United States Patent [19]

Hedin

[11] **3,851,227**

[45] **Nov. 26, 1974**

[54] **SECURITY APPARATUS INCLUDING A TAMPER DETECTION DEVICE**

[75] Inventor: **Robert A. Hedin,** Novi, Mich.

[73] Assignee: **Eaton Corporation,** Cleveland, Ohio

[22] Filed: **Mar. 16, 1973**

[21] Appl. No.: **341,941**

[52] **U.S. Cl.** ..... **317/134,** 317/148.5 R

[51] **Int. Cl.** **E05b 49/00,** H01h 47/32

[58] **Field of Search** ..... 317/134; 340/147 MD

[56] **References Cited**

UNITED STATES PATENTS

3,562,596	2/1971	Scheuer	317/134
3,754,213	8/1973	Morroni	317/134

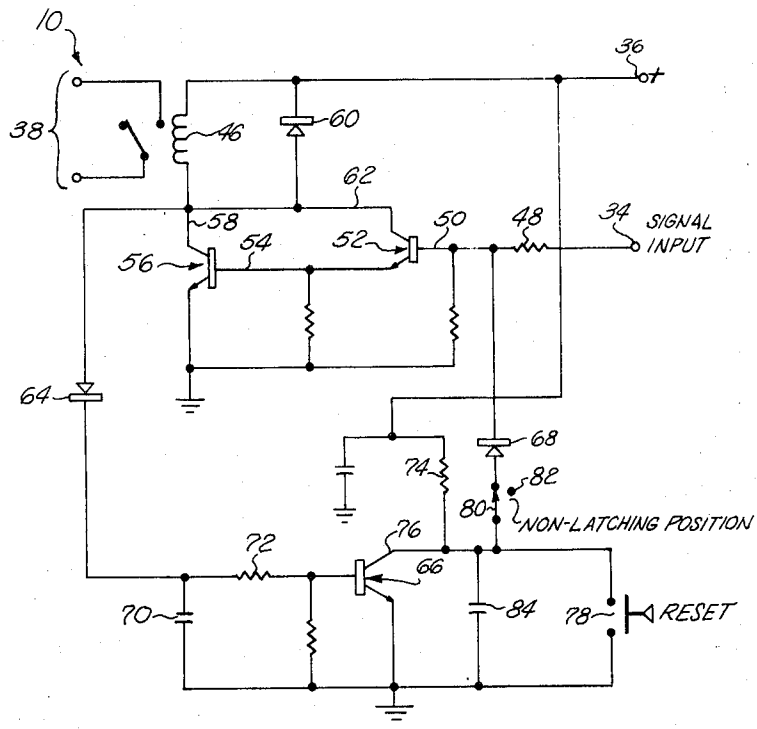
Primary Examiner—L. T. Hix

Attorney, Agent, or Firm—Teagno & Toddy

[57] **ABSTRACT**

A key actuated electronic security system such as a door lock to which a proper combination of binary signals must be applied by a valid key has a tamper detection device which is especially sensitive to attempts to pick the lock by making measurements or applying voltages at an input keyway. The device responds with an alarm upon application of improper signals to the input keyway of the security system, even when the spurious signals are supplied by a picking device applying voltages having very little power capability. Moreover, spurious signals of abnormally high power level are prevented from damaging and disabling the alarm device. The device can selectively operate in a latching mode wherein the alarm persists after the spurious signal that caused it has ceased until the system is intentionally reset, or in a non-latching mode in which the alarm signal ceases upon cessation of the spurious signal.

9 Claims, 2 Drawing Figures



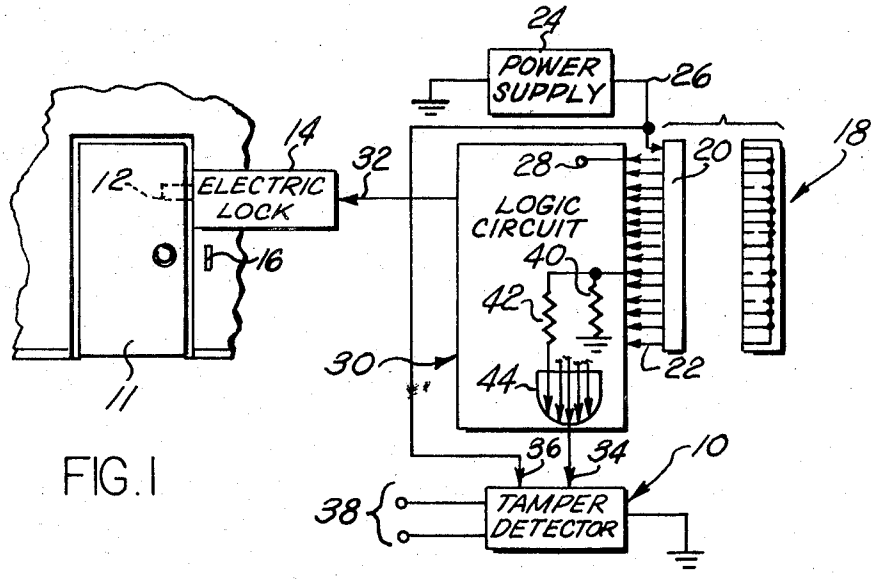
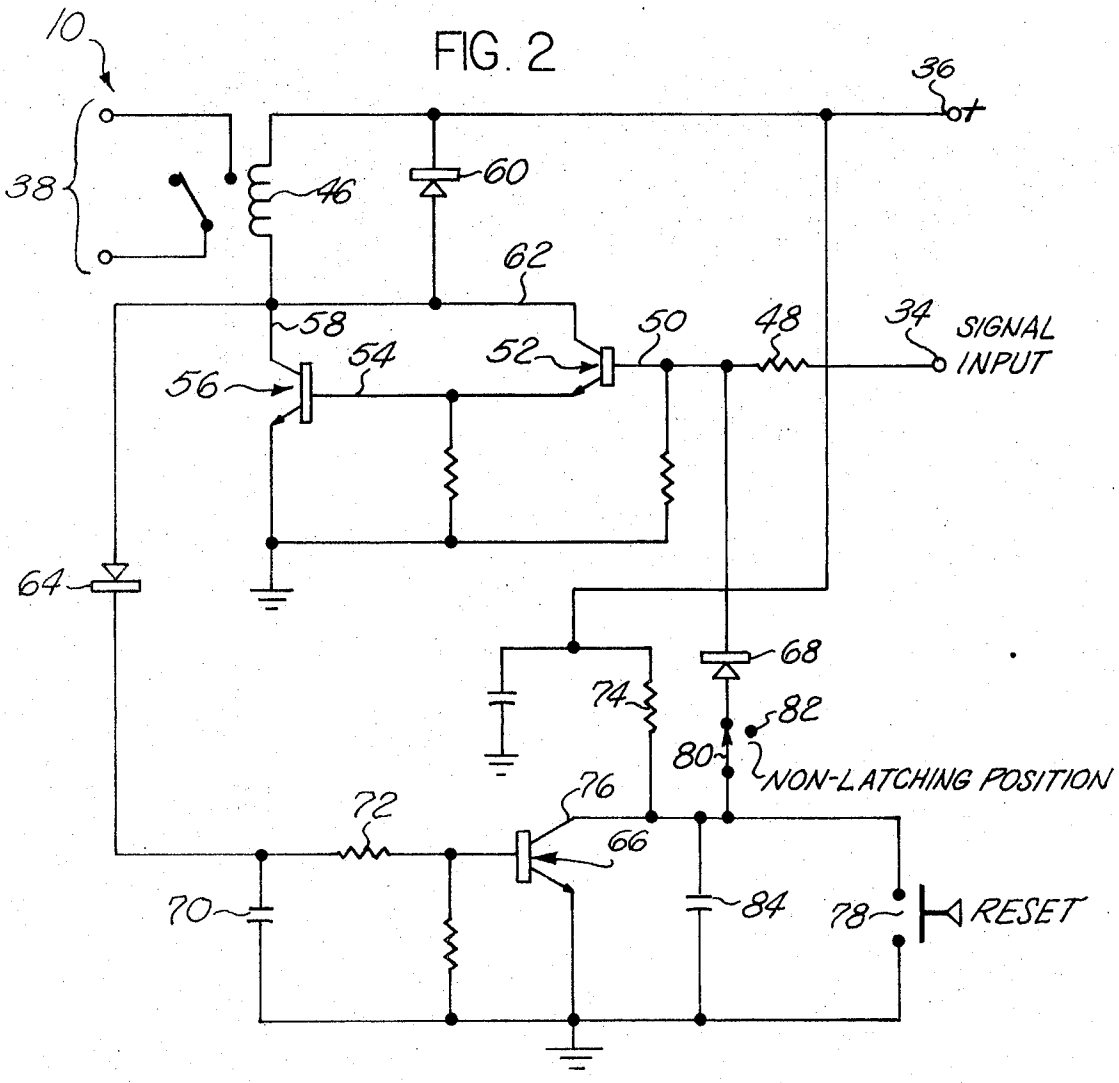

24
POWER SUPPLY
26
14
32
12
ELECTRIC LOCK
16
28
20
18
LOGIC CIRCUIT
40
42
30
44
22
11
36
34
10
38
TAMPER DETECTOR

FIG. 1

FIG. 2


10
36
38
46
60
62
58
50
48
34
SIGNAL INPUT
56
54
52
64
68
74
82
80
NON-LATCHING POSITION
72
76
66
70
84
78
RESET

SECURITY APPARATUS INCLUDING A TAMPER DETECTION DEVICE

BACKGROUND OF THE INVENTION

A key actuated electronic security system was disclosed in a patent to R. A. Hedin et al., Re.27,013, reissued on Dec. 22, 1970. That patent relates to security systems such as could be used for entrance door locks and the like, and more particularly to a key actuated electronic security system employing keys having electrical contacts which are permuted in a binary code to create various combinations of keys and electronic key responsive locks. In a typical installation of such a system, a key receptacle is located in a conveniently exposed position adjacent a door which is to be locked. Keys are provided which, when inserted in the key receptacle, perform switching functions at a plurality of circuit paths in the key receptacle. A proper key performs a predetermined proper combination of switching operations in the key receptacle, whereupon internal decoding circuitry causes an electrically operated lock to unlock the door. Keys having an incorrect combination, or other picking devices, are recognized by the system, which is not actuated by them. The system causes an alarm signal when some picking devices are employed. Prior to the present invention, some picking techniques in which voltages are applied at the key receptacle, were not recognized by the equipment as tampering, and did not cause an alarm, because the external source of the picking voltage was not powerful enough to actuate the relatively insensitive tamper-detection devices then being used. The present invention relates to improvements in the tamper detection and alarm apparatus that is used with key actuated electronic security systems to more effectively foil attempts to pick the lock with techniques involving the application of electrical voltages to the key receptacle. The present invention is also responsive to attempts to pick the lock by improper keys or external switches, as were the systems of the prior art.

SUMMARY OF THE INVENTION

The present invention is a key-actuated electronic security system having a tamper detection circuit which is connected to a decoder of the security system. The tamper detection device receives signals from the decoder, which were applied to an input keyway of the security system and which do not fit the pattern of proper or authorized signals such as would be expected from insertion of a legitimate key. The improper signals are conducted through a buffer resistance to a two-stage transistor amplifier whose output drives an alarm-controlling device such as a relay. The amplifier has a high degree of invulnerability to damage from improper signals of excessive voltage levels, and at the same time it is unusually sensitive not only to strong signals, but to very weak input signals, to create an alarm output signal when they occur. The uses of both passive picking circuits such as improperly encoded keys, or active picking circuits such as external voltage sources, are detected. The tamper detection device also has a completely static latching system which causes the output alarm signal to continue even after a signal which initiated it has ceased. The latching capability can be disabled by means of switching if desired.

Accordingly, one object of the present invention is to provide a key actuated electronic security system having a tamper detection device to detect when improper entry is attempted with a relatively high impedance low power source of voltages from a picking device.

Another object is to provide a system having a tamper detection device which, upon tampering, produces an alarm and latches the alarm in an ON condition to persist after the signal which initiated the alarm ceases, the latching circuit being a static type without mechanically moving parts.

Yet another object of the present invention is to provide a system having a tamper detection device that is selectively capable of either latching upon occurrence of an improper signal to cause a persistent alarm, or of operating in a non-latching mode in which the alarm signal ceases when the improper signal ceases.

An additional object is to provide a system having a tamper detection device which, when energized by application of supply power, rises in a non-latched state; that is, the device is automatically properly initialized.

A further object is to provide a system having a tamper detection device which is extraordinarily invulnerable to being disabled or damaged when abnormally high voltages are applied to the electronic security apparatus during attempted improper entry.

Still another object is to provide a system having a tamper detection device which is sensitive to occurrence of an improper input signal irrespective of whether or not a proper key is inserted.

BRIEF DESCRIPTION OF DRAWINGS

FIG. **1** is a block diagram of a key actuated electronic security system of a type disclosed in the prior art.

FIG. **2** is a schematic circuit diagram of a preferred embodiment of a tamper detection and alarm device for use with the system of FIG. **1.**

DESCRIPTION

As shown in FIG. **1,** a door **11** is equipped with a locking bolt **12** which is moved in and out of locking engagement with the door **11** by an electric lock device **14.** At a location **16** near the door, provision is made for insertion of a special key **18** which is shown diagrammatically at the right side of FIG. **1.** To unlock the door **11,** the key **18** is inserted at location **16** into a key receptacle **20** in which the key **18** performs switching functions by making contact with input conductors **22** in the key receptacle **20.** A power supply **24,** which can be turned on and off, provides DC electrical power for a logic circuit portion **30** of the key actuated security system when a key **18** is inserted in the key receptacle **20,** the key **18** establishing a circuit path from a power supply output lead **26** to a load input lead **28** for the logic circuit **30.** In addition, the key **18,** when inserted in the key receptacle **20,** establishes circuit paths from the power supply output lead **26** to selected other ones of the input conductors **22** in accordance with a predetermined permutation of continuous and discontinuous conductors on the key **18** corresponding to each of the input conductors **22.**

The input conductors **22** conduct a binary pattern of signals established by the key **18** to the decoding logic circuit **30** which automatically examines the pattern of signals on the input conductors **22** and supplies a signal on a line **32** to the electric lock **14** to unlock the door

11 when a proper authorized key 18 has been inserted.

When an unauthorized key is inserted in the key receptacle 20, an improper pattern of electrical signals is applied to the input conductors 22 and the electric lock 14 does not operate to unlock the door. The decoding logic circuit 30 is designed to minimize the probability that the door 11 can be unlocked by the application of spurious signals of any type to the input conductors 22 from an unauthorized key or other picking device. Such other devices include a source of external voltage arranged for application at the key receptacle 20, in an attempt to pick the lock 14. Certain types of improper signals at the input conductors 22 produce a signal at a terminal 34 of a tamper detection circuit 10, which is the subject matter of the present invention. The power supply voltage appears on another terminal 36 of the tamper detection device 10 regardless of whether or not the lead 28 is energized. Consequently, it is not necessary to insert a key 18 in the keyway 20 to make the tamper detection device alert to tampering. The tamper detection device 10 has output terminals 38 which are provided for operating an audible or visible alarm device or an information circuit indicating that an attempt is being made or has been made to pick the lock 14.

Those ones of the input conductors 22 which are not energized by the power supply 24 when a proper key 18 is inserted in the key receptacle 20 are employed both to assist in the controlling of the lock 14 and to provide input signals at the terminal 34 for the tamper detection device 10. These particular input conductors 22 are referred to herein as the false input conductors, while those conductors 22 to which a power supply voltage is applied by an authorized key are termed the true input conductors.

Each of the false input conductors is connected to a shunt resistor such as resistor 40 and through a series resistor such as resistor 42 to an OR gate 44. All of the false inputs are connected in a similar manner in common to the OR gate 44. The OR gate 44 can be a diode OR gate of a type well known in the prior art. The presence of a spurious voltage signal on any of the false input conductors 22 produces a signal at the terminal 34 of the tamper detection device 10.

FIG. 2 shows the principal subject matter of the present invention, which is the tamper detection device 10. The power supply input signal 36 is energized by a power supply voltage whenever the power supply 24 is energized. The output terminals 38 of the tamper detection device 10 are seen in FIG. 2 to be connected within the device to contacts of an output relay 46, which is energized whenever an alarm is to be indicated. A spurious signal created by an attempt to pick the lock 14 appears at the signal input terminal 34.

Spurious signals at the input signal terminal 34 are conducted through a series resistance 48 to the base 50 of a first transistor amplifier 52. A signal current at the base 50 is amplified by the transistor 52, and the amplified current is conducted from the emitter of the transistor 52 to the base 54 of a second transistor amplifier 56, where it is further amplified. Upon a spurious signal at the signal input terminal 34, current at a collector terminal 58 of the second transistor amplifier 56 flows through the coil of the relay 46. If the current in the coil exceeds a predetermined amount, the relay is energized to operate relay contacts that are connected to the output terminals 38. A protective diode 60 is connected in parallel with the coil of the relay 46, as is conventional. Spurious signals as small as one-tenth of the current level of normal legitimate signals are sufficient to cause an alarm.

Upon a spurious signal at the signal input terminal 34, the electrical potential of the collector 62 of the first transistor amplifier 52 decreases to a relatively low value because of an increased voltage drop in the coil of the relay 46. The voltage drop results from increased collector current in both the first and second transistor amplifiers, 52, 56, but especially from the larger current of the second transistor amplifier 56. This reduction of voltage at the collector 62 with respect to the emitter of the transistor 52 greatly reduces the power dissipation in the collector circuit of the transistor 52. At the same time the current limiting action of the large series resistor 48 protects the transistor 52 from thermal overloads due to base current, even when abnormally large picking voltages are applied to the input conductors 22. The tamper detection device itself is thereby made resistant to being disabled by high picking voltages.

FIG. 2 also shows a feedback circuit comprising a diode 64, a transistor 66, and a diode 68. Prior to the occurrence of a spurious signal at the input terminal 34, the diode 64 conducts charging current to a capacitor 70 in the feedback circuit and through a resistance 72 to the base of the transistor 66. This causes the transistor 66 to conduct current in its collector-emitter circuit through a resistor 74 connected from the power terminal 36 to the collector 76. This current flowing in the resistor 74 produces a low voltage at the collector terminal 76 of the transistor 66, so that the potential of the collector 76 is nearly equal to the potential of the emitter of the transistor 66, which is at ground potential.

Upon the occurrence of an alarm signal at the collector terminal 58, current flow through the diode 64 ceases. The capacitor 70 supplies current for a brief time delay through the resistor 72 to the base of the transistor 66. When the charge on the capacitor 70 becomes almost exhausted, the transistor 66 stops conducting collector current, and the voltage of its collector terminal 76 rises to a value close to the value of the power supply voltage. The diode 68 thereupon conducts current from the terminal 76 to the base terminal 50 of the first transistor amplifier 52.

The current through the diode 68 serves as a substitute input signal, which maintains the alarm signal at the output terminals 38 even after the initial input signal at the terminal 34 has ceased. The alarm circuit is seen to have latched in an alarm condition; it remains latched until the voltage of the terminal 76 is short circuited to ground by manual closing of a reset switch 78.

The tamper detection device 10 can be operated without the latching feature by placing a mode selection switch 80 in a non-latching position 82 so as to interrupt the current path of the diode 68. In the non-latching mode, the alarm signal at terminals 38 stops when the initial input signal at terminal 34, which caused the alarm, stops.

The tamper detection device 10 is prevented from being initially energized in a latched state when the power supply 24 is turned on. The resistor 74 together with a capacitor 84 which is connected from terminal

76 to ground produce a time delay in the rise of voltage at the terminal 76 following an application of voltage at the power terminal 36 upon energization of the power supply 24. No current flows in the diode 68 during the time delay. The tamper detection device 10 is therefore automatically initialized by the resistor 74 and the capacitor 84 in an unlatched condition, so that an improper signal is necessary at the signal input terminal 34 in order to latch the device. The transistor 66 can conduct discharge current from capacitor 84 without damage.

While the invention has been illustrated and described in terms of one particular embodiment, it is not intended to be limited to the details shown therein, since various modifications, omissions and structural changes may be made without departing in any way from the scope of the invention.

What is claimed is:

1. An improved key-actuated electronic security apparatus of the type wherein a lock and decoding logic circuit are provided with the decoding logic circuit having a plurality of input conductors to which a proper combination of binary signals must be applied by a key to identify a valid key, wherein the improvement comprises an improved tamper-detection device including input circuit means having an input junction communicating with said plurality of input conductors for receiving signal current therefrom indicative of an attempt to actuate the apparatus without a valid key, a semiconductor amplifier having an input electrode receiving the signal current for amplifying it above a predetermined level, output means connected with said semiconductor amplifier for producing alarm indicia when the amplified signal exceeds the predetermined level, said semiconductor amplifier having sufficient gain that said alarm indicia are produced by values of said signal current at said input conductors substantially lower than a current produced at a proper one of said input conductors by a proper one of said binary signals, latching means, connected to the input electrode of said amplifier, to provide a control signal to said amplifier sufficient to produce the alarm indicia from said output means, and first switching means connected to said latching means to actuate said latching means whenever said output means initially produces the alarm indicia.

2. An improved security apparatus as defined in claim 1 and wherein said input circuit means further comprises a series impedance element intermediate said input junction and said semiconductor amplifier for limiting the signal current conducted from the junction, and wherein said semiconductor amplifier comprises amplifier stages arranged for multiplication of their individual gains to produce the gain of the amplifier.

3. An improved security apparatus as defined in claim 1 and wherein said latching means further includes a second switching means for selectively blocking and transmitting the control signal from said latching means to said semiconductor amplifier.

4. An improved security apparatus as defined in claim 1 and further comprising power supply means for energizing said tamper detection device with supply power irrespective of whether or not binary signals are applied to said input conductors.

5. An improved key-actuated electronic security apparatus of the type wherein a lock and a decoding logic circuit are provided with the decoding logic circuit having a plurality of input conductors to which a proper combination of binary signals can be applied by a key to identify a valid key, wherein the improvement comprises an improved tamper-detection device including input circuit means having an input terminal for receiving an initial signal current from the security apparatus indicative of an attempt to actuate the apparatus without a valid key, an amplifier having an input connected with a junction at said input circuit means and producing an alarm signal at an output upon said initial signal, static feedback circuit means receiving said alarm signal and connected for providing a sustaining input signal for said amplifier upon occurrence of the alarm signal at the output to effectively latch the alarm signal to persist after the initial signal current ceases, said static feedback circuit means comprising switching means for selectively blocking and transmitting said sustaining signal to respectively disable and enable the latching capability of the alarm device.

6. An improved security apparatus as defined in claim 5 and wherein said input circuit means comprises a linear series-connected resistance means intermediate said input terminal and said amplifier for conducting the initial signal to said junction and wherein said static feedback circuit means comprises means for providing said sustaining input signal through a semiconductor to said junction for communication to said input of the amplifier.

7. An improved key-actuated electronic security apparatus of the type wherein a lock and decoding logic circuit are provided with the decoding logic circuit having a plurality of input conductors to which a proper combination of signals of predetermined voltage levels can be applied for system actuation by a proper key, wherein the improvement comprises an improved tamper-detection device including a current limiting impedance connected intermediate the input conductors and a first terminal for limiting the flow of improper input current from the input conductors to the first terminal, a first semiconductor amplifier having an input current electrode connected to receive current from said first terminal and having other electrodes for carrying amplified current, a second semiconductor amplifier receiving an amplified current signal from said first amplifier and causing an alarm signal thereupon as an output, circuit means responsive to occurrence of the alarm output signal for decreasing a voltage applied to one of said other electrodes with respect to another electrode of said first amplifier to reduce substantially the power dissipation of said first amplifier thereupon, said current limiting impedance preventing an improper picking voltage exceeding the predetermined voltage levels from disabling the alarm device, and static feedback circuit means connected to the output of said second semiconductor amplifier to receive said alarm signal and establish a sustaining input signal to said first semiconductor amplifier upon reception of the alarm signal output to effectively latch the alarm signal and allow the alarm signal to continue after the picking voltage has been removed.

8. An improved key-actuated electronic security apparatus of the type wherein a lock and a decoding logic circuit are provided with the decoding logic circuit having a plurality of input conductors to which an authorized key can apply a proper pattern of electrical signals to actuate the apparatus, wherein the improve-

ment comprises an improved tamper-detection device including input circuit means for transmitting improper signals applied to the input conductors to a first terminal of the tamper-detection device, an amplifier having an input connected with said first terminal and an output for producing an alarm signal upon said improper signals, static latching means including a static feedback circuit for providing a maintaining signal to the amplifier in response to said alarm signal, a voltage supply input for the tamper-detection device that is energized when the key is employed, and time delay means for disabling said static latching means until the expiration of a delay following energizing of said voltage supply input to prevent latching in the absence of said improper signals, said time delay means including capacitor means for producing said delay starting when said voltage supply is energized.

9. An improved security apparatus as defined in claim **8** and wherein said current limiting impedance comprises a resistance connected in series intermediate said input conductors and said first terminal, and wherein said first semiconductor amplifier is a transistor amplifier, and said circuit means for decreasing a voltage comprises feedback means from the output of said second semiconductor amplifier for applying a latching signal to said first amplifier to latch the alarm signal.

* * * * *