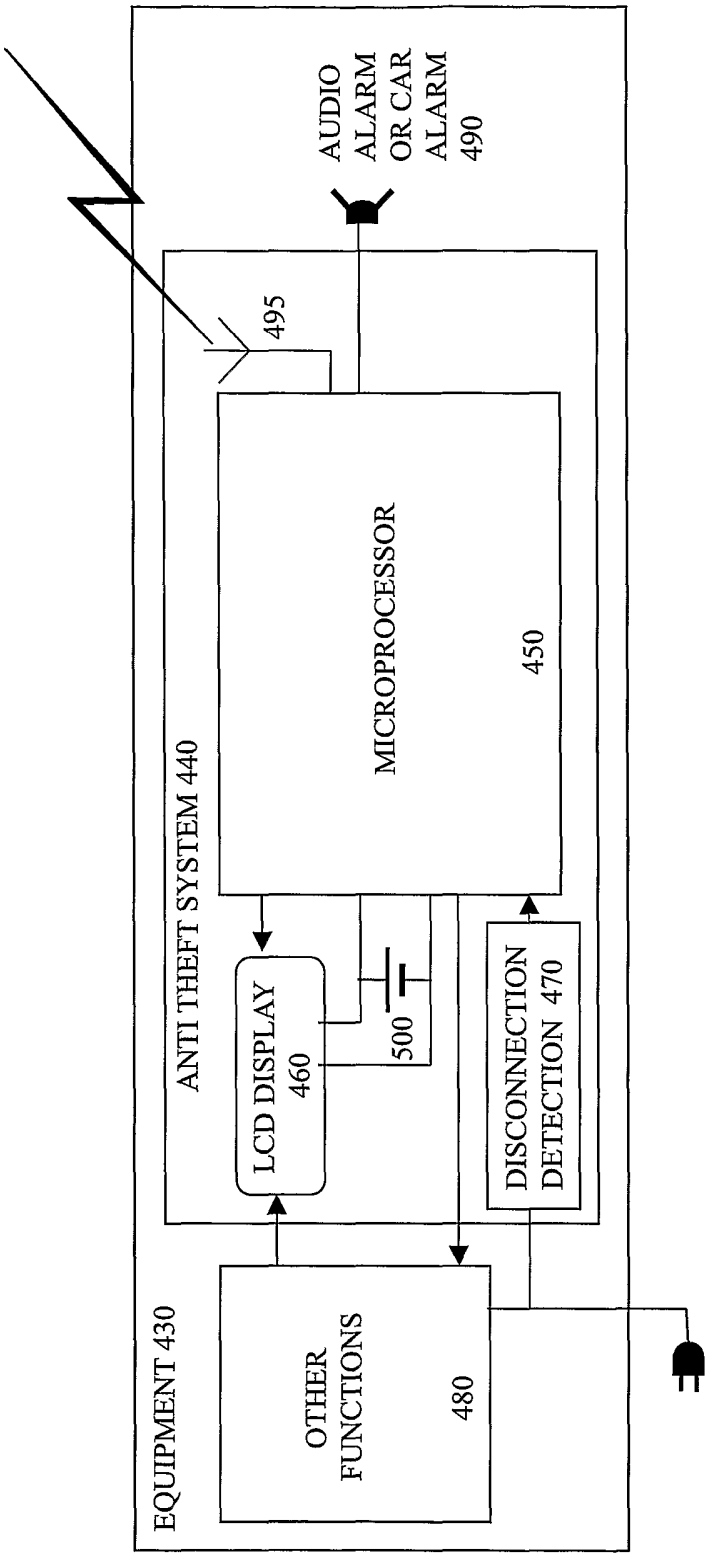

AUDIO ALARM OR CAR ALARM 490
495
MICROPROCESSOR
450
ANTI THEFT SYSTEM 440
LCD DISPLAY 460
500
DISCONNECTION DETECTION 470
OTHER FUNCTIONS
480
EQUIPMENT 430

FIG.3

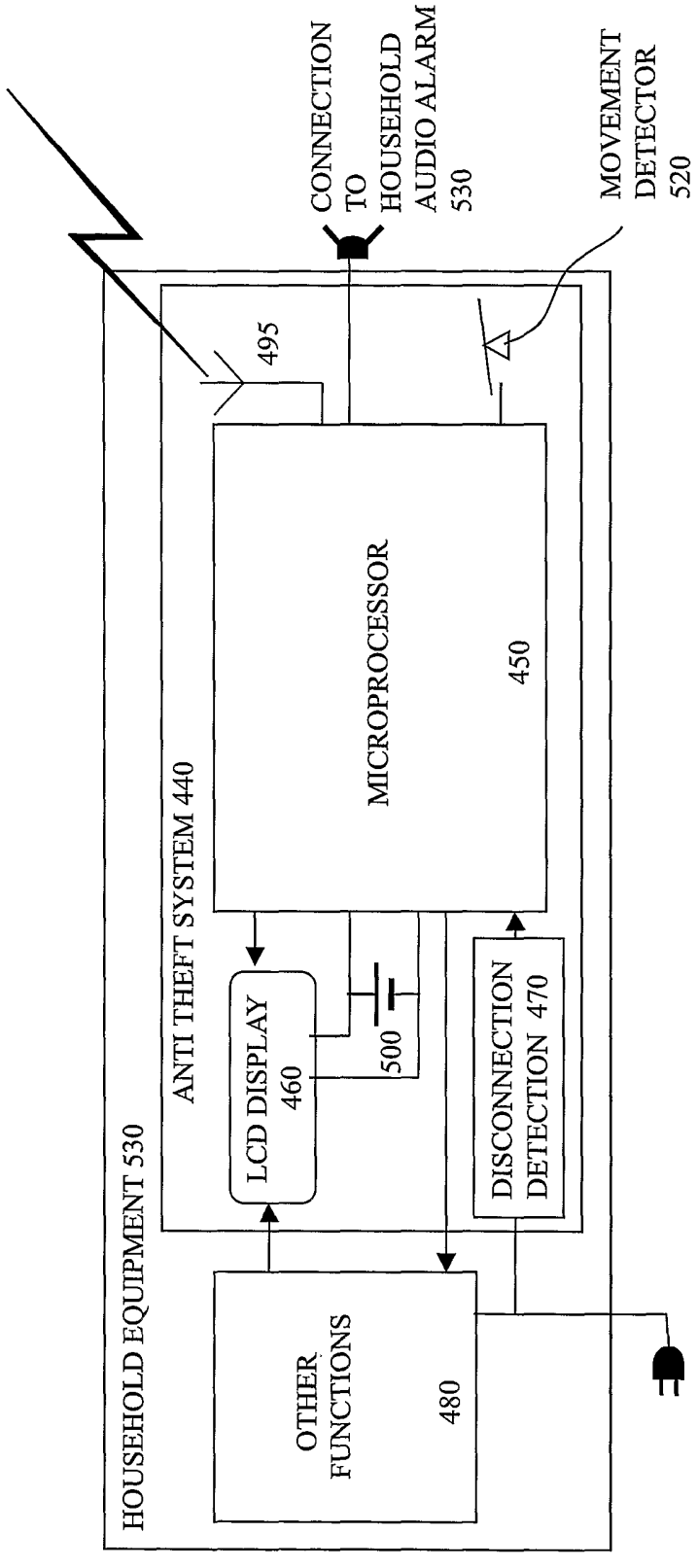

CONNECTION TO HOUSEHOLD AUDIO ALARM 530
MOVEMENT DETECTOR 520
495
HOUSEHOLD EQUIPMENT 530
ANTI THEFT SYSTEM 440
MICROPROCESSOR
450
LCD DISPLAY 460
500
DISCONNECTION DETECTION 470
OTHER FUNCTIONS
480

FIG.4

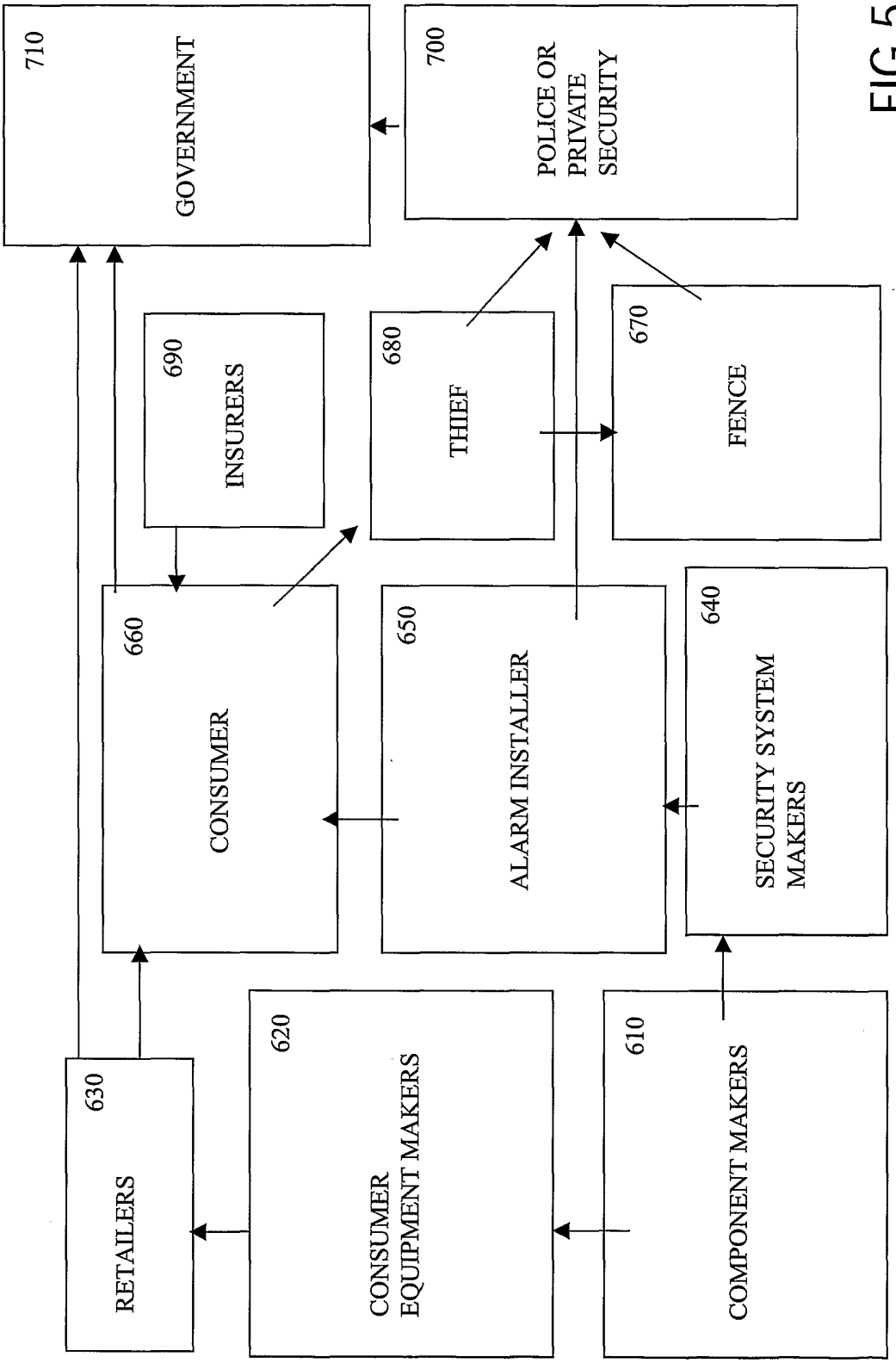

710
GOVERNMENT
700
POLICE OR PRIVATE SECURITY
690
INSURERS
680
THIEF
670
FENCE
660
CONSUMER
650
ALARM INSTALLER
640
SECURITY SYSTEM MAKERS
630
RETAILERS
620
CONSUMER EQUIPMENT MAKERS
610
COMPONENT MAKERS

FIG.5

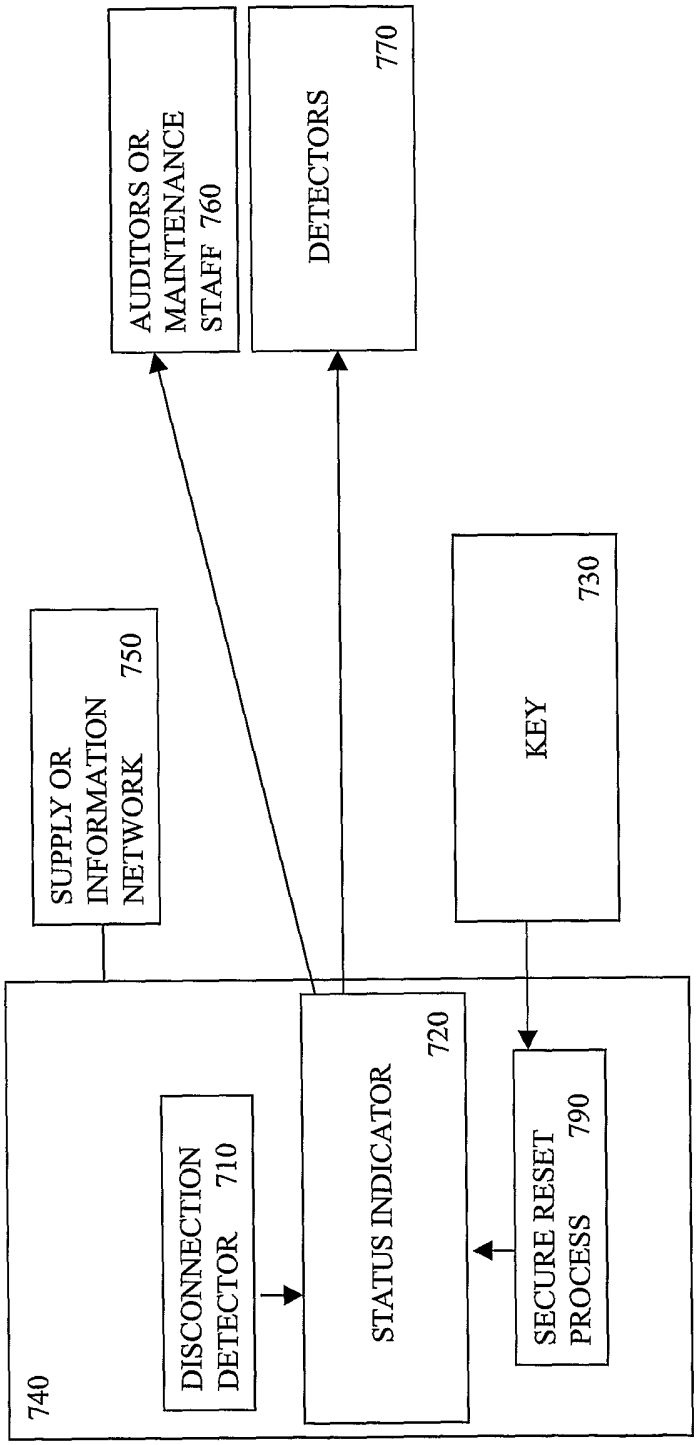

AUDITORS OR MAINTENANCE STAFF 760
DETECTORS 770
SUPPLY OR INFORMATION NETWORK 750
KEY 730
740
DISCONNECTION DETECTOR 710
STATUS INDICATOR 720
SECURE RESET PROCESS 790

FIG.6